DEPARTMENT OF TECHNOLOGY AND INFORMATION
William Penn Building
801 Silver Lake Boulevard
Dover, Delaware 19904-2407

CONFIDENTIALITY (NON-DISCLOSURE) AND INTEGRITY OF DATA AGREEMENT

The Department of Technology and Information is responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or medium on which they are stored; e.g., electronic data, computer output microfilm (COM), tape, or disk. Computer programs developed to process State Agency data will not be modified without the knowledge and written authorization of the Department of Technology and Information. All data generated from the original source data, shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State of Delaware and the Department of Technology and Information.

I/we, as an employee(s) of _____ or officer of my firm, when performing work for the Department of Technology and Information, understand that I/we act as an extension of DTI and therefore I/we are responsible for safeguarding the States' data and computer files as indicated above. I/we will not use, disclose, or modify State data or State computer files without the written knowledge and written authorization of DTI. Furthermore, I/we understand that I/we are to take all necessary precautions to prevent unauthorized use, disclosure, or modification of State computer files, and I/we should alert my immediate supervisor of any situation which might result in, or create the appearance of, unauthorized use, disclosure, or modification of State data.

Penalty for unauthorized use, unauthorized modification of data files, or disclosure of any confidential information may mean the loss of my position and benefits, and prosecution under applicable State or Federal law.

This statement applies to the undersigned Contractor and to any others working under the Contractor's direction.

I, the Undersigned, hereby affirm that I have read DTI's Policy on Confidentiality (Non-Disclosure) and Integrity of Data and understood the terms of the above Confidentiality (Non-Disclosure) and Integrity of Data Agreement, and that I/we agree to abide by the terms above.

Contractor Signature_____
Title: _____
Date: _____
Contractor Name: _____

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

Doc Ref Number:	AC-DIG-001	**Revision Number:** 0
Document Type:	Enterprise Policy	**Page:** 1 of 6
Policy Title:	Digital Accessibility Policy	

Synopsis:	This policy contains scope and technical requirements for State of Delaware agencies to ensure accessibility and usability for all digital information by individuals with disabilities.
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 Technology Investment Council on an ongoing basis and the CIO"
Applicability:	This policy is applicable to all users of the State of Delaware communications and computing resources. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the users in Legislative and Judicial Branches, as well as School Districts, 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:	1/30/2023
Reviewed:	1/30/2023
Approved By:	Chief Information Officer
Sponsor:	Chief Technology Officer

Table of Contents

Policy

POLICY SCOPE

This Policy applies to all State of Delaware public-facing digital assets that are developed, procured, maintained, or used while offering products, services, and online information to users. This includes any accompanying support documentation and services associated with the public-facing digital channel. Employees of the State of Delaware and third-party vendors shall comply with this Policy.

EXECUTIVE SUMMARY

The State of Delaware is committed to providing the most enjoyable and informative experience to all. This includes a commitment to accessibility, diversity, and inclusion. We are working to ensure that all State of Delaware Information and Communication Technology (ICT) is accessible to and usable by individuals with disabilities, in accordance with federal, state, and local law.

POLICY STATEMENT

We have policies and procedures in place to help guarantee that we comply with the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.1 Level A and AA guidelines for websites and mobile applications. We also have made a commitment to follow the W3C Web Content Accessibility Guidelines 2.1 (WCAG 2.1 levels A and AA) standards. We are firmly dedicated to complying with the Americans with Disabilities Act (ADA) Titles I, II and III, Section 504 and Section 508 of the Rehabilitation Act of 1973, the 21st Century Communications and Video Accessibility Act of 2010 (CVAA), and Title 6 Delaware Code 4504.

POLICY PROVISIONS

General Procedures

1. External communication - The State of Delaware will maintain a publicly available Accessibility Statement in support of the State's Digital Accessibility Policy. This statement should be available directly from the State of Delaware homepage. Each

department will maintain relevant information about the accessibility of public-facing websites, mobile apps, or other digital communications should be provided, as well as an accessible means by which individuals with disabilities can get further assistance. The information should be kept up to date with any new developments.

2. Training - This Policy will be communicated to all State of Delaware departments responsible for public-facing digital assets, including, but not limited to service representatives, product managers, project managers, designers, developers, engineers, content authors, QA analysts, and compliance/risk managers. The Policy will also be communicated to external vendors and contractors who develop public-facing digital assets for State of Delaware. Training will be offered through the Delaware Learning Center to help identified staff implement the Policy. Training will be coordinated and facilitated by the State of Delaware Digital Accessibility Program Senior Manager or their designate.

Responsibilities

1. State of Delaware Digital Accessibility Senior Manager - Upon adoption of this policy, the State of Delaware Digital Accessibility Senior Manager will be responsible for the enterprise accessibility program. All State of Delaware departments responsible for public-facing digital assets should contact the Digital Accessibility Senior Manager to answer any questions about accessibility, address the accessibility of covered digital assets, and assist in handling alternative format requests. The Digital Accessibility Senior Manager will review this policy annually, to ensure both its applicability and compliance with emerging regulations and standards.
2. Compliance - All State of Delaware departments responsible for public-facing digital assets shall collaborate with the State of Delaware Digital Accessibility Senior Manager to understand accessibility requirements, receive accessibility training, address accessibility of covered public-facing digital assets, and document how the public-facing digital assets conform to Technical Standards referenced in this Policy. Departments are responsible for implementing procedures that inform authors, developers, publishers, and procurers about applicable laws, policies, and contractual obligations.
3. Evaluation and Monitoring - All State of Delaware departments responsible for public-facing digital assets shall provide standards conformance reports on an annual basis. Reports will include both components developed by the State of Delaware and components developed by third-party vendors that are deployed on or integrated into State of Delaware managed platforms or applications. The State of Delaware will conduct

automated accessibility tests of its core website, at regularly scheduled intervals mandated by the State of Delaware Digital Accessibility Senior Manager, to identify any instances where the core website or other key digital communications are not in conformance with the Technical Standards referenced in this Policy.

EXCEPTIONS

Where compliance with this Policy is not possible, exceptions to this Policy may be granted by the State of Delaware. Requests for exceptions must be documented and submitted to the State of Delaware Digital Accessibility Program Senior Manager. Exceptions may be granted in scenarios such as not readily achievable, undue burden or fundamental alteration, user generated content, linked sites and resources, external digital content, short term digital content, orphaned digital content, back office, public safety systems, state contracts, ICT functions located in maintenance or monitoring spaces, etc. For more information, visit the following website (https://accessibility.dti.delaware.gov/).

Definitions

Accessibility – it means the degree to which an environment, service, or product allows access by as many people as possible, in particular, people with disabilities.

Accessibility Standards incorporated by reference – it means conventions, norms or requirements intended to provide access to an environment, product, or service, particularly to people with disabilities. The principle of accessibility may be mandated in law and specified in detail per regulations, standards, or codes.

Alternative Formats – it means information presented in Braille, in large print, via audio recording, or in an electronic format that can be accessed by people with disabilities. The Alternative Format must make the same content available and provide an equivalent level of access to the content by people with disabilities that is available to others who access the original document.

Public-Facing Digital Content - it includes, but is not limited to, electronic or digital content, communications or applications that are:

- In HTML, non-HTML, or mobile platform digital formats
- Public-facing and broadly disseminated, including products and services information, account information, etc.

- Public support mechanisms (e.g., chat, email, etc.)
- Digital marketing and social media content

For the purposes of this Policy – "Public-Facing Digital Content" shall not include Archival documents stored or retained solely for archival purposes to preserve an exact image of a hard copy; or draft versions of documents that are not public-facing, or which are intended for limited distribution.

Readily Achievable - it is defined as easily accomplishable and able to be carried out without much difficulty or expense. Failure to remove accessibility barriers where "readily achievable" might constitute discrimination. Determining what is "readily achievable" often involves analyzing the nature and cost of removing barriers and the overall financial resources of the business organization, among other factors. The analysis seeks to balance the benefit of the barrier's removal and the harm (e.g., cost) to the business.

Development and Revision History

Date	Revision
1/30/2023	Rev 0 - Initial version

Approval Signature Block

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

Listing of Appendices

Related Policies and Standards

Standard ID:	ES-SERV-001
Title:	**Enterprise Services**
Revision Number:	2
Domain:	Services
Discipline:	Solution Portfolio
Effective:	2/14/2020
Reviewed:	2/26/2024
Approved By:	Chief Information Officer
Sponsor:	Chief Technology Officer

I. Authority, Applicability and Purpose

A. 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 Technology Investment Council on an ongoing basis and the CIO".

B. Applicability: Applies to all 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 funding, access and continued use of these resources.

C. Purpose: In order to provide efficient, automated processes in State government, it is critical to have shared services that enable citizens and State users to access and analyze information and services. Robust and reliable access to common solutions is key to delivering government services.

II. Scope

A. Audience: This standard is intended for business and IT personnel.

B. Areas Covered: This document includes all of the solutions where it is required to use a common solution across all State organizations.

C. Environments: NA

III. Process

A. **Adoption:** These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the state of Delaware.

B. **Revision:** Technology is constantly evolving; therefore the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. **Contractors:** Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection of the proposed technology solution. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. **Enforcement:** DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. **Contact us:** Any questions, comments, or to request a copy of the detailed list of specific services, please email dti_tasc@delaware.gov.

IV. Definitions/Declarations

A. **Definitions**

1. Configuration – This involves using a feature within the standard deployment of a solution such as establishing security roles for a user and building email templates.
2. Customization – This involves altering the behavior of the standard deployment of a solution thru custom coding. Typically, a customization will impact the updates/upgrades of the solution.

