



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 3
to
Contract Number MA20000000187

| | |
|-------------------|------------------------|
| CONTRACTOR | NOVINZIO |
| | 132A N Euclid Ave |
| | Upland CA 91786 |
| | Sam Stickler |
| | 818-876-2983 |
| | sstickler@novinzio.com |
| | VS0100081 |

| | | | |
|--------------|-------------------------------|------------------------|------|
| STATE | Program Manager | Various | DTMB |
| | | | |
| STATE | Contract Administrator | Mecca Martin | DTMB |
| | | (517) 230-5694 | |
| | | MartinM42@michigan.gov | |

| CONTRACT SUMMARY | | | | |
|--|-------------------------|------------------------------------|---|-------------------|
| Enterprise eSignature Solution | | | | |
| INITIAL EFFECTIVE DATE | INITIAL EXPIRATION DATE | INITIAL AVAILABLE OPTIONS | EXPIRATION DATE BEFORE | |
| December 9, 2019 | December 8, 2024 | 5 - 12 Months | December 8, 2024 | |
| PAYMENT TERMS | | DELIVERY TIMEFRAME | | |
| NET45 | | N/A | | |
| ALTERNATE PAYMENT OPTIONS | | | EXTENDED PURCHASING | |
| <input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other | | | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | |
| MINIMUM DELIVERY REQUIREMENTS | | | | |
| N/A | | | | |
| DESCRIPTION OF CHANGE NOTICE | | | | |
| OPTION | LENGTH OF OPTION | EXTENSION | LENGTH OF EXTENSION | REVISED EXP. DATE |
| <input checked="" type="checkbox"/> | 60 Months | <input type="checkbox"/> | | December 8, 2029 |
| CURRENT VALUE | VALUE OF CHANGE NOTICE | ESTIMATED AGGREGATE CONTRACT VALUE | | |
| \$12,000,000.00 | \$0.00 | \$12,000,000.00 | | |
| DESCRIPTION | | | | |
| Effective 12/9/2024, the State is exercising 5 option years. The revised contract expiration date is 12/8/2029, see Schedule A, Attachment 2 – Pricing for option year cost. | | | | |
| 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 | Richard DeMello | 517-930-6301 | DeMelloR@michigan.gov |
| DTMB | Giget Schlyer | 517-582-8330 | SchlyerG@michigan.gov |

Schedule A, Attachment 2 - Pricing

Table 1: Implementation Milestones and Deliverables

| ID | Deliverable Item | Cost per deliverable |
|----|---|----------------------|
| | Project Planning | \$6,600.00 |
| | Requirements and Design Validation | \$7,700.00 |
| | SUITE/Keylight and other misc project documentation | \$29,600.00 |
| | Provision Environments | \$2,200.00 |
| | MiLogin Integration | \$2,200.00 |
| | Installation and Configuration | \$8,800.00 |
| | Training Services | \$4,400.00 |
| | Testing and Acceptance | \$4,400.00 |
| | Product Documentation | \$275.00 |
| | Post Production Warranty | \$1,096.00 |
| | Production Support Services | \$0.00 |
| | Total | \$67,271.00 |

Table 2: Transaction costs for FedRamp hosted transactions.

Transactions include email only, SMS and/or Static Knowledgebase Answers (SKBA) authentication for signers.

Sender Authentication may include phone authentication to confirm the sender's identity).

| ID | Deliverable Item | Annual Cost |
|----|------------------|-------------|
| | FedRAMP | \$12,600.00 |

| ID | Deliverable Item | Cost Per Transaction based on the annual Transaction Counts |
|----|------------------|---|
| | 1,000 to 4,999 | 3.09 |
| | 5,000-9,999 | 2.56 |
| | 10,000-15,000 | 2.04 |
| | 15,001-24,999 | 2.04 |
| | 25,000-49,999 | 1.77 |
| | 50,000-99,999 | 1.38 |
| | 100,000-249,999 | 1.11 |
| | 250,000-499,999 | 0.85 |
| | 500,000-999,999 | 0.66 |
| | 1,000,000+ | 0.56 |

Notes for usage transaction costs:

- Transaction totals for tables 3, 4, and 5 are independent.
- A transaction is 1 -10 documents, unlimited signers. A transaction is counted once a draft is created regardless of whether it is sent or completed.
- SOM will be billed quarterly for transaction usage based on the cost of the current transaction volume.
- Transactions can be purchased at the beginning of the term and an annual true up process then recalculates the transaction cost based on additional usage of transactions. All transactions are charged at the rate of the total transaction volume rate.
- Overages are billed at 1.2x the current transaction rate.
- Due to the limited reporting capabilities within the software and the State using a distributed cost model OSS will provide the State detailed monthly reports for transactions including but not limited to following fields: sender, sender user attributes, authentication method, number of signers, and transaction status.
- Non FedRAMP pricing receives a 20% discount off of the transactional pricing found in Table2

Optional Services

Table 3: Additional Optional Cost Items as part of the solution (Contractor can add additional items)

| ID | Deliverable Item | Cost per transaction | Define to define unit |
|----|---|----------------------|--------------------------|
| | API/SDK usage costs | \$0.00 | \$0.00 |
| | Cloud connector costs (e.g. Salesforce) | \$80.00 | Cost per user/per year |
| | SimpliGov Forms/Workflow - 20 workflows unlimited users | \$220,500.00 | Annual Cost |
| | SimpliGov Base Platform 1 Workflow SAPGOVPL | \$43,312.00 | Annual Cost |
| | SimpliGov 1-10 Workflows - Price per Workflow (SAPGOVWF1) | \$10,815.00 | Annual Cost |
| | SimpliGov 11-20 Workflows - Price per Workflow (SAPGOVWF11) | \$7,140.00 | Annual Cost |
| | SimpliGov Analytics (SAPGOVAN) | \$14,466.00 | Annual Cost |
| | OneSpan Archiver* | \$4,995.00 | Per API Key |
| | OneSpan Data File Writer* | \$3,995.00 | Per API Key |
| | DKIM/SMTP relay | \$2,000.00 | Per Domain |
| | Print Driver (not FedRAMP ready) | \$0.00 | Per Desktop |
| | Support for CAC/PIV | \$0.00 | |
| | Document Storage Cost | \$0.00 | |
| | Print Driver Enhancement for FedRAMP compatibility | \$23,000.00 | One Time Enhancement Fee |

*Note: The Archiver and Data File Writer will be licensed per API Key except for RMS usage. RMS will be able to use their software with all API Keys at no additional cost because of being the Enterprise eSignature administrators for all agencies. Individual agencies using the software will need to have their own copy per API Key as noted in the table.

Table 4: Customizations

| ID | Deliverable Item | Number of hours | Cost |
|----|--|-----------------|--------------------|
| | Each of these items ONLY include requirements and development | | |
| | Other Pre-Built API Modules - 20% Optional Annual Maintenance for each not included. These modules are built to be hosted on a client's Azure tenant. Add \$2,000 for On-Premise deployment for each. | | |
| | OneSpan Attachment to Package - | | \$3,995.00 |
| | OneSpan SharePoint Online / 2016 Archive | | \$6,995.00 |
| | OneSpan Office 365 Workflow Integration | | \$12,995.00 |
| | OneSpan Custom Email Notifications | | \$9,995.00 |
| | OneSpan Large File Split/Sign/Seal Utility | | \$12,300.00 |

Table 5: Labor Rates for Services for relevant Services

| ID | Rated Structure | Cost per hour |
|------|--------------------------------|---------------|
| I.11 | Novinzio Business Consultant | 183.75 |
| I.12 | Novinzio Project Manager | 194.25 |
| I.13 | Novinzio Integration Developer | 183.75 |
| I.14 | Novinzio QA Tester | 131.25 |
| I.15 | Novinzio Technical Writer | 131.25 |
| I.16 | Novinzio Trainer | 183.75 |
| I.17 | OneSpan Solution Consultant | 288.75 |
| I.18 | SimpliGOV Consultant | 262.50 |

Table 6: User Type and Capacity Based Pricing:

| ID | Deliverable Item | Initial purchase cost per user PER YEAR | Annual maintenance cost per user - Standard is included |
|----|--|---|---|
| | Procurement of Software Licenses (C.1) | | |
| | Administrator Accounts | | |
| | Up to 15 users | \$252.00 | 0 |
| | Up to 25 users | 252 | 0 |
| | Up to 50 users | 252 | 0 |
| | Agency Workgroup Administrators | | 0 |
| | Up to 50 users | 252 | 0 |
| | 50 to 100 users | 226.80 | 0 |
| | 100 to 150 users | 203.70 | 0 |
| | 100 to 200 users | 203.70 | 0 |
| | 100 to 250 users | 214 | 0 |
| | Over 250 users | 183.75 | 0 |
| | Senders | | |
| | Up to 100 users | 252 | 0 |

| | | | |
|--|------------------|---------------|----------|
| | 100 to 250 users | 203.70 | 0 |
| | 100 to 500 users | 203.70 | 0 |

| | | | |
|--|--------------------|--------|---|
| | 500 to 1000 users | 183.75 | 0 |
| | 1000 to 2000 users | 164.85 | 0 |
| | 1000 to 2000 users | 164.85 | 0 |
| | Signers | | 0 |
| | Up to 1000 users | 0 | 0 |
| | Up to 10000 users | 0 | 0 |
| | Up to 50000 users | 0 | 0 |
| | Up to 75000 users | 0 | 0 |
| | Up to 100000 users | 0 | 0 |
| | Over 500000 users | 0 | 0 |

Table 7: Signer Authentication Transactions (Optional service that uses Equifax for signer validation) for signers. These are additional transaction costs if using the Equifax Authentication.

| ID | Deliverable Item | Cost per transaction per month | Cost for Incomplete |
|----|-------------------|--------------------------------|---------------------|
| | 500 to 10,000 | 2.15 | 0.55 |
| | 10,001-15,000 | 2.15 | 0.55 |
| | 15,001-25,000 | 2.15 | 0.55 |
| | 25,001-50,000 | 1.91 | 0.55 |
| | 50,001-150,000 | 1.59 | 0.55 |
| | 150,000-250,000 | 1.49 | 0.49 |
| | 250,001-1,000,000 | 1.19 | 0.49 |
| | 1,000,001+ | 1.14 | 0.45 |

Table 8: Add – On OneSpan Remote Online Notary - Price per transaction. Transaction means a package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the “Transaction Limit”) created or sent through the SaaS Service (includes both Incomplete and Complete Transactions). Subscription license, cloud valid license for 1 year. RON includes Equifax KBA and IDV.

| ID | | Deliverable Item | Tiered Price level | Price |
|----|---------------|---|--------------------|---------|
| | 5414602905000 | Notary - RON - Txn Essentials (up to 500 notarizations) | 1-500 | \$32.55 |
| | 5414602905017 | Notary - RON - Txn Essentials (up to 1,000 notarizations) | 501-1000 | \$30.45 |
| | 5414602905031 | Notary - RON - Transactions (up to 2500 notarizations) | 1001-2500 | \$29.40 |

Table 9: Add On – Identity Verification (IDV) – Mobile Facial / Biometric Recognition - Price per transaction. Transaction means a package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the “Transaction Limit”) created or sent through the SaaS Service (includes both Incomplete and Complete Transactions). Subscription license, cloud valid license for 1 year

| ID | | Deliverable Item | Tiered Price level | Price |
|-----------|---------------|---------------------------------------|---------------------------|--------------|
| | 5414602966162 | IDV - Document Verification with Face | 1-5000 | \$4.15 |
| | 5414602966148 | IDV - Platform | 1-5000 | \$0.48 |
| | 5414602966179 | IDV - OTP | 1-5000 | \$0.37 |



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 2
 to
 Contract Number 200000000187

| | |
|-------------------|------------------------|
| CONTRACTOR | NOVINZIO |
| | 132A N Euclid Ave |
| | Upland, CA 91786 |
| | Sam Stickler |
| | 818-876-2983 |
| | sstickler@novinzio.com |
| | VS0100081 |

| | | | |
|--------------|-------------------------------|------------------------|------|
| STATE | Program Manager | Richard DeMello | DTMB |
| | | 517-930-6301 | |
| | | demellor@Michigan.gov | |
| | Contract Administrator | Mecca Martin | DTMB |
| | | (517) 230-5694 | |
| | | martinm42@michigan.gov | |

CONTRACT SUMMARY

ENTERPRISE ESIGNATURE SOLUTION

| INITIAL EFFECTIVE DATE | INITIAL EXPIRATION DATE | INITIAL AVAILABLE OPTIONS | EXPIRATION DATE BEFORE |
|------------------------|-------------------------|---------------------------|------------------------|
| December 9, 2019 | December 8, 2024 | 5 - 1 Year | December 8, 2024 |

| PAYMENT TERMS | DELIVERY TIMEFRAME |
|---------------|--------------------|
| | |

| ALTERNATE PAYMENT OPTIONS | EXTENDED PURCHASING |
|---|---|
| <input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

MINIMUM DELIVERY REQUIREMENTS

| |
|--|
| |
|--|

DESCRIPTION OF CHANGE NOTICE

| OPTION | LENGTH OF OPTION | EXTENSION | LENGTH OF EXTENSION | REVISED EXP. DATE |
|--------------------------|------------------|--------------------------|---------------------|-------------------|
| <input type="checkbox"/> | | <input type="checkbox"/> | | N/A |

| CURRENT VALUE | VALUE OF CHANGE NOTICE | ESTIMATED AGGREGATE CONTRACT VALUE |
|-----------------|------------------------|------------------------------------|
| \$12,000,000.00 | \$0.00 | \$12,000,000.00 |

DESCRIPTION

Effective September 20th, 2023, the following amendment is incorporated into this Contract to update Schedule A, Attachment 2 - Pricing for the addition of Remote Online Notary (RON) and Identity Verification (IDV). No additional funding is needed at this time; existing funds are adequate to support this change.

Please note, the State's Contract Administrator has been changed to Mecca Martin.

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

Schedule A, Attachment 2 - Pricing

Table 8: Add – On OneSpan Remote Online Notary - Price per transaction. Transaction means a package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the “Transaction Limit”) created or sent through the SaaS Service (includes both Incomplete and Complete Transactions). Subscription license, cloud valid license for 1 year. RON includes Equifax KBA and IDV.

| ID | | Deliverable Item | Tiered Price level | Price |
|-----------|---------------|---|---------------------------|--------------|
| | 5414602905000 | Notary - RON - Txn Essentials (up to 500 notarizations) | 1-500 | \$31.00 |
| | 5414602905017 | Notary - RON - Txn Essentials (up to 1,000 notarizations) | 501-1000 | \$29.00 |
| | 5414602905031 | Notary - RON - Transactions (up to 2500 notarizations) | 1001-2500 | \$28.00 |

Table 9: Add On – Identity Verification (IDV) – Mobile Facial / Biometric Recognition - Price per transaction. Transaction means a package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the “Transaction Limit”) created or sent through the SaaS Service (includes both Incomplete and Complete Transactions). Subscription license, cloud valid license for 1 year

| ID | | Deliverable Item | Tiered Price level | Price |
|-----------|---------------|---------------------------------------|---------------------------|--------------|
| | 5414602966162 | IDV - Document Verification with Face | 1-5000 | \$3.95 |
| | 5414602966148 | IDV - Platform | 1-5000 | \$0.46 |
| | 5414602966179 | IDV - OTP | 1-5000 | \$0.35 |

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 1
 to
 Contract Number 200000000187

| | |
|-------------------|------------------------|
| CONTRACTOR | NOVINZIO |
| | 132A N Euclid Ave |
| | Upland, CA 91786 |
| | Sam Stickler |
| | 818-876-2983 |
| | sstickler@novinzio.com |
| | VS0100081 |

| | | | |
|------------------------|-------------------------------|-----------------|------|
| STATE | Program Manager | Richard DeMello | DTMB |
| | | 517-930-6301 | |
| | demellor@Michigan.gov | | |
| | Contract Administrator | Jordan Sherlock | DTMB |
| 517-243-5556 | | | |
| sherlockj@michigan.gov | | | |

CONTRACT SUMMARY

| | | | |
|---------------------------------------|--------------------------------|----------------------------------|---|
| ENTERPRISE ESIGNATURE SOLUTION | | | |
| INITIAL EFFECTIVE DATE | INITIAL EXPIRATION DATE | INITIAL AVAILABLE OPTIONS | EXPIRATION DATE BEFORE |
| December 9, 2019 | December 8, 2024 | 5 - 1 Year | December 8, 2024 |
| PAYMENT TERMS | | DELIVERY TIMEFRAME | |
| | | | |
| ALTERNATE PAYMENT OPTIONS | | | EXTENDED PURCHASING |
| <input type="checkbox"/> P-Card | <input type="checkbox"/> PRC | <input type="checkbox"/> Other | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

MINIMUM DELIVERY REQUIREMENTS

| |
|--|
| |
|--|

DESCRIPTION OF CHANGE NOTICE

| | | | | |
|--------------------------|-------------------------------|---|----------------------------|--------------------------|
| OPTION | LENGTH OF OPTION | EXTENSION | LENGTH OF EXTENSION | REVISED EXP. DATE |
| <input type="checkbox"/> | | <input type="checkbox"/> | | December 8, 2024 |
| CURRENT VALUE | VALUE OF CHANGE NOTICE | ESTIMATED AGGREGATE CONTRACT VALUE | | |
| \$12,000,000.00 | \$0.00 | \$12,000,000.00 | | |

DESCRIPTION

Effective April 22nd, 2021, this contract is incorporating the following pricing table for optional services.

