STATE OF MICHIGAN PROCUREMENT

Department of Treasury
430 W. Allegan Street, Lansing, MI 48922

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **190000000423**

CONTRACTOR	
	Nebraska Student Loan Program, Inc., d/b/a NSLP/Inceptia
	1300 O Street
	Lincoln, NE 68508
	Matthew Nettleton
	888-529-2028 ext. 6880
	mattn@inceptia.org
	7379

STATE			
	Program Manager	Kara Scheeneman	Treasury
		517-335-3031	
		ScheenemanK@michigan.gov	
	Contract Administrator	Stacey Shaw	Treasury
		517-636-6816	
		ShawS11@michigan.gov	

CONTRACT SUMMARY

DESCRIPTION: Student Loan Default Aversion Services - MIDEAL

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
April 1, 2016	March 31, 2019	2 Years	March 31, 2019

PAYMENT TERMS	DELIVERY TIMEFRAME
N/A	N/A

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-card	☐ Payment Request (PRC)	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	3 Years	☐		March 31, 2021

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$0.00	$0.00	$0.00

DESCRIPTION:

1. Effective March 31, 2019, the following amendment is hereby incorporated into the Contract per attached SOW. This change includes the following:
   - Additional Services – Loan Summary - $2,500 pear year for each school using the service

2. 2-option years available on this Contract are hereby exercised. The revised Contract expiration date is March 31, 2021.

3. Please note the Contract Administrator has been changed to Stacey Shaw.

Loan Summary

1. Loan Summary will provide individual student loan summaries including all current loans
2. Inceptia will conduct outreach to students on school's behalf urging them to review the summaries
3. Loan summaries are sent to current, graduating and withdrawn borrowers
4. Loan Summary satisfied state reporting requirements where laws have been passed requiring such communications.
5. Costs for Loan Summary services are $2,500 per year for each school subscribed to the service.

Form No. DTMB-3522 (Rev. 10/2015)
AUTHORITY: Act 431 of 1984
COMPLETION: Required
PENALTY: Contract change will not be executed unless form is filed

STATE OF MICHIGAN

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

PROCUREMENT

525 W. ALLEGAN STREET
LANSING, MI 48933

P.O. BOX 30026
LANSING, MI 48909

NOTICE OF CONTRACT NO. **271B6600005**

between

THE STATE OF MICHIGAN

and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
Nebraska Student Loan Program, Inc., d/b/a NSLP/Inceptia	**Maggie Hackwith**	**inceptiacs@inceptia.org**
1300 O Street	**PHONE**	**VENDOR TAX ID # (LAST FOUR DIGITS ONLY)**
Lincoln, NE 68508	**888-529-2028 ext. 6306**	**4573**

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER	**Treasury**	**Kara Scheeneman**	**517-335-3031**	**ScheenemanK@michigan.gov**
CONTRACT ADMINISTRATOR	**Treasury**	**Julie Collins**	**517-636-6817**	**Collinsj17@michigan.gov**

CONTRACT SUMMARY

DESCRIPTION:

Student Loan Default Aversion Services - MiDEAL

INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
3 Years	**April 1, 2016**	**March 31, 2019**	**Two (2), One (1) Year Options**
PAYMENT TERMS	**F.O.B.**	**SHIPPED TO**	
N/A	**N/A**	**N/A**	

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

MINIMUM DELIVERY REQUIREMENTS

N/A

MISCELLANEOUS INFORMATION

N/A

ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION	$0.00

For the Contractor:

_____ _____

, **Date**

Contract Administrator

For the State:

_____ _____

Julie Collins, **Date**

Purchasing

State of Michigan

EXHIBIT A
STATEMENT OF WORK
CONTRACT ACTIVITIES

I. Background

This is a Contract for Student Loan Default Prevention Management Services for non-profit colleges and universities (Schools) in Michigan. These services and solutions for Schools is to assist students in borrowing responsibly and maintaining good standing in the repayment of their student loans.

II. Requirements

This Contract is for Student Loan Default Prevention Management Services to Schools in the State of Michigan (State) through the MiDEAL Program. The contractor must comply with all work and deliverables listed in this Exhibit A.

The Michigan Department of Treasury, Student Financial Services Bureau, is the main contact for this program as the Program Manager (see Standard Contract Terms).

This Contract will be 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. Contractor must supply all Contract Activities at the established Contract prices and terms of the resulting Contract to any MiDEAL Member that leverages the Contract.

III. Work and Deliverables

A. General Requirements

1. The Contractor must be able to provide Student Loan Default Prevention Management Services for Schools in Michigan.

2. The Contractor must be able to provide default aversion services from the start of the grace period through default.

3. The Contractor must provide Default Prevention Plan assistance to Schools.

4. The Contractor must have the ability to work with participating Schools to target high priority student groups. The School would only be charged for the student groups they choose to be worked/targeted**.**

5. The Contractor must be able to access school files through the National Student Loan Data System (NSLDS).

6. Reserved.

7. The Contractor must perform the following services as it pertains to the number and type of contacts made to borrowers during grace, repayment and delinquency.

   a. Grace Counseling Outreach

   1. The Contractor will send an introductory email to borrowers with valid email addresses on behalf of the School; advising of upcoming calls and emails, encouraging participation.
   2. The Contractor will make up to three outbound telephone attempts to make contact with the borrower. The three attempts will be made:

i. Within forty five (45) days of the date the Contractor is notified the student is less than half time *or*
ii. Beginning at 90 days into the grace period as designated in the file

3. If the borrower is unavailable, a toll-free number may be provided for a return call.
4. If necessary, the Contractor will employ proprietary skip tracing in an effort to locate the borrower.
5. The Contractor will send emails to borrowers with valid email addresses during the grace period at thirty (30), ninety (90), and one hundred and eighty (180) days.
6. All counseled and emailed borrowers will be provided with a toll free number for future questions; providing a lifeline to a student loan expert.
7. Borrowers are provided with access to the Contractor's Student Loan Repayment Overview website; providing detailed information on all repayment plans, useful links and helpful tips.
8. The Contractor will provide collateral to the School to assist with communicating service to student borrowers.
9. Activity reports are available online via the Contractor's website.
10. The School will select which student borrowers the Contractor will perform the Grace Outreach service to.

b. School Responsibilities: Grace Counseling Outreach

1. The school is responsible for providing the Contractor with an electronic file of accounts via the Contractor's website.
2. This file should be sent no more than weekly on a schedule agreed upon by both the School and the Contractor.
3. The School will provide a contact name, telephone number, and email address for inclusion in the introductory email and for cases where a student wishes to speak with a school representative.

c. Repayment Outreach

The Contractor's trained counselors contact student borrowers who are delinquent on their student loans to assist the borrower in resolving the delinquency. The service provides education to motivate student borrowers to take the necessary action to resolve their delinquency. Resolving delinquency sets the stage for reducing or maintaining a healthy Cohort Default Rate.

d. Repayment Outreach

1. The Contractor will retrieve and upload the School's NSLDS Delinquent Borrower Report (DELQ01) each week or on specific weeks as agreed upon by both the School and the Contractor.
2. The Contractor will load accounts within all active cohort years.
3. The Contractor will load accounts beginning with the most recent cohort year, and the prior cohort year. Additional cohort years will be added every October 1st.
4. Accounts that cannot default before the end of the active cohort years will not be loaded.
5. The Contractor will make an unlimited number of outbound calls to the borrower in an attempt to resolve all delinquent account(s).
6. If the borrower is unavailable, a toll-free number may be provided for a return call.
7. The Contractor may send emails and/or letters to the borrower in an effort to resolve delinquency.
8. Once contact is made, the Contractor will attempt to facilitate a three-way call with the borrower and servicer to resolve delinquency.

