STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **7**
to
Contract Number **MA071B7700119C**

CONTRACTOR	KnowBe4, Inc
	33 N Garden Ave
	Clearwater FL 33755-6604
	Sarah McHugh
	855-566-9234
	smchugh@knowbe4.com
	CV0135517

STATE	Program Manager	Various	DTMB
	Contract Administrator	Shane Desmier	DTMB
		517-246-8229	
		DesmierS@michigan.gov	

CONTRACT SUMMARY			
MCS Enterprise Security Awareness Training			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
March 28, 2017	March 28, 2022	5 - 12 Months	March 28, 2027
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
□ P-Card	□ Direct Voucher (PRC)	□ Other	□ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
□		□		

CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**
$1,007,930.00	$0.00	$1,007,930.00

DESCRIPTION

Effective 5/14/2025, Program Manager has been updated from Smurti Shah to Brandon Philip.

Please note the contract administrator has been changed to Shane Desmier.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Justin Fluharty	517-899-5977	FluhartyJ@michigan.gov
DTMB	Brandon Philip	517-749-7168	philipb@michigan.gov

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget

320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **6**
to
Contract Number **MA071B7700119C**

CONTRACTOR	KnowBe4, Inc
	33 N Garden Ave
	Clearwater FL 33755-6604
	Sarah McHugh
	855-566-9234
	smchugh@knowbe4.com
	VS0179188

STATE	Program Manager	Various	DTMB
	Contract Administrator	Sarah Platte	

CONTRACT SUMMARY			
MCS Enterprise Security Awareness Training			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
March 28, 2017	March 28, 2022	5 - 12 Months	March 28, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
☐ P-Card ☐ Direct Voucher (PRC) ☐ Other	☐ Yes ☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$987,930.00	$20,000.00	$1,007,930.00

DESCRIPTION

Effective 12/10/2024, the State adds $20,000.00 in funding to the Contract for future enhancements.

All other terms, conditions, specifications and pricing remain the same. Per Contractor, Agency, DTMB Central Procurement Services, and State Administrative Board approval on 8/20/2024.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Smruti Shah	517-582-4642	shahs1@michigan.gov
DTMB	Justin Fluharty	517-899-5977	FluhartyJ@michigan.gov

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES

Department of Technology, Management, and Budget

320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **5**
to
Contract Number **071B7700119**

CONTRACTOR	
	KnowBe4, Inc
	33 N Garden Ave
	Clearwater, FL 33755-6604
	Sarah Hughes
	855-566-9234
	smchugh@knowbe4.com
	VS0179188

STATE			
	Program Manager	Smruti Shah	DTMB
		517-582-4642	
		shahs1@michigan.gov	
	Contract Administrator	Jarrod Barron	DTMB
		(517) 249-0406	
		barronj1@michigan.gov	

CONTRACT SUMMARY

MCS ENTERPRISE SECURITY AWARENESS TRAINING

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
March 28, 2017	March 28, 2022	5 - 1 Year	March 28, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
☐ P-Card ☐ PRC ☐ Other	☒ Yes ☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		March 28, 2027

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$987,930.00	$0.00	$987,930.00

DESCRIPTION

Effective 1/19/2023, the parties add the additional tiered pricing detailed in the attached cost tables. All other terms, conditions, specifications and pricing remain the same. Per Contractor, Agency and DTMB Central Procurement Services approval. Remaining Ad Board funds after this CN: $290,049.99.

SLED Pricing for MiDeal

The below pricing is valid for one (1) year from the date of execution of this Contract Change Notice. All eligible MiDeal members MUST ask for the MiDeal pricing prior to purchasing. Discounts will not be refunded post-sale, nor applied to existing accounts or renewals of current KnowBe4 customers. Organizations with 24 users or less are only eligible to purchase the 3-Year Diamond subscription. All pricing below is expressed on a “per-seat” basis other than the “3-Year Diamond, 1-24 users” price, which is only available as a 3-year license that allows up to 24 users for a flat rate of $1647.00.

1 YEAR SLED PRICING						
Seats	Silver + SLED	Gold + SLED	Platinum+SLED	Diamond+SLED	PhishER+SLED	CMP + SLED
1-24	N/A	N/A	N/A	N/A	N/A	N/A
25-50	$16.20	$19.58	$22.95	$27.45	N/A	N/A
51-100	$14.40	$17.33	$20.25	$24.75	N/A	N/A
101-500	$11.70	$13.95	$16.20	$20.70	$9.90	$6.75
501-1000	$10.80	$12.83	$14.85	$19.35	$7.20	$5.85
1001-2000	$9.90	$11.70	$13.50	$18.00	$6.30	$5.18
2001-3000	$9.00	$10.58	$12.15	$16.65	$5.40	$4.50
3001-5000	$8.10	$9.45	$10.80	$15.30	$4.95	$3.83
5001-10000	$5.40	$6.53	$7.65	$9.00	$4.50	$3.15
10001-20000	$4.50	$5.40	$6.30	$7.20	$3.60	$2.48
20001-50000	$3.60	$4.28	$4.95	$5.85	$2.70	$1.80
50001-100000	$2.70	$3.15	$3.60	$4.50	$2.25	$1.35
100001+	$1.80	$2.25	$2.48	$3.15	$1.80	$0.90
3 YEAR SLED PRICING						
Seats	Silver + SLED	Gold + SLED	Platinum+SLED	Diamond+SLED	PhishER+SLED	CMP + SLED
1-24	N/A	N/A	N/A	$1647.00	N/A	N/A
25-50	$38.88	$46.98	$55.08	$65.88	N/A	N/A
51-100	$34.56	$41.58	$48.60	$59.40	N/A	N/A
101-500	$28.08	$33.48	$38.88	$49.68	$23.76	$16.20
501-1000	$25.92	$30.78	$35.64	$46.44	$17.28	$14.04
1001-2000	$23.76	$28.08	$32.40	$43.20	$15.12	$12.42
2001-3000	$21.60	$25.38	$29.16	$39.96	$12.96	$10.80
3001-5000	$19.44	$22.68	$25.92	$36.72	$11.88	$9.18
5001-10000	$12.96	$15.66	$18.36	$21.60	$10.80	$7.56
10001-20000	$10.80	$12.96	$15.12	$17.28	$8.64	$5.94
20001-50000	$8.64	$10.26	$11.88	$14.04	$6.48	$4.32
50001-100000	$6.48	$7.56	$8.64	$10.80	$5.40	$3.24
100001+	$4.32	$5.40	$5.94	$7.56	$4.32	$2.16

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
320 S. WALNUT STREET, LANSING, MI 48933

CONTRACT CHANGE NOTICE

Change Notice Number **4**
to
Contract Number **071B7700119**

CONTRACTOR	
	KnowBe4, Inc
	33 N Garden Ave
	Clearwater, FL 33755-6604
	Sarah Hughes
	855-566-9234
	smchugh@knowbe4.com
	VS0179188

STATE			
	Program Manager	Smruti Shah	DTMB
		517-582-4642	
		shahs1@michigan.gov	
	Contract Administrator	KeriAnn Trumble	DTMB
		(989) 259-2625	
		trumblek1@michigan.gov	

CONTRACT SUMMARY			
ENTERPRISE SECURITY AWARENESS TRAINING			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
March 28, 2017	March 28, 2022	5 - 1 Year	March 28, 2022
PAYMENT TERMS		DELIVERY TIMEFRAME	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
☐ P-Card	☐ PRC	☐ Other	☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☒	5 Years	March 28, 2027
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
$487,980.00	$499,950.00	$987,930.00		

DESCRIPTION

Effective 3/15/2022, this Contract is extended 5 years and is increased by $499,950.00. The revised contract expiration date is 3/28/2027. The following Master Service Agreement is also hereby incorporated into this Contract. These Terms and Conditions, together with all Schedules (including the Statement of Work), Exhibits and any other applicable attachments or addenda (Collectively this “Contract”) within this Master Service Agreement, are agreed to between the State of Michigan (the “State”) and KnowBe4 (“Contractor”) and it is the intent of the parties that the attached will replace, supersede, and otherwise eliminate the prior agreement between the State and KnowBe4. Per contractor and agency agreement, DTMB Central Procurement Services approval, and State Administrative Board approval on 3/15/2022.

MASTER AGREEMENT

This MASTER AGREEMENT ("**Agreement**") is effective as of the date of the last signature below ("**Effective Date**") by and between KnowBe4, Inc., a Delaware Corporation whose principal place of business is 33 N. Garden Ave., Suite 1200, Clearwater, Florida 33755, USA and its Affiliates (collectively, "**KnowBe4**"), and ______The State of Michigan__________________ ("**Customer**"), with a principal place of business at______________320 S. WALNUT STREET, LANSING, MI 48933____________________. Customer and KnowBe4 may be referred to in this Agreement individually as a "**party**" or jointly as the "**parties**". This Agreement governs all purchased Products and Services, as defined below, provided by KnowBe4 to Customer.

1. **Definitions.** For purposes of this Agreement:

"**Active User(s)**" means Customer's Users with active assigned Seats.

"**Affiliate**" means an entity that, directly or indirectly, through one or more entities, controls; is controlled by; or is under common control with, the specified entity.

"Beta Product" means the second phase of software testing in which a sampling of the intended audience samples a product prior to its general release and, in return, Customer provides KnowBe4 feedback about the Beta Product. Use of Beta Products by Customer is optional.

"**Confidential Information**" means all information or material disclosed by a party (the "**Disclosing Party**") to the other party (the "**Receiving Party**"), whether orally or in writing, which: (a) gives either party some competitive business advantage or opportunity of obtaining some competitive business advantage, or the disclosure of which may be detrimental to the interests of the Disclosing Party; and (b) is either (i) marked "Confidential," "Restricted," "Proprietary," or includes other similar markings, (ii) known by the parties to be confidential and proprietary, or (iii) from all the relevant circumstances should reasonably be assumed to be confidential and proprietary. The Products and Services are deemed Confidential Information of KnowBe4. Customer Data is deemed Confidential Information of Customer.

"Courseware" means training modules, games, posters, artwork, videos, newsletters, security documents, or other content and materials provided by KnowBe4.

"Direct Message Injection (DMI)" means a KnowBe4 product and add-on, specific to Microsoft 365 (formerly Office 365) that automatically bypasses Microsoft 365's protections to allow simulated phishing emails to reach the end user. Use of DMI by Customer is optional; in order to activate DMI, Customer must provide separate and specific permissions and authorizations in accordance with the Documentation. Customer has the ability to revoke any such access required to use DMI at any time. DMI is only applicable to Customers using Microsoft 365 for email.

"**Documentation**" means KnowBe4's then-current generally available documentation, specifications, user manuals, etc., for the Products and Services, located at https://knowbe4.zendesk.com/hc/en-us or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

"**LMS**" means learning management system that is software for the administration, documentation, tracking, reporting, and delivery of Courseware, which includes any e-learning education courses or training programs. KnowBe4 provides a cloud-based LMS through its Web Hosted Services. Upon approval by KnowBe4, Customer may also opt to use its own, or a third party's, LMS in accordance with the terms of this Agreement.

"PhishER™" means a KnowBe4 product that enables Customer to identify and respond to any potential threats in its email system. PhishER includes features such as PhishML and PhishRIP.

"PhishML™" means a feature included with a subscription to PhishER that uses machine learning to enable Customer to prioritize its evaluation of all user-reported emails for potential threats. This feature may be deactivated at Customer's option at any time.

"PhishRIP™" means a feature included with a subscription to PhishER that enables the Customer to quarantine and permanently delete specific emails (i.e., emails identified as potential threats) from its email system. Use of PhishRIP by Customer is optional; in order to activate PhishRIP, Customer must provide separate and specific permissions and authorizations in accordance with the Documentation. Customer has the ability to revoke any such access required to use PhishRIP at any time.

"**Product Privacy Notice**" means KnowBe4's Product Privacy Notice, that may be found at https://www.knowbe4.com/product-privacy-notice, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

"**Products**" means any Software, Services, Courseware, and/or Web Hosted Services that KnowBe4 offers to Customer, including any Documentation.

"**Product Support**" means any maintenance and support of any Products provided by KnowBe4.

"**Quote**" means a purchasing document or other similar document, such as a purchase order or statement of work ("**SOW**"), in connection with a purchase under this Agreement. The parties may attach a copy of the initial Quote as an exhibit to this Agreement. If such Quote is attached, the Quote will be deemed accepted upon execution of this Agreement.

"**Seat(s)**" refers to the number of Users permitted access to the Products and/or Services pursuant to the user count purchased via a Quote.

"Security Incident" means a breach of, or reasonably suspected, breach of security, confidentiality, integrity, or availability leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise processed.

"**Security Page**" means KnowBe4's security page that provides information about KnowBe4's information security practices which may be found at https://www.knowbe4.com/security, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

"**Services**" means any professional services, including implementation and installation services, managed services, consultancy services, or services for the customization or branding of Courseware, agreed upon by the parties, and set forth in a Quote or any additional Product Support purchased pursuant to a Quote. KnowBe4 may require Customer to enter into a statement of work ("**SOW**") detailing the Services to be performed.

"**Software**" means the object code version of any software that may be licensed by Customer under this Agreement for installation on Customer's systems. To the extent KnowBe4 delivers any updates or enhancements to Customer as part of Product Support, such updates and enhancements will be deemed included in the definition of "Software."

"**User(s)**" means any of Customer's employees or its other third parties to whom Customer gives access to the Products and Services.

"**Web Hosted Services**" means an application and/or database product hosted by KnowBe4 or its agents and made available for remote access and use by Customer under this Agreement.

2. Products.

2.1 ***Software License.*** This Section applies only in the event Customer licenses Software from KnowBe4 or through an authorized KnowBe4 channel partner. Subject to Customer's commitment to payment in accordance with this Agreement, KnowBe4 hereby grants to Customer, for use with Customer's authorized Users, and solely for internal business purposes and not for resale or publication, a limited; non-exclusive; non-sublicensable; non-transferable; royalty-free license to install, use, execute, display, and access the Software. The Term, as defined below, of the foregoing license will be as set forth in the applicable Quote. Apart from the foregoing limited licenses, Customer is not being granted any right, title, or interest in or to the Software, or otherwise the Products. All such rights are expressly reserved by KnowBe4. Some Software or components used in KnowBe4's Products may be offered under an open source license, which may be found at https://support.knowbe4.com/hc/en-us/articles/360000870387-Open-Source-Licensing-Information, or such other URL locations on KnowBe4's website as KnowBe4 may provide from time to time.

2.2 ***Courseware License.*** This Section applies only in the event Customer licenses Courseware from KnowBe4 or through an authorized KnowBe4 channel partner. Subject to Customer's commitment to payment in accordance with this Agreement, KnowBe4 hereby grants to Customer, for use with Customer's authorized Users, and solely for internal business purposes and not for resale or publication, a limited; non-exclusive; non-sublicensable; non-transferable; royalty-free license to install, use, execute, display, and access the Courseware. The Term, as defined below, of the foregoing license will be as set forth in the applicable Quote. Apart from the foregoing limited licenses, Customer is not being granted any right, title, or interest in or to the Courseware, or otherwise the Products. All such rights are expressly reserved by KnowBe4.

2.3 ***Web Hosted Services Access.*** This Section applies only in the event Customer orders Web Hosted Services from KnowBe4 or through an authorized KnowBe4 channel partner. Subject to Customer's commitment to payment in accordance with this Agreement, KnowBe4 hereby grants to Customer, for use with Customer's authorized Users, and solely for internal business purposes and not for resale or publication, a non-exclusive and non-transferable right to access and use the Web Hosted Services for its internal business purposes. The Term, as defined below, of the foregoing access right will be as set forth in the applicable Quote. Customer will be solely responsible for connection of Customer's systems to a telecommunications service that provides Internet access for purposes of Customer's access and use of the Web Hosted Services. KnowBe4 will use commercially reasonable efforts to make the Web Hosted Services available in accordance with the terms set forth in **Schedule D.**

2.4 ***Beta Products.*** KnowBe4 may offer Beta Products to Customer at no charge. Use of the Beta Products are at the election of Customer and are for evaluation purposes only. Beta Products are not considered "Services" and do not come with Product Support. Beta Products may be subject to additional terms. KnowBe4 reserves the right to discontinue the Beta Products at any time. Use of the Beta Products will automatically terminate at such time as KnowBe4 makes such Beta Products generally available. Beta Products may be unpredictable and lead to erroneous results. Customer acknowledges and agrees that: (a) Beta Products are experimental and have not been fully tested; (b) Beta Products may not meet Customer's requirements; (c) the use or operation of any Beta Products may not be uninterrupted or error free; (d) Customer's use of any Beta Products is for purposes of evaluating and testing the Beta Products and for providing feedback to KnowBe4; (e) Customer will inform its employees, staff members, and other Users regarding the nature of Beta Products; and (f) Customer will hold all information relating to Beta Products and Customer's use of Beta Products, including any performance measurements and other data relating to Beta Products, in strict confidence and will not disclose such information to any unauthorized third parties. Customer will promptly report any errors, defects, or other deficiencies in any Beta Products to KnowBe4. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, ALL BETA PRODUCTS ARE PROVIDED "AS-IS" AND "AS-AVAILABLE," WITHOUT WARRANTIES OF ANY KIND. Customer hereby waives any and all claims, now known or later discovered, that Customer may have against KnowBe4 and KnowBe4's suppliers and licensors arising out of Customer's use of Beta Products.

2.5 ***PhishER.*** This Section applies only in the event Customer orders PhishER from KnowBe4 or through an authorized KnowBe4 channel partner. For more information about PhishER and its additional features (such as PhishML and PhishRIP), Customer may refer to the Documentation. Customer is solely responsible for ensuring compliance with all applicable laws and regulations relating to Customer's use of PhishER. Customer acknowledges that PhishER may pose certain risks to Customer's email system. Customer is solely responsible for Customer's actions in the operation of PhishER and acknowledges KnowBe4 is not responsible for any of Customer's actions, nor is KnowBe4 responsible for backups to Customer's email system. CUSTOMER HEREBY WAIVES ANY COSTS, DAMAGES, OR EXPENSES ASSOCIATED WITH THESE RISKS AND HOLDS KNOWBE4 HARMLESS WITH RESPECT TO SUCH COSTS, DAMAGES, OR EXPENSES.

2.6 ***Direct Message Injection (DMI).*** This Section applies only in the event Customer: (a) utilizes Microsoft (formerly Office 365)365 for email; and (b) exercises the option to activate the DMI products and add-on from KnowBe4 or through an authorized KnowBe4 channel partner. For more information about DMI, Customer may refer to the Documentation. Customer is solely responsible for ensuring compliance with all applicable laws and regulations relating to its use of DMI. As a result, Customer acknowledges that DMI may pose certain risks to Customer's email system. Customer is solely responsible for the actions of its representatives in the operation of DMI and acknowledges KnowBe4 is not responsible for any actions of the Customer's representatives nor is it responsible for backups to the Customer's email system. CUSTOMER HEREBY WAIVES ANY COSTS, DAMAGES, OR EXPENSES ASSOCIATED WITH THESE RISKS AND HOLDS KNOWBE4 HARMLESS WITH RESPECT TO ANY SUCH COSTS, DAMAGES, OR EXPENSES.

3. **Product Usage & Rights**.

3.1 ***Statement of Work and Pricing.*** The parties agree that Services and Products under this Agreement and the requirements of the Products are set forth in the Statement of Work which is attached as **Schedule A** and the price of such Services and Products is set forth in the pricing schedule attached as **Schedule B**.

3.2 ***Acceptance.*** Customer is deemed to have committed to a purchase in full for the Products and Services (regardless of any split payment terms) once a purchase order is sent to KnowBe4 for processing or once payment has been tendered through check, credit card, or other form of payment. Payment via check, credit card, or other form of tendering payment will be deemed acceptance of the corresponding Quote or invoice sent to Customer by KnowBe4. Except as otherwise specified herein, all sales are final, non-refundable, and non-returnable except with respect to Products and Services that do not meet applicable specifications in the relevant Documentation or that are not identified in the Quote.

3.3 ***Operation of the Products.*** The implementation and operation of KnowBe4's Products, and any deliverables resulting from Services performed, are done so by designated admin(s) employed or contracted by Customer. Any Managed Services, as defined below, may be subject to additional fees.

3.4 ***Customer Users.*** The Products and Services are provided on a per-seat, subscription basis. Customers are responsible for managing the creation, modification, and revoking of access of their users. The Customer is solely responsible for the management of access to the Products and Services of their users. The concurrent number of Active Users receiving access may not exceed the purchased number of Seats. If the number of Active Users exceed the purchased number of Seats, Customer is obligated to either pay for any Seats that surpass the purchased amount or immediately reduce its number of Active Users. Customer is not permitted to freely re-assign Seats to Users. KnowBe4 prohibits cycling of Seats amongst Customer's personnel. If an Active User's account is terminated or removed, that User's Seat license is no longer considered in use and may be allocated to another User upon written approval by KnowBe4. Notwithstanding the foregoing, KnowBe4's approval is not required in the instance an Active User's account is terminated or removed due to Customer's termination of that Active User's employment or the Active User no longer being employed by Customer for any reason, or otherwise for termination of contract with that Active User, to account for Customer's normal attrition in workforce. Upon request by KnowBe4, Customer agrees to provide KnowBe4 with a certification of such compliance. KnowBe4 reserves the right to audit Customer's compliance with this Section, provided that any such audit shall be at no additional cost to Customer and shall not require KnowBe4's access to Customer's facilities. Additional Seats may be added mid-subscription term and such additional Seats will be co-pending with the then-current subscription term and will terminate on the same date. Add-ons for more Seats mid-term will be priced at the same volume/level discount purchased under the applicable co-pending Quote and will be valid only until the end of such co-pending subscription term. Upon renewal, new rates may apply.

3.5 ***Professional Services.*** In the instance Customer purchases Services to be performed by KnowBe4, Customer may be required to sign an SOW detailing the project specifications for the Services. Services may include, but are not limited to, the request for KnowBe4 to implement and operate the Products on behalf of Customer ("**Managed Services**"), additional maintenance and support (as opposed to any standard maintenance and support already included), customization and branding of any Courseware, and any additional consultancy or professional services. The completion time for any Services to be performed under an SOW, and any milestones, will be dependent on KnowBe4's receipt of all Customer assets and specifications necessary for the project, in addition to KnowBe4 receiving a validly signed SOW for processing, as requested by KnowBe4. The completion deadline will start from the date of delivery of all such assets and specifications, not the date of KnowBe4's receipt of the signed SOW. Customer acknowledges that delays in providing assets or specifications at the request of KnowBe4 for such Services may delay the completion of the Services. KnowBe4 will not be faulted for delays caused by Customer's failure to reasonably cooperate. Service hours purchased pursuant to an SOW or a Quote will expire upon the expiration or termination of Customer's subscription term and will not carry over to any subsequent renewal term.

3.6 ***Intellectual Property.*** This is not a work made-for-hire agreement, as defined by U.S. or other applicable law. KnowBe4 and its licensors own and reserve all right, title, and interest, including intellectual property rights, in the Products and all enhancements, modifications, and updates thereto. Except for express licenses granted in this Agreement, KnowBe4 is not granting or assigning to Customer any right, title, or interest, express or implied, in or to KnowBe4's intellectual property. KnowBe4 reserves all rights in such property.

3.7 ***Feedback.*** Customer may provide KnowBe4 with suggestions, comments, or other feedback (collectively, "**Feedback**") with respect to the Products. Feedback is voluntary. KnowBe4 is not obligated to hold any Feedback in confidence. KnowBe4 may use Feedback for any purpose without obligation of any kind. To the extent a license is required to make use of any intellectual property in any Feedback, Customer grants KnowBe4 an irrevocable, non-exclusive, perpetual, royalty-free license to use such Feedback in connection with KnowBe4's business, including the enhancement of the Products.

4. Data.

4.1 ***Customer Data.*** Customer grants KnowBe4 a non-exclusive, world-wide, royalty-free license to use the data and other information input by Customer into the Products ("**Customer Data**"): (a) to perform KnowBe4's obligations under this Agreement; (b) in compliance with the Product Privacy Notice; (c) in order to provide, maintain and improve the Products and/or (d) as may be required by law. Customer will be responsible for obtaining all rights, permissions, and authorizations to provide the Customer Data to KnowBe4 for use as contemplated under this Agreement. Except for the limited license granted in this Section, nothing contained in this Agreement will be construed as granting KnowBe4 any right, title, or interest in the Customer Data. Customer Data will be deemed Customer Confidential Information.

4.2 ***Aggregated Data.*** KnowBe4 may also use Customer Data in an aggregate, de-identified, and generic manner for marketing; survey; and benchmarking purposes, in the review, development and improvement of current and future Products, Product usage, and other similar purposes ("**Aggregated Data**"). To the extent such Aggregated Data is disclosed, it will only disclosed in a generic or aggregated manner that does not identify the Customer or any individual and will be for the purposes of sharing Product usage and statistical or benchmarking purposes. Aggregated Data will not be considered Customer Confidential Information.

4.3 ***Data Security.*** Customer Data is maintained in accordance with **Schedule E** using industry standard administrative, physical, and technical safeguards that are designed to provide for the protection of the security, confidentiality, and integrity of Customer Data. KnowBe4's security safeguards include means for preventing access, use, modification, and disclosure of Customer Data by unauthorized individuals. Notwithstanding the foregoing, Customer Data access may be provided: (a) to KnowBe4 and other personnel to the extent necessary to provide the Products, Services, and support; (b) as compelled by law; (c) as set forth in the Product Privacy Notice; or (d) as expressly permitted by Customer. KnowBe4's Products currently operate in third party datacenters located in the US or EU and have been built with high availability, business continuity, and disaster recovery in mind. KnowBe4's cloud architecture follows industry standard security practices and is regularly assessed for vulnerabilities and risks. Information about KnowBe4's information security practices may be found at KnowBe4's Security Page.

4.4 ***Data Protection.*** The collection, use, and disclosure of Customer Data in connection with Customer's use of the Products is subject to the Product Privacy Notice and this Agreement. By using the Products, Customer and each User acknowledge that the Customer Data will be processed in accordance with both the Product Privacy Notice and this Agreement. and may be processed in a country where it was collected, as well as in countries where privacy laws may be different or less stringent, provided KnowBe4 ensures compliance with applicable data protection laws. By using the Products, or submitting Customer Data via the Products, Customer expressly consents to such processing. To the extent Customer or User provides personal data or other information belonging to a third party, Customer represents and warrants that it has that person's, organization's, or other such third party's proper consent, or otherwise proper authorization, to do so. In the event Customer enters into a Data Processing Agreement with KnowBe4, such Data Processing Agreement will govern the data handling practices between the parties and will supersede the language contained in this Section in the event of a conflict.

4.5 ***Loss or Compromise of Customer Data.*** In the event of a Security Incident,, Know Be4 must, as applicable:

4.5.1 notify Customer as soon as practicable but no later than seventy-two (72) hours of becoming aware of such occurrence;

4.5.2 cooperate with Customer in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by Customer;

4.5.3 in the case of PII, at the Customer's sole election:

4.5.4 with approval and assistance from Customer, notify the affected individuals who comprise the PII as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or

4.5.5 reimburse Customer for reasonable costs in notifying the affected individuals;

4.5.6 perform or take any other actions required to comply with applicable law as a result of the occurrence;

4.5.7 pay for reasonable costs associated with the occurrence, including but not limited to any costs incurred by Customer in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

4.5.8 be responsible for recreating lost Customer Data in the manner and on a reasonable schedule without charge to Customer; and

4.5.9 provide to Customer a detailed plan without undue delay of the occurrence describing the measures KnowBe4 will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of KnowBe4's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps KnowBe4 has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; Customer will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by Customer in writing prior to its dissemination.

4.5.10 Section 4.5 survives termination or expiration of this Agreement.

4.5.11 ***Protected Health Information, Payment Card Information, and other Sensitive Information.*** KnowBe4 does not need, nor does KnowBe4 request, any protected health information ("**PHI**") governed by the Health Insurance Portability and Accountability Act and its implementing regulations

("**HIPAA**"). KnowBe4 does not need, nor does KnowBe4 request, any non-public consumer personally identifiable information or financial information governed by the Gramm-Leach-Bliley Act ("**GLBA**") or payment card information covered by the Payment Card Industry Data Security Standards ("**PCI DSS**") in order to provide KnowBe4's products and services. Customer should never disclose, nor allow to be disclosed, PHI, information protected by PCI DSS or GLBA, or other sensitive information to KnowBe4. Customer acknowledges that KnowBe4 does not take steps to ensure KnowBe4's products are GLBA, HIPAA, or PCI DSS compliant. All obligations of the aforementioned regulations remain solely with Customer. KnowBe4's Products and Services are not intended for use with minors (as defined by applicable law). Customer is prohibited from authorizing minors, as defined by applicable law, to use or access the Products and Services, except as otherwise provided in a signed writing by an authorized representative of KnowBe4.

5. **Customer Obligations.**

5.1 ***Connectivity.*** Customer is solely responsible for all telecommunication or Internet connections, and associated fees, required to access and use the Products, as well as all hardware and software. KnowBe4 is not responsible for: (a) Customer's access to the Internet; (b) interception or interruptions of communications through the Internet; or (c) changes or losses of data through the Internet.

5.2 ***User Credentials.*** Customer will ensure User credentials (e.g., usernames and passwords) remain confidential, and Customer and Users will not disclose any such credentials to any third party. In addition, Customer will notify KnowBe4 immediately upon discovery of an unauthorized disclosure of any such credentials or upon any unauthorized access. Upon any termination of the engagement or deactivation of any User with knowledge of any such credentials, Customer will change such credentials and remove access for that User in a reasonable timeframe.

5.3 ***Use of Customer or Third Party LMS.*** In the event Customer uses its own or a third party's LMS, or other mechanisms for hosting Courseware or other such content provided by KnowBe4 or its third party licensors, Customer will ensure strict compliance in accordance with this Agreement and will ensure an agreement is in place with any such third party that contains substantially the same level of protection for the Courseware and other such content as contained herein. After the termination of the applicable subscription term, Customer will ensure all Courseware and other such content is removed from such third party's possession.

5.4 ***Restrictions.***

5.4.1 Customer may not: (a) reverse engineer, disassemble, decompile, or otherwise attempt to reveal the trade secrets or know-how underlying the Products, except to the extent expressly permitted under applicable law; (b) use KnowBe4's intellectual property or Confidential Information to develop a product that is similar to the Products; (c) use any KnowBe4 Confidential Information to contest the validity of any KnowBe4 intellectual property; (d) remove or destroy any copyright notices, other proprietary markings, or confidentiality legends placed on or made available through the Products; or (e) use the Products in any manner or for any purpose inconsistent with the terms of this Agreement or the Documentation. Software will only be used by the licensed number of Active Users for whom Customer paid the applicable fees.