B. **Declarations –** N/A

V. Definitions of Ratings

COMPONENT RATING	USAGE NOTES
STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and solidly positioned in its product life cycle.	These components can be used without explicit DTI approval for both **new projects** and **enhancement** of existing systems.
DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.	Via the State's waiver process, these components must be explicitly approved by DTI for **all projects**. They must not be used for **minor enhancement** and **system maintenance** without explicit DTI approval via the State's waiver process.
DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	No waiver requests for new solutions with this component rating will be considered.

A. Missing Components – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information.

VI. Component Assessments

Component/Service	Rating	Usage	Comments
Collaboration - Email & Productivity			
Conferencing Services	Standard	Mandatory	Conferencing Services
Email and Collaboration Services	Standard	Mandatory	Office 365 GCC G3 or G1 Plan. Includes Secure Email

Component/Service	Rating	Usage	Comments
State Directory	Standard	Mandatory	List of State users
K12 Directory	Standard	Optional	List of K12 users
Enterprise Fax Service	Standard	Mandatory	Enterprise Fax Service for Users
Power Automate and Power Apps	Standard	Optional	Creation of automated workflows, synchronize files, notifications.
Enterprise Desktop LAN (EDL)			
Enterprise Desktop LAN Support	Standard	Optional	Enterprise Desktop LAN Support
Enterprise Voice			
Voice and Data Services	Standard	Optional	Voice and Data Services for the State's telephony infrastructure
Network & Connectivity			
Cell Booster Services	Standard	Mandatory	Cell Booster Services
Wide Area Network Services	Standard	Mandatory	Wide Area Network (WAN) Service
Domain Name Service (Internet)	Standard	Mandatory	Resolves names to IP Addresses
K12 DNS (Intranet)	Standard	Optional	Resolves names to IP Addresses
State DNS (Intranet)	Standard	Mandatory	Resolves names to IP Addresses
Wide Area Network (Commodity Internet)	Standard	Mandatory	Network connections such as circuits
Internet (Service Provider)	Standard	Mandatory	
Certificate Authority	Standard	Mandatory – internal certificates	Security certificates

Component/Service	Rating	Usage	Comments
		Optional – external certificates	
Content Filtering	Standard	Mandatory	Filtering internet access. Does not include K-12.
Secure Remote Access (SSL-VPN)	Standard	Mandatory	Secure Remote Access (SSL-VPN)
Wireless Services	Standard	Mandatory	Wireless Services
Global Server Load Balancing	Standard	Optional	Load balancing and/or health checking DNS answers across multiple servers/ip addresses
Security Suite			
Business Continuity Consulting	Standard	Optional	Business Continuity Consulting
Disaster Recovery	Standard	Optional	Disaster Recovery
Firewall Management	Standard	Mandatory	Firewall Management
Endpoint Detection and Response Services	Standard	Mandatory	Securing Endpoint Devices
Identity & Access Management (IAM)	Standard	Mandatory	State IAM solution. End-to-End User Lifecycle Management. Onboarding Web Applications to State IAM Solution
Security Information and Event Management (SIEM) Services	Standard	Mandatory	Logging and Security Information and Event Management
Web Access Firewall Management (WAF)	Standard	Mandatory	Application protection

Component/Service	Rating	Usage	Comments
Vendor Hosted Web Shielding Services	Standard	Optional	Securing vendor hosted applications
Vulnerability Management Services	Standard	Mandatory	Software patch management including discover/identifying, assess/classifying, prioritizing, remediating, and mitigating software vulnerabilities in Software.
Enterprise Service Desk			
Enterprise Service Desk	Standard	Optional	Reporting and resolution of IT incidents, service requests and general IT inquiries

Component/Service	Rating	Usage	Description
Time and attendance tracking	Standard	Mandatory	Contractors are not included. Does not include K12.
Enterprise Resource Planning (ERP)	Standard	Mandatory	Human Resources, Financial, Benefits, Pensions
Recruitment	Standard	Mandatory	Job Openings
Delaware Learning Center	Standard	Mandatory	This is a Learning Management System. Tracking contractor training is billable.
Open data	Standard	Mandatory	Sharing, viewing and analyzing data sets
Enterprise GIS (FirstMap)	Standard	Mandatory	Sharing, viewing, and analyzing data that have a location
Server Hosting	Standard	Optional	Provides computer resources to applications. Does not include K-12.
Notifications	Standard	Mandatory	Delaware Notification Service

VII. Development and Revision History

Date	Revision
2/14/2020	Rev 0 – Initial version
6/7/2022	Rev 1 – SEUS
8/19/2022	Rev 1 – Clarified that email and secure email are mandatory services
2/26/2024	Rev 2 – Updated to reflect the new SEUS structures

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

Doc Ref Number:	PL-OFF-001	**Revision Number:** 4
Document Type:	Enterprise Policy	**Page:** 1 of 6
Policy Title:	Offshore IT Staffing	

Synopsis:	Establish Guidelines for use of offshore IT staffing.		
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 Technology Investment Council on an ongoing basis and 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 Date:	03/01/2006	**Expiration Date:**	None
POC for Changes:	Chief Technology Officer		
Approval By:	Chief Information Officer		
Approved On:	2/10/2015		
Date Reviewed:	9/27/2019		

Page

I. Policy

PURPOSE - This policy addresses specific requirements for IT services provided by contracted vendors using personnel outside the United States. Additionally, this policy addresses contracted vendors that provide services such as custom application development and support on a SaaS platform. This practice has become increasingly common due to shortage of domestic IT resources and opportunity to reduce costs. The goal is to guide State organizations in the selection, contracting, management and oversight of contracted vendors that if they make an offshore contract, ensure that the results meet the short and long-term requirements of the State.

Business Considerations – There are several important business issues to be considered.

1. The quality and usability of a system developed and/or maintained offshore should be at least equal to that available through Domestic Contractors.
2. The State's information systems and data must remain secure during the development and continuing support of the resulting system.
3. In many cases, the use of offshore staff is a result of use of Subcontractors. It is important that the State organization be aware of and approves in advance the use of Subcontractor offshore staff.
4. Managing a project with offshore staff, especially when subcontracted, will require additional attention from the State organization.
5. State organizations should take into consideration that additional overhead is encountered when using offshore staff, especially subcontracted. Some studies estimate the overhead in the 20% range.

Legal Considerations – The full legal implications of using offshore staff and Subcontractors is beyond the scope of this policy.

1. The Primary (Domestic) Contractor shall be responsible for Subcontractor compliance with all terms, conditions and requirements of the primary contract, the Request for Proposal, and local, State and Federal Laws. The Primary Contractor must reside in the United States, and be licensed for business in Delaware. The Primary Contractor shall be liable for any noncompliance by any Subcontractor. Provisions must be placed in the contract to ensure the State is protected if any political/environmental crises arise that would prevent the successful completion of the contract by any Subcontractors.
2. It is the responsibility of the State Agency head and Data Steward to ensure that any offshore contract adheres to applicable local, State and Federal laws.
3. The full legal implications of using offshore staff and Subcontractors are beyond the scope of this policy. However, State Agencies should recognize that offshore contracts present complex legal issues. The State Agency should, in cooperation with its Counsel and Counsel for DTI, review and approve all contracts and subcontracts for any use of IT staffing personnel or services outside the United States.

Policy Details

1. Declare In Advance - Primary Contractors and Subcontractors must declare in advance or as early as is known during execution if offshore staff will be used for any tasks associated with the contract, and must fully disclose the scope (number and location) and role of the offshore staff. This disclosure must specifically identify the components or subcomponents being worked on, and what portion(s) of the lifecycle are being performed. This requirement for advance notice before offshoring applies to the entire life cycle of the effort.
2. Domestic Project or Support Manager - The Primary Contractor must provide a Domestic project or Support manager responsible for managing the relationship with offshore staff. This Domestic project or Support manager is responsible for ensuring that all communications (verbal and written) with the State are in English (American).
3. **Coding Standards** - All interim and final work products must be fully compatible with domestic practices. For example, source code, and documentation must be in English, and stored data must use U.S. Standard formats.
4. Suitability – Any decision to utilize offshore staffing or support for a system must be made formally by the head of the Agency.

5. System Access –
   A) The Data Steward must ensure that all aspects of the Administrative Safeguards and Technical Safeguards contained in the State of Delaware Information Security Policy are followed and that the Primary Contractor understands their obligation to require the same of any Subcontractor.
   B) It is considered a best practice for the Offshore staff to have access to only the Development Environment any Non-Public data on the Development Environment, which is accessible via Offshore staff, must be masked/obfuscated sufficiently to reduce its data classification to Public.
   C) Offshore staff must not have access to the production environment.
   D) Offshore staff must not have access to any State of Delaware confidential, secret or Top Secret data as outlined in the State's Data Classification Policy.
   E) It is a requirement for the Primary Contractor's Domestic staff or State staff to be responsible for promotion of system changes into the Test and Production environments.
   F) **State Policy prohibits the sharing of Logon ID's and Passwords among users of its infrastructure. It is explicitly forbidden for Primary Contractor or Subcontractor staff to "share" access privileges. This is particularly egregious when offshore staff is involved. Violation of this clause will be considered by the State to be a material security breach by the Primary Contractor and is grounds for discipline up to and including termination of the contract and exclusion from future IT contracting opportunities. State and Federal Attorneys General will be consulted for further State and Federal criminal and civil action if deemed necessary**
6. Review Components – The Primary Contractor's domestic staff must review all components developed by offshore staff for fitness, purpose and compliance with standards. One of the principle responsibilities of the Primary Contractor is to ensure that the components do not contain any published vulnerabilities or malicious software designed to damage or disrupt the application or its operating environment. **The State holds the Primary Contractor liable for any code containing vulnerabilities or malicious code produced by themselves or any Subcontractor.**

IMPLEMENTATION RESPONSIBILITY

DTI and/or the organization's technical staff will implement this policy during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This policy may also be enforced by others during the course of their normal business activities, including audits and design reviews.