9. If necessary, the Contractor will employ proprietary skip tracing in an effort to locate the borrower.

10. For accounts that resolve and become delinquent again within 365 days of the original placement date, the Contractor will attempt to resolve the delinquency at no additional charge.

11. Performance reports are available online and are updated on a weekly basis.

12. All borrowers who are resolved by the Contractor will be offered Financial Avenue's Foundations of Money and Credit and Protecting Your Money courses. Resolved borrowers will receive an email from the Contractor with login credentials.

e. School Responsibilities: Repayment Outreach (Outcome-Based)

1. The School will set up at least two Contractor's staff members with the School's NSLDS SAIG mailbox with access to NSLDS Online Reporting (Default Services).
2. The School will schedule the NSLDS Delinquent Borrower Report (DELQ01) to be automatically created and delivered to an the Contractor/School SAIG mailbox weekly or on specific weeks as agreed upon by both School and the Contractor.
3. The School is responsible for providing the Contractor with a weekly NSLDS Delinquent Borrower Report (DELQ01) via the Contractor's website or delivered to a Contractor/School mailbox.
4. If FFELP loans are to be worked, the School is responsible for providing the Contractor with a weekly Contractor FFELP Delinquent Borrower Report via the Contractor's website.
5. The School must upload, or have delivered, the NSLDS weekly file by close of business each Friday.

8. Contractor must provide skip-tracing services at no additional cost.

9. The Contractor must have the ability to co-brand with any School which utilizes its services.

10. Reserved.

11. Reserved.

12. Reserved.

13. Reserved.

14. At a minimum, a one year Contract will be provided to all Schools which participate in the MiDEAL Program.

15. The Contractor must provide a three-way call option with the Loan Servicer to help the student understand payment opportunities.

16. If applicable, entrance and exit interviews which are performed by the Contractor must comply with all security requirements specified by the Department of Education (ED).

17. The Contractor must utilize fair debt collection practices as outlined by the ED.

18. The Contractor must have the ability to service a large number of students.

19. Reserved.

20. The Contractor shall connect with students through the use of technology.

21. The Contractor shall provide financial literacy education materials, through the use of the Contractor's Financial Avenue, to students at no additional cost to the student if provided by their School.

22. The Contractor shall work with participating Schools to effectively transition default prevention services from an existing vendor.

23. The following service shall be provided to students. It includes but is not limited to:

    a. Borrower-Centric Approach
    1. Counselors look for the option or options which help the borrower in both the long and short term.
    2. The best interest of the borrower is to make a payment.
    3. Spanish speaking counselors are provided.
    5. Forbearance or deferment will be used only when appropriate and will not be the first option considered.
    6. Unlimited telephone attempts until a borrower's delinquency is resolved or default occurs.
    7. Default aversion efforts are performed through a combination of live dialing, email, and written correspondence.
    8. The Contractor's solution utilizes email as a general/informational contact supplement between scheduled letter correspondence, and for follow-up after other forms of contact have been made with delinquent borrowers.
    9. Three-way conference calling with the borrower and servicer.
    10. Assist borrowers with the processing of deferments and forbearances.
    11. Resolved borrowers receive complimentary access to two of the Contractor's online financial literacy courses, Foundations of Money and Credit and Protecting Your Money.

24. If extended, each MiDEAL Member wishing to participate under this contract must sign an addendum to this contract with the Contractor. The purpose of the addendum is to incorporate school specific third-party servicing contract language required in the regulations at 34 C.F.R. § 668.25(c) and to appropriately report each school's contract to the Federal Student Aid's Thirty-part Servicer Oversight Unit at the U.S. Department of Education. For reporting purposes the beginning of each school's contract will be the date the authorized school official signs the addendum. The addendum will also contain file layouts for the specific service(s) the school elects to utilize.

25. Contractor will continue to remain compliant with the controls in FISMA (NIST SP800-53 revision 4/Recommended Security Controls for Federal Information Systems), FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems), FTC Gramm-Leach-Bliley Act, Massachusetts State Resolution 201 CMR 17.00, and FTC Red Flags.

B. <u>Reports</u>

1. At a minimum, Contractors must make reports available monthly to participating Schools**.**

2. The Contractor must provide industry metrics to Schools and to the State at a minimum, annually.

3. The Contractor must provide activity reporting per student to participating Schools.

4. The Contractor must supply default forecasting information to participating Schools.

5. The Contractor must supply aggregate reports to the State at a minimum annually.

6. The Contractor must annually supply the State with a list of Schools and high schools which are utilizing their services through the MiDEAL Program.

7. Additional reports which will be made available to participating Schools at no additional cost are as follows:

a. Grace Counseling

Reporting is online so Schools can quickly track the borrowers contacted, the number of phone calls made, and the number of emails sent.

b. **Activity Report:**

Provides activity details on files uploaded. For each file uploaded, the following is provided: file upload date, number of borrowers in upload, number of phone calls made and emails sent, and number of borrowers counseled. For each file uploaded, the SSN and name of each borrower included is also available to view as additional detail. There is a cumulative total for each category provided for all files uploaded and the report is available for download in Excel.

c. Default Prevention Outreach

The Contractor's online reporting system will track the progress and performance of the school's delinquent portfolio. Reports include batch level performance data displaying the number of placements and resolutions. Individual borrower account details are also provided highlighting demographics, loan details, and all delinquent efforts performed.

Schools have the ability to track up to three active cohort years. With our cohort tracking tool and the NSLDS School Portfolio report, each school can keep track of its defaulted borrowers and proactively work to remove defaulted loans prior to the year(s) closing.

d. The school will have authenticated and secure online access to these seven reports:

I. Active Report: Contains delinquent borrower information including cohort year, days delinquent, loan amount, SSN, name, address, phone, servicer information, and date of birth.

II. Performance Report: Contains details on each file uploaded including file upload date, assignment date, number of loan assignments in each upload, the current status of each assignment (Outstanding, Resolved, or Defaulted), and the resolution rate for each batch. Borrower detail is also available for each file uploaded and includes SSN, name, loan amount, date of birth, and closed date (if applicable).

III. Borrower History Report: Provides borrower demographic, loan summary, and account history information. The demographic information includes SSN, name, address, date of birth, and phone numbers from each applicable servicer. The loan summary provides a record of each loan uploaded including: servicer, days delinquent or resolved date, and loan amounts. The history section provides the last 200 contact actions performed on the borrower's account including the date/time of the activity and the activity; such as, phone calls made/received, emails sent, letters mailed, etc.

IV. Bad Address Report: Provides SSN, name, address, phone number, date of birth, and servicer for each borrower identified by the servicer as having an invalid address.

V. Cohort Activity Report: Allows schools to track their open cohort years at any time by uploading their School Portfolio report. You'll have the ability to analyze your cohort data by major, enrollment status, and campus branch. In addition, you'll be able to compare your reported less-than-halftime (LTH) status for each borrower to what NSLDS is

reporting to easily identify discrepancies. You can monitor your defaulted borrowers and proactively work to correct defaulted loans prior to the year(s) closing, ultimately avoiding the strenuous challenge process. This report contains number in repayment, number in default, number of new defaulters from the last report upload, list of defaulters that moved to good standing prior to the cohort year ending, cohort rates, the percentage one borrower impacts the rate, and how many borrowers must be saved to reduce the rate by one percent. Borrower details are also available and include SSN, name, lender, loan type, guarantee number, guarantee date, guarantee amount, amount approved, amount cancelled, repayment date, loan begin date, loan end date, servicer, grade level, loan date, LTH status, claim type, claim activity date, cohort year, and consolidation indicator. The Cohort Activity report also has a graphical output to visually display the cohort year trends and default rate curves.