5.4.2 Access and use of KnowBe4 Products, Services, or other related materials (which the parties acknowledge are proprietary and Confidential Information of KnowBe4) is solely authorized for the internal business purposes of the Customer and Active Users, and only for the duration of the subscription term or evaluation period, as applicable. Use of KnowBe4 Products, Services, or other related materials for analytical or research purposes, to be used or disclosed outside of Customer's organization, is strictly prohibited. Sharing screenshots, downloads, or other forms of copying, duplicating, or replicating the Products, Services, or other related materials, publicly or outside of Active Users, is strictly prohibited. Customer acknowledges that some of KnowBe4's Products and Services are designed to assist Customer in training Users and may include developing, customizing, and sending fake cyber security attack campaigns for purposes of employee training, but that Customer, and not KnowBe4 or any KnowBe4 channel partners, will be responsible for Customer's compliance with all laws and governmental regulations, and any results in connection with the Customer's use of the Products (including any reports or information produced in connection therewith).

6. **Customer Content.**

6.1 Depending on the Products and Services purchased via a Quote, Customer may use KnowBe4's Products and Services for the hosting of its assets, content, and other materials, such as certain reports; documents; manuals; audiovisual materials; photos; videos; and audio files, to make available to Active Users on or through the Products and Services ("**Customer Content**"). All Customer Content will be considered Customer Data. Subject to, and conditioned on, Customer's and Users' compliance with the terms and conditions of this Agreement, during the applicable subscription term, KnowBe4 will provide Customer and Active Users remote electronic access to the Customer Content through the Web Hosted Services in accordance with this Agreement. KnowBe4 has the right to: (a) take any action with respect to any Customer Content that it deems necessary or appropriate, in KnowBe4's sole discretion, including if KnowBe4 reasonably believes that such Customer Content violates this Agreement, infringes any intellectual property right or other right of any person or entity, threatens the personal safety of any person, or creates potential liability for KnowBe4; (b) take appropriate legal action including, without limitation, referral to law enforcement related to any illegal or unauthorized Customer Content provided by Customer; or (c) terminate upon giving notice to Customer and allowing Customer to cure any such issue within a reasonable timeframe or suspend Customer's access to the Web Hosted Services for any violation of this Agreement. Customer grants KnowBe4, its service providers, and each of their respective licensees, successors, and assigns the right to use, reproduce, modify, perform, display, distribute, and otherwise disclose the Customer Content as necessary to provide the Web Hosted Services and to make the Customer Content available to Customer and Users.

6.2 Customer represents and warrants that: (a) Customer owns all rights in and to the Customer Content and/or has the right to grant the licenses granted herein to KnowBe4, service providers, and each of their respective licensees, successors, and assigns; and (b) all Customer Content does and will continue to comply with this Agreement; (c) all Customer Content does and will continue to comply with all international, federal, state, and local laws and regulations; and (d) the Customer Content does not: (i) contain any material which is defamatory, obscene, indecent, abusive, offensive, violent, hateful, inflammatory, or otherwise objectionable; (ii) promote sexually explicit or pornographic material, violence, or discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age; (iii) infringe any patent, trademark, trade secret, copyright, or other intellectual property or other rights of any person; (iv) violate the legal rights (including the rights of publicity and privacy) of others or contain any material that may give rise to any civil or criminal liability under applicable laws or regulations or that otherwise may be in conflict with this Agreement; (v) promote any illegal activity, or advocate, promote, or assist any unlawful act; (vi) intentionally create unreasonable disturbances to any other person or organization; or (vii) contain any: (A) viruses, trojan horses, worms, backdoors, or other software or hardware devices, the effect of which would permit unauthorized access to, or disable, erase, or otherwise harm, any computer, systems, software, or content; or (B) time bombs, drop dead devices, or other software or hardware devices designed to disable a computer program automatically with the passage of time or under the positive control of any person, or otherwise deprive KnowBe4, or its customers/users, of its lawful rights.

7. **Compliance.**

7.1 ***Anti-Bribery & Corruption.*** Neither party will: (a) make any unlawful payments to any government official or employee; (b) make any unlawful payment to any person, or unlawfully provide anything of value (whether as property, services, or in any other form) to any person, for the purpose of obtaining an improper business advantage; or (c) agree, commit, or otherwise offer to undertake any of the foregoing actions in connection with this Agreement or any related activities.

7.2 ***International Trade Compliance.*** The sale, resale, or other disposition of Products and any related technology or documentation are subject to various economic sanctions, export control laws, and other restrictive trade measures administered by the U.S. and other applicable governments. Because these laws may have extraterritorial effect, Customer will comply with all such measures, where applicable, including, without limitation: (a) the Export Administration Act of 1979, as amended (50 U.S.C. §§ 2401–2420) and the Export Administration Regulations, 15 C.F.R. §§ 730–774 ("**EAR**"); (b) the Arms Export Control Act, 22 U.S.C. § 2778, and the corresponding International Traffic in Arms Regulations ("**ITAR**"); (c) the economic sanctions laws and regulations enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), 31 C.F.R. §§ 500, et seq., and the U.S. Department of State; and (d) the anti-boycott regulations, guidelines, and reporting requirements under the Export Administration Regulations and Section 999 of the Internal Revenue Service Code. Customer understands and acknowledges that it is solely responsible for complying with such laws whenever applicable. Customer further understands and acknowledges that it will not directly or indirectly export, import, sell, disclose, or otherwise transfer any Products to any country or party subject to such restrictions, and that it is solely responsible for obtaining any license(s) to export, re-export, or import the Products that may be required.

7.3 ***Freedom of Information Act 442 of 1976 Notice of Exemption.*** This software, content, and information is proprietary to KnowBe4 and is an important business asset of KnowBe4 (the "Proprietary Information"). The Proprietary Information consists of protected financial data, trade secrets and commercially valuable information that, if disclosed, would harm the competitive position of KnowBe4. The Parties understand that the Proprietary Information may be the subject of a Freedom of Information Act 442 of 1976, MCL 15.231 through 15.246 ("FOIA") request. Customer acknowledges that the Trade Secrets or commercial financial information voluntarily provided for use in developing governmental policy may be exempted from public disclosure in accordance with M.C.L § 15.243(f). Customer also acknowledges that pursuant to M.C.L § 15.232(i), "public record" does not include computer software. In the event of a request for disclosure of KnowBe4's information, including any training materials, Customer will limit disclosure to the minimum necessary, in Customer's sole discretion, to be in compliance with the FOIA, based upon the opinion of Customer's counsel.

7.4 ***Background Checks.*** Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including KnowBe4 and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. The parties acknowledge and agree that KnowBe4 shall not have any access to any database of information maintained by the federal government that contains confidential or personal information and shall not be subjected to the above-stated requirements unless and until KnowBe4 gains such access. In accordance with KnowBe4's background check policy for its US entity, and to the extent allowed by applicable laws, KnowBe4 has not knowingly employed any persons who, in the past seven (7) years, have been convicted of an offense involving violence, theft, fraud, money laundering, sex crimes, or other offenses that pose an unacceptable level of risk, given the scope of the applicable employment position and KnowBe4's business needs. KnowBe4 is responsible for all costs associated with the requested background checks.

8. Product Support.

8.1 ***In General.*** Products are made available with standard Product Support for no additional charge. Customer may purchase priority level support for an additional fee as set forth in the applicable Quote. Product Support is made available in accordance with the terms and conditions set forth in **Schedule C**.

8.2 ***Exclusions.*** Notwithstanding the foregoing, KnowBe4 will have no obligation to support: (a) services, hardware, or software provided by anyone other than KnowBe4; (b) Product issues caused by Customer's negligence, abuse, or misapplication; or (c) Customer's use of Products other than as specified in the Documentation.

9. **Payment Terms.**

9.1 ***Invoices and Payment.*** Invoices must conform to the reasonable requirements communicated from time-to-time by Customer. All undisputed amounts are payable within 45 days of Customer's receipt of KnowBe4's invoice. KnowBe4 may only charge for Products and Services provided as specified in Statement(s) of Work or applicable Quote. Invoices must include an itemized statement of all charges. Customer is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for Customer's exclusive use. Customer must provide KnowBe4 with a valid tax exemption certificate authorized by the appropriate taxing authority. Notwithstanding the foregoing, all prices are exclusive of taxes, and KnowBe4 is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by Customer under this Agreement. Customer will only disburse payments under this Agreement through Electronic Funds Transfer (EFT). KnowBe4 must register with Customer at http://www.michigan.gov/SIGMAVSS to receive electronic fund transfer payments.

Invoice Disputes. Customer has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. Customer will notify KnowBe4 of any dispute within a reasonable time. Payment by Customer will not constitute a waiver of any rights as to KnowBe4's continuing obligations, including claims for deficiencies or substandard Products or Services.

Pricing/Fee Changes. All Pricing set forth in this Agreement will not be increased, except as otherwise expressly provided in this Section or as otherwise expressly authorized under this Agreement. The Fees will not be increased at any time except for upgrades in subscription level or the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in Schedule B. Except as otherwise specified herein or in a Quote: (a) fees are based on the Product acquired and not actual usage; (b) payment obligations are non-cancelable and fees paid are non-refundable, except where expressly permitted herein; and (c) subscription term and quantities purchased cannot be decreased during the applicable subscription term.

10. **Confidentiality.**

10.1 ***Confidential Information.*** During the Term, each party may disclose to the other certain Confidential Information to the other party. Notwithstanding the foregoing, Confidential Information does not include information that: (a) is or becomes publicly available through no breach by the Receiving Party of this Agreement; (b) was previously known to the Receiving Party prior to the date of disclosure, as evidenced by contemporaneous written records; (c) was acquired from a third party without any breach of any obligation of confidentiality; (d) was independently developed by a party hereto without reference to Confidential Information of the other party; or (e) is required to be disclosed pursuant to a subpoena or other similar order of any court or government agency, provided, however, that the party receiving such subpoena or order will promptly inform the other party in writing and provide a copy thereof (unless notice is precluded by the applicable process), and will only disclose that Confidential Information necessary to comply with such subpoena or order.

10.2 ***Protection of Confidential Information.*** Except as expressly provided in this Agreement, the Receiving Party will not use or disclose any Confidential Information of the Disclosing Party without the Disclosing Party's prior written consent, except disclosure to, and subsequent uses by, the Receiving Party's employees or consultants on a need-to-know basis, provided that such employees or consultants have executed written agreements restricting use or disclosure of such Confidential Information that are at least as restrictive as the Receiving Party's obligations under this Section. Subject to the foregoing nondisclosure and non-use obligations, the Receiving Party will use at least the same degree of care and precaution that it uses to protect the confidentiality of its own Confidential Information and trade secrets of similar nature, but in no event less than reasonable care. Each party acknowledges that due to the unique nature of the other party's Confidential Information, the Disclosing Party will not have an adequate remedy in money or damages in the event of any unauthorized use or disclosure of its Confidential Information. In addition to any other remedies that may be available in law, in equity, or otherwise, the Disclosing Party shall be entitled to seek injunctive relief to prevent such unauthorized use or disclosure.

10.3 ***Return and Destruction of Materials.*** All documents and other tangible objects containing or representing Confidential Information that have been disclosed by either party to the other party, and all summaries, copies, descriptions, excerpts, or extracts thereof that are in the possession of the other party will be, and remain, the property of the Disclosing Party and will be promptly returned to the Disclosing Party. The Receiving Party will use reasonable efforts to promptly delete or destroy all summaries, copies, descriptions, excerpts, or extracts thereof in their possession upon the Disclosing Party's written request. The Receiving Party will have no obligation to delete or destroy copies that: (a) are contained in an archived computer system backup that were made in accordance with such party's security, e-mail retention, and/or disaster recovery procedures; or (b) are kept by a party for record-keeping, archival, or governance purposes in compliance with such party's document retention policies. Any such retained Confidential Information will remain subject to the terms and conditions of this Agreement for so long as it is retained. Notwithstanding the return or destruction of the Confidential Information, the Receiving Party will continue to be bound by its confidentiality and other obligations hereunder in accordance with the terms of this Agreement. At the Disclosing Party's option, the Receiving Party will provide written certification of its compliance with this Section.

11. Warranties and Disclaimers.

11.1 ***Product Warranties.*** All purchased Products will materially conform to their then-current Documentation and during the applicable subscription term, KnowBe4 will not materially decrease the overall functionality of the Products. Customer must notify KnowBe4 of any breach of this warranty within thirty (30) days of discovery of the breach. Customer's sole and exclusive remedy, and KnowBe4's sole and exclusive liability, for a breach of the foregoing warranty, will be for KnowBe4 to provide Product Support to repair or replace the relevant Product within thirty (30) days of such notice of non-conformity. If KnowBe4 is unable to remedy such non-conformity within the period to cure, Customer will be entitled to terminate the relevant Quote and be issued a refund for any pre-paid, unearned fees for the affected portion of the Products. KnowBe4 will not be responsible for any breach of the foregoing warranty resulting from Customer's abuse or misuse of the Product or failure to use the Product as described in this Agreement, including failure to use the Product in accordance with its operational requirements. Customer is required to sufficiently detail the non-conformity in a manner that allows KnowBe4 to properly assist with the remediation. KnowBe4 will not be responsible for delays in remediation caused by Customer's failure to respond to requests by KnowBe4. Customer understands that the Products will only operate in accordance with KnowBe4's Documentation, and it is Customer's responsibility to ensure that the Products will be fit for its purposes and to ensure that the Products will be supported by Customer's technology and business environment.

11.2 ***Service Warranties.*** KnowBe4 warrants that KnowBe4 will provide the Services in a professional, workmanlike manner consistent with this Agreement. Customer must notify KnowBe4 of any breach of this warranty within thirty (30) days of discovery of the breach. Customer's sole and exclusive remedy, and KnowBe4's sole and exclusive liability, for a breach of the foregoing warranty will be for KnowBe4, in its sole discretion, to use reasonable efforts to re-perform the Services or terminate the relevant Quote and issue a refund for the portion of pre-paid fees for the non-conforming Services.

11.3 ***Compliance Warranties.*** Each party warrants that it will comply with all laws and regulations applicable to its provision or use of the Products and Services, as applicable (including applicable security breach notification laws).

11.4 ***Additional Warranties.***

11.4.1 KnowBe4 represents and warrants that the Products and Services will be delivered free of malware.

11.4.2 KnowBe4 represents and warrants that it is neither currently engaged in nor will engage in the boycott of Israel.

11.5 ***Disclaimers.*** EXCEPT FOR THE LIMITED WARRANTIES IN THIS SECTION: (A) THE PRODUCTS AND SERVICES ARE PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTIES OF ANY KIND; AND (B) KNOWBE4 EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, QUIET ENJOYMENT, QUALITY OF INFORMATION, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. KNOWBE4 DOES NOT WARRANT THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT DEFECTS IN THE PRODUCTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION, MARKETING, OR PROMOTIONAL MATERIALS, OR ADVICE GIVEN BY KNOWBE4 OR KNOWBE4'S AUTHORIZED REPRESENTATIVES WILL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THE EXPRESS WARRANTIES PROVIDED HEREIN. CUSTOMER ACKNOWLEDGES THAT COURSEWARE IS FOR GENERAL INFORMATION PURPOSES ONLY AND THAT KNOWBE4 IS NOT A LAW FIRM, NOR DOES IT PROVIDE ANY PROFESSIONAL OR ADVISORY SERVICES. THE INFORMATION PRESENTED IS NOT LEGAL ADVICE AND IS NOT TO BE ACTED ON AS SUCH. THE PRODUCTS MAY CONTAIN THE TRADE NAMES OR TRADEMARKS OF VARIOUS THIRD PARTIES AND, IF SO, ANY SUCH USE IS FOR ILLUSTRATIVE AND EDUCATIONAL PURPOSES ONLY. ALL PRODUCT AND COMPANY NAMES ARE PROPERTY OF THEIR RESPECTIVE OWNERS. USE OR DISPLAY OF THE MARKS DOES NOT IMPLY ANY AFFILIATION WITH, ENDORSEMENT BY, OR ASSOCIATION OF ANY KIND BETWEEN SUCH THIRD PARTIES AND KNOWBE4.

11.6 THE PRODUCTS AND SERVICES MAY BE USED TO ACCESS AND TRANSFER INFORMATION OVER THE INTERNET. CUSTOMER ACKNOWLEDGES AND AGREES THAT KNOWBE4 AND ITS VENDORS AND LICENSORS DO NOT OPERATE OR CONTROL THE INTERNET AND THAT: (A) VIRUSES, WORMS, TROJAN HORSES, OR OTHER UNDESIRABLE DATA OR SOFTWARE; OR (B) UNAUTHORIZED USERS (E.G., HACKERS) MAY ATTEMPT TO OBTAIN ACCESS TO, AND DAMAGE, CUSTOMER DATA, WEB-SITES, COMPUTERS, OR NETWORKS. KNOWBE4 WILL NOT BE RESPONSIBLE FOR THOSE ACTIVITIES. FURTHER, EACH PARTY DISCLAIMS ALL LIABILITY AND INDEMNIFICATION OBLIGATIONS FOR ANY HARM OR DAMAGES CAUSED BY ANY THIRD-PARTY HOSTING PROVIDERS EXCEPT TO THE EXTENT THAT KNOWBE4 HAS CHOSEN SUCH SERVICE PROVIDER TO PROVIDE SERVICES UNDER THIS AGREEMENT IN WHICH CASE SUCH SERVICE PROVIDER IS A SUBCONTRACTOR OF KNOWBE4 AND SHALL BE TREATED AS SUCH FOR THE PURPOSES OF LIABILITY AND INDEMNIFICATION.

12. Indemnification.

12.1 ***KnowBe4 Indemnity Obligations.*** KnowBe4 will defend and indemnify Customer from any and all claims, losses, deficiencies, damages, liabilities, costs, and expenses (including, but not limited to, reasonable attorneys' fees) finally awarded against Customer, as approved via a court-approved settlement, or via binding mediation or arbitration arising from a claim by a third party that Customer's authorized use of a Product infringes that third party's patent, copyright, or trade secret rights. The foregoing indemnification obligation of KnowBe4 is contingent upon Customer promptly notifying KnowBe4 in writing of such claim (provided the failure or delay in doing so will not relieve KnowBe4 from any obligations to indemnify Customer except to the extent that such delay or failure materially prejudices the defense of such claim), permitting KnowBe4 sole authority to control the defense or settlement of such claim and providing

KnowBe4 reasonable assistance (at KnowBe4's sole expense) in connection therewith. KnowBe4 will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding where the Customer may be subject to monetary damages or to liability in any action at law or in equity. Any litigation activity on behalf of Customer or any of its subdivisions, under this Section 12 must be coordinated with the Department of Attorney General. An attorney designated to represent Customer may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General. If a claim of infringement under this Section occurs, or if KnowBe4 determines a claim is likely to occur, KnowBe4 will have the right, in its sole discretion, to either (a) procure for Customer the right or license to continue to use the Products free of the infringement claim; or (b) modify the Products to make them non-infringing, without loss of material functionality. If neither of these remedies is reasonably available to KnowBe4, KnowBe4 may, in its sole discretion, immediately terminate this Agreement and related Quote and, upon return of the infringing Products from Customer, provide a prorated refund for any prepaid, unused fees for such Products for the remainder of the applicable subscription Term. Notwithstanding the foregoing, KnowBe4 will have no obligation with respect to any claim of infringement that is based upon or arises out of: (a) the use or combination of the Products with any third-party software, process, products, data, service, or other materials not provided by KnowBe4 unless such use or combination was contemplated or required for the Products to function or otherwise referenced in the Documentation; (b) modification or alteration of the Products by anyone other than KnowBe4; (c) use of the Products in excess of the rights granted in this Agreement; or (d) any specifications or other intellectual property provided by Customer (collectively, the "**Excluded Claims**").

12.2 ***Intentionally Omitted.***

13. Limitations of Liability.

13.1 NEITHER KNOWBE4 NOR ITS VENDORS OR LICENSORS NOR CUSTOMER WILL HAVE ANY LIABILITY TO THE OTHER OR ANY THIRD PARTY FOR ANY LOSS OF PROFITS, SALES, BUSINESS, DATA, OR OTHER INCIDENTAL, CONSEQUENTIAL, OR SPECIAL LOSS OR DAMAGE, INCLUDING EXEMPLARY AND PUNITIVE DAMAGES, OF ANY KIND OR NATURE RESULTING FROM, OR ARISING OUT OF, THIS AGREEMENT, THE PRODUCTS, AND ANY SERVICES RENDERED HEREUNDER. THE TOTAL LIABILITY OF KNOWBE4 AND ITS VENDORS AND LICENSORS TO CUSTOMER OR CUSTOMER TO KNOWBE4 OR ANY THIRD PARTY ARISING OUT OF THIS AGREEMENT, THE PRODUCTS, AND ANY SERVICES RENDERED HEREUNDER FOR ANY AND ALL CLAIMS OR TYPES OF DAMAGES WILL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE HEREUNDER BY CUSTOMER FOR THE PRODUCT OR SERVICE AS TO WHICH THE LIABILITY RELATES, IN THE TWELVE (12) MONTHS PRIOR TO THE FIRST EVENT GIVING RISE TO LIABILITY. THE ABOVE LIMITATIONS OF LIABILITY DO NOT APPLY TO: (I) EITHER PARTY'S MISAPPROPRIATION OR INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, (II) EITHER PARTY'S INDEMNIFICATION PROVISIONS, (III) EITHER PARTY'S BREACH OF CONFIDENTIALITY OBLIGATIONS, (IV) EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (V) CUSTOMER'S PAYMENT OBLIGATIONS. The allocations of liability in this Section represent the agreed, bargained-for understanding of the parties and KnowBe4's compensation hereunder reflects such allocations. The limitation of liability and types of damages stated in this Agreement are intended by the parties to apply, regardless of the form of lawsuit or claim a party may bring, whether in tort, contract, or otherwise, and regardless of whether any limited remedy provided for in this Agreement fails of its essential purpose.

14. Term and Termination.

14.1 ***Term.*** This Contract is effective on March 15, 2022 ("Effective Date"), and unless terminated, expires on March 28, 2027 (the "Term").

14.2 ***Suspension.*** In the event KnowBe4, in good faith, believes or otherwise becomes aware of a User's violation of this Agreement, then KnowBe4 may specifically request that Customer suspend such User's access to, and use of, the Products. In the event Customer fails to suspend such non-compliant User, Customer hereby authorizes KnowBe4 to suspend such User. The duration of such suspension is at the sole determination of KnowBe4 and will continue until such time as KnowBe4 determines that the applicable User has cured the breach resulting in such suspension. KnowBe4 may also suspend access to, and use of, the Products with respect to any individual User or the Customer account to: (a) prevent damages to, or degradation of, the Products or KnowBe4's systems; (b) comply with any law, regulation, court order, or other governmental request; or (c) otherwise protect KnowBe4 from potential legal liability. Any such suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the cause of the suspension.

14.3 ***Termination.***

14.3.1 If Customer fails to pay any invoice when due and does not make such payment within 45 days after receipt of notice from KnowBe4 of such failure, KnowBe4 may, in its sole discretion, either: (a) suspend delivery or performance of any Quote, or any remaining balance thereof, until such payment is made; or (b) terminate any Quote. In either event, Customer will remain liable to pay for the Products and Services.

14.3.2 Either party may terminate the Agreement or a Quote upon a material breach of the Agreement or Quote by the other, if the breaching party does not cure the breach within thirty (30) days after receipt of written notice from the other party specifying the breach.

14.3.3 Customer may terminate this Agreement or any applicable Quote at any time and for any reason, including in the event of non-appropriation or action by the Governor, upon providing thirty (30) days' written notice to KnowBe4, provided Customer will not be entitled to reimbursement or relief of its future payment obligations.

14.4 ***Effects of Termination.***

14.4.1 In the event of any termination of the Agreement or Quote without cause by Customer, or for cause by KnowBe4, Customer will pay for all Products and Services ordered as of the effective date of termination of the particular Quote. In the event Customer terminates the Agreement or a Quote for a material breach by KnowBe4 and the breach remains uncured, Customer will be entitled to a pro rata refund of fees paid that cover the timeframe from the date of receipt of the notice to terminate until the end of the Term. KnowBe4 will make full payment of the refund amount to Customer within forty (40) days of receipt of a written notice from Customer specifying the breach.

14.4.2 Upon any termination, Customer's right to use and access the Products and Services (including any Courseware and other materials provided by KnowBe4) will immediately cease. Customer must return or destroy all copies (original and duplicates) of such Products and Services, in accordance with this Agreement. Upon request by KnowBe4, Customer must provide to KnowBe4 a certification of destruction.

14.4.3 During the applicable subscription term and for ninety (90) days thereafter, Customer will have the ability to download a copy of its Customer Data contained in the Products in the form and format as such Customer Data exists in the Products. Ninety (90) days following termination of this Agreement or applicable subscription term, KnowBe4 will have the right to delete or destroy all Customer Data in KnowBe4, or in KnowBe4's agents' possession. Upon written request by Customer, KnowBe4 will delete all Customer Data. Notwithstanding the forgoing, KnowBe4 will be permitted to retain copies of data contained in an archived computer system backup that: (a) was made in accordance with its security, e-mail retention, and/or disaster recovery procedures; or (b) are kept by KnowBe4 for record-keeping, archival, or governance purposes in compliance with KnowBe4's document retention policies.

Any such retained data will remain subject to the provisions of this Agreement for so long as it is retained.

14.4.4 The exercise of the right to terminate this Agreement and any Quote will be in addition to any other rights or remedies provided in this Agreement, or existing at law or equity, that are not otherwise excluded or limited under this Agreement.

15. Miscellaneous Provisions.

15.1 ***U.S. Governmental Rights.*** The software Products and Services consist of commercial items and are commercial computer software as described in DFARS 252.227-7014(a)(1) and FAR 2.101. If acquired by or on behalf of any the Department of Defense or any component thereof, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in DFARS 227.7202-3, Rights in Commercial Computer Software or Commercial Computer Software Documentation. If acquired by or on behalf of any civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in FAR 12.212, Computer Software.

15.2 ***Insurance.*** KnowBe4 will maintain adequate insurance coverages as required by law or regulation as set forth in **Schedule C**

15.3 ***Independent Contractor.*** KnowBe4, its personnel, agents, subcontractors and independent contractors are not employees or agents of Customer and are acting as independent contractors with respect to Customer. Neither party is, nor will be, considered to be an agent; distributor; partner; joint venture; or representative of the other party for any purpose, and neither party will have the authority to act on behalf of, or in the name of, or to bind, the other party in any manner whatsoever.

15.4 ***Force Majeure.*** Neither party to this Agreement will be liable for delays or failures in performance under this Agreement (other than the payment obligations or breach of confidentiality requirements) resulting from acts or events beyond the reasonable control of such party, including acts of war, terrorism, acts of God, natural disasters (fires, explosions, earthquakes, hurricane, flooding, storms, explosions, infestations), embargos, riots, sabotage, governmental acts, failure of the Internet, power failures, energy interruptions or shortages, other utility interruptions, or telecommunications interruptions, provided that the delayed party: (a) gives the other party notice of such cause without undue delay; and (b) uses its reasonable commercial efforts to promptly correct such failure or delay in performance.

15.5 ***Entire Agreement; Construction; Modifications.*** This Agreement, including any and all Quotes, constitutes the entire understanding between the parties related to this Agreement which understanding supersedes and merges all prior understandings and all other proposals, letters, agreements, whether oral or written. The parties further agree that there are no other inducements, warranties, representations, or agreements regarding the matters herein between the parties except as expressly set forth in this Agreement. In the event of any conflict between the body of this Agreement and any Quote, or additional agreements entered into by the parties, the body of this Agreement will control, unless otherwise expressly stated in a signed writing by authorized representatives of the parties. In the event that the Customer or Users are presented with KnowBe4 click-wrap, the contents of this Agreement will supersede any conflicting terms. As used herein, the term “including” will mean “including, without limitation”; the term “includes” as used herein will mean “includes, without limitation”; and terms appearing in the singular will include the plural, and terms appearing in the plural will include the singular. This Agreement may not be modified, amended, or altered in any manner except by a written agreement signed by authorized representatives of the parties, and any attempt at oral modification will be void and of no effect.

15.6 ***Assignment.*** This Agreement may not be assigned or transferred by either party without the prior written consent of the other party, which consent will not be unreasonably withheld, conditioned, or delayed. Notwithstanding the foregoing, either party may assign its rights and obligations under this Agreement, in whole but not in part, without the other party's permission, to an Affiliate (provided previously purchased licenses, access rights, and Seats for the Products and Services will not be assignable or transferable without written consent from KnowBe4) or in connection with any merger, consolidation, sale of all or substantially all of such assigning party's assets, or any other similar transaction, provided, that the assignee: (a) is not a direct competitor of the non-assigning party; (b) is capable of fully performing the obligations of the assignor under this Agreement; and (c) agrees to be bound by the provisions of this Agreement.

15.7 ***No Waiver.*** The waiver or failure of either party to exercise any right in any respect provided for herein will not be deemed to be a waiver of any further right.

15.8 ***Purchase Order.*** KNOWBE4 SPECIFICALLY OBJECTS TO ANY ADDITIONAL TERMS BEING ADDED THROUGH A CUSTOMER PROVIDED PURCHASE ORDER OR SIMILAR DOCUMENT. IF A PURCHASE ORDER IS REQUIRED BY CUSTOMER, THE PARTIES AGREE THAT ANY ADDITIONAL TERMS CONTAINED THEREIN WILL NOT BECOME PART OF THE AGREEMENT BETWEEN THE PARTIES AND, SPECIFICALLY, THAT THE TERMS OF THIS AGREEMENT WILL SUPERSEDE AND REPLACE ANY AND ALL TERMS IN ANY PURCHASE ORDER.

15.9 ***Survivability.*** All provisions of this Agreement relating to confidentiality, non-disclosure, intellectual property, disclaimers, limitation of liability, indemnification, payment, and any other provisions which must survive in order to give effect to their meaning will survive the termination of this Agreement.

15.10 ***Severability.*** If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

15.11 ***Notices.*** Any notice provided pursuant to this Agreement, if specified to be in writing, will be in writing and will be deemed given: (a) if by hand delivery or by delivery service, upon receipt thereof; (b) if delivered by first class mail, registered mail, or certified mail, upon the earlier of actual delivery or three (3) calendar days after deposit in the U.S. mail, postage prepaid; or (c) if by email, upon the next business day. All notices will be addressed to the parties at the addresses specified below or at such other addresses as either party may in the future specify in writing to the other.

15.12 ***Headings; Counterparts; Electronic Signatures.*** The headings contained in this Agreement are for purposes of convenience, only, and will not affect the meaning or interpretation of this Agreement. This Agreement may be executed in two or more original or facsimile counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. The parties agree that the electronic signature of a party to this Agreement will be as valid as an original signature of such party and will be effective to bind such party to this Agreement. The parties agree that any electronically signed document (including this Agreement) will be deemed (a) to be "written" or "in writing"; (b) to have been signed; and (iii) to constitute a record established and maintained in the ordinary course of business and an original written record when printed from electronic files. Such paper copies or "printouts," if introduced as evidence in any judicial, arbitral, mediation, or administrative proceeding, will be admissible as between the parties to the same extent and under the same conditions as other original business records created and maintained in documentary form. For purposes hereof, "electronic signature" means a manually-signed original signature that is then transmitted by electronic means; "transmitted by electronic means" means sent via the internet as a ".pdf" (portable document format) or other replicating image attached to an email message; and, "electronically signed document" means a document transmitted by electronic means and containing, or to which there is affixed, an electronic signature.