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

Optional Services:

Table 3: Additional Optional Cost Items as part of the solution (Contractor can add additional items.)

| | Deliverable Item | Cost per Unit | Unit | Annual Maintenance |
|--|--|----------------------|----------------------|---------------------------|
| | API/SDK usage costs | \$0.00 | \$0.00 | N/A |
| | Cloud connector costs (e.g. Salesforce) | \$72.00 | Annual cost per user | N/A |
| | SimpliGov Forms/Workflow - 20 workflows unlimited users | \$210,000.00 | Annual Cost | N/A |
| | SimpliGov Base Platform 1 Workflow SAPGOVPL | \$41,250.00 | Annual Cost | N/A |
| | SimpliGov 1-10 Workflows - Price per Workflow (SAPGOVWF1) | \$10,300.00 | Annual Cost | N/A |
| | SimpliGov 11-20 Workflows - Price per Workflow (SAPGOVWF11) | \$6,800.00 | Annual Cost | N/A |
| | SimpliGov Analytics (SAPGOVAN) | \$13,777.00 | Annual Cost | N/A |
| | SimpliGov Workflow Transaction (SAPELATRANS) (new pricing alternative) Unlimited Forms, Users and Workflows 25,000 Transaction Minimum | \$4.00 | Annual Cost | N/A |
| | SimpliGov Data Storage (SAPSTORAGE) per each 1TB of Data | \$6,000.00 | Annual Cost | NA |
| | SimpliGov Additional Tenant (SAPTENANT) for additional Tenants within a Department | \$6,000.00 | Annual Cost | NA |
| | UiPath - Attended - Named User The Attended offering includes Task Capture, Action Center and an Attended Robot. The Attended Robot is deployed on a desktop and allows a user to access, manage, and run automations. Licenses a single named user. | \$2,400.00 | Annual Cost | NA |
| | UiPath - Orchestrated - RPA Developer Pro Multiuser The RPA Developer Pro offering includes Task Capture, Action Center, Attended Robot, StudioX, Studio and Studio Pro. Studio Pro is an advanced IDE that includes RPA testing and Application Testing capabilities, cutting-edge RPA features and coding services. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On. Orchestrated from the UiPath Automation Cloud. | \$12,000.00 | Annual Cost | NA |

| | | | |
|---|-------------|-------------|----|
| <p>UiPath - Orchestrated Action Center - Multiuser The Action Center offering includes Task Capture and Action Center. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. License per Named User with a minimum sale of 5 users. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On. Orchestrated from the UiPath Automation Cloud</p> | \$1,600.00 | Annual Cost | NA |
| <p>UiPath - Orchestrated - RPA Developer Pro - Named User The RPA Developer Pro offering includes Task Capture, Action Center, Attended Robot, StudioX, Studio and Studio Pro. Studio Pro is an advanced IDE that includes RPA testing and Application Testing capabilities, cutting-edge RPA features and coding services. Intended for a single named user. Orchestrated from the UiPath Automation Cloud.</p> | \$6,700.00 | Annual Cost | NA |
| <p>UiPath - Orchestrated Unattended Robot An Unattended Robot independently executes automations. It runs on a virtual desktop, in a secure session, end-to-end, without human intervention. Licenses a single robot. Orchestrated from the UiPath Automation Cloud.</p> | \$12,000.00 | Annual Cost | NA |
| <p>UiPath - AI Starter License Pack License AI Starter Pack, including 4 Cloud AI Robot, 1 Cloud AI Robot Pro, 3 Cloud Document Understanding Page Bundle and 5 Cloud Action Center - Named User.</p> | \$69,900.00 | Annual Cost | NA |
| <p>UiPath - Orchestrated Action Center - Multiuser The Action Center offering includes Task Capture and Action Center. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. License per Named User with a minimum sale of 5 users. Each Multiuser license adds 3 authorized users. Requires UiPath Multiuser Add-On. Orchestrated from the UiPath Automation Cloud</p> | \$980.00 | Annual Cost | NA |

| | | | |
|--|-------------|------------------------------|----------|
| <p>UiPath - Document Understanding Page Bundle - 40K Document Understanding enables UiPath robots to digitize, classify, and extract information from forms, documents, and unstructured text using a combination of OCR, template, and machine learning approaches. This offering is priced per page for each extraction method. This SKU contains a bundle of 40K pages, but certain features and models may be metered at different rates. For greater volumes, simply order as many as needed to meet required</p> | \$8,000.00 | Annual Cost | NA |
| <p>UiPath - Orchestrated Action Center - Named User The Action Center offering includes Task Capture and Action Center. Action Center is a central portal allowing humans and unattended robots to seamlessly collaborate on a process. License per Named User with a minimum sale of 5 users. Orchestrated from the UiPath Automation Cloud</p> | \$640.00 | Annual Cost | NA |
| <p>OneSpan Archiver/Data File Writer (Enterprise)*</p> | \$44,590.00 | State of Michigan Enterprise | \$11,238 |
| <p>OneSpan Archiver/Data File Writer (Department)*</p> | \$8990.00 | Per State Department | \$1,750 |
| <p>DKIM/SMTP relay</p> | \$2,000.00 | Per Domain | N/A |
| <p>Print Driver (not FedRAMP ready)</p> | \$0.00 | Per Desktop | N/A |
| <p>Support for CAC/PIV</p> | \$0.00 | | N/A |
| <p>Document Storage Cost</p> | \$0.00 | | N/A |
| <p>Print Driver Enhancement for FedRAMP compatibility</p> | \$23,000.00 | One Time Enhancement Fee | N/A |

*Note: RMS will be able to use their software with all OneSpan accounts at no additional cost because of being the Enterprise eSignature administrators for all agencies.



STATE OF MICHIGAN PROCUREMENT
 Department of Technology, Management, and Budget
 525 W Allegan St, Lansing, MI 48933

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. 200000000187
 between
 THE STATE OF MICHIGAN
 and

| | |
|-------------------|------------------------|
| CONTRACTOR | Novinzio |
| | 132A N Euclid Ave |
| | Upland, CA 91786 |
| | Sam Stickler |
| | (818) 876-2983 |
| | sstickler@novinzio.com |
| | VS0100081 |

| | | | |
|---------------------|------------------------|-----------------|------|
| STATE | Program Manager | Richard DeMello | DTMB |
| | | (517) 930-6301 | |
| | demellor@michigan.gov | | |
| | Contract Administrator | Mike Breen | DTMB |
| (517) 249-0428 | | | |
| breenm@michigan.gov | | | |

| CONTRACT SUMMARY | | | |
|---|-------------------------|---------------------------|---|
| DESCRIPTION: Enterprise eSignature Solution | | | |
| INITIAL EFFECTIVE DATE | INITIAL EXPIRATION DATE | INITIAL AVAILABLE OPTIONS | EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW |
| 12/9/2019 | 12/8/2024 | (5) 1-Year | |
| PAYMENT TERMS | | DELIVERY TIMEFRAME | |
| Net 45 | | | |
| ALTERNATE PAYMENT OPTIONS | | | EXTENDED PURCHASING |
| <input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other | | | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| MINIMUM DELIVERY REQUIREMENTS | | | |
| N/A | | | |
| MISCELLANEOUS INFORMATION | | | |
| N/A | | | |
| ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION | | | \$12,000,000.00 |

FOR THE CONTRACTOR:

Novinzio

Company Name

E-SIGNED by Samuel Stickler
on 2019-12-08 18:29:47 PST

Authorized Agent Signature

Samuel Stickler

Authorized Agent (Print or Type)

December 08, 2019

Date

FOR THE STATE:



Signature

Heather Calahan

Name & Title

Agency

12/a/19

Date

CONTRACT TERMS

This Software Contract (this “**Contract**”) is agreed to between the State of Michigan (the “**State**”) and Novinzio (“**Contractor**”), a California Corporation. This Contract is effective on December 9, 2019 (“**Effective Date**”), and unless earlier terminated, will expire on December 8, 2024(the “**Term**”).

This Contract may be renewed for up to 5 additional 1-year periods. Renewal must be by written notice from the State and will automatically extend the Term of this Contract.

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

“**Acceptance**” has the meaning set forth in **Section 12.5**.

“**Acceptance Tests**” means such tests as may be conducted in accordance with **Section 12** and the Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

“**Affiliate**” of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term “control” (including the terms “controlled by” and “under common control with”) means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

“**Allegedly Infringing Materials**” has the meaning set forth in **Section 28.3(b)(ii)**.

“**API**” means all Application Programming Interfaces and associated API Documentation provided by Contractor, and as updated from time to time, to allow the Software to integrate with various State and Third Party Software.

“**Approved Open-Source Components**” means Open-Source Components that may be included in or used in connection with the Software and are specifically identified in an exhibit to the Statement of Work, and approved by the State.

“**Authorized Users**” means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

“**Business Day**” means a day other than a Saturday, Sunday or other day on which the State is authorized or required by Law to be closed for business.

“**Business Owner**” is the individual appointed by the agency buyer to (a) act as the agency’s representative in all matters relating to the Contract, and (b) co-sign off on notice of Acceptance for the Software. The Business Owner will be identified in the Statement of Work.

“**Business Requirements Specification**” means the initial specification setting forth the State’s business requirements regarding the features and functionality of the Software, as set forth in the Statement of Work.

“**Change**” has the meaning set forth in **Section 2.2**.

“**Change Notice**” has the meaning set forth in **Section 2.2(b)**.

“**Change Proposal**” has the meaning set forth in **Section 2.2(a)**.

“**Change Request**” has the meaning set forth in **Section 2.2**.

“**Confidential Information**” has the meaning set forth in **Section 20.1**.

“**Configuration**” means State-specific changes made to the Software without Source Code or structural data model changes occurring.

“**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 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’s Bid Response**” means the Contractor’s proposal submitted in response to the RFP.

“**Contractor Personnel**” means all employees of Contractor or any Permitted Subcontractors involved in the performance of Services hereunder.

“**Contractor’s Test Package**” has the meaning set forth in **Section 11.2**.

“**Criminal Justice Information Data**” or “**CJI Data**” means data necessary for criminal justice agencies to perform their mission and enforce the laws.

“**Deliverables**” means the Software, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in the Statement of Work.

“**Dispute Resolution Procedure**” has the meaning set forth in **Section 33.1**.

“**Documentation**” means 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.

“**DTMB**” means the Michigan Department of Technology, Management and Budget.

“**Effective Date**” has the meaning set forth in the preamble.

“**Fees**” means collectively, the License Fees, Implementation Fees, and Support Services Fees.

“**Financial Audit Period**” has the meaning set forth in **Section 31.1**.

“Force Majeure” has the meaning set forth in **Section 34.1**.

“Harmful Code” means any: (a) virus, trojan horse, worm, backdoor or other software or hardware devices the effect of which is to permit unauthorized access to, or to disable, erase, or otherwise harm, any computer, systems or software; or (b) time bomb, drop dead device, or other software or hardware device designed to disable a computer program automatically with the passage of time or under the positive control of any Person, or otherwise prevent, restrict or impede the State’s or any Authorized User’s use of such software.

“HIPAA” has the meaning set forth in **Section 19.1**.

“Implementation Fees” has the meaning set forth in **Section 16.2**.

“Implementation Plan” means the schedule included in the Statement of Work setting forth the sequence of events for the performance of Services under the Statement of Work, including the Milestones and Milestone Dates.

“Integration Testing” has the meaning set forth in **Section 12.1(c)**.

“Intellectual Property Rights” means all or any of the following: (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 associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works 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 the 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.

“License Agreement” has the meaning set forth in **Section 3**.

“License Fee” has the meaning set forth in **Section 16.1**.

“Loss or Losses” 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.

“Maintenance Release” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“Milestone” means an event or task described in the Implementation Plan under the Statement of Work that must be completed by the corresponding Milestone Date.

“Milestone Date” means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under the Statement of Work.

“New Version” means any new version of the Software that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“Nonconformity” or **“Nonconformities”** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

“Open-Source Components” means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

“Open-Source License” has the meaning set forth in **Section 4**.

“Operating Environment” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in the Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software and system architecture and configuration.

“Permitted Subcontractor” has the meaning set forth in **Section 9.4**.

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

“Pricing” means any and all fees, rates and prices payable under this Contract, including pursuant to any Schedule or Exhibit hereto.

“Pricing Schedule” means the schedule attached as **Schedule A, Attachment 2**, setting forth the License Fees, Implementation Fees, Support Services Fees, and any other fees, rates and prices payable under this Contract.

“Project Manager” is the individual appointed by each party to (a) monitor and coordinate the day-to-day activities of this Contract, and (b) for the State, to co-sign off on its notice of Acceptance for the Software. Each party's Project Manager will be identified in the Statement of Work.

“Representatives” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

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

“Services” means any of the services Contractor is required to or otherwise does provide under this Contract, the Statement of Work, the Maintenance and Support Schedule (if applicable), or the Service Level Agreement (if applicable).

“Service Level Agreement” means, if applicable, the service level agreement attached as **Schedule B** to this Contract, setting forth Contractor’s obligations with respect to the hosting, management and operation of the Software.

“Site” means the physical location designated by the State in, or in accordance with, this Contract or the Statement of Work for delivery and installation of the Software.

“Software” means Contractor’s software set forth in the Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract and the License Agreement.

“Source Code” means the human readable source code of the Software to which it relates, in the programming language in which the 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 Software.

“Specifications” means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, RFP or Contractor’s Bid Response, if any, for such Software, or elsewhere in the Statement of Work.

“State” means the State of Michigan.

“State Data” has the meaning set forth in **Section 19.1**.

“State Materials” means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“State Resources” has the meaning set forth in **Section 10.1(a)**.

“Statement of Work” means any statement of work entered into by the parties and attached as a schedule to this Contract. The initial Statement of Work is attached as **Schedule A**, and subsequent Statements of Work shall be sequentially identified and attached as Schedules A-1, A-2, A-3, etc.

“Stop Work Order” has the meaning set forth in **Section 26**.

“Support Services” means the software maintenance and support services Contractor is required to or otherwise does provide to the State under the Maintenance and Support Schedule (if applicable) or the Service Level Agreement (if applicable).

“Support Services Commencement Date” means, with respect to the Software, the date on which the Warranty Period for the Software expires or such other date as may be set forth in the Statement of Work.

“Support Services Fees” has the meaning set forth in **Section 16.3**.

“Technical Specification” means, with respect to any Software, the document setting forth the technical specifications for such Software and included in the Statement of Work.

“Term” has the meaning set forth in the preamble.

“Test Data” has the meaning set forth in **Section 11.2**.

“Test Estimates” has the meaning set forth in **Section 11.2**.

“Testing Period” has the meaning set forth in **Section 12.1(b)**.

“Third Party” means any Person other than the State or Contractor.

“Transition Period” has the meaning set forth in **Section 25.3**

“Transition Responsibilities” has the meaning set forth in **Section 25.3**.

“Unauthorized Removal” has the meaning set forth in **Section 9.3(b)**.

“Unauthorized Removal Credit” has the meaning set forth in **Section 9.3(c)**.

“User Data” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input.

“Warranty Period” means the ninety (90) calendar-day period commencing on the date of the State's Acceptance of the Software.

“Work Product” means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Statements of Work. Contractor shall provide Services and Deliverables pursuant to Statements of Work entered into under this Contract. No Statement of Work shall be effective unless signed by each party's Contract Administrator. The term of each Statement of Work shall commence on the parties' full execution of the Statement of Work and terminate when the parties have fully performed their obligations.

The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and attached as a schedule to this Contract. The State shall have the right to terminate such Statement of Work as set forth in **Section 25**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.1 Statement of Work Requirements. Each Statement of Work will include the following:

- (a) names and contact information for Contractor's Contract Administrator, Project Manager and Key Personnel;
- (b) names and contact information for the State's Contract Administrator, Project Manager and Business Owner;
- (c) a detailed description of the Services to be provided under this Contract, including any training obligations of Contractor;
- (d) a detailed description of the Software to be provided under this Contract, including the:
 - (i) version and release number of the Software;
 - (ii) Business Requirements Specification;
 - (iii) Technical Specification; and
 - (iv) a description of the Documentation to be provided;
- (e) an Implementation Plan, including all Milestones, the corresponding Milestone Dates and the parties' respective responsibilities under the Implementation Plan;
- (f) the due dates for payment of Fees and any invoicing requirements, including any Milestones on which any such Fees are conditioned, and such other information as the parties deem necessary;
- (g) disclosure of all Open-Source Components (each identified on a separate exhibit to the Statement of Work), in each case accompanied by such related documents as may be required by this Contract;
- (h) description of all liquidated damages associated with this Contract; and
- (i) a detailed description of all State Resources required to complete the Implementation Plan.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 2.2**.

- (a) As soon as reasonably practicable, and in any case within twenty (20) Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

- (i) a written description of the proposed Changes to any Services or Deliverables;
- (ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under the Statement of Work;
- (iii) any additional State Resources Contractor deems necessary to carry out such Changes; and
- (iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within thirty (30) Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to the Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within fifteen (15) Business Days following the State's response to a Change Proposal, the State may, in its discretion:

- (i) require Contractor to perform the Services under the Statement of Work without the Change;
- (ii) require Contractor to continue to negotiate a Change Notice;
- (iii) initiate a Dispute Resolution Procedure; or
- (iv) notwithstanding any provision to the contrary in the Statement of Work, terminate this Contract under **Section 25**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with the Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as

necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

3. Software License. Contractor hereby grants to the State and its Authorized Users the right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract.

4. Open-Source Licenses. Any use hereunder of Open-Source Components shall be governed by, and subject to, the terms and conditions of the applicable open-source license (“**Open-Source License**”). Contractor shall identify and describe in an exhibit to the Statement of Work each of the Approved Open-Source Components of the Software, and include an exhibit attaching all applicable Open-Source Software Licenses or identifying the URL where these licenses are publicly available.

5. Software Implementation.

5.1 Implementation. Contractor will deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in the Statement of Work.

5.2 Site Preparation. Unless otherwise set forth in the Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in the Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor’s delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

6. Hosting. If the Operating Environment for the Software is externally hosted by Contractor or a subcontractor, Contractor will maintain the Availability Requirement and the Support Service Level Requirement set forth in the Service Level Agreement attached as **Schedule B** to this Contract.

7. Support Services

7.1 Support Services for Externally Hosted Software. If the Operating Environment for the Software is externally hosted by Contractor or a subcontractor, Contractor shall provide the State with the Support Services described in the Service Level Agreement attached as **Schedule B** to this Contract. Such Support Services shall be provided:

(a) Free of charge during the Warranty Period, it being acknowledged and agreed that the License Fee includes full consideration for such Services during such period.

(b) Thereafter, for so long as the State elects to receive Support Services for the Software, in consideration of the State’s payment of Support Services Fees in accordance with **Section 16** and the rates set forth in the Pricing Schedule.

8. Data Privacy and Information Security.

8.1 Undertaking by Contractor. Without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of the State Data; (b) protect against any anticipated threats or hazards to the security or integrity of the State Data; (c) protect against unauthorized disclosure, access to, or use of the State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all Contractor Representatives comply with all of the foregoing. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable State IT policies and standards, which are available at http://www.michigan.gov/dtmb/0,4568,7-150-56355_56579_56755--00.html.