Through this report, you can compare Cohort Default Rates with previous open years at the same point in time and forecast your final Cohort Default Rate once the cohort year closes.

- **Invoice Detail Report:** Contains borrower details for each monthly invoice including SSN, name, account load date, load fee, date of birth, resolution date, and resolution fee.

- **Cohort Impact Report:** Contains detail on the impact the Contractor's efforts had on accounts assigned within each cohort year including cohort year, number of accounts assigned, and the current status of each assignment (Saved, At Risk, or Defaulted). Borrower details for each are also available including SSN and name.

All reports can be run to include less or more results based on various selection criteria such as date ranges and cohort years. They are all available for download in Excel.

8. The Contractor must provide the State reports on industry metrics for each school, annual aggregate reports, and a list of schools and high schools that are utilizing services through the MiDEAL Program. Additional reports provided to the schools will be made available to the State with permission of the school(s).

9. Ad Hoc reporting must be available to participating colleges and universities upon request. Additional fees may apply.

C. <u>Customer Service</u>

1. The Contractor must assign each School a designated representative. A designated representative may be assigned to multiple colleges.

2. The Contractor's call center's days and hours of operation are Monday through Thursday 7:00 a.m. to 9:00 p.m., Friday 7:00 a.m. to 7:00 p.m., and Saturday 8:00 a.m. to 4:30 p.m. Central time.

3. The Contractor must be willing to visit and promote their services to any interested Schools.

D. <u>Training</u>

1. The Contractor must provide at a minimum the following training:
   a. On-line training or Webinars.

2. The Contractor shall provide the following training:

   To begin the process, the Contractor's Client Relations will send a welcome email introducing the Contractor's team and provide a link to a landing page which will be designed especially for the college or university. The landing page will provide detailed product information along with specifics on how to get started. The introductory email will also request scheduling an implementation conference call meeting between the school and the Contractor. This call lasts approximately one hour and will cover how to access reports, upload files, and any additional information the school needs to know to get started.

   In addition to the welcome resources and implementation call, the Contractor offers all clients access to our online Success Dashboard. Here, a school can view training videos at will, download supplemental materials, stay up-to-date with announcements, and utilize borrower communication tools for each product.

   Client support is available to all clients Monday through Friday 7:00 a.m. – 7:00 p.m. Central time by calling 888.529.2028 or by email at inceptiacs@inceptia.org.

3. The Contractor must provide In-school default management materials/resources at no additional cost.

IV. Contractor Staff, Roles, and Responsibilities

1. The following staff will be involved in the project:

   a. Matt Nettleton, Strategic Business Director
      Roles & Responsibilities: Main sales contact

   b. Maggie Hackwith, Client Relations Manager
      Roles & Responsibilities: Day-to-day client services contact

   c. David Macoubrie, Vice President of Repayment Solutions
      Roles & Responsibilities: Default Prevention expert; operations lead

   d. Tim Roethig, Call Center Director
      Roles & Responsibilities: Oversees day-to-day call center operations

   e. Inceptia's Default Prevention Counselors
      Roles & Responsibilities: Servicing higher education accounts

   f. Pam Beckmann, Director of Customer Service
      Roles & Responsibilities: Grace Counseling

   g. Carissa Uhlman, Vice President of Student Success
      Roles & Responsibilities: Financial education expert

   h. Staci Stewart, Director of Product Development and Support
      Roles & Responsibilities: Product manager

2. The Contractor's representative/Primary Contact is Maggie Hackwith, Client Relations Manager. The Contractor must notify the Contract Administrator at least 14 calendar days before removing or assigning a new Contractor Representative.

3. Reserved.

4. Reserved.

5. Reserved.

6. No subcontractors will be utilized in this Contract.

V. Project Plan

1. The Contractor will carry out this project under the direction and control of the Program Manager.

2. Within 5 working days of Contract award, the Contractor must submit to the Program Manager for final approval a project plan. Project Plan shall include:

    a. The Contractor's staffing table with names and title of personnel assigned to the project as well as any subcontractors.

VI. Authorizing Document and Invoicing

a. Authorizing Document. The appropriate authorizing document for the Contract will be a Purchase Order.
b. Payment Methods. Payment for Contract Activities will be made within 45 days of receipt of invoice.
c. Invoicing. Contractor shall invoice on a monthly.

VII. Liquidated Damages

Late or improper completion of the Contract Activities will cause loss and damage to the State and it would be impracticable and extremely difficult to fix the actual damage sustained by the State. Therefore, if there is late or improper completion of the Contract Activities the State is entitled to collect liquidated damages in the amount of $5,000 and an additional $100 per day for each day Contractor fails to remedy the late or improper completion of the Work.

EXHIBIT B - Reserved

EXHIBIT C
PRICING

1. Pricing provided shall remain firm/fixed for the duration of the Contract.
2. Services may be purchased individually or as a package.
3. The State does not guarantee a minimum or maximum volume of work.

Service Provided	**Pricing Unit**	**Price per Service**	**Additional Pricing**
Program Startup	Per School	$ FREE	
Grace Counseling	Per Borrower	$ 3.95	(see additional pricing information sheet)
Default Aversion Outreach	Per Borrower	$ 5.95 one-time load fee; $25 fee upon resolution	(see additional pricing information sheet)
Financial Literacy Program	Per School	$ FREE w/purchase of Grace and/or Default Prevention Outreach	$5,000 annually per school when purchased as a stand-alone product. Service is free to all Michigan public high schools who participate in the MiDEAL Program.

Proposed Service	Unit Price
Grace Counseling Outreach	$3.95 One-Time Fee Per Borrower Loaded

The Contractor's Grace Counseling Outreach is billed based on the actual number of new accounts loaded by the Member each month. Our clients have total control over the borrowers that are uploaded to our Grace Counseling Outreach program. This means that institutions may send all of their borrowers through Grace Counseling or they may choose to only send a portion of their borrowers.

Proposed Service	Unit Price
Default Prevention Outreach	$5.95 per Borrower Loaded $25.00 per Borrower Resolved

The Contractor charges a **one-time load fee and no other fees until the account is resolved**. This performance based pricing directly aligns our goals with yours – resolve borrower delinquency and minimize your cohort default rate.

Members will be invoiced monthly: $5.95 one-time fee for new delinquent accounts and $25.00 for each account resolved during the month. If a resolved borrower becomes delinquent again, within a twelve (12) month period of time, the Contractor will rework the account at no charge.

Our pricing is all inclusive and includes skip tracing, emails, letters, call dialer technology, telephone expenses, data security, customer service, staffing, etc.

Proposed Service	Unit Price
Financial Avenue	Free when purchased with Grace Counseling or Default Prevention services, or $5,000 annually per school when purchased as a stand-alone product. Service is free to all Michigan public high schools who participate in the MiDEAL Program.