If there is ambiguity or confusion regarding any part of this policy, contact the point of contact defined in the header of this policy.

II. Definitions

Criticality Classifications – Reference the State of Delaware Information Security Policy

Data Classifications – Reference the Data Classification Policy

Domestic - Domestic is defined as within the United States or its territories.

Offshore – Any location other than Domestic.

Primary Contractor - The Primary Contractor is the organization with whom the State organization has an executed contract. The Primary Contractor's right to use Subcontractors for all or part of the work under the contract depends on several factors, including Data Classification, Criticality Classification, and the stipulations of the contract.

Subcontractor – An entity under contractual arrangement to the Primary Contractor to provide all or part of the work under the primary contract. The various obligations of the Primary Contractor must extend to the Subcontractors as well.

III. Development and Revision History

Initial version established 03/01/2006

Second version established 8/15/2011

Third version established 8/28/2012

Minor revision – Changed POC on 10/15/2013

Fourth version established on 2/10/2015

Minor revision – Removed the references to the System Environment Standard on 1/25/2023

IV. Approval Signature Block

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

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

Doc Ref Number:	PI-EREC-001	**Revision Number:** 8
Document Type:	Enterprise Policy	**Page:** 1 of 7
Policy Title:	Disclosure of Individual User e-Resource Records	

Synopsis:	Users of the State's Communications and Computing resources can expect that their transactions are treated confidentially because DTI does not monitor e-mail transactions. However, e-mail messages, web access, mainframe and server access are all electronic records that could be subject to review with just cause. This policy provides a controlled process for obtaining access to individual e-resource records.
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 Technology Investment Council on an ongoing basis and the CIO"
Applicability:	This policy is applicable to all users of the State of Delaware communications and computing resources. The Department of Technology and Information (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. ** noted exception: As it pertains to email sent from a State, Legislative Hall email account, the following epilogue restrictions will be applied. *Notwithstanding any provisions of the Delaware Code to the contrary, the Delaware Department of Technology and Information is hereby prohibited from accessing or providing a legislator's e-mails or phone calls upon the request of another state department or agency, or branch of state government, except pursuant to the consent of the legislator, an Attorney General subpoena or a search warrant or other court order.*
Effective:	3/22/2005
Reviewed:	3/6/2023
Approved By:	Chief Information Officer
Sponsor:	Chief of Staff

TABLE OF CONTENTS

I. POLICY

POLICY STATEMENT

1. This State Policy provides a controlled process for obtaining access to individual e-resource records that do not leverage Consensual Access Permission processes.

2. 29 Delaware Code §502(8) defines the use of these e-resources as "public records." The state, through its "Acceptable Use Policy" (Appendix 1), makes it clear that any use of these e-resources are public records with no guarantee of privacy.

3. In order to comply with the Delaware Public Records Law (29 Delaware Code §501-526), DTI makes and retains copies of these transactions for the appropriate retention schedules. [See GAR-002 Administrative Support Records, Delaware Public Archives General Retention Schedule For State Agencies, available at Delaware Agency General Retention Schedule

4. DTI will cooperate with any agency/organization, as users of these resources, should they have a need to have access to these records in cases where the agency/organization needs to comply with the Freedom of Information Act, a legal hold, a court order, a valid subpoena, or a request to meet a legitimate Organizational Need. *Please see exceptions under the* **Applicability** *section on page one (1) of this policy.*

5. Only Authorizing Officials (see definitions) may request access and forwarding of electronic communication records. An alternative, high-level permission must be obtained for individuals with a direct reporting relationship to an Authorizing Official to act as a designee. Agency Authorizing Officials are responsible for notifying DTI when they leave the agency or stepdown from the e-Resource Records role. In addition, the Agency/Organization is responsible for notifying DTI when the Agency/Organization seeks to designate a new Authorizing Official (Appendix 3).

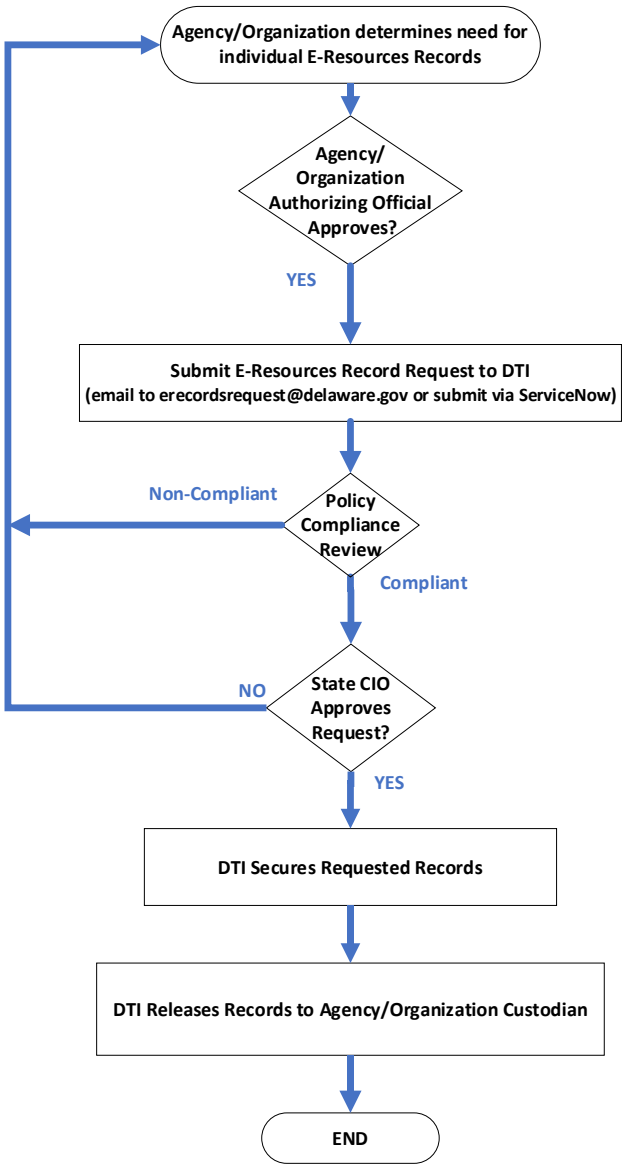
6. Such requests will be in writing and must be made only (a) when required by and consistent with law, (b) when there is substantiated reason to believe that violations of policy or law have taken place, or (c) when required to meet time-dependent, critical Organizational Needs. Written requests must be submitted using the "Request to Disclose Individual User e-Resource Records" form (Appendix 2).

   A) Delaware Attorney General Subpoenas or Court Orders - If DTI is compelled, under law, to disclose, copy, or transmit any agency information, DTI shall, prior to making such disclosure, reproduction, or transmittal, require that the requesting agency notify and obtain approval from the Data Steward. In such situations, unless notice to the Data Steward is precluded by the terms of the AG subpoena or court order, DTI will not release any records until such approval is obtained.

   B) Litigation Holds – If the requesting agency seeks a litigation hold, DTI requires that the agency update DTI as to the status of the need for the hold within one (1) year of the request. Should a requesting agency not pursue the hold as required by this policy, DTI cannot guarantee that the requested data will be maintained beyond one (1) year.

7. Upon receipt of a request, DTI will conduct a policy compliance review to ensure that the requesting agency's request meets the requirements of this policy. If DTI determines that the request is non-compliant, DTI will decline the request and return it to the requesting agency. Requests may then be resubmitted once policy compliance is achieved. Any requests not approved by the agency's Authorizing Official will be declined and returned.

Request to Disclose Individual User e-Resource Records Work Flow



II. DEFINITIONS

1. **Public Record** - 29 Delaware Code §502(8) defines a "public record" as "any document, book, photographic image, electronic data recording, paper, sound recording or other material regardless of physical form or characteristics, including electronic records created or maintained in electronic information systems, made, used, produced, composed, drafted or otherwise compiled or collected or received in connection with the transaction of public business or in any way related to public purposes by any officer or employee of this State or any political subdivision thereof."

   Email messages and website source files meet the definition of a record as they are "made or received pursuant to the law or ordinance in connection with the transaction of public business." Therefore, all provisions of the Delaware Public Records Law (29 Delaware Code §501-526) apply.

2. **FOIA** - Email messages (unless specifically prohibited by law) are subject to provisions of the Delaware Freedom of Information Act (FOIA) found in 29 Delaware Code §10001-10007 and the requirement of 29 Delaware Code §504 that public officials and employees "adequately document the transaction of public business" and "retain and adequately protect all public records in their custody."

3. **Delaware Public Records Law (29 Delaware Code §501-526)** DTI follows the Delaware Public Records Law's requirements for records retention and disposition schedules and uses the procedures of the Delaware Public Archives (DPA) for authorizing records disposition.

4. **e-Resource Records** – Records of usage of all state communications and computing systems.

5. **Acceptable Use Policy** – The Acceptable Use Policy provides guidelines for the appropriate use of the state's communications and computing systems. "State Communications and Computer Systems, including, but not limited to, computer networks, data files, e-mail, voice mail, and substance of dialogue found within collaborative communication tools, may be monitored and/or accessed by the State of Delaware to ensure the integrity of the technology, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes. Although DTI does

not randomly monitor message or network transactions, DTI may without notification or approval, monitor, access, and review any and all communications originating from the State of Delaware or delivered to the State of Delaware. Employees should have no expectation of privacy in regard to use of these services. This is in accordance with 19 Del. C. chapter 7."