8.2 To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see http://michigan.gov/cybersecurity/0,1607,7-217-34395_34476--00.html. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

8.3 Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract. During the providing of Services, on an ongoing basis from time to time and without notice, the State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

8.4 Audit Findings. With respect to State Data, Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

8.5 State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or the Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8**.

8.6 Security Requirements for Externally Hosted Software. If the Operating Environment for the Software is externally hosted by Contractor or a subcontractor, Contractor shall comply with the security requirements set forth in **Schedule C** to this Contract.

9. Performance of Services. Contractor will provide all Services and Deliverables in a timely, professional and workmanlike manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement of Work.

9.1 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

- (i) ensure that such Contractor Personnel have the legal right to work in the United States;
- (ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and
- (iii) upon request, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel. 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 Contractor 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. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or Subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

9.2 Contractor's Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor's Project Manager, who will be considered Key Personnel of Contractor. Contractor's Project Manager will be identified in the Statement of Work.

- (a) Contractor's Project Manager must:
 - (i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;
 - (ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor's Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan, and will otherwise be available as set forth in the Statement of Work.

(c) Contractor will maintain the same Project Manager throughout the Term of this Contract, unless:

- (i) the State requests in writing the removal of Contractor's Project Manager;
- (ii) the State consents in writing to any removal requested by Contractor in writing;
- (iii) Contractor's Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Project Manager on the occurrence of any event set forth in **Section 9.2(c)**. Such replacement will be subject to the State's prior written approval.

9.3 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 25.1**.

(c) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 25.1**, Contractor will issue to the State an amount equal to \$25,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection (c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be

impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

9.4 Subcontractors. Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any Third Party to perform Services. The State's approval of any such Third Party (each approved Third Party, a "**Permitted Subcontractor**") does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such Permitted Subcontractor (including such Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, shall be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) name the State a third party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

10. State Obligations.

10.1 State Resources and Access. The State is responsible for:

(a) providing the State Materials and such other resources as may be specified in the Statement of Work (collectively, "**State Resources**"); and

(b) if the Software is internally hosted on State systems, providing Contractor Personnel with such access to the Site(s) and Operating Environment as is necessary for Contractor to perform its obligations on a timely basis as set forth in the Statement of Work.

10.2 State Project Manager. Throughout the Term of this Contract, the State will maintain a State employee to serve as the State's Project Manager under this Contract. The State's Project Manager will be identified in the Statement of Work. The State's Project Manager will be available as set forth in the Statement of Work.

11. Pre-Delivery Testing.

11.1 Testing By Contractor. Before delivering and installing the Software, Contractor must:

(a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Operating Environment;

(b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and

(c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.

11.2 Test Data and Estimates. Unless otherwise specified in the Statement of Work, Contractor shall provide to the State all test data and testing scripts used by Contractor for its pre-delivery testing (“**Test Data**”), together with the results Contractor expects to be achieved by processing the Test Data using the Software (“**Test Estimates**,” and together with Test Data, “**Contractor’s Test Package**”).

12. Acceptance Testing.

12.1 Acceptance Testing.

(a) Unless otherwise specified in the Statement of Work, upon installation of the Software, Acceptance Tests will be conducted as set forth in this **Section 12** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation. The State may, but is not obligated, to perform its own pretest on the Software utilizing Contractor’s Test Package. If the State does perform a pretest, and Contractor’s Test Package does not successfully pass the Test Data or Test Estimate scripts as described by Contractor, the State, at its discretion, is not obligated to move into the formal Acceptance Tests set forth in this Section. The State may elect to send Contractor’s Test Package back to Contractor to correct any problems encountered with the Test Data or Test Estimates.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in the Statement of Work, commence on the Business Day following installation of the Software and be conducted diligently for up to thirty (30) Business Days, or such other period as may be set forth in the Statement of Work (the “**Testing Period**”). Acceptance Tests will be conducted by the party responsible as set forth in the Statement of Work or, if the Statement of Work does not specify, the State, provided that:

- (i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and
- (ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

Contractor is solely responsible for all costs and expenses related to Contractor’s performance of, participation in, and observation of Acceptance Testing.

(c) Upon delivery and installation of any API, Configuration or Customization to the Software under the Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software (“**Integration Testing**”). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 12.1**, **Section 12.3**, and **Section 12.4**.

(d) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

12.2 Notices of Completion, Non-Conformities, and Acceptance. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 12.3** and **Section 12.4**.

(b) If such notice is provided by the State, is signed by the State's Business Owner and Project Manager, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have thirty (30) Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which the State will, as appropriate:

- (i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 12.3** and **Section 12.4**; or
- (ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State's Business Owner and Project Manager.

12.3 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Section 12.1(a)** or **Section 12.2(c)(i)**, identifying any Non-Conformities.

12.4 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 12**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and the Statement of Work and terminate this Contract for cause in accordance with **Section 25.1**.

12.5 Acceptance. Acceptance (“**Acceptance**”) of the Software (subject, where applicable, to the State’s right to Integration Testing) will occur on the date that is the earliest of the State’s delivery of a notice accepting the Software under **Section 12.2(b)**, or **Section 12.2(c)(ii)**.

13. Training. Contractor shall provide, at no additional charge, training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in the Statement of Work. Upon the State’s request, Contractor shall timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

14. Maintenance Releases; New Versions

14.1 Maintenance Releases. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

14.2 New Versions. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

14.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions. If the State wishes to install any Maintenance Release or New Version, the State shall have the right to have such Maintenance Release or New Version installed, in the State’s discretion, by Contractor or other authorized party as set forth in the Statement of Work. Contractor shall provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State. The State’s decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract.

15. Source Code Escrow

15.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release. If the parties do enter into an escrow agreement **Sections 15.2, 15.3, and 15.4** will apply:

15.2 Deposit. Within thirty (30) business days of the Effective Date, Contractor will deposit with the Escrow Agent, pursuant to the procedures of the escrow agreement, the source code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. Promptly after release of any update, upgrade, patch, bug fix, enhancement, new version, or other revision to the Software, Contractor will deposit updated source code, documentation, names, and contact information with the Escrow Agent. (“Deposit Material” refers to material required to be deposited pursuant to this **Section 15.2**.)

15.3 Verification. At State’s request and expense, the Escrow Agent may at any time verify the Deposit Material, including without limitation by compiling source code, comparing it to the Software, and reviewing the completeness and accuracy of any and all material. In the event that the Deposit Material does not conform to the requirements of **Section 15.2** above: (i) Contractor will promptly deposit conforming Deposit Material; and (ii) Contractor will pay the Escrow Agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this Section will constitute material breach of

this Contract, and no further payments will be due from the State until such breach is cured, in addition to such other remedies as the State may have.

15.4 License. Contractor hereby grants the State a license to use, reproduce, and create derivative works from the Deposit Material, provided the State may not distribute or sublicense the Deposit Material or make any use of it whatsoever except for such internal use as is necessary to maintain and support the Software. Copies of the Deposit Material created or transferred pursuant to this Contract are licensed, not sold, and the State receives no title to or ownership of any copy or of the Deposit Material itself. The Deposit Material constitutes Confidential Information of Contractor pursuant to **Section 20** of this Contract (provided no provision of **Section 20.5** calling for return of Confidential Information before termination of this Contract will apply to the Deposit Material).

16. Fees

16.1 License Fee. In consideration of, and as payment in full for, the rights and license to use the Software and Documentation as provided in this Contract and the License Agreement, the State shall pay to Contractor the license fees (the “**License Fee**”) set forth on the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract and the License Agreement, including the applicable timetable and other provisions of the Statement of Work and this **Section 16**.

16.2 Implementation Fees. In consideration of, and as payment in full for, Contractor’s provision of implementation services as provided in this Contract and the Statement of Work, the State shall pay to Contractor the implementation fees (the “**Implementation Fees**”) set forth on the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable timetable and other provisions of the Statement of Work and this **Section 16**.

16.3 Support Service Fees. In consideration of Contractor providing the Support Services as required under the Maintenance and Support Schedule (as applicable) or the Service Level Agreement (as applicable), the State shall pay to Contractor the Support Services fees (the “**Support Service Fees**”) set forth in the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable provisions of the Maintenance and Support Schedule (as applicable) or the Service Level Agreement (as applicable) and this **Section 16**.

16.4 Firm Pricing/Fee Changes. All Pricing set forth in this Contract is firm and will not be increased, except as otherwise expressly provided in this **Section 16.4**.

(a) The License Fee will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

17. Invoices and Payment.

17.1 Invoices. Contractor will invoice the State for Fees in accordance with the requirements set forth in the Statement of Work, including any requirements that condition the rendering of invoices and the payment of Fees upon the successful completion of Milestones. Contractor must submit each invoice in both hard copy and electronic format, via such delivery means and to such address as are specified by the State in the Statement of Work. Each separate invoice must:

(a) clearly identify the Contract and purchase order number to which it relates, in such manner as is required by the State;

(b) list each Fee item separately;

(c) include sufficient detail for each line item to enable the State to satisfy its accounting and charge-back requirements;

(d) for Fees determined on a time and materials basis, report details regarding the number of hours performed during the billing period, the skill or labor category for such Contractor Personnel and the applicable hourly billing rates;

(e) include such other information as may be required by the State as set forth in the Statement of Work; and

(f) Itemized invoices must be submitted to DTMB-Accounts-Payable@michigan.gov.

17.2 Payment. 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. The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment

17.3 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables 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.

17.4 Payment Disputes. The State may withhold from payment any and all payments and amounts the State disputes in good faith, pending resolution of such dispute, provided that the State:

(a) timely renders all payments and amounts that are not in dispute;

(b) notifies Contractor of the dispute prior to the due date for payment, specifying in such notice:

(i) the amount in dispute; and

(ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Contractor and resolution by the parties;

(c) works with Contractor in good faith to resolve the dispute promptly; and

(d) promptly pays any amount determined to be payable by resolution of the dispute.

Contractor shall not withhold any Services or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this **Section 17.4** or any dispute arising therefrom.

17.5 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

18. Intellectual Property Rights

18.1 Ownership Rights in Software

(a) Subject to the rights and licenses granted by Contractor in this Contract and the License Agreement, and the provisions of **Section 18.1(b)**:

- (i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and
- (ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(b) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

18.2 Rights in Open-Source Components. Ownership of all Intellectual Property Rights in Open-Source Components shall remain with the respective owners thereof, subject to the State's rights under the applicable Open-Source Licenses.

18.3 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all API and Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(a) Contractor will create all API and Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any API, Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

- (i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such API or Work Product, including all Intellectual Property Rights; and
- (ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the API or Work Product.

19. State Data.

19.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes: (a) User Data; and (b) any other data collected, used, processed, stored, or generated by the State 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; and (iii) CJI Data and (iv) metadata that may uniquely identifying user access devices or locations. 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 19.1** survives termination or expiration of this Contract.

19.2 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 must: (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 19.2** survives termination or expiration of this Contract.

19.3 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 must, 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; (h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and (i) 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, 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 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, must be reviewed and approved by the State in writing prior to its dissemination. The parties agree that any damages relating to a breach of this **Section 19.3** are to be considered direct damages and not consequential damages. This **Section 19.3** survives termination or expiration of this Contract.

19.4 State's Governance, Risk and Compliance (GRC) platform. Contractor is required to assist the State with its security accreditation process through the development, completion and ongoing updating of a system security plan using the State's automated GRC platform and implement any required safeguards or remediate any security vulnerabilities as identified by the results of the security accreditation process.

20. Confidential Information. Each party acknowledges that it may be exposed to or acquire communication or data of the other party that is confidential in nature and is not intended to be disclosed to third parties. This **Section 20** survives termination or expiration of this Contract.

20.1 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) should 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.

20.2 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 20.2**.

20.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must 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 must 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.

20.4 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.

20.5 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 must, 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 must destroy the Confidential Information and certify the same in writing within five (5) Business Days from the date of termination to the other party.

21. HIPAA Compliance. The State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.

22. 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. Contractor's Service Software must comply, where relevant, with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

23. CJIS Compliance. Contractor will comply with all Criminal Justice Information Services (CJIS) Security Policy requirements that are communicated to the Contractor in writing, including the FBI CJIS Security Addendum attached as **Schedule D**. Changes required to Contractor's performance due to a change in CJIS requirements will be subject to **Section 2.2 Change Control Process**.

Contractor personnel who will be subject to State performed background check, as determined by the State, will complete security awareness training within six (6) months of initial assignment and biennially thereafter. The State will provide Contractor with the required training materials. Documentation of completion of the training will be provided to the State upon request.

The State reserves the right to perform additional background checks on Contractor personnel as may be required to comply with the CJIS Security Policy.

During the term, Contractor will 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 23**. Contractor will make all such records, appropriate personnel, and relevant materials available in the event of an audit initiated by the State or the FBI.

Contractor will comply with all CJIS requirements for the Infrastructure Services Provider's data center including, if necessary, entering into an FBI CJIS Security Addendum or other required agreements with

its Infrastructure Services Provider on behalf of the State. Contractor will assist the State with entering into any other necessary agreements with the Infrastructure Services provider.

24. Tax Information Compliance. Contractor will comply with all IRS and State of Michigan Department of Treasury requirements if contractor will have access to or host tax information. These requirements include those stated in **Schedule E** and **Schedule F**.

25. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

25.1 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 25.1**, the State will issue a termination notice specifying whether Contractor must: (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 25.2**.

(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 must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Support Services Fees. Further, Contractor must 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.

25.2 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 must: (a) cease performance immediately, or (b) continue to perform in accordance with **Section 25.3**. 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.

25.3 Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, 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 Contract 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.

25.4 Survival. This **Section 25** survives termination or expiration of this Contract.

26. Stop Work Order. The State may, at any time, order the Services of Contractor fully or partially stopped for its own convenience for up to ninety (90) calendar days at no additional cost to the State. The State will provide Contractor a written notice detailing such suspension (a “**Stop Work Order**”). Contractor must comply with the Stop Work Order upon receipt. Within 90 days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate this Contract. The State will not pay for any Services, Contractor’s lost profits, or any additional compensation during a stop work period.

27. Contractor Representations and Warranties.

27.1 Authority. 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; and

(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.

27.2 Bid Response. Contractor represents and warrants to the State that:

(a) 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;

(b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor’s Bid Response, 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;

(c) 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; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

27.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(d) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable Law;

(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 to any third party;

(e) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software or Documentation as delivered or installed by Contractor does not or will not:

(i) infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable Law;

(f) as provided by Contractor, the Software does not or will not at any time during the license term contain any:

(i) Harmful Code; or

(ii) Open-Source Components or operate in such a way that it is developed or compiled with or linked to any Open-Source Components, other than Approved Open-Source Components specifically described in the Statement of Work.

(g) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(h) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(i) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation; and

(j) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

27.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

28. Indemnification

28.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any Third Party; and (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

28.2 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 must, 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 cost and 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 28**, must 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.

28.3 Infringement Remedies.

(a) The remedies set forth in this **Section 28.3** 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 for such actions.

(b) If any Software or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

- (i) procure for the State the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or

- (ii) modify or replace the materials that infringe or are alleged to infringe (“**Allegedly Infringing Materials**”) to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

(c) If neither of the foregoing is possible notwithstanding Contractor’s best efforts, 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 all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under the Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and
- (ii) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to six (6) months to allow the State to replace the affected features of the Software without disruption.

(d) If Contractor directs the State to cease using any Software under **subsection (c)**, the State may terminate this Contract for cause under **Section 25.1**.

(e) Contractor will have no liability for any claim of infringement arising solely from:

- (i) Contractor’s compliance with any designs, specifications, or instructions of the State; or
- (ii) modification of the Software by the State without the prior knowledge and approval of Contractor;

unless the claim arose against the Software independently of any of the above specified actions.

29. Liquidated Damages.

29.1 The parties agree that any delay or failure by Contractor to timely perform its obligations in accordance with the Implementation Plan and Milestone Dates agreed to by the parties will interfere with the proper and timely implementation of the Software, to the loss and damage of the State. Further, the State will incur major costs to perform the obligations that would have otherwise been performed by Contractor. The parties understand and agree that any liquidated damages Contractor must pay to the State as a result of such nonperformance are described in the Statement of Work, and that these amounts are reasonable estimates of the State’s damages in accordance with applicable Law.

29.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event if Contractor fails to timely perform its obligations by each Milestone Date.

29.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor’s breach of this Contract, including without limitation, the State’s right to terminate this Contract for cause under **Section 25.1**, and the State will be entitled in its discretion to recover actual damages caused by Contractor’s failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

29.4 Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

30. Damages Disclaimers and Limitations.

30.1 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.

30.2 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 PAYABLE UNDER THIS CONTRACT.

31. Records Maintenance, Inspection, Examination, and Audit.

31.1 Right of Audit. The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain, and provide to the State 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 four (4) 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, Contractor must retain the records until all issues are resolved.

31.2 Right of Inspection. Within ten (10) calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within forty-five (45) calendar days.

31.3 Application. This **Section 31** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

32. Insurance

32.1 Required Coverage.

(a) **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (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 a company with an A.M. Best rating of "A" or better and a financial size of VII or better.

| Insurance Type | Additional Requirements |
|--|--|
| Commercial General Liability Insurance | |
| <p><u>Minimal Limits:</u></p> <p>\$1,000,000 Each Occurrence Limit</p> <p>\$1,000,000 Personal & Advertising Injury Limit \$2,000,000 General Aggregate Limit</p> <p>\$1,000,000 Products/Completed Operations</p> <p><u>Deductible Maximum:</u></p> <p>\$50,000 Each Occurrence</p> | <p>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 2010 07 04 and CG 2037 07 0.</p> |
| Umbrella or Excess Liability Insurance | |
| <p><u>Minimal Limits:</u></p> <p>\$5,000,000 General Aggregate</p> | <p>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.</p> |
| Automobile Liability Insurance | |
| <p><u>Minimal Limits:</u></p> <p>\$1,000,000 Per Occurrence</p> | |
| Workers' Compensation Insurance | |
| <p><u>Minimal Limits:</u></p> <p>Coverage according to applicable laws governing work activities.</p> | <p>Waiver of subrogation, except where waiver is prohibited by law.</p> |
| Employers Liability Insurance | |
| <p><u>Minimal Limits:</u></p> <p>\$500,000 Each Accident</p> | |

| | |
|---|--|
| \$500,000 Each Employee by Disease | |
| \$500,000 Aggregate Disease. | |
| Privacy and Security Liability (Cyber Liability) Insurance | |
| <u>Minimal Limits:</u> \$1,000,000 Each Occurrence \$1,000,000 Annual Aggregate | Contractor must have their policy: (1) endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds; and (2) cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability. |

(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 claim-made coverage, the Contractor must: (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 must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

(d) Contractor must: (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.