STATE OF MICHIGAN

STANDARD CONTRACT TERMS

This STANDARD CONTRACT ("**Contract**") is agreed to between the State of Michigan (the "**State**") and the Nebraska Student Loan Program, Inc., d/b/a Inceptia, National Student Loan Program and/or NSLP **(Contractor),** a Nebraska nonprofit corporation located in Lincoln, Nebraska. This Contract is effective on April 1, 2016 ("**Effective Date**"), and unless terminated, expires on March 30, 2019.

[**Add if appropriate:** This Contract may be renewed for up to two (2) additional one (1) year period(s). Renewal must be by written agreement of the parties and will automatically extend the Term of this Contract.]

The parties agree as follows:

1. **Duties of Contractor.** Contractor must perform the services and provide the deliverables described in **Exhibit A – Statement of Work** (the "**Contract Activities**"). An obligation to provide delivery of any commodity is considered a service and is a Contract Activity.

   Contractor must furnish all labor, equipment, materials, and supplies necessary for the performance of the Contract Activities, and meet operational standards, unless otherwise specified in Exhibit A.

   Contractor must: (a) perform the Contract Activities in a timely, professional, safe, and workmanlike manner consistent with standards in the trade, profession, or industry; (b) meet or exceed the performance and operational standards, and specifications of the Contract; (c) provide all Contract Activities in good quality, with no material defects; (d) not interfere with the State's operations; (e) obtain and maintain all necessary licenses, permits or other authorizations necessary for the performance of the Contract; (f) cooperate with the State, including the State's quality assurance personnel, and any third party to achieve the objectives of the Contract; (g) return to the State any State-furnished equipment or other resources in the same condition as when provided when no longer required for the Contract; (h) not make any media releases without prior written authorization from the State; (i) assign to the State any claims resulting from state or federal antitrust violations to the extent that those violations concern materials or services supplied by third parties toward fulfillment of the Contract; (j) comply with all State physical and IT security policies and standards which will be made available upon request; and (k) provide the State priority in performance of the Contract except as mandated by federal disaster response requirements. Any breach under this paragraph is considered a material breach.

   Contractor must also be clearly identifiable while on State property by wearing identification issued by the State, and clearly identify themselves whenever making contact with the State.

2. **Notices.** All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Julie Collins 7285 Parsons Drive Dimondale, MI 48821 Collinsj17@michigan.gov 517-636-6817	Randy Heesacker 1300 O Street Lincoln, Ne 68508 Randyh@nslp.org (402) 479-6605

3. **Contract Administrator.** The Contract Administrator for each party is the only person authorized to modify any terms of this Contract, and approve and execute any change under this Contract (each a "**Contract Administrator**"):

State:	Contractor:
Julie Collins 7285 Parsons Drive Dimondale, MI 48821 Collinsj17@michigan.gov 517-636-6817	Randy Heesacker 1300 O Street Lincoln, NE 68508 Randyh@nslp.org (402) 479-6605

4. **Program Manager.** The Program Manager for each party will monitor and coordinate the day-to-day activities of the Contract (each a "**Program Manager**"):

State:	Contractor:
Kara Scheeneman 430 W. Allegan St. Lansing, MI 48922 ScheenemanK@michigan.gov 517-335-3031	Maggie Hackwith 1300 O Street Lincoln, NE 68508 inceptiacs@inceptia.org 888-529-2028 ex. 6306

5. **Performance Guarantee**. Contractor must at all times have financial resources sufficient, in the opinion of the State, to ensure performance of the Contract and must provide proof upon request. The State may require a performance bond (as specified in Exhibit A) if, in the opinion of the State, it will ensure performance of the Contract.

6. **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.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimal Limits: $1,000,000 Each Occurrence Limit $1,000,000 Personal & Advertising Injury Limit $2,000,000 General Aggregate Limit $2,000,000 Products/Completed Operations Deductible Maximum: $50,000 Each Occurrence	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.
Umbrella or Excess Liability Insurance	
Minimal Limits: $5,000,000 General Aggregate	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds.
Automobile Liability Insurance	
Minimal Limits: $1,000,000 Per Occurrence	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) include Hired and Non-Owned Automobile coverage.

Workers' Compensation Insurance	
Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimal Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimal Limits: $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.

Professional Liability (Errors and Omissions) Insurance	
Minimal Limits: $3,000,000 Each Occurrence $3,000,000 Annual Aggregate Deductible Maximum: $50,000 Per Loss	

If any of the required policies provide **claims-made** coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (c) if coverage is 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.

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.

This Section 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).

7. **Reserved.**

8. **Extended Purchasing Program.** Upon written agreement between the State and Contractor, this Contract may be extended to: (a) MiDEAL members, (b) other states (including governmental subdivisions and authorized entities), or (c) State of Michigan employees. 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.

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

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

9. **Independent Contractor.** Contractor is an independent contractor and assumes all rights, obligations and liabilities set forth in this Contract. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor

10. **Subcontracting.** Contractor may not delegate any of its obligations under the Contract without the prior written approval of the State. Contractor must notify the State at least 90 calendar days before the proposed delegation, and provide the State any information it requests to determine whether the delegation is in its best interest. If approved, Contractor must: (a) be the sole point of contact regarding all contractual matters, including payment and charges for all Contract Activities; (b) make all payments to the subcontractor; and (c) incorporate the terms and conditions contained in this Contract in any subcontract with a subcontractor. Contractor remains responsible for the completion of the Contract Activities, compliance with the terms of this Contract, and the acts and omissions of the subcontractor. The State, in its sole discretion, may require the replacement of any subcontractor.

11. **Staffing.** The State's Contract Administrator may require Contractor to remove or reassign personnel by providing a notice to Contractor.

12. **Background Checks.** Upon request, Contractor must perform background checks on all employees and subcontractors and its employees 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.

13. **Assignment.** Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

14. **Change of Control.** Contractor will notify, at least 90 calendar days before the effective date, the State of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following: (a) a sale of more than 50% of Contractor's stock; (b) a sale of substantially all of Contractor's assets; (c) a change in a majority of Contractor's board members; (d) consummation of a merger or consolidation of Contractor with any other entity; (e) a change in ownership through a transaction or series of transactions; (f) or the board (or the stockholders) approves a plan of complete liquidation. A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes.

    In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

15. **Ordering.** Contractor is not authorized to begin performance until receipt of authorization as identified in Exhibit A.

16. **Acceptance.** Contract Activities are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("**State Review Period**"), unless otherwise provided in Exhibit A. If the Contract Activities are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the Contract Activities are accepted, but noted deficiencies must be corrected; or (b) the Contract Activities are rejected. If the State finds material deficiencies, it may: (i) reject the Contract Activities without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with Section 22, Termination for Cause.

    Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Contract Activities, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Contract Activities to the State. If acceptance with deficiencies or rejection of the Contract Activities impacts the content or delivery of other non-completed Contract Activities, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

    If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may perform the Contract Activities and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

17. **Reserved.**

18. **Reserved.**

19. **Terms of Payment.** Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Contract Activities performed as specified in Exhibit A. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for the State's exclusive use. Notwithstanding the foregoing, all prices 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.

    The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Contract Activities. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

    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/cpexpress to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment.
    Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

20. **Liquidated Damages.** Liquidated damages, if applicable, will be assessed as described in Exhibit A.

21. **Stop Work Order.** The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar 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 the Contract or purchase order. The State will not pay for Contract Activities, Contractor's lost profits, or any additional compensation during a stop work period.