6. **Authorizing Officials:**

   - Cabinet Secretaries – Executive Branch

   - Controller General, Speaker of the House, Senate Pro Tempore - Legislative Branch

   - Chief Justice – Judicial Branch

   - School Superintendents (users of the state education network)

   - Federal, State, and Local Government Agencies – These would require signatures from the highest-ranking member of the organization.

   An Agency/Organization head may designate a direct report of their organization to fulfill the obligations of the policy by completing the "Electronic Records (Resources) Request Form" (Appendix 3).

7. **Requestor** - Select individuals within the requesting organization who would ensure their organization follows this policy and associated processes when requesting information. In most cases it will be the organization's Information Resource Manager (IRM), or Director Level and above who will coordinate this request.

8. **Organizational Need** - This is a non-consensual access of individual records to meet operational or legitimate management purposes, including an audit.

9. **Data Steward -** The agency whose data is being requested.

10. **Consensual Access Permission** - This permission or delegation occurs when a user grants access to their mailbox for a business purpose, i.e. Outlook delegation, or to another digital record or file maintained on the State's network. This type of consensual access permission does not require an eRecords Request and should be handled by an agency's IT team or by contacting the DTI Service Desk.

III. DEVELOPMENT AND REVISION HISTORY

Date	Revision
3/22/2005	Rev 1 – Initial version
3/7/2008	Rev 2 – Updated version
1/6/2010	Rev 3 – Updated version
4/25/2012	Rev 4 – Updated version
4/8/2013	Rev 5 – Updated version
8/13/2013	Rev 6 – Updated version
2/18/2015	Rev 7 – Updated version
2/21/2023	Rev 8 – Updated version

IV. APPROVAL SIGNATURE BLOCK

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

V. RELATED DOCUMENTS

Appendix 1 - Acceptable Use Policy
Appendix 2 - eRecords_Request_Form.pdf (delaware.gov) (Request to Disclose Individual User e-Resource records)
Appendix 3 – Designee Form (Electronic Records (Resources) Request Form)

Standard ID:	AR-SYSARCH-001
Title:	**Systems Architecture**
Revision Number:	10
Domain:	Architecture
Discipline:	Systems Design Architecture
Effective:	7/1/2023 (new systems), 3/1/2024 (existing systems)
Reviewed:	12/15/2022
Approved By:	Chief Operating Officer, Chief Security Officer
Sponsor:	Chief Operating Officer, Chief Security Officer

I. Authority, Applicability and Purpose

A. **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 Technology Investment Council on an ongoing basis and the CIO"

B. **Applicability:** Applies to all State of Delaware communications and computing resources. The Department of Technology and Information (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 funding, access and continued use of these resources.

C. **Purpose:** This standard communicates how to construct IT solutions intended for production status. A good architecture builds into itself the ability to change not only in expected ways, but also in unexpected ways. This standard addresses systems from a high level and from the viewpoint of data and who is accessing a system. This standard will continue to evolve and enhance the understanding of Systems Architecture within the State.
.

II. Scope

A. **State of Delaware:** Project Leaders, Application Developers, Systems Administrators, Network Administrators, IT Security Personnel, Computer Auditors, and their managers and application development contractors for the State are the intended audience. IT personnel are the only intended users of this document.

B. **Areas Covered:** This standard will cover all State on-premise systems and systems that utilize IaaS.

C. **Environments:** All technology environments are covered except Mainframe systems.

III. Process

A. **Adoption:** These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. **Revision:** Technology is constantly evolving; therefore the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. **Contractors:** Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. **Implementation responsibility:** DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. **Enforcement:** DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. **Contact us:** Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Definitions/Declarations/Controls

A. Definitions

1. Control - an effective technique to guide the design of a system that satisfies the organization's requirements.
2. Pattern – a collection of controls applied in a reference architecture, enabling consistent design and deployment of systems.
3. System components – an operating system, hardware, software, etc.
4. Advanced Web Application Firewall – this is a solution that is focused on protecting web applications and APIs. The protection methods are consistent with industry practices, are application and protocol aware, and include behavior-driven protection mechanisms.
5. North-South and East-West network traffic – North-South refers to ingress/egress traffic to a subnet. East-West refers to lateral network traffic within a subnet.
6. Network level filtering – filtering of traffic implemented at the network subnet boundary.
7. Demilitarized zone (DMZ) – a physical or logical subnet whose resources are separated from other networks. Examples
   - Internet-facing app DMZ – designed for internet/external facing solutions where only applications reside.
   - management DMZ – designed for internal solutions where IT management solutions reside.
   - 'xxx' DMZ – a specific design to match the requirements.

B. Declarations

1. Patterns will be established to document a specific use case that satisfies the system controls.
2. Mandatory State enterprise services must be used in systems as defined in the Enterprise Services Standard.
3. Services must be configured to listen on well-known ports or reasonable alternative (associated with correct protocol). Utilize IANA.
4. Use the State's Enterprise Service 'Identity & Access Management' to authenticate employee, vendor, and constituent identities when accessing State applications and systems.
5. Authenticate access to non-public applications or data
6. All Internet access to the web application or API (xml, REST, etc) must be front-ended by the State's Enterprise Service 'Advanced Web Application Firewall' which is web protocol and web application aware.

- Provide any synchronous application integration via API call or via asynchronous methods such as flat file transfer.
- If not using API or flat file transfer for integration with a third party (vendor, SaaS, PaaS, IaaS, etc), private network communication will be required (ipsec tunnel, extranet, etc) and all system architecture standards apply to the related communication.

7. Design your applications to scale according to the user audience.
8. The following insecure protocols are forbidden for user to system access: SMB, RPC, Netbios, NFS.
9. The use of an encrypted tunnel to bypass network security controls or otherwise obfuscate communication is not permitted. Scenarios or designs that utilize client VPN or IPSec tunnels to secure communication in-flight are generally acceptable.
10. Infrastructure components other than servers should use centralized admin authentication or centralized automated management of accounts (e.g. appliances, ilo's etc)
11. Each system must have an identified business sponsor and technical owner.
12. All system components must be on supported versions and updates applied on a regular scheduled basis, including vendor/3rd party supported solutions.
13. When considering design in cloud environments, use native tooling that satisfies the required controls wherever possible. For example, in AWS leverage S3 buckets for object storage and Security Groups for policing east-west traffic.
14. Due to the integrity and availability requirements of production business applications, development business applications should not communicate with production business applications.
15. Only DTI approved devices may span network segments.
16. System architecture compliance must be reviewed when the system is life cycled.
17. When possible, establish and maintain unidirectional management DMZs.
18. No conclusions should be inferred if a specific topic is not listed. Instead, contact the TASC to obtain further information.

C. Controls

- SYS1 - Limit connections to (north-south) and between the application components network socket listener(s), including lateral movement (east-west) within the same network segment.
- SYS2 - Ensure there is network isolation between business systems/applications and supporting infrastructure/management platforms.
- SYS3 - Protect data in transit. Typically, this is provided by encryption.
- SYS4 - Protect data at rest. Typically, this is provided by encryption.
- SYS5 - Utilize application/protocol aware filtering methods to detect and protect our assets such as servers, applications, data. For example, IPS, WAF, Fail2Ban, and other tools.
- SYS6 - Maintain robust north/south internet protections appropriately for the exposed service (such as brute force protections, protocol level attacks, botnet and malicious ip blocklisting).
- SYS7 - Log user authentication events to the State's Log Management and SIEM service.
- SYS8 - Use allow-listed controls for outbound internet access.
- SYS9 - Establish centralized system admin authentication or centralized automated management of accounts to servers. For example, servers Active Directory joined, or Ansible managed user accounts.
- SYS10 - Enable server logging, vulnerability scanning, and protections from risks such as malware.
- SYS11 - Management and infrastructure communication must be limited and secured to that which is needed to support the business application. For example, Solarwinds agent communication, SNMP, Splunk, etc, must be scoped to that which is required for the function of the tool.
- SYS12 - Manage and secure the integration to user and system directories such as Active Directory.
- SYS13 – Network level filtering must exist between Systems and Users.

V. Development and Revision History

Date	Revision
3/19/2007	Rev 0 – Initial version
12/15/2022	Rev 10 – Complete rewrite with a focus on controls and patterns

Standard ID:	PL-DR-002
Title:	**Backup, Recovery and Retention Guidelines**
Revision Number:	1
Domain:	Information
Discipline:	Backup
Effective:	01/13/2023
Reviewed:	06/27/2023
Approved By:	Chief Operating Officer
Sponsor:	Chief Operating Officer

I. Authority, Applicability and Purpose

A. 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 Technology Investment Council on an ongoing basis and the CIO"

B. Applicability: Applies to all State of Delaware communications and computing resources. The Department of Technology and Information (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 funding, access and continued use of these resources.

C. Purpose: The objective of this guideline is to define the minimum procedures and guidelines for backup, recovery, and retention of the State of Delaware electronically stored information. Information stored and processed on Information Technology (IT) systems is vulnerable to accidental degradation, intentional corruption or deletion, hardware/software failures, and natural or man-made disasters. A backup and restore guideline is essential to ensuring recovery of information and the ability to continue IT support of critical State business functions. System backups also are an essential component of contingency planning strategies. Backups enable IT support personnel to quickly and reliably recover essential data and software in case of events such as natural or environmental disasters, system or application failures, sabotage, data/system integrity errors and/or system operations errors. In addition, to define when data should be archived for retention purposed to comply with state or federal regulations.

