DELAWARE DEPARTMENT OF TRANSPORTATION

State of Delaware

Request for Proposal

Title:

DelDOT Drug and Alcohol Program – FMCSA- Compliant Employee Assistance Services for CDL and Safety-Sensitive Personnel

Agreement Number: **2157S**

- Deadline to Respond –

Thursday, July 10, 2025

PRIOR TO 2:00 P.M. Local Time

Issued by:

State of Delaware
DEPARTMENT OF TRANSPORTATION
Administration Building
Contract Administration
800 Bay Road, Dover, DE 19901

Questions must be submitted before the due date identified in the Procurement Schedule for this RFP. All inquiries must be submitted in the Q/A section of the project listing in the Bonfire Procurement Portal.

The Department's response to questions will be posted, according to the procurement schedule, under the project listing in Bonfire and to the State of Delaware Bid Solicitation Directory Website: http://bids.delaware.gov/.

2157 DelDOT Drug and Alcohol Program – FMCSA- Compliant
Employee Assistance Services for CDL and Safety-Sensitive Personnel

ALL AUTHORIZED SERVICE PROVIDERS:

The enclosed packet contains a "REQUEST FOR PROPOSAL" consisting of the following documents:

Table of Contents

REQUIRED BID DOCUMENTS: *(**MUST** be completed and returned with your bid)*

APPENDIX A – REQUIRED DOCUMENTS
APPENDIX B – BID PAGE
APPENDIX C – BUSINESS ASSOCIATE AGREEMENT
APPENDIX D – RESPONSE EXCEPTION FORM
APPENDIX E – CYBER RESPONSIBILITIES, LIABILITY AND INSURANCE
APPENDIX F – STATE OF DELAWARE SECURITY POLICY
APPENDIX G – STATE OF DELAWARE CLOUD TERMS AND CONDITIONS

All above documents are made part of this solicitation and are contained within this file, or available for download at the following site: https://deldot.bonfirehub.com/portal/.

In order for your response to be considered, the REQUIRED PROPOSAL DOCUMENTS must be complete and correct and submitted electronically through Bonfire (https://deldot.bonfirehub.com/portal/).

PROJECT INFORMATION

The Delaware Department of Transportation (DelDOT) is issuing this Request for Proposal (RFP) to procure a qualified vendor to provide a specialized Employee Assistance Program (EAP) designed to support employees—particularly those in safety-sensitive positions—who are struggling with substance abuse issues. This initiative is essential to maintaining compliance with U.S. Department of Transportation (DOT) and Federal Motor Carrier Safety Administration (FMCSA) regulations.

The EAP will serve roughly 500 Commercial Driver's License (CDL) holders and roughly 1,200 safety-sensitive employees across DelDOT's operational divisions. The program must adhere to the regulatory requirements outlined in 49 CFR Part 40 and Part 382, ensuring that services provided—including confidential assessments, counseling, SAP evaluations, substance use disorder treatment, return-to-duty protocols, and follow-up testing—meet the highest standards of compliance and care.

Through this dedicated EAP, DelDOT aims to enhance employee well-being, uphold federal safety mandates, and maintain a drug- and alcohol-free workplace that supports recovery and professional accountability.

PROJECT DESCRIPTION

This Scope of Work (SOW) outlines the requirements for providing the Delaware Department of Transportation (DelDOT) with an Employee Assistance Program (EAP) that focuses on drug and alcohol support services. The objective is to offer confidential counseling, referrals, and resources to assist employees with substance abuse issues.

Given the increasing concern over employee well-being and productivity, DelDOT seeks to implement a comprehensive EAP to address drug and alcohol-related challenges among its workforce.

The goal is to deliver a confidential and accessible EAP that provides support and resources to employees facing drug and alcohol issues, including the following objectives:

- Improve employee health and productivity.
- Reduce absenteeism and turnover related to substance abuse.
- Promote a supportive and stigma-free work environment.

DelDOT maintains a critical transportation infrastructure and public safety mission, necessitating strict adherence to federal drug and alcohol testing standards. The selected vendor will provide comprehensive services that meet all FMCSA and DOT mandates and support timely and effective return-to-duty outcomes.

SERVICES REQUIRED

Comprehensive Assessment and Evaluation:

- Conduct initial assessments to identify substance use issues and mental health concerns, in alignment with 49 CFR Part 40 requirements.
- Provide detailed evaluations and determine the need for specialized treatment for employees.

Confidential Counseling Services:

- Individual Counseling: Delivered by licensed Substance Abuse Professionals (SAPs) trained in substance use disorders, available in-person, by telehealth video, or phone.
- Group Therapy: Support groups available in-person and via telehealth, fostering shared experiences and mutual support.

Crisis Intervention and Support:

- 24/7 crisis hotline for immediate assistance and urgent intervention.
- Up to three (3) counseling sessions per problem (e.g., substance use, mental health concerns) per contract term, confidentiality, and service access standards per 49 CFR Part 40 Subpart P.

Substance Use Disorder Treatment:

- Access to evidence-based treatment, including outpatient, intensive outpatient (IOP), and inpatient rehabilitation services, consistent with return-to-duty and SAP recommendations per 49 CFR Part 40 Subpart O.

Prevention and Education Programs:

- Workshops and seminars on substance abuse prevention, coping strategies, and healthy lifestyles.

Family Support Services:

- Counseling and support programs for family members of affected employees.
- Access to up to three (3) sessions per issue (e.g., substance use, mental health concerns) per contract term, ensuring holistic support.

Relapse Prevention and Aftercare:

- Follow-up services post-treatment, including ongoing counseling and support groups.
- SAP to determine duration and nature of follow-up treatment per 49 CFR §40.309.

Workplace Policies and Compliance:

- Guidance on maintaining compliance with DOT/FMCSA drug and alcohol testing regulations, with a focus on CDL and safety-sensitive positions.

Referral Services:

- Access to a comprehensive referral network for specialized treatment programs and rehabilitation centers.

Wellness Programs:

- Holistic wellness initiatives supporting mental and physical health, stress management, and resilience building.
- Access to three (3) to six (6) sessions per issue (e.g., substance use, mental health concerns) annually, in line with EAP best practices.

Substance Abuse Professional (SAP) Services:

- Provide access to DOT-qualified SAPs as defined in 49 CFR Part 40 Subpart O.
- SAPs must meet DOT credentialing and training under 49 CFR §40.281 and provide certification and continuing education compliance.
- Manage assessments, treatment plans, follow-ups, and return-to-duty documentation.
- Coordinate with Drug and Alcohol Program Manager (DAPM) and treatment providers to manage referrals and track compliance.
- Assign a liaison with FMCSA regulatory knowledge to handle all SAP-related case management.

Coordination With DAPM:

- Establish communication protocols and shared responsibilities for tracking return-to-duty and follow-up testing under 49 CFR §40.305.
- Ensure timely, compliant documentation is shared with DAPM and other relevant parties.

Case Management and Reporting:

- Oversee end-to-end case management for DOT violations.
- Maintain records and support FMCSA Clearinghouse reporting per 49 CFR §382.705.
- Provide compliance metrics and utilization reports quarterly and annually.

Confidentiality and Data Security:

- Ensure adherence to HIPAA and 49 CFR confidentiality rules.
- Implement secure data storage and controlled access protocols.

Eligibility Requirements:

- Demonstrated experience providing DOT-compliant SAP and EAP services to public sector or transportation clients.
- Access to a national network of certified SAPs.
- A dedicated liaison with a minimum of three years' experience in DOT/FMCSA drug and alcohol program management, including SAP coordination and return-to-duty processes.
- The liaison must possess in-depth knowledge of 49 CFR Part 40 and Part 382, and demonstrate capability in quality assurance, including conducting case audits, ensuring compliance with federal guidelines, standardizing documentation procedures, and improving service delivery through feedback and review cycles.

Proposal Evaluation Criteria:

- Compliance with 49 CFR regulations
- SAP network strength and availability
- Case management system and reporting capabilities
- Staff qualifications and experience
- Cost effectiveness and pricing model
- Quality and relevance of the proposed liaison:
- Demonstrated experience in DOT/FMCSA program coordination
- Proven quality assurance capabilities (auditing, documentation, compliance tracking)

- Depth of regulatory knowledge (49 CFR Part 40 and 382)
- Communication and coordination effectiveness with DAPM and SAPs

Evaluation and Feedback Mechanisms:

- Program Evaluations: These evaluations will assess the program's effectiveness, collect feedback from employees on their experiences, continuously improve the services, and identify immediate challenges or gaps in service delivery. The recommendation for Program Evaluations: Evaluation after the first three (3) months of service. Quarterly Evaluation (4 times a year), to track the continued effectiveness of the program over time and identify any issues or trends. Annual Evaluation; A detailed review of the program's overall success.
- Vendor shall meet all Delaware Department of Technology and Information (DTI) standards and policies as specified here: https://dti.delaware.gov/information/standards- policies.shtml

Additional Administrative Services:

- Web Access: 24/7 access to an EAP website for employees, offering additional resources and support.
- Telephonic Management Consultation: Ongoing consultation with management and supervisors to address issues that arise within the workplace regarding employee substance use.
- Designated Account Management: Providing EAP administrative expertise for ongoing coordination and program management.
- Printed and Electronic Materials: Providing standard printed communication materials and additional promotional materials in electronic format to raise awareness and ensure utilization of the program.
- Quarterly Utilization Reports: Providing the organization with insights into program usage, helping to assess how effectively the program is being utilized.

Additional Considerations:

- DOT Compliance: Services must be designed to ensure that they are in full compliance with DOT/FMCSA regulations regarding drug and alcohol use, particularly in transportation roles where drug testing and alcohol screenings are mandatory.
- Training for Supervisors: Special attention is required to provide training for supervisors in handling situations involving employees with substance abuse problems, particularly in safety- sensitive positions within DelDOT.

QUESTIONS

Questions must be submitted before the due date identified in the Procurement Schedule for this RFP. All inquiries must be submitted in the Q/A section of the project listing in the Bonfire Procurement Portal.

The Department's response to questions will be posted, according to the procurement schedule, under the project listing in Bonfire and to the State of Delaware Bid Solicitation Directory Website: https://mmp.delaware.gov/Bids/.

Direct contact with State of Delaware employees other than DelDOT's Contract Administration staff regarding this RFP is expressly prohibited without prior consent. Companies directly contacting State of Delaware employees risk elimination of their proposal from further consideration. Exceptions exist only for organizations currently doing business in the State who require contact in the normal course of doing that business.

PROCUREMENT SCHEDULE

Action Item	Date	Time
Deadline for Questions to ensure response:	Ten (10) business days prior to the proposal due date	2:00 P.M. Local Time
Final Response to Questions posted by:	Five (5) business days prior to the proposal due date	2:00 P.M. Local Time
Proposals Due no later than: *	Thursday, July 10, 2025	2:00 P.M. Local Time

NOTE: Only asterisk (*) marked date changes will be communicated (via posted Addendums).

PROPOSAL REQUIREMENTS

Interested companies must submit the material required herein or they may not be considered for the project:

1. Proposals must be received before the Proposal Due Date and Time, as identified in the Procurement Schedule for this RFP. Responses submitted by hard copy, mail, facsimile, or e-mail will not be accepted. Responses received after the Proposal Due Date and Time will not be considered.

2. **Upload your submission at**: https://deldot.bonfirehub.com/portal/

   Important Notes:
   - Logging in and/or uploading the file(s) does not mean the response is submitted. Users must successfully upload all the file(s) and MUST click the submit button before the proposal due date and time.
   - Users will receive an email confirmation receipt with a unique confirmation number once the submission has been finalized. This will confirm that the proposal has been submitted successfully.

- Each submitted item of Requested Information will only become visible to DelDOT after the proposal due date and time.
- If the file is mandatory, you will not be able to complete your submission until the requirement is met.
- Uploading large documents may take significant time depending on the size of the file(s) and your Internet connection speed. The maximum upload file size is 1000 MB.
- Minimum system requirements: Internet Explorer 11, Microsoft Edge, Google Chrome, or Mozilla Firefox. Java Script must be enabled.

Need Help? Please contact Bonfire directly at Support@GoBonfire.com for technical questions related to your submission. You can also visit their help forum at https://bonfirehub.zendesk.com/hc.

3. **The Vendor must be Registered,** or submit application for registration, with DelDOT at or before the time of submission in order to be considered. For registration information, click here.

4. **Submit one (1) Original and one (1) Redacted copy** of the Proposal. The original must be a .pdf file of the original signed proposal and should be clearly marked "**Original**" on the first page of the document. The redacted copy must be a .pdf file of the original signed proposal with any proprietary or confidential information redacted, and this copy should be clearly marked as "**Redacted**" on the first page of the document. The redacted copy is required even if the submission contains no proprietary or confidential information.

   To determine what information may be considered proprietary or confidential and may be redacted from their Proposal, companies should review Delaware's Freedom of Information Regulations here; http://regulations.delaware.gov/AdminCode/title8/1400.shtml#TopOfPage. Under Delaware FOIA law, 29 Del. C, §10002(l)(2), "Trade secrets and commercial or financial information…which is of a privileged or confidential nature" are "records that shall not be deemed public" and are therefore exempt from disclosure under FOIA.

5. **Bid Page** – All Vendors who wish to perform services on this contract shall specify unit bid amounts on the attached Appendix B – Bid Page. The unit bid amounts shall be inclusive of all services, materials, equipment, and incidentals necessary for implementation of the full performance system and for ongoing maintenance, technical support, and engineering updates for any equipment. The specified unit bid amount will remain in effect during the thirty-six (36) month contract period. All figures entered on the bid form shall be typewritten. If commission fees are to be variable, the proposer must describe the possible variations in detail in their proposal and show same on the bid form.

6. **Joint venture** submissions will not be considered.

7. DelDOT reserves the right to reject any and all submissions. Submissions become property of the Department and shall be retained electronically for a minimum period of three (3) years from the date of receipt. DelDOT reserves the right to any and all ideas included in this response without incurring any obligations to the responding companies or committing to procurement of the proposed services.

8. **Required Certification Forms.** All companies responding to the RFP must complete and return the submission forms located in 'Appendix A' of this document.

No promotional materials or brochures are to be included as part of the submission.

RATING CRITERIA

#	**Criteria Description**:	**Weight**
1	Technical Approach and Methodology: • The vendor must clearly outline how they will deliver DOT/FMCSA-compliant EAP services, including confidential counseling, SAP evaluations, return-to-duty protocols, and follow-up testing under 49 CFR Parts 40 and 382. The methodology should demonstrate a clear plan for managing substance use cases among CDL holders and safety-sensitive employees while ensuring regulatory reporting, documentation, and follow-through. The approach must also emphasize accessibility, confidentiality, and support for a drug- and alcohol-free workplace	30%
2	Firm's experience with EAP and Regulatory Compliance: • Proven experience managing DOT-regulated EAPs, including oversight of SAP functions, FMCSA Clearinghouse interaction, and successful return-to-duty program administration. Demonstrated understanding of challenges in transportation environments and familiarity with 49 CFR Part 40 SAP procedures. Experience supporting large public-sector workforces is strongly preferred.	25%

4	• Personnel must include certified SAPs, licensed behavioral health professionals, and staff with expertise in DOT/FMCSA compliance. The team should show demonstrated experience in managing EAP services for CDL drivers and safety-sensitive staff. SAP qualifications must meet standards under 49 CFR §40.281.	15%
5	Firm's resources and capability to accomplish proposed work on schedule • Ability to deploy qualified staff and services promptly and maintain continuity of care across all DelDOT locations. Evidence of infrastructure to support compliance, case tracking, and timely communication with DelDOT's DAPM and DERs. Ability to respond to urgent SAP referrals and testing coordination without delay.	10%
	TOTAL:	**100%**

OVERVIEW OF SELECTION PROCESS

- This is a project-specific agreement where the services as described in this RFP will be provided over the life of the project.
- This is a single-phase solicitation process with the availability for discussions with up to three (3) of the most highly qualified companies. Based upon the listed criteria and evaluation of each company's submitted proposal, the Selection Committee may decide if a small sample task and/or discussions will be held with the most highly qualified consultants. If discussions are held, they will serve to clarify the technical approach, qualifications, and capabilities provided in response to the RFP, after which the committee will determine the ranking of the candidate companies.
- Selection Committee members will individually score each company's submitted proposal, which determines individual ranking. The Department's ranking is the combined ranking of all Committee members. Companies, in order of ranking, will have the opportunity to negotiate an agreement with the

Department. If the Department cannot reach an agreement with the highest-ranked company(s), the Department terminates negotiations and begins negotiations with the next highest-ranked company, and so on, until an agreement is reached. The Department notifies via email the awarded company(s) of the opportunity to enter into an agreement with the Department. This notification also includes information on the next steps in the agreement process.

- After the ranking process has been completed, applicable price information will be requested from the successful candidate company(s), such as salary rates for various classifications of personnel, and an indirect cost derivation for the most current accounting period.
- Payroll burden and overhead will be computed on direct salary costs only (not including overtime) at the consultant's audited rate, as per Federal Acquisition Regulations Part 31, and Department policies. Computer and CADD costs are not allowable as direct cost for this project. Rate determination and applicability are subject to audit by the Department. Additionally, candidates should be prepared for the Department to work with your current accounting company to provide information and backup documentation. Full and immediate cooperation is required to avoid delays in execution of an agreement. Failure to cooperate may result in breaking off negotiations and moving to the next ranked company.
- Shortlist and Selection Committee membership appointments are confidential. The Department's Professional Services Procurement Manual may be viewed here.

CONTRACT TERMS AND CONDITIONS

- **General Information**
  - The term of the contract between the successful vendor and DelDOT shall be for three years with two optional extensions for a period of one (1) year for each extension.
  - It is imperative that the contract drafting and finalization process be timely and accurately reflect the minimum requirements and other applicable contractual terms in the RFP. The vendor is expected to use the State of Delaware's professional agreement contract template (Appendix B) and incorporate all the terms of the RFP, their proposal, and follow-up responses so that wholesale changes are not required. The vendor's failure to meet this requirement may result in a fee as set forth in the Performance Guarantees (Attachment 16).
  - The selected vendor will be required to enter into a written agreement with DelDOT. The State of Delaware reserves the right to incorporate standard State contractual provisions into any contract negotiated as a result of a proposal submitted in response to this RFP. Any proposed modifications to the terms and conditions of the standard contract are subject to review and approval by the State. Vendors will be required to sign the contract for all services and may be required to sign additional agreements.
  - The selected vendor or vendors will be expected to enter negotiations with DelDOT representatives, which will result in a formal contract between parties. Procurement will be in accordance with

subsequent contracted agreement. This RFP and the selected vendor's response to this RFP will be incorporated as part of any formal contract.

- The State of Delaware's standard contract will most likely be supplemented with the vendor's software license, support/maintenance, source code escrow agreements, and any other applicable agreements. The terms and conditions of these agreements will be negotiated with the finalist during actual contract negotiations.
- The successful vendor shall promptly execute a contract incorporating the terms of this RFP prior to the start date of the contract. No vendor is to begin any service prior to receipt of a signed State of Delaware purchase order, properly processed through the State of Delaware Accounting Office and the Department of Finance. The purchase order shall serve as the authorization to proceed in accordance with the proposal specifications and the special instructions, once it is received by the successful vendor.
- If the vendor to whom the award is made fails to enter into the agreement as herein provided, the award will be annulled, and an award may be made to another vendor. Such vendor shall fulfill every stipulation embraced herein as if they were the party to whom the first award was made.
- The State reserves the right to extend the contract on a month-to-month basis for a period of up to three months after the term of the full contract has been completed.
- Vendors are not restricted from offering lower pricing at any time during the contract term.

- **Collusion or Fraud**

  Any evidence of agreement or collusion among vendor(s) and prospective vendor(s) acting to illegally restrain freedom from competition by agreement to offer a fixed price, or otherwise, will render the offers of such vendor(s) void.

  By responding, the vendor shall be deemed to have represented and warranted that its proposal is not made in connection with any competing vendor submitting a separate response to this RFP, and is in all respects fair and without collusion or fraud; that the vendor did not participate in the RFP development process and had no knowledge of the specific contents of the RFP prior to its issuance; and that no employee or official of the State of Delaware participated directly or indirectly in the vendor's proposal preparation.

  Advance knowledge of information which gives any particular vendor advantages over any other interested vendor(s), in advance of the opening of proposals, whether in response to advertising or an employee or representative thereof, will potentially void that particular proposal.