22. **Termination for Cause.** The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State: (a) endangers the value, integrity, or security of any location, data, or personnel; (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; (c) engages in any conduct that may expose the State to liability; (d) breaches any of its material duties or obligations; or (e) fails to cure a breach within the time stated in a notice of breach. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

    If the State terminates this Contract under this Section, 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 the 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 24, Termination for Convenience.

    The State will only pay for amounts due to Contractor for Contract Activities 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. The 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 Contract Activities from other sources.

23. **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 of the Contract Activities immediately, or (b) continue to perform the Contract Activities in accordance with Section 24, Transition Responsibilities. 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.

24. **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), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract Activities to

continue without interruption or adverse effect, and to facilitate the orderly transfer of such Contract Activities to the State or its designees. Such transition assistance may include, but is not limited to: (a) continuing to perform the Contract Activities at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Contract Activities, training, equipment, software, leases, reports and other documentation, 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 materials, data, property, and confidential information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State, at the State's discretion, all completed or partially completed deliverables prepared under this Contract as of the Contract termination date; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). This Contract will automatically be extended through the end of the transition period.

25. **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; (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); and (d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

    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 if the State deems necessary. Contractor will not, without the State's 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. To the extent that any State employee, official, or law may be involved or challenged, the State may, at its own expense, control the defense of that portion of the claim.

    Any litigation activity on behalf of the State, or any of its subdivisions under this Section, 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.

26. **Infringement Remedies.** If, in either party's opinion, any piece of equipment, software, commodity, or service supplied by Contractor or its subcontractors, or its operation, use or reproduction, is likely to become the subject of a copyright, patent, trademark, or trade secret infringement claim, Contractor must, at its expense: (a) procure for the State the right to continue using the equipment, software, commodity, or service, or if this option is not reasonably available to Contractor, (b) replace or modify the same so that it becomes non-infringing; or (c) accept its return by the State with appropriate credits to the State against Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

27. **Limitation of Liability.** The State is not liable for consequential, incidental, indirect, or special damages, regardless of the nature of the action.

28. **Disclosure of Litigation, or Other Proceeding.** Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a subcontractor, or an officer or director of Contractor or subcontractor, that arises during the term of the Contract, including: (a) a criminal Proceeding; (b) a parole or probation Proceeding; (c) a Proceeding under the Sarbanes-Oxley Act; (d) a civil Proceeding involving: (1) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or (2) a governmental or public entity's claim or written allegation of fraud; or (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

29. **Reserved.**

30. **State Data.**

    a. Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes: (a) the State's data collected, used, processed, stored, or generated as the result

of the Contract Activities; (b) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Contract Activities, 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, (c) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Contract Activities, which is defined under the Health Insurance Portability and Accountability Act (HIPAA) and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This Section survives the termination of this Contract.

b. Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Contract Activities, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Contract Activities. 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 Contract Activities, 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 survives the termination of this Contract.

c. Extraction of State Data. Contractor must, within five (5) business days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of the State Data in the format specified by the State.

d. Backup and Recovery of State Data. Unless otherwise specified in Exhibit A, Contractor is responsible for maintaining a backup of State Data and for an orderly and timely recovery of such data. Unless otherwise described in Exhibit A, Contractor must maintain a contemporaneous backup of State Data that can be recovered within two (2) hours at any point in time.

e. Loss of Data. In the event of any act, error or omission, negligence, misconduct, or breach 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) 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 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) 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 expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (g) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and, (h) provide to the State a detailed plan within 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, 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. This Section survives the termination of this Contract.

31. **Non-Disclosure of Confidential Information**. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. The provisions of this Section survive the termination of this Contract.

    a. Meaning of Confidential Information. For the purposes of this Contract, 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: (a) 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). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

    b. 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 a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; and (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor or any subcontractor may be required to execute a separate agreement to be bound by the provisions of this Section.

    c. 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 and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

    d. 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.

    e. Surrender of Confidential Information upon Termination. Upon termination of this Contract or a Statement of Work, in whole or in part, each party must, within 5 calendar 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; provided, however, that Contractor must return State Data to the State following the timeframe and procedure described further in this Contract. Should Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and must certify the same in writing within 5 calendar days from the date of termination to the other party.

32. **Data Privacy and Information Security**.

    a. 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 employees, agents, and subcontractors of Contractor, if any, 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 to Contractor upon request.

b. Audit by Contractor. No less than annually, Contractor must conduct a comprehensive independent third-party audit of its data privacy and information security program and provide such audit findings to the State.

c. 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 Contract Activities and from time to time during the term of this Contract. During the providing of the Contract Activities, 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 45 calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

d. Audit Findings. Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

e. State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or a 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.

33. **Reserved.**

34. **Reserved.**

35. **Records Maintenance, Inspection, Examination, and 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 the Contract through the term of the Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Audit Period, Contractor must retain the records until all issues are resolved.

    Within 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 Contract Activities are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If any 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 the Contract must be paid or refunded within 45 calendar days.

    This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

36. **Warranties and Representations.** Contractor represents and warrants: (a) Contractor is the owner or licensee of any Contract Activities that it licenses, sells, or develops and Contractor has the rights necessary to convey title, ownership rights, or licensed use; (b) all Contract Activities are delivered free from any security interest, lien, or encumbrance and will continue in that respect; (c) the Contract Activities will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party; (d) Contractor must assign or otherwise transfer to the State or its designee any manufacturer's warranty for the Contract Activities; (e) the Contract Activities are merchantable and fit for the specific purposes identified in the Contract; (f) the Contract signatory has the authority to enter into this Contract; (g) all information furnished by Contractor in connection with the Contract fairly and accurately represents Contractor's business, properties, finances, and operations as of the dates covered by the information, and Contractor will inform the State of any material adverse changes; and (h) all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading. A breach of this Section is considered a material breach of this Contract, which entitles the State to terminate this Contract under Section 22, Termination for Cause.

37. **Conflicts and Ethics.** Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of

impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

38. **Compliance with Laws.** Contractor must comply with all federal, state and local laws, rules and regulations.

39. **Reserved.**

40. **Reserved.**

41. **Nondiscrimination.** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq*., Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, or mental or physical disability. Breach of this covenant is a material breach of this Contract.

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

43. **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 Michigan Court of Claims. Contractor consents to venue in Ingham County, and waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint agents in Michigan to receive service of process.

44. **Non-Exclusivity.** Nothing contained in this Contract is intended nor will 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 Contract Activities from other sources.

45. **Force Majeure.** Neither party will be in breach of this Contract because of any failure arising from any disaster or acts of god that are beyond their control and without their fault or negligence. Each party will use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors. If immediate performance is necessary to ensure public health and safety, the State may immediately contract with a third party.

46. **Dispute Resolution.** The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

    Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely, or fails to respond within 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 does not limit the State's right to terminate the Contract.

47. **Media Releases.** News releases (including promotional literature and commercial advertisements) pertaining to the Contract or project to which it relates must not be made without prior written State approval, and then only in accordance with the explicit written instructions of the State.

48. **Website Incorporation.** The State is not bound by any content on Contractor's website unless expressly incorporated directly into this Contract.

49. **Order of Precedence.** In the event of a conflict between the terms and conditions of the Contract, the exhibits, a purchase order, or an amendment, the order of precedence is: (a) the purchase order; (b) the amendment; (c) Exhibit A; (d) any other exhibits; and (e) the Contract.

50. **Severability.** If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

51. **Waiver.** Failure to enforce any provision of this Contract will not constitute a waiver.

52. **Survival.** The provisions of this Contract that impose continuing obligations, including warranties and representations, termination, transition, insurance coverage, indemnification, and confidentiality, will survive the expiration or termination of this Contract.