II. Scope

A. Areas Covered: Any location such as on-premise, cloud, etc.

B. Environments: Production environments

III. Process

A. Adoption: These guidelines have been adopted by DTI through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. Revision: Technology is constantly evolving; therefore the guidelines will need to be regularly reviewed. It is the intent of the TASC to review this guideline annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors: Contractors or other third parties are required to comply with these guidelines when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection of the proposed technology solution. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. Implementation responsibility: DTI and/or the organization's technical staff will implement these guidelines during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement: DTI will enforce these guidelines during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These guidelines may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us: Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Definitions/Declarations

A. Definitions

1. Backup

   i. Backup – The saving of electronic information onto magnetic tape or other offline mass storage media for a limited time for the purpose of preventing loss of data in the event of equipment failure, destruction, accidental loss, or corruption. While most backups are on magnetic tape-based media today, the term "Backup" or "Backup Media" may also reference other backup media technology including but not limited to, Optical (CD, DVD, etc), virtual tape systems, USB drives, and other removable media.

   ii. Backup Plan – The schedule of which files should be saved and when. A Backup Plan defines how many backup cycles are to be kept and how media is reused.

2. Recovery
    i. Recovery Point Objective (RPO) – The recovery point objective (RPO) is an important consideration in disaster recovery planning. It represents the age of files that is recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a failure.
    ii. Recovery Time Objective (RTO) – The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application is down after a failure or disaster occurs.
    iii. Restore – The process of bringing ESI back from off-line media and putting it on an online storage system when the data on the online storage system is lost or corrupted.
    iv. Disaster Recovery – The policies, process, and procedures related to preparing for recovery or continuation of technology infrastructure critical to the State of Delaware after a disaster. Disaster recovery focuses on the restoration of IT or technology systems that support business functions that fail in the event of a disaster.
3. Retention
    i. Archives –
        1. The records created or received and accumulated by a person or organization in the course of the conduct of affairs, and preserved because of their historical or continuing value
        2. The agency responsible for selecting, preserving, and making available records determined to have permanent or continuing value.
        3. The building in which an archival repository is located. See also Delaware Public Archives.
    ii. Archival Value – The enduring worth of documentary materials for continued preservation in an archival repository. May also be referred to as historical, continuing, or enduring value.
    iii. Data Archiving – Data archiving is the process of moving data that is no longer actively used to a separate data storage device for long-term retention. Data archives consist of older data that is no longer changing or shouldn't be changing, is still important and necessary for future reference, as well as data that must be retained for regulatory compliance. Data archives are indexed and have search capabilities so that files and parts of files can be easily located and retrieved.

iv. Public Records – Any document, book, photographic image, electronic data recording, paper, sound recording or other material regardless of physical form or characteristics, including electronic records created or maintained in electronic information systems, made, used, produced, composed, drafted or otherwise compiled or collected or received in connection with the transaction of public business or in any way related to public purposes by any officer or employee of this state or any political subdivision thereof.

v. Retention Instructions – Specific instructions directing the minimum retention for each record series. Remarks indicate length of time that the record should be retained by the agency and the events or time periods that need to occur before disposition of the record series can be effected. Exceptions to the retention instructions are noted.

vi. Retention Schedule – A list of record series which describes an agency's records; establishes a minimum period for their retention by the agency and provides mandatory instructions on what to do with them when they are no longer needed for current business. Also called records disposition schedule, records control schedule, records retention schedule, records retention and disposition schedule, or schedule.

vii. Retention Time – The amount of time in which a given set of data will remain available in compliance with state or federal regulations.

4. Electronically Stored Information (ESI) – General term for any electronic information stored in any medium (i.e., hard drives, back-up tapes, CDs, DVDs, jump drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
5. Encryption – The process by which data is temporarily rearranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.
6. IT Systems – The hardware and software used to store, retrieve, and manipulate information.

.

B. Declarations

1. This guideline applies to all State of Delaware electronically stored information, whether stored on premise or in the cloud.
    - An agency should create a backup plan that provides a minimum of four or more weeks of restoration for all production IT systems.
    - Non-production environments are not required to be backed up unless there is a specific business need.
    - Database and file storage servers should be backed up on a daily basis.
    - Web and application servers can be backed up less often depending upon the frequency of changes to the server.

2. Backups should be frequent to match stated RPO for the application. A daily database backup does not meet RTO of anything less than 1 day.
3. The recommended philosophy for backups is the 3-2-1 strategy. There should be 3 copies of the data (production, backup, offsite backup). The copies should be stored on at least 2 types of media (tape or different storage). Finally, one offsite copy for disaster recovery is recommended.

V. Guidelines

A. Backup

1. A backup of the organization's data files and the ability to recover such data is a top priority. Organizations' local management should assess the business process by the supported data and/or systems and assign a Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The backup of the associated media should correlate to the RPO/RTO. In addition to RPO and RTO, recovery objects need to account for time to restore or make operational the backup system. If there are multiple systems with same or similar RPO, there should be priority of recovery. In addition, the backup methods must support the RPO and RTO.
2. Data backups must be encrypted for State of Delaware confidential, secret and top secret data. Furthermore, State of Delaware confidential, secret and top secret data must only reside at rest on State owned or DTI approved systems or devices.
3. The vendor(s) providing offsite backup storage for State data should have appropriate clearances for the highest level of data classification stored. Physical access controls implemented at offsite backup storage locations should meet or exceed the physical access controls of the source systems. Additionally, backup media is protected in accordance with the highest State sensitivity levels for information stored.
4. Storage media protection and authentication controls at the storage system and media levels should be implemented to provide strong barriers against unauthorized stored data disclosure, theft, and corruption.
5. Backup media should be stored in a locked, fireproof container (UL-rated for media protection) during transport and while being retained at a pre-determined offsite location unless an approved offsite vaulting service is used (e.g. Iron Mountain, VRI, etc.). Backup media must be stored according to the application's Disaster Recovery Criticality and Level, as specified in the Delaware Information Security Policy, unless other DTI approved mitigating factors are put in place to protect the State's data.

B. Recovery

1. IT management should ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files, especially where such files may replace more recent files.

2. A process should be implemented to verify the success of the electronic information backup. Backups are periodically tested to ensure that they are recoverable within the expected timeframe. Testing helps to identify if:
   - **a)** Backups are incomplete.
   - **b)** Backup software was wrongly configured.
   - **c)** Encryption has caused a lockout (unknown password).
   - **d)** Backup is only readable by an earlier version of your software.
   - **e)** Backup cannot perform the restore from backup media which is several months old.
   - **f)** Dormant backup software bugs now plague your newly upgraded operating system.
   - **g)** The tape breaks during backup process.
   - **h)** Unexplained reboots could have caused a system crash and tape rewind during the backup process.
3. Signing Authorities held by the offsite backup storage vendor(s) for access to State backup media is reviewed annually or when an authorized individual leaves or changes job responsibilities.
4. Procedures between organization and the offsite backup storage vendor(s) are reviewed at least annually.
5. Backup tapes and/or containers should be identified by labels and/or a bar-coding system.

C. Retention

1. The retention of electronic data files should reflect the business needs of an agency, as well as any legal and regulatory requirements for records retention, such as Delaware Public Records Law (29 Delaware Code §501-526) and the Delaware Freedom of Information Act (29 Delaware Code Ch. 100 et seq.). The storage media used for the archiving of information should be appropriate to its expected longevity. The format in which the data is stored is carefully considered, especially where proprietary formats are involved. The archiving of electronic data is to be retained in a manner consistent with the Delaware Public Records Law requirements as provided in the Agency's Specific Retention Schedules and the State General Retention Schedules and by using the procedures of the Delaware Public Archives (DPA) for authorizing records disposition:
   - **a)** Model Guidelines for Electronic Records
   - **b)** State of Delaware retention schedules are located here
2. Regulations often include the retention period that is required for certain types of data.

D. To maximize efficiency, reduce costs, and minimize risks agencies should manage data and information effectively to lower the storage footprint. Through active storage management, storing key information in shared repositories appropriate to its classification, avoiding storing duplicates, utilizing deduplication, and routinely reviewing retention schedules agencies should be able to contain and lower storage growth.

VI. Development and Revision History

Date	Revision
1/13/2023	Rev 0 – Initial version based on a prior policy
6/27/2023	Rev 1 – Clarifying the backup vs recovery vs retention guidance.

Guideline ID:	IN-DBMS-002
Title:	**Database Management Systems Guideline**
Revision Number:	1
Domain:	Platform
Discipline:	Data Management
Effective:	01/13/2023
Reviewed:	05/15/2023
Approved By:	Chief Technology Officer
Sponsor:	Chief Technology Officer

I. Authority, Applicability and Purpose

A. 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 Technology Investment Council on an ongoing basis and the CIO"

B. Applicability: Applies to all State of Delaware communications and computing resources. The Department of Technology and Information (DTI) is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, 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 funding, access and continued use of these resources.

C. Purpose: Currently, the State has multiple database management systems in production with multiple number of versions of these database management systems. This guideline will identify those database management systems and versions that are considered appropriate for the State to concentrate on in the future.

II. Scope

A. Areas Covered: Only general use DBMS are covered by this guideline, not proprietary use databases such as laboratory or instrumentation databases, not Document Management Systems or specific-use applications like Active Directory, Outlook, e-mail, or Calendaring. When available, a general use DBMS is recommended over a proprietary solution.

B. Environments: This guideline will cover all database management systems (DBMS) installed or in use by the State of Delaware, including data owned by the State but housed by third-party contractors. This guideline does not apply to computer systems where the Federal Government dictates what DBMS to be used.