- **Lobbying and Gratuities**

  Lobbying or providing gratuities shall be strictly prohibited. Vendors found to be lobbying, providing gratuities to, or in any way attempting to influence a State of Delaware employee or agent of the State of Delaware concerning this RFP or the award of a contract resulting from this RFP shall have their

proposal immediately rejected and shall be barred from further participation in this RFP.

The selected vendor will warrant that no person or selling agency has been employed or retained to solicit or secure a contract resulting from this RFP upon agreement or understanding for a commission, or a percentage, brokerage or contingent fee. For breach or violation of this warranty, the State of Delaware shall have the right to annul any contract resulting from this RFP without liability or at its discretion deduct from the contract price or otherwise recover the full amount of such commission, percentage, brokerage or contingent fee.

All contact with State of Delaware employees, contractors or agents of the State of Delaware concerning this RFP shall be conducted in strict accordance with the manner, forum and conditions set forth in this RFP.

- **Solicitation of State Employees**

  Until contract award, vendors shall not, directly or indirectly, solicit any employee of the State to leave the State's employ in order to accept employment with the vendor, its affiliates, actual or prospective contractors, or any person acting in concert with vendor, without prior written approval of the State's contracting officer. Solicitation of State employees by a vendor may result in rejection of the vendor's proposal.

  This paragraph does not prevent the employment by a vendor of a State employee who has initiated contact with the vendor. However, State employees may be legally prohibited from accepting employment with the contractor or subcontractor under certain circumstances. Vendors may not knowingly employ a person who cannot legally accept employment under state or federal law. If a vendor discovers that they have done so, they must terminate that employment immediately.

- **General Contract Terms**

  - Independent Contractors

    The parties to the resulting contract shall be independent contractors to one another, and nothing herein shall be deemed to cause the agreement to create an agency, partnership, joint venture or employment relationship between parties. Each party shall be responsible for compliance with all applicable workers compensation, unemployment, disability insurance, social security withholding and all other similar matters. Neither party shall be liable for any debts, accounts, obligations or other liability whatsoever of the other party or any other obligation of the other party to pay on the behalf of its employees or to withhold from any compensation paid to such employees any social benefits, workers compensation insurance premiums or any income or other similar taxes.

  - Temporary Personnel are Not State Employees Unless and Until They are Hired (if applicable)

    The vendor shall agree that any individual or group of temporary staff person(s) provided to the State of Delaware pursuant to this RFP shall remain the employee(s) of the vendor for all purposes including any required compliance with the Affordable Care Act by the vendor. The vendor shall

agree that it shall not allege, argue, or take any position that individual temporary staff person(s) provided to the State pursuant to this RFP must be provided any benefits, including any healthcare benefits by the State of Delaware and the vendor shall agree to assume the total and complete responsibility for the provision of any healthcare benefits required by the Affordable Care Act to aforesaid individual temporary staff person(s). In the event that the Internal Revenue Service, or any other third party governmental entity determines that the State of Delaware is a dual employer or the sole employer of any individual temporary staff person(s) provided to the State of Delaware pursuant to this Solicitation, the vendor shall agree to hold harmless, indemnify, and defend the State to the maximum extent of any liability to the State arising out of such determinations.

Notwithstanding the content of the preceding paragraph, should the State of Delaware subsequently directly hire any individual temporary staff employee(s) provided pursuant to this RFP, the aforementioned obligations to hold harmless, indemnify, and defend the State of Delaware shall cease and terminate for the period following the date of hire. Nothing herein shall be deemed to terminate the vendor's obligation to hold harmless, indemnify, and defend the State of Delaware for any liability that arises out of compliance with the ACA prior to the date of hire by the State of Delaware. The vendor will waive any separation fee provided an employee works for both the vendor and hiring agency, continuously, for a three (3) month period and is provided thirty (30) days written notice of intent to hire from the agency. Notice can be issued at second month if it is the State's intention to hire.

- Work Performed in a State Building (if applicable)

Awarded vendor(s) who have any employees carrying out any work related to the awarded contract at a State facility shall have those employees comply with any health mandate or policy issued by the State of Delaware related to a pandemic or other State of Emergency issued by any State authority during the term of the awarded contract, including those that apply directly to State employees.

- ACA Safe Harbor (if applicable)

The State of Delaware and its utilizing agencies are not the employer of temporary or contracted staff. However, the State of Delaware is concerned that it could be determined to be a Common-law Employer as defined by the Affordable Care Act ("ACA"). Therefore, the State of Delaware seeks to utilize the "Common-law Employer Safe Harbor Exception" under the ACA to transfer health benefit insurance requirements to the staffing company. The Common-law Employer Safe Harbor Exception can be attained when the State and/or its agencies are charged and pay for an "Additional Fee" with respect to the employees electing to obtain health coverage from the vendor.

The Common-law Employer Safe Harbor Exception under the ACA requires that an Additional Fee must be charged to those employees who obtain health coverage from the vendor but does not state the required amount of the fee. The State of Delaware requires that all vendors shall identify the Additional Fee to obtain health coverage from the vendor and delineate the Additional Fee from all other charges and fees. The vendor shall identify both the Additional Fee to be charged and the basis

of how the fee is applied (i.e., per employee, per invoice, etc.). The State of Delaware will consider the Additional Fee and prior to award reserve the right to negotiate any fees offered by the vendor. Further, the Additional Fee shall be separately scored in the proposal to ensure that neither prices charged, nor the Additional Fee charged will have a detrimental effect when selecting vendor(s) for award.

- Licenses and Permits

  In performance of the contract, the vendor will be required to comply with all applicable federal, state and local laws, ordinances, codes, and regulations. The cost of permits and other relevant costs required in the performance of the contract shall be borne by the successful vendor. The vendor shall be properly licensed and authorized to transact business in the State of Delaware as provided in 30 Del. C. § 2101 or through the Delaware Department of Insurance, whichever is applicable.

  Prior to receiving an award, the successful vendor shall either furnish the State of Delaware with proof of State of Delaware Business Licensure or authorization obtained through the Delaware Department of Insurance, whichever is applicable, or initiate the process of application where required.

  An application for a Delaware Business License may be requested in writing to: Division of Revenue, Carvel State Building, P.O. Box 8750, 820 N. French Street, Wilmington, DE 19899 or by telephone to one of the following numbers: (302) 577-8200 Public Service, (302) 577-8205 Licensing Department.

  Information regarding the award of the contract will be given to the Division of Revenue and/or the Delaware Department of Insurance. Failure to comply with the State of Delaware licensing requirements may subject vendor to applicable fines and/or interest penalties.

- Notice

  Any notice to the State of Delaware required under the resulting contract shall be sent by registered mail to:

  Delaware Department of Transportation
  800 S. Bay Road Dover, DE 19904
  CONTACT: Contract Administration

- Indemnification

  a) General Indemnification

     By submitting a proposal, the proposing vendor agrees that in the event it is awarded a contract, it will indemnify and otherwise hold harmless the State of Delaware, its agents and employees from any and all liability, suits, actions, or claims, together with all costs, expenses for attorney's fees, arising out of the vendor's, its agents and employees' performance of work or services in connection with the contract.

b) Proprietary Rights Indemnification

Vendor shall warrant that all elements of its solution, including all equipment, software, documentation, services and deliverables, do not and will not infringe upon or violate any patent, copyright, trade secret or other proprietary rights of any third party. In the event of any claim, suit or action by any third party against the State of Delaware, the State of Delaware shall promptly notify the vendor in writing and vendor shall defend such claim, suit or action at vendor's expense, and vendor shall indemnify the State of Delaware against any loss, cost, damage, expense or liability arising out of such claim, suit or action (including, without limitation, litigation costs, lost employee time, and counsel fees) whether or not such claim, suit or action is successful.

If any equipment, software, services (including methods) products, or other intellectual property used or furnished by the vendor (collectively "Products") is or in vendor's reasonable judgment is likely to be, held to constitute an infringing product, vendor shall at its expense and option either:

i. Procure the right for the State of Delaware to continue using the Product(s);

ii. Replace the product with a non-infringing equivalent that satisfies all the requirements of the contract; or

iii. Modify the Product(s) to make it or them non-infringing, provided that the modification does not materially alter the functionality or efficacy of the product or cause the Product(s) or any part of the work to fail to conform to the requirements of the Contract, or only alters the Product(s) to a degree that the State of Delaware agrees to and accepts in writing.

- **Insurance Requirements**

The selected firm(s) must obtain at its own cost and expense and keep in force and effect during the term of the agreement, including all extensions, the minimum coverage limits specified below with a carrier satisfactory to the State.

a. Worker's Compensation and Employer's Liability Insurance in accordance with applicable law.

b. Commercial General Liability - $1,000,000 per occurrence/$3,000,000 per aggregate.

c. Errors and Omissions - $1,000,000 per occurrence/$3,000,000 per aggregate.

d. Automotive Liability Insurance covering all automotive units used in the work (including all units leased from and/or provided by the State to Vendor pursuant to this Agreement as well as all units used by Vendor, regardless of the identity of the registered owner, used by Vendor for completing the Work required by this Agreement to include but not limited to transporting Delaware clients or staff), providing coverage on a primary non-contributory basis with limits of not less than:

- $1,000,000 combined single limit each accident, for bodily injury;
- $250,000 for property damage to others;

- $25,000 per person per accident Uninsured/Underinsured Motorists coverage;
- $25,000 per person, $300,000 per accident PIP benefits if carrying any of our clients or employees; and

Comprehensive coverage for all vehicles leased from the State of Delaware Fleet Services which shall cover the replacement cost of the vehicle in the event of collision, damage or other loss.

Certificate of Insurance and/or copies of the insurance policies will be requested at time of award.

In no event shall the State of Delaware be named as an additional insured on any policy required under this agreement.

- **Performance Requirements**

  The selected vendor will warrant that it possesses, or has arranged through subcontractors, all capital and other equipment, labor, materials, and licenses necessary to carry out and complete the work in the contract in compliance with any and all federal and State laws, and County and local ordinances, regulations and codes.

- **BID BOND**

  There is no Bid Bond Requirement.

- **PERFORMANCE BOND**

  There is no Performance Bond requirement.

- **Vendor Emergency Response Point of Contact**

  The awarded vendor(s) shall provide the name(s), telephone, or cell phone number(s) of those individuals who can be contacted twenty four (24) hours a day, seven (7) days a week where there is a critical need for commodities or services when the Governor of the State of Delaware declares a state of emergency under the Delaware Emergency Operations Plan or in the event of a local emergency or disaster where a state governmental entity requires the services of the vendor. Failure to provide this information could render the proposal as non- responsive.

  In the event of a serious emergency, pandemic or disaster outside the control of the State of Delaware, the State of Delaware may negotiate, as may be authorized by law, emergency performance from the vendor to address the immediate needs of the State of Delaware, even if not contemplated under the original contract or procurement. Payments are subject to appropriation and other payment terms.

- **Warranty**

  The vendor will provide a warranty that the deliverables provided pursuant to the contract will function as designed for a period of no less than one (1) year from the date of system acceptance. The warranty shall require the vendor correct, at its own expense, the setup, configuration, customizations or modifications so that it functions according to the State of Delaware's requirements.

- **Costs and Payment Schedules**

  All contract costs must be as detailed specifically in the vendor's cost proposal. No charges other than as specified in the proposal shall be allowed without written consent of the State of Delaware. The proposal costs shall include full compensation for all taxes that the selected vendor is required to pay.

  The State of Delaware will require a payment schedule based on defined and measurable milestones. Payments for services will not be made in advance of work performed. The State of Delaware may require holdback of contract monies until acceptable performance is demonstrated (as much as 25%).

- **Liquidated Damages**

  The State of Delaware may include in the final contract liquidated damages provisions for non-performance.

- **Dispute Resolution**

  At the option of the parties, they shall attempt in good faith to resolve any dispute arising out of or relating to the final contract promptly by negotiation between executives who have authority to settle the controversy and who are at a higher level of management than the persons with direct responsibility for administration of the contract. All offers, promises, conduct and statements, whether oral or written, made in the course of the negotiation by any of the parties, their agents, employees, experts and attorneys are confidential, privileged and inadmissible for any purpose, including impeachment, in arbitration or other proceeding involving the parties, provided evidence that is otherwise admissible or discoverable shall not be rendered inadmissible.

  If the matter is not resolved by negotiation, as outlined above, or, alternatively, the parties elect to proceed directly to mediation, then the matter will proceed to mediation as set forth below. Any disputes, claims, or controversies arising out of or relating to the contract shall be submitted to a mediator selected by the parties. If the matter is not resolved through mediation, it may be submitted for arbitration or litigation. The State of Delaware reserves the right to proceed directly to arbitration or litigation without negotiation or mediation. Any such proceedings held pursuant to this provision shall be governed by State of Delaware law, and jurisdiction and venue shall be in the State of Delaware. Each party shall bear its own costs of mediation, arbitration, or litigation, including attorneys' fees.

- **Remedies**

  Except as otherwise provided in this solicitation, including but not limited to Section V.G.16 above, all claims, counterclaims, disputes, and other matters in question between the State of Delaware and vendor arising out of, or relating to, this solicitation, or a breach of it may be decided by arbitration if the parties mutually agree, or in a court of competent jurisdiction within the State of Delaware.

- **Termination of Contract**

  The contract resulting from this RFP may be terminated as follows by the State of Delaware:

  a) Termination for Cause

If, for any reasons, or through any cause, the vendor fails to fulfill in timely and proper manner its obligations under the contract, or if the vendor violates any of the covenants, agreements, or stipulations of the contract, the State of Delaware shall thereupon have the right to terminate the contract by giving written notice to the vendor of such termination and specifying the effective date thereof, at least thirty (30) days before the effective date of such termination. In that event, all finished or unfinished documents, data, studies, surveys, drawings, maps, models, photographs, and reports or other material prepared by the vendor under the contract shall, at the option of the State of Delaware, become its property, and the vendor shall be entitled to receive just and equitable compensation for any satisfactory work completed on such documents and other materials which is usable to the State of Delaware.

On receipt of the contract cancellation notice from the State of Delaware, the vendor shall have no less than five (5) days to provide a written response and may identify a method(s) to resolve the violation(s). A vendor response shall not affect or prevent the contract cancellation unless the State of Delaware provides a written acceptance of the vendor response. If the State of Delaware does accept the vendor's method and/or action plan to correct the identified deficiencies, the State of Delaware will define the time by which the vendor must fulfill its corrective obligations. Final retraction of the State of Delaware's termination for cause will only occur after the vendor successfully rectifies the original violation(s). At its discretion, the State of Delaware may reject in writing the vendor's proposed action plan and proceed with the original contract cancellation timeline.

b) Termination for Convenience

The State of Delaware may terminate the contract at any time by giving written notice of such termination and specifying the effective date thereof, at least thirty (30) days before the effective date of such termination. In that event, all finished or unfinished documents, data, studies, surveys, drawings, models, photographs, reports, supplies, and other materials shall, at the option of the State of Delaware, become its property and the vendor shall be entitled to receive compensation for any satisfactory work completed on such documents and other materials, and which is usable to the State of Delaware.

c) Termination for Non-Appropriations

In the event the General Assembly fails to appropriate the specific funds necessary to enter into or continue the contractual agreement, in whole or part, the contract shall be terminated as to any obligation of the State of Delaware requiring the expenditure of money for which no specific appropriation is available at the end of the last fiscal year for which no appropriation is available or upon the exhaustion of funds. This is not a termination for convenience and will not be converted to such.

d) Data and Participant Records

In the event of contract termination, Vendor shall electronically transfer to the State of Delaware (or to a successor administrator) within thirty (30) days of termination all data and participant records

necessary for the continued administration of the plan.

Vendor must agree to continue operations until the transfer of data has been completed.

- **Non-discrimination**

  In performing the services subject to this RFP, the vendor, as set forth in 19 Del. C. §711, will agree that it will not discriminate against any employee or applicant with respect to compensation, terms, conditions or privileges of employment because of such individual's race, marital status, genetic information, color, age, religion, sex, sexual orientation, gender identity, or national origin. The successful vendor shall comply with all federal and state laws, regulations and policies pertaining to the prevention of discriminatory employment practice. Failure to perform under this provision constitutes a material breach of contract.

- **Covenant against Contingent Fees**

  The successful vendor will warrant that no person or selling agency has been employed or retained to solicit or secure the contract upon an agreement of understanding for a commission or percentage, brokerage or contingent fee excepting bona-fide employees, bona-fide established commercial or selling agencies maintained by the vendor for the purpose of securing business. For breach or violation of this warranty, the State of Delaware shall have the right to annul the contract without liability or at its discretion to deduct from the contract price or otherwise recover the full amount of such commission, percentage, brokerage or contingent fee.

- **Vendor Activity**

  No activity is to be executed in an offshore facility, either by a subcontracted firm or a foreign office or division of the vendor. The vendor must attest to the fact that no activity will take place outside of the United States in its transmittal letter. Failure to adhere to this requirement is cause for elimination from future consideration.

- **Vendor Responsibility**

  The State of Delaware will enter into a contract with the successful vendor(s). The successful vendor(s) shall be responsible for all products and services as required by this RFP whether or not the vendor or its subcontractor provided final fulfillment of the order. Subcontractors, if any, shall be clearly identified in the vendor's proposal by completing Attachment 6, and are subject the approval and acceptance of the State.

- **Personnel, Equipment and Services**

  - Vendor represents that it has, or will secure at its own expense, all personnel required to perform the services required under the contract.

  - All of the equipment and services required hereunder shall be provided by or performed by the vendor or under its direct supervision, and all personnel, including subcontractors, engaged in the

work shall be fully qualified and shall be authorized under State and local law to perform such services.

- None of the equipment and/or services covered by the contract shall be subcontracted without the prior written approval of the State of Delaware. Only those subcontractors identified in Attachment 6 are considered approved upon award. Changes to those subcontractor(s) listed in Attachment 6 must be approved in writing by the State of Delaware.

- **Fair Background Check Practices**

Pursuant to 29 Del. C. § 6909B, the State of Delaware does not consider the criminal record, criminal history, credit history or credit score of an applicant for state employment during the initial application process unless otherwise required by state and/or federal law. Vendors doing business with the State of Delaware are encouraged to adopt fair background check practices. Vendors can refer to 19 Del. C. § 711(g) for applicable established provisions.

- **Vendor Background Check Requirements**

Vendor(s) selected for an award that access state property or come in contact with vulnerable populations, including children and youth, shall be required to complete background checks on employees serving the State's on premises contracts. Unless otherwise directed at a minimum, this shall include a check of the following registry:

Delaware Sex Offender Central Registry at: https://sexoffender.dsp.delaware.gov/

Individuals that are listed in the registry shall be prevented from direct contact in the service of an awarded state contract but may provide support or off-site premises service for contract vendors. Should an individual be identified and the vendor(s) believes their employee's service does not represent a conflict with this requirement, may apply for a waiver to the primary agency listed in the solicitation. The Agency's decision to allow or deny access to any individual identified on a registry database is final and at the State of Delaware's sole discretion.

By request of the State of Delaware, the vendor(s) shall provide a list of all employees serving an awarded contract and certify adherence to the background check requirement. Individual(s) found in the central registry in violation of the terms stated, shall be immediately prevented from a return to state property in service of a contract award. A violation of this condition represents a violation of the contract terms and conditions, and may subject the vendor to penalty, including contract cancellation for cause.

Individual contracts may require additional background checks and/or security clearance(s),

depending on the nature of the services to be provided or locations accessed, but any other requirements shall be stated in the contract scope of work or be a matter of common law. The vendor(s) shall be responsible for the background check requirements of any authorized subcontractor providing service to the State of Delaware's contract.

- **Work Product**

  All materials and products developed under the executed contract by the vendor are the sole and exclusive property of the State of Delaware. The vendor will seek written permission to use any product created under the contract.

- **Contract Documents**

  The RFP, the purchase order, the executed contract and any supplemental documents between the State of Delaware and the successful vendor may constitute the contract between the State of Delaware and the vendor. In the event there is any discrepancy between any of these contract documents, the following order of documents governs so that the former prevails over the latter: contract, the RFP, vendor's response to the RFP, and purchase order. No other documents shall be considered. These documents will constitute the entire agreement between the State of Delaware and the vendor.

- **Applicable Law**

  The laws of the State of Delaware shall apply, except where federal Law has precedence. The successful vendor shall consent to jurisdiction and venue in the State of Delaware.