15.13 ***Right of Audit.*** Pursuant to MCL 18.1470, Customer or its designee may audit KnowBe4 to verify compliance with this Contract. KnowBe4 must retain and provide to Customer or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for three (3) years after the latter of termination, expiration, or final payment under this Contract or any extension ("Financial Audit Period"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, KnowBe4 must retain the records until all issues are resolved. Within thirty (30) calendar days of providing notice, Customer and its authorized representatives or designees have the right to enter and inspect KnowBe4's premises, and examine, copy, and audit all records related to this Contract. The audit shall be: (a) performed at Customer's sole expense and solely for the purposes of verifying compliance with the terms of this Agreement; (b) performed during KnowBe4's regular business hours in a manner that, in KnowBe4's reasonable judgment, does not disrupt or degrade KnowBe4's regular business operations and is done in accordance with KnowBe4's security and data protection policies; (c) limited to KnowBe4's facilities and personnel of KnowBe4 in scope of this Agreement; and (d) proprietary financial and accounting data and records associated with the contract or grant shall be exempt from disclosure to the extent allowable under the freedom of information act. KnowBe4 must cooperate and provide reasonable assistance. Any overcharges revealed by the audit must be paid or refunded within forty-five (45) calendar days.

15.14 ***Nondiscrimination.*** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, et seq., the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., and Executive Directive 2019-09, KnowBe4 and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position.

15.15 ***Unfair Labor Practice.*** Under MCL 423.324, Customer may void any Contract with a KnowBe4 or subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

15.16 ***Governing Law.*** This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Agreement are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Agreement must be resolved in the Michigan Court of Claims. Complaints against Customer must be initiated in Ingham County, Michigan. KnowBe4 waives any objections, such as lack of personal jurisdiction or forum non conveniens. KnowBe4 must appoint an agent in Michigan to receive service of process. Notwithstanding the foregoing, the parties will have the right to seek injunctive or pre-judgment relief in any court of competent jurisdiction to prevent or enjoin the misappropriation, misuse, infringement or unauthorized disclosure of its Confidential Information or intellectual property rights. No Federal Acquisition Regulations will be construed to apply to KnowBe4 without KnowBe4's written agreement thereto.

15.17 ***Non-Exclusivity.*** Nothing contained in this Agreement is intended nor is to be construed as creating any requirements contract with KnowBe4, nor does it provide KnowBe4 with a right of first refusal for any future work. This Agreement does not restrict Customer or its agencies from acquiring similar, equal, or like Services from other sources.

15.18 ***Administrative Fee and Reporting.*** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract. Administrative fee payments must be made online by check or credit card at: https://www.thepayplace.com/mi/dtmb/adminfee. Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov. The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

16. Accessibility Requirements.

16.1 The Courseware provided by KnowBe4 under this Agreement will conform to WCAG 2.0 Level AA, and if not conforming, KnowBe4 will provide Customer an alternate format upon written request (i.e. an accessible PDF). KnowBe4 must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed VPAT for each WCAG 2.0 Level AA complaint Courseware provided under the Agreement. At a minimum, KnowBe4 must comply with the WCAG 2.0 Level AA conformance claims it made to Customer in the Documentation, including the level of conformance provided in any VPAT. Throughout the Term of the Agreement, KnowBe4 must:

16.1.1 maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each VPAT;

16.1.2 comply with reasonable plans and timelines approved by Customer to achieve conformance in the event of any deficiencies;

16.1.3 ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Agreement, will have any adverse effect on the conformance of KnowBe4's Courseware to WCAG 2.0 Level AA;

16.1.4 promptly respond to and resolve any complaint Customer receives regarding accessibility of KnowBe4's Courseware; and

16.1.5 upon Customer's written request, provide evidence of compliance with this Section by delivering to Customer KnowBe4's most current VPATs.

16.1.6 Participate in the State of Michigan Digital Standards Review process at no additional cost.

KNOWBE4		**CUSTOMER**	
By:		**By:**	
Name:		**Name:**	
Title:		**Title:**	
Date:		**Date:**	
Address for Notices:		**Address for Notices:**	
	33 N. Garden Ave., Suite 1200		
	Clearwater, Florida 33755 USA		
E-mail:	legal@knowbe4.com	**E-mail:**	
Phone:	(855) 566-9234 ext. 102	**Phone:**	
Attention:	Legal Department	**Attention:**	

SCHEDULE A - STATEMENT OF WORK

1. DEFINITIONS

The following terms have the meanings set forth below. All initial capitalized terms that are not defined in this Schedule shall have the respective meanings given to them in Section 1 of the Contract Terms and Conditions.

Term	Definition
SECT	Secure Electronic Compliance Technologies
ESAT	Enterprise Security Awareness Training
ADL	Advanced Distributed Learning
SCORM	Sharable Content Object Reference Model

2. BACKGROUND

The State of Michigan (SOM) in accordance with the Federal Information Security Modernization Act (FISMA) is required to provide the State of Michigan employees and contractors general Security Awareness Training as defined in the National Institute of Standards and Technology (NIST) Special Publications 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, 800-50 Building an Information Technology Security Awareness and Training Program, Role-Based Security training as defined in NIST 800-16 Role-Based Model for Federal Information Technology / Cyber Security Training, and other statutory and regulatory compliance requirements

The State of Michigan (SOM) requires a Contractor hosted Software as a Service (SaaS) Security Awareness training solution that is compliant with FISMA and NIST special publications for approximately fifty-five thousand (55,000) employees and contractors. The solution implementation start date for Security Awareness training is required to start in March of 2022 and shall commence in short phases to all SOM employees within thirty (30) days.

State of Michigan employees and contractors are required to participate in Enterprise Security Awareness Training (ESAT) activities yearly and new hires need to complete select core security courses before starting daily work activities and accessing SOM information systems and data.

Role-based security training shall include Knowledge and Skills courses defined in Appendix B of the NIST Special Publication 800-16 Revision 1 (2nd Draft, Version 2) A Role-Based Model for Federal Information Technology / Cyber Security Training https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf.

Security Awareness training and Role-based security training are required to prevent security incidents and safeguard all State of Michigan assets.

PURPOSE

The purpose of this Contract is to provide a *Contractor Hosted* Software Solution and applicable Services for Enterprise Security Awareness Training.

Specific business goals: To provide enterprise Security Awareness training to comply with various statutory requirements, assess the effectiveness of the training, and retain the information for federal and State audits.

This training program will educate and test SOM users with cybersecurity fundamentals, bring consistency across the departments, optimize the training curriculum to improve effectiveness of training, reduce overall cost of conducting security awareness at the agency level, increase compliance with various statues and regulations, reduce incidents, and improve overall security posture of the state of Michigan.

This effort will provide measurable results and utilize that information to focus/spot-train specific users. This program's data will be utilized to report SOM's on-going efforts to administer security awareness training.

- Contractor hosted solution to provide Phishing Software as a Service (SaaS) email services
- Contractor will provide Maintenance and Support of the security awareness training and Phishing solution in compliance with FISMA and NIST requirements
- Contractor will assist with User file imports and deletes
- Contractor provided Program introduction and administrator training
- First campaign walkthrough guidance with contractor's support team
- Full State access to assessment, testing, education, and reporting tools
- State access to comprehensive library of phishing campaign emails and landing pages
- Ability for the State to deploy unlimited number of security awareness training and phishing campaigns

The Contractor's solution shall assist the State of Michigan (SOM) in complying with NIST Special Publications 800-50 Building an Information Technology Security Awareness and Training Program and 800-16 Role-Based Model for Federal Information Technology / Cyber Security Training special publications by offering course content on the following:

Core Security Awareness Training Topic's include:
Contractor must have the ability to spread trainings out throughout the year.

Intro to Security Awareness
Data Security
Information Privacy
Computer Security
Protecting Data Assets
Email Security
Reporting Incidents
Passwords
Phishing
Office Security
Social Networking
Web Security
Public Wi-Fi
Mobile Security Including Bring Your Own Device (BYOD)
Identity Theft
Social Engineering (email, Phone, In Person, Instant Messaging)
Acceptable Use
Safe Disposal
Remote Work
Information Privacy
Ransomware
Malicious Insider Threat

Security Awareness course content shall be available to all State of Michigan employees and contractors for the duration of the Contract

Role-Based Security Knowledge and Skills Training Catalog in compliance with NIST 800-16 shall include:

Overall Security Management courses
Advanced network Technology and Protocols

Architecture
Compliance
Computer Network Defense
Configuration Management
Cryptography and Encryption
Data Security
Digital Forensics
Emerging Technologies
Enterprise Continuity
Identity management / Privacy
Incident Management
Industrial Control Systems
Information Assurance
Information Systems
IT Systems and Operations
IT Security Awareness and Training
Management
Modeling and Simulation
Network and Telecommunications Security
Personnel Security
Physical and Environmental Security
Procurement
Security Risk Management
Software
Systems and Application Security
Web Security
Compliance with IRS 1075, HIPAA, CJIS for basic security awareness

IN SCOPE

- Security Awareness & Role-based Software as a Service (SaaS), contractor hosted solution.
- Security Awareness Training course content
- Role-Based Security Training course content
- Maintenance and Support of the solution in compliance with FISMA and NIST
- User file imports and deletes
- Simulated Phishing Exercises
- The system should allow for SOM to make simple text substitutions without having to create a custom solution. For example, replace “company” with “state of Michigan”, replace “employees” with “employees and contractors”. This is a WANT not a MUST.
- KMSAT provides Customers with a means to mitigate potential false-positive clicks from anti-phishing tools like Microsoft SafeLinks.
- Phishing tool must have the ability to be integrated with reporting to abuse@michigan.gov. Bottom line, for every user we must have a clear, accurate phishing result of (1) Clicked, (2) Reported, (3) Neither
- The solution must be SCORM compliant
- Security Awareness Training courses completion metrics
- The solution must have the ability to import users account information from Microsoft Active Directory service exports.

3. IT ENVIRONMENT RESPOSIBILITIES

Contractor Hosted Software Solution

Definitions:
Facilities – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.

Infrastructure – Hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.
Platform – Computing server software components including operating system (OS), middleware (e.g., Java runtime, .NET runtime, integration, etc.), database and other services to host applications.
Application – Software programs which provide functionality for end user and Contractor services.
Storage – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations.
Backup – Storage and services that provide online and offline redundant copies of software and data.
Development - Process of creating, testing, and maintaining software components.

Component Matrix	**Contract components with contractor or subcontractor name(s)**
Facilities	AWS via KnowBe4
Infrastructure	AWS via KnowBe4
Platform	KnowBe4
Application	KnowBe4
Storage	AWS via KnowBe4
Backup	AWS via KnowBe4
Development	KnowBe4

4. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
State Employee & Contractors	Read	55,000	Up to 5,500

Contractor Solution must meet the expected number of concurrent Users.

5. Reserved

6. DATA RETENTION AND REMOVAL

The State will need to retain all data for the entire length of the Contract. Upon Contract expiration, the State must have the ability to export all data in KnowBe4's standard format, so that the State can retain data for at least 5 years after the last expenditure.

The State will need to retrieve data, even data that may be stored off-line or in backups.

7. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM, with supporting platforms, enterprise storage, monitoring, and management running in house and in cloud hosting provides.

8. SOFTWARE

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet.**

Contractor must provide a list of any third-party components, and open source component included with or used in connection with the deliverables defined within this Contract.

Mobile Responsiveness
If the software will be used on a mobile device as define in Schedule A – Table 1, Business Specification Worksheet, the Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

SOM IT Environment Access

To the extent Contractor has access to State systems Contractor will comply with the standards as set forth in **Schedule E – Data Security Requirements**.
Contractor must support integration with Active Directory and SAML 2.0 based single sign on (SSO).

9. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency.

The Contractor will need to provide the SOM Administrator's with training and training materials to properly administer the SECT solution and all available functionality in the solution. The administrator training duration should be dependent on the complexity of the solution and the amount of customization functionality the SOM administrator will be able to perform. Live WebEx/MS Teams training or on-site training is preferred for more complex solution administration activities so SOM Administrators may ask questions if needed.

10. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

The Contractor's user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests.

11. ADDITIONAL PRODUCTS AND SERVICES

Reporting
The State of Michigan (SOM) will require user activity reporting from the solution. The SOM Project Manager and administrators will require the ability to provide Enterprise statistics on pending training courses for employees from all agencies or from one specific agency as needed. The report will need to be shared with agency assigned sub-Managers to only track employee's progress in an assigned agency or agency group. The report will need to contain the following field elements: Employee Name, Agency, Course Name Outstanding, and date assigned. This report will require permissions such that 1) The SOM Project Manager/Administrator and backup Project Manager/Administrator will have full control to report all agencies or specific agencies, and 2) Agency sub-Managers can only report on limited agency users that have been delegated to them.

A similar report for course completions will be required with like permissions to track user courses completed by the Enterprise or sub agency users. The agency completion report needs to contain the following field elements: Employee Name, Agency, Course Completed Name, and Completion Date. As with the permissions above, the SOM SECT Project Manager/Administrator and the backup will require Enterprise-wide reporting abilities and sub-Managers will need delegated limited agency access.

The SECT solution will require a standard report of SOM employee data by agency so employee records can be reviewed in bulk and updates identified.

The SECT solution will require a standard employee report that lists all the training an employee completed or has not completed. Ideally employees would have access to print their own report if needed.

If the SECT solution includes a dashboard reporting feature on the above reports at a higher level with drill down functionality the bidder should insert examples below.

The SECT solution will allow the SOM SECT Administrators some level of customization in report generation. This may include ad hoc filtering on report data, inserting the SOM logo on report headers, exporting filtered raw data to Microsoft Excel or searching for specific data elements from assessment information captured in the SECT.

For all reports, provide role-based access control (RBAC) that limits what reports a user can run based on their role (admin, team leader, general user), and their agency (DTMB, DNR, etc.).

1. **Phishing Overall:** Generate the following report where AGENCY is driven from the department field in Active Directory with the use of smart groups. The “Ignored” metric is comprised of users that have been "delivered" an email, but have not "opened" it. The reports do not explicitly say "Ignored", however "Smart Groups" may be leveraged to generate a group of users that have received the email, but have not opened it. This data can be exported in CSV format. “Reported” are those people who clicked the Phish Alert Button in Outlook to report the phish. The “Clicked” means someone clicked on a link in the email or within an attachment. Attachment opens are tracked as "Attachment Opens". The “Clicked” should ignore clicks that do not come from the end user (for example, anti-malware tools interrogating the link or Demisto interrogating the link) if clicks come from an IP range that has been included in "Ignored IPs" list in the Phishing Tab of KMSAT. If they click multiple times during the same campaign that only counts as one.

Agency	# Ignored	# Clicked	# Reported	Total
DTMB	56	7	2	65
DNR	40	4	1	45
…				

All High level Percentages are available in the GUI but not all are available in exports. Some percentages such as "Phish Prone Percentage" are available in CSV/PDF exports such as. Raw numbers can be viewed in the GUI, or exported in CSV.

2. **Phishing Detail:** Reports are available at a user and group level. CSV reports may be sorted by any of the exportable fields.

3. **Phishing Repeat Offenders:** Shows individuals who failed more than one phish by clicking on multiple campaigns, sorted by the number of campaigns they failed.

4. **Awareness Training Overall:** Generate the following report where AGENCY is driven from the department field in Active Directory. This report is by agency and for one specific training class. This type of report was not available previously in Litmos.

Agency	# Not Started	# In Progress	# Complete	% Complete
DTMB	45	20	35	35%
DNR	30	10	10	20%
…				

5. **Awareness Training Detail:** Reports are available at a user and group level. CSV reports may be sorted by any of the exportable fields.

User Detail: Completion status for a particular user, for all awareness classes assigned to them.

Solution Implementation Plan

The SOM will have access to an Implementation Plan which will identify the typical process steps recommended by the Contractor to setup, configure, and deploy the proposed solution training to fifty-five thousand (55,000) SOM users. The Solution Implementation Plan shall outline all steps required, the timeframe for each step and the expected roles and responsibilities of the State of Michigan personnel during the implementation processes.

12. CONTRACTOR PERSONNEL

Contractor Contract Administrator. Contractor resource who is responsible to(a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
Name: Legal Department **Address: 33 N Garden Ave** **Clearwater, FL 33755-6604** **Phone: 855-566-9234** **Email: legal@knowbe4.com**

13. CONTRACTOR KEY PERSONNEL

Contractor Project Manager. Contractor resource who is responsible to serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services, matters pertaining to the receipt and processing of Support Requests and the Support Services.

The Contractor will identify a Contractor Project Manager and their duties shall include, but not be limited to:

- Subject matter expert in working knowledge of the product and product deployment
- Support the management of the Contract,
- Facilitate dispute resolution, and
- Advise the State of performance under the terms and conditions of the Contract.
- Work with the State to set up and implement the SECT solution
- Point of contact for SECT issue resolution
- Provide SECT update information on new course options
- Assist with SECT user administration if required
- Serve as the point person for all project issues

- Assess and report project feedback and status
- Escalate project issues, project risks, and other concerns
- Review all project deliverables and provide feedback
- Proactively propose/suggest options and alternatives for consideration
- Utilize change control procedures
- Act as ongoing contact person throughout the life of the contract

The State reserves the right to require a change in the current Contractor Project Manager (CPM) if the assigned CPM is not, in the opinion of the State, adequately serving the needs of the State.

Contractor
Name: Legal Department **Address: 33 N Garden Ave** **Clearwater, FL 33755-6604** **Phone: 855-566-9234** **Email: legal@knowbe4.com**

Contractor Security Officer. Contractor resource who is responsible to respond to State inquiries regarding the security of the Contractor's Solution. This person must have sufficient knowledge of the security of the Contractor Solution and the authority to act on behalf of Contractor in matters pertaining thereto.

Contractor
Name: InfoSec Team **Address33 N Garden Ave** **Clearwater, FL 33755-6604** **Email:** insfosec@knowbe4.com

CONTRACTOR PERSONNEL REQUIREMENTS
Contractor will provide the State with a designated Customer Service Manager (“CSM”) to assist the State’s administrators with onboarding and training on how to use the Products, and will be the State’s point of contact for any Product Support requests during the subscription term. If at any time the State is not satisfied with its CSM support, Contractor will provide the State with a replacement CSM within a reasonable time upon written request.

14. STATE RESOURCES/RESPONSIBILITIES

State resources remain blank until contract execution.

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Contract Administrator
Name: KeriAnn Trumble **Phone: 989-259-2625** **Email: trumblek1@michigan.gov**

Program Managers. The DTMB and Agency Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

DTMB Program Manager
Name: Smruti Shah **Phone: 517-582-4642** **Email: shahs1@michigan.gov**

Agency Program Manager
Name: Kemal Tekinel **Phone: 517-242-4287** **Email: TekinelK@michigan.gov**

15. ADDITONAL INFORMATION

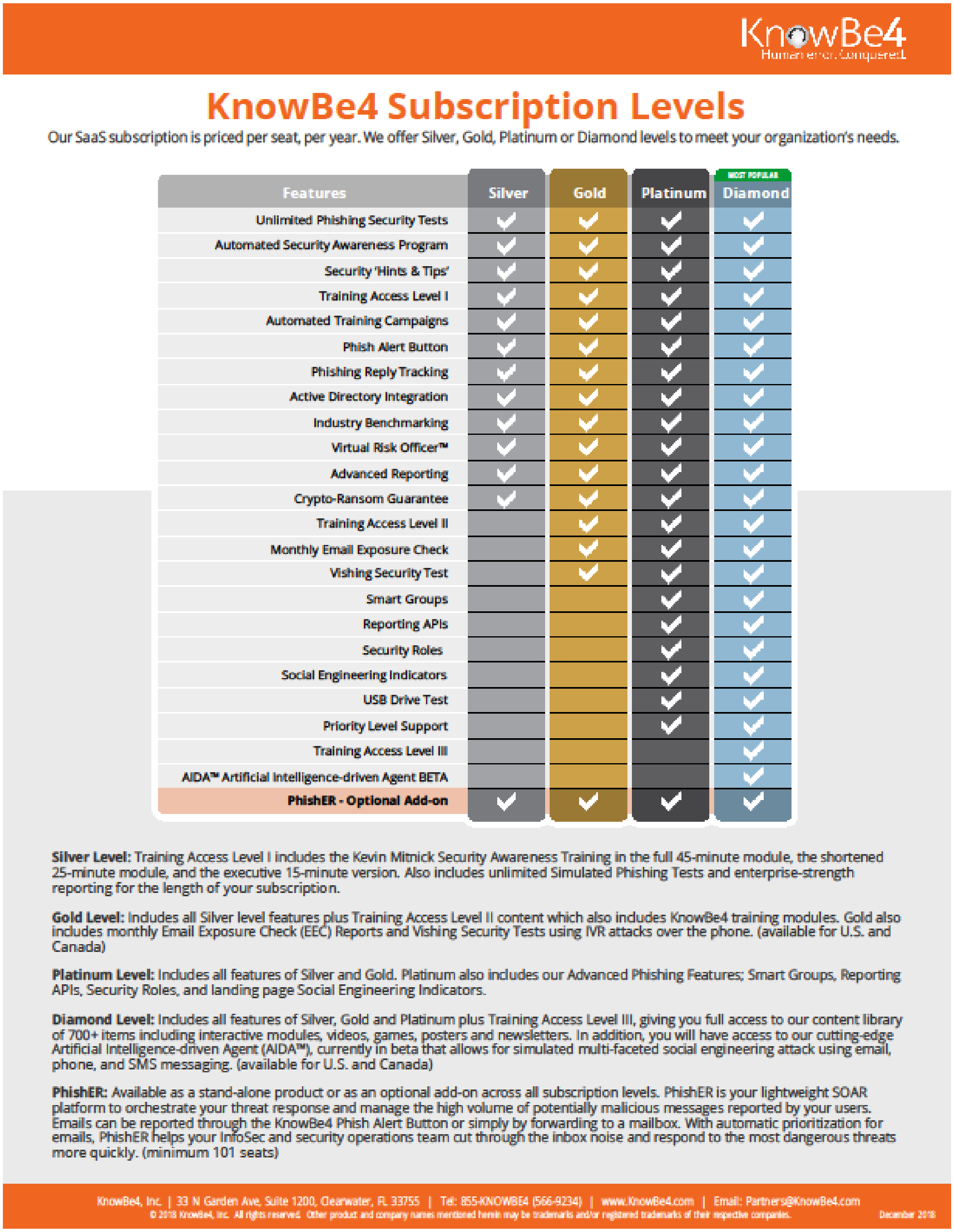
The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE A – TABLE 1 - Business Specification Worksheet

B
Business **Specifications**
Contractor Hosted Software Solution
All State Data including backups and Disaster Recovery will reside within the Continental United States of America (CONUS).
The proposed solution must be a Software as a Service (SaaS) solution that provides Security Awareness Training and advanced IT and managerial security training content courses.
The solution must have the ability to import users account information from Microsoft Active Directory service exports.
The solution content must allow branding of the State of Michigan logo.
The solution must provide email notification messages to employees when a class is available, with a URL link to the class and when they should complete the course by.
The learner experience and Courseware shall be Section 508 and ADA compliant.
The solution must be Sharable Content Object Reference Model (SCORM) compliant.
The Contractors SECT solution must be hosted in the United States.
The Contractors SECT solution user interface must maintain acceptable response times so users are not waiting more than two-four (2-4) seconds for pages to load.
The Contractors State of Michigan SECT solution must be sized to accommodate 55,000 users and up to 5,500 concurrent users
The Contractor must ensure that adequate security is in place to prevent access by non-authorized parties.
The Contractor must back up all SOM SECT data and perform restoration of data if needed.
SECT course content updates shall be available to SOM users for the duration of the contract.
The Contractor must ensure that all operating systems, applications and server maintenance tasks are configured in accordance with NIST industry best security practices and/or software provider recommendations.
Training shall communicate effectively to all staff on a non-technical level.
Training content shall be updated regularly as threats change and available to SOM users.
Training content shall be engaging, entertaining, interactive, relevant, utilizing a variety of instructional approaches.
The SECT shall have the ability to add the State of Michigan branding logo.
The SECT shall offer course content, brochure, poster, screensaver and newsletter customization functionality features.
The SECT solution must allow for user information updates to include mass updates such as organization name changes.
The SECT solution must deliver training using industry standard web browsers, without the need for installation of browser add-ons.
The SECT solution must have high availability and data recovery capabilities
The SECT solution shall allow administrators to make lessons required throughout the year.
The SECT solution shall allow for sub-organization administrative delegation so appointed SOM SECT Managers may monitor their organizations' employee training statistics and allocate role-based training packages agencies / sub-organizations purchase.
The SECT solution shall easily allow users to stop courses and pick up where they left off.

The SECT solution shall notify employees by email they have a class to take and track the employee’s training status, scores, and interactions.
The SECT solution shall offer brief 10–15 minute training classes for general Security Awareness topics.
The SECT solution shall provide employees with a certificate of completion once they have successfully completed each course.
Reports from the SECT solution will reflect users that have not completed assigned Security Awareness training and are sortable by agency.
Reports from the SECT solution that reflect users that have completed assigned Security Awareness Training that are sortable by agency.
SECT dashboard reporting abilities or standard reports the SOM Project Manager/Administrator and sub-agency managers will have access to use.
Phishing module must be compatible with SOM Office 365 email environment, excluding mobile Phish Alert Button deployment (Android, iOS).

SCHEDULE A - EXHIBIT 1 – KnowBe4 Subscription Levels



KnowBe4
Human error. Conquered.

KnowBe4 Subscription Levels

Our SaaS subscription is priced per seat, per year. We offer Silver, Gold, Platinum or Diamond levels to meet your organization's needs.

Features	Silver	Gold	Platinum	MOST POPULAR Diamond
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program	✓	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Crypto-Ransom Guarantee	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓
Smart Groups			✓	✓
Reporting APIs			✓	✓
Security Roles			✓	✓
Social Engineering Indicators			✓	✓
USB Drive Test			✓	✓
Priority Level Support			✓	✓
Training Access Level III				✓
AIDA™ Artificial Intelligence-driven Agent BETA				✓
PhishER - Optional Add-on	✓	✓	✓	✓

Silver Level: Training Access Level I includes the Kevin Mitnick Security Awareness Training in the full 45-minute module, the shortened 25-minute module, and the executive 15-minute version. Also includes unlimited Simulated Phishing Tests and enterprise-strength reporting for the length of your subscription.

Gold Level: Includes all Silver level features plus Training Access Level II content which also includes KnowBe4 training modules. Gold also includes monthly Email Exposure Check (EEC) Reports and Vishing Security Tests using IVR attacks over the phone. (available for U.S. and Canada)

Platinum Level: Includes all features of Silver and Gold. Platinum also includes our Advanced Phishing Features; Smart Groups, Reporting APIs, Security Roles, and landing page Social Engineering Indicators.

Diamond Level: Includes all features of Silver, Gold and Platinum plus Training Access Level III, giving you full access to our content library of 700+ items including interactive modules, videos, games, posters and newsletters. In addition, you will have access to our cutting-edge Artificial Intelligence-driven Agent (AIDA™), currently in beta that allows for simulated multi-faceted social engineering attack using email, phone, and SMS messaging. (available for U.S. and Canada)

PhishER: Available as a stand-alone product or as an optional add-on across all subscription levels. PhishER is your lightweight SOAR platform to orchestrate your threat response and manage the high volume of potentially malicious messages reported by your users. Emails can be reported through the KnowBe4 Phish Alert Button or simply by forwarding to a mailbox. With automatic prioritization for emails, PhishER helps your InfoSec and security operations team cut through the inbox noise and respond to the most dangerous threats more quickly. (minimum 101 seats)

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Partners@KnowBe4.com

December 2018

SCHEDULE B – PRICING

The following pricing is valid for the Term of the contract and includes all costs for subscription licensing and support.

Subscription Pricing					
Product	**Product Description**	**Quantity**	**Term**	**Product Price for Term**	**Total price**
KMSATD- N-K60-G	KnowBe4 Security Awareness Training Diamond Subscription	55,000	60 Months	$9.09	$499,950.00
MediaPro- N-60-G	MediaPro Training Center Access Subscription 1 Year	1	12 Months*	$0.00	$0.00

*MediaPro Training Center Access Subscription Term begins on 03/20/2022 and ends after 03/19/2023. This subscription is excluded from Additional Subscription Purchases

Additional Subscription Purchases

The State may purchase additional diamond level subscriptions at the rate listed above, as set forth in Section ***3.4 Customer Users*** and Section ***9.3 Pricing/Fee Changes*** of the Master Agreement.

Optional Product Pricing (per user with 55,000 subscriptions)						
Product	**Product Description**	**5 Year Price**	**4 Year Price**	**3 Year Price**	**2 Year Price**	**1 Year Price**
PhishER Add-on	Security Orchestration, Automation and Response (SOAR) platform	$7.20	$5.76	$4.32	$3.06	$1.80
Compliance Plus Add-on	Access to Compliance Plus Library for additional compliance training	$4.32	$3.46	$2.59	$1.84	$1.08

Optional Services Pricing		
Service	**Service Description**	**Rate**
Customization	Security Awareness Course Content Customization	$200.00/hour

SCHEDULE C - INSURANCE SCHEDULE

Required Coverage.

1. Insurance Requirements. Contractor, at its sole expense, must maintain the insurance coverage identified below. All required insurance, except for cyber/professional, must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or otherwise result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Personal & Advertising Injury $2,000,000 Products/Completed Operations $2,000,000 General Aggregate	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: $1,000,000 Each Claim $1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

If any of the required policies provide claims-made coverage, the Contractor must: (a) provide coverage with a retroactive date before the Effective Date of the Contract or the beginning of Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (c) if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Contract Effective Date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or delivery order number, at Contract formation and within twenty (20) calendar days of the expiration date of the applicable policies; (b) notify the Contract Administrator promptly if any insurance is cancelled; and (c) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

This Section is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

SCHEDULE D - SERVICE LEVEL AGREEMENT

This Service Level Agreement ("SLA") is for the provisioning of services required to support and sustain the Products under the Agreement to which this SLA is attached.

Term

This SLA is valid for the subscription term specified in the applicable Quote. Termination of the Agreement and/or a Quote will result in termination of this SLA.

Availability & Uptime

KnowBe4 agrees to: (a) make the Products available to Customer pursuant to the Agreement and the applicable Quote, (b) provide support for the Products to Customer at no additional charge, and/or upgraded support if purchased; and (c) use commercially reasonable efforts to make the online Services available 99.9% of the time to be measured annually, excluding any planned downtime, maintenance windows, or any unavailability caused by circumstances beyond KnowBe4's reasonable control, such as a force majeure event in accordance with the Agreement. If Customer would like to receive status updates on the availability of KnowBe4's Products, Customer may subscribe to receive updates at https://status.knowbe4.com/, or such other URL as KnowBe4 may provide from time to time.