III. Process

A. Adoption: These guidelines have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. Revision: Technology is constantly evolving; therefore the guidelines will need to be regularly reviewed. It is the intent of the TASC to review this guideline annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors: Contractors or other third parties are required to comply with these guidelines when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. Implementation responsibility: DTI and/or the organization's technical staff will implement these guidelines during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement: DTI will enforce these guidelines during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These guidelines may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us: Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Definitions/Declarations

A. Definitions

1. Database: A collection of information organized in such a way that a computer program can quickly select desired pieces of data. Traditional databases are organized by field, record and file. A field is a single piece of information; a record is one complete set of fields; and a file is a collection of records. To access information from a database, a database management system (DBMS) is needed. This is a collection of programs that enables the user to enter, organize, and select data in a database.

2. Database Management System (DBMS): A collection of programs that provides the capability to store, modify, and extract information from a database. There are many different types of DBMS's, ranging from small systems that run on personal computers to large systems that run on midrange or mainframes. The terms relational, flat, network and hierarchical all refer to the way a DBMS organizes information internally. The internal organization can affect how quickly information can be extracted. Requests for information from a database are made in the form of a query, which is a stylized question. The set of rules for constructing queries is known as a query language. Different DBMS's support different query languages, although there is a semi-standardized query language called SQL (structured query language). For the purposes of this document, database and database management system are used interchangeably.
3. Scalable: Scalable database is defined as the capability of the database to meet current/future requirements without major effects on the existing structures. A scalable database will easily grow in both size and infrastructure with little or no measurable impact on the performance of the operational database, system, or network
4. Enterprise Database: A database or group of databases supporting a Statewide or multi-agency function or system with a single administrative authority. A database or group of databases supporting operations deemed critical to the business of the State or agency.
5. Desktop DBMS: a type of DBMS which is designed for running small scale databases, generally located on personal computers.
6. Mission Critical System: A system that is critical to the functioning of an organization and the accomplishment of its mission. Therefore, if a mission critical system is lost or unavailable, the agency will be unable to perform some or all of its most basic functions. Also, a system is deemed mission critical if its loss would cause an unacceptable slowdown in the functioning of an agency.
7. Personal Workstation: Any computing device engineered to remain stationary that contains a hard drive, memory, and CPU (the monitor and keyboard are usually separate pieces from the PC case) and expansion slots. The intent of the device is to be used by one person at a time, or perhaps one person and a print service.
8. Embedded: An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, that is specifically designed for a particular kind of application device. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines, and toys are among the possible hosts of an embedded system. Embedded systems that are programmable are provided with a programming interface, and embedded systems programming is a specialized occupation.
9. System Administrator: The human being responsible for running and maintaining a computer system at the Operating System (OS) level especially a mainframe, minicomputer, or local area network. System administrators, sometimes called network administrators, issue login names, maintain security, fix failures, and advise management about hardware and software purchases.

10. Remote Access: It is a means by which users can gain authenticated access to internal network resources, preferably without posing a security risk to valuable assets within the network.
11. Programmable Access: It is a means of reading and updating data in a database management system through controlled machine instructions.
12. Database Administrator: A database administrator (DBA) is a person responsible for the design, implementation, maintenance and repair of an organization's database. A DBA maintains database logins, maintains database security, monitors performance and performs database software patches/upgrades.

.

B. Declarations

A DBMS should:

1. Be tunable for performance and space maximization.
2. Be scalable.
3. Work within the State's IT Infrastructure.
4. Provide the ability to minimize redundant data.
5. Be able to secure data structures.
6. Contain data integrity facilities;
    - Provide Point-in-time recovery
    - General backup/restore methodology
    - Ensure that what was intended to be written was, in fact written.
7. Be 'system administrator' friendly;
    - Contain tunable operational parameters
    - Provide tools for modifying data file/table design
    - Utility suite for support functionality.
8. Provide audit trail capabilities.
9. Provide for transaction rollback.
10. Have a search/update engine that will accompany the relational database or provide a "vehicle" to interface with existing 3gl/4gl integrated software.
11. Adhere to the Software Policy, Delaware Information Security Policy, and Systems Architecture Standard.

V. Guidelines

A. Definition of Ratings

1. Component Ratings

COMPONENT RATING	USAGE NOTES
STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and can be expected to enjoy a useful life of 3+ years from the Effective Date.	These components can be used without explicit DTI approval for both **new projects** and **enhancement** of existing systems.
DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.	Via the State's waiver process, these components should be explicitly approved by DTI for **all projects**. They should not be used for **minor enhancement** and **system maintenance** without explicit DTI approval via the State's waiver process.
DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	No waiver requests for new solutions with this component rating will be considered.

2. Missing Components – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information
3. Component Assessments
    i. All DBMS's should be licensed in a manner appropriate to the way they are used and up-to-date with all appropriate publisher service patches.
    ii. All multiple-user DBMS's should be placed on servers. No multiple-user DBMS will be hosted on a PC.
    iii. All multiple-user DBMS's should be under formal support and approved by the IRM.
    iv. To determine the supported versions for the various release levels, consult the vendor's web site.
4. Components

Component	Rating	Comments
Relational DB		
Oracle Standard or Enterprise (See Appendix I)	Standard	General Release Levels
	Declining	Extended Support Release Levels
	Disallowed	Unsupported Release Levels
DB2 Mainframe	Standard	General Release Levels
	Declining	Extended Support Release Levels
	Disallowed	Unsupported Release Levels
SQL Server (See Appendix I)	Standard	General Release Levels
	Declining	Extended Support Release Levels
	Disallowed	Unsupported Release Levels
SQL Server Express	Standard	This version of SQL Server can be appropriate for a smaller database where the data size is less than 4GB and the end users are limited to a single organization.
	Declining	Extended Support Release Levels
	Disallowed	Unsupported Release Levels
Personal Workstation DBMSs (e.g., Microsoft Access, SQL Server Express LocalDB)	Standard	For use on a desktop by one user when the DR/BCP criticality classification is minimal (5) and the data classification is public
	Disallowed	For a system with a DR/BCP criticality classification of limited (4) or higher. Or for a system with a DR/BCP criticality classification of minimal (5) and the data classification is confidential, secret, or top secret.

SYBASE	Declining	(General or Extended Support Release Levels)
DB2 Server	Declining	
Open Source		Please review the State Software Policy Software Policy for Open Source Implications
MySQL	Standard	Supported versions with current patches
PostgreSQL	Standard	General Release Levels
MongoDB (See Appendix I)	Standard	General Release Levels
Non Relational		
IMS	Disallowed	No New Development (General or Extended Support Release Levels)
Adabas	Standard	General Support Release Levels
	Declining	Extended Support Release Levels
Lotus Domino	Declining	Database server service only (Notes Storage Facility) Version 8.5 and above

5. Lifecycle Roadmap

Lifecycle Roadmap

Databases

DTI	Jun-23	Dec-23	Jun-24	Dec-24	Jun-25	Dec-25	Jun-26	Dec-26	Jun-27	Dec-27
Oracle 19c	GA	GA	GA	Decline	Decline	EOL				
MSSQL 2014	Decline	Decline	Decline	Decline	EOL					
MSSQL 2016	Decline	Decline	Decline	Decline	Decline	Decline	Decline	Decline	EOL	
MSSQL 2017	Decline	Decline	Decline	Decline	Decline	Decline	Decline	Decline	Decline	Decline
MSSQL 2019	GA	GA	GA	GA	GA	GA	Decline	Decline	Decline	Decline
MSSQL 2022	GA	GA	GA	GA	GA	GA	GA	GA	GA	GA
Mongo DB 4.2	EOL									
Mongo DB 4.4	GA	GA	EOL							
Mongo DB 5.0	GA	GA	GA	EOL						
Mongo DB 6.0	GA	GA	GA	GA	EOL					

Vendor	Jun-23	Dec-23	Jun-24	Dec-24	Jun-25	Dec-25	Jun-26	Dec-26	Jun-27	Dec-27
Oracle 19c	PS/MS	PS/MS	ES	ES	ES	Paid ES	Paid ES	Paid ES	Paid ES	
MSSQL 2014	ES	ES	ES	ES	EOL					
MSSQL 2016	ES	ES	ES	ES	ES	ES	ES	ES	EOL	
MSSQL 2017	ES	ES	ES	ES	ES	ES	ES	ES	ES	ES
MSSQL 2019	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	ES	ES	ES	ES
MSSQL 2022	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS	PS/MS
Mongo DB 4.2	EOL									
Mongo DB 4.4	PS/MS	PS/MS	EOL							
Mongo DB 5.0	PS/MS	PS/MS	PS/MS	EOL						
Mongo DB 6.0	PS/MS	PS/MS	PS/MS	PS/MS	EOL					

GA	General Availability – Enterprise-wide standard with full deployment and support.
Decline	Direction is to reduce use and dependence on over time. No new development. Support Only.
EOL	Retiring from DTI enterprise. No implementation, development or support.
PS/MS	Premier/Mainstream Support – Five years from General Availability date
ES	Waived Extended Support
Paid ES	Paid Extended Support
MDS	Market Driven Support
LEC	Limited Error Correction

References for Vendor Support Type details:

Oracle:	Oracle Software Technical Support Policies Guide
MSSQLSVR:	Search Product and Services Lifecycle Information - Microsoft Lifecycle | Microsoft Docs
MONGO DB:	MongoDB Software Lifecycle Schedules | MongoDB

VI. Development and Revision History

Date	Revision
1/13/2023	Rev 0 – Initial version based on a prior standard
5/15/2023	Rev 1 – Updated Lifecycle Roadmap

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

Doc Ref Number:	IN-DataClass-001	**Revision Number:** 3
Document Type:	Enterprise Policy	**Page:** 1 of 8
Policy Title:	**Data Classification Policy**	

Synopsis:	The goal of this policy is to enhance the State's ability to protect data and information through data classification.
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 Technology Investment Council on an ongoing basis and 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:	3/1/2006
Reviewed:	02/26/2024
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

I. Policy

EXECUTIVE SUMMARY

This policy requires Data Stewards to classify all of the data used by their organization. It describes the roles and responsibilities of a Data Steward, the four types of data classifications and the minimum set of classifications. Generally, it lays the groundwork for the proper classification and handling of data used by the State. Further insight into this policy may be obtained through the organization's IRM (Information Resource Manager) or the DTI CES (Customer Engagement Specialist) assigned to the organization.