32.2 Non-waiver. This **Section 32** 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).

33. Dispute Resolution.

33.1 Unless otherwise specified in the Statement of Work, the parties will endeavor to resolve any Contract dispute in accordance with **Section 33** (the “**Dispute Resolution Procedure**”). The initiating party will reduce its description of the dispute to writing (including all supporting documentation) and deliver it to the responding party's Project Manager. The responding party's Project Manager must respond in writing within five (5) Business Days. The initiating party has five (5) Business Days to review

the response. If after such review resolution cannot be reached, both parties will have an additional five (5) Business Days to negotiate in good faith to resolve the dispute. If the dispute cannot be resolved within a total of fifteen (15) Business Days, the parties must submit the dispute to the parties' Contract Administrators. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

33.2 Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' Contract Administrators, and either Contract Administrator concludes that resolution is unlikely, or fails to respond within fifteen (15) Business Days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This **Section 33** does not limit the State's right to terminate this Contract.

34. Administrative Fee and Reporting

34.1 Contractor must pay an administrative fee of 1.5% on all payments made to Contractor under the MiDEAL program, and for other state use (including governmental subdivisions and authorized entities).

Administrative fee payments must be made online by check or credit card at the following links:

State of MI Admin Fee: <https://www.thepayplace.com/mi/dtmb/adminfee> and State of MI MiDEAL Fees: <https://www.thepayplace.com/mi/dtmb/midealfee>.

34.2 Contractor must submit an itemized purchasing activity report, which includes at minimum, the name of the purchasing entity and the total dollar volume in sales. Report should be emailed 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.

35. Extended Purchasing Program.

35.1 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.

35.2 Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

35.3 If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

35.4 Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

Email: sstickler@novinzio.com

Attention: Sam Stickler, VP of Sales and Technical Services

If to State: State of Michigan

525 W/ Allegan, 1st floor

Lansing, MI 48913

Email: BreenM@michigan.gov

Attention: Mike Breen, Category Specialist, IT

Notices sent in accordance with this **Section 34.5** 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.

36.6 Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

36.7 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 25.1**, 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 34.7** is void.

36.8 No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. 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.

36.9 Amendment and Modification; Waiver. No amendment to or modification of this Contract is effective unless it is in writing, identified as an amendment to this Contract and signed by both parties Contract Administrator. Further, certain amendments to this Contract may require State Administrative Board Approval. No waiver by any party of any of the provisions of this Contract will be 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. Nor will any single or partial exercise of any right, remedy, power or privilege under this Contract preclude the exercise of any other right, remedy, power or privilege.

36.10 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.

36.11 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 must be resolved in the Michigan Court of Claims. Complaints against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or forum non conveniens. Contractor must appoint agents in Michigan to receive service of process.

36.12 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 may 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 34.12**.

36.13 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](#). 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 (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. Breach of this covenant is a material breach of this Contract.

36.14 Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

36.15 Schedules All Schedules that are referenced herein and attached hereto are hereby incorporated by reference.

36.16 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.

36.17 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 all Software and Deliverables are 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**”). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar Laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate shall become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor’s rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State’s possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

36.18 Compliance with Laws. Contractor and its Representatives must comply with all Laws in connection with this Contract.

36.19 Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

36.20 Entire Agreement. This Contract, together with all Schedules, Exhibits, and the Statement of Work 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, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Contract, the Schedules, Exhibits, and the Statement of Work, the following order of precedence governs: (a) first, this Contract, excluding its Exhibits and Schedules, and the Statement of Work; and (b) second, the Statement of Work as of the Effective Date; and (c) third, the Exhibits and Schedules to this Contract as of the Effective Date. NO TERMS ON CONTRACTORS INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH 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.

Schedule A - Project Scope

1. *PURPOSE*

This Contract shall provide an Enterprise eSignature Solution owned and managed by DTMB Records Management Services. DTMB-RMS is the primary contact for agencies using the service and the Contractor awarded this contract. As the service owner, DTMB-RMS will perform the business analysis, recommendation for implementation, system administration, ongoing maintenance and support related to State agencies activities, service rate management, and billing. The Contractor shall not work directly with State agencies on eSignature projects, unless requested in writing by DTMB-RMS.

The Contractor must train Records Management Services (RMS) as the selected State Solution owner to administer and use the software. This will allow RMS to provide the Solution services required to guide and train State agencies in the use of the Solution.

This Solution is a discretionary service for State agencies. It is supported by billing the agencies based on their actual use of the service.

The Enterprise eSignature Solution shall offer features that can help facilitate direct and indirect cost savings for both the agency and their customers, including:

- Bulk export capabilities that allow documents and metadata to be moved to State of Michigan repositories for storage, collaboration and retention purposes (IBM FileNet, Microfocus Content Manager and others);
- Workflow automation;
- Integrate with the State's MILogin platform;
- Audit trail capabilities that track documents through every step of the signing process; and
- The ability to embed signing into line-of-business applications and provide a documented Software Development Kit (SDK).

2. *SPECIFIC STANDARDS*

The Contractor shall comply with all Federal and State laws, policies, and regulations regarding the use of computers, IT services, and the dissemination of information obtained from their use, along with any other applicable federal or State privacy and/or confidentiality laws, policies, and regulations. These include, but are not limited to:

- Must remain compliant with the Center for Medicare and Medicaid Services (CMS) Policies.
- Must sign the FBI Criminal Justice Information Services (CJIS) Security Addendum and maintain compliance with such document.
- Must remain compliant with the Internal Revenue Service (IRS) Policies.
- Must remain compliant with the Health Insurance Portability and Accountability Act (HIPAA) Policies.
- Must remain compliant with the Family Educational Rights and Privacy Act (FERPA) Policies.
- Must remain compliant with the Credit Card Holder information (PCI) Policies.

IT Policies, Standards and Procedures (PSP)

All services and products provided by Contractor must comply with all applicable State IT policies and standards as stated herein.

- Public IT Policies, Standards and Procedures (PSP): https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html
- Controlled IT Policies, Standards and Procedures (PSP): Controlled PSP's applicable to this Solution, which are not publicly available, have been provided to Contractor subject to the terms of an executed Nondisclosure Agreement (NDA) agreement.

Acceptable Use Policy

To the extent that Contractor has access to the State’s computer system, Contractor must comply with the State’s Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State’s Acceptable Use Policy before accessing the State’s system. The State reserves the right to terminate Contractor’s access to the State’s system if a violation occurs.

Look and Feel Standard

All software items provided by the Contractor must adhere to the State of Michigan Application/Site standards which can be found at www.michigan.gov/standards.

Mobile Responsiveness

Contractor’s Solution must utilize responsive design practices to ensure the application is accessible via a mobile device.

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. Contractor’s Solution, where relevant, must comply with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. 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. The State may require Contractor to complete a Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document for the proposed Solution.

http://www.michigan.gov/documents/dmb/1650.00_209567_7.pdf?20151026134621

3. USER TYPE AND CAPACITY

The Solution must meet the expected number of total and concurrent Users below.

| Type of User | Access Type | Number of Users | Number of Concurrent Users |
|-----------------------|--------------|-----------------|----------------------------|
| Trusted Third Parties | Write Access | 2,000 | 200 |
| State Employees | Admin Access | 55,000 | 500 |
| Public Citizens | Write Access | 9,960,000 | 25,000 |

*4. ACCESS CONTROL AND AUDIT***Identity Federation/Single Sign-On (SSO)**

The Solution must be configured to support integration with MilLogin, the State standard federated SSO for end user access. The solution must support SAML2 authentication and be available for use with both senders and signers.

Web-based Capabilities to Manage Users and Data

The Solution must provide various user management functions including registration, profile setup, permission setup/assignment along with specific approval workflow processes to maintain compliance with segregation of duties mandated policies. Supporting administration screens allows managing data setup and controlling permissions at data level (like program, county etc.).

The Solution must include the ability for both administrators and users. The administrators define and control the use and rights of the users as provided within the software's configuration options. RMS will perform the administrator function for all State of Michigan eSignature accounts.

Audit Logging and Access Management

The Solution must be designed on a point-in-time versioning data model and must create an audit trail for all actions performed. Users with appropriate permissions will have access to this data and will be able to review it in real time on the same web application without having to parse through application logs.

Note: The standard logging of actions to application logs will be enabled for related maintenance support or special audit needs.

5. DATA RETENTION

The solution must provide the ability for account administrators to obtain a list of signed documents and download them so they can be delivered to any agencies who have not performed their own downloads. The agency will then place them in their business repository to apply retention and disposal. The solution must allow the account administrators to identify and delete documents (signed or abandoned) from the hosted solution.

6. SECURITY

Contractor's solution must comply with the following:

- Must provide a Solution that is hosted in a FedRAMP authorized computing environment and maintain FedRAMP authorization for the solution provided.
- Must be encrypted in transit and at rest using encryption modules with 256 bit or higher keys, managed in compliance with FIPS/NIST published documentation.
- Must be encrypted in transit and at rest using currently validated encryption modules in accordance with FIPS PUB 140-2 (as amended), Security Requirements for Cryptographic Modules.
- Must remain compliant with FISMA and the NIST Special Publication 800.53 (most recent version) HIGH controls using minimum control values as established in the applicable SOM PSP's.

Secure Web Application Security Standard

Contractor's solution must meet the State's Secure Application Development Standards as mandated by the State.

Secure Application Development Life Cycle (SADLC)

Contractor is required to meet the States Secure Application Development Life Cycle requirements that include:

Security Accreditation

Contractor is required to complete the State Security Accreditation process for the solution.

Application Scanning

Contractor is required to grant the right to the State to scan either the application code or a deployed version of the solution; or in lieu of the State performing a scan, Contractor must provide the State a vulnerabilities assessment after Contractor has used a State approved application scanning tool. These scans must be completed and provided to the State on a regular basis or at least for each major release.

For COTS or Contractor owned applications, Contractor, at its sole expense, must provide resources to complete the scanning and to complete the analysis, remediation and validation of vulnerabilities identified by the scan as required by the State Secure Web Application Standards.

Types of scanning and remediation may include the following types of scans and activities

Application scanning and remediation must include the following types of scans and activities

- Dynamic Application Security Testing (DAST) - Scanning interactive application for vulnerabilities, analysis, remediation and validation (May include IAST)
- Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation and validation

Application scanning and remediation may include the following types of scans and activities as required based on data classification and/or composition

- Software Composition Analysis (SCA) - Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation and validation
- Native mobile application software scanning (if applicable) including any interaction with an Application Programming Interface (API)
- Penetration Testing - Simulated attack on the application and infrastructure to identify security weaknesses

Infrastructure Scanning

A Contractor providing Hosted Services must scan the infrastructure using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least once every 30 days and provide the scan's assessment to the State in a format that can be uploaded by the State and used to track the remediation. Remediation time frame requirements are documented in SOM PSP's.

7. END USER OPERATING ENVIRONMENT

Contractor must support the current and future State standard environment at no additional cost to the State. The current SOM environment is X86 VMware, IBM Power VM and Oracle VM, with supporting enterprise storage monitoring and management. Future changes to the user-operating environment (limited to installed browser versions) must be accommodated as follows:

- Browser upgrades that are backward compatible but resulting in minor application issues must be fixed and resolved as part of the on-going maintenance contract
- Major browser upgrades adopted through software end of life transition policies due to backward compatibility changes to ECMAScript must be resolved as part of the ongoing support contract

Development teams must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers and the state standard browser without the use of special plugins or extensions. The rules used to base the minimum browser requirements include:

- Over 2% of site traffic, measured using Sessions or Visitors (or)
- The current browser identified and approved as the State of Michigan standard

This information can be found at www.michigan.gov/browserstats. Please use the most recent calendar quarter to determine browser statistics. For those browsers with over 2% of site traffic, except Internet Explorer which requires support for at minimum version 11, the current browser version as well as the previous two major versions must be supported.

8. SOFTWARE

Contractor must provide an eSignature solution that is configured to DTMB Records Management Services (RMS) specific needs. The Solution must meet the specifications detailed in Exhibit A-1 – Business Specifications in the manner described therein.

9. SOLUTION REQUIREMENTS

The Solution must meet the specifications detailed in **Exhibit A-1 – Business Specifications** in the manner described therein.

10. INTEGRATION

Integrations will be performed with MiLogin and the eSignature solutions API.

11. MIGRATION

There are no migration services needed at the time of Contract execution., However, the State may require migration services in the future and these services would be added to the Contract through a Contract Change Notice.

12. TESTING Services and acceptance

Contractor agrees to **Section 11. Pre-Delivery Testing and Section 12. Acceptance Testing, of the Software Contract Terms.**

13. TRAINING SERVICES

State of Michigan Records Management Services solution administrators must be trained by Contractor via web application. The training provided will enable the administrators to train other state personnel.

The Enterprise Launch Program detailed below includes the following and is included within the SUITE/Keylight and other misc project documentation deliverable;

- One (1) week onsite
- Standard SAML integration only
- One (1) DKIM Integration
- API requirement definition and high-level design only - development is a separate cost.

| Novinzio - OneSpan Enterprise Launch Program | | | |
|--|---|--|--|
| This program includes tasks and activities designed to establish a methodology and the foundation for an enterprise rollout of the OneSpan Sign™ electronic signature platform. This work will be done on a number of Use Case examples selected by RMS that fit within the number of hours Novinzio has scoped for the training process. It is expected that RMS will be trained and perform some of the work on the Use Cases as part of the exercise. | | | |
| Task | Activities | Deliverables | Acceptance Criteria |
| 1: Assist with the RMS Shared Services Enterprise Rollout Methodology utilizing E-Signature Best Practices Consulting session to better understand the needs of the RMS. | Contractor must provide consulting services to: <ul style="list-style-type: none"> • Review defined RMS business requirements & enterprise setup. • Provide best practices to fully leverage the OneSpan Sign SaaS platform. • Outline the e-Signature process lifecycle requirements, from signer | Completed consulting engagement with sufficient knowledge transfer to inform the participating technical staff and other participants to successfully understand and support the solution. This is largely a training deliverable with input from RMS staff. | RMS staff will participate in the consulting engagement and the overall work product/training will be evaluated and accepted upon the conclusion of the consulting session. The RMS retains the right to request additional advice, clarification, or input from the Contractor to ensure that the |

| | | | |
|--|---|--|---|
| | <p>authentication to automated signed document retrieval.</p> <ul style="list-style-type: none"> • Prepare for and conduct Kick-Off Meeting. | | <p>participants are fully trained.</p> |
| <p>2: Define and Provision OneSpan Sign production accounts for use by RMS and participating agencies.</p> | <p>Contractor must deliver OneSpan Sign signature transactions into the production OneSpan Sign application, ready for RMS use.</p> <p>Contractor and OneSpan works with RMS to define the SOM account setup for those agencies that plan on coming onboard.</p> | <p>Agreed Upon OneSpan Sign signature transactions, fully functional and ready for use by Snohomish RMS.</p> | <p>Visual confirmation that the production account identifies that the desired number of transactions have been provisioned to this account. Visual confirmation that all Accounts are set up and accessible by the users assigned to those accounts.</p> |
| <p>3: Plan and complete one Project Solution Requirements Workshop Training session.</p> <p>This task defines the “As Is” and “To Be” requirements for the signature processes.</p> | <p>Contractor must schedule and complete one Project Solution Requirements Workshop Training with key stakeholders and RMS technical resources. Key to this task is a walk-through of the Requirements Gathering Survey that is a line of questioning used to define the requirements for each document/process being proposed for the creation of an electronic signature workflow. The requirements gathering workshop defines the following items for each workflow:</p> <ul style="list-style-type: none"> • Initiation • Authentication (SAML) | <ul style="list-style-type: none"> • “As Is” Requirements Definition Document • “As Is” Flow Diagram | <p>RMS staff will participate in the Workshop and the overall work product/training will be evaluated and accepted upon the conclusion of the Workshop. RMS retains the right to request additional advice, clarification, or input from Contractor to ensure that workflows and staff training are sufficient for overall project success.</p> |

| | | | |
|---|---|--|--|
| | <ul style="list-style-type: none"> • Transaction Configuration • Workflow • Data Capture • Branding • Integration (Email-DKIM and others) • Archival | | |
| <p>4: Design “To Be” Signature Process</p> <p>This task takes the requirements defined in Task 3 and creates a design for the “To Be” signature process.</p> | <p>Contractor must work with RMS to take each requirement and align it with the available OneSpan Sign™ functionality to meet that requirement.</p> | <ul style="list-style-type: none"> • “To Be” Design Document • “To Be” Flow Diagram • System Test Plan including <ul style="list-style-type: none"> ○ SAML ○ Email Integration ○ Branding and Custom Messaging. | <p>RMS staff will confirm the completion of this task.</p> |
| <p>5: Create single sign-on configuration (using SAML integration) to provide single sign-on capability for Authorized Users</p> | <p>Contractor must work with RMS to configure the OneSpan Sign production environment by delegating authentication to the RMS organization’s Security Assertion Markup Language (SAML) provider to utilize single sign-On capability.</p> | <p>Single Sign-on (SAML) environment integration with OneSpan Sign production environment tested and fully functional.</p> | <p>RMS staff will test single sign-on functionality using the System Test Plan with acceptance based upon the recorded results and the determination that the integration is fully functional.</p> |
| <p>6: Complete one OneSpan Sign messaging and account branding/customization consulting session.</p> <p>The purpose of this task is to convert the default OneSpan Sign site/interface to a personalized RMS site/interface.</p> | <p>OneSpan to configure all defines branding and email messaging modifications</p> | <p>Validation that all branding and custom message are in place.</p> | <p>RMS staff will test branding and email messaging using the System Test Plan with acceptance based upon the recorded results and the determination that the</p> |

| | | | |
|---|---|--|--|
| | | | integration is fully functional. |
| 7: Configure DKIM/SMTP relay email integration between the RMS email environment and the OneSpan Sign production environment. | OneSpan Sign™ to configures DKIM/SMTP relay | Configuration of RMS email environment (if available) to ensure necessary mail functionality through OneSpan Sign. | RMS staff will test email integration using the System Test Plan with acceptance based upon the recorded results and the determination that the integration is fully functional. |
| Task 8: Signature Workflow Creation This task focuses on the actual configuration of the up to 6 workflows defined in Task 3. | Contractor must plan for and create up to 6 signature workflows (specified by the RMS). The workflows will be migrated into the production OneSpan Sign environment as a result of this task. | <ul style="list-style-type: none"> • Up to 6 completed signature workflows. • Completes System Test Plan. • User Acceptance Test Plan. • All accepted workflows implemented into the final OneSpan Sign application with all functionality tested and shown to be fully functional | RMS staff will test all functionality as integrated into OneSpan Sign application and acceptance is based on the successful functional testing of the workflows. |
| Task 8: Plan for and complete User Acceptance training and testing | Contractor must conduct an online training session for designated RMS testers to understand and complete the UAT Plan. | Completed UAT Plan and Results | The training will be accepted upon the successful completion of the four training sessions. |
| Task 9: Plan for and complete end user training with two sessions for (up to) 10 end users each. | Contractor must create a Training plan that outlines the execution of two (2) online training sessions with designated RMS staff, to be delivered. | <ul style="list-style-type: none"> • Training Plan • Training Guide | Training will be accepted by the RMS staff after delivery. |

14. HOSTING

The solution is externally hosted.