53. **Entire Contract and Modification.** This Contract is the entire agreement and replaces all previous agreements between the parties for the Contract Activities. This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Notice**").

Exhibit 1
Security Requirements

On award of the Contract, the Contractor must comply with State and Federal statutory and regulatory requirements, and rules; National Institute of Standards and Technology (NIST) publications; Control Objectives for Information and Related Technology (COBIT); all other industry specific standards; national security best practices and all requirements herein.

The Contractor must perform annual testing of all security control requirements to determine they are working as intended. Annual certification must be provided in writing to the Contract Compliance Inspector (CCI) or designee in the form of a SSAE16 or similar audit report, or as requested by the CCI.

0

A. Governing Security Standards and Publications

1 The State of Michigan information is a valuable asset that must be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised.

The Contractor must collect, process, store, and transfer Department of Treasury personal, confidential or sensitive data in accordance with the contractual agreement, State of Michigan policies and the laws of the State of Michigan and the United States, including but is not limited to the following:

1. The Michigan Identity Theft Protection Act, MCL 445.61 et seq;
2. The Michigan Social Security Number Privacy Act, MCL 445.82 et seq.
3. Family Educational Rights and Privacy Act
4. National Institute of Standards and Technology 800-53 v4
5. State of Michigan Policies: The Contractor must comply with the State of Michigan information technology standards (http://www.michigan.gov/dmb/0,4568,7-150-56355-108233--,00.html).

   Note: Contractor has its own architecture and although there is some overlap, Contractor uses some products other than those requested in the Michigan IT standards. Contractor meets Hardening Standards with NIST. Exceptions to the Michigan information technology standards are noted in Exhibit 3.

B. Security Risk Assessment

The Contractor must conduct assessments of risks and identify the damage that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Department of Treasury. Security controls should be implemented based on the potential risks. The Contractor must ensure that reassessments occur whenever there are significant modifications to the information system and that risk assessment information is updated.

C. System Security Plan

The Contractor must develop, document, and implement a security plan that provides detailed security controls implemented in the information system. If a security plan does not exist, the contractor shall provide a description of the security controls planned for implementation. The security plan must be reviewed periodically and revised to address system/organizational changes or problems.

D. Network Security

The Contractor is responsible for the security of and access to Department of Treasury data, consistent with legislative or administrative restrictions. Unsecured operating practices, which expose other connected networks to malicious security violations, are not acceptable. The Contractor must

coordinate with the Michigan Department of Technology, Management and Budget to enter the proper pointers into the State of Michigan infrastructure.

E. Data Security

The Contractor has the responsibility to protect the confidentiality, integrity, and availability of State of Michigan data that is generated, accessed, modified, transmitted, stored, disposed, or used by the system, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

The Contractor must:

1. process the personal data in accordance with the personal data protection laws of the State of Michigan and the United States.

2. have in place appropriate technical and organizational internal and security controls to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. Technical and organizational security controls must be implemented that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing.

3. provide secure and acceptable methods of transmitting personal, confidential or sensitive information over telecommunication devices such as data encryption (128 bit minimum), Secure Socket Layer (SSL), dedicated leased line or Virtual Private Network (VPN).

4. supply the Department of Treasury, Security Division with information associated with security audits performed in the last three years.

A. 5. have in place procedures so that any third party it authorizes to have access to the personal data, including processors, will respect and maintain the confidentiality, integrity, and availability of the data.
B.
6. process the personal, confidential and sensitive data only for purposes described in the contract.

7. identify to the Department of Treasury a contact point within its organization authorized to respond to enquiries concerning processing of the personal, confidential or sensitive data, and will cooperate in good faith with the Department.

8. not disclose or transfer the personal, confidential or sensitive data to a third party unless it is approved under this contract.

9. not use data transferred by the Department of Treasury as a result of this contract for marketing purposes.

F. Media Protection

1. The Contractor must implement measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media containing Department of Treasury's personal, confidential and sensitive information to prevent the loss of confidentiality, integrity, or availability of information including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output.

2. The Contractor must ensure that only authorized users have access to information in printed form or on digital media removed from the information system, physically control and securely store information media, both paper and digital, restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

G. Media Destruction and Disposal

1. The Contractor must sanitize or destroy information system digital media containing personal, confidential or sensitive information before its disposal or release for reuse to prevent unauthorized individuals from gaining access to and using information contained on the media.

2. Personal, confidential or sensitive information must be destroyed by burning, mulching, pulverizing or shredding. If shredded, strips should not be more than 5/16-inch, microfilm should be shredded to affect a 1/35-inch by 3/8-inch strip, and pulping should reduce material to particles of one inch or smaller.

3. Disk or tape media must be destroyed by overwriting all data tracks a minimum of three times or running a magnetic strip over and under entire area of disk at least three (3) times. If the CD, DVD or tape cannot be overwritten it must be destroyed in an obvious manner to prevent use in any disk drive unit and discarded. Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal. Electronic data residing on any computer systems must be purged based on retention periods required by the Department of Treasury.

H. Access Control

The Contractor must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. Access must be immediately removed when a staff changes job duties or leaves the employment.

Authentication Process

Authentication is the process of verifying the identity of a user. Authentication is performed by having the user enter a user name and password in order to access the system.

To help protect information from unauthorized access or disclosure, users must be identified and authenticated per the table below prior to accessing confidential or sensitive information, initiating transactions, or activating services.

Publicly available information such as the mother's maiden name, birth date, and address as the sole authenticator is not a secure means of authentication and should not be used.

Automatic user logons are prohibited. Device-to-device logons must be secured (preferably using client certificates or password via tunneled session). For certain implementations, source restrictions (sign-on can occur only from a specific device) provide a compensating control, in addition to the ID and password.

Authentication information (e.g., a password or PIN) must never be disclosed to another user or shared among users.

The authentication process is limited to three (3) unsuccessful attempts and must be reinstated by the authorized personnel (preferably the System security Administrator). User accounts should be systematically disabled after 90 days of inactivity and must be deleted after 1 year of inactivity

Password Requirements

The purpose of a password is to authenticate a user accessing the system and restrict use of a userID only to the assigned user. To the extent that the functionality is supported within the technology or product, the controls listed must be implemented.

These following controls or content rules apply at any point where a new password value is to be chosen or assigned. These rules must be enforced automatically as part of a new password content checking process:

Password Property	Value
Minimum Length	8 characters with a combination of alpha, numeric and special characters
Composition	• At least two numeric characters (0 through 9), neither of which may be at the beginning or the end of the password • A combination of two upper (A through Z) and lower case (a through z) letters • Special characters (!, @, #, $, %, ^, &, *, (,), +, =, /, <, >, ?,., :, ;, \) • UserID in password is not allowed
Expiration Requirement (Maximum Password Age):	90 days
Revocation	Passwords should be revoked after three (3) failed attempts. (Treasury strongly supports password revocation after three failed attempts if system allows) Passwords should be systematically disabled after 90 days of inactivity to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods.
Temporary passwords	• Must be randomly chosen or generated • System must force the user to change the temporary password at initial login
Change process	System must force user to: • Confirm their current password/PIN, • Reenter current password/PIN • Create a new password/PIN • Reenter new password/PIN System must prevent users from being able to consecutively change their password value in a single day (The goal is to prevent recycling through password history records to reuse an earlier-used password value)
Login process	Password/PIN must not appear on the screen during the login process (The exception to this is during selection of a machine-generated password).
Encryption of passwords/PINs	Passwords must be stored and transmitted with a minimum of 128-bit encryption. Passwords must be masked when entered on any screen
Compromise of password/PIN	Must be changed immediately
Forgotten password/PIN	Must be reset by authorized person (system Security Administrator)
Current user password/PIN	Must not be maintained or displayed in any readable format on the system
Audit logs	Maintain a record of when a password was changed, deleted, or revoked. The audit trail shall capture all unsuccessful login and authorization attempts for a one year period.
Password history	Keep a password history and perform a check against the history to verify the password has not been used for a minimum

	of one year
Privileged account access (e.g. supervisor or root)	Security administrator must change the password for that account immediately when user changes responsibilities