This policy does not limit or redefine FOIA (Freedom of Information Act) laws or regulations. In case of any conflict, the law shall prevail.

PURPOSE

This policy provides instruction for State organizations to better handle, secure, access, and use data. Sound business judgment and practices must be applied, and the State must comply with applicable Federal, State and Local laws and regulations, as well as any agency-specific guidelines then in effect. Examples of such are HIPAA and Gramm-Leach-Bliley (GLB), Federal Information Security Management Act

(FSMA), Privacy Act, PCI DSS, Federal Tax Data Safeguards (IRS Publication 1075), etc.[1] This policy will be reviewed and revised periodically. However, the State is obligated to comply with new laws or regulations coming into effect between revisions.

This policy is expected to be referenced by other State policies and standards that will further define the implications of the data classification. As such, the actual data classification designations will have far-reaching effects on various aspects of Information Technology throughout the State.

The National Institute of Standards and Technology (NIST) has drafted a comprehensive approach to data classification and the risks that are associated with different levels of data classification. Specifically, it addresses the integrity and availability of data as well as confidentiality, which is the focal point of this policy. NIST standards were used in the development of this policy.

DATA CLASSIFICATIONS

The Data Steward is responsible for classifying all data under the organization's control into one of the following classes.

State of Delaware Public – Information available to the general public; eligible for public access.

State of Delaware Confidential – Information covered by one or more laws. The disclosure of this information could endanger citizens, corporations, business partners and others. The types of information might be covered under non-disclosure agreements; or safeguarded by a general reference in law or best practices.

State of Delaware Secret – Information that, if divulged, could compromise or endanger the people, or assets of the State; such as Public Safety

[1] HIPAA is the United States Health Insurance Portability and Accountability Act of 1996, PL 104-191. The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act.

Information. Data that is specifically protected by law (e.g.. HIPAA).

State of Delaware Top Secret – Information that could, if divulged, expose the State's citizens and assets to great risk.

Generally, any data classification that is higher than public should be considered non-public. The classifications stated herein are to be considered as **minimum classification levels** for the data. The Data Steward may not specify a lower classification.

These classifications are in line with the Federal Government data classifications. The exception is that the Federal Government has no consistent designation for Public data. In some cases, the term Unclassified is used to denote non-Confidential, non-Secret and non-Top Secret data. For clarity, the State of Delaware chose to use the term State of Delaware Public data rather than non-Confidential, non-Secret and non-Top Secret data. One core value that distinguishes a classification from another is the Risk of Harm. What is the risk that harm can result from the inappropriate disclosure or use of this information?

Minimum Classifications

The following data elements are examples of data that must be classified no lower than as shown regardless of the context in which they are represented.

Data Element	Classification
Social Security Number	State of Delaware Confidential
Employee ID	State of Delaware Confidential
Bank Account Number	State of Delaware Confidential
Credit Card Number	State of Delaware Confidential
Mother's Name	State of Delaware Confidential

Father's Name	State of Delaware Confidential
Place of Birth	State of Delaware Confidential

The statewide policies and standards pertaining to data protection can be found at the DTI website. Local guidelines are established by the state organization itself. For a complete list, please contact the organization's Information Resource Manager (IRM).

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including review of proposed projects and during the design, development or support of systems. This policy may also be enforced by others during the course of their normal business activities, including audits.

If any dispute arises regarding the minimum classifications of data contained in this policy, the waiver process will resolve the issue. If any disputes or questions arise from the Data Classification Guidelines, the data steward or designee can present them to the State's Chief Security Officer for help in determining the proper classification.

Failure to Comply
Failure to comply with the policy is a serious matter whether through intentional act or negligence and may be 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 shall be subject to appropriate discipline without recourse, except as provided by law. While DTI has no authority to discipline employees of other agencies/organizations in the Executive, Legislative, or Judicial branches of government, it will take the appropriate steps to ensure any misconduct is appropriately addressed.

II. Definitions

Data – Distinct pieces of information in digital (computer-readable) format that can be stored, read, manipulated, or transmitted.

Dataset – A Dataset is a collection of data elements in a structure that is its own unique entity and usually associated with a name. Examples include files, databases, etc. A Dataset's classification must be at least as high as that of the highest data element contained therein (classification by association). This also applies to multiple Datasets when stored or transmitted together; the classification of the combined Datasets must be at least as high as that of the highest Dataset in the combination.

Data Owner –
Consult the Delaware Information Security Policy for this definition

Data Steward –

Consult the Delaware Information Security Policy for this definition

Data User -
Consult the Delaware Information Security Policy for this definition

Information Resource Manager (IRM) – Those assigned the responsibility to act as the primary points of contact for appropriate communications between DTI and the organization.

Personally Identifiable Information (PII) – Information which can be used to identify or contact a person uniquely and reliably, or can be used with other sources to uniquely identify an individual. Examples include but are not limited to full name, full social security number, full date of birth, street address, telephone number, email address, and fingerprints or other biometric data.

III. Development and Revision History

Date	Revision
3/1/2006	Rev 1 – Initial version
2/28/2008	Rev 2 – Updated version
3/22/2011	Rev 2 – Minor revision
4/4/2014	Rev 2 – Minor revision
1/19/2021	Rev 2 – Updates for data destruction
2/3/2023	Rev 2 – Updates for links
02/26/2024	Rev 3 – Updates for definitions and NIST reference

IV. Approval Signature Block

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

V. Other Documents

A Data Classification Guideline has been published and it is hereby noted. If there is any conflict between the Data Classification Guideline and this policy, the policy shall prevail. To obtain more information, please reference the Enterprise Standards and Policies and notable the Delaware Information Security Policy for further insight.

External Providers must provide written Certificate of Destruction as directed in the Delaware Terms and Conditions Governing Cloud Services and Data Usage Agreement.

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 Technology Investment Council on an ongoing basis and 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.

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

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

Doc Ref Number:	SE-CLD-001	**Revision Number:** 7
Document Type:	Enterprise Policy	**Page:** 1 of 6
Policy Title:	Terms and Conditions Governing Cloud Services and Data Usage	

Synopsis:	This policy provides guidance for State of Delaware organizations to utilize offsite or cloud facilities and services, including hosting and computing (XaaS: e.g, Software-, Infrastructure-, Platform-, etc., as-a-Service). Additionally, it addresses situations when State data is used by an entity for audit, research, or other purposes.
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 Technology Investment Council on an ongoing basis and 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:	5/15/2013
Reviewed:	4/14/2023
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

Section **Page**

I. Policy

EXECUTIVE SUMMARY

Cloud and offsite hosting and services (contracted Xaas: Infrastructure-, Platform-, Software-as-a-Service) offer credible alternatives to traditional IT delivery models. Contracted XaaS can provide benefits such as rapid delivery, enhanced scalability, development agility and new funding models.

PURPOSE

This policy establishes the terms and conditions for contracted XaaS and establishes terms and conditions for data usage. All IT-related RFPs, Contracts, etc. and data sharing engagements that may involve offsite hosting must abide by this policy. The terms and conditions set forth in this policy will help to protect the State's organizations by mitigating the risks associated with entrusting the State's computing operations and data to a third party.

POLICY STATEMENT

New contracts and amendments to contracts with service providers, as well as agreements regarding others (including but not limited to audit, research, etc.), are expected to include a cloud services and data usage signed agreement, as applicable, approved by DTI. When it applies, the *Terms and Conditions Governing Cloud Services and Data Usage* policy requires a signed *Terms and Conditions Governing Cloud Services and Data Usage Agreement*. Contracts or other agreements already in force will be expected to include the applicable signed agreements approved by DTI at the next renewal or revision date. The following standard agreement is available:

- *Terms and Conditions Governing Cloud Services and Data Usage Agreement* (PDF)

Nothing in this policy statement or its related agreement precludes state agencies from imposing their own industry-specific terms and conditions as their business might require, above and beyond those promulgated by DTI.

IMPLEMENTATION RESPONSIBILITY

DTI and/or the organization's technical staff will implement this policy during the course of normal business activities, including project execution and the design, development, or support of systems.

Service providers should be familiar with, and adhere to, security guidelines closely aligned with standardized industry approaches to assessment, documentation, monitoring, and controls for cloud products and services, such as those promulgated by the Federal Risk and Authorization Management Program (FedRAMP), Cloud Security Alliance (CSA), the National Institute of Standards and Technology (NIST), and other accreditation authorities as these become recognized by the industry.

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including review of proposed projects and during the design, development, or support of systems. This policy may also be enforced by others during the course of their normal business activities, including contract execution, review or amendment, audits, and design reviews.

Cyber Security Liability Insurance

The State of Delaware places paramount importance on protection of sensitive Personally Identifiable Information (PII) or otherwise confidential information as defined by 6 *Del. C.* §1202C (15) and §12B-101(7)a, and as noted below under Section II – Definitions.