CSM

Customer will be assigned a designated customer service manager ("**CSM**") to assist the Customer's admin with onboarding and training on how to use the Products, as applicable.

Maintenance Windows

Maintenance windows for other Products not specified below may be found on the KnowBe4 Documentation page, as defined in the Agreement.

- **KMSAT** maintenance windows may be found at https://support.knowbe4.com/hc/en-us/articles/360024057834-KnowBe4-Security-Awareness-Training-KMSAT-Site-Maintenance-, or such other URL as KnowBe4 may provide from time to time.
- **KCM GRC** maintenance windows may be found at https://support.knowbe4.com/hc/en-us/articles/360025164193-KCM-GRC-Platform-Maintenance-Window, or such other URL as KnowBe4 may provide from time to time.
- **PhishER** maintenance windows may be found at https://support.knowbe4.com/hc/en-us/articles/360025164473-PhishER-Platform-Site-Maintenance-, or such other URL as KnowBe4 may provide from time to time.

Support

KnowBe4's support parameters, including its support hours, may be found at https://www.knowbe4.com/hubfs/KnowBe4-Support-Document.pdf?t=1518625292505, or such other URL as KnowBe4 may provide from time to time. To make a support request, Customer may submit a ticket at https://support.knowbe4.com/hc/en-us/requests/new, or such other URL as KnowBe4 may provide from time to time.

Customer Requirements

Customer responsibilities and/or requirements in support of this SLA include: (a) Customer's compliance with the Agreement and the applicable Quote; (b) reasonable availability of Customer's admin and/or technical representative(s) when resolving a service-related incident or request; and (c) providing proper notice of KnowBe4's non-compliance with any Product or Service warranty in accordance with the Agreement and sufficiently detailing the non-compliance in a manner that enables KnowBe4 to properly assist with the remediation. KnowBe4 will not be responsible for delays in remediation caused by Customer's failure to respond to requests by KnowBe4. Customer understands that the Products and Services will only operate in accordance with KnowBe4's Documentation, as defined in the Agreement, and it is Customer's responsibility to ensure that the Products and Services will be fit for its purposes and to ensure that the Products and Services will be supported by Customer's technology and business environment. Customer understands that KnowBe4's Products and Services are non-mission critical to Customer's business.

Response Times

In support of services outlined in this SLA, KnowBe4 will respond to service-related incidents and/or requests submitted by Customer within the following time frames:

- Within 2 business days for issues classified as **High Priority**.
  - "**High Priority**": Complete failure of platform or the complete unavailability of core functionality such as training and phishing.
- Within 3 business days for issues classified as **Medium Priority**.
  - "**Medium Priority**": Impacted operations, core operations such as user and admin login operational but functionality impaired or requiring workarounds to achieve documented operation.
- Within 5 business days for issues classified as **Low Priority**.
  - "**Low Priority**": Inconvenience due to operations not performing as defined or at a significantly degraded speed.

KMSAT Support Tiers

Tier 1 Support will assist with:

- Password resets
- Phishing and Training Campaign creation
- Explaining overall navigation of the KMSAT Products
- Providing KnowBe4's recommended best practices
- Issues accessing the training console
- Whitelisting to ensure successful delivery of email from our servers
- Issues related to accessing/completion of training modules
- Resolving phishing/training result discrepancies
- SAML Single Sign-On support and troubleshooting
- Phish Alert Button installation
- Active Directory Integration support
- Channel partner support

Tier 2 and Tier 3 Support will be available for the escalation of more advanced support requests related to issues occurring with the KMSAT Products.

Channel Partners

In the event Customer purchases through a KnowBe4-authorized channel partner, such channel partner may have its own SLA associated with the purchase. Customer acknowledges that KnowBe4 is not responsible, nor is KnowBe4 liable, for ensuring compliance with such channel partner SLA.

SCHEDULE E - INFORMATION SECURITY REQUIREMENTS

1. **Security.**

   a. KnowBe4 will maintain Customer Confidential Information and its information technology environment secure from unauthorized access by using commercially reasonable efforts and industry standard organizational, physical and technical safeguards, and refrain from implementing changes that materially lower the level of security protection provided as of the Effective Date of the Agreement. KnowBe4 will comply with the minimum security standards set forth in this Exhibit and provide prior written notice to Customer of any significant changes to KnowBe4's information security policy that would lessen the security posture of the environment.

   b. KnowBe4 will conduct a SOC-2 Type 2 or such similar or successor audit on an annual basis. Upon request, KnowBe4 will provide Customer with a copy of such audit report and promptly remediate and/or mitigate any non-conformance findings in like with KnowBe4's existing vulnerability remediation process. Such audit report will be considered Confidential Information of KnowBe4.

2. **Audit Rights.** Not more than once per calendar year during the term of the Agreement and with at least thirty (30) days' prior written notice by Customer to KnowBe4, Customer may, at Customer's sole expense, audit KnowBe4 to verify compliance with the terms and conditions of this Exhibit. Such audit will be:

   a. Completed within two (2) weeks;

   b. Performed during KnowBe4's regular business hours in a manner that, in KnowBe4's reasonable judgment, does not disrupt or degrade KnowBe4's regular business operations and is done in accordance with KnowBe4's security and data protection policies;

   c. Limited to KnowBe4's facilities and personnel of KnowBe4 in scope of this Agreement; and

   d. Conducted by either Customer's employees or, with KnowBe4's approval, by an independent third party agreed to by the parties.

   Customer may create an audit report summarizing the findings and observations of the audit ("Audit Report"). Audit Reports are deemed to be Confidential Information of KnowBe4 and the Customer will not disclose the Audit Reports to third parties except to Customer's legal counsel and consultants bound by obligations of confidentiality using at least the same degree of care Customer employs in maintaining in confidence its own Confidential Information of a similar nature, but in no event less than a reasonable degree of care. Customer will disclose the results of its audit to KnowBe4 within one week after its completion. KnowBe4 will promptly respond to audit findings and, at KnowBe4's expense, discuss the findings with Customer, and if applicable, remediate and/or mitigate any critical and high risk findings to the satisfaction of Customer.

3. **Technical Security Controls.** With respect to KnowBe4 infrastructure that processes, stores, or transmits Customer Confidential Information, KnowBe4 will use the following technical security controls where applicable (and keep them current by incorporating and using all updates commercially available):

   a. Network Protection

      (i) Network based firewalls or equivalent

      (ii) Network intrusion detection/protection systems

   b. Client Protection

      (i) Malware and malicious code protection is applied to all applicable workstations. No workstations are permitted to store or process customer data

      (ii) Host-based firewall/intrusion prevention software that blocks activity not directly related to or useful for business purposes

   c. System and Software Protection

      (i) All system and applications must utilize secure authentication and authorization mechanisms

      (ii) All KnowBe4-developed applications must be designed and implemented using secure coding standards and design principles (e.g., OWASP)

      (iii) Operating systems must be hardened appropriately according to industry standard practices

      (iv) Systems must be inspected for known vulnerabilities and all identified known vulnerabilities must be patched as soon as reasonably possible

   d. Encryption

      (i) KnowBe4 will review and update encryption configurations on all systems that utilize encryption. KnowBe4 will utilize only modern industry accepted encryption algorithms, ciphers, modes and key sizes

   e. Customer Confidential Information Protection

      (i) Customer Confidential Information Access: KnowBe4 will ensure that only authorized individuals (based on role) will, on behalf of KnowBe4, have access to Customer Confidential Information

      (ii) Customer Confidential Information Storage: KnowBe4 will not process Customer Confidential Information on or transfer such to any portable storage medium, unless the storage medium is fully encrypted in accordance with encryption requirements set forth in this Exhibit

      (iii) Customer Confidential Information Transmission: All transmission or exchange of Customer Confidential Information by Company will use secure protocol standards in accordance with encryption requirements set forth in this Exhibit

4. **Incidents.**

   a. If KnowBe4 becomes aware of any unauthorized access to the Customer Confidential Information on systems owned, managed, or subcontracted by KnowBe4, KnowBe4 will without undue delay, notify Customer; consult and reasonably cooperate with investigations and potentially required notices; and provide any information reasonably requested by Customer

   b. In the event of a breach or any unauthorized disclosure of Customer Confidential Information, at no additional cost to Customer, KnowBe4 will reasonably cooperate with Customer in investigating the incident including, but not limited to, the provision of system, application, and access logs, conducting forensics reviews of relevant systems, imaging relevant media, and making personnel available for interview

   c. On notice of any actual breach, KnowBe4 will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the breach in accordance with industry standard practices

5. **Integration.** The terms of this Exhibit apply in addition to, not in lieu of, any other terms and conditions agreed with KnowBe4, except as specifically and expressly agreed in writing with explicit reference to this Exhibit.

6. **Training.** KnowBe4 will periodically provide those employees, consultants, and any approved third parties (affiliated or not) that manage, or have access to, Confidential Information, including personally identifiable information, provided or made available by Customer, with privacy and security awareness training.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **071B7700119**

CONTRACTOR	KnowBe4, Inc
	33 N Garden Ave
	Clearwater, FL 33755-6604
	Sarah Hughes
	855-566-9234
	smchugh@knowbe4.com
	VS0179188

STATE	Program Manager	Smruti Shah	DTMB
		517-582-4642	
		shahs1@michigan.gov	
	Contract Administrator	KeriAnn Trumble	DTMB
		989-259-2625	
		trumblek1@michigan.gov	

CONTRACT SUMMARY

SECURITY TRAINING

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
March 28, 2017	March 28, 2022	5 - 1 Year	March 28, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		March 28, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$481,220.00	$6,760.00	$487,980.00

DESCRIPTION

Effective 1/31/2022, this Contract is increased by $6,760.00 to purchase Enterprise Phishing simulations for DTMB. All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
525 W ALLEGAN ST., LANSING, MI 48913
P.O. BOX 30026, LANSING, MI 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**
to
Contract Number **071B7700119**

CURRENT CONTRACTOR	MediaPro Holdings, LLC
	20021 120th Avenue NE
	Bothell, WA 98011
	David Nelson
	425-483-4702
	David.nelson@mediapro.com
	CV0135517

NEW CONTRACTOR	KnowBe4, Inc
	33 N Garden Ave
	Clearwater, FL 33755-6604
	Sarah Hughes
	855-566-9234
	smchugh@knowbe4.com
	VS0179188

STATE CONTACTS

Program Manager	Rock Rakowski	DTMB-IT	Contract Administrator	KeriAnn Trumble	DTMB
	517-898-6028			989-259-2625	
	RakowskiJ@Michigan.gov			Trumblek1@Michigan.gov	

CONTRACT SUMMARY

DESCRIPTION: ENTERPRISE SECURITY TRAINING

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
March 28, 2017	March 28, 2022	5 – 1 Year	March 28, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-card	☐ Direct Voucher (DV)	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		March 28, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$481,220.00	$0	$481,220.00

DESCRIPTION: Effective 10/14/2021, The Contractor for this Contract is changed to KnowBe4, Inc. Please note the Contract Administrator has been changed to KeriAnn Trumble.

All other terms, conditions, specifications, and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **071B7700119**

CONTRACTOR	
	MediaPro Holdings, LLC
	20021 120th Avenue NE
	Bothell, WA 98011
	David Nelson
	425-483-4702
	david.nelson@mediapro.com
	*******3354

STATE			
Program Manager	Rock Rakowski	DTMB-IT
	517-898-6028	
	RakowskiJ@Michigan.gov	
Contract Administrator	Mike Breen	DTMB
	(517) 284-7002	
	breenm@michigan.gov	

CONTRACT SUMMARY			
ENTERPRISE SECURITY TRAINING			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
March 28, 2017	March 28, 2022	5 - 1 Year	March 28, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ Direct Voucher (DV)	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		March 28, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$352,220.00	$129,000.00	$481,220.00

DESCRIPTION

Effective with mutual signature the contract is amended to add Phishing software as a service module and adding $129,000.00 to acquire that module. All other terms and condtions remain the same.

Technology, Management & Budget

MICHIGAN DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET IT SERVICES STATEMENT OF WORK

Project Title: **Media Pro Phishing SaaS Contract Amendment**	**Period of Coverage:** **03/28/2017 – 03/28/2018**
Requesting Department: **DTMB-CIP/MCS**	**Date:** **5/2/2017**
Agency Sponsor: **Richard Reasner**	**Phone:** **517-241-4090**
DTMB Managers: **Rock Rakowski / Natalie Lake**	**Phone:** **517-898-6028 / 517-241-0344**

Brief Description of Services to be provided:

SWERVICES TO BE PROVIDED AND BACKGROUND:

The State of Michigan (SOM, State), throught the Department of Technology, Management & Budget (DTMB) has issued a contract with MediaPro Holding, LLC to provide the State with Enterprise Security Training as a Software as a Service (Saas).

MediaPro Holding, LLC will provide the State a hosted Software as a Service (SaaS) Security Awareness training solution that is compliant with FISMA and NIST special publications for approximately fifty thousand (50,000) employees for the next five (5) years.

This Statement of Work (SOW) is a **change request** SOW for modification to the orginal contract with MediaPro Holding, LLC, contract number #071B7700119. DTMB-CIP/MCS wishes to purchase MediaPro's Phishing Software as a Service (SaaS) as an add on product to the Security Training SaaS. The funding to be added to the orginal contract to cover the Phishing SaaS for the duration of the five (5) year contract is in the total amount of $129,000.00, each yearly installment price will be $25,800.00.

PROJECT OBJECTIVE:

State of Michigan network users are required to participate in Security Awareness Training (SECT) activities yearly. Almost every year training is deployed to users advising them of the warning signs and dangers associated wtih phishing emails. The MediaPro Phishing product will simulate phishing emails that can be sent out to SOM users and test training effectiveness and measure employee responses to the email.

Periodic testing reminds users to apply the knowledge they have gained and works as a refresher to those that might have forgotten to look for email warning signs.

SCOPE OF WORK:

Purchase 50,000 yearly user licenses of MediaPro's Phishing software

TASKS:

The Contractor will provide all infrastructure and software maintenance for the Phishing solution in accordance with industry best security practices defined by FISMA and NIST guidance to provide adequate security and prevent access by non-authorized parties.

Contractors will contemplate that the Phishing solution will be configured, tested and in operation by mid June 2017.

The Contractor will assist the State of Michigan with the setup, configuration and implementation of the Phishing solution.

DELIVERABLES:

- Contractor hosted solution to provide Phishing Software as a Service (SaaS) email services
- Contractor will provide Maintenance and Support of the Phishing solution in compliance with FISMA and NIST
- Contractor will assist with User file imports and deletes
- Program introduction and administrator training
- First campaign walkthrough guidance with MediaPro team
- Full access to assessment, testing, education, and reporting tools
- Access to library of 150 phishing emails and landing pages
- Unlimited campaigns

ACCEPTANCE CRITERIA:

Phishing test completed successfully.
Medric reports on user response are available.
No system error's.
Sign-off of Project Sponsor on the first implementation test.

PROJECT CONTROL AND REPORTS:

A bi-weekly implementation progress report will be submitted to the Agency Project Manager up through Solution Implementation, at which point bi-weekly progress reports will be submitted monthly through the life of this Contract. Each progress report will contain the following:

- Any planned solution updates or changes
- Functionality changes or updates
- New Reporting features or help guides
- Project Issues
- Project Risks
- Project Change Requests
- Work completed since last report and work to be done before the next reporting date

SPECIFIC DEPARTMENT STANDARDS:

Agency Specific Technical Environment Requirements for the SECT Solution

- The Contractors Phishing solution will be hosted in the United States.
- The Contractor will back up all SOM Phishing data and perform restoration of data if needed.
- The Contractor will ensure that all operating systems, applications and server maintenance tasks are configured in accordance with NIST industry best security practices and/or software provider recommendations.
- The Contractor will ensure that adequate security is in place to prevent access by non-authorized parties.
- The Contractor will destroy all SOM data on termination of the contract after the State of Michigan receives deliverables.
- The solution will have the ability to import users account information from Microsoft Active Directory service exports.

PAYMENT SCHEDULE:

Method of Payment

This will be a firm, fixed price Contract modification based on the following deliverables

- Initial Subscription Payment – 100% of first year subscription contract amount after signature and approval of the DTMB Agency Project Manager of:
    - Deliverable – Phishing SaaS Setup and Configuration
    - Deliverable – Phishing Support Services
    - Deliverable – Testing & Implementation
    - Deliverable – User Phishing Response Reporting
    - Successful testing of deliverables above.

- Payment for renewal subscriptions will be paid yearly on the contract start date anniversary thereafter.

Payment will be made on the Satisfactory acceptance of the defined milestone above. DTMB will pay CONTRACTOR upon receipt of properly completed invoice(s) which shall be submitted to the billing address on the State issued purchase order. DTMB Accounts Payable area will coordinate obtaining Agency and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date, and must be approved by the Agency and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed, the progress of the project, and fees.

Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

EXPENSES:

The State will NOT pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:

The designated Agency Sponsor is:

Richard Reasner
DTMB CIP -MCS
515 Westshire Dr.
Lansing MI 48917
517-373-3832
ReasnerR@michigan.gov

The designated DTMB Project Manager is:

Rock Rakowski
DTMB CIP -MCS
515 Westshire Dr.
Lansing MI 48917
517-898-6028
RakowskiR@michigan.gov

AGENCY RESPONSIBILITIES:
State Project Manager- (MDTMB and Agency)
MDTMB will provide a Project Manager who will be responsible for the State's infrastructure and coordinate with the Contractor in determining the solution configuration.

The State's Project Manager will provide the following services:

- Coordinate the State resources necessary for the project

- Facilitate coordination between various external Contractors
- Facilitate communication between different State departments/divisions
- Provide acceptance and sign-off of deliverable/milestone
- Review and sign-off of timesheets and invoices
- Resolve project issues
- Escalate outstanding/high priority issues
- Utilize change control procedures
- Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
- Document and archive all important project decisions
- Arrange, schedule and facilitate State staff attendance at all project meetings.

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

The work is to be performed, completed, and managed at the Contractor work site location(s) in the United States.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:

Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.

No overtime will be permitted.

This purchase order is a change request for Contract Number #071B7700119. This purchase order, statement of work, and the terms and conditions of Contract Number #071B7700119 constitute the entire agreement between the State and the Contractor.

Attachment A - Cost Table

Applicable MediaPro Price Table Options

***SaaS Self Service** - The self-managed application suite works well for businesses that prefer in-house or hands on analytics and training. This program includes:*

- Program introduction and administrator training
- First campaign walkthrough guidance with MediaPro team
- Full access to assessment, testing, education, and reporting tools
- Access to library of 150 phishing emails and landing pages
- Unlimited campaigns

Phishing & Social Engineering Campaigns	Users	License Fee
Base 1 year cost	50,000	$28,660

For the State of Michigan 5 year contract, the annual payment will be:

Payments 1 through 5 ***$25,800 x 5 = $129,000.00***

Quotation provided by:

***David Nelson | MEDIAPRO** | 1-425-483-4702 (office)*

MEDIAPRO
Learn. Improve. Succeed.

Phishing Simulator Tool Proposal for State of Michigan

Executive Summary: MediaPro offers best-in-class security awareness training and reinforcement programs to the world's most security-conscious companies. Given our extended history and innovative approach, we believe we are uniquely suited to help create a security-aware culture within your organization.

Deliverables: Pricing and Access to the "Phishing" training content and the MediaPro Phishing Simulator.

MediaPro Phishing Simulator:

Managed Service - up to four (4) simulated phishing and social engineering campaigns:
With the managed service, MediaPro operates your anti-phishing program on your behalf. Experienced experts assess your employees' behavior to identify the most effective training messages and improve employee performance. The Managed Service is perfect for companies that prefer to outsource training and analytics to experienced experts or minimize employee involvement. The program includes:

- Program guidance by our experienced team
- Assessment, education, and reporting tools
- Post campaign reports that include campaign results, metrics, and risk-based observations
- Access to library of 150 phishing emails and landing pages

Phishing & Social Engineering Campaigns	Users	License Fee
1 year	50,000	$39,370

SaaS Self Service - The self-managed application suite works well for businesses that prefer in-house or hands on analytics and training. This program includes:

- Program introduction and administrator training
- First campaign walkthrough guidance with MediaPro team
- Full access to assessment, testing, education, and reporting tools
- Access to library of 150 phishing emails and landing pages
- Unlimited campaigns

Phishing & Social Engineering Campaigns	Users	License Fee
Base 1 year cost	50,000	$28,660

For the State of Michigan 5 year contract, the annual payment will be:
Payments 1 through 5 $25,800 x 5 = $129,000.00

Quotation provided by:

David Nelson | MEDIAPRO | 1-425-483-4702 (office)

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
P.O. BOX 30026 Lansing, MI 48909
525 W. Allegan, Lansing, MI 48913

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **071B7700119**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	MediaPro Holdings, LLC
	20021 120th Avenue NE, Suite 102
	Bothell, WA 98011
	David Nelson
	425-483-4702
	David.nelson@mediapro.com
	3354

STATE	Program Manager	Rock Rakowski	DTMB
		RakowskiJ@Michigan.Gov	
		517-898-6028	
	Contract Administrator	Michael Breen	DTMB
		breenm@michigan.gov	
		517-284-7002	

CONTRACT SUMMARY			
DESCRIPTION: Enterprise Security Training			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
3-28-2017	3-28-2022	5 one year options	3-28-2022
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45			
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card	☐ Direct Voucher (DV)	☐ Other	☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
Per bid 007116B0008932 this contract is hereby granted with the attached documentation. Orders for delivery of service will be issued directly through the issuance of a Purchase Order.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$352,220.00**

FOR THE CONTRACTOR:

____
Company Name

____
Authorized Agent Signature

____
Authorized Agent **(Print or Type)**

____
Date

FOR THE STATE:

____
Signature

____
Name & Title

____
Agency

____
Date

SCHEDULE A

Security Training (SECT)
Statement of Work (SOW)

1.000 Project Identification

1.001 PROJECT REQUEST

The State of Michigan (SOM, State), through the Department of Technology, Management & Budget (DTMB) has issued a contract with a qualified firm to provide the State with a Software as a Service (SaaS), vendor hosted solution to provide Security Awareness and Role Based security training to State employee's.

The State seeks to have the project begin within twenty one (21) days after the execution of the contract, as per the approximate date indicated on the cover page of the contract. The negotiated contract will have a term of one five (5) year contract, with five, 1 year extension options. Contract option year extensions will be at the sole discretion of the SOM and will be based upon funding and acceptable performance of the product as determined by the SOM.

1.002 BACKGROUND

The State of Michigan (SOM) in accordance with the Federal Information Security Modernization Act (FISMA) is required to provide the State of Michigan employees and Contractors general Security Awareness Training as defined in the National Institute of Standards and Technology (NIST) Special Publications 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, 800-50 Building an Information Technology Security Awareness and Training Program, and Role-Based Security training as defined in NIST 800-16 Role-Based Model for Federal Information Technology / Cyber Security Training.

The State of Michigan (SOM) requires a Contractor hosted Software as a Service (SaaS) Security Awareness training solution that is compliant with FISMA and NIST special publications for approximately fifty thousand (50,000) employees. The solution implementation start date for Security Awareness training is required to start in May of 2017 and will commence in short phases to all SOM employees within thirty (30) days.

State of Michigan employees are required to participate in Security Training (SECT) activities yearly and new hires need to complete select core security courses before starting daily work activities and accessing SOM information systems and data.

Role-based security training will include Knowledge and Skills courses defined in Appendix B of the NIST Special Publication 800-16 Revision 1 (2nd Draft, Version 2) A Role-Based Model for Federal Information

Technology / Cyber Security Training or http://csrc.nist.gov/publications/drafts/800-16-rev1/sp800_16_rev1_3rd-draft.pdf Appendix B.

Security Awareness training and Role-based security training are required to prevent security incidents, and safe guard all State of Michigan assets.

1.100 Scope of Work and Deliverables

1.101 IN SCOPE

- Security Awareness & Role-based Software as a Service (SaaS), Contractor hosted solution.
- Security Awareness Training course content
- Role-Based Security Training course content
- Maintenance and Support of the solution in compliance with FISMA and NIST
- User file imports and deletes if a Single Sign-on solution cannot be established

A more detailed description of the required SECT Software as a Service (SaaS) solution and deliverables for this project is provided in **Schedule A**, Section 1.104, Work and Deliverables.

1.102 OUT OF SCOPE

- State of Michigan hosted solution

1.103 ENVIRONMENT

The links below provide information on the State's Enterprise information technology (IT) policies, standards and procedures which includes security policy and procedures, eMichigan web development, and the State Unified Information Technology Environment (SUITE).

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractors are expected to provide Contract's that conform to State IT policies and standards. All services and products provided as a result of this contract will comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response.

Enterprise IT Policies, Standards and Procedures:
http://michigan.gov/dtmb/0,4568,7-150-56355_56579_56755---,00.html

All software and hardware items provided by the Contractor will run on and be compatible with the MDTMB Standard Information Technology Environment.

It is recognized that technology changes rapidly. The Contractor may request, in writing, a change in the standard environment, providing justification for the requested change and all costs associated with any change. The State's Project Manager will approve any changes, in writing, and MDTMB, before work may proceed based on the changed environment.

Enterprise IT Security Policy and Procedures:
http://www.michigan.gov/documents/dmb/1210.32.pdf
http://www.michigan.gov/documents/dmb/1325_193160_7.pdf
http://www.michigan.gov/documents/dmb/1335_193161_7.pdf
http://www.michigan.gov/documents/dmb/1340_193162_7.pdf

The State's security environment includes:

MDTMB Single Login.
Secured Socket Layers.
RSA SecureID (State Security Standard for external network access and high risk Web systems)
Policies and procedures to achieve compliance with FISMA and NIST IT security controls

The State's Partner security environment will include:

TLS or Secured Socket Layers Web encryption
Policies and procedures to achieve compliance with FISMA and NIST IT security controls

ADA Compliance

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's solution conform, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may provide a description of conformance with the above mentioned specifications by means of a completed Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. Any additional compliance requirements will be specified in the Statement of Work.

See DTMB Policy at http://www.michigan.gov/documents/dmb/1650.00_209567_7.pdf?20151026134621.

The State Unified Information Technology Environment (SUITE):

Includes standards for project management, systems engineering, and associated forms and templates – will be followed: http://www.michigan.gov/suite

Agency Specific Technical Environment Requirements for the SECT Solution

- The Contractors SECT solution will be hosted in the United States.
- The Contractors SECT solution will be compatible with current versions of Internet Explorer and upgraded as needed for future versions.
- The Contractor will back up all SOM SECT data and perform restoration of data if needed.
- The Contractor will ensure that all operating systems, applications and server maintenance tasks are configured in accordance with NIST industry best security practices and/or software provider recommendations.
- The Contractor will ensure that adequate security is in place to prevent access by non-authorized parties.
- The Contractors State of Michigan SECT solution will be sized to accommodate 50,000 users and not limit the number of concurrent users.
- The Contractors SECT solution user interface will maintain acceptable response times so users are not waiting more than two-four (2-4) seconds for pages to load.
- The Contractor will destroy all SOM data on termination of the contract after the State of Michigan receives deliverables.
- The solution User Interface will be Section 508 and ADA compliant.
- The solution content will allow branding of the State of Michigan logo.
- The solution will follow Advanced Distributed Learning (ADL) Experience API specifications also known as Tin Can API, and be Sharable Content Object Reference Model (SCORM) compliant.
- The SECT solution will deliver training using industry standard web browsers, without the need for installation of browser add-ons.

- The solution will have the ability to import users account information from Microsoft Active Directory service exports.
- The solution will provide email notification messages to employees when a class is available, with a URL link to the class and when they should complete the course by.

1.104 WORK AND DELIVERABLES

The State of Michigan has procured a Security Training (SECT) solution as a Software as a Service (SaaS), Contractor hosted solution. The Contractor's solution will assist the State of Michigan (SOM) in complying with NIST Special Publications 800-50 Building an Information Technology Security Awareness and Training Program and 800-16 Role-Based Model for Federal Information Technology / Cyber Security Training special publications.

The Contractor will provide all infrastructure and software maintenance for the SECT solution in accordance with industry best security practices defined by FISMA and NIST guidance to provide adequate security and prevent access by non-authorized parties.

The Contractor will work with the State of Michigan to establish a Single Sign-on solution by utilizing Microsoft's Active Directory's Azure, Federated Services, Rights Management Services, or another compatible Lightweight Directory Access Protocol (LDAP) utility to read or securely import specific SOM user data for use by the SECT solution.

The SECT solution will follow Advanced Distributed Learning (ADL) Experience API (xAPI) specifications to enhance the user learning experience, track training progress and user experience statistics. The SECT course content will be Sharable Content Object Reference Model (SCORM) compliant.

Contractors will contemplate that the SECT solution will be configured, tested and in operation by May 2017 and training courses will start shortly thereafter.

The Contractor will assist the State of Michigan with the setup, configuration and implementation of the SECT solution.

The State of Michigan (SOM) will purchase a bulk five (5) year subscription package for Security Awareness Training courses for fifty thousand (50,000) SOM employees with bundled Role-Based Security Training courses included in the base subscription pricing package for Security Awareness training.

A. Security Training Solution Requirements

The Contractor's solution will assist the State of Michigan (SOM) in complying with NIST Special Publications 800-50 Building an Information Technology Security Awareness and Training Program and 800-16 Role-Based Model for Federal Information Technology / Cyber Security Training special publications by offering course content on the following:

Core Security Awareness Topic's include:

Intro to Security Awareness
Computer Security
Protecting Data Assets
Email Security
Reporting Incidents
Passwords
Phishing
Office Security
Social Networking
Web Security
Public Wi-Fi
Mobile Security Including Bring Your Own Device (BYOD)
Identity Theft
Social Engineering (email, Phone, In Person, Instant Messaging)
Acceptable Use
Safe Disposal
Information Privacy

All Security Awareness course content will be available to State employee's for the duration of the contract to include any exercised option years.