Contractor must conform to the State's standard **Service Level Agreement (SLA) attached as Schedule B** to the Software Contract Terms.

15. SUPPORT AND OPERATIONS

Support-Hours

The State requires the Contractor to provide Support Hours as 8 a.m. to 5 p.m. Eastern, Monday thru Friday via phone, email, and chat. The State requires the Contractor to assign a customer support resource during on-boarding.

16. DOCUMENTATION

Contractor must provide access to 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.

Contractor must develop and submit for State approval complete, accurate, and timely Solution documentation to support all users, and must update any discrepancies, or errors through the life of the contract.

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.

17. TRANSITION SERVICES

Upon termination or expiration of the agreement, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days unless otherwise agreed to be the parties)(the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the agreement 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 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 (in a format specified by the State) to the State all data stored in the solution; and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

Contractor must provide a detailed transition-in and transition-out project plan, including any roles or responsibilities expected of the State. The plan must adequately demonstrate the steps to migrate between Contractor's Solution and third-party Solutions.

18. PRODUCTS AND SERVICES

Contractor must describe additional Solution functionality, products or services that the State specifications do not address but are necessary to implement and support this solution.

19. CONTRACTOR KEY PERSONNEL

Contractor must identify all Contractor resources and responsibilities required for the successful implementation and ongoing support of the Solution.

Contractor Contract Administrator. Contractor must identify the individual appointed by it to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

| |
|---|
| Contractor Novinzio |
| Name Sam Stickler |
| Address 132A North Euclid Avenue |
| Phone 818-876-2983 |
| Email sstickler@novinzio.com |

Contractor Project Manager. Contractor must identify the Contractor Project Manager who will 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.

| |
|--|
| Contractor Novinzio |
| Name Sam Stickler Address 1425 Clayton Ave, Simi Valley, CA Phone 818-876-2983 Email sstickler@novinzio.com |

Contractor Service Manager. Contractor to provide name of individual to serve as 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.

| |
|---|
| Contractor OneSpan |
| Name David Hemens Address 8200 Decarie Blvd, Mtl, Qc, H4P-2P5 Phone 514-616-0427 Email dhemens@onespan.com |

Contractor Security Officer. Contractor to provide name of individual to respond to State inquiries regarding the security of the Contractor's systems. This person must have sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto.

| |
|--|
| Contractor OneSpan |
| Name Christian Vezina Address 8200 Decarie Blvd, Mtl, Qc, H4P-2P5 Phone 1 514 337 5255 x. 1124 Email Christian.vezina@onespan.com |

20. CONTRACTOR PERSONNEL REQUIREMENTS

Contractor must present certifications evidencing satisfactory Michigan State Police Background checks ICHAT and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

21. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation 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 Project Manager. The State Project Manager will serve as the primary contact with regard to implementation Services who will have the authority to act on behalf of the for tracking and scheduling day to day activities.

Agency Business Owner. The Agency Business Owner will serve as the primary contact for the business area with regard to business advisement who will have the authority to act on behalf of the State in matters pertaining to the business Specifications and approving Deliverables.

State Technical Lead. The State Technical Lead will serve as the primary contact with regard to implementation technical advisement.

22. MEETINGS

Contractor must attend the following meetings at no additional cost to the State.

At start of the engagement, the Contractor Project Manager must attend a project kick off meeting with the support from the State's Project Manager and the identified State resources. The State Project Manager will review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, the State Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, the State Project Manager must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

23. PROJECT REPORTS

Once the Project Kick-Off meeting has occurred, the State Project Manager will monitor project implementation progress and report on a weekly basis to the Contractor's Project Manager and the State project team the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified

The above Report metrics are very consistent with those have as part of our Status Meeting Agenda and Report.

The following items are tracked on the Status Report;

- Overall Health Status of project (Green, Yellow, Red)
- Dashboard view of project(s) in progress across Stages/Milestones and % completed
- Progress Overview
- Goals Accomplished in Previous Period
- Goals for Next Period
- Project Issues
- Tasks Affecting Critical Path
- Project Risks

The frequency of the meetings during an ongoing project should be weekly, mostly to keep the momentum moving forward and maintaining a strong line of communication.

In addition to the Status Meeting Report, Notes are taken as part of every conversation or meeting and when action items are identified they are captured on an Action Log and distributed to all members of both teams. Action Items are discussed in the status meetings as well.

24. MILESTONES AND DELIVERABLES

The State’s proposed milestone schedule and associated deliverables are set forth below.

| Milestone Event | Associated Milestone Deliverable(s) | Schedule |
|--|--|------------------------------|
| Project Planning | Project Kickoff | Contract Execution + 10 days |
| MILogin Integration | Start of MILogin Integration | Execution + 1 days |
| Requirements and Design Validation | Validation sessions, Final Requirement Validation Document, Final Design Document, Final Implementation Document | Execution + 30 days |
| Provision environments | Validate Test and Production environments | Execution + 1-3 days |
| MILogin Integration | Development of MILogin Integration | Execution + 1-2 days |
| Installation and Configuration of software | Final Solution and Testing Document | Execution + 1 day |
| Testing and Acceptance | Final Test Results Report, Final Training Documentation, Final Acceptance | Execution + 15 - 20 days |
| Post Production Warranty | Maintenance and Support (free of charge) | Production + 90 days |
| Production Support Services | Ongoing after Final Acceptance. | Ongoing |

Table 1-SOM Project Milestones

The SOM Project Manager will be responsible for keeping a MS Project Plan to track the project progress and direct project resources since this is a hosted SaaS solution.

The SUITE documentation will be developed by SOM resources with input from the contractor as needed. The contractor will be required to provide the OSS FedRamp SSP, a current SOC 2 Type II report, and provide input to the State’s security assessment processes as needed.

25. PRICING

Appendix C - Pricing is a detailed description of all costs associated with implementing, maintaining and supporting the Solution.

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

Travel and Expenses

The State does not pay for overtime or travel expenses.

26. ADDITIONAL INFORMATION

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

STATE OF MICHIGAN

Contract No. 19000000####

Schedule A, Attachment 1 - Business Specifications Worksheet

| A | B |
|-------------------------------|--|
| Business Specification Number | Business Specification |
| MANDATORY MINIMUM | |
| 1.0 | The Contractor must have three (3) recent years of experience providing the proposed solution to other government entities |
| 2.0 | A Contractor that will be submitting a cloud-based solution must be FedRAMP authorized. |
| REQUIRED | GENERAL REQUIREMENTS |
| 1.0 | The system shall have the ability for any transaction to include one or more documents |
| 2.0 | The system shall have the ability for not all documents in the transaction to require a signature |
| 3.0 | The system shall have the ability to apply templates/forms to documents to ensure a consistent execution of the transactions |
| 4.0 | The system shall have the ability to include multiple signers into a single transaction |
| 5.0 | The system shall allow signing order to be sequential or in parallel |
| 6.0 | The system shall allow a combination of serial and parallel signing in a single workflow signing transaction |
| REQUIRED | TRANSACTION RECIPIENTS ROLES: |
| 7.0 | The system shall have the ability to require a recipient to sign the document |
| 8.0 | The system shall allow the signature to be “generated” and accepted by the signer as theirs |
| 9.0 | The system shall allow the signer to draw their signature |
| 10.0 | The system shall allow for in person signing |

| A | B |
|--------------------------------------|---|
| Business Specification Number | Business Specification |
| 11.0 | The system shall allow for transaction recipients to receive a copy of transactions without requiring them to be signers |
| 12.0 | The system shall allow the recipients list to be modified by selected signers |
| 13.0 | The system shall allow signing to be delegated to alternate signers |
| 14.0 | The system shall allow a single signer from a group to sign on the group's behalf |
| 15.0 | In some cases, a signer may be required to use the signature of someone else that they have been designated to sign on behalf of. The system shall be able to support and maintain security controls. |
| 16.0 | The Contractor system should be able to be managed when you have to sign for multiple other people using their name |
| 17.0 | The system shall allow for Notary Public "signing" of documents |
| 18.0 | The system shall allow for "Approve" and "Reject" type signing options for when approval is required, but a signature is not required |
| 19.0 | The system shall allow custom fields for transaction recipients |
| 20.0 | The system shall allow customization of email title and content for transactions |
| 21.0 | The system shall have ability to schedule reminder emails for unsigned documents to signers |
| 22.0 | The system shall have ability to cancel inflight envelopes |
| 23.0 | The system shall have ability to provide edit/annotate capabilities for inflight signing. Describe the impact on prior signers |
| REQUIRED | TEMPLATES/FORMS |
| 24.0 | The system shall have ability to save transaction settings as part of a template/form |
| 25.0 | The system shall have ability to have roll-based security to allow template/form to use or modification of templates/forms options |
| 26.0 | The system shall have ability to share templates/forms with other users within your group |
| 27.0 | The system shall allow templates/forms to enforce the signer security requirements (e.g. require second factor authentication) |
| REQUIRED | ROLE BASED SECURITY |

| A | B |
|--------------------------------------|--|
| Business Specification Number | Business Specification |
| 28.0 | The system shall allow role-based security, multiple levels of administration including overall account administration and the ability to delegate the administration to subgroups of users |
| 29.0 | The system shall enable user accounts be managed via MILogin and/or the application |
| 30.0 | The system shall have the ability to have users accounts be limited to the roles of either sender or signer |
| 31.0 | The system shall have the ability to have Users be grouped for security and sharing purposes with the ability to assign one or more group administrators |
| 32.0 | The system shall have the ability to have Users who are signers only be automatically provisioned using a standard security template. This feature's goal is to limit the creation and management of signer only user accounts |
| 33.0 | The system shall have the ability to prevent unauthorized signatures by accidental email forwarding instead of signature delegation |
| 34.0 | The system shall have the ability to Support authentication Options based on NIST 800-63 for Senders |
| 35.0 | The system shall authenticator Assurance Level (AAL) 1 Support |
| 36.0 | The system shall authenticator Assurance Level (AAL) 2 Support |
| 37.0 | The system shall authenticator Assurance Level (AAL) 3 Support |
| 38.0 | The system shall support the Authentication Options based on NIST 800-63 for Signers |
| 39.0 | The system shall have an authenticator Assurance Level (AAL) 1 Support |
| 40.0 | The system shall have an authenticator Assurance Level (AAL) 2 Support |
| 41.0 | The system shall have an authenticator Assurance Level (AAL) 3 Support |
| REQUIRED | DOCUMENT MARKUP OPTIONS |
| 42.0 | The system shall allow a signee signature block to be placed on documents requiring signing |
| 43.0 | The system shall allow a signee initial block to be placed on documents requiring initialing |
| 44.0 | The system shall allow a title field to be placed on documents |
| 45.0 | The system shall allows a company field to be placed on documents |

| A | B |
|-------------------------------|---|
| Business Specification Number | Business Specification |
| 46.0 | The system shall allow a date field to be placed on documents |
| 47.0 | The system shall allow a name field to be placed on documents |
| 48.0 | The system shall allow an email field to be placed on documents |
| 49.0 | The system shall allow a Text Field to be placed on the document for text entry |
| 50.0 | The system shall allow the automatic placing of fields on documents based on specific text. This feature will automate repeating processes and repetitive placement of items |
| 51.0 | The system shall provide the ability to include fields that include mathematical formulas, which may include calculations based on other fields placed on the document |
| 52.0 | The system shall allow selection between two or more options using radio buttons |
| 53.0 | The system shall allow selection between multiple items using dropdown fields |
| 54.0 | The system shall allow conditional fields that appear or are disabled/enabled based on the selection of other items (e.g. radio buttons, dropdowns, etc.) |
| 55.0 | The system shall allow the signer to add/upload attachments to the signing transaction. Please include the limitations on the size and number of attachments that are allowed |
| 56.0 | The system shall allow collaboration features that allow ad hoc type notes by signers Describe the impact on prior signers |
| 57.0 | The system shall allow validation of text field content |
| 58.0 | The system shall allow text values to be placed on the documents as "hidden" |
| 59.0 | The system shall allow labels to be placed on documents as necessary |
| 60.0 | The system shall allow Document Recognition to enable for automating signature block locations |
| 61.0 | The system shall allow notes to be added to letters |
| 62.0 | The system shall allow approve/deny on documents for acceptance when a signature is not required |
| 63.0 | The system shall allow notes during the signature process like an annotation (as either private or shared with all signers) |

| A | B |
|--------------------------------------|---|
| Business Specification Number | Business Specification |
| 64.0 | The system shall allow form input validation for values (e.g. dates) |
| 65.0 | The system shall allow for additional attachments to be added during the signing process |
| REQUIRED | SENDING OPTIONS |
| 66.0 | The system shall allow one of a group of people to sign a document |
| 67.0 | The system shall allow a list of signers to be imported for bulk signing of documents |
| 68.0 | The system shall allow the visibility of some documents to other signers can be controlled |
| 69.0 | The system shall allow automation using workflow during the eSignature process |
| 70.0 | The system shall have ability for users (with administratively granted permissions) to assign signatories in later steps of the signing process |
| 71.0 | During the signing process, if someone in the process fails to sign, the system shall allow the sender to determine who receives the notice of failure to sign so action can be taken |
| REQUIRED | REPORTING |
| 72.0 | The system shall for out of the box reports |
| 73.0 | The system shall be able to total the initiated transactions |
| 74.0 | The system shall be able to total the completed transactions |
| 75.0 | The system shall be able to provide a summary of user activity |
| 76.0 | The system shall have the ability to create custom reports |
| 77.0 | Reports can be generated and managed at both the account administrator and group administrator levels |
| REQUIRED | MISC. PRODUCT FEATURES |
| 78.0 | The system shall have the ability to schedule report execution and delivery via email |
| 79.0 | The system shall have bulk transaction capabilities for large volume distributions |
| 80.0 | The system shall have bulk retrieval of completed documents using an out-of-the-box application |

| A | B |
|--------------------------------------|---|
| Business Specification Number | Business Specification |
| 81.0 | The system shall have the ability of the account administrator to retrieve completed documents for all users |
| 82.0 | The system shall have bulk transfer log of transferred documents |
| 83.0 | The system shall have certification of completion to ensure the authenticity and completeness of the transaction |
| 84.0 | The ability to capture and export all metadata and field information that was part of the signing process |
| 85.0 | The system shall have automatic report generation and delivery via email |
| REQUIRED | ACCOUNT ADMINISTRATOR FUNCTIONS |
| 86.0 | The system shall have billing and usage functions and reports. Contractor should specify what functionally you provide |
| 87.0 | The system shall have account Profile to allow user details to be managed. The Contractor should specify what functionally you provide |
| 88.0 | The system shall have a regional setting that are applied for time/date stamps on transactions, reporting and other product features |
| 89.0 | The system shall allow customization of branding for business units and groups of users (e.g. colors, logos, etc.) |
| REQUIRED | AUTHENTICATION/IDENTITY SETTINGS |
| 90.0 | The system shall have an Identity proofing options/features included in the Solution. The Contractor should specify what functionally you provide |
| 91.0 | The system shall have support for second factor authentication options: |
| 92.0 | The system shall have user generated second factor codes to be delivered by the sender |
| 93.0 | The system shall have Support for automated SMS PIN code |
| 94.0 | The system shall have support for phone based second factor authentication |
| 95.0 | The system shall specify any additional functionality provided for second factor authentication |
| REQUIRED | AUDITING |
| 96.0 | The system shall have user account activity auditing reports that can be run by the account administrator or the user's group administrator |
| 97.0 | The system shall specify any additional auditing features you provide and the security controls that are provided to control access to them |

| A | B |
|-------------------------------|---|
| Business Specification Number | Business Specification |
| REQUIRED | INTERFACE SOFTWARE DEVELOPMENT KIT (SDK) |
| 98.0 | The system shall have a Web Service Interface that provides a WSDL |
| 99.0 | The system shall have a REST SDK interface |
| 100.0 | The system shall have the ability to use the SDK to do application embedded signing |
| 101.0 | The system shall Interfaces with Cloud platform solutions, provide a list of interfaces that are currently supported (e.g. Salesforce, Dynamics, Acella) |
| 102.0 | The system shall have ample code showing how to use the SDKs using Java. The Contractor will need to provide details on the examples available |
| 103.0 | The system shall have Sample code showing how to use the APIs using .NET. Provide details on the examples available |
| 104.0 | The system shall have documentation and sample code showing how to use the SDKs on the Android platform |
| 105.0 | The system shall have documentation and sample code showing how to use the SDKs on the iOS platform |
| REQUIRED | PLATFORM SUPPORT FOR SENDING / SIGNING DOCUMENTS |
| 106.0 | The system shall support the Windows platform versions currently supported by Microsoft. The Contractor will need to provide details on how you support the platform (e.g. platform specific application, web browser interface, etc.) |
| 107.0 | The system shall support the iOS platform. The Contractor will need to provide details on how you support the platform (e.g. platform specific application, web browser interface, etc.) |
| 108.0 | The system shall support the Android platform. The Contractor will need to provide details on how you support the platform (e.g. platform specific application, web browser interface, etc.) |
| REQUIRED | APPLICATION SECURITY |
| 109.0 | The system shall have encryption of documents in flight during ingestion into the Solution. The Contractor will need to describe the type of encryption that is implemented |
| 110.0 | The system shall have encryption of documents during the signing process. The Contractor will need to describe the type of encryption that is implemented |

| A | B |
|--------------------------------------|--|
| Business Specification Number | Business Specification |
| 111.0 | The system shall have encryption of documents at rest during the signing process. The Contractor will need to describe the type of encryption that is implemented |
| 112.0 | The system shall have HIPPA Compliant – The Contractor will need to Describe how you meet HIPPA compliance |
| 113.0 | The system shall have CJIS compliant – The Contractor will need to describe how you meet CJIS compliance based on CJIS Security Compliance v5.6 |
| REQUIRED | SIGNATURE SECURITY SUPPORTED (SOURCE OF DEFINITIONS - IATA.ORG) |
| 114.0 | The system shall support Electronic Signature – “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication” |
| 115.0 | The system shall support Advanced Electronic Signature – capable of identifying the signatory. The signatory generates the signature on their own and link it to the data to which it relates. This ensures that changes to the data are detectable. Guarantees the integrity and authentication of the signatures and document contents |
| 116.0 | The system shall support Qualified Digital Signature – a qualified certificate is created by a secure-signature-creation device. All technical elements used apply such a signature |
| REQUIRED | CLIENT INITIATED FORMS |
| 117.0 | The system shall allow client-initiated forms to be published and initiate an eSignature workflow process? |
| 118.0 | The system shall have client-initiated forms allow for conditional fields within client-initiated forms? |
| 119.0 | The system shall Support conditional fields when the client is entering data so only the required fields are available based on the information entered |
| 120.0 | The system shall allow the optional attachment of documents. Please include the limitations on the size and number of attachments that are allowed |
| 121.0 | Integration with Single Sign on (SSO) Solutions (see Mi Login in Section 4) |
| 122.0 | The Contractor shall describe their products ability to integrate with SSO solutions using SAML2 for senders |

| A | B |
|--------------------------------------|---|
| Business Specification Number | Business Specification |
| 123.0 | The Contractor shall describe their products ability to integrate with SSO solutions using SAML2 for signers when a line of business application is not used to perform the integration |
| REQUIRED | Integration for Line-of-Business Applications |
| 124.0 | The Contractor shall describe their products ability to integrate using security web service interfaces including performance limitations and key features |
| 125.0 | The Contractor shall describe any out of the box integration tools or utilities that are provided to help download completed documents into the State environment. |
| OPTIONAL | |
| 1.0 | The system may support electronic notary |
| 2.0 | The system may support remote notary |