  In submitting a proposal, vendors certify that they comply with all federal, state, and local laws applicable to its activities and obligations, including:

  a) the laws of the State of Delaware;

  b) the applicable portion of the federal Civil Rights Act of 1964;

  c) the Equal Employment Opportunity Act and the regulations issued there under by the federal government;

  d) a condition that the proposal submitted was independently arrived at, without collusion, under penalty of perjury;

  e) that programs, services, and activities provided to the general public under resulting contract conform with the Americans with Disabilities Act of 1990, and the regulations issued there under by the federal government.

  f) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (45 C.F.R. Parts 160, 162 and 164, as may thereafter be amended); Electronic Data Interchange (EDI) Rule (45 C.F.R. Parts 160, 162 and 164, as may thereafter be amended); and Privacy laws that are relevant to the scope of services covered by the resulting contract.

  If any vendor fails to comply with (a) through (f) of this paragraph, the State of Delaware reserves the right to disregard the proposal, terminate the contract, or consider the vendor in default.

The selected vendor shall keep itself fully informed of and shall observe and comply with all applicable existing federal and State laws, and County and local ordinances, regulations and codes, and those laws, ordinances, regulations, and codes adopted during its performance of the work.

- **Severability**

If any term or provision of the contract is found by a court of competent jurisdiction to be invalid, illegal or otherwise unenforceable, the same shall not affect the other terms or provisions thereof or the whole of the contract, but such term or provision shall be deemed modified to the extent necessary in the court's opinion to render such term or provision enforceable, and the rights and obligations of the parties shall be construed and enforced accordingly, preserving to the fullest permissible extent the intent and agreements of the parties therein set forth.

- **Assignment of Antitrust Claims**

As consideration for the award and execution of the contract by the State of Delaware, the vendor shall grant, convey, sell, assign, and transfer to the State of Delaware all of its right, title and interest in and to all known or unknown causes of action it has or may thereafter acquire under the antitrust laws of the United States and the State of Delaware, regarding the specific goods or services purchased or acquired for the State pursuant to the contract. Upon either the State of Delaware's or the vendor notice of the filing of or reasonable likelihood of filing of an action under the antitrust laws of the United States or the State of Delaware, the State of Delaware and vendor shall meet and confer about coordination of representation in such action.

- **Scope of Agreement**

If the scope of any provision of the contract is determined to be too broad in any respect whatsoever to permit enforcement to its full extent, then such provision shall be enforced to the maximum extent permitted by law, and the parties thereto shall consent and agree that such scope may be judicially modified accordingly and that the whole of such provisions of the contract shall not thereby fail, but the scope of such provisions shall be curtailed only to the extent necessary to conform to the law.

- **Affirmation**

The vendor must affirm that within the past five (5) years the firm or any officer, controlling stockholder, partner, principal, or other person substantially involved in the contracting activities of the business is not currently suspended or debarred and is not a successor, subsidiary, or affiliate of a suspended or debarred business.

- **Audit Access to Records**

The vendor shall maintain books, records, documents, and other evidence pertaining to the contract to the extent and in such detail as shall adequately reflect performance thereunder. The vendor shall agree to preserve and make available to the State of Delaware, upon request, such records for a period of seven (7) years from the date services were rendered by the vendor. Records involving matters in litigation shall be retained for one (1) year following the termination of such litigation. The vendor agrees to make such records available for inspection, audit, or reproduction to any official State representative in the performance of their duties under the contract. Upon notice given to the vendor, representatives of the State of Delaware or other duly authorized State or federal agency may inspect, monitor, and/or evaluate the cost

and billing records or other material relative to the contract. The cost of any contract audit disallowances resulting from the examination of the vendor's financial records will be borne by the vendor. Reimbursement to the State of Delaware for disallowances shall be drawn from the vendor's own resources and not charged to cost of the contract or cost pools indirectly charging contract costs.

- **IRS 1075 Publication (If Applicable)**

1. Performance:

   In performance of the contract, the vendor shall agree to comply with and assume responsibility for compliance by his or her employees with the following requirements:

   - All work will be performed under the supervision of the vendor or the vendor's responsible employees.
   - The vendor and the vendor's employees with access to or who use Federal Tax Information ("FTI") must meet the background check requirements defined in IRS Publication 1075.
   - Any federal tax returns or federal tax return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of the contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone other than an officer or employee of the vendor is prohibited.
   - All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
   - No work involving returns and return information furnished under the contract will be subcontracted without prior written approval of the IRS.
   - The vendor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
   - The agency will have the right to void the contract if the vendor fails to provide the safeguards described above.
   - The vendor shall comply with agency incident response policies and procedures for reporting unauthorized disclosures of agency data.

2. Criminal/Civil Sanctions:

   Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized therein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein

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

Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of the contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to- know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

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

Granting a vendor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Vendors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting

unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the vendor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

3. Inspection:

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

- Other General Conditions

a) Volumes and Quantities – Activity volume estimates and other quantities have been reviewed for accuracy; however, they may be subject to change prior or subsequent to award of the contract.

b) Status Reporting – The selected vendor will be required to lead and/or participate in status meetings and submit status reports covering such items as progress of work being performed, milestones attained, resources expended, problems encountered, and corrective action taken, until final system acceptance.

c) Regulations – All equipment, software and services must meet all applicable local, State and federal regulations in effect on the date of the contract.

d) Assignment – Any resulting contract shall not be assigned except by express prior written consent from the State of Delaware.

e) Changes – No alterations in any terms, conditions, delivery, price, quality, or specifications of items ordered will be effective without the written consent of the State of Delaware.

f) Payment – The State of Delaware reserves the right to pay by Automated Clearing House (ACH), Purchase Card (P-Card), or check. The agencies will authorize and process for payment of each administrative invoice within thirty (30) days after the date of receipt of a correct invoice. The agencies will authorize and process for payment of each claim invoice within 24 hours. Vendors are invited to offer in their proposal value added discounts (i.e. speed to pay discounts for specific payment terms). Cash or separate discounts should be computed and incorporated as invoiced.

g) W-9 – The State of Delaware requires registration and completion of a W-9 through the Supplier Public Portal available at https://esupplier.erp.delaware.gov to make payments to vendors. Successful completion of this form enables the creation of a State of Delaware vendor record.

h) Purchase Orders – Agencies that are part of the First State Financial (FSF) system are required to identify the contract number 2157S on all Purchase Orders (P.O.) and shall complete the same when entering P.O. information in the state's financial reporting system.

i) Additional Terms and Conditions – The State of Delaware reserves the right to add terms and conditions during the contract negotiations.

MISCELLANEOUS

The Department is not liable for any cost incurred by the consultant in the preparation or presentation of the Proposal.

Any individual, business, organization, corporation, consortium, partnership, joint venture, or any other entity, including subconsultants currently debarred or suspended, is ineligible to participate as a candidate for this process. Any entity ineligible to conduct business in the State of Delaware for any reason is ineligible to respond to the RFP.

The Department of Transportation will affirmatively ensure that individuals and businesses will not be discriminated against on the grounds of race, creed, color, sex, or national origin in consideration for an award. Minority business enterprises will be afforded the full opportunity to submit bids/proposals in response to this invitation.

Department of Transportation
State of Delaware
By: Shanté Hastings
Secretary
Dover, DE

Appendix A - REQUIRED FORMS

The following completed forms are required to be returned with each proposal:

- Certification of Eligibility
- Certificate of Non-Collusion

CERTIFICATION OF ELIGIBILITY

Delaware Department of Transportation

Request for Proposal 2157S – DelDOT Drug and Alcohol Program – FMCSA- Compliant Employee Assistance Services for CDL and Safety-Sensitive Personnel

We have read Request for Proposal number **2157S** and fully understand the intent of the RFP as stated, certify that we have adequate personnel and knowledge to fulfill the requirements thereof, and agree to furnish such services in accordance with the contract documents as indicated should we be awarded the contract.

_____ hereby certifies that it is not included on the United States Comptroller General's Consolidated List of Persons or Companies Currently Debarred for Violations of Various Public Contracts Incorporating Labor Standard Provisions.

_____Signature of the Bidder or Offeror's Authorized Official

_____Name and Title of the Bidder or Offeror's Authorized Official

_____Date

Sworn and subscribed before me this _____ day of _____, 20___

_____ My commission expires: _____ / _____ / 20___

Notary Public Month Day Year

CERTIFICATE OF NON-COLLUSION

By submission of this bid, each bidder and each person signing on behalf of any bidder certifies, and in the case of a joint bid, each party thereto certifies as to its own organization, under penalty of perjury, that to the best of knowledge and belief:

1) The prices in this bid have been arrived at independently without collusion, consultation, communication, or agreement for the purpose of restricting to such prices, with any other bidder or with any competitor;

2) Unless otherwise required by law, the prices which have been quoted in this bid have not been knowingly disclosed by the Bidder and will not knowingly be disclosed by the Bidder prior to opening, directly or indirectly, to any other bidder or to any competitor; and

3) No attempt has been made or will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition.

_____Signature of the Bidder or Offeror's Authorized Official

_____Name and Title of the Bidder or Offeror's Authorized Official

_____Date

Sworn and subscribed before me this _____ day of _____, 20___

_____ My commission expires: _____ / _____ / 20___
Notary Public Month Day Year

APPENDIX B – Bid Page

Plan feature services as set forth in the Scope of Services and Minimum Requirements: Provide a per employee per month (PEPM) rate assuming there are approximately 1,882 eligible employees in the plan. *Employee* is defined as an eligible active employee; non-State participating group employee and non-Medicare eligible pensioner and does not include dependents. The services provided and time spent on the services outlined in the "Services Required" section of the RFP should be in your quoted PEPM rates.

			Optional Years - Rate Cap %	
Year 1 **2025**	**Year 2** **2026**	**Year 3** **2027**	**Year 4** **2028**	**Year 5** **2029**
$0.00	$0.00	$0.00	0.00%	0.00%

Service Category	Service Description	Unit Price	Frequency/Duration
Comprehensive Assessment and Evaluation	Initial assessments to identify substance use and mental health concerns.		
Confidential Counseling Services	Individual Counseling Group Therapy		
Crisis Intervention and Support	24/7 crisis hotline for immediate assistance.		
Substance Use Disorder Treatment	Access to outpatient services		
Prevention and Education Programs	Workshops and seminars		
Employee Training	Training to recognize substance abuse signs		
Family Support Services	Counseling, support groups, and resources for family members.		
Relapse Prevention and Aftercare	Follow-up services, ongoing counseling, and support groups post-treatment.		
Workplace Policies and Compliance	Assistance with regulatory guidance for drug and alcohol testing, particularly for safety-sensitive positions.		
Referral Services	Comprehensive network for specialized treatment programs, rehabilitation centers, etc.		
Wellness Programs	Holistic wellness programs focusing		

Service Category	Service Description	Unit Price	Frequency/Duration
	on physical and mental health.		
Legal and Financial Guidance	Legal resources for substance use issues and financial counseling for employees.		
Cultural Competence	Culturally sensitive services for employees from diverse backgrounds.		
Evaluation and Feedback Mechanisms	Regular program evaluations and employee feedback collection.		
Additional Administrative Services	Web Access Telephonic Management Consultation Designated Account Management Printed and Electronic Materials Quarterly Utilization Reports		
DOT/FMCSA Compliance	Ensuring full compliance with DOT/FMCSA regulations regarding drug and alcohol use.		
Training for Supervisors (Specialized)	Specialized training for supervisors to handle substance abuse issues in safety-sensitive roles.		

Optional / Value-Added Services: In addition to the services listed above, list any optional or value-added services not included in the plan features in the Scope of Services, Minimum Requirements, or your quoted PEPM fees above. Indicate whether or not there is a cost, and if so, whether the pricing for each optional service is based on a PEPM fee, hourly rate, or flat fee.

APPENDIX C – BUSINESS ASSOCIATE AGREEMENT

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BA Agreement") is undertaken pursuant to the parties' performance of a certain contract ("Contract") effective, by and between the State of Delaware by and through the Delaware Department of Transportation ("Plan Sponsor"), on its own behalf and on behalf of the group health plan it sponsors for employees or other covered persons (the "Plan"), and ("Vendor").

In the performance of services on behalf of the Plan pursuant to the Contract, and in order for Vendor to use, disclose or create certain information pursuant to the terms of the Contract, some of which may constitute Protected Health Information ("PHI") (defined below), Contractor is a Business Associate of the Plan as that term is defined by the Health Insurance Portability and Accountability Act of 1996, including the modifications required under the American Recovery and Reinvestment Act of 2009 ("ARRA"), and its implementing Administrative Simplification regulations (45 C.F.R. §§142, 160, 162 and 164) ("HIPAA"). Accordingly, Contractor, the Plan and Plan Sponsor mutually agree to modify the Contract to incorporate the terms of this BA Agreement to comply with the requirements of HIPAA, and to include additional provisions that Plan Sponsor, the Plan, and Contractor desire to have as part of the Contract.

Therefore, in consideration of the mutual covenants contained herein and for other good and valuable consideration, the parties agree as follows:

I. DEFINITIONS

The following terms used in the Contract shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

A. Specific Definitions

- Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to the Contract, shall mean Vendor.

- Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to the Contract, shall mean the Plan.

- HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

II. PERMITTED USES AND DISCLOSURES BY VENDOR

A. During the continuance of the Contract, Vendor will perform services necessary in connection with the Plan as outlined in the Contract. These services may include Payment activities, Health Care Operations, and Data Aggregation as these terms are defined in 45 CFR §164.501. In connection with the services to be performed pursuant to the Contract, Vendor is permitted or required to use or disclose PHI it creates or receives for or from the Plan or to request PHI on the Plan's behalf as provided below.

B. **Functions and Activities** on the Plan's Behalf. Unless otherwise limited in this BA Agreement, Vendor may use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Plan as specified in the Contract. Vendor may decide in its own reasonable discretion what uses and disclosures of PHI are required for it to perform administrative services for the Plan as outlined in this BA Agreement and in the Contract as well as in accordance with the law.

1. Use for Vendor's Operations. Vendor may use PHI it creates or receives for or from the Plan for Vendor's proper management and administration or to carry out Vendor's legal responsibilities in connection with services to be provided under the Contract.

2. Disclosures for Vendor's Operations. Vendor may disclose the minimum necessary of such PHI for Vendor's proper management and administration or to carry out Contractor's legal responsibilities, but only if the following conditions are met:
   - The disclosure is required by law; or
   - Vendor obtains reasonable assurance, evidenced by written contract, from any person or organization to which Vendor will disclose such PHI that the person or organization will:
     i. Hold such PHI in confidence and use or further disclose it only for the purpose for which Vendor disclosed it to the person or organization or as required by law; and
     ii. Promptly notify Vendor (who will in turn promptly notify the Plan) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI was breached.

3. Minimum Necessary Standard. In performing functions and activities in connection with the Contract, Vendor agrees to make reasonable efforts to use, disclose or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure or request.

C. Data Aggregation Services. The Plan agrees and recognizes that Vendor performs Data Aggregation services for the Plan, as defined by the HIPAA Rules. In the course of performing normal and customary services under the Contract, this data aggregation is an essential part of Vendor's work on behalf of the Plan under the Contract. Accordingly, Vendor can perform these data aggregation services in its own discretion, subject to any limitations imposed by the Contract. The term "Data Aggregation" is defined under the HIPAA Rules to mean, with respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a covered entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

D. Prohibition on Unauthorized Use or Disclosure

1. Non-permitted Use and Disclosure of PHI. Vendor will neither use nor disclose PHI it creates or receives for or from the Plan or from another Business Associate of the Plan, except as permitted or required by the Contract and this BA Agreement, as required by law, as otherwise permitted in writing by the Plan, or as authorized by a Covered Person.

2. Disclosure to the Plan and the Plan Business Associates. To the extent permitted or required by the Contract and this BA Agreement, Vendor will disclose PHI to other Business Associates of the Plan which the Plan has identified in a writing provided to Vendor. Vendor shall only disclose such PHI to such Business Associates, in their capacity as Business Associates of the Plan. Other than disclosures permitted by this Section II or as otherwise specifically identified in the Contract, Vendor will not disclose Covered Persons' PHI to the Plan or to a Business Associate of the Plan except as directed by the Plan in writing.

3. No Disclosure to Plan Sponsor. Vendor will not disclose any Covered Persons' PHI to Plan Sponsor, except as permitted by and in accordance with Section VII or as otherwise specifically identified in the Contract.

III. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR

A. Vendor will develop, document, implement, maintain and use appropriate administrative, technical and physical safeguards to preserve the integrity and

confidentiality of, and to prevent non-permitted use or disclosure of, PHI created or received for or from the Plan.

B. Vendor agrees to mitigate, to the extent practicable, any harmful effect that is known to Vendor of a use or disclosure of PHI by Vendor in violation of the requirements of this BA Agreement.

C. Vendor agrees to report to Covered Entity, without unreasonable delay and in any event within thirty (30) days, any use or disclosure of the PHI not provided for by this BA Agreement or otherwise in writing by the Plan. Vendor shall maintain a written log recording the date, name of Covered Person and description of PHI for all such unauthorized use or disclosure and shall submit such log to the Plan Sponsor semiannually and by request. Vendor agrees to directly provide notice to any effected participants in the event of a Breach and to send a written log each such Breach and notice to participants to the Covered Entity within thirty (30) days of notification. Vendor agrees to notify participants in accordance with the guidelines and standards set forth by the Department of Health and Human Services under the American Reinvestment & Recovery Act and the HITECH Act. Upon termination of BA Agreement, the Vendor agrees to transfer all logs that contain the accounting of PHI Disclosure to the Plan or a designee.

D. Vendor will require that any agent, including a subcontractor, to whom it provides PHI as permitted by this BA Agreement (or as otherwise permitted with the Plan's prior written approval), agrees to the same restrictions and conditions that apply through this BA Agreement to Vendor with respect to such information.

E. Vendor agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Vendor on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Rules.

F. Vendor agrees to implement administrative, physical, and technical safeguards (as set forth in the Security Rule) that reasonably and appropriately protect the confidentiality and integrity (as set forth in the Security Rule), and the availability of Electronic PHI, if any, that Vendor creates, receives, maintains, or transmits electronically on behalf of Covered Entity. Vendor agrees to establish and maintain security measures sufficient to meet the safe harbor requirements established pursuant to ARRA by making data unreadable, indecipherable, and unusable upon receipt by an unauthorized person. Vendor agrees to provide adequate training to its staff concerning HIPAA and Vendors responsibilities under HIPAA.

G. Vendor agrees to report to Covered Entity any Security Incident of which Vendor becomes aware.

H. Vendor agrees to ensure that any agent, including a subcontractor, to whom it provides Electronic PHI, agrees to implement reasonable and appropriate safeguards to protect such information.

IV. INDIVIDUAL RIGHTS OBLIGATIONS

A. Access. Vendor and the Plan agree that, wherever feasible, and to the extent that responsive information is in the possession of Vendor, Vendor will provide access to PHI as required by 45 CFR §164.524 on the Plan's behalf. Vendor will provide such access according to its own procedures for such access. Vendor represents that its procedures for such access comply with the requirements of 45 CFR §164.524. Such provision of access will not relieve the Plan of any additional and independent obligations to provide access where requested by an individual. Accordingly, upon the Plan's written or electronic request or the direct request of a Covered Person or the Covered Person's Personal Representative, Vendor will make available for inspection and obtaining copies by the Plan, or at the Plan's direction by the Covered Person (or the Covered Person's personal representative), any PHI about the Covered Person created or received for or from the Plan in Vendor's custody or control contained in a Designated Record Set, so that the Plan may meet its access obligations under 45 CFR §164.524. All fees related to this access, as determined by Vendor, shall be borne by Covered Persons seeking access to PHI.

B. Amendment. Vendor and the Plan agree that, wherever feasible, and to the extent that responsive information is in the possession of Vendor, Vendor will amend PHI as required by 45 CFR §164.526 on the Plan's behalf. Vendor will amend such PHI according to its own procedures for such amendment. Vendor represents that its procedures for such amendment comply with the requirements of 45 CFR §164.526. Such amendment will not relieve the Plan of any additional and independent obligations to amend PHI where requested by an individual. Accordingly, upon the Plan's written or electronic request or the direct request of a Covered Person or the Covered Person's Personal Representative, Vendor will amend such PHI contained in a Designated Record Set, in accordance with the requirements of 45 CFR §164.526. Upon receipt of written or electronic notice from the Plan, Vendor will amend or permit the Plan access to amend any portion of the PHI created or received for or from the Plan in Vendor's custody or control, so that the Plan may meet its amendment obligations under 45 CFR §164.526.