Role-Based Security Knowledge and Skills Training Catalog in compliance with NIST 800-16 will include:

Overall Security Management courses
Advanced network Technology and Protocols
Architecture
Compliance
Computer Network Defense
Configuration Management
Cryptography and Encryption
Data Security
Digital Forensics
Emerging Technologies
Enterprise Continuity
Identity management / Privacy
Incident Management
Industrial Control Systems
Information Assurance
Web Security
Information Systems
IT Systems and Operations
IT Security Awareness and Training
Management

Modeling and Simulation
Network and Telecommunications Security
Personnel Security
Physical and Environmental Security
Procurement
Security Risk Management
Software
Systems and Application Security

Specific Technical Requirements for the SECT Solution

- The contracted solution will be a Software as a Service (SaaS) solution that provides Security Awareness Training and advanced IT and managerial security training content courses.
- The Contractors SECT solution will be hosted in the United States.
- The Contractors SECT solution will be compatible with current versions of Internet Explorer and upgraded as needed for future versions.
- The Contractor will back up all SOM SECT data and perform restoration of data if needed.
- The Contractor will ensure that all operating systems, applications and server maintenance tasks are configured in accordance with NIST industry best security practices and/or software provider recommendations.
- The Contractor will ensure that adequate security is in place to prevent access by non-authorized parties.
- The Contractors State of Michigan SECT solution will be sized to accommodate 50,000 users and not limit the number of concurrent users.
- The Contractors SECT solution user interface will maintain acceptable response times so users are not waiting more than two-four (2-4) seconds for pages to load.
- The Contractor will destroy all SOM data on termination of the contract after the State of Michigan receives deliverables.
- The solution User Interface will be Section 508 and ADA compliant.
- The solution content will allow branding of the State of Michigan logo.
- The solution will follow Advanced Distributed Learning (ADL) Experience API specifications also known as Tin Can API, and be Sharable Content Object Reference Model (SCORM) compliant.
- The SECT solution will deliver training using industry standard web browsers, without the need for installation of browser add-ons.
- The solution will have the ability to import users account information from Microsoft Active Directory service exports.
- The SECT solution will allow for user information updates to include mass updates such as organization name changes.
- The solution will provide email notification messages to employees when a class is available, with a URL link to the class and when they should complete the course by.
- The SECT solution will have high availability and data recovery capabilities
- The SECT solution will offer brief 10-15 minute training classes for general Security Awareness topics.
- Training content will be engaging, entertaining, interactive, relevant, utilizing a variety of instructional approaches.
- Training will communicate effectively to all staff on a non-technical level.
- Training content will be updated regularly as threats change and available to SOM users.
- SECT course content updates will be available to SOM users for the duration of the contract and any option years exercised.
- The SECT will offer course content, brochure, poster, screensaver and newsletter customization functionality features.
- The SECT solution will easily allow users to stop courses and pick up where they left off.

- The SECT solution will notify employees by email they have a class to take and track the employee's training status, scores, and interactions.
- The SECT solution will allow administrators to make lessons required throughout the year.
- The SECT solution will allow for sub-organization administrative delegation so appointed SOM SECT Managers may monitor their organizations' employee training statistics and allocate role based training packages agencies / sub-organizations purchase.
- The SECT solution will provide employees with a certificate of completion once they have successfully completed each course.
- The SECT will have the ability to add the State of Michigan branding logo.

	SECT SOLUTION	**MEDIAPRO RESPONSE**
1.	Is the contracted solution considered a Software as a Service (SaaS)?	**Yes**
2.	How long has the Contractor's organization been offering Security Training SaaS solutions?	**12 Years**
3.	How will the contracted solution meet the demand of fifty thousand (50,000) users training concurrently with no noticeable performance issues?	**MediaPro LMS solution is hosted and professionally manages by Rackspace in their Virginia Data Center**
4.	Will the solution be available 24 hours a day, 7 days a week and 365 days a year (24x7x365)?	**Yes**
5.	Is the solution load balanced such that routine maintenance activities will not interrupt service?	**Yes**
6.	Does the solution resources self-scale at high demand usage?	**Yes**
7.	Describe the solutions data backup technology, schedule and restore timelines.	**MediaPro is committed to providing our clients with secure and reliable service. To support this commitment, MediaPro leverages a number of systems to continue its services in the event of pandemic, loss of facility, natural disaster, or other significant events. MediaPro's Business Continuity Plan outlines the processes, and resources required to continue its business operations. The following are high-level examples of how MediaPro's plan addresses disruptions:** **1. Geo-diverse backup systems are in place to protect business data** **2. Cloud services, such as Microsoft's Azure platform, are utilized to provide the virtual hardware needed to provide access to data and services in the event of an extended datacenter disruption**

		3. Telecommunication systems can be re-routed to public systems including cellular networks **4. Remote offices allow employees to continue to be productive during a pandemic, or loss of facilities** **MediaPro maintains plans for both internal and customer-facing communications in the event of an emergency. MediaPro's plans address all mission critical systems, financial and operational assessments, alternative communications with employees, clients, and vendors, alternate physical location of employees, and the varying scope and severity of specific disruptions.** **MediaPro continually assesses these plans to ensure that they meet the needs of the business and are in line with industry best practices. Further detail is available upon request with executive approval.**
8.	Explain Contractor's general process steps on ensuring the solution meets FISMA and NIST security compliances.	**MediaPro's Adaptive Security Library content supports the Security Awareness and Security Basics and Literacy components of 800-53 and 800-16, with state-specific modifications very easily incorporated as needed.**
9.	Will SOM data be segregated from other customer data?	**Yes**
10.	Is SOM data at rest encrypted?	**Yes**
11.	Explain how SOM data will be protected from non-authorized access. Policy, not how.	MediaPro: Personal Identity Information (PII) Security, Notification and Confidentiality Policy Purpose of this Policy MediaPro recognizes its need to maintain the confidentiality of Personal Identity Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from various types of individuals performing tasks on behalf of the company and includes employees, applicants, independent contractors and any PII maintained on its customer base. The scope of this policy is intended to be comprehensive and will include company requirements for the security and protection of such information

		throughout the company and its approved vendors both on and off work premises. Departments named in this policy have delegated authority for developing and implementing procedural guidance for ensuring that their departmental responsibilities under this policy are communicated and enforced. Key Elements of the Policy *Personal Identity Information (PII)*: Unique personal identification numbers or data, including: Social Security Numbers (or their equivalent issued by governmental entities outside the United States). Taxpayer Identification Numbers (or their equivalent issued by governmental revenue entities outside the United States). Employer Identification Numbers (or their equivalent issued by government entities outside the United States). State or foreign driver's license numbers or passport numbers. Date(s) of birth. Corporate or individually held credit or debit transaction card numbers maintained in organizational or approved vendor records. PII may reside in hard copy or electronic records; both forms of PII fall within the scope of this policy. *Vendors:* Individual(s) or companies that have been approved by MediaPro as a recipient of organizational PII and from which MediaPro has received certification of their data protection practices conformance with the requirements of this policy. Vendors include all external providers of services to the company and include proposed vendors. No PII information can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information. *PII Retention*: MediaPro understands the importance of minimizing the amount of PII data it maintains and retains such PII only as long as necessary. A joint task force comprising members of the Finance, Contracts and Human Resources departments maintains organizational record retention procedures, which dictate the length of data retention and data destruction methods for both hard copy and electronic records. *PII Training:* All new hires entering the company who may have access to PII are provided with introductory training regarding the provisions of this policy, a copy of this policy and implementing procedures for the

		department to which they are assigned. Employees in positions with regular ongoing access to PII or those transferred into such positions are provided with training reinforcing this policy and procedures for the maintenance of PII data and will receive annual training regarding the security and protection of PII data and company proprietary data *PII Audit(s)*: MediaPro conducts audits of PII information maintained by the company in conjunction with fiscal year closing activities to ensure that this policy remains strictly enforced and to ascertain the necessity for the continued retention of PII information. Where the need no longer exists, PII information will be destroyed in accordance with protocols for destruction of such records and logs maintained for the dates of destruction. The audits are conducted by the Finance, IT, Contracts and Human Resources departments. *Data Breaches/Notification:* Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the company will notify all affected individuals whose PII data may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible and in no event be later than thirty (30) days after which the breach was discovered. The Finance department will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with time frames specified under these laws. Notices to affected employees will be communicated by Human Resources after consultation with legal counsel and within the time frame specified under the appropriate law(s). Notices to affected customers will be communicated by the Contracts Department after consultation with legal counsel and within the time frame specified under the appropriate law(s). *Data Access:* MediaPro maintains multiple IT systems where PII data may reside; thus, user access to such IT systems is the responsibility of the IT department. The IT department has created internal controls for such systems to establish legitimate access for users of data, and access will be limited to those approved by IT and the respective department managers. Any change in vendor status or the termination

		of an employee or independent contractor with access will immediately result in the termination of the user’s access to all systems where the PII may reside. Data Transmission and Transportation *Company Premises Access to PII:* The Finance, Contracts, Human Resources and IT departments have defined responsibilities for on-site access of data that may include access to PII; IT has the oversight responsibility for all electronic records and data access capabilities. Finance, Contracts, and Human Resources have the operational responsibility for designating initial access and termination of access for individual users within their organizations and providing timely notice to IT. *Vendors:* MediaPro may share data with vendors who have a business need to have PII data. Where such inter-company sharing of data is required, the IT department is responsible for creating and maintaining data encryption and protection standards to safeguard all PII data that resides in the databases provided to vendors. Approved vendor lists will be maintained by the Finance department, and Contracts has responsibility to notify IT of any changes to vendor status with the company. *Portable Storage Devices:* MediaPro reserves the right to restrict PII data it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate company business. To protect such data, the company will also require that any such devices use IT department-approved security protection software while such devices are in use on or off company premises. The IT department has responsibility for maintaining data protection standards to safeguard PII data that resides on these portable storage devices. *Off-Site Access to PII:* MediaPro understands that employees may need to access PII while off site or on business travel, and access to such data will not be prohibited, subject to the provision that the data to be accessed is minimized to the degree possible to meet business needs and that such data will reside only on assigned laptops/approved storage devices that have been secured in advance by the IT department. *Regulatory Requirements:* It is the policy of the company to comply with any international, federal or state statute and reporting regulations. MediaPro has delegated the

		responsibility for maintaining PII security provisions to the departments noted in this policy. MediaPro Finance will be the sole entity named to oversee all regulatory reporting compliance issues. If any provision of this policy conflicts with a statutory requirement of international, federal or state law governing PII, the policy provision(s) that conflict will be superseded. *Employee Reporting*: If an employee has reason to believe that his or her PII data security has been breached, is at risk, or that company representative(s) are not adhering to the provisions of this policy, an employee should immediately contact the company HR manager. If an employee has reason to believe that a customer's PII data security has been breached is at risk, or that company representative(s) are not adhering to the provisions of this policy, an employee should immediately contact the company Finance department. *Confirmation of Confidentiality*: All company employees must maintain the confidentiality of PII as well as company proprietary data to which they may have access and understand that that such PII is to be restricted to only those with a business need to know. Employees with ongoing access to such data will sign acknowledgement reminders annually attesting to their understanding of this company requirement. *Violations of PII Policies and Procedures*: MediaPro views the protection of PII data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the company's discipline policy and may include suspension or termination in the case of severe or repeat violations. PII violations and disciplinary actions are incorporated in the company's PII onboarding and refresher training to reinforce the company's continuing commitment to ensuring that this data is protected by the highest standards.
12.	Upon contract termination what is the standard process and timeframe to delete customer data?	**MediaPro will return all requested data to SOM within one week of the terminated contract. All customer data related to our engagement will be deleted within one week.**
13.	Briefly describe how the solution is compliant with Advanced Distributed Learning (ADL)	**Mediapro currently does not support Tin Can API, but we are very familiar with these**

	Experience API specifications also known as Tin Can API.	**specifications and can build these into our code base at no extra cost.**
14.	What is the physical location (City and State) of the solution data and solution administration staff?	**Ashburn, Virginia**
15.	Describe how the solution complies with 508 and ADA.	**Making courseware accessible to all learners is very important to MediaPro. We have worked with many companies and organizations to address their organizational-specific requirements for accessibility. Organizational interpretation and policy around accessibility compliance (ADA, Section 508, w3c etc.) vary widely. The general accessibility commitments that we adhere to are:** • **Access keys act as an alternative to the mouse for users with impaired motor skills (i.e. Tab sequencing key, menu, exit, audio, etc.)** • **Full text transcript and/or on-screen text in place to assist hearing-impaired learners.** • **Style sheets are used but only for the formatting of text.** • **All graphic UI elements and content visuals are tested for color-blindness/chroma compatibility.** • **The text of the course is arranged to allow for the use of screen-reader utilities for the sight-impaired (i.e. Windows JAWS)**
16.	Will the solution support log-in authentication locally within the system or can it be Microsoft Active Directory (AD) enabled with SOM? Identify all authentication methods available.	**Our solution supports both authentication within the system or it can be AD enabled. MediaPro has worked with many types of AD environments and we have the technical expertise to provide Single Sign On in all environments.**
17.	Explain how new employees are added/loaded to the solution and how terminated employees are removed or archived in the solution.	**There is the ability to bulk-create/upload users via a .CSV file, as well as the ability to add them one at a time. If Single Sign On is set up, we can have the system check for an existing account and if one is not in the system, it will create the user automatically and assign the training to the employee/user.**
18.	Describe how employee data in the solution can be updated? To include name changes, agency changes or employment status updates?	**Typically these changes are made through an Excel or .CSV file upload. They can also be done on an individual basis.**

19.	Describe how the solution enables bulk configuration of employee data if needed.	**This can be done through either an Excel or .CSV file.**
20.	Briefly describe any features that are unique to the Contractor's solution or exceed the contract requirements.	**Our LMS was specifically designed to be very user friendly. Training of administrators typically takes less than an hour.**

SOLUTION CONTENT

1.	Describe how the training content is engaging, entertaining, interactive, relevant, fun, and utilizing a variety of instructional approaches.	**Keeping learners involved in online content ultimately comes down to providing relevant content with opportunities to engage and explore. We've been developing training for adults for over 20 years, and we've learned a few tricks along the way. We pose questions to users and provide immediate feedback; we create content that simulates the real tasks they'll perform in the workplace; and we include game-like simulations whenever the subject matter allows. These are not just our tricks, of course; they are backed by the leading research in instructional design.**
2.	Describe how the training communicates effectively to all staff on a non-technical level.	**MediaPro's security awareness training is designed so that anyone with an eight grade education of above should be able to understand our courseware.**
3.	Describe how often and the process of how the content is kept up to date with changing technology threats. Are content updates immediately available for SOM to deploy and included on an ongoing bases for the duration of the contract and exercised option years?	**We are continually updating our libraries by updating existing topics and adding new topics and courses. These updates are intended to keep our library in alignment with changing threats to information or compliance risks, or to align with the ever-changing legal and regulatory landscape. If you have purchased a multi-year contract, you may wish to swap out some of the topics in your existing course with new or updated topics, and this new content is available to you at no charge. The updates are provided on a quarterly basis.**
4.	Is the course content SCORM compliant?	**Yes, both 1.2 or 2004**
5.	Is the course content customizable? Explain what SOM administrators will be able to customize in the solution and training course content.	**Yes, all course content is customizable. SOM administrators have the ability to customize colors, branding,**
6.	Will SOM administrators be able to brand the solution with the States logo?	**Yes**

7.	Does the solution allow users to stop and easily pick up where they left off in the training course? Explain how or insert a graphic of how the user will do this.	**Every course**
8.	How many of the core Security Awareness courses are 10-12 minutes or less in length?	**MediaPro's courseware is customizable so all core Security Awareness courses could be 10-12 minutes or less in length.**
9.	Are there Brochures, Posters, videos, screensavers, and newsletters that correlate with and promote the online material? Are these SOM customizable or Contractor customizable?	**Yes. MediaPro has a large library of reinforcement content that is included with our pricing. They can be branded by SOM, and MediaPro can customize any of the content.**
10.	List by name the courses that are considered part of the Security Awareness content package.	**Safe Computing Physical Security Role-Based Security Topics Privacy Principles PCI Security Standards Preventing Phishing Safe Remote and Mobile Computing Bring Your Own Device Introduction to Secure Coding Security Awareness For Privileges Users Protecting and Handling Data Social Media Risks and Benefits Complying with HIPAA Information Assurance Security at a Glance Topics**
11.	List by name the courses that are considered Role Based Knowledge content classes.	**Several topics that would be included in the Role Based Knowledge content are included in the base SECT package. In addition, we have the courseware below that includes many of the required topics for Role Based Knowledge Content. Cryptography an Encryption Computer Network Defense Authentication Authorization Configuration Management IT Systems and Operations Systems and Application Security Session Management Input/Output Handling Information Systems Network and Telecommunications Security Logging Web Services Security**
12.	List any industry security standards classes offered by the solution.	**These are not available directly from MediaPro, but through a partner. Depending on your specific requirements, MediaPro can provide course lists and pricing.**
13.	List any additional content items that set the Contractors solution apart from others.	**MediaPro also has a Privacy and Compliance library with additional topics.**

CONTENT DELIVERY

1.	Is the solution web enabled and what current browsers will it work with?	**Yes, the solution is web enabled. The following internet browsers will be supported: Internet Explorer, Firefox, Safari, and Google Chrome.**
2.	What is the typical response time for user training screens to open?	**Less than 1 second**
3.	Is the solution sound enabled? If sound is required what solution is the Contractor willing to propose so it is not disruptive to other staff in the area?	**The solution is sound enabled, but all of the courseware can be taken on a text only basis as well.**
4.	Will users be able to take Security Awareness classes multiple times if they wish to do so for the duration of the contract to include possible option years?	**Yes**
5.	Will the solution allow the state administrators to make lessons required throughout the year?	**Yes**
6.	Does the solution notify employee's via email that they have an outstanding obligation to complete a lesson? How many times and at what frequency if so? Is this feature customizable?	**Yes, How many times and the frequency can be set by the client.**
7.	Explain how the solution tracks the employee training status, scores, and interactions by the State sub-organization they are in and what assessment reports are available to identify training accomplishments or deficiencies by sub-organization.	**Our LMS hosting and SaaS solution provides an easy-to-use, scalable, and secure infrastructure that enables you to deliver, measure, track, and report on training content delivery. Using our simple graphical reporting, you can easily track and audit employee compliance training requirements, measure student competencies, and report on the status of your overall training objectives. The reporting can be segmented into unlimited sub-organizations based on client requirements.**
8.	Describe how the solution can delegate administration to sub-organization units to administer the core Security Awareness Training and/or the core Role Based training purchased.	**There is no limit as to the number of units or the number of administrators assigned to each unit.**
9.	Describe how the solution provides a status notification message to employees when a class is assigned and when the employee is alerted.	**The employee receives an email notification every time a class is assigned.**
10.	Does the employee receive a certificate after successful completion of a class? Is there a	**A certificate is optional for every class and the passing score for the class is customizable by SOM.**

	success factor that needs to be met to acquire a certificate? Is this customizable by SOM?	
11.	Will SECT courses run on mobile browsers such as Android and Apple?	**Yes, courses run on both Android and Apple devices that are of tablet size.**
12.	Are there any additional content delivery options that exceed the contract requirements? If so, please explain.	**Some of MediaPro's content can also be delivered via an MP4 file through the SOM's Intranet or through email.**

B. Solution Support Services

The Contractor will provide solution support services twenty four (24) hours a day, seven (7) days a week, and three hundred sixty five (365) days a year. This includes any solution issues reported by the approved State of Michigan DTMB Project Manager and/or SOM Administrator any time during the contract year(s).

The Contractor will provide a central point of contact phone number for the SOM administrator to call if the SECT solution is not functioning as anticipated. A ticket with a HIGH, MEDIUM, or LOW issue status will be opened and worked within reasonable time frames based on the issue status. For critical HIGH system outage issues the Contractor will escalate the ticket and start resolution actions within thirty (30) minutes of ticket initiation. Issues with software functionality will be fixed at no cost to the SOM. Notices will be sent to SOM Project managers for all scheduled maintenance down time of the SOM SECT solution.

The SOM will require special support services for training content or course customizations, report creation, solution user administration and/or updates depending on the flexibility and configuration options offered in the SECT solution.

C. RESERVED
D. RESERVED
E. RESERVED

F. Solution Implementation Plan

The Contractor will submit a Solution Implementation Plan which will be used after award for a final Implementation plan. The Solution Implementation plan needs to identify the typical process steps recommended by the Contractor to setup, configure, and deploy the solution training to fifty thousand (50,000) SOM users. The Solution Implementation Plan will outline all steps required, the timeframe for each step and the expected roles and responsibilities of the Contractor and the State of Michigan personal during the implementation processes.

The desired format of the Solution Implementation Plan is in a Microsoft Project format with Milestones, Tasks, and subtasks defined in a Work Breakdown structure.

The Contractor will provide a Solution Implementation Plan; it may be embedded in the overall Contract Project Plan but will have definitive Implementation Start and Implementation Completion tasks to clearly define all steps of the Implementation Plan.

G. Training

The Contractor will need to provide the SOM Administrator's with training and training materials to properly administer the SECT solution and all available functionality in the solution. The administrator training duration will be dependent on the complexity of the solution and the amount of customization functionality the SOM administrator will be able to perform. Live WebEx training or on-site training is preferred for more complex solution administration activities so SOM Administrators may ask questions if needed.

H. Reporting

The State of Michigan (SOM) will require user activity reporting from the solution. The SOM Project Manager and administrators will require the ability to provide Enterprise statistics on pending training courses for employees from all agencies or from one specific agency as needed. The report will also need to be shared with agency assigned Sub Managers to track only employee's residing in an assigned agency or agency group. The report will need to contain the following field elements: Employee Name, Agency, Course Name Outstanding, date assigned and email reminder dates. This report will require permissions such that the SOM Project Manager/Administrator and backup Project Manager/Administrator have full control to report all agencies or specific agencies, and sub-agency managers can only report on limited agency users that have been delegated to them.

A similar report for course completions will be required with like permissions to track user courses completed by the Enterprise or sub agency users. The agency completion report will contain the following field elements: Employee Name, Agency, Course Completed Name, and Completion Date. As with the permissions above the SOM SECT Project Manager/Administrator and the backup will require Enterprise wide reporting abilities and sub Managers will need delegated limited agency access.

The SECT solution will require a standard report of SOM employee data by agency so employee records can be reviewed in bulk and updates identified.

The SECT solution will require a standard employee report that lists all the training an employee completed or has not completed. Ideally employees would have access to print their own report if needed.

The SECT solution includes a dash board reporting feature of the above reports at a higher level with drill down functionality.

The SECT solution will allow the SOM SECT Administrators some level of customization in report generation. This will include ad hoc filtering on report data, inserting the SOM logo on report headers, exporting filtered raw data to Microsoft Excel or searching for specific data elements from assessment information captured in the SECT.

Deliverable(s)

- Reports from the SECT solution that reflect users that have not completed assigned Security Awareness training that are sortable by agency.
- Reports from the SECT solution that reflect users that have completed assigned Security Awareness Training that are sortable by agency.
- SECT dash board reporting abilities or standard reports the SOM Project Manager/Administrator and sub-agency managers will have access to use.
- Customizable report functionality in the SECT solution.

1.200 Roles and Responsibilities

1.201 CONTRACTOR STAFF, ROLES, AND RESPONSIBILITIES

A. Contractor Staff

The Contractor provided resumes for staff, who will be assigned to the Contract, indicating the duties/responsibilities and qualifications of such personnel, and stating the amount of time each will be assigned to the project. The competence of the personnel the Contractor selects for this project will be measured by the candidate's education and experience with particular reference to experience on similar projects as described in this Statement of Work. The Contractor will provide sufficient qualified staffing to satisfy the deliverables of this Statement of Work.

1. **SECT Primary Single Point of Contact (SPOC) - Key Personnel**

   The Contractor will identify a Primary Single Point of Contact (SPOC). The duties of the SPOC will include, but not be limited to:

   - Support the management of the Contract,
   - Facilitate dispute resolution, and
   - Advise the State of performance under the terms and conditions of the Contract.
   - Work with the State to set up and implement the SECT solution
   - SPOC for SECT issue resolution
   - Provide SECT update information on new course options
   - Assist with SECT user administration if required
   - Develop the project plan and schedule, and update as needed
   - Serve as the point person for all project issues
   - Coordinate and oversee the day-to-day implementation project activities
   - Assess and report project feedback and status
   - Escalate project issues, project risks, and other concerns
   - Review all project deliverables and provide feedback
   - Proactively propose/suggest options and alternatives for consideration
   - Utilize change control procedures
   - Prepare project documents and materials
   - Manage and report on the project's budget

   The State reserves the right to require a change in the current SPOC if the assigned SPOC is not, in the opinion of the State, adequately serving the needs of the State.

2. **SECT Secondary Single Point of Contact Key Personnel**

   The Contractor will identify a Secondary Single Point of Contact (SSPOC) in case the primary SPOC is unavailable. The duties of the SSPOC in the absence of the Primary SPOC will include, but not be limited to:

   - Support the management of the Contract,
   - Facilitate dispute resolution, and
   - Advise the State of performance under the terms and conditions of the Contract.
   - Work with the State to set up and implement the SECT solution
   - SPOC for SECT issue resolution
   - Provide SECT update information on new course options
   - Assist with SECT user administration if required
   - Develop the project plan and schedule, and update as needed

- Serve as the point person for all project issues
- Coordinate and oversee the day-to-day implementation project activities
- Assess and report project feedback and status
- Escalate project issues, project risks, and other concerns
- Review all project deliverables and provide feedback
- Proactively propose/suggest options and alternatives for consideration
- Utilize change control procedures
- Prepare project documents and materials
- Manage and report on the project's budget

The Contractor will provide, and update when changed, an organizational chart indicating lines of authority for personnel involved in performance of this Contract and relationships of this staff to other programs or functions of the firm. This chart will also show lines of authority to the next senior level of management and indicate who within the firm will have prime responsibility and final authority for the work.

All Key Personnel will be subject to the State's interview and approval process. Any key staff substitution will have the prior approval of the State. The State has identified the following as key personnel for this project:

- *Single Point of Contact (SPOC)*
- *Secondary Single Point of Contact (SSPOC)*

3. RESERVED

4. RESERVED

B. Site Work Requirements

1. Location of Work

The work is to be performed, completed, and managed at the Contractor work site location(s) in the United States.

2. SOM Hours of Operation:

a. Normal State working hours are 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, with work performed as necessary after those hours to meet project deadlines. No overtime will be authorized or paid.

b. The State is not obligated to provide State management of assigned work outside of normal State working hours. The State reserves the right to modify the work hours in the best interest of the project.

c. Contractor will observe the same standard holidays as State employees. The State does not compensate for holiday pay.

3. Travel:

a. No travel or expenses will be reimbursed. This includes travel costs related to training provided to the State by Contractor.

b. Travel time will not be reimbursed.

1.202 STATE STAFF, ROLES, AND RESPONSIBILITIES

The State project team will consist of Executive Subject Matter Experts (SME's), project support, and a MDTMB project manager:

Executive Subject Matter Experts
The Executive Subject Matter Experts representing the business units involved will provide the vision for the business design and how the application will provide for that vision. They will be available on an as needed basis. The Executive SME's will be empowered to:

- Resolve project issues in a timely manner
- Review project plan, status, and issues
- Resolve deviations from project plan
- Provide acceptance sign-off
- Utilize change control procedures
- Ensure timely availability of State resources
- Make key implementation decisions, as identified by the Contractor's SPOC / project manager, within 48-hours of their expected decision date.

Name	Agency/Division	Title	Phone/e-mail
Richard Reasner	DTMB-CIP/MCS	Director – MCS	517-241-4090

State Project Manager- (MDTMB and Agency)
MDTMB will provide a Project Manager who will be responsible for the State's infrastructure and coordinate with the Contractor in determining the solution configuration.

The State's Project Manager will provide the following services:

- Coordinate the State resources necessary for the project
- Facilitate coordination between various external Contractors
- Facilitate communication between different State departments/divisions
- Provide acceptance and sign-off of deliverable/milestone
- Review and sign-off of timesheets and invoices
- Resolve project issues
- Escalate outstanding/high priority issues
- Utilize change control procedures
- Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
- Document and archive all important project decisions
- Arrange, schedule and facilitate State staff attendance at all project meetings.

Name	Agency/Division	Title
Rock Rakowski	DTMB-CIP/MCS	Project Manager

MDTMB will provide a Contract Administrator whose duties will include, but not be limited to, supporting the management of the Contract.

Name	Agency/Division	Title
Michael Breen	MDTMB-Procurement	Contract Administrator

1.203 RESERVED

1.300 Project Plan

1.301 PROJECT PLAN

Preliminary Project Plan

Contractor will provide a Preliminary Contract Project Plan for approval, including necessary time frames and deliverables for the various stages of the contract project and the responsibilities and obligations of both the Contractor and the State. The Implementation Plan defined in section 1.104 F. may be imbedded in the overall Contract project plan to address both sections.

1. In particular, the Preliminary Project Plan will include a MS Project plan or equivalent (check the SUITE/PMM standard):
   a. A description of the services/deliverables to be provided under this contract.
   b. Target dates and critical paths for the deliverables.
   c. Identification of roles and responsibilities, including the organization responsible. Contractor is to provide a roles and responsibility matrix.
   d. The labor, materials and supplies required to be provided by the State in meeting the target dates established in the Preliminary Project Plan.
   e. Internal milestones
   f. Task durations

Note: A Final Project Plan will be required as stated in **Schedule A**, Section 1.301 Project Control.

Orientation Meeting

Upon twenty one (21) calendar days from execution of the Contract, the Contractor will be required to attend an orientation meeting to discuss the content and procedures of the Contract. The meeting will be held in Lansing, Michigan, at a date and time mutually acceptable to the State and the Contractor. The State will bear no cost for the time and travel of the Contractor for attendance at the meeting.

Performance Review Meetings

The State will require the Contractor to attend weekly working and status meetings during the planning, implementation and deployment phases of the project. Once deployment is complete the Contractor will continue to attend monthly meetings, at a minimum, to review the Contractor's performance under the Contract. All meetings will be held in Lansing, Michigan, or by teleconference, as mutually agreed by the State and the Contractor. The State will bear no cost for the time and travel of the Contractor for attendance at the meeting.

Project Control

1. The Contractor will carry out this project under the direction and control of MDTMB, Cyber Security & Infrastructure Protection agency.
2. Within thirty five (35) working days of the execution of the Contract, the Contractor will submit to the State project manager(s) for final approval of the contract project plan to include the

implementation project plan. This project plan will be in agreement with **Schedule A**, Section 1.104 Work and Deliverables, and will include the following:

- The Contractor's project organizational structure.
- The Contractor's staffing table with names and title of personnel assigned to the project. This will be in agreement with staffing of accepted proposal. Necessary substitutions due to change of employment status and other unforeseen circumstances may only be made with prior approval of the State.
- The project work breakdown structure (WBS) showing sub-projects, activities and tasks, and resources required and allocated to each.
- The time-phased plan in the form of a graphic display, showing each event, task, and decision point in the WBS.

3. The Contractor will manage the project in accordance with the State Unified Information Technology Environment (SUITE) methodology, which includes standards for project management, systems engineering, and associated forms and templates which is available at http://www.michigan.gov/suite
   a. Contractor will use an automated tool for planning, monitoring, and tracking the Contract's progress and the level of effort of any Contractor personnel spent performing Services under the Contract. The tool will have the capability to produce:
      - Staffing tables with names of personnel assigned to Contract tasks.
      - Project plans showing tasks, subtasks, deliverables, and the resources required and allocated to each (including detailed plans for all Services to be performed within the next thirty 30 calendar days, updated semi-monthly).
      - Updates will include actual time spent on each task and a revised estimate to complete.
      - Graphs showing critical events, dependencies and decision points during the course of the Contract.
   b. Any tool(s) used by Contractor for such purposes will produce information of a type and in a manner and format that will support reporting in compliance with the State standards.