Schedule A, Attachment 2 - Pricing

Table 1: Implementation Milestones and Deliverables

| ID | Deliverable Item | Cost per deliverable |
|----|---|----------------------|
| | Project Planning | \$6,600.00 |
| | Requirements and Design Validation | \$7,700.00 |
| | SUITE/Keylight and other misc project documentation | \$29,600.00 |
| | Provision Environments | \$2,200.00 |
| | MiLogin Integration | \$2,200.00 |
| | Installation and Configuration | \$8,800.00 |
| | Training Services | \$4,400.00 |
| | Testing and Acceptance | \$4,400.00 |
| | Product Documentation | \$275.00 |
| | Post Production Warranty | \$1,096.00 |
| | Production Support Services | \$0.00 |
| | Total | \$67,271.00 |

Table 2: Transaction costs for FedRamp hosted transactions.

Transactions Include email only, SMS and/or Static Knowledgebase Answers (SKBA) authentication for signers.

Sender Authentication may include phone authentication to confirm the sender's identity).

| ID | Deliverable Item | Annual Cost |
|----|------------------|-------------|
| | FedRAMP | \$12,000.00 |

| ID | Deliverable Item | Cost Per Transaction based on the annual Transaction Counts |
|----|------------------|---|
| | 1,000 to 4,999 | 2.94 |
| | 5,000-9,999 | 2.44 |
| | 10,000-15,000 | 1.94 |
| | 15,001-24,999 | 1.94 |
| | 25,000-49,999 | 1.69 |
| | 50,000-99,999 | 1.31 |
| | 100,000-249,999 | 1.06 |
| | 250,000-499,999 | 0.81 |
| | 500,000-999,999 | 0.63 |
| | 1,000,000+ | 0.53 |

Notes for usage transaction costs:

- Transaction totals for tables 3, 4, and 5 are independent
- SOM will be billed quarterly for transaction usage based on the cost of the current transaction volume.
- Transactions can be purchased at the beginning of the term and an annual true up process then recalculates the transaction cost based on additional usage of transactions. All transactions are charged at the rate of the total transaction volume rate.
- Due to the limited reporting capabilities within the software and the State using a distributed cost model OSS will provide the State detailed monthly reports for transactions including but not limited to following fields: sender, sender user attributes, authentication method, number of signers, and transaction status.
- Non FedRAMP pricing receives a 20% discount off of the transactional pricing found in Table 2

Optional Services

Table 3: Additional Optional Cost Items as part of the solution (Contractor can add additional items)

| ID | Deliverable Item | Cost per transaction | Define to define unit |
|----|---|----------------------|--------------------------|
| | API/SDK usage costs | \$0.00 | \$0.00 |
| | Cloud connector costs (e.g. SalesForce) | \$72.00 | Cost per user/peryear |
| | SimpliGov Forms/Workflow - 20 workflows unlimited users | \$210,000.00 | Annual Cost |
| | SimpliGov Base Platform 1 Workflow SAPGOVPL | \$41,250.00 | Annual Cost |
| | SimpliGov 1-10 Workflows - Price per Workflow (SAPGOVWF1) | \$10,300.00 | Annual Cost |
| | SimpliGov 11-20 Workflows - Price per Workflow (SAPGOVWF11) | \$6,800.00 | Annual Cost |
| | SimpliGov Analytics (SAPGOVAN) | \$13,777.00 | Annual Cost |
| | OneSpan Archiver* | \$4,995.00 | Per API Key |
| | OneSpan Data File Writer* | \$3,995.00 | Per API Key |
| | DKIM/SMTP relay | \$2,000.00 | Per Domain |
| | Print Driver (not FedRAMP ready) | \$0.00 | Per Desktop |
| | Support for CAC/PIV | \$0.00 | |
| | Document Storage Cost | \$0.00 | |
| | Print Driver Enhancement for FedRAMP compatibility | \$23,000.00 | One Time Enhancement Fee |

*Note: The Archiver and Data File Writer will be licensed per API Key except for RMS usage. RMS will be able to use their software with all API Keys at no additional cost because of being the Enterprise eSignature administrators for all agencies. Individual agencies using the software will need to have their own copy per API Key as noted in the table.

Table 4: Customizations

| ID | Deliverable Item | Number of hours | Cost |
|----|------------------|-----------------|------|
|----|------------------|-----------------|------|

| | | | |
|--|--|--|--------------------|
| | Each of these items ONLY include requirements and development | | |
| | Other Pre-Built API Modules - 20% Optional Annual Maintenance for each not included. These modules are built to be hosted on a client's Azure tenant. Add \$2,000 for On-Premise deployment for each. | | |
| | OneSpan Attachment to Package - | | \$3,995.00 |
| | OneSpan SharePoint Online / 2016 Archive | | \$6,995.00 |
| | OneSpan Office 365 Workflow Integration | | \$12,995.00 |
| | OneSpan Custom Email Notifications | | \$9,995.00 |
| | OneSpan Large File Split/Sign/Seal Utility | | \$12,300.00 |

Table 5: Labor Rates for Services for relevant Services

| ID | Rated Structure | Cost per hour |
|-----------|--------------------------------|----------------------|
| I.11 | Novinzio Business Consultant | 175 |
| I.12 | Novinzio Project Manager | 185 |
| I.13 | Novinzio Integration Developer | 175 |
| I.14 | Novinzio QA Tester | 125 |
| I.15 | Novinzio Technical Writer | 125 |
| I.16 | Novinzio Trainer | 175 |
| I.17 | OneSpan Solution Consultant | 275 |
| I.18 | SimpliGOV Consultant | 250 |

Table 6: User Type and Capacity Based Pricing:

| ID | Deliverable Item | Initial purchase cost per user PER YEAR | Annual maintenance cost per user - Standard is included |
|-----------|--|--|--|
| | Procurement of Software Licenses (C.1) | | |
| | Administrator Accounts | | |
| | Up to 15 users | \$240.00 | 0 |
| | Up to 25 users | 240 | 0 |
| | Up to 50 users | 240 | 0 |
| | Agency Workgroup Administrators | | 0 |
| | Up to 50 users | 240 | 0 |
| | 50 to 100 users | 216 | 0 |
| | 100 to 150 users | 194 | 0 |
| | 100 to 200 users | 194 | 0 |
| | 100 to 250 users | 194 | 0 |
| | Over 250 users | 175 | 0 |
| | Senders | | |
| | Up to 100 users | 240 | 0 |
| | 100 to 250 users | 194 | 0 |
| | 100 to 500 users | 194 | 0 |

| | | | |
|--|--------------------|-----|---|
| | 500 to 1000 users | 175 | 0 |
| | 1000 to 2000 users | 157 | 0 |
| | 1000 to 2000 users | 157 | 0 |
| | Signers | | 0 |
| | Up to 1000 users | 0 | 0 |
| | Up to 10000 users | 0 | 0 |
| | Up to 50000 users | 0 | 0 |
| | Up to 75000 users | 0 | 0 |
| | Up to 100000 users | 0 | 0 |
| | Over 500000 users | 0 | 0 |

Table 7: Signer Authentication Transactions (Optional service that uses Equifax for signer validation) for signers. These are additional transaction costs if using the Equifax Authentication.

| ID | Deliverable Item | Cost per transaction per month | Cost for Incomplete |
|----|-------------------|--------------------------------|---------------------|
| | 500 to 10,000 | 2.05 | 0.55 |
| | 10,001-15,000 | 2.05 | 0.55 |
| | 15,001-25,000 | 2.05 | 0.55 |
| | 25,001-50,000 | 1.91 | 0.55 |
| | 50,001-150,000 | 1.51 | 0.55 |
| | 150,000-250,000 | 1.42 | 0.49 |
| | 250,001-1,000,000 | 1.19 | 0.49 |
| | 1,000,001+ | 1.14 | 0.45 |

Schedule B - Service Level Agreement

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

“Actual Uptime” means the total minutes in the Service Period that the Hosted Services are Available.

“Availability” has the meaning set forth in **Section 4.1**.

“Availability Requirement” has the meaning set forth in **Section 4.1**.

“Available” has the meaning set forth in **Section 4.1**.

“Contractor Service Manager” has the meaning set forth in **Section 3.1**.

“Corrective Action Plan” has the meaning set forth in **Section 5.6**.

“Critical Service Error” has the meaning set forth in **Section 5.4(a)**.

“Exceptions” has the meaning set forth in **Section 4.2**.

“Force Majeure Event” has the meaning set forth in **Section 6.1**.

“High Service Error” has the meaning set forth in **Section 5.4(a)**.

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

“Low Service Error” has the meaning set forth in **Section 5.4(a)**.

“Medium Service Error” has the meaning set forth in **Section 5.4(a)**.

“Resolve” has the meaning set forth in **Section 5.4(b)**.

“Scheduled Downtime” has the meaning set forth in **Section 4.3**.

“Scheduled Uptime” means the total minutes in the Service Period.

“Service Availability Credits” has the meaning set forth in **Section 4.6(a)**.

“Service Error” means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

“Service Level Credits” has the meaning set forth in **Section 5.5**.

“Service Level Failure” means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

“Service Period” has the meaning set forth in **Section 4.1**.

“**Software**” has the meaning set forth in the Contract.

“**Software Support Services**” has the meaning set forth in **Section 5**.

“**State Service Manager**” has the meaning set forth in **Section 3.2**.

“**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.

“**Support Request**” has the meaning set forth in **Section 5.4(a)**.

“**Support Service Level Requirements**” has the meaning set forth in **Section 5.4**.

“**Term**” has the meaning set forth in the Contract.

2. **Services.**

2.1. Services. Throughout the Term, Contractor will, in accordance with all terms and conditions set forth in the Contract and this Schedule, provide to the State and its Authorized Users the following services :

- (a) the hosting, management and operation of the Software and other services for remote electronic access and use by the State and its Authorized Users (“**Hosted Services**”);
- (b) the Software Support Services set forth in **Section 5** of this Schedule;

3. **Personnel**

3.1. Contractor Personnel for the Hosted Services. Contractor will appoint 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 Software Support Services (the “**Contractor Service Manager**”). The Contractor Service Manager will be considered Key Personnel under the Contract.

3.2. State Service Manager for the Hosted Services. 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 Software Support Services, including the submission and processing of Support Requests (the “**State Service Manager**”).

4. **Service Availability and Service Availability Credits.**

4.1. 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 99.9% 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 Contract. “**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.

4.2. 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) Scheduled Downtime as set forth in **Section 4.3**.

4.3. Scheduled Downtime. Contractor must 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 the State to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

4.4. Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

4.5. 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. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement 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 are fully met.

4.6. Remedies for Service Availability Failures.

- (a) Should OneSpan fail to achieve such Availability during any calendar month, Customer will receive a credit for the Subscription Service Fees paid for said month for each day or fraction thereof when the Service is not Available to Customer equivalent to 1/30th of the applicable monthly Subscription Service Fee, provided Customer properly requests such credit. The credit granted shall be Customer’s sole and exclusive remedy and OneSpan’s sole and exclusive liability for any unavailability or downtime of the Service.

Customer must submit a request for credit for the Service unavailability by sending an email to sign.support@onespan.com stating the following: (i) billing information, including company name and billing address, billing contact and billing contact phone number; and (ii) dates and time periods for each instance of downtime that Customer experienced in the relevant calendar month. Credit may only be made on a calendar month basis, and only

when Customer makes the credit request within ten (10) days of the end of the calendar month when unavailability is experienced. All credit requests will be verified against OneSpan system records. Should any credit request be disputed, OneSpan will provide Customer a record of Service availability for the period in question. Any credit owed will be applied against Customer's current or future invoices and is not refundable.

- (b) 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 the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

5. Support and Maintenance Services. Contractor will provide Hosted Service maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this **Section 5**. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

5.1. **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 8 a.m. to 5 p.m. Eastern, Monday thru Friday,
- (c) provide unlimited online support 24 hours a day, seven days a week;
- (d) 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
- (e) respond to and Resolve Support Requests as specified in this **Section 5**.

5.2. **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):
 - (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 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 5.4**, 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.

5.3. 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, Maintenance Releases, New Versions and other improvements to the Hosted Services, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; provided that Contractor shall consult with the State and is required to receive State approval prior to modifying or upgrading Hosted Services, including Maintenance Releases and New Versions of Software; 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 the Contract and this Schedule.

5.4. 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 5.4 ("Support Service Level Requirements")**, and the Contract.

- (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 Service Manager will notify Contractor of Support Requests by email, 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 | <ul style="list-style-type: none"> • Issue affecting entire system or single critical production function; |

| | |
|----------------------|---|
| | <ul style="list-style-type: none"> • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions. |
| High Service Error | <ul style="list-style-type: none"> • Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis. |
| Medium Service Error | <ul style="list-style-type: none"> • Hosted Service is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work around. |
| Low Service Error | <ul style="list-style-type: none"> • 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 | Service Level Metric | Service Level Credits (For Failure to Respond to any | Service Level Credits (For Failure to Resolve any |
|--------------------------------|----------------------|----------------------|---|--|
|--------------------------------|----------------------|----------------------|---|--|

| | (Required Response Time) | (Required Resolution Time) | Support Request Within the Corresponding Response Time) | Support Request Within the Corresponding Required Resolution Time) |
|------------------------|---------------------------------|-----------------------------------|--|---|
| Critical Service Error | One (1) hour | Three (3) 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-hour increment. |
| High Service Error | One (1) hour | Four (4) hours | Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour | Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for the first additional hour |

| | | | | |
|----------------------|-----------------|------------------------|--|--|
| | | | or portion thereof that the corresponding Service Error is not responded to within the required response time. | or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment. |
| Medium Service Error | Three (3) hours | Two (2) Business Days | N/A | N/A |
| Low Service Error | Three (3) hours | 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.

5.5. Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 5.4(b)** ("**Service Level Credits**") in accordance with payment terms set forth in the Contract.

5.6. 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, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must 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.

6. Force Majeure.

6.1. Force Majeure Events. Subject to **Section 6.3**, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the 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 the 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.

6.2. State Performance: Termination. In the event of a Force Majeure Event affecting Contractor’s performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the 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 the Contract pursuant to the preceding sentence, any date specifically designated for Contractor’s performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

6.3. Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

- (a) in no event will any of the following be considered a Force Majeure Event:
 - (i) shutdowns, disruptions or malfunctions of 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.
- (b) no Force Majeure Event modifies or excuses Contractor’s obligations under **Sections 19** (State Data), **20** (Confidentiality), or **27** (Indemnification) of the Contract, **Section 7** (Disaster Recovery and Backup) of this Schedule, the Availability Requirement defined in this Schedule, or any security requirements under the Contract, the Statement of Work, or applicable Schedule.

7. Disaster Recovery and Backup. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

- (a) maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 24 hours, and a Recovery Time Objective (RTO) of 2 hours (the “**DR Plan**”), and implement such DR Plan in the event of any unplanned interruption of the

Hosted Services. 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 7**; 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.

Schedule C - Data Security Requirements

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract.

“**Contractor Security Officer**” has the meaning set forth in **Section 2** of this Schedule.

“**Contractor Systems**” has the meaning set forth in **Section 5** of this Schedule.

“**FedRAMP**” means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

FISMA” means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014)). “**Hosted Services**” means the hosting, management and operation of the computing hardware, ancillary equipment, Software, networking, firmware, data, other services (including support services), subcontractors, and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**NIST**” means the National Institute of Standards and Technology.

“**PSP**” means the State’s IT Policies, Standards and Procedures

“**PCI**” means the Payment Card Industry.

2. Contractor will appoint 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**”). The Contractor Security Officer will be considered Key Personnel under the Contract.