I. System Security Application Control

Application controls apply to individual computer systems and may include such controls as data origin, input controls, processing controls, output controls, application access controls, application interfaces, audit trail controls, and system documentation. Application controls consist of mechanisms in place over each separate computer system to ensure authorized data is processed completely, accurately, and reliably. The contractor is responsible for ensuring application controls are in place and functioning properly within their organization. Ongoing testing and reporting of controls must be part of the business process in order to have a solid understanding of risks, strengths and weaknesses. A comprehensive solution is required to ensure that business critical applications are handled efficiently and are prioritized. Dynamic recovery procedures and fail over facilities shall be incorporated into the scheduling process whenever possible; and where manual processes are needed, extensive tools must be available to minimize delays and ensure critical services are least impacted.

J. System Auditing

The Contractor must (i) create, protect, and retain information system audit log records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

The Contractor must observe the following guidelines regarding system auditing:

1. Audit record should contain the following:

   a. date and time of the event
   b. subject identity
   c. type of event
   d. how data changed
   e. where the event occurred
   f. outcome of the event.

2. System alerts if audit log generation fails

3. System protects audit information from unauthorized access

4. Audit record should be reviewed by individuals with a “need to know” on a regular basis

5. Audit logs are retained for sufficient period of time.

K. Configuration Control and Management

The configuration management policy and procedures must be consistent with applicable federal laws, directives, policies, regulations, standards and guidance.

L. Incident Reporting

1. The Contractor must notify any security incidents and/or breaches to the CCI within 24 hours and incidents threatening aspects of physical or financial security relevant to this contract and the systems which support it within 24 hours. [see Exhibit 2, Form 4621 What is an Incident? (brochure)].

2. The Contractor must have a documented and implemented Incident Response Policy and Procedure

3. The Contractor must have an incident handling form for consistent, repeatable process for monitoring and reporting when dealing with incidents.

4. The Contractor must have an incident response resource identified to assist users in handling and reporting incidents.

5. Personnel trained in their incident response roles and responsibilities at least annually.

M. Physical and Environmental Security

The Contractor must have established physical and environmental security controls to protect systems, the related supporting infrastructure and facilities against threats associated with their physical environment.

1. The Contractor must have established environmental protection for magnetic and other media from fire, temperature, liquids, magnetism, smoke, and dust.

2. The Contractor must control all physical access points to facilities containing information systems (except those areas within the facilities officially designated as publicly accessible), review physical security logs periodically, investigate security violations or suspicious physical access activities, and initiate remedial actions.

3. The Contractor must periodically review the established physical and environmental security controls to ensure that they are working as intended.

N. Disaster Recovery and Business Continuity Plan

The Contractor must have developed, periodically update, and regularly test disaster recovery and business continuity plans designed to ensure the availability of Department of Treasury's data in the event of an adverse impact to the contractors information systems due to a natural or man-made emergency or disaster event.

O. Security Awareness Training

The Contractor must ensure their staff having access to Treasury information are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security identified in Section A of this document, and ensuring that personnel are trained to carry out their assigned information security related duties.

Contracted employees must obtain Department of Treasury provided security awareness training. (On-line training to be identified by the CCI).

P. Web Application Security

The Contractor shall have established adequate security controls for web application(s) to provide a high level of security to protect confidentiality and integrity of personal, confidential and sensitive data. The controls include, but are not limited to:

1. Secure coding guidelines to ensure that applications are not vulnerable to, at a minimum, the following:

   - Injection flaws, particularly SQL injection, OS command injection, LDAP and Xpath injections
   - Buffer overflow
   - Insecure cryptographic storage
   - Insecure communications
   - Improper error handling

- Cross-site scripting (XSS)
- Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)
- Cross-site request forgery (CSRF).

2. Authentication
3. Authorization and access control
4. Web application and server configuration (e.g., patch management, deletion of unnecessary services, separation of the operating system and the web server)
5. Session management (e.g., randomly generate unique session IDs, encrypt sessions, enforce session expiration date, establish time-out setting for inactive session)
6. Input validation (e.g., avoid shell commands, system calls, and malicious codes),
7. Encryption (e.g., personal, confidential and sensitive data, encryption keys, passwords, shared secret),
    a. The system shall use SSL (128 bit or higher) for secure communication between the user's browser and the system. SSL will be utilized for:

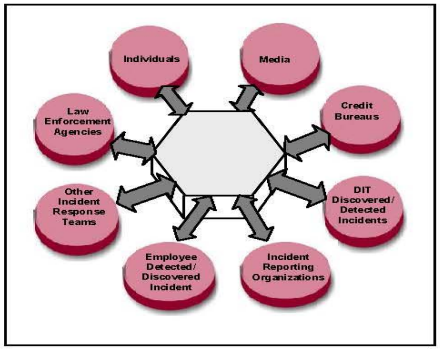
        i. Log-on process (authentication information -UserID and passwords)
        ii. Specific field in the HTML forms and links (URLS) within the pages.
        iii. Cookies
        iv. Session id
        v. Confidential and sensitive data files
        vi. Encryption keys, certificates, and passwords
        vii. Audit log file.
8. Audit logs (e.g., all authentication and authorization events, logging in, logging out, failed logins).

Exhibit 2
Form 4621, What Is An Incident (Brochure)

Exhibit 2

Identifying/Sensitive Information on Mobile Devices and Portable Media; also refer to Treasury Policy ET-03169 Data Security).

- Avoid sending or receiving unencryped confidential, personal or sensitive information via e-mail.
- Avoid sending confidential, personal or sensitive information via fax.
- Secure confidential, personal or sensitive papers on the fax, printer or copy machines.
- Keep conversations at a volume level and/or in a location that will protect information.
- Back up data on a regular basis; make sure data files from an approved portable device are stored on the network server.
- Never store more data than needed.
- Shred documents with confidential, personal or sensitive information (see Treasury Policy ET-03115 Confidential Information, Handle and Discard).
- Have computers and hard drives properly wiped or overwritten when discarding or transferring (see DIT Procedure 1350.90, Secure Disposal of Installed and Removable Digital Media, and Treasury Policy ET-03169).
- Use a log-in password that is not easily guessed. Make it at least eight characters long, composed of upper- and lower-case letters, numbers and symbols such as "#" (see DIT Standard 1310.03, Active Directory Password, and Treasury Policy ET-03175 Passwords).
- Never set any log-in dialog box to remember your password (see Treasury Policy ET-03175 Passwords).
- Use a password-protected screen saver that comes on after a few minutes of inactivity. Initiate screen lock system (if a Treasury employee, press the key with Microsoft Windows logo and "L" on the keyboard) when you leave your office, even for a short period.
- Limit access to confidential, personal or sensitive information to those who need to use it to perform their job duties (see DIT Policy 1335.00, Informative Access Control, and Treasury Policy ET-03164 Access Control).