1.302 REPORTS

In addition to the SECT solution reports defined in 1.104 H. Reporting a bi-weekly implementation progress report will be submitted to the Agency Project Manager up through Solution Implementation, at which point bi-weekly progress reports will be submitted monthly through the life of this Contract. Each progress report will contain the following:

- Any planned SECT solution updates or changes
- Curriculum Content changes or updates
- New SECT Reporting features or help guides
- Project Issues
- Project Risks
- Project Change Requests
- Work completed since last report and work to be done before the next reporting date

1.400 Contract Project Management

1.401 ISSUE MANAGEMENT

An issue is an identified event that if not addressed may affect schedule, scope, quality, or budget.

The Contractor will maintain an issue log for issues relating to the provision of services under this Contract. The issue management log will be communicated to the State's Project Manager on an agreed upon schedule, with email notifications and updates. The issue log will be updated and will contain the following minimum elements:

- Description of issue
- Issue identification date
- Responsibility for resolving issue.
- Priority for issue resolution (to be mutually agreed upon by the State and the Contractor)
- Resources assigned responsibility for resolution
- Resolution date
- Resolution description

Issues will be escalated for resolution from level 1 through level 3, as defined below:

Level 1 – Business leads
Level 2 – Project Managers
Level 3 – Executive Subject Matter Experts (SME's)

1.402 RISK MANAGEMENT

A risk is an unknown circumstance or event that, if it occurs, may have a positive or negative impact on the project.

The Contractor is responsible for establishing a risk management plan and process, including the identification and recording of risk items, prioritization of risks, definition of mitigation strategies, monitoring of risk items, and periodic risk assessment reviews with the State.

A risk management plan format will be submitted to the State for approval within twenty (20) business days after the effective date of the contract. The risk management plan will be developed during the initial planning phase of the project, and be in accordance with the State's PMM methodology. Once both parties have agreed to the format of the plan, it will become the standard to follow for the duration of the contract. The plan will be updated bi-weekly, or as agreed upon.

The Contractor will provide the tool to track risks. The Contractor will work with the State and allow input into the prioritization of risks.

The Contractor is responsible for identification of risks for each phase of the project. Mitigating and/or eliminating assigned risks will be the responsibility of the Contractor. The State will assume the same responsibility for risks assigned to them.

1.403 CHANGE MANAGEMENT

Change management is defined as the process to communicate, assess, monitor, and control all changes to system resources and processes. The State also employs change management in its administration of the Contract.

If a proposed contract change is approved by the Agency, the Contract Administrator will submit a request for change to the Department of Technology, Management and Budget, Procurement Buyer, who will make recommendations to the Director of DTMB-Procurement regarding ultimate approval/disapproval of change request. If the DTMB Procurement Director agrees with the proposed modification, and all required approvals are obtained (including State Administrative Board), the DTMB-

Procurement Buyer will issue an addendum to the Contract, via a Contract Change Notice. **Contractors who provide products or services prior to the issuance of a Contract Change Notice by the DTMB-Procurement, risk non-payment for the out-of-scope/pricing products and/or services.**

The Contractor will employ change management procedures to handle such things as "out-of-scope" requests or changing business needs of the State while the migration is underway.

The Contractor will employ the change control methodologies to justify changes in the processing environment, and to ensure those changes will not adversely affect performance or availability.

1.500 Acceptance

1.501 CRITERIA

Deliverables that are documents will:

- Be allowed no less than five (5) business days for review by the State of Michigan.
- Be in electronic format, compatible with State of Michigan software in accordance with **Schedule A** 1.103 Environment
- Provide a heading indicating document name on each page
- Provide page number and "of pages" on each page.
- Provide an "as of" date.
- Indicate final and not draft status
- If required by SUITE, will leverage the SUITE template or leverage a template that serves the same purpose and contains similar information but only with prior approval of the DTMB Project Manager.
- Reflect correction of feedback provided by the State, regarding but not limited to, level of detail and clarifications.
- Reflect correction of issues identified by State personnel during the review of said documents unless waived in writing by the DTMB Project Manager.

The approval process is defined in more detail in the attachment **Schedule - D** – SECT SaaS Terms of Agreement.

1.502 FINAL ACCEPTANCE

The following requirements for final acceptance apply:

- The SOM SECT solution is configured, implemented, passed testing and performs all the functions defined in **Schedule A**, 1.104 Security Training (SECT) Requirements.
- The DTMB Project Manager has approved and signed off on all SECT system and document deliverables and project milestones.
- Attended Lessons Learned meeting with the DTMB Project Manager

1.600 Compensation and Payment

1.601 COMPENSATION AND PAYMENT

Method of Payment

This will be a firm, fixed price Contract based on the following deliverables

A. Initial Subscription Payment – #1 - 50% of first year subscription contract amount after signature and approval of the DTMB Agency Project Manager of:

a. Deliverable 1.104 A. – SECT Setup and Configuration defined in SECT Requirements
b. Deliverable 1.104 B. – SECT Support Services
c. Deliverable 1.104 F. – SECT Implementation Plan
d. Deliverable 1.104 G. – SECT Training
e. Deliverable 1.104 H. – SECT Reporting
f. Successful testing of deliverables above.

B. Payment #2 – 50% of first year subscription contract amount after signature and approval of the DTMB Agency Project Manager of:
   a. Successful SECT Deployment and Implementation to all SOM employees shortly after completion of all prior deliverables in section A. Initial Subscription Payment above.

C. Payment for solution subscription will be paid yearly on the contract start date anniversary thereafter.

D. Reserved

Method of Payment

The first year's payment will be made as indicated above. Additional years will be paid annually at the beginning of the contract/option year.

The Contractor will be required to submit an Administrative Fee of 1% (see Section 8.2 of SECT SAAS Term of Agreement) on all payments remitted under the Contract.

Extended purchasing program volume requirements are not included, unless stated otherwise.

If Contractor reduces its prices for any of the software or services during the term of this Contract, the State will have the immediate benefit of such lower prices for new purchases. Contractor will send notice to the State's MDTMB Contract Administrator with the reduced prices within fifteen (15) Business of the reduction taking effect.

Statements of Work and Issuance of Purchase Orders

Unless otherwise agreed by the parties, each Statement of Work will include:

1. Background
2. Project Objective
3. Scope of Work
4. Deliverables
5. Acceptance Criteria
6. Project Control and Reports
7. Specific Department Standards
8. Payment Schedule
9. Travel and Expenses
10. Project Contacts
11. Agency Responsibilities and Assumptions
12. Location of Where the Work is to be performed
13. Expected Contractor Work Hours and Conditions

The parties agree that the Services/Deliverables to be rendered by Contractor pursuant to this Contract (and any future amendments of it) will be defined and described in detail in Statements of Work or Purchase Orders (PO) executed under this Contract. Contractor will not be obliged or authorized to commence any work to implement a Statement of Work until authorized via a PO issued against this

Contract. Contractor will perform in accordance with this Contract, including the Statements of Work/Purchase Orders executed under it.

Invoicing
Contractor will submit properly itemized invoices to

DTMB – Financial Services
Accounts Payable
P.O. Box 30026
Lansing, MI 48909
or
DTMB-Accounts-Payable@michigan.gov

. Invoices will provide and itemize, as applicable:
Contract number;
Purchase Order number
Contractor name, address, phone number, and Federal Tax Identification Number;
Description of any commodities including quantity ordered;
Date(s) of delivery and/or date(s) of installation and set up;
Price for each item, or Contractor's list price for each item and applicable discounts;
Maintenance charges;
Net invoice price for each item;
Other applicable charges;
Total invoice price; and
Payment terms, including any available prompt payment discount.

Incorrect or incomplete invoices will be returned to Contractor for correction and reissue.

Attachment A - Cost Table

Applicable MediaPro Price Table Options

Customization Services

Option No.	**Service Description**	**Number of Units, Hours, Classes, etc. included**	**Hourly Rate**	**Number of Licenses**	**Price Per Package**
C1.	Customization	10-hours	180.00	N/A	$ 1,800.00

Subscription Package Pricing

Option No.	**Package Description**	**Number of Units, Hours, Classes, YR's, etc. included**	**Number of Licenses**	**Price Per Package**
D2.	Package Option 2	5 SECT Year Subscription	50,000 Users licenses – plus Manager Security Training, LMS Hosting	$ 352,220.00
OPTION YEAR	**Follow on option year pricing packages to be considered for contract yearly extensions.**			
1	Option Year 1 – Package	Option Year 1	50,000 Users licenses – Security Training, LMS Hosting	$ 82.900.00
2	Option Year	Option Year 2	50,000 Users licenses – Security Training, LMS Hosting	$ 70,500.00
3	Option Year	Option Year 3	50,000 Users licenses – Security Training, LMS Hosting	$ 70,500.00
4	Option Year	Option Year 4	50,000 Users licenses – Security Training, LMS Hosting Manager Security Training, LMS Hosting	$ 70,500.00
5	Option Year	Option Year 5	50,000 Users licenses – Security Training, LMS Hosting	$ 70,500.00
		Total Contract Value:		$787,620.00

STATE OF MICHIGAN

SCHEDULE C –

SOM POLICY 1340.00 Information Technology Information Security

State of Michigan
Administrative Guide to State Government

POLICY 1340.00 Information Technology Information Security

Issued: April 12, 2007
Revised: July 18, 2016
Next Review Date: July 18, 2017

APPLICATION

This policy is for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using state of Michigan (SOM) information networks and information technology (IT) Resources.

The DTMB Deputy Director of Cybersecurity & Infrastructure Protection (CIP) as the Chief Security Officer (CSO) shall enforce SOM IT security standards with authority under MCL 18.1101, et seq; MCL 18.41; Executive Order 2001-3; and Executive Order 2009-55. CIP is accountable to the DTMB Chief Information Officer (CIO) for identifying, managing, and mitigating physical and IT security risks and vulnerabilities within SOM facilities and computing, communication, and technology resources. CIP also oversees physical and IT security risk management, awareness, and training; assists SOM agencies with their security issues; and enforces oversight of SOM security policies, standards, and procedures to maintain suitable levels of enterprise-wide security.

To secure the enterprise IT environment, Michigan Cyber Security (MCS) has selected the cybersecurity framework published by the National Institute of Standards and Technology (NIST) Special Publication 800.53, Assessing Security and Privacy Controls for Federal Information Systems and Organizations
(http://csrc.nist.gov/publications/PubsSPs.html), (Revision 4 – moderate controls) as the minimum security controls for SOM information systems. Each System Security Plan will address NIST security standards and guidelines in the following policies and corresponding standards.

PURPOSE

MCS is committed to securing SOM assets and provides the NIST security framework for developing, implementing and enforcing security policies, standards, and procedures to prevent or limit the effect of a failure, interruption or security breach of the SOM's facilities and system. This policy establishes the SOM strategic view of IT security information systems that process, store and transmit SOM information. Those who implement and manage information systems must address security controls applicable to corresponding systems as addressed in this policy and corresponding standards and procedures.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Cybersecurity & Infrastructure Protection (CIP)
Michigan Cyber Security (MCS)

Telephone: 517-241-4090

Fax: 517-241-2013

SUMMARY

Security controls be implemented to protect SOM information from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure confidentiality, integrity and availability of SOM information. All SOM employees, trusted partners, or entities authorized to access, store, or transmit SOM information shall protect the confidentiality, integrity and availability of the information as set forth in this and all SOM enterprise IT policies. Information is not limited to data in computer systems and is included wherever it resides in an agency, whatever form it takes, (electronic, printed, etc.), whatever technology is used to handle it, or whatever purposes it serves. Any data that is originated, entered, processed, transmitted, stored or disposed of for the SOM is considered SOM information.

Policies, standards and procedures addressed in this document and corresponding sub-level documents include management, personnel, operational, and technical issues over:

- NIST Control Families
- Data Classification
- Ownership and Transfer of SOM Information
- Authorization Prerequisites
- Acceptable Use of Information Technology
- Electronic Processing
- IT Network Infrastructure
- Database Security
- Sensitive Information

SOM or environmental changes may require changes to this security policy. Any effort to request, approve, implement, or communicate changes to policies, standards, or procedures that this policy regulates or governs must be made under SOM 1305.00.01 IT Policy Administration Standard.

Policy exceptions occur for many of reasons. Examples include an overriding business need, a delay in vendor deliverables, new regulatory or statutory requirements, and temporary configuration issues. The exception process must ensure these circumstances are addressed while making all stakeholders aware of the event, risks, and timetable to eliminate the exception. Any exception must be made under SOM 1305.00.02 Technical Policy and Product Exception Standard.

CIP will duly implement and enforce security policies, standards, and procedures to ensure their effective dissemination and availability. MCS may enforce compliance through audits, vulnerability scanning, and corrective actions. If an Agency does not comply with mandates in this policy and corresponding sub-level documents, the Agency, Business Owner, and Information System Owner accept the associated risks due to non-compliance.

POLICIES

General

The following SOM policies are established in accordance with corresponding NIST controls. Each SOM Agency is bound to each policy. The policies establish the standards and procedures to effectively implement corresponding SOM Cyber Security baseline controls on the subject. All SOM Agencies must develop, adopt, and adhere to a formal, documented procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among

SOM entities, and demonstrates compliance with each of the following policy areas. Each policy, security standard, and procedure must be reviewed and updated annually.

020 Access Control (AC-1)

SOM IT Standard 1340.00.020.01 establishes the Access Control standards in this SOM policy.

These standards require automated security controls, authorized access and use of information systems, special and limited access conditions, physical and automated process monitoring, and authorized system account activities by approved personnel. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities, access management requirements, and separation of duties necessary to effectively manage information system accounts; and coordinate, plan, and execute appropriate physical and account access control activities.

030 Security Awareness and Training (AT-1)

SOM IT standard 1340.00.030.01 establishes the Security Awareness and Training standards in this SOM policy.

These standards require role-specific training on security controls, authorized access and use of information systems, physical and automated process monitoring, and authorized system activities and functions by approved personnel. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities and training requirements necessary to effectively maintain organizational awareness, minimize insider threats, and prevent additional security related incidents.

040 Audit and Accountability (AU-1)

SOM IT standard 1340.00.040.01 establishes the Audit and Accountability standards in SOM policy.

These standards require approved personnel to audit essential information, manage audit service devices and locations, integrate audit events, manage audit repositories, and process and generate audit reports. These standards ensure that SOM Authorizing Officials with auditing responsibilities understand the responsibilities required to successfully manage audit information, assign audit roles and tasks, and prevent the compromise of SOM information.

050 Security Assessment and Authorization (CA-1)

SOM IT standard 1340.00.050.01 establishes the Security Assessment and Authorization standards in SOM policy.

These standards require approved personnel to conduct impartial security and organizational assessments, establish external system restrictions, and conduct penetration testing and other necessary vulnerability assessments. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities necessary to establish effective security assessment and authorization controls, prevent conflicts of interest, and maintain continuous monitoring strategies.

060 Configuration Management (CM-1)

SOM IT standard 1340.00.060.01 establishes the Configuration Management standards in SOM policy.

These standards require approved personnel to adequately manage the configuration of SOM's configuration systems, including retaining previous system configurations, configuring approved devices for high-risk areas, tracking and documenting system changes, and assigning privileges to authorized personnel. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to maintain up-to-date system configuration, support rollbacks and system change requirements, and prevent unauthorized system changes, including software and program installs.

070 Contingency Planning (CP-1)

SOM IT standard 1340.00.070.01 establishes the Contingency Planning standards in SOM policy.

These standards require approved personnel to coordinate contingency plans with existing organizational contingency development, designate key resumption activities, define service-level priorities, and define critical assets and offsite backup sites, including telecommunications, transaction systems and operational separation measures. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent conflicts with other organizational contingency elements, effectively resume essential operations during and after a disruption, prevent loss or compromise of assets, and provide alternate methods to secure, store and access SOM information.

080 Identification and Authentication (IA-1)

SOM IT standard 1340.00.080.01 establishes the Identification and Authentication standards in SOM policy.

These standards require personnel to manage network systems that employ multifactor and public key information (PKI)-based authentication, replayresistant mechanisms, identification of connected devices, and registration process requirements. These standards ensure that SOM Authorizing Officials and third parties understand the responsibilities necessary in order to regulate non-privileged access of SOM accounts, minimize authentication attacks, and prevent unauthorized devices and connections with SOM networks.

090 Incident Response (IR-1)

SOM IT standard 1340.00.090.01 establishes the Incident Response standards in SOM policy.

These standards require approved personnel to apply incident response capabilities, including automated response and reporting processes, establish a test process for those incident response capabilities, and coordinate with existing SOM contingency plans. These standards ensure that SOM Authorizing Officials and all other associated personnel understand the responsibilities necessary to ensure the SOM's incident response capability is effective, prevents conflicts with other organizational contingency elements, and relies on automated system response, reporting, and support.

100 Maintenance Policy (MA-1)

SOM IT standard 1340.00.100.01 establishes the Maintenance standards in SOM policy. These standards require approved personnel to employ adequate and approved information maintenance tools, inspect all maintenance tools entering SOM facilities, including supporting media, and apply priority or time sensitive maintenance procedures. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to effectively diagnose and repair SOM information systems, ensure maintenance tools and supporting media are not modified beyond the SOM's authorized specifications, and determine the levels of risk and priority for each particular information system affected during an incident.

110 Media Protection (MP-1)

SOM IT standard 1340.00.110.01 establishes the Media Protection standards in SOM policy.

These standards require all SOM personnel to apply proper information system media markings on all approved media, devices, and systems property; properly designate and control both physical and digital storage locations; execute approved and secure transport methods; ensure cryptographic protection is applied to required devices; and prohibit the use of unidentifiable devices. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to ensure all SOM media is adequately used, handled, and distributed and also properly protected, stored, and transported, including applying additional security mechanisms and restrictions on the use of unauthorized media devices.

120 Physical and Environmental Protection (PE-1)

SOM IT standard 1340.00.120.01 establishes the Physical and Environmental Protection standards in SOM policy.

These standards require definition of both physical facility and information system management processes. All corresponding personnel will apply and manage security safeguards accordingly for facilities and information system distribution and transmission lines; control and monitor physical information output devices and locations, including the use of safety, intrusion and surveillance equipment; and implement appropriate power protection and alternate location practices and measures. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent unauthorized communication or transmission access, maintain access records, minimize the compromise of sensitive output information, and protect SOM equipment, facilities and environments, including emergency power procedures and relocation contingencies.

130 Security Planning (PL-1)

SOM IT standard 1340.00.130.01 establishes the Security Planning standards in SOM policy.

These standards require all assigned SOM personnel to effectively coordinate security related activities with other organizations and outside entities, provide and enforce social media and network rules and restrictions, and implement an adequate information security architecture. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent security activity conflicts within and throughout the SOM, prevent negative impact and restraints on other organizations, minimize unauthorized access to SOM information available on public information sites, and ensure a proper security architecture is in place and is continuously assessed.

140 Personnel Security (PS-1)

SOM IT standard 1340.00.140.01 establishes the Personnel Security standards in the SOM policy.

These standards require that the organization employs automated mechanisms to control both SOM personnel and third-party providers of employee transfers, commencement and termination status, including disabling access for specific information systems, designating a risk status for specific positions and roles, and conducting personnel screening before granting authorization or access. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to ensure that appropriate personnel have limited or appropriate access, that changes in personnel status properly control further access or restriction to information systems, and that appropriate documentation and processes are followed to track corresponding authorization changes and access.

150 Risk Assessment (RA-1)

SOM IT standard 1340.00.150.01 establishes the Risk Assessment standards in SOM policy.

These standards require that appropriate vulnerability scanning tools are employed, accurate updates of scanned vulnerabilities are maintained, and legitimate vulnerabilities are remediated. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to readily identify and respond to system vulnerabilities.

160 System and Services Acquisition (SA-1)

SOM IT standard 1340.00.160.01 establishes the System and Services Acquisition standards in SOM policy.

These standards require that the organization applies visually functional security interface controls; controlled levels of systems design and implementation; and appropriate systems engineering, configuration, and service principles. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to ensure that SOM sensitive information is excluded from open and unauthorized view, that system functionality and requirements are defined during early development, and that proper process life-cycle strategies are in place.

170 System and Communications Protection (SC-1)

SOM IT standard 1340.00.170.01 establishes the System and Communications Protection standards in SOM policy.

These standards require that the organization employs application, information, and functionality partitioning measures, limits external network connection points, properly manages external telecommunications, prevents non-remote connections, and secures and monitors all transmitted and stored data, including all channeling networks. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to prevent unauthorized system management access and control information flow via shared information sources, connections, networks, and other data sources.

180 System and Information Integrity (SI-1)

SOM IT standard 1340.00.180.01 establishes the System and Information Integrity standards in SOM policy.

These standards require that the organization employs mechanisms that alert the organization and identify information system flaws during malfunction or failure, designates central management for automated malicious code protection measures, applies real-time event analysis, validation, and verification tools, including traffic communications monitoring, and logs detected events for use in contingency planning. These standards ensure that SOM Authorizing Officials understand the responsibilities necessary to effectively determine changing states within the SOM's information systems, obtain accurate event-based system information, and determine suitable corrective actions for security relevant events.

Agency Director

- Ensures proper levels of protection for their Agency information are determined and documented, and necessary safeguards are implemented in accordance with SOM 1340.00.150.02 Data Classification Standard.
  - Data management complies with federal and state laws and regulations and SOM policies.
  - Information security controls are implemented to protect SOM information, and sufficiently to ensure the confidentiality, integrity, and availability of SOM information.
- Ensures Business Owner identification of data. Although it is not recommended to have multiple owners for the same data, this sometimes occurs. Where there is more than one owner, Information Owners must designate a Business Owner who has authority to decide for all owners of the data.
- Ensures anyone requiring access to confidential or restricted information owned by another Agency obtains permission from the Business Owner.
- Ensures a formalized process is developed to manage user access to the SOM Network and IT resources in compliance with this and all SOM policies.
- Ensures a process is established to review technical controls and recommendations identified by SOM Data Custodians.
- Ensures Agencies follow DTMB policy on the system security planning process including System Security Plans.
- Ensures internal Agency security policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
- Ensures all SOM employees and Trusted Partners handle information for which they are responsible in compliance with this policy and all SOM policies.
- Ensures all Agency employees are trained to handle information in accordance with this and all SOM policies.
- Appoints an Agency Security Training Coordinator.
- Establishes an overall strategy for the Agency's Role-Based Security Program.

  Ensures that high priority is given within the Agency to implement effective security awareness and role-based security training for employees to protect stat assets.
- Ensures SOM employees and Trusted Partners are trained to ensure awareness of their role in protecting SOM information and data as set forth in this policy.
-

- Ensures employees are advised of the necessity of complying with SOM policies and laws on the protection of SOM information, because noncompliance may leave the SOM and employees subject to prosecution, civil suits, and disciplinary action.
- May implement more stringent policies than those developed by DTMB for the SOM in conjunction with DTMB.

Agency Authorizing Official

- Authorizes operation of and budgetary oversight for an information system.
- Assumes responsibility for the mission and business operations supported by the system.
- Assumes responsibility for operating an information system at an acceptable level of risk to the Agency’s operations, assets or individuals.
- Assumes accountability for the security risks associated with the information system operations.
- Approves System Security Plans, memoranda of agreement, and Plans of Action and Milestones (POAMs).
- Denies authorization to operate the information system or if unacceptable security risks exist.
- Issues an interim authorization to operate the information system under specific terms and conditions.
- Assigns an Agency Senior Information Security Officer and necessary Agency Security officers and Agency Privacy Officers.
- Coordinates activities with Agency Security Officers, Common Control Providers, Information System Owners, Information Owners, Information Security Officers, and DTMB officials.
- If an information system has multiple Agency Authorizing Officials, establishes agreements among them and documents them in the information System Security Plan.

Agency Authorizing Official Designated Representative

- Acts for an Agency Authorizing Official to coordinate and conduct the required day-to-day activities associated with the security authorization process.

  As authorized by Agency Authorizing Officials, makes decisions on planning and resourcing of the security authorization process, approval of the System Security Plan, approval and monitoring the implementation of POAMs, and assessment and determination of risk.
- Cannot authorize an information system to operate or approve POAMs.
-

Agency Senior Information Security Officer

- Assists the Agency Information System Owners, Information Owners and Agency Authorizing Official in ensuring that information systems have adequate security controls in place to meet all state and federal laws, regulations and policies.
- May administer an Agency information security program or serve as the Agency Authorizing Official Designated Representative or Security Control Assessor.
- May serve as primary liaison between the Agency and DTMB, Data Custodians, Common Control Providers and External Service Providers.

Agency Security Officer

- Ensures and maintains the appropriate operational security posture of the information system.
- May assist in the development and compliance of security policies and classifying information assets.
- May assist the Information System Owner and Information Owner in completing the System Security Plan and POAM.

Agency Privacy Officer

- Ensures that the Agency's collection, processing, dissemination, and disposal of data complies with the state and federal privacy laws and regulations.
- May assist the Information System Owner and Information Owner in completing the System Security Plan and POAM.

Agency POAM Coordinator

- Handles continuous monitoring and updating of the POAM.

Cannot authorize an Information System to operate or approve a POAM.

Agency Security Training Coordinator

- Implements security awareness training within the Agency.
- Works with the Statewide Security Awareness Coordinator to implement statewide general security awareness programs in the Agency.
- Ensures that appropriate role-based training materials are timely developed for intended Agency audiences.

Assists Agency managers in establishing a tracking and reporting strategy.

-

DTMB Chief Information Officer (CIO)

- Directs the strategic design, acquisition, management, and implementation of the statewide technology infrastructure.
- Consistent with the Federal Information Security Modernization Act (FISMA) administers training and oversees personnel with significant IT/cybersecurity responsibilities.
- Ensures a statewide IT/cybersecurity program is implemented.
- Ensures resources and budgets are available to support the IT/cybersecurity program.
- Measures effectiveness of the IT/cybersecurity program.
- Designates a Chief Technology Officer (CTO) to manage information systems and assets for Enterprise Architecture, Service Providers, Infrastructure and Operations, Network Strategies, and Research and Technology Implementation.
- Designates a Chief Security Officer (CSO) to develop and maintain a statewide Cybersecurity and Infrastructure Protection program to fulfill the Director's responsibilities for system security planning.
- Ensures that Agency Directors, Agency Authorized Officials, Information System Owners, Information Owners, Data Custodians, and other related personnel understand the concepts and strategy of the IT/cybersecurity program.
- Ensures that Agencies have access to SOM policies, standards, procedures and guidelines governing user access to the SOM network and IT Resources.
- Ensures a formal process is established to manage user access to the SOM network and IT Resources (local area network (LAN), wide area network (WAN), file and print, desktop, etc.).
- Ensures a formal process is established to implement and audit Agency approved access requests to established services, (wireless, Telecom catalog services, application access, new employee access, etc.) on the SOM network in compliance with this and all SOM policies.
- Ensures a formal process is established that ensures the proper implementation and integration of service continuity with other system operations and technical security controls as required by DTMB in conjunction with Agencies.
- Ensures Agency-required security controls and safeguards are implemented and monitored for compliance.
- Ensures that all System End Users of information systems are sufficiently trained in their security responsibilities.

DTMB Chief Technology Officer (CTO)

- Determines the strategic direction of SOM technology function.
-

- Maintains technology policies and standards on Enterprise Information Technology, IT Network and Infrastructure, and Configuration Management.
- Directs the activities necessary to keep the technology infrastructure efficient and effective while ensuring compliance with established policies, standards and procedures.
- Manages information systems implementation and monitors effectiveness.
- Maintains information systems security and maintenance.
- Manages staff in functional areas such as LAN/WAN architecture, systems operations, and hardware support.
- Anticipates and reacts to major technology changes.
- Collaborates with the executive team to assess and recommend technologies in support of SOM needs.

DTMB Chief Security Officer (CSO)

- Establishes an enterprise information security program that includes planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets.
- Establishes and creates an overall strategy for a Statewide General Security Awareness Program available to all SOM Agency employees.
- Ensures that the Statewide General Security Awareness Program is funded.
- Ensures that SOM senior managers and others understand the concepts and strategy of the Statewide General Security Awareness Program, and are informed of the progress of the program's implementation.
- Appoints a Statewide Security Awareness Coordinator to develop and implement the SOM Information Security and Privacy Awareness program.
- Develops and maintains information security policies, standards, procedures, and control techniques to address system security planning.
- Manages identification, implementation, and assessment of common security controls.
- Coordinates the development, review, and acceptance of System Security Plans with Information System Owners, DTMB Information System Security Officers, and Agency Authorizing Officials.
- Ensures that personnel with significant responsibilities for System Security Plans are trained.
- Assists senior Agency officials with their responsibilities for System Security Plans.
- Ensures the policies defined in the Cyber Security Program align with the enterprise information security program.
- Develops and maintains data classification policies, procedures and control techniques to protect SOM data from security incident or data breach.

- Establishes a governance body to direct the development of SOM enterprise entity-specific information security plans, policies, standards, and other authoritative documents.
- Oversees the creation, maintenance, and enforcement of established enterprise information security policies, standards, procedures, and guidelines.
- Develops and tracks information security and privacy risk key performance indicators.
- Develops and disseminates security and privacy metrics and risk information to SOM entity executives and other managers for decision making purposes.
- Coordinates security efforts with SOM entities and other branches of government as applicable.
- Establishes an access control program for state-owned, DTMB-managed facilities that includes planning, oversight, and coordination of program activities to effectively manage risk and provide a secure environment for employees and visitors.
- Provides monitoring of safety, security and building systems in DTMB managed facilities and initiates emergency response as needed.
- Develops and maintains policies, standards, and procedures to address facility security planning and manages the identification, implementation, and assessment of common security controls.

DTMB Authorizing Official

- Coordinates and conducts the required day-to-day technological management activities associated with the security authorization process.
- As authorized by the Agency Authorizing Official, may decide on the technological planning and resourcing of the System Security Plan and POAM.
- Cannot approve the System Security Plan or POAM.

MCS Authorizing Official

- Reviews Security Authorization Packages and authorizes implementation of the information system.
- May authorize the information system to operate or deny the authorization to operate based on the level of risk to SOM operations, assets or individuals.

DTMB MCS Security Liaison

- Coordinates and facilitates completion of the System Security Plan, Risk Assessment and POAM for an Agency.
- Works closely with the DTMB Information System Security Architects, Information System Owners, Information Owners, Agency Security Officers, Common Control Providers and Data Custodians on security related issues and services.

DTMB Information System Security Officer

- Ensures that the appropriate operational security posture is maintained for an information system working closely with the Agency Security Officers, Information System Owner, and Information Owner.
- Serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system.
- Has the detailed knowledge and expertise required to manage the security aspects of an information system.
- As authorized by the Information Owner, may handle the day-to-day security operations of a system.
- Oversees an information system's physical and environmental protection, personnel security, incident handling, and security training and awareness.
- Assists in the developing of the security policies and procedures and ensures compliance with those policies and procedures.
- As authorized by the Information System Owner and Information Owner, may play an active role in:
    - The system's operational environment.
    - Developing and maintaining the System Security Plan.
    - Managing and controlling changes to the system. o Assessing the security

      impact of changes to the system.