3. 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, Contractor will:

3.1. maintain FedRAMP authorization for the Hosted Services throughout the Term, and in the event the contractor is unable to maintain FedRAMP authorization, the State may move the Software to an alternative provider, at contractor’s sole cost and expense;

3.2. ensure that the Software is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, , including any backup and secondary systems as well as location where any disposal, processing or transmittal of data will occur and provide a complete listing of all data centers and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

3.3. 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 the Contract, and must, at a minimum, remain compliant with FISMA and the NIST Special Publication

800.53 (most recent version) HIGH Controls using minimum control values as established in the applicable PSP;

3.4. 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;

3.5. take all reasonable measures to:

- (a) 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; and
- (b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) the State's Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State's Confidential Information;

3.6. ensure that State Data is encrypted in transit and at rest using AES encryption and a key size of 256 bits or higher;

3.7. ensure that State Data is encrypted in transit and at rest using currently validated encryption modules in compliance with FIPS PUB 140-2 (as amended) and that the State, at all times, has the encryption key. *Security Requirements for Cryptographic Modules*;

3.8. ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML) or comparable mechanisms;

3.9. ensure the Hosted Services implements FIPS/NIST compliant multi-factor authentication for privileged/administrative and other identified access in compliance with all applicable regulatory frameworks; and

3.10. assist the State, at no additional cost, with development and completion of a system security plan using the State's automated governance, risk and compliance (GRC) platform.

4. Unauthorized Access. Contractor may not access, and shall 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 must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this **Section 4**. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

5. 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 in connection with the Services (“**Contractor Systems**”) and shall prevent unauthorized access to State systems through the Contractor Systems.

6. Security Audits. During the Term, Contractor will:

6.1. maintain complete and accurate records relating to its data protection practices, IT security controls, and the security logs 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 Schedule;

6.2. 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 (5) 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 the Contract. The State may, but is not obligated to, perform such security audits, which shall, 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

6.3. if requested by the State, provide a copy of Contractor’s FedRAMP System Security Plan to the State within thirty (30) days. The System Security Plan will be recognized as Contractor’s Confidential Information.

7. Nonexclusive Remedy for Security Breach. Any failure of the Services to meet the requirements of this Schedule 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 the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

8. PCI Compliance.

8.1. Contractors that process, transmit, store or affect the security of credit/debit cardholder data, must adhere to the PCI Data Security Standard. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

8.2. The Contractor must notify the State’s Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, and Discover) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder

data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

8.3. The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.

8.4. Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must 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 breach.

8.5. The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

8.6. The Contractor must provide the State's Contract Administrator with an annual Report on Compliance (ROC) or an Attestation of Compliance (AOC) if a ROC has not been completed, showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

Schedule D – CJIS Security Addendum

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.1 Definitions

1.2 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.3 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.1 Responsibilities of the Contracting Government Agency.

2.2 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.1 Responsibilities of the Contractor.

3.2 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.1 Security Violations.

4.2 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.3 Security violations can justify termination of the appended agreement.

4.4 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.1 Audit

5.2 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.1 Scope and Authority

6.2 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.3 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.4 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.5 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.6 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

Schedule E – IRS Pub 1075, Exhibit 7

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- (8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (11) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see *Exhibit 4, Sanctions for Unauthorized Disclosure*, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Schedule F - Safeguard Requirements of Confidential Tax Data

This section sets forth the safeguard requirements for handling, storage, and processing of confidential tax information for a Contractor and their subcontractor(s) and is incorporated as an integral part of the Contract. It will facilitate administration and enforcement of the laws of the State of Michigan in a manner consistent with the applicable statutes, regulations, published rules and procedures or written communication.

I. Authority

Authority for the Michigan Department of Treasury to require that this section be included in the Contract is contained in 1941 PA 122, as amended, MCL 205.28(1)(f), which subjects current or former contractors to the same restrictions and penalties imposed upon department employees regarding the treatment of confidential information. A private contractor or its employees are strictly prohibited from disclosing taxpayer information to a third party. The prohibition against disclosure does not bar an employee of a private contractor with whom the State of Michigan (State) contracts that processes tax returns or payments pursuant to the Contract from having access to confidential information that is reasonably required for the processing or collection of amounts due this State. Private contractors and any subcontractors will follow Treasury guidelines for Authorized representatives.

II. Confidentiality

It is agreed that all information exchanged under this section will be kept confidential in accordance with the confidentiality provisions contained in the Revenue Act, MCL 205.28(1)(f) which states in part;

“Except as otherwise provided in this subdivision, an employee, authorized representative, or former employee or authorized representative of the department or anyone connected with the department will not divulge any facts or information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the department for a tax administered by the department.”

Confidential information obtained under this contract will not be disclosed except as required by state law, or in the proper administration of applicable laws, promulgated rules and procedures. In the event, confidentiality statutes are amended, Treasury will notify Contractor of any changes. No employee, agent, authorized representative or legal representative of Contractor will disclose any information obtained by virtue of this section to any other division within their company or any other governmental agency, department or unit within such governmental agency whether local, state, federal or foreign, department or unit within such governmental agency, or any unauthorized third party. No tax returns or tax return information accessed by Contractor will be duplicated or disseminated within or outside the company without the written approval of the Contract Compliance Inspector. Tax returns and tax return information remain the property of Treasury.

Contractor may use a taxpayer's name, address and Social Security number or employer identification number to the extent necessary in connection with the processing and mailing of forms for any report or return required in the administration of any tax in the performance of the Contract. The use of the Social Security number must be in accordance with the state Social Security Number Privacy Act 454 of 2004, as amended.

Confidential information obtained under this agreement will not be disclosed in part of a report or document that is subject to FOIA.

The penalties for violating the confidentiality provisions of the Revenue Act are contained in, MCL 205.28(2) and MCL 205.27(4). MCL 205.28(2) states:

“A person who violates subsection (1)(e), (1)(f), (4) or (5) is guilty of a felony, punishable by a fine of not more than \$5,000.00, or imprisonment for not more than 5 years, or both, together with the costs of prosecution. In addition, if the offense is committed by an employee of this state, the person will be dismissed from office or discharged from employment upon conviction.”

MCL 205.27(4) states:

A person who is not in violation pursuant to subsection (2), but who knowingly violates any other provision of this act, or of any statute administered under this act, is guilty of a misdemeanor, punishable by a fine of not more than \$1,000.00, or imprisonment for not more than 1 year, or both.

Information received by Treasury from the U.S. Internal Revenue Service, pursuant to section 6103(d) of the Internal Revenue Code or any other federal agency will not be subject to the exchange.

III. Procedure for Security

Contractor will safeguard any tax return information obtained under the Contract as follows:

- A. Access to the tax returns and tax return information will be allowed only to those authorized employees and officials of Contractor who need the information to perform their official duties in connection with the uses of the information authorized in this Contract.
- B. Any records created from tax returns and tax return information will be stored in an area that is physically safe from access by unauthorized persons during duty hours and locked in a secure area during non-duty hours, or when not in use.
- C. Any records matched and any records created by the match will be processed under the immediate supervision and control of authorized personnel in a manner in which will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve any such records by means of a computer, remote terminal or other means.

- D. All personnel who will have access to the tax returns and tax return information and to any records created by the tax return information will be advised annually of the confidential nature of the information, the safeguards required to protect the information and the civil and criminal sanctions for noncompliance contained in MCL 205.28 (2) and MCL 205.27(4) and will sign confidentiality certifications.
- E. All confidential information, electronic and paper, will be secured from unauthorized access and with access limited to designated personnel only. State tax return information will not be commingled with other information. All Michigan tax returns and return information will be marked as follows: **CONFIDENTIAL - DO NOT DISCLOSE - MICHIGAN TREASURY TAX RETURN INFORMATION**
- F. Treasury, Office of Privacy and Security or Contract Compliance Inspector may make onsite inspections or make other provisions to ensure that adequate safeguards are being maintained by the Contractor.
- G. The Treasury Office of Privacy and Security may monitor compliance of systems security requirements during the lifetime of the Contract or any extension.
- H. Contractor will also adopt policies and procedures to ensure that information contained in their respective records and obtained from Treasury and taxpayers will be used solely as stipulated in the Contract.

IV. Computer System Security of Tax Data

The identification of confidential tax records and defining security controls are intended to protect Treasury tax return information from unlawful disclosure, modification, destruction of information and unauthorized secondary uses.

Computer system security and physical security of tax data stored and processed by Contractor must be in compliance with the following security guidelines and standards established by Treasury. These guidelines apply to any computer system developed by Contractor, either through its own systems staff, or through a contractor, subcontractor):

A. Controlled Access Protection

All computer systems processing, storing and transmitting Michigan tax information must have computer access protection controls. These security standards are delineated in the National Institute of Standards and Technology (NIST) Special Publications number 800-53 "Recommended Security Controls for the Federal Information Systems" at <http://csrc.nist.gov/publications/PubsSPs.html>. To meet these standards, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance, and documentation.

- 1) **Security Policy** – A security policy is a written document describing the system in terms of categories of data processed, users allowed access and access rules between the users and the data. Additionally, it describes procedures to prevent unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of

or into the system. Further protection must be provided where the computer system contains information for more than one program/project, office, or Agency and that personnel do not have authorization to see all information on the system.

- 2) **Accountability** – Computer systems processing Michigan tax information must be secured from unauthorized access. All security features must be available (audit trails, identification and authentication) and activated to prevent unauthorized users from indiscriminately accessing Michigan tax information. Everyone who accesses computer systems containing Michigan tax information is accountable. Access controls must be maintained to ensure that unauthorized access does not go undetected. Computer programmers and contractors who have a need to access databases, and are authorized under the law, must be held accountable for the work performed on the system. The use of passwords and access control measures must be in place to identify who accessed protected information and limit that access to persons with a need to know.

a) On-line Access –Users will be limited to any Treasury on-line functions, by limiting access through functional processing controls and organization restrictions.

Any employee granted access privileges through the Contractor’s Security Administrator will be approved for access and viewing rights to Treasury on-line systems by the Department of Treasury, Office of Privacy and Security.

b) Operating Features of System Security

Contractor must meet the following levels of protection with respect to tax return information. Individual user accountability must be ensured through user identification number and password.

- i. Access rights to confidential tax information must be secured through appropriate levels of authorization.
- ii. An audit trail must be maintained of accesses made to confidential information.
- iii. All confidential and protected information must be cleared from a system before it is used for other purposes not related to the enforcement, collection or exchange of data not covered by this section or by an addendum to this Contract.
- iv. Hard copies made of confidential tax return information must be labeled as confidential information.
- v. Confidential Treasury tax information will be blocked or coded as confidential on system.
- vi. Any computer system in which Michigan tax return information resides must systematically notify all users upon log-in of the following disclosure penalties for improperly accessing or making an authorized disclosure of Michigan tax return information:

**NOTICE TO EMPLOYEES AND AUTHORIZED
REPRESENTATIVES**

This system contains Michigan Department of Treasury tax return information. **DO NOT DISCLOSE OR DISCUSS MICHIGAN RELATED TAX RETURN INFORMATION** with unauthorized individuals. The Revenue Act at MCL 205.28(1)(f) prohibits such disclosure.

MICHIGAN PENALTIES

A person making a willful unauthorized disclosure or inspection (browsing) of tax return information may be charged with the following Michigan penalties:

- Criminal penalties up to \$5,000 and/or imprisonment for 5 years, plus costs and dismissal from employment if it is found that a current or former employee or authorized representative has made an unauthorized disclosure of a tax return or tax return information or divulged audit selection or processing parameters. [MCL 205.28(2)]
- A misdemeanor, punishable by a fine of not more than \$1,000.00, or imprisonment for not more than 1 year, or both if the person is not in violation pursuant to MCL 205.27(2), but who knowingly violates any other provision of this act, or of any statute administered under this act.

This statement is subject to modification. A confidentiality statement, subject to modification, will be sent as needed by the Security Administrator to all employees, contractors, and legal representatives of Contractor.

- 3) **Assurance** – Contractor must ensure that all access controls and other security features are implemented and are working when installed on their computer system. Significant enhancements or other changes to a security system must follow the process of review, independent testing, and installation assurance. The security system must be tested at least annually to assure it is functioning correctly. All anomalies must be corrected immediately.
 - a) The Contractor must initiate corrective action for all non-conformities as soon as detected and immediately advise the Contract Compliance Inspector. Notice of the corrective action must be provided to the Contract Compliance Inspector. All non-conformities must be reported to the Contract Compliance Inspector with the following:
 - a. Duration of non-conformity/interruption
 - b. Reason for non-conformity/interruption
 - c. Resolution.
 - b) All non-conformities to the specifications/tasks of the Contract must be corrected within four (4) hours. The State recognizes there will be instances when adherence to

this time frame will not be possible. However, the State will only tolerate this on an exception basis. To request an exception to this time frame, the Contractor must submit a detailed project plan to address the non-conformity within four (4) hours to the Contract Compliance Inspector for approval.

- 4) **Documentation** – Design and test documentation must be readily available to the state. The developer or manufacturer should initially explain the security mechanisms, how they are implemented and their adequacy (limitations). This information should be passed on to the security officer or supervisor. Test documentation should describe how and what mechanisms were tested and the results. If recognized organizations/tests/standards are used, then a document to that effect will suffice. For example, a system that has been tested and certified as meeting certain criteria may have a document stating this fact, without detailed tests/results of information. Contractor, however, must ensure the documentation covers the exact system and that it includes the specific computer system used by Contractor.

Additionally, documentation must include a security administrator's guide. The security administrator's guide is addressed to the System's Administrator and Security Officer and will describe the protection mechanisms provided by the security system, guidelines on their use and how they interact. This document will present cautions about security functions and describe privileges that should be controlled when running a secure system. The document will be secured and locked at all times with access rights only by the Systems Administrator and Security Officer.

Note: When a security system is designed or purchased for a specific computer or computer system, the security mechanisms must be reviewed by the State to ensure that needed security parameters are met. An independent test should be implemented on the specific computer or computer system to ensure that the security system meets the security parameters within this contract and developed with the computer system. The test may be arranged by the developer but must be done by an independent organization. Contractor must assign responsible individuals (Security Officers) with knowledge of information technology and applications to oversee the testing process. These individuals must be familiar with technical controls used to protect the system from unauthorized entry.

Finally, contingency and backup plans must be in place to ensure protection of Michigan tax information.

V. Electronic Transmission of Michigan Tax Information

The two acceptable methods of transmitting Michigan tax information over telecommunications devices are encryption and using guided media. Encryption involves altering data objects in a way that the objects become unreadable until deciphered with the appropriate software at the intended destination. Guided media involves transmission of data over twisted pair cable, coaxial cable or end to end fiber optics which are typically used in secure computer networks like the state's Local Area Network (LAN), telephone systems, and television distribution.

Cryptography standards have been adopted by the IRS and can be used to provide guidance for encryption, message authentication codes or digital signatures and digital signatures with or without an associated certification infrastructure. For further information, see IRS Publication 1075 at the IRS web site.

Unencrypted cable circuits of fiber optics are an acceptable alternative for transmitting Michigan tax information. Adequate measures must be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio or microwave transmission. Additional precautions should be taken to protect the cable, i.e., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms and switching centers.

A. Remote Access

Accessing databases containing Michigan tax information from a remote location – that is, a location not directly connected to the Local Area Network (LAN) will require adequate safeguards to prevent unauthorized entry.

For remote access, the contractor is required to use an identification security card that requires both PIN and card in possession. The State identified and approved methods for remote vendor access are as follows:

- SecureID through VPN – State provided SecureID token and VPN software in order to access State of Michigan resources. Appropriate Acceptable Use policies and signoffs are required
- Follow-the Sun SecureID – Contractor is provided with VPN software and a SOM technical resource coordinates with the DTMB Client Service Center to provide secure ID code access to specific State of Michigan resources. Appropriate Acceptable Use Policies and signoffs are required.

B. Portable Computer Devices

Any entrusted confidential information collected or accessed during this Contract must be encrypted when stored on all storage devices and media. This includes, but not limited to, disk drives for servers and workstations, and portable memory media (PDAs, RAM drives, memory sticks, etc.).

VI. Record Keeping Requirements for Information Received

Each Contractor, requesting and receiving information will keep an accurate accounting of the information received. The audit trail will be required which will include the following information:

- a. Taxpayer's name
- b. Identification number
- c. Information requested
- d. Purpose of disclosure request
- e. Date information received
- f. Name of Division and employee making request
- g. Name of other employees who may have had access
- h. Date destroyed
- i. Method of destruction

The Contractor will adopt and implement formal procedures to:

- Ensure proper handling of tax returns and tax return information;
- Secure and safeguard information from unauthorized use; and
- Ensure appropriate destruction of information and materials retrieved from Treasury.

A. Electronic Media

Contractor will keep an inventory of magnetic and electronic media received under the Contract.

Contractor must ensure that the removal of tapes and disks and paper documents containing Michigan tax return information from any storage area is properly recorded on charge-out records. Contractor is accountable for missing tapes, disks, and paper documents.

B. Recordkeeping Requirements of Disclosure Made to State Auditors

When disclosures are made by Contractor to State Auditors, these requirements pertain only in instances where the Auditor General's staff extracts Michigan tax returns or tax information for further review and inclusion in their work papers. Contractor must identify the hard copies of tax records or if the tax information is provided by magnetic tape format or through other electronic means, the identification will contain the approximate number of taxpayer's records, the date of inspection, the best possible description of the records and the name of the Auditor(s) making the inspection.

The Disclosure Officer must be notified, in writing, of any audits done by auditors, internal or otherwise, of Contractor that would involve review of Treasury processing parameters.

VII. Contract Services

To the extent the Contractor employs an independent agency, consultant, or agent to process confidential information which includes Michigan tax return information; the Contractor will notify the Treasury Disclosure Officer before the execution of any such agreement. Each agreement will include in the agreement the following recommended safeguard provisions:

- A. The identification of confidential tax records and defining security controls are intended to protect Treasury tax return information from unlawful disclosure, modification, destruction of information and unauthorized secondary uses.

Definition of Treasury Tax Return Information as defined in Revenue Administrative Bulletin (RAB) 1989-39:

Taxpayer's identity, address, the source or amount of his/her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments whether the

taxpayer's return was, is being or will be examined or subject to their investigation or processing, or any other data, received by, recorded by, prepared by, furnished to or collected by the agency with respect to a return or with respect to the determination of the existence, or liability (or the amount thereof) of any person under the tax laws administered by the Department, or related statutes of the state for any tax, penalty, interest, fine, forfeiture, or other imposition or offense. The term "tax return information" also includes any and all account numbers assigned for identification purposes.