C. **Disclosure Accounting.** So that the Plan may meet its disclosure accounting obligations under 45 CFR §164.528, Vendor and the Plan agree that, wherever feasible and to the extent that disclosures have been made by Vendor, Vendor will provide the accounting that is required under 45 CFR §164.528 on the Plan's behalf. Vendor will provide such accounting according to its own procedures for such accounting. Vendor represents that its procedures for such accounting comply with the requirements of 45 CFR §164.528. Such provision of disclosure accounting will not relieve the Plan of any additional and independent obligations to provide disclosure accounting where requested by an individual. Accordingly, upon the Plan's written or electronic request or the direct request of a Covered Person or the Covered Person's Personal Representative, Vendor will provide an accounting as set forth below.

1. Disclosure Tracking

   Starting as of the Effective Date of the Contract, Vendor will record each disclosure of Covered Persons' PHI, which is not exempted from disclosure accounting that Vendor makes to the Plan or to a third party.

   The information about each disclosure that Vendor must record ("Disclosure Information") is (a) the disclosure date, (b) the name and (if known) address of the person or entity to whom Vendor made the disclosure, (c) a brief description of the PHI disclosed, and (d) a brief statement of the purpose of the disclosure.

   For repetitive disclosures of Covered Persons' PHI that Vendor makes for a single purpose to the same person or entity (including the Plan), Vendor may record (a) the Disclosure Information for the first of these repetitive disclosures, (b) the frequency, periodicity or number of these repetitive disclosures, and (c) the date of the last of these repetitive disclosures.

2. Exceptions from Disclosure Tracking

   Vendor is not required to record disclosure information or otherwise account for disclosures of PHI that this BA Agreement or the Plan in writing permits or requires: (i) for the purpose of the Plan's payment activities or health care operations, (ii) to the individual who is the subject of the PHI disclosed, or to that individual's personal representative; (iii) to persons involved in that individual's health care or payment for health care; (iv) for

notification for disaster relief purposes, (v) for national security or intelligence purposes, (vi) to law enforcement officials or correctional institutions regarding inmates; (vii) pursuant to an authorization; (viii) for disclosures of certain PHI made as part of a limited data set; (ix) for certain incidental disclosures that may occur where reasonable safeguards have been implemented; (x) for disclosures prior to April 14, 2003; or (xi) as otherwise excepted under 45 CFR §164.528.

3. Disclosure Tracking Time Periods

Vendor will have available for the Plan or for Covered Persons the Disclosure Information required for the six (6) years immediately preceding the date of the Plan's request for the Disclosure Information (except Vendor will not be required to have Disclosure Information for disclosures occurring before April 14, 2003) or when it was last in effect, whichever is later.

D. Right to Request Restrictions and Confidential Communications. So that the Plan may meet its obligations to evaluate requests for restrictions and confidential communications in connection with the disclosure of PHI under 45 CFR §164.522, Vendor and the Plan agree that, wherever feasible and to the extent that communications are within the control of Vendor, Vendor will perform these evaluations on behalf of the Plan. Vendor will evaluate such requests according to its own procedures for such requests and shall implement such appropriate operational steps as are required by its own procedures. Vendor represents that its procedures for evaluating such requests comply with the requirements of 45 CFR §164.522. Such evaluation will not relieve the Plan of any additional and independent obligations to evaluate restrictions or implement confidential communications where requested by an individual. Accordingly, upon the Plan's written or electronic request or the direct request of a Covered Person or the Covered Person's Personal Representative, Vendor will evaluate requests for restrictions and requests for confidential communications and will respond to these requests as appropriate under Vendor's procedures.

V. OBLIGATIONS OF THE COVERED ENTITY

A. Covered Entity shall provide Vendor with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect Vendor's permitted or required uses and disclosures.

B. Covered Entity shall notify Vendor of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522.

C. Covered Entity shall not request Vendor to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity except as provided in this BA Agreement. In no event shall Covered Entity request Vendor to disclose to Covered Entity or agents of Covered Entity any PHI unless such disclosure is the minimum necessary disclosure that satisfies the request and that such disclosure is solely for the purpose of treatment, payment or plan operations.

VI. BREACH OF PRIVACY OBLIGATIONS

Without limiting the rights of the parties under the Contract, the Plan will have the right to terminate the Contract if Vendor has engaged in a pattern of activity or practice that constitutes a material breach or violation of Vendor's obligations regarding PHI under this BA Agreement and, on notice of such material breach or violation from the Plan, fails to take reasonable steps to cure the breach or end the violation.

If Vendor fails to cure the material breach or end the violation after the Plan's notice, the Plan may terminate the Contract by providing Vendor written notice of termination, stating the uncured material breach or violation that provides the basis for the termination and specifying the effective date of the termination. Such termination shall be effective sixty (60) days from this termination notice.

A. Effect of Termination.

1. Return or Destruction upon Contract End

Upon cancellation, termination, expiration or other conclusion of the Contract, Vendor will if feasible return to the Plan or destroy all PHI, in whatever form or medium (including in any electronic medium under Vendor's custody or control), that Vendor created or received for or from the Plan, including all copies of such PHI that allow identification of any Covered Person who is a subject of the PHI. Vendor will complete such return or destruction as promptly as practical after the effective date of the cancellation, termination, expiration or other conclusion of the Contract.

Following notice, Vendor shall pay the costs incurred in returning or destroying such PHI unless Plan Sponsor agrees to reimburse Vendor for reasonable costs following good faith

negotiation between Vendor and Plan Sponsor subject to the requisite appropriation by the Delaware General Assembly as required by 29 Del. C. §§ 65 and Article 8, Section III of the Delaware Constitution.

2. Disposition When Return or Destruction Not Feasible

The Plan recognizes that in many situations, particularly those involving data aggregation services performed by Contractor for the Plan and others, that it will be infeasible for Contractor to return or destroy PHI. Accordingly, where in Contractor's discretion such return or destruction is infeasible, for any such PHI, upon cancellation, termination, expiration or other conclusion of the Contract, Contractor will limit its further use or disclosure of the PHI to those purposes that make their return to the Plan or destruction infeasible.

VII. PLAN SPONSOR'S PERFORMANCE OF PLAN ADMINISTRATION FUNCTIONS

A. Communication of PHI. Except as specifically agreed upon by Vendor, the Plan and Plan Sponsor, and in compliance with any requirements imposed by this Section VII, all disclosures of PHI from Vendor pursuant to the Contract shall be made to the Plan, except for disclosures related to enrollment or disenrollment in the Plan.

B. Summary Health Information. Upon Plan Sponsor's written request for the purpose either to obtain premium proposals for providing health insurance coverage for the Plan, or (b) modify, amend or terminate the Plan, Vendor is authorized to provide Summary Health Information regarding the Covered Persons in the Plan to Plan Sponsor.

C. Plan Sponsor Representation. Plan Sponsor represents and warrants (A) that the Plan has been established and is maintained pursuant to law, (B) that the Plan provides for the allocation and delegation of responsibilities for the Plan, including the responsibilities assigned to Vendor under the Contract, (C) that the Plan includes or incorporates by reference the appropriate terms of the Contract and this BA Agreement, and (D) that the Plan incorporates the provisions required by 45 CFR §164.504.

D. Plan Sponsor's Certification. Vendor will not disclose Covered Persons' PHI to Plan Sponsor, unless and until the Plan authorizes Vendor in writing to disclose the minimum necessary Covered Persons' PHI to Plan Sponsor for the plan administration functions to be performed by Plan Sponsor as specified in the Plan.

E. Vendor Reliance. Vendor may rely on Plan Sponsor's certification and the Plan's written authorization and will have no obligation to verify that the Plan complies with the requirements of 45 CFR §164.504 or this BA Agreement or that Plan Sponsor is complying with the Plan.

F. The Plan Amendment. Before the Plan will furnish Plan Sponsor's certification described above to Vendor, the Plan will ensure (1) that its Plan establishes the uses and disclosures of Covered Persons' PHI consistent with the requirements of 45 CFR §164 that Plan Sponsor will be permitted and required to make for the plan administration functions Plan Sponsor will perform for the Plan, and (2) that Plan Sponsor agrees to all the applicable conditions imposed by §164.504 on the use or disclosure of PHI.

VIII. MISCELLANEOUS

A. Regulatory References. A reference in this BA Agreement to a section in the HIPAA Rules means the section as in effect or as amended, and for which compliance is required.

B. Survival. The respective rights and obligations of Vendor under Section IV of this BA Agreement shall survive the termination of this BA Agreement.

C. Interpretation. Any ambiguity in this BA Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules. Except to the extent specified by this BA Agreement, all of the terms and conditions of the Contract shall be and remain in full force and effect. In the event of any inconsistency or conflict between this BA Agreement and the Contract, the terms and provisions and conditions of this BA Agreement shall govern and control. Nothing express or implied in this BA Agreement and/or in the Contract is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever. This BA Agreement shall be governed by and construed in accordance with the same internal laws that are applicable to the Contract.

D. Duration. This BA Agreement will continue in full force and effect for as long as the Contract remains in full force and effect. This BA Agreement will terminate upon the cancellation, termination, expiration or other conclusion of the Contract.

E. Term. The Term of this BA Agreement shall be effective as of the date appearing on the signature page, and shall terminate when all of the PHI provided by Covered Entity to Vendor, or created or received by Vendor on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions of this BA Agreement.

F. Amendment. Upon the effective date of any final regulation or amendment to final regulations with respect to the HIPAA Rules, this BA Agreement will automatically amend such that the obligations imposed on Plan Sponsor, the Plan and Vendor remain in compliance with such regulations, unless (1) Contractor elects to terminate the Contract by providing Plan Sponsor and the Plan notice of termination in accordance with the Contract at least thirty (30) days before the effective date of such final regulation or amendment to final regulations; or (2) Vendor notifies the Plan of its objections to any such amendment. In the event of such an objection, the parties will negotiate in good faith in connection with such changes or amendment to the relevant final regulation.

G. Conflicts. The provisions of this BA Agreement will override and control any conflicting provision of the Contract. All nonconflicting provisions of the Contract will remain in full force and effect.

H. Independent Relationship. None of the provisions of this BA Agreement are intended to create, nor will they be deemed to create any relationship between the parties other than that of independent parties contracting with each other as independent parties solely for the purposes of effecting the provisions of this BA Agreement and the Contract.

I. Rights of Third Parties. This BA Agreement is between Vendor and the Plan and the Plan Sponsor and shall not be construed, interpreted, or deemed to confer any rights whatsoever to any third party or parties.

J. Notices. All notices and notifications under this BA Agreement shall be sent in writing by traceable carrier to the listed persons on behalf of Vendor, the Plan and Plan Sponsor at the addresses indicated on the signature page hereof, or such other address as a party may indicate by at least ten (10) days' prior written notice to the other parties. Notices will be effective upon receipt.

K. Expenses. Unless otherwise stated in this BA Agreement or the Contract, each party shall bear its own costs and expenses related to compliance with the above provisions. Any additional expenses incurred by Vendor in connection with services to be provided pursuant to this BA Agreement shall be included in the Contract.

L. Documentation. All documentation that is required by this BA Agreement or by the HIPAA Rules must be retained by Vendor for six (6) years from the date of creation or when it was last in effect, whichever is longer.

APPENDIX D – RESPONSE EXECPTION TRACKING

RESPONSES EXCEPTION TRACKING

Responses must include all exceptions to the requirements, specifications, terms or conditions in the RFP. These are exceptions to the requirement relative to your offering, not an objection to the requirement itself. For example, if the requirement is to provide a certain report within thirty days and you would provide the report within sixty days, that is your offering or response - not an objection to the request or requirement.

☐ By checking this box, the vendor acknowledges that they take no exceptions to the specifications, terms or conditions found in the RFP.

Name of Section Page # And ?#	(Copied) Term	Detailed Exception	Proposed Alternative, if Different

Note: Vendor may use additional pages as necessary, but the format shall be the same as provided above.

APPENDIX E – CYBER RESPONSIBILITIES, LIABILITY

AND INSURANCE

Cyber Responsibilities, Liability, and Insurance

A. Vendor Protection of Customer Data

1. The awarded vendor shall, at a minimum, comply with all Delaware Department of Technology and Information (DTI) security standards identified in this Request for Proposals and any resultant contract(s).

B. Definitions

Data Breach

1. In general, the term "data breach" means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data for the State of Delaware that results in, or there is a reasonable basis to conclude has resulted in:

    1.1 The unauthorized acquisition of personally identifiable information (PII); or

    1.2 Access to PII that is for an unauthorized purpose, or in excess of authorization,

2. Exclusion

    2.1 The term "data breach" does not include any investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

Personally Identifiable Information (PII)

1. Information or data, alone or in combination that identifies or authenticates a particular individual.

    1.1 Such information or data may include, without limitation, Name, Date of birth, Full address (e.g. house number, city, state, and/or zip code), Phone Number, Passwords, PINs, Federal or state tax information, Biometric data, Unique identification numbers (e.g. driver's license number, social security number, credit or debit account numbers, medical records numbers), Criminal history, Citizenship status, Medical information, Financial Information, Usernames, Answers to security questions or other personal identifiers.

2. Information or data that meets the definition ascribed to the term "Personal Information" under §6809(4) of the Gramm-Leach-Bliley Act or other applicable law of the State of Delaware.

Customer Data

1. All data including all text, sound, software, or image files provided to Vendor by, or on behalf of, Delaware which is occasioned by or arises out of the operations, obligations, and responsibilities set forth in this contract.

Security Incident

1. Any unauthorized access to any Customer Data maintained, stored, or transmitted by Delaware or a third party on behalf of Delaware.

C. Responsibilities of Vendor in the Event of a Data Breach

1. Vendor shall notify State of Delaware, Department of Technology and Information (DTI) and State Benefits Office (SBO) without unreasonable delay when the vendor confirms a data breach. Such notification is to include the nature of the breach, the number of records potentially affected, and the specific data potentially affected.

    1.1 Should the State of Delaware or the awarded vendor determine that a data breach has actually occurred; the awarded vendor will immediately take all reasonable and necessary means to mitigate any injury or damage which may arise out of the data breach and shall implement corrective action as determined appropriate by VENDOR, DTI, and SBO.

    1.2 Should any corrective action resultant from Section B.1.1. above include restricted, altered, or severed access to electronic data; final approval of the corrective action shall reside with DTI.

    1.3 In the event of an emergency the awarded vendor may take reasonable corrective action to address the emergency. In such instances the corrective action will not be considered final until approved by DTI.

    1.4 For any record confirmed to have been breached whether such breach was discovered by the awarded vendor, the State, or any other entity and notwithstanding the definition of personally identifiable information as set forth at 6 *Del. C.* § 12B-101 the awarded vendor shall:

        1.4.1. Notify in a form acceptable to the State, any affected individual as may be required by 6 *Del. C*. § 12B-101 of the Delaware Code.

1.4.2. Provide a preliminary written report detailing the nature, extent, and root cause of any such data breach no later than two (2) business days following notice of such a breach.

1.4.3. Meet and confer with representatives of DTI and SBO regarding required remedial action in relation to any such data breach without unreasonable delay.

1.4.4. Bear all costs associated with the investigation, response and recovery from the breach, such as 3-year credit monitoring services, mailing costs, website, and toll-free telephone call center services.

D. No Limitation of Liability for Certain Data Breaches

1. Covered Data Loss

   1.1 The loss of Customer Data that is not (1) Attributable to the instructions, acts or omissions of Delaware or its users or (2) Within the published recovery point objective for the Services

2. Covered Disclosure

   2.1 The disclosure of Customer Data as a result of a successful Security Incident.

3. Notwithstanding any other provision of this contract, there shall be no monetary limitation of vendor's liability for the vendor's breach of its obligations under this contract which proximately causes a (1) Covered Data Loss or (2) Covered Disclosure, where such Covered Data Loss or Covered Disclosure results in any unauthorized public dissemination of PII.

E. Cyber Liability Insurance

1. An awarded vendor unable to meet the DTI Cloud and Offsite Hosting Policy requirement of encrypting PII at rest shall, ***prior to execution of a contract***, present a valid certificate of cyber liability insurance at the levels indicated below. Further, the awarded vendor shall ensure the insurance remains valid for the entire term of the contract, inclusive of any term extension(s).

2. Levels of cyber liability insurance required are based on the number of PII records anticipated to be housed within the solution at any given point in the term of the contract. Should the actual number of PII records exceed the anticipated number, it is the vendor's responsibility to ensure that sufficient coverage is obtained (see table below). In the event that vendor fails to obtain sufficient

coverage, vendor shall be liable to cover damages up to the required coverage amount.

Level	Number of PII records	Level of cyber liability insurance required (occurrence = data breach)
1	1-10,000	$2,000,000 per occurrence
2	10,001 – 50,000	$3,000,000 per occurrence
3	50,001 – 100,000	$4,000,000 per occurrence
4	100,001 – 500,000	$15,000,000 per occurrence
5	500,001 – 1,000,000	$30,000,000 per occurrence
6	1,000,001 – 10,000,000	$100,000,000 per occurrence

F. Compliance

1. The awarded vendor(s) is required to comply with applicable security-related Federal, State, and Local laws.

G. Media Notice

1. No media notice may be issued without the approval of the State.

H. Points of Contact – Data Breach

1. State of Delaware

   Department of Technology and Information
   Aashish Patel, Security Director
   Aashish.Patel@delaware.gov

   Delaware Department of Human Resources
   DelDOT Administration Building
   Michelle Daniels HR Manager/Labor Relations
   Michelle.Daniels@delaware.gov

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-ESP-001	**Revision Number:** 7
Document Type:	Enterprise Policy	**Page:** 1 of 61
Policy Title:	State of Delaware Information Security Policy	

Synopsis:	The goal of this policy is to preserve the Confidentiality, Integrity and Availability (known as the CIA triad) for all State communications and computing resources. Confidentiality ensures that information is accessible only to those authorized to have access. Integrity ensures the accuracy and completeness of the data is safeguarded. And Availability ensures that authorized users have access to the information. In many areas this policy leads the users to more detailed policies, standards, and procedures to help them align with this overall policy. Delaware's Information Security Program is designed to be in alignment with ISO/IEC 27002:2013 (International Organization for Standardization Information Technology – Security techniques - Code of Practice for Information Security Management.)
Authority:	Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the CIO"
Applicability:	This policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as Local Education Agencies, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.
Effective:	2/1/2007
Reviewed:	1/19/2021
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

I. Policy

Policy Compliance

The State of Delaware is committed to safeguarding the State's information assets against unauthorized use, damage, and loss. Information security is everyone's concern and an information security incident that violates an explicit or implicit security policy can come in all shapes and sizes. An intrusion may be a comparatively minor event involving a single site or a major event in which tens of thousands of users or sites are compromised. It is for this reason that compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues and protecting information. Failure to comply with this or any other security policy that results in the compromise of information assets confidentiality, integrity, privacy, or availability may result in appropriate action as permitted by law, rule, regulation or negotiated agreement. Each State Organization will take every step necessary, including legal and administrative measures, to protect its information assets. Also, State Organizations that extend access to Local and Federal governments, as well as others (paramedics/fire companies/DHIN/contractors, etc.) need to ensure that these extended users that are provided this privilege are in alignment with this policy and they must ensure that these users understand and abide by all published policies and standards that impact the use of information assets.

DTI will periodically review compliance with this policy. Each State Organization shall implement a process to determine the level of compliance with this policy. A review to ensure compliance with this policy must be conducted at least annually or as directed by the DTI Chief Security Officer. Organization Management will certify and report the Organization's level of compliance in writing to the DTI Chief Security Officer. Areas where compliance with the policy requirements are not met will be documented and a plan will be developed to address deficiencies. The DTI Chief Security Officer will submit the applicable findings in writing to the Organization Head and Organization Information Security Officer (ISO) for review and follow up. This review process is facilitated with the State of Delaware Information Security Policy (DISP) Scorecard that is produced every other year/biennial.