DTMB Information System Security Architect

- Ensures that information system security requirements necessary to protect the Agency's core missions and business processes are adequately addressed in all aspects of enterprise architecture.
- Identifies information security requirements necessary to protect the information system and ensures these requirements are adequately addressed in the System Security Plan.
- Assists in providing a wide range of security-related services including:
    - Establishing information system boundaries. o Assessing the

      severity of weaknesses and deficiencies. o Creating POAMs.
    - Risk mitigation approaches. o Security alerts. o Potential

      adverse effects of identified vulnerabilities.

Statewide Security Awareness Coordinator

- Oversees the Statewide General Security Awareness Program.
- Ensures that appropriate general security awareness materials are timely developed for the intended audiences.
- Ensures that awareness and training material is effectively deployed to reach the intended audience.
- Ensures that Agency Awareness Coordinators have an effective way to provide feedback on the awareness and training material.
- Ensures that awareness and training material is reviewed periodically and updated as necessary.
- Assists management in establishing a tracking and reporting strategy.
- Assists Agency Security Awareness Coordinators with the enterprise program.

Information System Information System Owner

- Agency official responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of the information system. The Information System Owner has the following responsibilities for System Security Plans:
    - Develops the System Security Plan in coordination with the Information Owner, system administrator, DTMB Information System Security Officer, Common Control Provider, Security Liaison, and functional end users.
    - Categorizes the information system based on (Federal Information Processing Standards) FIPS 199, NIST SP 800-60, 1340.00.150.02 Data Classification Standard, and other standards encompassed by SOM IT Policy 1340.00.
    - Maintains the System Security Plan and ensures that the system is deployed and operated according to agreed-upon security requirements.
    - Decides who has access to the system and the types of privileges and access rights.
    - Ensures that system users and support personnel receive required security training.
    - Updates the System Security Plan when a significant change occurs.
    - Assists in identifying, implementing, and assessing the common security controls.
- Based on guidance from the Agency Authorizing Official creates and maintains the POAM.
- Based on guidance from the Agency Authorizing Official, informs appropriate Agency and DTMB officials of the need to conduct the security authorization, ensures necessary resources are available and provides the required information system access, information, and documentation.

- Coordinates with MCS on assembling and submitting the authorization package to the Authorizing Officials identified in the System Security Plan.
- Permits and documents information from multiple Information Owners, if applicable.

Information Owner

- An individual or organization with (1) statutory or operational authority for specified information, (2) responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal, and (3) ultimately responsibility for ensuring the protection and use of data.
- Establishes the rules for appropriate use and protection of the subject data or information.
- In coordination with the Information System Owner, categorize the information system based on FIPS 199, NIST SP 800-60, SOM 1340.00.150.02 Data Classification Standard and other standards encompassed by SOM IT Policy 1340.00.
- Provides input to Information System Owners on the security requirements and security controls for the information system where the information resides.
- Assists in identifying and assessing the common security controls where information resides.
- Decides who can access the information system and the types of privileges and access rights.
- Establishes the rules for behavior for appropriate use and protection of the information and retains that responsibility when the information is shared with or provided to other organizations.

Data Custodian

- An individual or organization delegated by an Information Owner with responsibility for technological maintenance and management of information systems and corresponding data.
- Implements and manages the necessary safeguards to protect data based on requirements established by the Information Owner and documented in the System Security Plan.

  o Protects the information from unauthorized access. o Performs

  backup and recovery functions.

Common Control Provider

- An individual, group or organization responsible for developing, implementing, assessing, and monitoring common controls inherited by an information system.
- Documents organization-identified common controls in a System Security Plan, ensuring that a security risk assessment is performed by appropriate personnel and a POAM is produced.

- Informs Information System Owners when problems arise in inherited common controls.

Risk Assessment Team

• A group of individuals defined in the initiation phase of the information system to identify and document the information system security risks that is led by the MCS Security Liaison and may include DTMB Information System Security Architects, Information System Owners, Information Owners, Agency Security Officers and Subject Matter Experts.

POAM Team

• A group of individuals which may include Information Owners, Information System End Users, Common Control Providers, and support personnel such as database administrators, web administrators, programmers, DTMB Information System Security Architects or other security professionals that remediates risks documented in the POAM.

Roles Agency

• Gathers data, enters it into the system, verifies its accuracy, specifies why it can or will be used, designates who can use it, and ultimately fills a business need for its use.

Business Owner

- Designated by Information Owners when multiple Information Owners own the same information.
- Makes decisions for all owners of this data.
- Administers systems and may be delegate to the System Administrators.
- Usually owns the primary business functions served by the application and is the application’s largest stakeholder.

Managers

- Comply with IT security awareness and training requirements established for their users.
- Work with their Agency Security Awareness Coordinator to meet shared responsibilities.
- Serve in the role of System Owner and Data Owner, where applicable.
- Consider developing individual development plans (IDPs) for employees with significant security responsibilities.
- Promote the professional development and certification of IT security program employees and others with significant security responsibilities.
- Ensure that all employees are appropriately trained in how to fulfil their security responsibilities before allowing access to Agency information systems.
- Ensure that employees understand specific rules of each system and application they use.

- Work to reduce errors and omissions by users due to lack of awareness and training.

Non-privileged Users

- Individuals without appropriate authorizations.

Security Control Assessor

- An individual, group, or organization officially assigned by the Agency.
- Conducts a comprehensive assessment of the management, operational, and technical security controls employed by an information system to determine the overall effectiveness.
- Determines if controls are implemented correctly, operating as intended and producing the desired outcome.
- Prepares the final security assessment report documenting any weaknesses or deficiencies discovered.
- Recommends a corrective action plan to address identified vulnerabilities.
- Conducts an assessment of the System Security Plan to ensure security controls meet the stated security requirements.

Subject Matter Experts

• Individuals with in-depth knowledge of the system and its functions and operations, which may include information system end users and information support personnel such as database administrators, web administrators, programmers, security architects or other security professionals.

System Administrator

• Assigned by the Business Owner for the upkeep, configuration, and reliable operation of computer systems.

Trusted Partner

- A person (vendor, contractor, Third party, etc.) or entity that has contracted with the SOM to perform a service or provide a product in exchange for valuable consideration.
- Information technology services implemented outside information system boundaries.
- External services can be provided by entities (1) within the SOM but outside the authorization boundaries established for the information system or (2) outside the SOM either in the public or private sector.
- External information services are typically not part of SOM information systems but must meet the same federal and state laws, regulations, executive orders, directives, policies, and standards. Security requirements for external service providers, including the security controls for external information systems, are usually stated in contracts or other formal agreements.

Users

- Includes state employees, contractors, guests, visitors, other collaborator and associates requiring access to SOM data or resources working in staff augmentation positions, students, or Trusted Partners.
- Understand and comply with federal, statewide and Agency IT/cybersecurity policies and procedures.
- Trained in the rules of behavior for the systems and applications to which they have access.
- Works with management to meet training needs.
- Keeps software and applications updated with security patches.
- Aware of actions they can take to better protect SOM information, including:
    - Proper password usage.
    - Using proper antivirus protection
    - Reporting any suspected incidents or violations of security policy.
    - Following rules established to avoid social engineering attacks.

System Security Aggregate Data

- Data resulting from combining individual data elements into a group or category.
- May become sensitive data as a result of combination.

Availability of Information

- Security Objective to which a Data Impact Level is assigned.
- Ensuring timely and reliable access to and use of information.
- Assuring that the systems for delivering, storing and processing information are accessible when needed, by those who need them.

Confidential Data

- Available only to authorized personnel on a need-to-know basis.
- Requires a signed non-disclosure statement.
- Applicable state and federal laws and regulations, policies, standards, procedures and privacy compliance requirements must be followed.
- May require additional security control requirements.

Confidentiality of Information

- Security Objective to which a Data Impact Level is assigned.

- Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.

Data

• SOM Agency information. No distinction between data and information is made in this policy.

Data Classification

- Establishes information ownership and location where data resides.
- Categorizes data's security level based on sensitivity, criticality and risk of the information.
- Increases the confidentiality, integrity and availability of data.

Data Impact Level

• Level assigned to data relevant to the sensitivity, criticality and risk to the primary business function of the Agency or individuals and potential impact of loss or compromise.

Data Type

- Specific category of information as defined by an Agency or specified by law, executive order, directive, policy, or regulation.
- Examples include privacy, medical, proprietary, financial, investigative, contractor sensitive, and security management.

External Information Systems/Non-organizationally Owned Devices

- Information systems or components of information systems outside of the authorization boundary established by the SOM.
- Information systems or components of information systems for which the SOM typically has no direct supervision or authority over the application of required security controls or assessing control effectiveness.

Information

• SOM Agency information. No distinction between data and information is made for this policy.

Information Security

• For this policy, information is not limited to data in computer systems, but includes data wherever it resides in the agency, what form it takes (electronic, printed, etc.), whatever technology is used to handle it, or whatever purpose it serves.

Information Technology (IT) Resources

• Includes devices, networks, data, software, hardware, email, system accounts, and facilities provided to conduct official SOM business.

Information Type

• Specific category of information as defined by an Agency or specified by law, executive order, directive, policy, or regulation. Examples includes privacy, medical, proprietary, financial, investigative, contractor sensitive, and security management.

Integrity of Information

- Security Objective to which a Data Impact Level is assigned.
- Maintaining the intrinsic validity of information and assurance that the information can be relied on to be sufficiently accurate by guarding against improper information modification or destruction to ensure information has not been altered by unauthorized people.

Internal Data

• Information created, updated, or stored by the Agency that is not sensitive to disclosure within the Agency.

Nonpublic Information

- Any information that the general public cannot access in accordance with state or federal laws, executive orders, directives, policies, regulations, standards, or guidance.
- Information protected under the Privacy Act of 1974 and vendor proprietary information are examples of nonpublic information.

Plan of Action and Milestone (POAM)

- Created during the implementation phase of the System Development Life Cycle (SDLC) and is updated along with the System Security Plan and Risk Assessment until all tasks have been completed.
- Describes specific measures planned to correct weakness or deficiencies identified in the risk assessment.
- Addresses known vulnerabilities in the information system.
- Details the Information System Owner and Authorizing Official’s risk response.

  - Proposed risk mitigation approach.
  - Rationale for accepting risk.
  - Responsible party for risk mitigation.
  - Date due and date complete.

- Based on the recommended corrective action and level of risk, the Information System Owner, Information Owner and Authorizing Officials may:
  - Mitigate the risk by implementing the recommended security controls.
  - Accept the risk. o Transfer the risk, by obtaining insurance to cover potential losses. o Transfer the risk to another organization.
  - Avoid the risk by ceasing the activity that is presenting the risk or never engaging in the activity.

Privileged Functions

• Functions requiring authorization such as establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities.

Public Data

- Information explicitly approved for distribution to the public.
- Can be disclosed to anyone without violating an individual's or organization's right to privacy or causing potential harm.

Restricted Data

- Extremely Sensitive Information.
- Disclosure or corruption could be hazardous to life or health, cause extreme damage to integrity or image, or impair the effective delivery of services.
- Made available to named individuals or specific positions on a need-toknow basis.

Risk Assessment

- Provides an objective analysis of the system-specific and common controls identified in the System Security Plan.
- Determines if controls were implemented and meeting the identified security requirements.
- Initial risk assessment is created during the construction phase of the SDLC.
- Updated annually or whenever changes are made to the security controls implemented.

o Updates to the risk assessment ensure that the Information System Owner, Information Owner and Authorizing Officials know of the security state of the information system.

- Required for the System Authorization Package.
- Does not assess security controls to determine if they are operating correctly or producing the desired outcome.

Security Assessment

- SOM grants access to its facilities, provides network access, outlines detailed information about the network and security plans, etc. to study security and identify improvements to secure the systems.
- Ensures that necessary security controls are integrated into the design and implementation of the project under assessment.
- Provides documentation outlining any security gaps between a project designs and approved corporate security policies.

Security Authorization Package

- Documentation that includes the System Security Plan, Risk Assessment and POAM.
- Used by Authorizing Officials to make risk-based decisions to permit or deny system operations.

Security Categorization

- Basis for determining proper security controls to protect information.
- Determined for both data type and system level.
- Based on Data Impact Level and Security Objective.

Security Controls

• Management, operational, and technical controls, (e.g., safeguards or countermeasures) required for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security-Relevant Information

- Any information within information systems that can potentially impact the operation of security functions or the provision of security services that could result in failure to enforce system security policies or maintain the isolation of code and data.
- Includes filtering rules for routers and firewalls, cryptographic key management information, configuration parameters for security services and access control lists.

Sensitive Information

- Data of such nature that its compromise, change, misuse, or loss can significantly harm an individual or the SOM.
- Must be protected from unauthorized access to safeguard the privacy or security of individuals and the SOM.
- Personal Identifying Information (PII)
- Confidential non-public information that relates to an Agency's business.

System Security Plan

- Overview of the information system and security requirements including:
  - information assets o security

    categorization o applicable laws and

    regulations o system interconnections o

    information sharing o system

    dependencies o network diagrams o

    network devices and components o

    system hardware o system software o

    data flow diagrams
  - implementation of the security controls
- Describes the controls in place or planned to be in place required to provide the appropriate level of security.
- Required for the System Authorization Package.

User Location

• Information that can be determined by information systems, such as internet protocol (IP) addresses from which network logons occurred, device identifiers, or notifications of local logons.

AUTHORIZATION

Authority

• This policy obtains its authority from:

- Administrative Guide Policy 1305 Enterprise Information Technology. o The

  Administrative Guide to State Government.

- DTMB IT Technical Policies, Standards and Procedures, which can be found on the DTMB Intranet.

Enforcement

• All enforcement for this policy must comply with the standards and procedures of Administrative Guide Policy 1305 Enterprise Information Technology.

Developing Standards and Procedures for this Policy

• All requirements for developing standards and procedures for this policy must comply with Administrative Guide Policy 1305 Enterprise Information Technology.

Exceptions

• All exception requests to this policy must be processed in compliance with Administrative Guide Policy 1305 Enterprise Information Technology.

Effective Date

• This policy is effective upon signature of the Administrative Guide approval memo by the DTMB Director.

***

STATE OF MICHIGAN

SCHEDULE D CONTRACT TERMS

Software as a Service (SaaS)

This Software as a Service proposed Contract is agreed to between the State of Michigan (the "**State**") and MediaPro Holdings, LLC. (the "**Contractor**"), a Washington Limited Liability company. This proposed Contract is effective on March 28, 2017 ("**Effective Date**"), and unless earlier terminated, will expire on March 38, 2022 (the "**Termination Date**").

This Contract may be renewed for up to five (5) additional option year periods. Renewal must be by written notice from the State and will automatically extend the Term of this proposed Contract.

1. Definitions.

"**Accept**" has the meaning set forth in **Section 4.2(b)**.

"**Acceptance**" has the meaning set forth in **Section 4.2(b)**.

"**Action**" has the meaning set forth in **Section 13.1**.

"**Actual Uptime**" means the total minutes in the Service Period that the Hosted Services are Available.

"**Allegedly Infringing Features**" has the meaning set forth in **Section 13.3(b)(ii)**.

"**Authorized Users**" means all Persons authorized by the State to access and use the Services through the State's account under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

"**Availability**" has the meaning set forth in **Section 5(a)**.

"**Availability Requirement**" has the meaning set forth in **Section 5(a)**.

"**Available**" has the meaning set forth in **Section 5(a)**.

"**Business Day**" means a day other than a Saturday, Sunday or State Holiday.

"**Change Notice**" has the meaning set forth in **Section 2.2**.

"**Code**" has the meaning set forth in **Section 18**.

"**Confidential Information**" has the meaning set forth in **Section 10.1**.

"Contract" has the meaning set forth in the preamble.

"**Contract Administrator**" is the individual appointed by each party to (a) administer the terms of this Contract, and (B) approve and execute any Change Notices under this Contract. Each party's Contract Administrator will be identified in the Statement of Work.

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor Personnel**" means all employees and agents of Contractor, all Subcontractors and all employees and agents of any Subcontractor, involved in the performance of Services.

"**Contractor Security Officer**" has the meaning set forth in **Section 2.5(a)**.

"**Contractor Service Manager**" has the meaning set forth in **Section 2.5(a)**.

"**Contractor Systems**" has the meaning set forth in **Section 11.3**.

"**Corrective Action Plan**" has the meaning set forth in **Section 6.6**.

"**Critical Service Error**" has the meaning set forth in **Section 6.4(a)**.

"**Documentation**" means all generally available documentation relating to the Services, including all user manuals, operating manuals and other instructions, specifications, documents and materials, in any form or media, that describe any component, feature, requirement or other aspect of the Services, including any functionality, testing, operation or use thereof.

"**DR Plan**" has the meaning set forth in **Section 12.3(a)**.

"**Effective Date**" has the meaning set forth in the preamble.

"**Exceptions**" has the meaning set forth in **Section 5.2**.

"**Fees**" has the meaning set forth in **Section 8.1**.

"**Force Majeure Event**" has the meaning set forth in **Section 17.1**.

"**Harmful Code**" means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner, any (i) computer, software, firmware, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services or Contractor Systems as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

"**High Service Error**" has the meaning set forth in **Section 6.4(a)**.

"**HIPAA**" has the meaning set forth in **Section 9.1**.

"**Hosted Services**" has the meaning set forth in **Section 2.1(a)**.

"**Intellectual Property Rights**" means any and all rights comprising or relating to: (a) patents, patent disclosures and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names and domain names, together with all of the goodwill associated therewith; (c) authorship rights, copyrights and copyrightable works (including computer programs) and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable Law in any jurisdiction throughout the world.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in this Contract or any Statement of Work.

"**Law**" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement or rule of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

"**Loss**" means all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers. "Losses" has a correlative meaning.

"**Low Service Error**" has the meaning set forth in **Section 6.4(a)**.

"**Medium Service Error**" has the meaning set forth in **Section 6.4(a)**.

"**Person**" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

"**Personal Health Information (PHI)**" has the meaning set forth in **Section 9.1**.

"**Personally Identifiable Information (PII)**" has the meaning set forth in **Section 9.1**.

"**Process**" means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. "**Processing**" and "**Processed**" have correlative meanings.

"**Reject**" has the meaning set forth in **Section 4.2(b)**.

"**Rejection**" has the meaning set forth in **Section 4.2(b)**.

"**Representatives**" means a party's employees, officers, directors, consultants, legal advisors and, with respect to Contractor, Contractor's Subcontractors.

"**Resolve**" has the meaning set forth in **Section 6.4(b)**.

"**RFP**" means the State's request for proposal designed to solicit responses for Services under this Contract.

"**Scheduled Downtime**" has the meaning set forth in **Section 5.3**.

"**Scheduled Uptime**" means the total minutes in the Service Period.

"**Service Availability Credits**" has the meaning set forth in **Section 5.5(a)**.

"**Service Error**" means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Contract and the Specifications.

"**Service Level Credits**" has the meaning set forth in **Section 6.5**.

"**Service Level Failure**" means a failure to perform the Support Services fully in compliance with the Support Service Level Requirements.

"**Service Period**" has the meaning set forth in **Section 5(a)**.

"**Service Software**" means any and all software applications and any third-party or other software, and all new versions, updates, revisions, improvements and modifications of the foregoing, that Contractor provides remote access to and use of as part of the Services.

"**Service Support Level Requirements**" has the meaning set forth in **Section 6.4**.

"**Services**" has the meaning set forth in **Section 2.1**.

"**Source Code**" means the human readable source code of the Service Software to which it relates, in the programming language in which the Service Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Service Software.

"**Specifications**" means the specifications for the Services set forth in the applicable Statement of Work and, to the extent consistent with and not limiting of the foregoing, the Documentation.

"**State**" has the meaning set forth in the preamble.

"**State Data**" has the meaning set forth in **Section 9.1**.

"**State Modification**" has the meaning set forth in **Section 13.2(a)**.

"**State Project Manager**" has the meaning set forth in **Section 2.8**.

"**State Systems**" means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

"**Statement of Work**" has the meaning set forth in **Section 2.1(a)**. The Initial Statement of Work is attached as **Schedule A**, and subsequent Statements of Work will be sequentially identified and attached as Schedule A-1, A-2, A-3, etc.

"**Subcontractor**" means any entity that performs any Services under this Contract and otherwise has the meaning set forth in **Section 2.4(a)**.

"**Support Request**" has the meaning set forth in **Section 6.4(a)**.

"**Support Service Level Requirements**" has the meaning set forth in **Section 6.4**.

"**Support Services**" has the meaning set forth in **Section 6**.

"**Term**" has the meaning set forth in the preamble.

"**Transition Period**" has the meaning set forth in **Section 7.3.**

"**Transition Responsibilities**" has the meaning set forth in **Section 7.3.**

"**User Data**" means any and all information reflecting the access or use of the Hosted Services by or on behalf of the State or any Authorized User, including any end user profile, visit, session, impression, click-through or click-stream data and any statistical or other analysis, information or data based on or derived from any of the foregoing.

2. Services.

2.1 Services. Throughout the Term and at all times in connection with its actual or required performance under this Contract, Contractor will, in accordance with all terms and conditions set forth in this Contract and each applicable Statement of Work, provide to the State and its Authorized Users the following services ("**Services**"):

(a) the hosting, management and operation of the Service Software and other services for remote electronic access and use by the State and its Authorized Users ("**Hosted Services**") as described in one or more written, sequentially numbered, statements of work referencing this Contract, including all Specifications set forth in such statements of work, which, upon their execution will be attached as **Schedule A** to this Contract and by this reference are incorporated in and made a part of this Contract (each, a "**Statement of Work**");

(b) service maintenance and the Support Services as set forth in **Section 6** and in the applicable Statement of Work; and

(c) such other services as may be specified in the applicable Statement of Work.

2.2 Change Notices.

(a) Any modifications or changes to the Services under any executed Statement of Work will be effective only if and when memorialized in a mutually agreed written change notice ("**Change Notice**") signed by both Parties, provided, however, that for any Services provided on a limited basis (for example, on a per user, server, CPU or named-user basis), the State may, at any time, increase or decrease the number of its licenses hereunder subject to a corresponding forward-going adjustment of the Fees to reflect these changes in accordance with the pricing set forth in the applicable Statement of Work.

(b) In the event the Services are customizable, a more detailed change control process may be specified in the applicable Statement of Work. In such event, the change control process set forth in such Statement of Work will control.

2.3 Compliance With Laws. Contractor will comply with all applicable Laws as they concern this Contract, including securing and maintaining all required and appropriate visas, work permits, business licenses and other documentation and clearances necessary for performance of the Services.

2.4 Subcontracting. Contractor will not itself, and will not permit any Person to, subcontract any Services, in whole or in part, without the State's prior written consent, which consent may be given or withheld in the State's sole discretion. Without limiting the foregoing:

(a) Contractor will ensure each Contractor subcontractor (including any subcontractor of a Contractor subcontractor, each, a "**Subcontractor**") complies with all relevant terms of this Contract, including all provisions relating to State Data or other Confidential Information of the State;

(b) the State's consent to any such Subcontractor does not relieve Contractor of its representations, warranties or obligations under this Contract;

(c) Contractor will remain responsible and liable for any and all: (i) performance required hereunder, including the proper supervision, coordination and performance of the Services; and (ii) acts and omissions of each Subcontractor (including, such Subcontractor's employees and agents, who, to the extent they are involved in providing any Services, are deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor;

(d) any noncompliance by any Subcontractor or its employees or agents with the provisions of this Contract or any Statement of Work will constitute a breach by Contractor;

(e) prior to the provision of Services by any Subcontractor, Contractor will obtain from each such proposed Subcontractor:

(i) the identity of such Subcontractor and the location of all its data centers, if any, that will be used in Processing any State Data, which information Contractor will promptly disclose to the State in writing; and

(ii) a written confidentiality, restricted use, work-for-hire and intellectual property rights assignment Contract in form and substance acceptable to the State, giving the State rights at least equal to those set forth in **Section 9** (State Data), **Section 10** (Confidentiality), **Section 11** (Security) and **Section 12** (Redundancy, Data Backup and Disaster Recovery) and containing the Subcontractor's acknowledgment of, and agreement to, the provisions of **Section 2.5** (Contractor Personnel), a fully-executed copy of which agreement Contractor will promptly provide to the State upon the State's request.

2.5 Contractor Personnel. Contractor will:

(a) subject to the prior written approval of the State, appoint: (i) a Contractor employee to serve as a primary contact with respect to the Services who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Support Services (the "**Contractor Service Manager**"); and (ii) a Contractor employee to respond to the State's inquiries regarding the security of the Contractor Systems who has sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**"); and (iii) other Key Personnel, who will be suitably skilled, experienced and qualified to perform the Services;

(b) provide names and contact information for Contractor's Key Personnel on this Contract;

(c) maintain the same Contractor Service Manager, Contractor Security Officer and other Key Personnel throughout the Term and such additional period, if any, as Contractor is required to perform the Services, except for changes in such personnel due to: (i) the State's request pursuant to **Section 2.5(d)**; or (ii) the death, disability, resignation or termination of such personnel or other circumstances outside Contractor's reasonable control; and

(d) upon the reasonable written request of the State, promptly replace any Key Personnel of Contractor.

2.6 Management and Payment of Contractor Personnel.

(a) Contractor is solely responsible for the payment of Contractor Personnel, including all fees, expenses and compensation to, by or on behalf of any Contractor Personnel and, if applicable, the withholding of income taxes and payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Contractor will ensure that no Person who has been convicted of a felony or any misdemeanor involving, in any way, theft, fraud, or bribery provides any Services or has access to any State Data, State Systems or State facilities. On a case-by-case basis, the State may request that Contractor initiate a background check on any Contractor Personnel before they may have access to State Data, State Systems or State facilities. Any request for a background check will be initiated by the State and will be reasonably related to the type of work requested. The scope of the background check is at the discretion of the State and the results will be used solely to determine the eligibility of Contractor Personnel to work with State Data, State Systems or in State facilities. If provided to the State, results of background checks will be promptly returned to Contractor, and will be treated as Confidential Information. All investigations will include a Michigan State Police Background check (ICHAT) and may include a National Crime Information Center (NCIC) Finger Print check. Contractor will present attestation of satisfactory completion of such tests. Contractor is responsible for all costs and expenses associated with such background checks.

2.7 Time is of the Essence. Contractor acknowledges and agrees that time is of the essence with respect to its obligations under this Contract and that prompt and timely performance of all such obligations, including all timetables and other requirements of this Contract and each Statement of Work, is strictly required.

2.8 State Project Manager. The State will appoint and, in its reasonable discretion, replace, a State employee to serve as the primary contact with respect to the Services who will have the authority to act on behalf of the State in matters pertaining to the Support Services, including the submission and processing of Support Requests (the "**State Project Manager**").

3. License Grant and Restrictions.

3.1 Contractor License Grant. Contractor hereby grants to the State, exercisable by and through its Authorized Users, a nonexclusive, royalty-free, irrevocable (except as provided herein) right and license during the Term and such additional periods, if any, as Contractor is required to perform Services under this Contract or any Statement of Work, to:

(a) access and use the Hosted Services, including in operation with other software, hardware, systems, networks and services, for the State's business purposes, including for Processing State Data;

(b) generate, print, copy, upload, download, store and otherwise Process all GUI, audio, visual, digital and other output, displays and other content as may result from any access to or use of the Services;

(c) prepare, reproduce, print, download and use a reasonable number of copies of the Specifications and Documentation for any use of the Services under this Contract; and

(d) access and use the Services for all such non-production uses and applications as may be necessary or useful for the effective use of the Hosted Services hereunder, including for purposes of analysis, configuration, integration, testing, training, maintenance, and support which access and use will be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Services, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Hosted Services as described in **Section 3.3**.

3.2 License Restrictions. The State will not: (a) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make the Hosted Services available to any third party, except as expressly permitted by this Contract or in any Statement of Work; or (b) use or authorize the use of the Services or Documentation in any manner or for any purpose that is unlawful under applicable Law.

3.3 Use. The State will pay Contractor the corresponding Fees set forth in the Statement of Work for all Authorized Users access and use of the Service Software. Such Fees will be Contractor's sole and exclusive remedy for use of the Service Software, including any excess use.

3.4 State License Grant. The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work.

4. Service Preparation, Testing and Acceptance.

4.1 Service Preparation. Promptly upon the parties' execution of a Statement of Work, Contractor will take all steps necessary to make the Services procured thereunder ready and available for the State's use in accordance with the Statement of Work and this Contract, including any applicable milestone date or dates set forth in such Statement of Work.

4.2 Testing and Acceptance.

(a) When Contractor notifies the State in writing that the Hosted Services are ready for use in a production environment, the State will have thirty (30) days (or such other period as may be agreed upon by the Parties in writing) from receipt of the notice to test the Hosted Services to determine whether they comply in all material respects with the requirements of this Contract and the Specifications.

(b) Upon completion of the State's testing, the State will notify Contractor of its acceptance ("**Accept**" or "**Acceptance**") or, if it has identified any noncompliance with the Specifications, rejection

(“**Reject**” or “**Rejection**”) of the Hosted Services. If the State Rejects the Hosted Services, the State will provide a written list of items that will be corrected. On receipt of the State’s notice, Contractor will promptly commence, at no additional cost or charge to the State, all reasonable efforts to complete, as quickly as possible and in any event within twenty (20) days (or such other period as may be agreed upon by the Parties in writing) from receipt of the State’s notice, such necessary corrections, repairs and modifications to the Hosted Services to bring them into full compliance with the Specifications.

(c) If any corrective measures are required under **Section 4.2(b)**, upon completion of all such measures, Contractor will notify the State in writing and the process set forth in **Section 4.2(a)** and **Section 4.2(b)** will be repeated; provided that if the State determines that the Hosted Services, as revised, still do not comply in all material respects with the Specifications, the State may, in its sole discretion:

(i) require the Contractor to repeat the correction, repair and modification process set forth in **Section 4.2(b)** at no additional cost or charge to the State; or

(ii) terminate any and all of the relevant Statement of Work, this Contract and any other Statements of Work hereunder.

(d) The parties will repeat the foregoing procedure until the State Accepts the Hosted Services or elects to terminate the relevant Statement of Work as provided in **Section 4.2(c)(ii)** above. If the State so terminates the relevant Statement of Work, Contractor will refund to the State all sums previously paid to Contractor under such Statement of Work within ten (10) Business Days of the State’s written notice of termination, and the State will be relieved of all obligations thereunder.

5. Service Availability and Service Availability Credits.

(a) Availability Requirement. Contractor will make the Hosted Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a “**Service Period**”), at least 99.95% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the “**Availability Requirement**”). “**Available**” means the Hosted Services are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Specifications. “**Availability**” has a correlative meaning. The Hosted Services are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) x 100 = Availability.

5.2 Exceptions. No period of Hosted Service degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following (“**Exceptions**”):

(a) failures of the State's or its Authorized Users' internet connectivity;

(b) internet or other network traffic problems other than problems arising in or from networks actually or required to be provided or controlled by Contractor; or

(c) Scheduled Downtime as set forth in **Section 5.3**.