- B. An acknowledgment that a taxpayer has filed a return is known as a "fact of filing" and may not be disclosed. All tax return data made available in any format will be used only for the purpose of carrying out the provisions of the Contract between Contractor and the subcontractor. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract between Contractor and the subcontractor. In addition, all related output will be given the same level of protection as required for the source material.
- C. The subcontractor will certify that the data processed during the performance of the Contract between Contractor and the subcontractor will be completely purged from all data storage components of the subcontractor's computer facility, and no output will be retained by the subcontractor at the time the work is completed.
- D. Destruction of tax data, including any spoilage or any intermediate hard copy printout which may result during the processing of Michigan tax return information, will be documented with a statement containing the date of destruction, description of material destroyed, and the method used. Destruction parameters must meet the standards of Section IX, Disposal of Tax Information, of this agreement.
- E. Computer system security and physical security of tax data stored and processed by the subcontractor must be in compliance with security guidelines and standards established by this contract. See section VI (Record Keeping Requirements for Information Received in Paper Format) for more details.
- F. The Contractor will be responsible for maintaining a list of employees authorized to access Michigan tax return information and will provide a copy of such list to Treasury.
- G. No work involving information furnished under the contract will be subcontracted without the specific approval of Treasury. Contractor and approved subcontractors handling Michigan tax return information will be required to sign the *Vendor, Contractor or Subcontractor Confidentiality Agreement* provided by Treasury, (Form 3337, see Attachment A). The original agreements will be returned to the Disclosure Officer for the Department of Treasury and a copy sent to the Contract Compliance Inspector.

VIII. Transport of Tax Information

In the event, it is necessary to transport confidential tax return information the Contractor is responsible for holding the carrier responsible for safeguarding the records. The Contractor must

obtain a signed *Vendor, Contractor or Subcontractor Confidentiality Agreement* (Form 3337, see Attachment A) for each carrier employee who has access to Michigan tax return information. The original agreements will be returned to the Department of Treasury, Disclosure Officer and a copy sent to the Contract Compliance Inspector.

If it is necessary to transfer records and responsibility for transport to a third carrier due to a mishap during transportation, the Contractor is responsible for ensuring safeguard standards remain enforce. This type of incident will be documented in accordance with the incident reporting guidelines in procedure PT-03253, "Incident Reporting and Handling".

Any such incidents must be reported to the Contract Administrator immediately.

IX. Disposal of Tax Information

Materials furnished to Contractor, such as tax returns, remittance vouchers, W-2 reports, correspondence, computer printouts, carbon paper, notes, memorandums and work papers will be destroyed by burning, mulching, pulverizing or shredding. If shredded, destroy paper using cross cut shredders which produce particles that are 1 mm x 5mm (0.04in x 0.2 in.) in size (or smaller).

Data tracks should be overwritten or reformatted a minimum of three times or running a magnetic strip over entire area of disk at least three (3) times to remove or destroy data on the disk media. Electronic data residing on any computer systems must be purged based on Treasury's retention schedule.

Contractor and its subcontractor(s) will retain all confidential tax information received by Treasury only for the period of time required for any processing relating to the official duties and then will destroy the records. Any confidential tax information that must be kept to meet evidentiary requirements must be kept in a secured, locked area and properly labeled as confidential return information. See Procedure for Security (Section III of this agreement) for more details.

X. Security Responsibility

Contractor will designate a security person who will ensure that each individual having access to confidential tax information or to any system which processes Michigan tax return information is appropriately screened, trained and executes a *Vendor, Contractor or Subcontractor Confidentiality Agreement* (Form 3337, see Attachment A to this Schedule) before gaining access or transaction rights to any process and computer system containing Treasury tax return information.

Each Contractor or their subcontractor(s) employees' access and transaction rights will be reviewed periodically to ensure that there is a need to know Treasury tax return information displayed in any media.

Michigan tax return information will be made available only to individuals authorized by the Contract. Contractor will maintain a list of persons authorized to request and receive information and will update the list as necessary. A copy of the list must be furnished to the Michigan Department of Treasury Disclosure Officer and Contract Compliance Inspector.

XI. Security Breach Notification

The Contractor is required to report to Treasury, on Form 4000, Incident Reporting (Attachment B to this Schedule) any use or disclosure of confidential information, whether suspected or actual, **immediately** after becoming aware of the misuse or disclosure. The Contractor may substitute its internal form for Form 4000 if all pertinent information is included.

The Contractor agrees to immediately contain the breach if it is determined ongoing.

Treasury has the right to terminate the Contract when a breach has occurred, and the Contractor cannot demonstrate proper safeguards were in place to avert a breach. Treasury must approve Contractor's resolution to the breach.

XII. Certification of Compliance

The Contractor will fully protect State Tax Information (STI) entrusted to them. Each Contractor or subcontractor who will have access to STI must read and sign a confidentiality agreement. This contract requires that all information obtained from the Michigan Department of Treasury under the Revenue Act, PA 122 of 1941, MCL 205.28 (1)(f) be kept confidential. In the event of a security breach involving STI in the possession of the Contractor, the Contractor agrees to provide full cooperation to conduct a thorough security review. The review will validate compliancy with the Contract, and state laws and regulations.

If, as a result of the Contractor's failure to perform as agreed, the State is challenged by a governmental authority or third party as to its conformity to or compliance with State, Federal and local statutes, regulations, ordinances or instructions; the Contractor will be liable for the cost associated with loss of conformity or compliance.

The Contractor understands the cost reflects violation fines identified by the Michigan Social Security Number Privacy Act, 454 of 2004 and the Michigan Identity Theft Protection Act, Act 452 of 2004 as amended.

XIII. Effective Date

These Safeguard requirements will be reviewed whenever the Contract modifications include specifications or processes that affect tax data.

Schedule F, Attachment 1 - Confidentiality Report

Reset Form

Michigan Department of Treasury
3337 (Rev. 10-16)

Vendor, Contractor or Subcontractor Confidentiality Agreement

The Revenue Act, Public Act 122 of 1941, MCL 205.28(1)(f), the City Income Tax Act, Public Act 284 of 1964, MCL 141.674(1), and Internal Revenue Code (IRC) 6103(d), make all information acquired in administering taxes confidential. The Acts and IRC hold a vendor, contractor or subcontractor and their employees who sell a product or provide a service to the Michigan Department of Treasury, or who access Treasury data, to the strict confidentiality provisions of the Acts and IRC. Confidential tax information includes, but is not limited to, information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the Michigan Department of Treasury for a tax administered by the department.

INSTRUCTIONS. Read this entire form before you sign it. If you do not complete this agreement, you will be denied access to Michigan Department of Treasury and federal tax information. After you and your witness sign and date this form, keep a copy for your records. Send the original to the address listed below.

| | | | |
|---|----------|---|------------------|
| Company Name and Address (Street or RR#, City, State, ZIP Code) | | Last Name | First Name |
| | | Driver License Number/Passport Number | Telephone Number |
| State of Michigan Department | Division | Subcontractor Name if Product/Service Furnished to Contractor | |
| Describe here or in a separate attachment the product or service being provided to the State of Michigan Agency (Required). | | | |

Confidentiality Provisions. It is illegal to reveal or browse, except as authorized:

- All tax return information obtained in connection with the administration of a tax. This includes information from a tax return or audit and any information about the selection of a return for audit, assessment or collection, or parameters or tolerances for processing returns.
- All Michigan Department of Treasury or federal tax returns or tax return information made available, including information marked "Official Use Only". Tax returns or tax return information shall not be divulged or made known in any manner to any person except as may be needed to perform official duties. Access to Treasury or federal tax information, in paper or electronic form, is allowed on a **need-to-know** basis only. Before you disclose returns or return information to other employees in your organization, they must be authorized by Michigan Department of Treasury to receive the information to perform their official duties.
- Confidential information shall not be disclosed by a department employee to confirm information made public by another party or source which is part of any public record. 1999 AC, R 2005.1004(1).

Violating confidentiality laws is a felony, with penalties as described:

Michigan Penalties

MCL 205.28(1)(f) provides that you may not willfully disclose or browse any Michigan tax return or information contained in a return. Browsing is defined as examining a return or return information acquired without authorization and without a need to know the information to perform official duties. Violators are guilty of a felony and subject to fines of \$5,000 or imprisonment for five years, or both. State employees will be discharged from state service upon conviction.

Any person who violates any other provision of the Revenue Act, MCL 205.1, et seq., or any statute administered under the Revenue Act, will be guilty of a misdemeanor and fined \$1,000 or imprisonment for one year, or both, MCL 205.27(4).

City Penalties

MCL 141.674(2) provides that any person divulging confidential City Tax information is guilty of a misdemeanor and subject to a fine not exceeding \$500 or imprisonment for a period not exceeding 90 days, or both, for each offense.

Federal Penalties

If you willfully disclose federal tax returns or tax return information to a third party, you are guilty of a felony with a fine of \$5,000 or imprisonment for five years, or both, plus prosecution costs according to the Internal Revenue Code (IRC) §7213, 26 USC 7213.

In addition, inspecting, browsing or looking at a federal tax return or tax return information without authorization is a felony violation of IRC §7213A subjecting the violator to a \$1,000 fine or imprisonment for one year, or both, plus prosecution costs. Taxpayers affected by violations of §7213A must be notified by the government and may bring a civil action against the federal government and the violator within two years of the violation. Civil damages are the greater of \$1,000 or actual damages incurred by the taxpayer, plus the costs associated with bringing the action, 26 USC 7431.

Failure to comply with this confidentiality agreement may jeopardize your employer's contract with the Michigan Department of Treasury.

| Certification | | |
|---|---------------------------------|-------------|
| By signing this Agreement, I certify that I have read the above confidentiality provisions and understand that failure to comply is a felony. | | |
| Print name of employee signing this agreement | Signature of person named above | Date signed |
| Print Witness Name (Required) | Signature of Witness (Required) | Date signed |

Submit your form to the following address:
Office of Privacy and Security/ Disclosure Unit
Michigan Department of Treasury
430 W. Allegan Street
Lansing, MI 48922

Questions, contact the Office of Privacy and Security by telephone, 517-636-4239; fax, 517-636-5340; or email: Treas_Disclosure@michigan.gov

Schedule F, Attachment 2 - Incident Report

Michigan Department of Treasury
4000 (Rev. 05-14)

Reset Form

Incident Report

INSTRUCTIONS: Complete Parts 1 and 2 and immediately submit Initial Report to the Office of Privacy and Security. After incident resolution, submit Final Report (Parts 1, 2 and 3) to the Office of Privacy and Security. Refer to Procedure PT-03253, Incident Reporting and Handling.

| PART 1: A. CONTACT INFORMATION (Reporting Entity) | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--------------------------|--|--|---|---|--|--|--|--|---|---|--|--|---|---|--|--|--|--|--|--------------------------------|--------------------------------|
| Full Name (Last, First, Middle Initial) | | Division/Office | | | | | | | | | | | | | | | | | | | | | | |
| Telephone Number | Fax Number | E-Mail Address | | | | | | | | | | | | | | | | | | | | | | |
| B. CONTACT INFORMATION (Affected Entity) | | | | | | | | | | | | | | | | | | | | | | | | |
| Full Name (Last, First, Middle Initial) | | Division/Office | | | | | | | | | | | | | | | | | | | | | | |
| Telephone Number | Fax Number | E-Mail Address | | | | | | | | | | | | | | | | | | | | | | |
| PART 2: INCIDENT INFORMATION | | | | | | | | | | | | | | | | | | | | | | | | |
| Whose information was involved in the incident? | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Treasury <input type="checkbox"/> Federal Tax Information <input type="checkbox"/> Other State Agency, specify _____ <input type="checkbox"/> Other _____ | | | | | | | | | | | | | | | | | | | | | | | | |
| Incident Category (select all that apply) | | | | | | | | | | | | | | | | | | | | | | | | |
| <table style="width: 100%; border: none;"> <tr> <td style="width: 33%;"><input type="checkbox"/> Passwords Shared/Stolen</td> <td style="width: 33%;"><input type="checkbox"/> Computer Virus/Spam</td> <td style="width: 33%;"><input type="checkbox"/> Paper Archives Compromised</td> </tr> <tr> <td><input type="checkbox"/> Misrouted Communications</td> <td><input type="checkbox"/> Data Destruction/Deletion</td> <td><input type="checkbox"/> Safe/Lockbox/other Compromise</td> </tr> <tr> <td><input type="checkbox"/> Unauthorized Access</td> <td><input type="checkbox"/> Backups Missing or Stolen</td> <td><input type="checkbox"/> Delivery of Documents Lost</td> </tr> <tr> <td><input type="checkbox"/> Fraudulent Actions</td> <td><input type="checkbox"/> Hacking of Networks/Systems</td> <td><input type="checkbox"/> Inappropriate Destruction Paper</td> </tr> <tr> <td><input type="checkbox"/> Lost/Stolen Information/Data</td> <td><input type="checkbox"/> Improperly Secured Sys/Web</td> <td><input type="checkbox"/> Inappropriate Destruction Media</td> </tr> <tr> <td><input type="checkbox"/> Lost/Stolen Cash/Checks</td> <td><input type="checkbox"/> Circumvention of Security Protocols</td> <td><input type="checkbox"/> Lost/Stolen Equipment</td> </tr> <tr> <td><input type="checkbox"/> Inappropriate Building Access</td> <td><input type="checkbox"/> _____</td> <td><input type="checkbox"/> _____</td> </tr> </table> | | | | <input type="checkbox"/> Passwords Shared/Stolen | <input type="checkbox"/> Computer Virus/Spam | <input type="checkbox"/> Paper Archives Compromised | <input type="checkbox"/> Misrouted Communications | <input type="checkbox"/> Data Destruction/Deletion | <input type="checkbox"/> Safe/Lockbox/other Compromise | <input type="checkbox"/> Unauthorized Access | <input type="checkbox"/> Backups Missing or Stolen | <input type="checkbox"/> Delivery of Documents Lost | <input type="checkbox"/> Fraudulent Actions | <input type="checkbox"/> Hacking of Networks/Systems | <input type="checkbox"/> Inappropriate Destruction Paper | <input type="checkbox"/> Lost/Stolen Information/Data | <input type="checkbox"/> Improperly Secured Sys/Web | <input type="checkbox"/> Inappropriate Destruction Media | <input type="checkbox"/> Lost/Stolen Cash/Checks | <input type="checkbox"/> Circumvention of Security Protocols | <input type="checkbox"/> Lost/Stolen Equipment | <input type="checkbox"/> Inappropriate Building Access | <input type="checkbox"/> _____ | <input type="checkbox"/> _____ |
| <input type="checkbox"/> Passwords Shared/Stolen | <input type="checkbox"/> Computer Virus/Spam | <input type="checkbox"/> Paper Archives Compromised | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Misrouted Communications | <input type="checkbox"/> Data Destruction/Deletion | <input type="checkbox"/> Safe/Lockbox/other Compromise | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Unauthorized Access | <input type="checkbox"/> Backups Missing or Stolen | <input type="checkbox"/> Delivery of Documents Lost | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Fraudulent Actions | <input type="checkbox"/> Hacking of Networks/Systems | <input type="checkbox"/> Inappropriate Destruction Paper | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Lost/Stolen Information/Data | <input type="checkbox"/> Improperly Secured Sys/Web | <input type="checkbox"/> Inappropriate Destruction Media | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Lost/Stolen Cash/Checks | <input type="checkbox"/> Circumvention of Security Protocols | <input type="checkbox"/> Lost/Stolen Equipment | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Inappropriate Building Access | <input type="checkbox"/> _____ | <input type="checkbox"/> _____ | | | | | | | | | | | | | | | | | | | | | | |
| Incident Affects | | | | | | | | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> Financial Information/Resources <input type="checkbox"/> Personal Information (SSN, Driver License No. Financial information) <input type="checkbox"/> Unauthorized/Unlawful Activity <input type="checkbox"/> Confidential/Sensitive Information <input type="checkbox"/> Human Resources (threat) <input type="checkbox"/> Other _____ | | | | | | | | | | | | | | | | | | | | | | | | |
| Date Incident Occurred | Time Incident Occurred | Date Incident Discovered | Time Incident Discovered | | | | | | | | | | | | | | | | | | | | | |
| Incident Location | | Number of Individuals Affected | | | | | | | | | | | | | | | | | | | | | | |
| Involved Parties/Entities | | Does this involve personal information (first and last name along with a SSN, driver license number, or credit/debit card account number)? | | | | | | | | | | | | | | | | | | | | | | |
| | | <input type="checkbox"/> Yes <input type="checkbox"/> No | | | | | | | | | | | | | | | | | | | | | | |
| Date of Initial Report | | | | | | | | | | | | | | | | | | | | | | | | |
| Description of Incident | | | | | | | | | | | | | | | | | | | | | | | | |

| PART 1: CONTACT INFORMATION (Affected Entity) | | | |
|--|-----------------------------------|---|-----------------------------|
| Full Name (Last, First, Middle Initial) | | Division/Office | |
| PART 3: INCIDENT RESOLUTION | | | |
| Notification issued to affected individuals? <input type="checkbox"/> Yes <input type="checkbox"/> No | How many notifications were sent? | Breach Notification Method? <input type="checkbox"/> E-mail <input type="checkbox"/> Telephone <input type="checkbox"/> US Mail <input type="checkbox"/> Web | |
| Who was notified? | | Date notification was issued | |
| Incident Cost <input type="checkbox"/> Check if incident costs are less than \$250. If \$250 or more, complete the detailed summary of costs below. | | | |
| <u>Manhours:</u> Treasury \$ _____ DTMB-OES \$ _____ DTMB-Treasury Agency Services \$ _____ | | <u>Other:</u> Postage \$ _____ Credit Monitoring Service \$ _____ _____ \$ _____ Total Cost of Incident \$ _____ | |
| Action Taken | | | |
| Incident Impact | | | |
| Post Incident Recommendations | | | |
| PART 4: REPORT PREPARER INFORMATION | | | |
| Final Report Prepared By: | Date Prepared | Preparer Title | Preparer's Telephone Number |
| Preparer Signature | | | Date |
| OFFICE OF PRIVACY AND SECURITY USE ONLY | | | |
| Administrator, Office of Privacy and Security Signature | | | Date |