In addition to this policy, State organizations are required to comply with applicable security-related Federal, State, and Local laws, including the following:

- Delaware Security Breach Notification (Title 6, Commerce and Trade, Chapter 12B. Computer Security Breaches).
- Health Insurance Portability Accountability Act of 1996 (HIPAA).
- The Privacy Act of 1974, 5 U.S.C. § 552 a, Public Law No. 93-579.
- Gramm-Leach Bliley Act (GLB Act), also known as the Financial Modernization Act of 1999.
- The Sarbanes-Oxley Act of 2002 (SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002.
- Federal Information Security Management Act of 2002 (FISMA).
- National Security Presidential Directive 38 – National Strategy to Secure Cyberspace.
- National Security Presidential Directive 51 – National Continuity Policy.
- National Security Presidential Directive 54 – Comprehensive National Cyber Security Initiative.
- Federal Preparedness Circular 65 – Continuity of Operations.
- Children's Internet Protection Act (CIPA).
- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
- Tax Information Security Guidelines for Federal, State, and Local Agencies, Safeguard for Protecting Federal Tax Returns and Return IRS Publication 1075 (Rev. 11-2016).
- Agencies carry the responsibility to understand and abide by specific compliance requirements that are specialized and unique to them.

General Security

Related Documents

Related ISO 27002:2013 clause(s): **5.1.1**

Related published State, DTI policies, standards, and procedures are available for review at https://dti.delaware.gov/technology-services/standards-and-policies/.

Roles

Related ISO 27002:2013 clause(s): **6.1.1, 6.1.3, 6.1.4, 7.1.2, 7.3.1, 8.1.1, 8.1.2, 8.1.3, 13.2.4, 18.2.2**

Data Owner

Data in use by State of Delaware organizations, in transit through, or residing within the State's computing infrastructure or in State contracted external hosting facilities are considered State property and owned and controlled by the State of Delaware according to statute.
Please consult the ISO 27002 standard for clarification.

Data Steward

The head of a state organization, or an employee delegated by the head of the organization, with appropriate knowledge and authority to carry out the responsibilities of the Data Steward as defined in this policy. The Data Steward will have a cleared background check.

Acquires, creates, and maintains information about the data within their assigned area of control and reports this to the DTI Data Management Office. All assets must be clearly documented in a single repository and updated at least every six months. The inventory shall include the type of asset, format, Data Steward, ISO, Data Custodian, data classification, DR criticality level, location, backup information, license information, and a business value.

A current inventory of assets helps to ensure that effective asset protection and risk management takes place, and is required for other business purposes, such as health and safety, insurance or financial asset management reasons.

Data Stewards should be aware that data classification applies to all copies of the data regardless of form or media, especially backups. Full compliance will require a thorough examination of retention periods, numbers of copies, and proliferation of data.

Sending and Receiving Data:

The following definitions apply when an organization sends data to or receives data from another entity within the State or outside the State.

- **Sending Data Steward** – The Data Steward (or equivalent if outside the State) of the source data being sent.
- **Receiving Data Steward** – The Data Steward (or equivalent if outside the State) of the data being received.

1. Analyze all computerized data for appropriate data classification at regular intervals as the data/databases are updated or changed. The Data Steward maintains a working knowledge of the data under their care and aligns the organization's data classification selections with it.
2. Establishes Data Privacy rules as appropriate.
3. Notifies the DTI Data Management Office in advance of any planned changes in the type of data (new data base, new interface, decommissioned or archived databases, for example) in their area of control.
4. Evaluates and approves requests for data transfers to or from another party. These parties may be State organizations or external partners or hosting providers.
5. The Sending Data Steward is to clearly communicate to the Receiving Data Steward the classification of the data to be transferred,
6. Obtains written or otherwise binding documentation whereby the Receiving Data Steward agrees to treat the transmitted data according to the classification as declared by the Sending Data Steward. (Upon transfer of the data, the Receiving Data Steward bears the responsibility for properly protecting that data.)
7. The Sending Data Steward must take into consideration any issues involved in releasing this data outside of the State and, if deemed appropriate, may increase the data classification rating.
8. Ensures appropriate data retention periods according to State and Federal laws and organization policies.
9. Ensures appropriate backups are taken and tested.

10. Restricts computer applications and data access to authorized persons in coordination with the Data Custodian.

11. Attends classes or takes Computer Based Training in accordance with DTI Data Management Office requirements.

12. Ensures, in conjunction with the organization's Information Security Officer (ISO) and the Data Custodian, the implementation and enforcement of appropriate security control procedures to protect the data against unauthorized modification, destruction, or disclosure.

13. Reviews and recommends changes to the handling of data with respect to integrity, security and privacy.

14. Authorizes appropriate data access to Data Users. This process is coordinated through the Information Security Officer (ISO) and the use of the Statewide Security Request System

- The data classification hierarchy is implemented and adhered to for the types of data processed for their particular business unit/department. See Data Classification Policy.

- Data is categorized for the area that the business unit/department manager (Data Steward) has been designated as a Steward using classifications defined in the Data Classification Policy.

15. Ensures appropriate continuity of operations planning efforts exists including a defined State organization liaison to work with authorities.

16. Ensures the planning and testing of COOP efforts at least annually with the appropriate State of Delaware BC/DR criticality recovery requirements.

17. Categorizes data application systems according to a criticality scale defined by the business unit/department according to the Disaster Recovery/Continuity of Operations Plan (DR/COOP) criticality levels.

18. Ensures that user and system administrator access to data is on a need-to-know basis rather than by rank, position, or affiliation-based. Personnel must undergo appropriate screening relevant to the classification of the data.

19. Adheres to appropriate Federal and State privacy regulations in the classification of data.

20. Checks are periodically made to ensure that data classifications are appropriate and that safeguards remain valid and operative.

21. Reports and coordinates all requests for deviations or clarifications to any Data Policy with the DTI Data Management Office.

22. Documents and coordinates such with the DTI Data Management Office all delegated responsibilities, including the submission of security access requests to specific Data Custodians as needed.

Data Custodian

A Data Custodian is an IT individual who works with the Data Steward to oversee and implement the necessary safeguards to protect the information assets in compliance with the policies, rules, and regulations governing the types and classification of the data. Data Custodians must remain current with applicable certifications, available training and data management best practices.

1. Provides information technology services that are consistent with the instructions of the Data Steward, including information security measures such as data access controls. Using physical and logical access control and audit/monitoring systems, the Data Custodians must protection of the data in their possession from unauthorized access, alteration, destruction, or usage. Data Custodians are individuals who have the administrative rights to access, modify, delete, and/or utilize data as authorized in writing by the Data Steward.
2. Oversees the operation of information systems to ensure the confidentiality, integrity, and availability of data in their care is maintained as directed by

Federal and State law, State Policies and Standards and organization management.

3. Responsible for viewing/amending/updating the information metadata.
4. Reports any violation of this policy to the Data Steward, the DTI Data Management Team, The DTI IT Security Team, DTI Chief Security Officer, and their organization's supervisor/manager. This includes violations by employees, casual seasonal employees, temporary personnel, contractors, vendors and all State third party associates.
5. All State of Delaware data must have a designated Data Custodian who is responsible for implements and maintains requisite security controls prescribed in relevant policies, procedures, guidelines, and standards.
6. Approves security access requests as needed at the appointment of the Data Steward.
7. Data Custodians must ensures that the information is used only for the purposes specifically approved by the Data Steward. Data Custodians must also comply with all security measures defined by the Data Steward and the DTI Chief Security Office and Data Management Team. Additionally, Data Custodians must refrain from disclosing data in their possession (unless it is designated as State of Delaware Public) without first obtaining permission from the Data Steward.
8. Reports to their manager, ISO, IRM, DTI Chief Security Officer and DTI Data Management Office all situations where they believe an information security vulnerability or violation may exist. Local management must also provide Data Custodians with sufficient time and materials to receive periodic information security training.

Data User

Data Users are authorized users who access information assets and use the State's data. This also includes the use of data on an individual's State issued computer and any related files shares. A Data User can be an employee, casual seasonal employee, temporary personnel, contractor, vendors, outsourcers, and/or all others who have access to the State's data.

State Chief Information Officer

The Chief Information Officer (CIO) in Delaware is an Organization Head and is also the Secretary of the Department of Technology & Information. As such, the CIO is the key advisor to the Governor on all matters regarding technology and telecommunications. The CIO is also the primary liaison in all Information Technology (IT) matters with the Legislative and Judicial branches of State government. The CIO is responsible For:

- Developing the establishment of State of Delaware Information Technology Policy that best supports the States' IT security goals, statewide direction, and objectives.
- Ensuring that officials have thorough and accurate information to inform IT decision making.
- Monitor the overall effectiveness of policy through performance monitoring and reporting.

DTI Chief Security Officer

The DTI Chief Security Officer (CSO) takes primary responsibility for the information security-related affairs of the entire State enterprise. The CSO is responsible for providing a governance structure for Information Security, Disaster Recovery, and Continuity of Operations. The CSO is responsible for the developing, communicating, management, and enforcing of the overall Statewide Information Security Program to include the State of Delaware Information Security Policy, and logical and physical controls, as well as the coordination of efforts between DTI staff and other State organizations. The CSO directs and supports DTI security professionals in the attainment of objectives. The CSO is responsible for:

- Developing and managing the statewide Continuity of Business/Disaster Recovery Program.
- Identifying strengths, areas of vulnerability and opportunities to mitigate risks.
- Establishing an enterprise-wide information security, disaster recovery and COOP education and awareness program.
- Coordinating efforts between DTI staff and other State organizations.
- Directing and supporting DTI security professionals in the attainment of objectives.

- Protecting the cyber security of State resources and ensuring that the personnel can respond and recover those resources in the event of a disaster.
- Managing the development, implementation, and enforcement of DTI-wide physical security policies, procedures, guidelines, and standards.
- Managing the development and implementation of statewide information security policies, procedures, guidelines, and standards.
- Measuring information security performance and reporting regularly to senior executives and management.
- Ensuring that Delaware is at a high state of readiness for responding to incidents, to include a cyber terrorist attack.
- Interfacing with customers and partners on issues related to security, disaster recovery, and COOP.

DTI Chief Security Officer Team

The DTI Chief Security Officer (CSO) Team takes primary responsibility for communicating and enforcing CSO directives pertaining to the information security-related affairs of the enterprise. The DTI CSO Team supports the State's mission and objectives by providing security-related services to the various State organizations. This involves the coordination of efforts between technical persons and business persons responsible for data and its security.

The DTI CSO Team must be independent of both development and operations staff.

DTI is responsible for working with the Organization ISO Team, the Technology and Architecture Standards Committee (TASC), and other DTI teams and/or committees to:

- Enforce statewide information security policies, procedures, guidelines, and standards.
- Educate the general user population on the information security policies
- Assist State organizations in developing and implementing their own disaster recovery and continuity of operation plans.

- Annually test and validate information security, disaster recovery, and COOP controls.
- Offer appropriate training and awareness programs for information security, disaster recovery, and COOP.
- Administer the information security exception process.
- Monitor, evaluate, and modify the Information Security and COOP/DR program with respect to relevant changes in technology, the sensitivity of its customer information, known or perceived internal or external threats, and the changing business arrangements or changes to customer information systems.
- Retain Subject Matter Experts for information security affairs as needed.

Organization Information Security Officers

Organization Information Security Officers (ISOs) are individuals who are responsible for all security aspects within their organization on a day-to-day basis. These ISOs are responsible for the implementation and monitoring of security controls on an operational basis. They serve as the primary point of contact for security issues within their assigned organization or department. Their responsibilities include, but are not limited to:

- Conduct periodic, at least annually, risk assessments of information and data assets.
- Provide situation awareness of security-related issues to DTI.
- Participate in the investigation of organization level information security incidents or violations of State security policies and report them to management.
- Investigating and reporting local level security incidents or violations.
- Conduct periodic, at least annually, reviews to ensure compliance with security standards and policies.
- Initiating incident reporting or issues of non-compliance to the organization head and to DTI.
- Prepare and submit security reports to the organization head and to DTI as needed.
- Periodically test information security.

- Annually test disaster recovery, and COOP controls.
- Offer and participate in training and awareness programs for information security, disaster recovery, and COOP.

Organization Head

The Organization Head, typically the Cabinet Secretary, Department Head, School Superintendent, or Elected Official is ultimately responsible for managing information risk in their organization. An Organization Head could formally delegate performance of these tasks and activities, but at all times remains accountable for such activities. Key responsibilities include the following:

- Ensure that information risk is assessed, monitored and managed in compliance with regulatory requirements and Policies and Standards for Information Security.
- Maintain an inventory that establishes clear ownership of the major information and data assets in the organization.
- Periodic reporting occurs, at least quarterly, on the status of information security across the organization.
- Ensure that information security requirements for services provided by outside providers are defined, implemented, maintained and supported with appropriate agreements.

All Staff

All staff is personally responsible for information security. The roles and responsibilities of staff is defined in local policies and procedures and incorporated into the staff orientation process. All staff has the following responsibility:

- Compliance with the State of Delaware Information Security policies, procedures and standards established to maintain the confidentiality, integrity and availability of State information and data assets.
- Actions associated with assigned accounts, equipment, and removable media.

- Protecting the secrecy of their passwords.
- Participating in risk assessment processes as requested by management.
- Reporting known or suspected security incidents.
- Participate in annual information security awareness training.
- Users must report any weaknesses in State computer security, and any incidents of possible misuse or violation of this policy to their manager, ISO, IRM, or DTI management. Any weaknesses that are a threat to State infrastructure are promptly reported to DTI.
- Users must not attempt to access any data or programs contained on State systems for which they do not have authorization or explicit consent.

Changes in Status

Any changes to employment status of personnel must be reported to the organization ISO by the hiring manager and/or organization's human resource personnel within two (2) days prior to the last day of employment or the day of employment termination. The ISO must then notify the Enterprise Security Operations Team of any access changes to DTI managed systems.

Due to promotions, transfers, retirements, etc., the individuals who serve the roles of Data Stewards and Data Custodians may change on a regular basis. When there is a change in the Data Stewards and/or Data Custodians it is the responsibility of the local manager to report status changes to the Organization Head and to the DTI ISO via an email and a follow up appointment letter. This notification is required for all data that is hosted or co-located at DTI. Data Stewards must maintain access control systems so that previously provided access privileges are no longer provided whenever there has been a Data Custodian status change. When a Data Steward has a change in status, it is the responsibility of the Organization Head to promptly designate a new Data Steward and notify affected parties. This policy applies to all employees, casual seasonal employees, temporary personnel, contractors, vendors, outsourcers, and/or all others who have access to the State's data.

This policy applies, but is not limited to, unique user access credentials accessing state and local networks, ACF2, email, state databases as well as remote security access keys

Asset Inventory and Data Classification

Related ISO 27002:2013 clause(s): 8.1.1, 8.2.1

Consult the Data Classification Policies.

Disaster Recovery/Continuity of Operations Plan (DR/COOP) Criticality Classifications

Related ISO 27002:2013 clause(s): **8.2.1, 17.1.1, 17.1.2, 17.1.3**

Production systems must be categorized based on a Business Impact Analysis each with separate handling requirements. This criticality classification system is used statewide, and forms an integral part of the Continuity of Operations Planning process.

Critical (1)

Loss of business function threatens the ability for the State to operate and disrupts the security and well-being of the State.

Significant (2)

Loss of business function significantly reduces the effectiveness of the State's operations, has a negative citizen impact and affects the financial well-being of the State.

Moderate (3)

Loss of business function affects multiple State Organizations and their ability to operate, has a negative citizen impact and impacts a State Organization's mission critical business function.

Limited (4)

Loss of business function is limited to only the person or State Organization using the application and has little or no effect on the State's ability to carry out business.

Minimal (5)

Loss of business function does not have a direct impact on a State Organization's ability to do business.

Policy Maintenance

Related ISO 27002:2013 clause(s): **5.1.2, 18.1.1**

Periodic Policy Review and Evaluation

The State of Delaware Information Security Policy is subject to a policy review at least annually by DTI. The purpose of the review is to assure that the policy is up-to-date with respect to the current data assets, potential threats, applicable legislation, and other changes that impact information security.

Minor changes, such as hyperlink updates, do not require the full approval process.

Exception Process

In rare circumstances, exceptions to this policy are permitted if the DTI Chief Security Officer (CSO) has signed off in writing.

Consequences and Disciplinary Action

Related ISO 27002:2013 clause(s): **7.2.3, 7.3.1**

Failure to comply with the policy is a serious matter, whether through intentional act or negligence, and is grounds for discipline up to and including dismissal based on the just cause standard set forth by Merit Rules, or collective bargaining agreement, whichever is applicable to the subject employee. Exempt employees are subject to appropriate discipline without recourse, except as provided by law. While DTI has no authority to discipline employees or other parties of other State Organizations in the Legislative or Judicial branches of government, it shall take the appropriate steps to ensure any misconduct is appropriately addressed.

Administrative Safeguards

Privacy

Related ISO 27002:2013 clause(s): **7.1.2, 7.2.1, 8.1.3, 16.1.2, 16.1.3**

To manage systems and enforce security, State Information Security personnel may log, review, and otherwise utilize any information stored on or passing through its

computing resources systems. For these same purposes, the State may also capture user activity such as telephone numbers dialed and Web sites visited. DTI management reserves the right to examine electronic mail messages, files on personal computers, Web browser cache files, Web browser bookmarks, logs of Web sites visited, and other data stored on or passing through State computers as permitted by Federal and State laws, policies, standards, and guidelines. Such management access assures compliance with internal policies, assists with internal investigations, and assists with the management of State information systems.

Therefore, electronic data created, hosted, managed, sent, received, or stored on computing resources owned, leased, administered, hosted by another entity, or otherwise under the custody and control of a State entity are not private and are accessed by authorized DTI employees. Authorized DTI employees have exclusive right to monitor and inspect an individual user data or other information, and will do so in the normal course of business to ensure the security of the State's information systems and/or at the request of a State investigative authority or a law enforcement agency at any time without knowledge of the computing resource's user or owner. No Data User shall have any expectation of privacy as to his or her Information System usage. DTI shall cooperate with any organization, as users of these resources, should they have a need to have access to these records. See eRecords request – Disclosure of Individual User e-Resource Records.

Random, scheduled and/or routine searches, logs, reviews, and examinations conducted by DTI and not initiated by the Organization that result in possible acceptable use and/or security violations must be reported to the Organization's ISO within four (4) business days.

This policy includes a commitment to maintaining the security, confidentiality and privacy of personal information. State Organizations shall take reasonable steps, through contractual or other means, to ensure that a comparable level of personal information protection is implemented by suppliers and agents who provide services to the State of Delaware, which involve handling of personal information in any form.

For additional information, consult the Acceptable Use Policy, Data Classification Policy, and Offshore IT Staffing Policy.

Security Clearances

Related ISO 27002:2013 clause(s): **7.1.1, 13.2.4, 15.1.2, 15.1.3**

All new hires and transfers into Information Technology (IT) employees (fulltime, part-time, casual/seasonal, and temporary) with a hire date on or after August 14, 2008 are required to pass a criminal background check. Also, it is strongly recommended that all IT employees sign a Non-Disclosure agreement.

In addition, it is strongly recommended that all IT contractors, IT vendors, and other IT third-party service providers sign a Non-Disclosure Agreement. If they handle State non-public data, it is strongly recommended that they pass a criminal background check.

All IT employees, IT contractors and IT vendors must sign an Acceptable Use Policy, if they require access to the State network.

A criminal background check consists of providing fingerprints for a full State Bureau of Identification (SBI) and Federal Bureau of Investigation (FBI) check or a third party CBC process approved by DTI. The outcome of these checks determines hiring approval, system and facility access, and access required to perform job duties at State Organizations.

As a general policy, clearance is not provided to any person who has been convicted of a felony or class A misdemeanor. State Organizations retain discretion regarding expunged convictions and convictions for offenses other than felonies or class A misdemeanors. Exceptions are made upon review of extenuating circumstances, such as the length of time since the last conviction. In these instances, a case-by-case evaluation is made by the State Organization Head in conjunction with the Human Resource Management Division of the Office of Management and Budget (OMB/HRM) to ensure that exceptions are handled consistently across the State.

The State of Delaware and State Organizations retain the right to run random checks on active employees, contractors, and vendors and terminate employment when the findings are in violation of this policy. Checks also are run at the request of the Organization Head and/or the Chief Information Officer (CIO).

For returning employees, if the last background check was completed more than twelve (12) months ago, a full background check is required with new fingerprints. If the last background check was conducted less than twelve (12) months ago, a background check with the existing fingerprints on file is performed. See DTI Security Clearance Policy (accessible via the State network only).