See the following guidelines in the Security Guide for more information:

- ET-03180, Incident Reporting
- BT-03084, Security Breach Involving Personal Information
- PT-03253, Incident Reporting and Handling
- CT-03070, Incident/Security Breach Examples
- DIT Operating Procedure, How to Handle a Breach of Personal Identifiable/Sensitive Information Incidents

Other References:

- BT-03049, Employee Conduct, General Guidelines
- ET-03140, Workplace Safety
- PT-03246, Potential Dangerous Taxpayer/Debtor, Report
- PT-03095, Theft or Irregularities in Public Funds/ Property or Violations of Departmental Policies and Procedures, Report and Investigate

Contact Information:

Contact Division/Bureau Security Liaison or the Security Division at (517) 636-4081 with any questions.

4621 (Rev. 5-09)

What is an Incident?
What is a Security Breach?

What must I do?
How should it be handled?

What is an Incident?

An incident is any event threatening some aspects of physical or financial security, when financial resources or items valued at $100 or more are missing or misused, any event violating confidentiality or privacy of information, where data is manipulated or missing, or any event involving unauthorized or unlawful activity.

Examples of Incidents:

- Missing computer equipment containing non-personal information.
- Missing briefcase that contains non-personal information.

Examples of Material Incidents:

- Missing laptop computer or other mobile device, portable media or paper records that do not contain Treasury personal information but do contain confidential or sensitive information.
- Missing warrant stock.

What makes an incident a Security Breach?

An incident becomes a security breach when an unauthorized person gains access to or acquires:

1. Unencrypted or unredacted (data not altered or truncated) personal information, or
2. The encryption key to an area storing personal information.

Beware: If personal information is discovered during the investigative process, an incident will become a potential security breach.

Examples of a Potential/Actual Security Breach:

- Missing laptop computer or other mobile device, or portable media that contains Treasury personal information.
- Missing paper records that contain personal information

Page 1 of 2

Exhibit 2

- Accessing personal information when there is no business need for it
- Using another individual's User ID and Password to access personal information
- Stealing Treasury records that include personal information
- Hacking into records containing Treasury personal information
- Obtaining Treasury personal information from employees without proper authorization to access the information
- Unauthorized and unescorted persons entering secure areas that house personal information.
- Theft of a server.

What is personal information?

The Identify Theft Protection Act, Public Act 452 of 2004, as amended, defines personal information as information containing the first name or initial of the first name and the last name **along with** one of the following:

1. Social Security number
2. Driver's License number or State Personal Identification card number
3. Account number; Credit or Debit Card number **in combination with** any required security code, access code or password that would permit access to a person's financial account.

Personal information may be in written or printed form or may reside electronically on devices or media such as mainframes, servers, personal computers (desktops and laptops), CDs, DVDs, tapes, flash drives, memory sticks, USB keys, microfiche, PDAs, Blackberrys, cell phones, or may exist on other state-of-the-art devices that have been or may be developed.

What should I do if my laptop is missing or if an incident is suspected?

Employee must:

1. File a report with local police immediately if asset valued at $100 or more is missing.
2. Notify immediate supervisor no later than beginning of the next business day.
3. Complete Parts 1 and 2 of *Incident Report* (Form 4000*.) This form is available on Treasury's Intranet.
4. Forward the Incident Report (with attached police report if applicable) to immediate supervisor and a copy to Treasury's Security Division.

Management Staff must:

1. Report the incident immediately through the chain of command to the Treasury Division Administrator and the Security Division, if unreported. If personal information is involved, follow the guidelines for Security Breach.

Exception: If another state agency/governmental entity, report incident to Treasury Disclosure Officer, Technical Services Division and the Security Division. If contractor or vendor, report incident to Contract Compliance Inspector and Security Division.

2. The Division Administrator must notify the Bureau Director if it is a material incident or involves non-Treasury information.
3. The Bureau Director must notify the other entity immediately.
4. The Division Administrator must inform the Department of Information Technology (DIT) Agency Services (Treasury) Director right away if incident involves information technologyresources.
5. Notify other Treasury divisions/offices that may be affected or should be involved with investigation.
6. The Disclosure Office must notify the IRS Office of Safeguards if Federal tax information is involved.
7. Investigate and resolve the incident.
8. Prepare the final form 4000 and submit it to Treasury's Security Division.

What should I do if I witness, discover, or am informed of a potential security breach?

Employee must:

1. Report the security breach immediately (no later than beginning of the next business day) to immediate supervisor.
2. Complete Parts 1 and 2 of Form 4000.
3. Forward the Incident Report (with attached police report if applicable) to immediate supervisor and a copy to Treasury's Security Division.

Management Staff must:

1. If the breach is ongoing, **CONTAIN IT.**
2. Report the potential breach immediately through the chain of command to the Bureau Director or Deputy Treasurer, whichever is applicable.
3. The Bureau Director or the Deputy Treasurer, whichever is applicable, must notify the Chief Deputy Treasurer immediately if a breach involving a database of personal information.
4. The Bureau Director must notify the other entity if the potential breach involves non-Treasury information.
5. The Division Administrator must inform the DIT Agency Services (Treasury) Director right away if incident involves information technology resources and personal information.
6. The Disclosure Office must notify the IRS Office of Safeguards if Federal tax information is involved.
7. Convene appropriate personnel so the scope of the breach can be determined and a plan for appropriate action can be agreed upon.
   Note: If a database of personal information is involved, the Chief Deputy Treasurer must approve the Plan of Action.
8. If appropriate, issue breach notifications by telephone, in writing, on the Web or by email.
9. Notify the three major credit bureaus of the breach if more than 1,000 residents of the State of Michigan will receive or have received breach notifications.
10. Prepare the final form 4000 and submit it to Treasury's Security Division.

*Another entity may substitute its internal form for form 4000 if pertinent information is included.

Treasury must protect personal information against risks such as unauthorized access, modification or loss with reasonable security safeguards. Some safeguards are:

- Do not store confidential, personal or sensitive Treasury information on mobile devices or portable media (including laptops, notebooks, memory sticks, CDs, DVDs, floppies) unencrypted: ENCRYPT files or the full disk. (Refer to DIT Standard 1340, Storing and Managing Personal

Exhibit 3
Michigan Information Technology Standards Exceptions

The Contractor's security standards meet all the State of Michigan Information Technology Standards with the exception of the specific items noted below.

Client and Office Suite	NSLP/Inceptia Standard
Office Suite	Mozilla Firefox 38.2.1, Google Chrome, Adobe Acrobat DC
Collaboration Portal Technology	
Collaboration	SharePoint 365
Collaboration – Audio Conferencing	Citrix Goto Meeting
Document Management	SharePoint 365
Data and Development Technology	
Database	MySQL
Database Tools	MySQL Workbench 6.3
Reporting Tools	Jasper Reports
Version Control	MS Team Foundation Server 2008, Git
Platform Technologies	
Server Platform	Dell PowerEdge various generations, HP Proliant various generations
Service Automation Technologies	
Job Schedulers	SCCM 2012R2
Monitoring Tools	SCCM 2012R2, WSUS Services, OpenNMS 1.15, Solarwinds Log & Event Monitoring
Storage and Backup Technologies	
Backup Management Software	CA Arcserv 16.x
Enterprise Fiber Channel Disk	HP SAN P2000G
Tape Libraries/Backup Storage	HP/Compaq MSL5000