5.3 Scheduled Downtime. Contractor will notify the State at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request for the State's approval, extensions of Scheduled Downtime above five (5) hours and such approval by the State may not be unreasonably withheld or delayed.

5.4 Service Availability Reports. Within thirty (30) days after the end of each Service Period, Contractor will provide to the State a report describing the Availability and other performance of the Hosted Services during that calendar month as compared to the Availability Requirement and Specifications. The report will be in electronic or such other form as the State may approve in writing and will include, at a minimum: (a) the actual performance of the Hosted Services relative to the Availability Requirement and Specifications; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement or Specifications during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement and Specifications are fully met.

5.5 Remedies for Service Availability Failures.

(a) If the actual Availability of the Hosted Services is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the Fees payable for Hosted Services provided during the Service Period ("**Service Availability Credits**"):

Availability	**Credit of Fees**
≥99.95%	None
<99.9% but ≥99.0%	15%
<99.0% but ≥95.0%	35%
<95.0%	100%

(b) Any Service Availability Credits due under this **Section 5.5** will be applied in accordance with **Section 8.11**.

(c) If the actual Availability of the Hosted Services is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate this Contract and/or the applicable Statement of Work on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

6. Support and Maintenance Services. Contractor will provide Hosted Service maintenance and support services (collectively, "**Support Services**") in accordance with the provisions of this **Section 6**. The Support Services are included in the Services, and Contractor may not assess any additional Fees, costs or charges for such Support Services.

6.1 Support Service Responsibilities. Contractor will:

(a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;

(b) provide unlimited telephone support during the hours of 8 a.m. to 5 p.m. Eastern Time on Business Days;

(c) Provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

(d) Respond to and Resolve Support Requests as specified in this **Section 6**.

6.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

(a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;

(b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein or in the applicable Statement of Work):

(i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii) if Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein or in the applicable Statement of Work that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 6.4**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

6.3 Service Maintenance. Contractor will continuously maintain the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

(a) all updates, bug fixes, enhancements, new releases, new versions and other improvements to the Hosted Services, including the Service Software, that Contractor provides at no additional charge to its other similarly situated customers; and

(b) all such services and repairs as are required to maintain the Hosted Services or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosted Services, so that the Hosted Services operate properly in accordance with this Contract and the Specifications.

6.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 6.4** ("**Support Service Level Requirements**"), this Contract and the applicable Statement of Work.

(a) Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). The State Project Manager will notify Contractor of Support Requests by e-mail, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
Critical Service Error	• Issue affecting entire system or single critical production function;

	• System down or operating in materially degraded state; • Data integrity at risk; • Material financial impact; • Declared a Critical Support Request by the State; or • Widespread access interruptions.
High Service Error	• Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	• Hosted Service is operating with minor issues that can be addressed with a work around.
Low Service Error	• Request for assistance, information, or services that are routine in nature.

(b) Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. "**Resolve**" (including "**Resolved**", "**Resolution**" and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

Support Request Classification	**Service Level Metric** **(Required Response Time)**	**Service Level Metric** **(Required Resolution Time)**	**Service Level Credits** **(For Failure to Respond to any Support Request Within**	**Service Level Credits** **(For Failure to Resolve any Support Request Within**

			the Corresponding Response Time)	**the Corresponding Required Resolution Time)**
Critical Service Error	One (1) hour	Two (2) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one (1) hour increment.
High Service Error	Two (2) hours	Four (4) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional four (4) hour period or portion thereof that the corresponding Service Error remains un-Resolved.
Medium Service Error	Twenty-four (24) hours	Forty-Eight (48) hours	N/A	N/A

Low Service Error	Two (2) Business Days	Five (5) Business Days	N/A	N/A

(c) Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Service Manager and Contractor's management or engineering personnel, as appropriate, each of whom will be Key Personnel.

6.5 Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 6.4(b)** ("**Service Level Credits**") in accordance with **Section 8.11**.

6.6 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, will be a part of, and by this reference is incorporated in, this Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan will include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

7. Termination, Expiration and Transition.

7.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State: (i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel; (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or (iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If the State terminates this Contract under this **Section 7.1**, the State will issue a termination notice specifying whether Contractor will: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 7.2**.

(c) The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor will promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination. Further, Contractor will pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

7.2 Termination for Convenience. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor will: (a) cease performance immediately, or (b) continue to perform in accordance with **Section 7.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

7.3 Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor will, for a period of time specified by the State (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to: (a) continuing to perform the Services at the established Statement of Work rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all State Data; and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

7.4 Effect of Termination. Upon and after the termination or expiration of this Contract or one or more Statements of Work for any or no reason:

(a) Contractor will be obligated to perform all Transition Responsibilities specified in **Section 7.3**.

(b) All licenses granted to Contractor in State Data will immediately and automatically also terminate. Contractor will promptly return to the State all State Data not required by Contractor for its Transition Responsibilities, if any.

(c) Contractor will (i) return to the State all documents and tangible materials (and any copies) containing, reflecting, incorporating, or based on the State's Confidential Information; (ii) permanently erase the State's Confidential Information from its computer systems; and (iii) certify in writing to the State that it has complied with the requirements of this **Section 7**, in each case to the extent such materials are not required by Contractor for Transition Responsibilities, if any.

(d) Notwithstanding any provisions of this Contract or any Statement of Work to the contrary, upon the State's termination of this Contract or any Statement of Work for cause pursuant to **Section 7.1**, the State will have the right and option to continue to access and use the Services under each applicable Statement of Work, in whole and in part, for a period not to exceed one hundred and eighty (180) days from the effective date of such termination pursuant to the terms and conditions of this Contract and each applicable Statement of Work and at a reduced rate of fifty (50%) off the applicable Fees set forth in each such Statement of Work.

7.5 Survival. The rights, obligations and conditions set forth in this **Section 7.5** and **Section 1** (Definitions), **Section 7.3** (Effect of Termination; Data Retention), **Section 9** (State Data), **Section 10** (Confidentiality), **Section 11** (Security), **Section 13.1** (Indemnification), **Section 14** (Limitations of Liability), **Section 15** (Representations and Warranties), **Section 16** (Insurance) and **Section 18** (Effect of Contractor Bankruptcy) and **Section 19** (General Provisions), and any right, obligation or condition that, by its express terms or nature and context is intended to survive the termination or expiration of this Contract, survives any such termination or expiration hereof.

8. Fees and Expenses.

8.1 Fees. Subject to the terms and conditions of this Contract and the applicable Statement of Work, including the provisions of this **Section 8**, the State will pay the fees set forth in the applicable Statement of Work, subject to such increases and adjustments as may be permitted pursuant to **Section 8.2** ("**Fees During Option Years**").

8.2 Fees During Option Years. Contractor's Fees are fixed during the initial period of the Term. Contractor may increase Fees for any renewal period by providing written notice to the State at least sixty (60) calendar days prior to the commencement of such renewal period. An increase of Fees for any renewal period may not exceed three percent (3%) of the Fees effective during the immediately preceding twelve (12) month period. No increase in Fees is effective unless made in compliance with the provisions of this **Section 8.2**.

8.3 Administrative Fee and Reporting. Contractor will pay an administrative fee of [1]% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments will be made by check payable to the State of Michigan and mailed to:

Department of Technology, Management and Budget
Financial Services – Cashier Unit

Lewis Cass Building
320 South Walnut St.
P.O. Box 30681
Lansing, MI 48909

Contractor will submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports will be mailed to DTMB-Procurement. The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

8.4 Responsibility for Costs. Contractor is responsible for all costs and expenses incurred in or incidental to the performance of Services, including all costs of any materials supplied by Contractor, all fees, fines, licenses, bonds, or taxes required of or imposed against Contractor, and all other of Contractor's costs of doing business.

8.5 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees are inclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

8.6 Invoices. Contractor will invoice the State for all Fees in electronic format, via such delivery means and to such address as are specified by the State in writing from time to time. If more than one Statement of Work is in effect, Contractor will provide separate invoices for each Statement of Work. Each separate invoice will: (a) clearly identify the Statement of Work to which it relates, in such manner as is required by the State; (b) list each Fee item and Service Credit separately; (c) include sufficient detail for each line item to enable the State to verify the calculation thereof; (d) for Fees determined on a time and materials basis, report details of time taken to perform Services, and such other information as the State requires, on a per-individual basis; and (e) include such other information as may be required by the State as set forth in the applicable Statement of Work.

8.7 Payment Terms. Invoices are due and payable by the State, in accordance with the State's standard payment procedures as specified in 1984 Public Act no. 279, MCL 17.51, *et seq*., within forty-five (45) calendar days after receipt, provided the State determines that the invoice was properly rendered.

8.8 State Audits of Contractor.

(a) During the Term, and for four (4) years after, Contractor will maintain complete and accurate books and records regarding its business operations relevant to the calculation of Fees and any other information relevant to Contractor's compliance with this **Section 8**. During the Term, and for four (4) years after, upon the State's request, Contractor will make such books and records and appropriate personnel, including all financial information, available during normal business hours for inspection and audit by the State or its authorized representative, provided that the State: (a) provides Contractor with at least fifteen (15) days prior notice of any audit, and (b) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations.

(b) The State may take copies and abstracts of materials audited. The State will pay the cost of such audits unless an audit reveals an overbilling or over-reporting of five percent (5%) or more, in which case Contractor will reimburse the State for the reasonable cost of the audit. Contractor will immediately upon written notice from the State pay the State the amount of any overpayment revealed by the audit, together with any reimbursement payable pursuant to the preceding sentence.

8.9 Payment Does Not Imply Acceptance. The making of any payment or payments by the State, or the receipt thereof by Contractor, will in no way affect the responsibility of Contractor to perform the Services in accordance with this Contract, and will not imply the State's Acceptance of any Services or the waiver of any warranties or requirements of this Contract, including any right to Service Credits.

8.10 Withhold Remedy. In addition and cumulative to all other remedies in law, at equity and under this Contract, if Contractor is in material default of its performance or other obligations under this Contract or any Statement of Work and fails to cure the default within fifteen (15) days after receipt of the State's written notice of default, the State may, without waiving any other rights under this Contract, elect to withhold from the payments due to Contractor under this Contract during the period beginning with the sixteenth (16th) day after Contractor's receipt of such notice of default, and ending on the date that the default has been cured to the reasonable satisfaction of the State, an amount that, in the State's reasonable judgment, is in proportion to the magnitude of the default or the Service that Contractor is not providing. Upon Contractor's cure of the default, the State will cause the withheld payments to be paid to Contractor, without interest. Upon a final and binding legal determination that the State has withheld any payment in bad faith, such payment will promptly be paid to Contractor.

8.11 Availability and Support Service Level Credits. Contractor acknowledges and agrees that each of the Service Availability Credits and Service Level Credits assessed pursuant to **Section 5** and **Section 6**, respectively: (a) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the corresponding Service Error or Service Level Failure, which would be impossible or very difficult to accurately estimate; and (b) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract or be payable to the State upon demand. No Service Availability Credits, Service Level Credits, or combination thereof, for any Service Period may exceed the total amount of Fees that would be payable for that Service Period if the Services were fully provided in accordance with this Contract and the Specifications.

8.12 Right of Set-off. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

8.13 Support Not to be Withheld or Delayed. Contractor may not withhold or delay any Hosted Services or Support Services or fail to perform any other Services or obligations hereunder by reason of: (a) the State's good faith withholding of any payment or amount in accordance with this **Section 8**; or (b) any dispute whatsoever between the parties, including any payment or other dispute arising under or concerning this Contract or any other agreement between the parties.

9. State Data.

9.1 Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes: (a) User Data; and (b) the State's data collected, used, processed, stored, or generated in connection with the Services, including but not limited to (i) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and (ii) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This **Section 9.1** survives termination or expiration of this Contract.

9.2 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor will: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This **Section 9.2** survives termination or expiration of this Contract.

9.3 Extraction of State Data. Contractor will, within one (1) Business Days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of State Data in the format specified by the State.

9.4 Discovery. Contractor will immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Hosted Services. Contractor will notify the State Project Manager by the fastest means available and also in writing. In no event will Contractor provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for State review, revision and approval.

9.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor will, as applicable: (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or (ii) reimburse the State for any costs in notifying the affected individuals; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twenty-four (24) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (g) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and (h) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, will comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, will be reviewed and approved by the State in writing prior to its dissemination. This **Section 9.5** survives termination or expiration of this Contract.

9.6 Reserved – No HIPAA Compliance required of SaaS solution

9.7 ADA Compliance. The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's solution conform, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may provide a description of conformance with the above mentioned specifications by means of a completed Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. Any additional compliance requirements will be specified in the Statement of Work.

10. Confidentiality.

10.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; and, (c) will reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was or is: (a) in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). Notwithstanding the above, in all cases and for all matters, State Data is deemed to be Confidential Information.

10.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor's subcontractor is permissible where: (a) the subcontractor is a Permitted Subcontractor; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and (c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any of the Contractor's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 10.2**.

10.3 Cooperation to Prevent Disclosure of Confidential Information. Each party will use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party will advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

10.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

10.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party will, within five (5) Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. If Contractor or the State determine that the return of any Confidential Information is not feasible, such party will destroy the Confidential Information and certify the same in writing within five (5) Business Days from the date of termination to the other party.

11. Security.

11.1 Protection of the State's Confidential Information. Throughout the Term and at all times in connection with its actual or required performance of the Services hereunder, Contractor will:

(a) ensure that the Service Software and all State Data is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com);

(b) maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in Schedule C (POLICY 1340.00 Information Technology Information Security) and, to the extent such practices and standards are consistent with and not less protective than the foregoing requirements, are at least equal to applicable best industry practices and standards;

(c) provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or Processing of such information that ensure a level of security appropriate to the risks presented by the Processing of the State's Confidential Information and the nature of such Confidential Information, consistent with best industry practice and standards.

(d) take all reasonable measures to:

(i) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein;

(ii) prevent (A) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (B) the State's Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (C) unauthorized access to any the State's Confidential Information;

(e) continuously monitor its systems for potential areas where security could be breached.

11.2 Unauthorized Access. Contractor may not access, and will not permit any access to, State Systems, in whole or in part, whether through Contractor's Systems or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State Systems will be solely in accordance with this Contract, and in no case exceed the scope of the State's authorization pursuant to this **Section 11.2**. All State-authorized connectivity or attempted connectivity to State Systems will be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in **Schedule C** as the same may be supplemented or amended by the State and provided to Contractor from time to time.

11.3 Contractor Systems. Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for Contractor to access State Systems or otherwise in connection with the Services ("**Contractor Systems**") and will prevent unauthorized access to State Systems through the Contractor Systems.

11.4 Security Audits. During the Term, Contractor will:

(a) maintain complete and accurate records relating to its data protection practices and the security of any of the State's Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State's Confidential Information and any other information relevant to its compliance with this **Section 11**;

(b) upon the State's request, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of this Contract. The State may, but is not obligated to, perform such security audits, which will, at the State's option and request, include penetration and security tests, of any and all Contractor Systems and their housing facilities and operating environments; and

(c) if Contractor engages a third party auditor to perform a Statement on Standards for Attestation Engagements No. 16 (SSAE 16) audit of Contractor's operations, information security program or disaster recovery/business continuity plan, Contractor will provide a copy of the audit report to the State within thirty (30) days after Contractor's receipt of such report. Any such audit reports will be recognized as Contractor's Confidential Information.

11.5 Nonexclusive Remedy for Security Breach. Any failure of the Services to meet the requirements of this Contract with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of this Contract for which the State, at its option, may terminate this Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor will promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

12. Redundancy, Data Backup and Disaster Recovery. Contractor will, in accordance with the provisions of this **Section 12**, maintain or cause to be maintained disaster avoidance procedures designed to safeguard State Data and the State's other Confidential Information, Contractor's Processing capability and the availability of the Hosted Services, in each case throughout the Term and at all times in connection with its actual or required performance of the Services hereunder. The force majeure provisions of **Section 17.1** do not limit Contractor's obligations under this **Section 12**.

12.1 Redundant Hosting and Connectivity. Contractor will simultaneously operate a mirror system at a location in the United States that is geographically remote from the primary system on which the Service Software and Hosted Services are hosted. Except for its location, the mirror system will: (a) be identical in all respects to the primary system; (b) have hardware and software, network connectivity, power supplies, backup generators and other similar equipment and services that operate independently of the primary system; (c) have fully current backups of all the State Data stored on the primary system; and (d) have the ability to provide the Hosted Services in accordance with this Contract and the Specifications during the performance of routine and remedial maintenance or any outage or failure of the primary system fails. Contractor will operate, monitor and maintain such mirror system so that it may be activated within five (5) hours of any failure of the Hosted Services to be Available.

12.2 Data Backup. Contractor will conduct, or cause to be conducted, daily back-ups of State Data and perform, or cause to be performed, other periodic back-ups of State Data on at least a weekly basis and store such back-ups as specified in **Schedule D**. All backed up State Data will be located in the continental United States. On written notice from the State and, in any case, on a quarterly basis, Contractor will provide the State with a copy of the backed up State Data in such machine readable format as is specified in **Schedule D** or the State otherwise reasonably requests. Contractor will provide all quarterly back-ups at its sole cost and expense. The State will reimburse Contractor for all media costs and shipping charges reasonably incurred in fulfilling the State's additional requests for copies of backed up the State Data.

12.3 Disaster Recovery/Business Continuity. Throughout the Term and at all times in connection with its actual or required performance of the Services hereunder, Contractor will:

(a) maintain a Business Continuity and Disaster Recovery Plan for the Hosted Services (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor's current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule E**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 12.3**; and

(b) provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default under **Section 7.1(a)**.

13. Indemnification.

13.1 General Indemnification. Contractor will defend, indemnify and hold harmless the State, and the State's agencies, departments, officers, directors, employees, agents, and contractors from and against all Losses arising out of or resulting from any third party claim, suit, action or proceeding (each, an "**Action**") that does or is alleged to arise out of or result from:

(a) the Contractor's breach of any representation, warranty, covenant or obligation of Contractor under this Contract (including, in the case of Contractor, any action or failure to act by any Contractor Personnel that, if taken or not taken by Contractor, would constitute such a breach by Contractor); or

(b) any negligence or more culpable act or omission (including recklessness or willful misconduct) in connection with the performance or nonperformance of any Services or other activity actually or required to be performed by or on behalf of, Contractor (including, in the case of Contractor, any Contractor Personnel) under this Contract, provided that, to the extent that any Action or Losses described in this **Section 13.1** arises out of, results from, or alleges a claim that any of the Services does or threatens to infringe, misappropriate or otherwise violate any Intellectual Property Rights or other rights of any third party, Contractor's obligations with respect to such Action and Losses, if any, will be subject to the terms and conditions of **Section 13.2(a)** through **Section 13.2(b)** and **Section 13.3**.

13.2 Infringement Indemnification By Contractor. Contractor will indemnify, defend and hold the State, and the State's agencies, departments, officers, directors, employees, agents, and contractors harmless from and against all Losses arising out of or resulting from any Action that does or is alleged to arise out of or result from a claim that any of the Services, or the State's or any Authorized User's use thereof, actually does or threatens to infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of a third party, provided however, that Contractor will have no liability or obligation for any Action or Loss to the extent that such Action or Loss arises out of or results from any:

(a) alteration or modification of the Hosted Services or Service Software by or on behalf of the State or any Authorized User without Contractor's authorization (each, a "**State Modification**"), provided that no infringement, misappropriation or other violation of third party rights would have occurred without such State Modification and provided further that any alteration or modification made by or for Contractor at the State's request will not be excluded from Contractor's indemnification obligations hereunder unless (i) such alteration or modification has been made pursuant to the State's written specifications and (ii) the Hosted Services, as altered or modified in accordance with the State's specifications, would not have violated such third party rights but for the manner in which the alteration or modification was implemented by or for Contractor; and

(b) use of the Hosted Services by the State or an Authorized User pursuant to this Contract in combination with any software or service not provided, authorized or approved by or on behalf of Contractor, if (i) no violation of third party rights would have occurred without such combination and (ii) such software or service is not commercially available and not standard in Contractor's or the State's industry and there are no Specifications, Documentation, or other materials indicating Contractor's specification, authorization or approval of the use of the Hosted Services in combination therewith.

13.3 Mitigation.

(a) If Contractor receives or otherwise learns of any threat, warning or notice alleging that all, or any component or feature, of the Services violates a third party's rights, Contractor will promptly notify the State of such fact in writing, and take all commercially reasonable actions necessary to ensure the State's continued right to access and use such Services and otherwise protect the State from any Losses in connection therewith, including investigating such allegation and obtaining a credible opinion of counsel that it is without merit.

(b) Subject to the exclusions set forth in clauses (a) and (b) of **Section 13.2**, if any of the Services or any component or feature thereof is ruled to infringe or otherwise violate the rights of any third party by any court of competent jurisdiction, or if any use of any Services or any component thereof is threatened to be enjoined, or is likely to be enjoined or otherwise the subject of an infringement or misappropriation claim, Contractor will, at Contractor's sole cost and expense:

(i) procure for the State the right to continue to access and use the Services to the full extent contemplated by this Contract and the Specifications; or

(ii) modify or replace all components, features and operations of the Services that infringe or are alleged to infringe ("**Allegedly Infringing Features**") to make the

Services non-infringing while providing equally or more suitable features and functionality, which modified and replacement services will constitute Services and be subject to the terms and conditions of this Contract.

(c) If neither of the remedies set forth in **Section 13.3(b)** is reasonably available with respect to the Allegedly Infringing Features then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(i) refund to the State any prepaid Fees for Services that have not been provided; and

(ii) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Features for a transition period of up to six (6) months to allow the State to replace the affected Services or Allegedly Infringing Features without disruption.

(d) The remedies set forth in this **Section 13.3** are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified pursuant to **Section 13.1** and **Section 13.2**.

13.4 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor will, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel; and to (iv) retain control of the defense, at its own expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 13**, will be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

14. Limitations of Liability.

(a) The State's Disclaimer of Damages. THE STATE WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

(b) The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR

OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES SPECIFIED IN THE STATEMENT OF WORK.

15. Contractor Representations and Warranties.

15.1 Authority and Bid Response. Contractor represents and warrants to the State that:

(a) it is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) it has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) the execution of this Contract by its Representative has been duly authorized by all necessary organizational action;

(d) when executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms;

(e) the prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other bidder to the RFP; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(f) all written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's bid response to the RFP, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading; and

(g) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous five (5) years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract.

15.2 Software and Service Warranties. Contractor represents and warrants to the State that:

(a) Contractor has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

(b) neither Contractor’s grant of the rights or licenses hereunder nor its performance of any Services or other obligations under this Contract does or at any time will: (i) conflict with or violate any applicable Law, including any Law relating to data privacy, data security or personal information; (ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or (iii) require the provision of any payment or other consideration by the State or any Authorized User to any third party, and Contractor will promptly notify the State in writing if it becomes aware of any change in any applicable Law that would preclude Contractor’s performance of its material obligations hereunder;

(c) as accessed and used by the State or any Authorized User in accordance with this Contract and the Specifications, the Hosted Services, Documentation and all other Services and materials provided by Contractor under this Contract will not infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of any third party;

(d) there is no settled, pending or, to Contractor’s knowledge as of the Effective Date, threatened Action, and it has not received any written, oral or other notice of any Action (including in the form of any offer to obtain a license): (i) alleging that any access to or use of the Services or Service Software does or would infringe, misappropriate or otherwise violate any Intellectual Property Right of any third party; (ii) challenging Contractor’s ownership of, or right to use or license, any software or other materials used or required to be used in connection with the performance or receipt of the Services, or alleging any adverse right, title or interest with respect thereto; or (iii) that, if decided unfavorably to Contractor, would reasonably be expected to have an actual or potential adverse effect on its ability to perform the Services or its other obligations under this Contract, and it has no knowledge after reasonable investigation of any factual, legal or other reasonable basis for any such litigation, claim or proceeding;

(e) the Service Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in **Section 5**;

(f) all Specifications are, and will be continually updated and maintained so that they continue to be, current, complete and accurate and so that they do and will continue to fully describe the Hosted Services in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Hosted Services have any material undocumented feature;

(g) the Contractor Systems and Services are and will remain free of Harmful Code;

(h) Contractor will not advertise through the Hosted Services (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by the State;

(i) Contractor will perform all Services in a timely, professional and workmanlike manner with a level of care, skill, practice and judgment consistent with generally recognized industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet Contractor’s obligations (including the Availability Requirement and Support Service Level Requirements) under this Contract;

(j) During the term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Services, will apply solely to Contractor’s (or its subcontractors) facilities and systems that host the Services (including any disaster recovery site), and regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against State systems or networks; and

(k) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever.

15.3 DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS CONTRACT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE UNDER OR IN CONNECTION WITH THIS CONTRACT OR ANY SUBJECT MATTER HEREOF.

16. Insurance.

16.1 Required Coverage.

(a) **Insurance Requirements.** Contractor will maintain the insurances identified below and is responsible for all deductibles. All required insurance will: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by an company with an A.M. Best rating of "A" or better and a financial size of VII or better

Required Limits	Additional Requirements
Workers' Compensation Insurance	
Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	

Minimal Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	

(b) If Contractor's policy contains limits higher than the minimum limits, the State is entitled to coverage to the extent of the higher limits. The minimum limits are not intended, and may not be construed to limit any liability or indemnity of Contractor to any indemnified party or other persons.

(c) If any of the required policies provide **claims-made** coverage, Contractor will: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of contract work; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the contract of work; and (c) if coverage is canceled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor will purchase extended reporting coverage for a minimum of three (3) years after completion of work.

(d) Contractor will: (a) provide insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

16.2 Non-waiver. This **Section 16** is not intended to and is not be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

17. Force Majeure.

17.1 Force Majeure Events. Subject to **Section 17.2**, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached this Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

17.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under this Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate this Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates this Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under this Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

17.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of this Contract:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of the Contractor Systems or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Contractor Systems; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event; and

(b) no Force Majeure Event modifies or excuses Contractor's obligations under **Section 5** (Service Availability and Service Availability Credits), **Section 6.5** (Support Service Level Credits), **Section 9** (State Data), **Section 10** (Confidentiality), **Section 11** (Security), **Section 12** (Data Backup and Disaster Recovery) or **Section 13** (Indemnification), or any Availability Requirement, Support Service Level Requirement, Service Availability Credit or Service Level Credit obligations under this Contract or an applicable Statement of Work.

18. Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and the subject matter of this agreement, including the Services, is and will be deemed to be "embodiments" of "intellectual property" for purposes of and as such terms are used in and interpreted under section 365(n) of the United States Bankruptcy Code (the "**Code**") (11 U.S.C. § 365(n) (2010)). The State has the right to exercise all rights and elections under the Code and all other applicable bankruptcy, insolvency and similar laws with respect to this Contract (including all executory Statement of Works). Without limiting the generality of the foregoing, if Contractor or its estate becomes subject to any bankruptcy or similar proceeding, subject to the State's rights of election, all rights and licenses granted to the State under this Contract will continue subject to the respective terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract.

19. General Provisions.

19.1 Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

19.2 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for or bind the other party in any manner whatsoever.

19.3 Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates will not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

19.4 Notices. All notices, requests, consents, claims, demands, waivers and other communications hereunder, other than routine communications having no legal effect, will be in writing and addressed to the parties as follows (or as otherwise specified by a party in a notice given in accordance with this Section):

If to Contractor:

MediaPro Holdings, LLC

20021 120th Avenue NE, Suite 102

Bothell, WA 98011

E-mail: David.nelson@mediapro.com

Attention: David Nelson

Title: Account Manager

If to the State:

DTMB-Procurement

525 West Allegan Street

Lansing Michigan 48933

E-mail: BreenM@michigan.gov

Attention: Michael Breen

Title: Buyer – IT Division

Notices sent in accordance with this **Section 19.4** will be deemed effectively given: (a) when received, if delivered by hand (with written confirmation of receipt); (b) when received, if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by e-mail (with confirmation of transmission), if sent during normal business hours of the recipient, and on the next business day, if sent after normal business hours of the recipient; or (d) on the fifth (5th) day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid.

19.5 Extended Purchasing Program. This Contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal. Upon written agreement between the State and Contractor, this Contract may also be extended to: (a) State of Michigan employees, and (b) other states (including governmental subdivisions and authorized entities). If extended, Contractor will supply all Contract Activities at the established Contract prices and terms, and the State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions. Contractor will submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

19.6 Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

19.7 Entire Agreement. This Contract, including all Statements of Work and other Schedules and Exhibits, constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, both written and oral, with respect to such subject matter. In the event of any conflict between the terms of this Contract and those of any Schedule, Exhibit or other document, the following order of precedence governs: (a) first, this Contract, excluding its Exhibits and Schedules; and (b) second, the Exhibits and Schedules to this Contract as of the Effective Date. NO TERMS ON CONTRACTORS WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE.

ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

19.8 Assignment. Contractor may not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Contract, in each case whether voluntarily, involuntarily, by operation of law or otherwise, without the State's prior written consent. The State has the right to terminate this Contract in its entirety or any Services or Statements of Work hereunder, pursuant to **Section 7.2**, if Contractor delegates or otherwise transfers any of its obligations or performance hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, and no such delegation or other transfer will relieve Contractor of any of such obligations or performance. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation or reorganization involving Contractor (regardless of whether Contractor is a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations, or performance under this Contract for which the State's prior written consent is required. Any purported assignment, delegation, or transfer in violation of this **Section 19.8** is void.

19.9 No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

19.10 Amendment and Modification; Waiver. This Contract may only be amended, modified or supplemented by an agreement in writing signed by each party's Contract Administrator. No waiver by any party of any of the provisions hereof is effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Contract, no failure to exercise, or delay in exercising, any right, remedy, power or privilege arising from this Contract will operate or be construed as a waiver thereof; nor will any single or partial exercise of any right, remedy, power or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege.

19.11 Severability. If any term or provision of this Contract is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability will not affect any other term or provision of this Contract or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal or unenforceable, the parties hereto will negotiate in good faith to modify this Contract so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

19.12 Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract will be resolved in the Michigan Court of Claims. Complaints against the State will be initiated in Ingham

County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or forum non conveniens. Contractor will appoint agents in Michigan to receive service of process

19.13 Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract would give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this **Section 19.13**.

19.14 Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, or mental or physical disability. Breach of this covenant is a material breach of this Contract.

19.15 Unfair Labor Practice. Under 1980 PA 278, MCL 423.321, *et seq.*, the State will not award a contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled under MCL 423.322. This information is compiled by the United States National Labor Relations Board. A contractor of the State, in relation to the contract, will not enter into a contract with a subcontractor, manufacturer, or supplier whose name appears in this register. Under MCL 423.324, the State may void any contract if, after award of the contract, the contractor as an employer or the name of the subcontractor, manufacturer or supplier of the contractor appears in the register.

19.16 Schedules - All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	General Proposal Requirements
Schedule C	POLICY 1340.00 Information Technology Information Security
Attachment A	Cost Table Pricing

19.17 Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.