The Organization ISO is responsible for ensuring compliance with the criminal background check requirement for its users and employees and the affected Organizations are responsible for processing these checks through the State Bureau

of Identification (SBI) and responsible for the costs associated with these checks. With respect to IT contractors, IT vendors and other IT third-party service providers requiring a criminal background check, Organizations reserve the right to require vendors, contractors and third-party providers to assume responsibility for the costs associated with processing criminal background checks.

Information collected is handled in accordance with all appropriate methods to ensure privacy, confidentiality, and compliance with applicable laws. This policy does not supplant applicable court orders and/or applicable laws.

Authentication and Authorization

Related ISO 27002:2013 clause(s): **9.1.1, 9.2.1, 9.2.2, 9.2.3, 9.3.1**

Access to all information is approved and authorized by the Data Steward on a need-to-know basis.

Authorization must be documented via an appropriate request process that involves specific approvals by organization management.

All business applications or systems are secured by access controls compliant with approved State standards.

Multiple-factor authentication will become part of the authentication process as appropriate.

Identity and Access Management Service

- State Identity Solution - Identity and access management, or IAM, is the process of codifying not only users and groups in a software system, but also what resources they are each able to access and what functions they are each able to perform. IAM addresses authentication, authorization, and access control. The State Identity Solution is an Enterprise Service and solution detail can be found via the Enterprise Services Guide available upon request from EA or the Partner Services Engagement Team.

Privileged Access Rights

Related ISO 27001:2013 clause(s): **9.2.3, IRS Publication 1075: Account Management, pp. 56-57**

Inappropriate use of system administration privileges is a contributor to failures or breaches of systems. Administrative privileges allow access to resources that are unavailable to most users and permit the execution of actions that would otherwise be restricted. When such privileges are administered improperly, granted widely, and not closely audited, attackers are able to exploit them and move effortlessly through a network.

The assignment and use of privileged access rights shall be restricted, controlled, and minimized. Members in privileged groups are high value targets for attackers. Privileged accounts shall be restricted to a limited number of individuals with a clear need to perform administrative duties. Non-privileged users shall be prevented from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

Implementation Requirements:

1) Privileged access rights shall be allocated to users on a need-to-use basis and on an event-by-event basis, using the minimum requirement for their functional roles.
2) Privileged access rights shall not be granted until the authorization process is complete.
3) An inventory of all privileges allocated shall be maintained and validated at least annually.
4) Regular business activities shall not be performed from privileged ID. Privileged accounts shall not be used to perform general tasks such as accessing emails and browsing the Internet.
5) The job responsibilities of users with privileged access rights shall be reviewed at least annually in order to verify if they are in line with their duties.
6) Shared generic administration user IDs are discouraged. When unavoidable, the confidentiality of secret authentication information shall be rigorously maintained. For example, a password vault where an approved user would check out an ID and check it back in with a one-time password that changes when it is checked back in.
7) Multi-factor authentication shall be implemented for all remote network access to privileged and non-privileged accounts.
8) Where possible, system administrators shall not have permission to erase or de-activate logs of their own activities.

Unique User Access Credentials

Related ISO 27002:2013 clause(s): **9.1.2. 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.1, 9.4.2, 9.4.4, 11.2.2**

All Data Users must have unique user access credentials. Access to computing resources via a shared username, shared passwords, shared access credentials and anonymous logins is strictly prohibited.

All personnel must treat passwords and other access credentials as private and highly confidential.

All Data Users are responsible for all activity performed with their personal IDs. These IDs are not authorized to be utilized by anyone but the individual to whom they have been issued.

Security access for non-Full Time Employees (Non-FTE) (contractor, vendor, casual/seasonal, temporary personnel, etc.) must be set to expire no more than one (1) year from the date of the initial approved security access request. If needed, a new security access request for renewal can be submitted prior to expiration of said access for a period of no more than one year.

A machine/system/interface User ID is a set of access credentials that facilitates the automated transfer of data files between machines with no human intervention. These User IDs are not attached to any individual and therefore the User ID name is the name of the process in combination with the job number. It is acceptable for this class of User ID to not require an expiration date. The individual ultimately responsible for placement and activity of such a User ID is the applicable Data Steward and the ISO.

Administrator Accounts require special protection commensurate with the data that is accessed/controlled. This is also known as a privileged account. See Data Classification Policy.

Identification: General

Related ISO 27002:2013 clause(s): **9.2, 9.2.1, 9.2.3, 9.2.5, 9.3, IRS Publication 1075: 9.3.7, IA-1**

Management of Identifiers Associated with Federal Tax Information (FTI)

Identifiers/User IDs are a controlled value within the State's network, systems, and databases. They are not to be shared.

The following are required attributes of Identifiers/User IDs:

1. User ID cannot be reassigned to another individual after the original person leaves. Any deviation from this requires the approval of the DTI Chief Security Officer.
2. User ID and associated access is allocated by the ISO and signed off by the Data Custodian when applicable based on job functions assigned to the individual.
3. When applicable, Mainframe User ID access will be processed through the standard request process via DTI's Service Desk request system. This activity will include creating, managing, adding access, removing access, and deleting the User ID as required.
4. Mainframe User ID will follow the naming standard currently identified by Enterprise Security Operations Team.
5. Mainframe Accounts will be reviewed at least twice a year for correctness and usage. See the Disabling Inactive Accounts section below.
6. Mainframe Accounts will be updated when an individual's employment status or job functions change. (New hire, transfer, termination of employment, and/or access no longer required).
7. Record of Mainframe access request for User ID will be retained for a specific timeframe as required by the DTI retention schedule.

Life cycle of identifiers/user IDs will be in compliance with IRS Publication 1075 (Section 9.3.7, page 76 - 78, and IA-1 on page F-90 of the NIST SP 800-53r4).

Password Management

Related ISO 27002:2013 clause(s): **9.2.3, 9.2.4, 9.3.1, 9.4.2, 9.4**

The Organizations shall ensure information security user access credentials, such as user IDs and passwords, are aligned with State policies and standards.

User IDs and passwords (access credentials) for new users must be distributed in a secure manner. User credentials must not be sent by email unless it is encrypted. Initial passwords are set up in a way so non-authorized individuals cannot gain access.

Initial passwords shall require changing on initial login and after requesting a password reset.

Passwords shall conform to guidelines presented in the Identity and Access Management Guidelines documentation.

Passwords must not be sent in clear text during logon process and must not be comprised of personal identifiable information which can uniquely identify a person. Examples are social security number, name, date of birth, etc.

Passwords must not be recorded and stored on paper or electronically, in human readable form. Exceptions are granted for specific IT administration applications with the approval of the Data Steward. Passwords are encrypted when electronically stored or transmitted. Any exceptions must be reviewed, approved, or denied by the DTI Chief Security Officer (CSO).

For additional information, consult the Identity and Access Management Guidelines.

Circumvention of the Password Policy

Data Custodians shall ensure that the Password Policy is not circumvented. Examples of circumventions include auto logon, remembering user access credentials, embedded scripts, clear text transmission of passwords, or hard coded passwords in software. If the security of a password is in doubt, the password must be changed immediately. Password resets require formal user validation. When a password requires a reset or changes on a production critical system, a password change request process is required.

Computing Resource Log Off and Screensavers

Related ISO 27002:2013 clause(s): **11.2.8, 11.2.9**

All Staff shall log off, lock-out or implement a secure mechanism to prevent unauthorized entry to their workstation or other computing resource(s). Password protected screensavers or terminal locks must be activated after inactivity. Users must not attempt to circumvent the use of these controls. All systems and workstations shall have a password protected automatic log-off, lock-out screensaver or secure mechanism to prevent unauthorized entry.

Login Failure Lockout

Related ISO 27002:2013 clause(s): **9.4.2**

Login failure lockout is an effective defense against brute force hacker attacks.

After a specified number of consecutive authentication failures, users are locked out of the resources to which they are attempting to gain access and shall need to have their account manually reset.

Multiple failed login attempts to access systems, applications, platforms, and network appliances must be reviewed by a Data Custodian within a 24-hour period.

Disabling Inactive Accounts

Related ISO 27002:2013 clause(s): **9.2.4, 9.2.6**

User accounts that are not used for at least ninety (90) days are disabled.

Accounts on all platforms are reviewed at least twice a year for usage and activity and the status evaluated by the ISO and Data Steward. Where applicable, a list of unused and inactive user IDs is sent to the Organization ISOs by DTI. Accounts that are dormant over ninety (90) calendar days are evaluated and deleted by the Organization ISO. This includes both local and state email credentialed accounts.

Active machine IDs accounts that are used for machine to machine processing with no human intervention are the only exception to this requirement. Examples are accounts for automated file transfers, printers, batch, or starter tasks.

The ISO and/or network administrator are responsible for ensuring Active Directory (AD) accounts are accurate, including deleting accounts within two (2) days of personnel changes. Audits are conducted at least twice per year for usage and activity. Stale accounts (accounts that have not logged into the system for over ninety (90) days) are evaluated and if appropriate deleted by the Agency's AD Organizational Unit (OU) manager. If required, the mail associated with this account is transferred to an agency appointed person by submitting an eRecords Request Form to the DTI Executive Branch. An "Out of Office" response is configured for a period of two (2) weeks prior to deleting the account for notification purposes. AD policies are in place to automatically purge the associated mailbox thirty (30) days after the AD account has been deleted.

The organization ISO shall follow DTI's policies, standards, and directives to exercise sound judgment through the life cycle of accounts. The organization ISOs are required to monitor and maintain control over the accounts he/she requests for

approval, creation, modification, and deletion on all State platforms. All activities related to accounts are submitted through the current process.

All requests to retain unused accounts beyond one (1) year require approval by the DTI Chief Security Officer (CSO).

Review of System Access

Related ISO 27002:2013 clause(s): **9.2.5**

System access and privileges are reviewed at least once per year. Data Stewards are responsible to oversee that the review of system access and privileges are performed. Data Custodians/ISOs will perform the review of the system access and privileges to ensure that they are revoked when no longer needed.

Roles Based

Related ISO 27002:2013 clause(s): **9.2.3**

Profiles are set up on all systems to restrict user access to only the information and access needed to perform job functions. Captive accounts (no operating system level access) are required. It is the responsibility of the Data Steward and ISO to review the profiles at least once per year to ensure that individuals do not have access above and beyond what is needed to perform their job function. The Enterprise Security Operations Team is available to provide additional guidance.

Terminations and Transfers

Related ISO 27002:2013 clause(s): **7.1.2, 7.3.1, 8.1.4, 9.2.6**

Each employee manager is responsible for providing prompt notification to their Human Resources Office and/or Organization ISO when there is a change to an employee or vendor status. This includes changes in a job function that may impact the type of information they are authorized to access. The ISO shall work with Human Resources and/or the hiring manager to cross check all terminations and transfers, and ensure that all State assets are returned.

Access shall expire on the last day of employment or transfer. Timeliness in carrying out these responsibilities will help to maintain effective account maintenance and will mitigate security risks.

Segregation of Duties

Related ISO 27002:2013 clause(s): **6.1.2, 12.7.1, 14.2.6**

The principle of segregation of duties will be employed when designing and defining job duties. Organizations must implement processes and control procedures that, to the extent feasible, segregate duties among employees and that include effective oversight of activities and transactions.

To the extent possible, at least two (2) people must coordinate their information-handling activities; one (1) to perform the critical work/task, and one (1) to audit the critical work/task. Findings from such audits must be provided to those originally tasked for corrective action.

Beyond that which they need to do their jobs, staff must not be given access to, or permitted to modify production data, production programs, or the operating system.

Segregation of Production and Test

Related ISO 27002:2013 clause(s): **12.1.4, 13.1.3**

Production, development, and test environments must be kept strictly separate, either physically, logically, or virtually, with strictly enforced access controls.

Change Control

Related ISO 27002:2013 clause(s): **12.1.2, 12.5, 12.5.1, 14.1.1, 14.2.2**

Every change to a production State computing resource, such as operating systems, computing hardware, networks, and applications, is subject to this policy and must follow appropriate change control procedures.

System Documentation

Related ISO 27002:2013 clause(s): **6.1.5, 12.1.1, 14.2.2**

System documentation is a necessary part of the State's information system management. Such documentation is kept up-to-date by authorized staff and available using existing tools and resources, and placed in read-only format in a secure, organization central document repository or a secure, document management solution.

Security Awareness and Training

Related ISO 27002:2013 clause(s): **6.1.4, 7.2.1, 7.2.2**

DTI provides regular information security awareness communications to all staff, including contractors, by various means, such as webcasts, briefings, newsletters, advisories, etc. in direct support of the ISOs and IRMs, and System Administrators.

Furthermore, DTI takes its responsibility seriously to assist managers and ISO personnel in conducting relevant training for their users and their involvement with relevant industry special interest groups.

Effective January 1, 2012, all Executive Branch employees, contractors, temporary and casual seasonal staff that require a state email account must complete a computer based training (CBT) class that covers non-technical material about information security basics, suitable for users at all knowledge levels. This training will help staff become knowledgeable of ways to minimize security risks and ensure they understand the importance of protecting sensitive citizen and State data.

Protection from Malicious Software

Related ISO 27002:2013 clause(s): **12.2, 12.2.1**

All computing resources must be current with operating system and software security patches and virus protection software before connecting to the network, and configured to stay current as new patches are released. More guidance is located within the Software Policy.

All computing resources must run State standard real-time virus protection software. The virus protection software is not disabled or altered in a manner that shall reduce the effectiveness of the software. The software's virus definitions are kept current on a regular scheduled basis.

For users who access the network from home or other remote locations, a Secure Remote Access service is provided as an enterprise service in the Enterprise Services standard.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and is reported to the Organization ISO. (See Security Incident Procedures, below.) Endpoint protection is provided as an enterprise service in the Enterprise Services Standard.

Security Incident Procedures

Related ISO 27002:2013 clause(s): **6.1.3, 16.1, 16.1.1, 16.1.2**

Cyber security incident response includes the actions taken to report, analyze, assess risk, and if necessary, coordinate, respond and mitigate any cyber security incident.

The ISO shall follow pre-defined incident response procedures. Incidents must be escalated to DTI to ensure that these procedures are followed and a review process is implemented to allow the organization to learn from the incident and reduce their risk level.

If any security incident has been detected it must be reported to the relevant ISO and to DTI immediately.

Cyber incident response service must include a well-defined framework with the following elements:

- Detection and Analysis
  - Determine if there has been a security breach
  - All information security breaches must be reported without delay to the relevant ISO and to DTI. Prompt reporting will speed the identification of any damage caused, including information spillage, effect any restoration and repair, prevent further contamination, and facilitate the gathering of any associated evidence.
- Communication
  - Central communication point to receive information on security incidents and to disseminate vital information to appropriate State entities about the incidents
  - Ability to quickly notify organization management and the DTI Service Desk of the security incident
- Containment, Eradication, and Recovery
- Post-incident Activity
  - Document and catalog security incidents.
  - Continually update current systems and procedures
  - Analyze event information and reports to determine trends and patterns of intruder activity

For further questions on security incident procedures, contact the Enterprise Security Operations Team.

Security incidents determined by the State or Federal authorities to have homeland security implications require Organizations to follow specific procedures due to the nature of the threat and interrelation of effects.

Data Backup Plan

Related ISO 27002:2013 clause(s): **8.2.2, 8.3.1, 8.3.3, 11.2.6, 12.3, 15.1.2**

Note – A new Data Backup and Retention Policy is CIO approved. The effective date is under consideration at this time. When available the reference link will be inserted. Please refer any questions regarding this policy to the Enterprise Architecture Team.

Disaster Recovery Plan and Testing

Related ISO 27002:2013 clause(s): **17.1.1, 17.1.2, 17.1.3**

Data Stewards must evaluate, prepare, periodically update, and annually test a disaster recovery plan or as material changes are made to policy or systems. The listed activity shall allow all designated critical computer and communication systems made available in the event of a major loss, such as a flood, earthquake, hurricane, or tornado, on a predefined priority basis.

Continuity of Operations Planning

Related ISO 27002:2013 clause(s): **17.1.1**

Data Stewards must create and maintain a Continuity of Operations Plan (COOP) that includes development, documentation, and implementation of a comprehensive plan of action to guide the complete organization in the return of essential business operations and, eventually, full business recovery following an unforeseen disruption. The Emergency Response Plan, IT and Business Recovery plans are documented in the Continuity of Operations Plan.

The Continuity of Operations Plan (COOP) includes the implementation of the Emergency Response plan in order to contain the crisis, secure the health and safety of people, and prevent further spread or continuation of the crisis (e.g., a fire). The Emergency Response Plan must account for a response level potentially resulting in the declaration of a disaster should critical business processes not able to perform as normal. A disaster declaration enacts IT and business recovery plans coordinated by

the Disaster Management Team. Emergency Response and Disaster Declaration stand-downs are enacted only after normal business resumption.

The COOP must identify the critical people, roles and responsibilities, business processes, information, systems, assets, and other infrastructure considerations that are required to enable the business to operate. The COOP shall lay out a predetermined plan as assessed by a business impact analysis, which are executed to assure minimum disruption. All COOP plans are reviewed and updated to include, but not limited to, employee contact information at least once a year. However, it is highly recommended that plans are updated as change occurs within the organization.

Third-Party Business Contracts

Related ISO 27002:2013 clause(s): **13.2.2, 13.2.4, 15.1.1, 15.1.2, 15.1.3, 15.2**

Due diligence in selecting a third-party business associate who has access to State non-public information involves a thorough evaluation of all available information about the third party. In addition, it is strongly recommended that all IT contractors, IT vendors, and other IT third-party service providers sign a Non-Disclosure Agreement. If they handle State non-public data, it is strongly recommended that they pass a criminal background check. If they require access to the State network, they must sign the Acceptable Use Policy.

The contract with the third party must include clauses that assign responsibility to the third party for data protection and implementation of appropriate safeguards based on data classifications to protect the confidentiality, integrity, and availability of the confidential and sensitive information to which it has access to on behalf of the State. See Offshore Staffing Policy and Security Clearance section of this Policy (page 14).

Software Copyright (Licensure)

Related ISO 27002:2013 clause(s): **18.1.2**

The State of Delaware prohibits the illegal duplication of software and its related documentation.

Third-party copyrighted information or software that the organization or district does not have specific approval to store and/or use are not stored on State systems or networks. System administrators shall remove such information and software unless the involved users can provide authorization from the rightful owner(s) and that the license, binary, and authorization are held by the State.

The State strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Data Users shall not make unauthorized copies of software and documentation since the State strictly forbids all such copying.

Data Users shall only install software that has been properly purchased/licensed to the State. Software evaluation copies are installed for the specified timeframe after approval by applicable Data Steward/management. Continuous re-installs of an evaluation copy is not permitted.

Organizations must follow state contracting, procurement and legal exemption guidelines for both generic licensing and end-user-license-agreement (EULA) contracts. Careful attention is noted, but not limited to provisions regarding taxes, indemnification, choice of law, exculpation, liability, statutes of limitation and fees; some, or all of which may be exempted under Delaware law.

Further guidance is available in the Acceptable Use Policy and Software Policy.

Computer Resource Usage

To ensure that State computer resources are used for their intended purposes and to further safeguard the confidentiality, integrity, and availability of all information, all data users must abide by the terms of the Acceptable Use Policy.

Communications & Messaging

All existing State policies apply to the conduct of employees, casual seasonal employees, temporary personnel, contractors, and vendors on the Internet and via email systems through State facilities or using State resources, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of organization resources, sexual harassment, information security, and confidentiality.

An Internet user is held accountable for any breaches of security or confidentiality resulting from their use of the State Internet connection.

Peer to peer software must not be used on the State network.

Only voice systems including VOIP solutions owned and managed by the State are permitted for use on the State network. State Organization(s) shall establish, document, and control usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies when they apply. Instant Messaging (IM) solutions owned and managed by the State are permitted for use on the State network. The use of Internet based IM is permitted only through the State proxy servers.

Communication guidelines are as follows for State organizations:

1. Personnel must comply with the Acceptable Use Policy (AUP), applicable laws, policies, standards, and guidelines at all times when using State's systems.

2. Communication technologies are not used to communicate confidential and/or sensitive information unless they are configured to include security features with encryption.

3. Only State internal contacts are loaded in your contact list or "buddy list".

4. Non-state users shall be excluded from the Exchange Global Address List (GAL) except for quasi-state entities such as National Guard, DSHA, etc. Any exceptions shall be approved by DTI Telecommunications Team.

5. Users are aware that IM messages are no different than other electronic communications and are monitored, retrieved and archived. The same privacy principles described on page 14 (privacy section) of this policy apply.

6. Keep messages simple and to the point.

7. Contact names are clear and concise so that no mistakes are made on who you are communicating with.

Voice Device Security

To secure the confidentiality of State business and protect the government's reputation, care is taken when speaking on any type of voice device whether inside

or outside of department facilities, so that others cannot overhear conversations of a sensitive nature.

Wireless and Mobile LAN Computing

Wireless connectivity is governed by best practices as reflected in the following DTI policies, standards, and guides:

Acceptable Use Policy
Data Classification Policy

Technical Safeguards

Transmission Security

Related ISO 27002:2013 clause(s): **13.2, 13.2.1, 13.2.2**

All electronic data transmitted must be protected based on the classification of the data. All users are required to protect the integrity of the State's data. All State non-public data must be appropriately secured over electronic communications networks in accordance with the Data Classification Policy and all applicable published standards.

Integrity Controls

Related ISO 27002:2013 clause(s): **14.1.2, 14.1.3**

Organization management must make reasonable efforts to ensure there is an ongoing process to monitor integrity of systems and data.

To the extent feasible, management must be periodically notified about the accuracy, timeliness, relevance, and other information integrity attributes that describe the information they use for decision-making.

If controls which assure the integrity of information fail, if such controls are suspected of failing, or if such controls are not available, management is notified of these facts each time they are presented with the involved information.

Cryptography

Related ISO 27002:2013 clause(s): **18.1.5**

Organization management and Data Steward is responsible for determining the appropriate level of encryption algorithm for computing resources and data by adhering to applicable policies and standards.

In addition to following the cryptography and encryption policies contained herein. Organizations must consult with DTI prior to deploying third party and/or commercial encryption software, and solutions to ensure compatibility with state and localized networks and systems to ensure compatibility with these systems as well as operating systems.

Cryptographic Controls

Related ISO 27002:2013 clause(s): **10.1**

To protect the confidentiality, authenticity or integrity of information, cryptographic techniques are used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

General Cryptography

Related ISO 27002:2013 clause(s): **10.1.1, 10.1.2**

State of Delaware Confidential, State of Delaware Secret or State of Delaware Top Secret data stored and/or transmitted as a file over the network are encrypted at the file level where practical.

Encryption is applied to protect the confidentiality of information and shall follow the rules outlined in the Data Classification Policy.
Encryption keys, encryption procedures, and encryption software is not disclosed to anyone that does not need to know.

Any encryption mechanism is approved by the ISO according to DTI published standards.

Encryption keys, encryption procedures, and encryption software are securely backed up to ensure recoverability. When keys are changed, methods to decrypt encrypted data are ensured.

Contact the Organization ISO if the security of a secret key, private key, or pass phrase is in doubt.

Technical Cryptography Policy Statements

Related ISO 27002:2013 clause(s): **10.1.1, 13.2.1, IRS Publication 1075: Systems and Communications Protection, page 151**

The preferred mechanisms for encrypting files are asymmetric encryption methods. Public Key Infrastructure (PKI) systems that combine symmetric and asymmetric methods for bulk data encryption are also acceptable.

For applications that require access credentials, the credentials must be encrypted and not stored in human readable form.

For applications that require password entry via a keyboard, the password must be not echoed to a device so that it is human readable.

Network connections to exchange State non-public data with third parties must be either point-to-point or frame relay circuits. If the Internet is used for information transport, virtual private network circuits or SSL is required.

Web-based applications, whether internally developed or purchased, must use strong encryption for the logon page or any page where user credentials are entered as input and for any page that displays State non-public information.

All Federal Tax Information (FTI) will be encrypted during transmission. The information system must protect the confidentiality of the FTI during electronic transmission. The system must perform all cryptographic operations using Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules with approved modes of operation. Cryptographic data transmissions shall be ciphered and consequently unreadable until deciphered by the recipient.

Cryptography Key Management

Related ISO 27002:2013 clause(s): **10.1.2**

Secret and private encryption keys are communicated only via an out-of-band process like CD or USB drive exchange, not via in-band processes like email or the Internet.

Secret encryption keys, if approved, used for file encryption are changed at a minimum of twice per year.

The organization's ISO shall store and secure (escrow) backup copies of all encryption keys in an offsite location.

Backup copies of encryption keys are not stored in an insecure manner.

Approved Encryption Techniques

Approved algorithms and standards are established through DTI published standards.

Monitoring

Related ISO 27002:2013 clause(s): **12.4**

Organization management shall ensure that monitoring tools appropriate to the data or system are installed in order to log activity and possible security violations. Automated tools provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline and the tools to report exceptions are developed. This monitoring scheme extends a responsibility for Data Steward management to further monitor ISO and IT staff system administration activities.

In order to ensure the validity of audit trails and certify required evidence, all system clocks across the enterprise are synchronized on a regular basis with the Network Time Protocol (NTP) server, and audit logs are protected as classified information.

Intrusion Detection

Related ISO 27002:2013 clause(s): **12.4.1, 13.1**

Operating system, user accounting, and application software audit logging processes are enabled on all production systems.

Alarm and alert functions of any firewalls and other network perimeter access control systems are enabled.

Audit logging of any firewalls and other network perimeter access control systems are enabled.

Audit logs from the perimeter access control systems are monitored/reviewed by the system administrator.

System integrity checks of the firewalls and other network perimeter access control systems are performed on a routine basis.

Audit logs for servers and hosts on the internal, protected network are reviewed on a regular basis or at any frequency identified and approved by the Data Steward. The system administrator shall furnish any audit logs as requested by the ISO or DTI.

Intrusion tools are used to check systems on a routine basis.

All trouble reports are reviewed for symptoms that might indicate intrusive activity.

All suspected and/or confirmed instances of successful and/or attempted intrusions are immediately reported according to the computer security incident response procedures.

ISOs shall train users to report any anomalies related to system performance and signs of wrongdoing.

Audit logs, trouble reports, and intrusions detection documentation must be retained for a period of time in accordance with current document retention schedule(s).

Server Hardening

Related ISO 27002:2013 clause(s): **12.6, 9.4.4, 14.1.1, 14.1.2, 18.2.3**

All servers are set up securely (hardened) by completing the appropriate security procedures, identified as:

- Installing the operating system from a DTI-approved source.
- Applying vendor-supplied patches.
- Removing unnecessary software, system services, and drivers.
- Setting security parameters and file protections, and enabling audit logging.

- Disabling or changing the password of default accounts.
- Disabling remote content management directly over the Internet. Content is managed from within the State network or via VPN.
- Controlling physical and logical access to ports.
- Restricting usage of system.
- Perform routine scans for vulnerabilities and configuration weaknesses and report findings to the organization's ISO.
- Server Operating System (OS) shall comply with the Software Policy
- Host based firewall for servers.

The integrity and security of the State network is the responsibility of all participants. As DTI is the custodian of the State IT infrastructure, DTI shall disconnect any computing device that jeopardizes the network, State systems or State data for remediation.

Mobile Device Management

Related ISO 27002:2013 clause(s): **9.1.2, 9.3.1, 9.4.1, 14.1.1**

For guidance outlining the management requirements and security expectations when using either personal or State owned mobile devices that access State content reference the Enterprise Services Standard for an enterprise service for collaboration – email and productivity from mobile devices.

Patch Management

Related ISO 27002:2013 clause(s): **12.1.2, 12.6, 18.2**

Security patches are implemented via change control within a specified timeframe of notification of available patches as defined by organization management and related information technology staff. Patches are tested appropriately prior to implementation.

Security Reviews

Related ISO 27002:2013 clause(s): **12.6.1, 12.7, 18.2.1, 18.2.3**

Independent Baseline Security Reviews, Vulnerability Testing (every 30 days), and Penetration Testing are completed as scheduled to determine the minimum set of controls required to reduce and maintain risk at an acceptable level. Furthermore, audit tools and results are safeguarded to prevent any possible misuse or compromise. Audit findings are reported to organization management for mitigation and corrective actions.

Network Security

Related ISO 27002:2013 clause(s): **9.1.2, 12.6.2, 13.1.1, 13.1.2, 13.1.3, IRS Publication 1075: Systems and Communications Protection, page 151**

Users are permitted to use only those network addresses issued to them by DTI.

Users must not extend or retransmit network services in any way. Devices that connect to or through an external network require DTI approval.

Users and/or devices inside the State firewall are not connected to the State network at the same time they are connected to an external network.

Logon to State systems and networks from remote computing locations are required to comply with the authentication and authorization policy and utilize enterprise services in the Enterprise Services Standard.

Users must not install or alter existing network hardware or software that provides network access services without approval by the Organization ISO and DTI.

DTI shall have the authority to remove without prior notice any computing resource that threatens the security of the State network. DTI shall notify the organization ISO of any such action taken via encrypted email notification within two (2) business days after the event.

Use of tunneling technology to circumvent security is forbidden.

To safeguard information classified as State of Delaware Confidential, Secret, or Top Secret (For additional information, consult the Data Classification Policy), remote activation of collaborative computing mechanisms without an explicit indication of use to the local users is prohibited. Collaborative computing examples include networked white boards, cameras, microphones, and recording devices. Users must be notified if there are collaborative devices connected to the system.

Equipment and System Setup and Configuration

Related ISO 27002:2013 clause(s): **12.1.1, 12.6.2**

For all equipment and system setup and configuration, vendor supplied default usernames and passwords and other access credentials are disabled, deleted, or changed before the system or application is moved into production.

Remote Access

Related ISO 27002:2013 clause(s): **6.2**

All remote access to the State network is in accordance with the Enterprise Services Standard and the Acceptable Use Policy.

Cloud Computing and External Hosting

Cloud Computing offers an alternative to traditional IT delivery models. Potential benefits include significant cost savings, enhanced scalability, agility, and rapid delivery. Conversely, entrusting infrastructure and data to a third party reduces control and introduces risks that need to be managed. The State of Delaware **PRIVATE** cloud offers server replacements to organizations at potential cost savings. Movement to the **PUBLIC** cloud shall be evaluated carefully for the protection of sensitive data, access control, and identity management. Organizations shall take an assertive stance, hold the providers accountable, and ensure security is an early consideration. Any engagement that is cloud-based or externally hosted or sends non-public data outside of the state network shall be vetted through the DTI Business Case Process, Architecture Review Board, the internal Technology Investment Council (iTIC), and the State's Attorney General's Office. Contracts for cloud-based and external hosting engagements shall include the public terms and conditions or non-public terms and conditions that have been approved by DTI and

the State Department of Justice. The statement of work clauses should be considered, and their relevance will depend on the nature of the engagement. For additional details, see the Cloud and Offsite Hosting Policy.

Firewalls

Related ISO 27002:2013 clause(s): **9.1.2, 13.1.1, 13.1.2**

All in-bound, real-time external connections to internal State networks and/or multi-user computer systems must pass through an additional access control point (e.g., a firewall, gateway, VPN concentrator) before users can successfully connect.

All firewalls used to protect the State internal network must run on separate dedicated computers. These computers may not serve other purposes such as acting as Web servers.

Firewall configuration rules are maintained by DTI. Rule changes are administered and approved by the organization's ISO and DTI.

Connections between internal State networks and the Internet (or any other publicly or privately-accessible computer network) must include an approved firewall and/or related access controls.

Well-known port numbers are only used by the appropriate well known service.

Internal Network Addresses and Designs

Related ISO 27002:2013 clause(s): **13.1, 13.1.1**

The following items are confidential internal system information: IP addresses, system and server configurations, and related system and network design information for State computer systems. They are restricted whereby both systems and users outside the State internal network cannot access this information. DTI restricts network computer systems and external users from accessing internal network system addresses, configurations, and related system design information. The DTI Chief Security Officer (CSO) must approve release of this information.

Software Development and Intellectual Property

Related ISO 27002:2013 clause(s): **7.1.1, 9.4.5, 14.1, 15.1.2, 18.1.2, IRS Publication 1075, NIST SP 800-28 Version 2,**

All source code developed for the State of Delaware is the property of the State unless otherwise specified by contract.

Organization management shall ensure respect for the legal rights, all copyrights, and the copying of proprietary material restrictions that are imposed on the use of intellectual property. The organization shall respect procedures surrounding design rights, licenses, and trademarks. Where applicable, both DTI and state organizations must consult with their designated Deputy Attorneys General concerning intellectual property, contractual and other related legal matters to ensure compliance with these policies as well as federal and state laws.

During development, developers shall safeguard computing systems against Trojan code and covert channels by using programs that are evaluated and are purchased from reputable sources, testing the source code to ensure the source code is harmless.

Application code is subject to a code review from a security standpoint, regardless of whether it was outsourced or produced in-house. This is an iterative process, occurring during requirements gathering, system design, development, and before the final version is readied for deployment.

Special attention must be given to active content, which refers to electronic documents that can carry or trigger actions automatically without an individual directly or knowingly invoking the actions. Active content can provide a useful capability for delivering essential government services, but it can also become a source of vulnerability for exploitation by an attacker. Organizations are required to understand the concept of active content and how it affects the security of their systems, and maintain consistent system-wide security when integrating products using active content. This requirement also applies to system development/hosted by a third party.

Special attention is given to input validation on web-based applications. Careful input validation is a vital step to prevent malicious users from attacking applications. Applications shall make use of centralized logging and log analysis which includes

failed and successful authentication attempts, administrative changes, error messages, and exception handling.

Vulnerability scans and/or penetration tests are performed on systems before they are connected to the network and on a regular schedule (every 30 days) thereafter. Regular and authorized request scans are performed by DTI security staff.

Data Stewards and Data Custodians shall control access to the source code during development and once it has been installed. Organization management shall implement development change control processes to control the modifications and to support separation of duties. The organization management shall also protect the source code by performing workforce security background checks for staff involved with the development and operation of key systems (which are Disaster Recovery/Continuity of Operations Plan (DR/COOP) rated at moderate (3) or higher.

Hosted applications that are developed and supported by an external vendor shall comply with the above-mentioned terms and with all security requirements as directed by Federal and State laws, policies, standards, and industry best practices.

Outsourced Software Development

Related ISO 27002:2013 clause(s): **14.2.7**

All outsourced software development shall follow the same policy as shown above. In addition, the source code ownership, licensing arrangements, and quality assurance processes must be identified before the development is outsourced. The contracting authority shall identify the right to audit the quality and accuracy of the outsourced software development work, and shall specify quality requirements before work begins. All contract language shall comply with State contract requirements. For additional information, consult the Offshore IT Staffing Policy.

Procurement Security

Related ISO 27002:2013 clause(s): **14.2.8, 14.2.9**

When purchasing computing resources—hardware, software, or services that utilize the State Information Technology infrastructure, the procurement process must comply with State standards and policies, specifically those dealing with information security. All IT contracts and RFPs must include contract and security clauses approved by DTI and the Attorney General's Office. Sample clauses are available on the DTI extranet under eSecurity Tools/Tips.

Physical Safeguards

Facility Access Control

Related ISO 27002:2013 clause(s): **9.1.1, 9.2.5, 9.2.6, 11.1, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 12.4**

All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

Physical access to computing resources in restricted facilities is documented and managed via access cards and logs by the security staff and/or organization level ISO.

All data center facilities are physically protected in proportion to the criticality of the business functions and associated systems, assets and infrastructure. See the Data Classification Policy, and the DTI Physical Security Policy.

Access to data center facilities is granted only to State support personnel and contractors whose job responsibilities require access to that facility. Security Clearance requirements are determined by the data center owner.

The process for granting card and/or key access to data center facilities must include the approval of the ISO and Organization management.

Access cards and/or keys are not shared or loaned to others. Access cards and/or keys that are no longer required are returned to the employee's direct supervisor. Cards are not reallocated to another individual, bypassing the return process.

Lost or stolen access cards and/or keys are reported immediately to the Organization ISO.

Any Data Center must use appropriate tracking process and procedures to track visitor access including visitor application and/or visitor access log.

Keycard access records and visitor logs for the Data Center are kept for routine review as identified in the organization's retention schedule.

The person responsible for the data center access control must remove the card and/or key access rights of individuals that change roles or are otherwise separated from State service.

Visitors are escorted in card access-controlled areas of facilities along with signing sign-in/out log.

The person responsible for the facility must review access records and visitor logs for the facility on a periodic basis, and investigate any unusual access.

Organization management must review card and/or key access rights for the facility at least annually and remove access for individuals whose employment terminates or transfers.

Maintenance authorizations, reason for repair, and logs for repairs and modifications to physical components (hardware, walls, doors and locks) are maintained.

Facility access and staff response procedures are threat-based in accordance with the DTI Homeland Security Policy. Consult this document for appropriate measures taken during period of elevated threat as declared by Federal and State authorities.

Workstation & Computing Resource Access

Related ISO 27002:2013 clause(s): **6.2, 8.3.1, 9.1.1, 9.3, 9.4.2, 11.1, 11.1.5, 11.2.1, 11.2.8, 11.2.9, 14.1.2**

All computing resources containing State of Delaware non-public information must be adequately protected from unauthorized access through appropriate access controls, theft deterrents, and screensavers.

All portable computing resources are secured to prevent compromise of confidentiality and integrity. No computer device may store or transmit State of Delaware non-public information without suitable protective measures in place that are approved by the Data Steward. Users must not place State of Delaware Confidential, State of Delaware Secret, and State of Delaware Top Secret data on a laptop or mobile device without prior approval of the Data Steward. See the Data Classification Policy.

Multifunction peripherals are hardened when used or connected to the network. They are configured to harden the network protocols used, management services,

processing services (print, copy, fax, and scan), logging, and physical security. Care is taken to ensure that any State non-public data is removed from memory before service calls and/or equipment disposal.

Whenever a State entity provides data on mobile computer media (laptops, tapes, disks, compact disks, USB drives, etc.) to an external entity, they must make sure that appropriate steps are taken, per Data Steward request and the Data Classification Policy to keep State of Delaware non-public data protected. The external entity must have pre-approved permission to move mobile computer media out of a State Organization's physical site by the Data Steward.

Any electronic equipment (PC, Laptop, iPad, iPod, etc.) that is not owned by the State cannot connect from an internal source (inside the firewall) to the State's network.

Employee owned Smart Phones are allowed to sync with the state network only if the owner agrees to comply with the required security controls and approval is granted by the ISO. This access must be authorized and processed by a written approval of their Cabinet Secretary, District Superintendent, or similar approving authority. Concurrence of the State of Delaware Chief Information Officer (CIO) or designee is required for new service or transfers. See the DTI Personally-Owned Smart Phones/Mobile Devices – Exchange ActiveSync FAQs for the application process. If the Smart Phone(s) cannot be provisioned to support the security policy, it shall not connect to the State's Exchange email system.

By not allowing specific electronic equipment to connect, it eliminates unnecessary risk to the State's network via an unauthorized internal source. This action of not allowing specific personally owned electronic equipment (as listed above) to connect from an internal point maintains the operational validity and condition of the State's network. This does not apply to Guest Net.

Equipment Security

Related ISO 27002:2013 clause(s): **11.1.4, 11.1.6, 11.2**

Data Stewards must ensure that computer resources and facilities are afforded appropriate security and protection from environmental threats. Considerations for

resource security extend to supporting infrastructure, such as utilities and cabling, to ensure the availability of information.

The placement of equipment within facilities shall ensure a physical separation of information processing or operational areas and public use areas such as shipping or loading areas. Equipment is placed within discrete, non-descript areas.

Special care is taken to ensure that relatively small areas housing utilities, telephones, switches, and associated computing resources (mini Data Centers) are afforded appropriate protection. Physical safeguards and access controls should include high security deadbolt locks and a manual access control device (cipher lock) if electronic access control is deemed too expensive.

For more information, consult the DTI Physical Security Policy.

Disposal of Electronic Storage Media

Related ISO 27002:2013 clause(s): **8.3.2, 11.2.7, IRS Publication 1075: Systems and Communications Protection page 151**

Whenever any State-owned or leased computing resource is released from use, State information and/or software is made unrecoverable. Appropriate electronic computing resource disposal pertains to hardware or other electronic media computing resources used at State sites or vendor sites for such purposes as Data Contingency Planning tests.

Electronic information storage devices (hard drives, tapes, diskettes, compact disks, USB, multifunction peripherals, etc.) are disposed of in a manner corresponding to the classification of the stored information, up to and including physical destruction.

Whenever a State entity provides external entity information on computer media (tapes, disks, compact disks, etc.), the entity must make sure that appropriate confidentiality contract clauses are in place to protect the confidentiality of the data.

Information systems must be configured to prevent residual data from being shared with, recovered, or accessed by unauthorized users or processes.

External Providers must provide written Certificate of Destruction as directed in the DELAWARE DATA USAGE TERMS AND CONDITIONS AGREEMENT.

For further information, consult the Disposal of Electronic Equipment and Storage Media Policy and the Non-Disclosure Policy.

Hard Copy Information Handling

Related ISO 27002:2013 clause(s): **18.1.3, 18.1.4, 8.2.2, 8.2.3**

State information is only generated in hard copy to the extent necessary to complete normal business operations. Copies of information are kept to a minimum to better facilitate control and distribution. Information classified State of Delaware non-public is not left unattended when it is printed, faxed, and/or copied. Persons monitoring these processes and/or having access to these computing resources are authorized to examine the information being printed, faxed, and/or copied. Faxes must be secure for all non-public classified data.

Hard copies containing State non-public information classified per the Data Classification Policy are locked in file cabinets, desks, safes, or other furniture when not being used by authorized staff, or not clearly visible in an area where there are persons who are unauthorized to view the documents.

All information is clearly labeled as to its classification level in accordance with the Data Classification Policy.

State of Delaware non-public information existing in hard copy form is shredded using equipment or service providers that reasonably ensure that information cannot be reconstructed.

Critical vital records assessed and or identified through a Business Impact Analysis (BIA) must have a backup system by which hard copies or electronic copies are sent off site in accordance with the offsite storage contract.

Photography Controls

Related ISO 27002:2013 clause(s): **6.2, 11, 11.2.9**

Cameras and camera-equipped mobile devices whether state owned and/or personally owned are generally allowed in State facilities. Data Stewards have the authority to restrict certain areas from photography or the presence of camera and

recording-equipped resources. Organization management shall restrict the use of photography within Data Centers, except of course for the purpose of physical security surveillance. Any exception requires the express consent of the Organization ISO. Vendors and contractors are asked not to bring camera-equipped devices into facilities. Any media or prints containing images of facilities are considered State of Delaware Secret unless released by the Organization ISO or executive management.

II. Definitions

Active Content

Electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user.

Assets

These are items considered owned by the State of Delaware. They include data, software, hardware (including network equipment), wiring, and all items purchased with state-appropriated funds. Per Delaware Code, "(a) All equipment, supplies and materiel, including vehicles, purchased in whole or in part with state-appropriated funds shall be considered as assets of the State and not of the state agency which holds or uses the materiel." [1]

Authentication

Authentication is proving the person is who they say they are.

Authorization

It is those things and only those things this authenticated person can do.

Availability

Assurance that the systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them.

[1] Title 29, State Government, Budget, Fiscal, Procurement & Contracting Regulations, http://delcode.delaware.gov/title29/c070/index.shtml.

Business Impact Analysis (BIA)

Business impact analysis is the process of figuring out which processes are critical to the company's ongoing success, and understanding the impact of a disruption to those processes. Various criteria are used including customer service, internal operations, legal or regulatory, and financial. From an IT perspective, the goal is to understand the critical business functions and tie those to the various IT systems. As part of this assessment, the interdependencies need to be fully understood. Understanding these interdependencies is critical to both disaster recovery and business continuity, especially from an IT perspective.[2]

Captive Account

A captive account limits the activities of the user, provides controlled login to the system and typically denies the user access to the command level.

***Cloud Computing (*NIST & US National Archives Cloud Definitions)**

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

[2] "Business Impact Analysis for Business Continuity: Overview", Search Storage Channel.com, January 22, 2008, 5th paragraph, Syngress Publishing.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[3]

[3] "The NIST Definition of Cloud Computing", by Peter Nell and Timothy Grance, SP800-145, September 2011.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Computer Based Training (CBT)

Computer-Based Trainings (CBTs) are self-paced learning activities accessible via a computer or handheld device.[4]

Computing Resource

Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any computing resource capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data, including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network-attached and computer-controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Confidentiality

Assurance that information is shared only among authorized persons or Organizations. Breaches of confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, emailing or creating documents and other data, etc. The classification of the information shall determine its confidentiality and, hence, the appropriate safeguards.

Continuity of Operations Planning (COOP)

Preparation for the continuance of government services in the case of any interruptive event. These events range from short term delays in operating procedures, such as software or electrical failures, to major events such as terrorist strikes or fires. COOP focuses on creating plans to keep essential services flowing including identifying what resources are needed for recovery and the order in which the business units will be recovered. COOP is nearly interchangeable with the term Business Continuity Planning (BCP) in the private industry sector.

[4] Computer Based Training definition, http://en.wikipedia.org/wiki/Computer_based_training

Criminal Background Check

This consists of providing fingerprints for a full State Bureau of Identification (SBI) and Federal Bureau of Investigation (FBI) check or a third party CBC process approved by DTI.

Data Custodian

Reference the description on page 10

Data Owner

Reference the description on page 7

Data Steward

Reference the description on page 7

Data User

Data User is an individual who accesses and uses the State's data. Reference the description on page 11

Display

Display includes monitors, flat panel active or passive matrix displays, monochrome LCDs, projectors, televisions, and virtual reality tools.

Document

Document pertains to any kind of file that is read on a computer screen as if it were a printed page, including HTML files read in an Internet browser; any file meant to accessed by a word processing or desktop publishing program or its viewer; or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

DR Levels

a) DR1 - Required at a minimum of 150 mile radius, offsite redundancy and offsite tape storage required.
b) DR2 - Required at a minimum of 150 mile radius, offsite redundancy recommended, and offsite tape storage required
c) DR3 - May be housed offsite at a DTI Data Center (under 150 mile radius) or other facility, and offsite tape storage required

d) DR4 - Not required unless specified at the department level. Offsite tape storage required.
e) DR5 – No solution required. Tape storage optional.

DTI Technical Team(s)

The DTI Technical Team(s) are comprised of representatives from the following DTI sections: Application Delivery, Data Center and Operations, Engineering.

Electronic Media

Data that is stored on physical objects, such as hard drives, zip drives, floppy disks, compact disks, DVDs, USB drives, memory sticks, MP3 players (iPod), PDAs, digital cameras, smart phones, and tapes.

Encryption

The process by which data is temporarily rearranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.

Federal Tax Information

The IRS defines federal tax information, which is subject to safeguarding requirements, as any tax return-derived information received from the IRS. This includes but is not limited to address information, social security numbers, federal tax filing status, payment source.

Graphics

Graphics includes photographs, pictures, animations, movies, or drawings.

Information remnance control

Control of information remnance prevents unauthorized and unintended information transfer.

Information Resource Manager (IRM)

Information Resource Managers are organization IT managers or administrators.

Information Security Officer (ISO)

Organization Information Security Officers are individuals who are responsible for all security aspects of a system on a day-to-day basis.

Integrity

Integrity is assurance that information is authentic and complete. Ensuring that information relied upon is sufficiently accurate for its purpose. The term 'integrity' is used frequently when considering Information Security as it represents one (1) of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it is trusted and relied upon. For example, making copies (e.g., by emailing a file) of a sensitive document threatens both confidentiality and the integrity of the information.

Intellectual Property

Intellectual property is information that is protected under federal law, including copyrightable works, ideas, discoveries, and inventions. Such property would include software development.

Multifunction Peripheral (MFP)

A multifunction peripheral is a device that performs a variety of functions that would otherwise be carried out by separate peripheral devices. Typical multifunction peripherals include functionality to copy, print, fax, and scan in a single device.

Multiple-Factor Authentication

Multiple-factor authentication is any authentication protocol that requires two (2) or more independent ways to establish identity and privileges.

Non-FTE

Individual that is not a full time employee, such as a contractor, vendor, casual/seasonal or temporary staff.

Object reuse

The reassignment of storage medium containing residual information to potentially unauthorized users or processes.

Privileged user

A user that has advanced privileges with access to resources that are unavailable to most users and permit the execution of actions that would otherwise be restricted. Such users in general include system administrators.

Risk Assessment Model

The model of an Information Security Risk Assessment is an initiative that identifies the:

1. Nature and value of the information assets or business assets.
2. Threats against those assets, both internal and external.
3. Likelihood of those threats occurring.
4. Impact upon the organization.

Risk is defined as a danger, possibility of loss or injury, and the degree of probability of such loss. Before introducing information security safeguards, you are aware of the dangers to which you are exposed, the risks and likelihood of such events taking place, and the estimated impact upon your organization were each to actually occur.

Sanitization

To erase data from storage media so that data recovery is impossible. The most common types of sanitization are destruction, degaussing, and overwriting.

Security Breach

Is an incident where sensitive, protected or confidential information has potentially been stolen, viewed or accessed by an unauthorized person. The more common concept of a breach is where an attacker uses a piece of malicious software to gain unauthorized access to a computer system and access sensitive information. Other, more common breaches, involve simple, seemingly harmless actions where sensitive information is left visible on a computer screen in an unsecured setting.

Security Incident

Refers to any adverse event that affects the confidentiality, integrity or availability of information that is processed by a computer system, regardless whether information was exposed or exfiltrated. A computer virus is an example of a security incident. Whether or not that incident constitutes a breach must be determined.

Segregation of Duties

A method of working, whereby tasks are apportioned between different members of staff in order to reduce the scope for error and fraud. For example, users who create data are not permitted to authorize processing; or Systems Development staff is not allowed to be involved with live operations. This approach shall not eliminate collusion between members of staff in different areas, but is a deterrent. In addition, the segregation of duties provides a safeguard to your staff and contractors against the possibility of unintentional damage through accident or incompetence – 'what they are not able to do (on the system) they cannot be blamed for.'

III. Development and Revision History

Date	Revision
2/1/2007	Rev 0 – Initial version
12/5/2008	Updated
11/15/2011	Updated
1/6/2012	Updated
8/28/2012	Updated
4/4/2014	Added sections to comply with IRS Publication 1075; clarified definition of background check; clarified DTI team names, clarified data roles.
1/13/2015	Added additional IRS 1075 references and updates to the international standard ISO/IEC 27002:2013.
2/16/2016	Removed language regarding Backup Data Plan. Removed RPO and RTO from Definitions. Added Reference to Data Backup & Retention Policy. Added new language to Authentication and Authorization regarding Identity and Access Management Service as per SME. Updated Security Incident Procedures for clarification. Updated Network Security as per IRS finding to clarify FTI and Collaborative Computing. Added Privileged Access Rights section.
5/30/2017	Updated IRS 1075 references and hyperlinks for IRS Publication 1075 (Rev. 11-2016). Updated NIST references.
1/19/2021	Rev 7 - Added Data Destruction Certification Form Reference
1/20/2023	Rev 7 – Updated references to retired policies and standards. Add definitions from Data Management Policy and System Architecture Standard.
1/29/2024	Rev 7 – Added a definition for Federal Tax Information.
11/4/2024	Rev 7 - Removed a reference to the Technology Investment Council

IV. Approval Signature Block

Name & Title: State Chief Information Officer	**Date**

V. Listing of Appendices

None.

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Terms and Conditions Governing Cloud Services and Data Usage Agreement

Contract/Agreement # _____, Appendix ____

between State of Delaware and _____dated _____

This document shall become part of the final contract.

	Public Data	Non Public Data	
1	✔	✔	**Data Ownership:** The State of Delaware shall own all right, title and interest in its data that is related to the services provided by this contract. The PROVIDER shall not access State of Delaware user accounts, or State of Delaware data, except (i) in the course of data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State of Delaware's written request. All information obtained or generated by the PROVIDER under this contract shall become and remain property of the State of Delaware.
2	✔	✔	**Data Usage:** The PROVIDER shall comply with the following conditions. At no time will any information, belonging to or intended for the State of Delaware, be copied, disclosed, or retained by PROVIDER or any party related to PROVIDER for subsequent use in any transaction. The PROVIDER will take reasonable steps to limit the use of, or disclosure of, and requests for, confidential State data to the minimum necessary to accomplish the intended purpose under this agreement. PROVIDER may not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service. Protection of Personally Identifiable Information (PII, as defined in the State's *Terms and Conditions Governing Cloud Services and Data Usage Policy*), privacy, and sensitive data shall be an integral part of the business activities of the PROVIDER to ensure that there is no inappropriate or unauthorized use of State of Delaware information at any time. The PROVIDER shall safeguard the confidentiality, integrity, and availability of State information. No party related to the PROVIDER or contracted by the PROVIDER may retain any data for subsequent use in any transaction that has not been expressly authorized by the State of Delaware.
3	✔	✔	**Termination and Suspension of Service:** In the event of termination of the contract, PROVIDER shall implement an orderly return of State of Delaware data in CSV, XML, or another mutually agreeable format. The PROVIDER shall guarantee the subsequent secure disposal of State of Delaware data. a) Suspension of services: During any period of suspension, contract negotiation, or disputes, the PROVIDER shall not take any action to intentionally erase any State of Delaware data. b) Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the PROVIDER shall not take any action to intentionally erase any State of Delaware data for a period of ninety (90) days after the effective date of the termination. All obligations for protection of State data remain in place and enforceable during this 90-day period. After such 90-day period has expired, the PROVIDER shall have no obligation to maintain or provide any State of Delaware data and shall thereafter, unless legally or contractually prohibited, dispose of all State of Delaware data in its systems or otherwise in its possession. Within this 90-day timeframe, the PROVIDER will continue to secure and back up State of Delaware data covered under the contract. c) Post-Termination Assistance: The State of Delaware shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement. d) Secure Data Disposal: When non-public data is provided by the State of Delaware, the PROVIDER shall destroy all requested data in all of its forms (e.g., disk, CD/DVD, backup tape, paper). Data shall be permanently deleted, and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) approved methods after ninety (90) days of the contract termination. The PROVIDER shall provide written certificates of destruction to the State of Delaware.

Form Revision Date: 8/21/23

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Terms and Conditions Governing Cloud Services and Data Usage Agreement

Contract/Agreement # _____, Appendix _____

between State of Delaware and _____ dated _____

This document shall become part of the final contract.

	Public Data	Non Public Data	
4		✔	**Data Location:** The PROVIDER shall not store, process, or transfer any non-public State of Delaware data outside of the United States, including for back-up and disaster recovery purposes. The PROVIDER will permit its personnel and subcontractors to access State of Delaware data remotely only as required to provide technical or call center support.
5		✔	**Encryption:** The PROVIDER shall encrypt all non-public **data in transit** regardless of the transit mechanism. For engagements where the PROVIDER stores sensitive personally identifiable or otherwise confidential information, this data shall be **encrypted at rest.** The PROVIDER's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the PROVIDER cannot offer encryption at rest, they must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach in accordance with the Terms and Conditions Governing Cloud Services and Data Usage Policy.
6		✔	**Breach Notification and Recovery:** The PROVIDER must notify the State of Delaware at eSecurity@delaware.gov immediately or within 24 hours of any determination of the breach of security as defined in 6 Del. C. §12B-101(2) resulting in the destruction, loss, unauthorized disclosure, or alteration of State of Delaware data. The PROVIDER shall send a preliminary written report detailing the nature, extent, and root cause of any such data breach no later than two (2) business days following notice of such a breach. The PROVIDER will continue to send any and all reports subsequent to the preliminary written report. The PROVIDER shall meet and confer with representatives of DTI regarding required remedial action in relation to any such data breach without unreasonable delay. If data is not encrypted (*see* CS3, below), Delaware Code (6 Del. C. §12B-100 et seq.) requires public breach notification of any incident resulting in the loss or unauthorized disclosure of Delawareans' Personally Identifiable Information (PII, as defined in Delaware's *Terms and Conditions Governing Cloud Services and Data Usage Policy*) by PROVIDER or its subcontractors. The PROVIDER will assist and be responsible for all costs to provide notification to persons whose information was breached without unreasonable delay but not later than sixty (60) days after determination of the breach, except 1) when a shorter time is required under federal law; 2) when law enforcement requests a delay; or 3) reasonable diligence did not identify certain residents, in which case notice will be delivered as soon as practicable. All such communication shall be coordinated with the State of Delaware. Should the PROVIDER or its contractors be liable for the breach, the PROVIDER shall bear all costs associated with investigation, response, and recovery from the breach. This includes, but is not limited to, credit monitoring services with a term of at least three (3) years, mailing costs, website, and toll-free telephone call center services. The State will retain all determining authority for breach accountability and responsibility. The State of Delaware shall not agree to any limitation on liability that relieves the PROVIDER or its subcontractors from its own negligence, or to the extent that it creates an obligation on the part of the State to hold a PROVIDER harmless. The PROVIDER shall not issue a media notice without the approval of the State.
7		✔	**Background Checks:** The PROVIDER must warrant that they will only assign employees and subcontractors who have passed a federally compliant (IRS Pub 1075 2.C.3) criminal background check. The background checks must demonstrate that staff, including subcontractors, utilized to fulfill the obligations of the contract,

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Terms and Conditions Governing Cloud Services and Data Usage Agreement

Contract/Agreement # _____, Appendix _____

between State of Delaware and _____ dated _____

This document shall become part of the final contract.

	Public Data	Non Public Data	
			have no convictions, pending criminal charges, or civil suits related to any crimes of dishonesty. This includes but is not limited to criminal fraud, or any conviction for any felony or misdemeanor offense for which incarceration for a minimum of one (1) year is an authorized penalty. The PROVIDER shall promote and maintain an awareness of the importance of securing the State's information among the PROVIDER's employees and agents. Failure to obtain and maintain all required criminal history may be deemed a material breach of the contract and grounds for immediate termination and denial of further work with the State of Delaware.
8		✔	**Security Logs and Reports:** The PROVIDER shall allow the State of Delaware access to system security logs that affect this engagement, its data, and or processes. This includes the ability for the State of Delaware to request a report of the records that a specific user accessed over a specified period of time.
9		✔	**Sub-contractor Flowdown:** The PROVIDER shall be responsible for ensuring its subcontractors' compliance with the security requirements stated herein.
10		✔	**Contract Audit:** The PROVIDER shall allow the State of Delaware to audit conformance including contract terms, system security, and data centers, as appropriate. The State of Delaware may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least thirty (30) days advance written notice and shall not unreasonably interfere with the PROVIDER's. business. In lieu of performing its own audit, the State may request the results of a third party audit from the PROVIDER or an attestation of compliance.
11		✔	**Cyber Liability Insurance:** An awarded vendor unable to meet the Terms and Conditions Governing Cloud Services and Data Usage Policy requirement of encrypting PII at rest shall, prior to execution of a contract, present a valid certificate of cyber liability insurance at the levels indicated below. Further, the awarded vendor shall ensure the insurance remains valid for the entire term of the contract, inclusive of any term extension(s). Levels of cyber liability insurance required are based on the number of PII records anticipated to be housed within the solution at any given point in the term of the contract. Should the actual number of PII records exceed the anticipated number, it is the vendor's responsibility to ensure that sufficient coverage is obtained (see table below). In the event that vendor fails to obtain sufficient coverage, vendor shall be liable to cover damages up to the required coverage amount.

Level	Number of PII records	Level of cyber liability insurance required (occurrence = data breach)
1	1-10,000	$2,000,000 per occurrence
2	10,001 – 50,000	$3,000,000 per occurrence
3	50,001 – 100,000	$4,000,000 per occurrence
4	100,001 – 500,000	$15,000,000 per occurrence
5	500,001 – 1,000,000	$30,000,000 per occurrence
6	1,000,001 – 10,000,000	$100,000,000 per occurrence

STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd., Dover, Delaware 19904

PUBLIC AND NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Terms and Conditions Governing Cloud Services and Data Usage Agreement

Contract/Agreement # _____, Appendix ____

between State of Delaware and _____dated _____

This document shall become part of the final contract.

The terms of this Agreement shall be incorporated into the aforementioned contract. Any conflict between this Agreement and the aforementioned contract shall be resolved by giving priority to this Agreement. By signing this Agreement, the PROVIDER agrees to abide by the following applicable Terms and Conditions [check one]:

FOR OFFICIAL USE ONLY

☐ **1-3 (Public Data)**

☐ **1-11 (Non-Public Data)**

Provider Name/Address (print): _____

_____

_____

Provider Authorizing Official Name (print): _____

Provider Authorizing Official Signature: _____

Date: _____

Form Revision Date: 8/21/23