In accordance with the State's Terms and Conditions Governing Cloud Services and Data Usage Agreement Item 5, non-public state data shall be encrypted in transit and, for PII data, at rest. A service provider will employ validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2 Security Requirements. When the Service 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. Such a liability protection policy shall comply with the State's requirements, incorporated by addendum to this policy (see Addendum 1: Cyber Security Liability Insurance Requirement).

In the event a service provider fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to pursuing any other remedies available, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

If there is ambiguity or confusion regarding any part of this policy, seek clarification from the point of contact defined in the header of this policy.

II. Definitions

Personally Identifiable Information (PII)

1. Information or data, alone or in combination, that identifies or authenticates a particular individual. 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 Delaware Code Title 6 § 12B-101 Title 6, §1202C, and Title 29 §9017C or any other applicable State of Delaware or Federal law.

III. Development and Revision History

Date	Revision
5/15/2013	Rev 0 – Initial version
8/27/2014	Rev 1 – Updated version
11/17/2014	Rev 2 – Updated version
11/23/2015	Rev 3 - Removed language regarding the State's inclusion on the insured list.
3/1/2016	Rev 4 - Added Tiered Coverage Schedule. Added PII definition. Adjusted Ponemon value. Updated link for The Center for Digital Government 2014 study of Cloud Security Procurements.
10/10/2016	Rev 5 - Added language and references to State standards in the Implementation Responsibility section.
2/1/2018	Rev 5 - Added language and references to State standards in the Implementation Responsibility section.
6/18/2018	Rev 6 - Revised policy titles and agreement references. Added language and references to new Data Usage Terms and Conditions Policy, as well as to State standards in the Implementation Responsibility section; revised DelCode references with respect to definitions of Personally Identifiable Information (PII); moved information regarding Cyber Liability Insurance Requirement to be incorporated by Addendum 1.
4/14/2023	Rev 7 – Revised the wording to reflect the consolidated policy and agreement documents.

IV. Approval Signature Block

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

Listing of Appendices

APPENDIX 1 - CYBER SECURITY LIABILITY INSURANCE REQUIREMENTS

- Issued by an insurance company acceptable to the State of Delaware and valid for the entire term of the contract, inclusive of any term extension(s).
- Liability limits will be calculated based on the maximum system record count over the life of the contract and the ***Ponemon Institute*** average Public Sector Breach cost per record as published in the most recent *Cost of Breach Study* (e.g., 2017, $141). Refer to the Tiered Coverage Schedule below.

Tiered Coverage Schedule

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

- Shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
- At a minimum, the policy must include third party coverage for credit monitoring; notification costs to data breach victims; and regulatory penalties and fines.
- Shall apply separately to each insured against whom claim is made or suit is brought subject to the Service Provider's limit of liability.
- Shall include a provision requiring that the policy cannot be cancelled without thirty days written notice to the State Chief Information Officer.
- The Service Provider shall be responsible for any deductible or self-insured retention contained in the insurance policy.
- The coverage under the policy shall be primary, and not excess, to any other insurance carried by the Service Provider.
- The State of Delaware shall not be a named or additional insured under the policy.

DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION
CERTIFICATE OF DATA DESTRUCTION
By External Entity/Company

The information described below was destroyed in the normal course of business pursuant to State of Delaware retention schedule and the following policies and contract(s):

- The Delaware Information Security Policy:
  http://dti.delaware.gov/pdfs/pp/StateOfDelawareInformationSecurityPolicy.pdf

- Data Classification Policy:
  http://dti.delaware.gov/pdfs/pp/DataClassificationPolicy.pdf

- Disposal of Electronic/Storage Media Policy:
  http://dti.delaware.gov/pdfs/pp/DisposalOfElectronicEquipmentAndStorageMedia.pdf

- Enter Contract Name and number here, along with a brief description:
  <for example> XXX will destroy all data files at the conclusion of the project and send a certified letter to the DTI Chief Security Officer indicating the date, time and confirmation of the destruction. Include with the Data Destruction Certification Letter and this form and any documentation produced from the data destruction/data wipe software such as a certificate or certification log.

Date of Destruction:	Authorized By:
Description of Information Disposed of/Destroyed:	
Inclusive Dates Covered:	
METHOD OF DESTRUCTION: ☐ Burning ☐ Overwriting ☐ Pulping ☐ Pulverizing ☐ Reformatting ☐ Shredding ☐ Other:_____	
Records Destroyed By*:	
If On Site, Witnessed By:	
Department Manager:	
**If records destroyed by outside firm, must confirm a contract exists.*	

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

Doc Ref Number:	DTI-0051.01	**Revision Number:** 6
Document Type:	Enterprise Policy	**Page:** 1 of 4
Policy Title:	Disposal of Electronic Equipment/Storage Media	

Synopsis:	Provides requirements on the Disposal of Storage Media, Personal Computers, Peripherals, Handheld Devices, other electronic media that store State's data, and printed media generated from State systems.
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 Technology Investment Council on an ongoing basis and 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:	8/7/2006
Reviewed:	6/8/2023
Approved By:	Chief Information Officer
Sponsor:	Chief Operating Officer

TABLE OF CONTENTS

I. Policy

DISPOSAL OF STORAGE MEDIA, COMPUTERS, MOBILE DEVICES, PRINTERS, COPIERS, PERIPHERALS OR OTHER PROPERTY THAT STORES DIGITAL DATA

When applicable assets are no longer suitable for use, they shall be destroyed according to National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization SP 800-88 Rev. 1.This requirement applies to all permanent disposal of property identified by the Data Steward as containing State of Delaware confidential, secret, or top secret information. This requirement applies regardless of the identity of the recipient, e.g. transfer to schools via Partners in Technology, Division of Support Services, Surplus Services or landfill disposal. Additionally, disposal of digital media that contained or contains Federal Tax Information (FTI) must adhere to the IRS Publication 1075. The appropriate sanitization must be performed by authorized technicians who are qualified to perform such procedures. Certificates of destruction must be kept on file and a copy sent to eSecurity@delaware.gov.
External Providers must provide written Certificate of Destruction as directed in the Terms and Conditions Governing Cloud Services and Data Usage Agreement.

Whenever possible, computer purchases should include the option of retaining qualified hard drives while receiving a replacement drive. This maintains control over sensitive and

confidential data and gives flexibility to identify the best method of disposal for failed drives.

For item(s) going in for maintenance and repair, equipment shall have a backup of the stored information/data taken for a future reinstall. Then the information/data shall be removed according to NIST 800-88 from the equipment to be serviced. Verification of the removal of the information/data must be certified by the technicians that are performing this function. This is done to reduce the risk of data leakage. Once the item is received back from repair and is functional, the information/data will be restored onto the equipment. If the drive is not functional, then the maintenance personnel performing the repairs must be bonded and sign the organization's confidentiality statement. A confidentiality reminder notice must accompany the equipment during this type of repair.

DISPOSAL OF PRINTED OUTPUT

Based on the data classification, the resulting printed media from the State's systems shall be disposed of based on the retention schedule from the Delaware State Archives, data classification, Data Custodian's agency policy, and all State and Federal guidelines. All printed media that contains data that is classified as State of Delaware confidential, secret, or top secret shall be shredded and destroyed to maintain the privacy, confidentiality, and integrity of the State's data. If the data on the printed medium is not considered State of Delaware confidential, secret, or top secret, then it may be recycled. The following requirements must be observed when destroying FTI printed media – IRS Publication 1075.

II. Definitions

1) **FTI** – Federal Tax Information. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

Date	Revision
3/27/2004	Rev 0 – Initial version
8/7/2006	Rev 1 – Reformatted version
1/7/2008	Rev 2 – Updates
4/13/2011	Rev 3 – Updates
10/15/2013	Rev 3 - POC changed
5/27/2014	Rev 3 - Removed the reference to the Dell program
2/16/2018	Rev 4
1/19/2021	Rev 5 - Added Data Destruction Certification Form Reference
6/8/2023	Rev 6 – Updated external references and added a requirement to email certificates of destruction to esecurity@delaware.gov

IV. Approval Signature Block

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

Guidelines ID:	SE-IAM-003
Title:	**Identity and Access Management Guideline**
Revision Number:	1
Domain:	Security
Discipline:	Identity and Access Management
Effective:	6/14/2022
Reviewed:	10/17/2023
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

I. Authority, Applicability and Purpose

A. 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 Technology Investment Council on an ongoing basis and the CIO"

B. Applicability: Applies to all 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 funding, access and continued use of these resources.

C. Purpose: This guideline describes many of the features that are provided by the State Identity Management service.

II. Scope

A. Audience: This guideline addresses how applications and user will interact with several of the features of the State's Identity Management service

B. Areas Covered: This guideline covers a variety of areas such as strong password, multi-factor authentication, identity proofing, lifecycle management and additional areas.

C. Environments: This guideline addresses all the environments in use by consuming applications and systems.

III. Process

A. Adoption: These guidelines have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the State of Delaware.

B. Revision: Technology is constantly evolving; therefore the guidelines will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors: Contractors or other third parties are required to comply with these guidelines when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection of the proposed technology solution. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. Implementation responsibility: DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement: DTI will enforce these guidelines during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These guidelines may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us: Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Declarations

A. Definitions

1. Multi-factor authentication – It consists of a combination of two or more authentication methods. The State of Delaware currently uses RSA Keys. Multi-factor Authentication is to be reserved for those instances where strong passwords do not provide adequate security.
2. Pass phrases – They are strings of words and characters typed to authenticate into a network as opposed to a password of usually 6 – 12 characters. Pass Phrases can be much longer, up to 100 characters or more.
3. Resource Account – It is a user account created to facilitate non-interactive authentication. Examples include Windows service accounts, Exchange resource accounts and accounts created exclusively for inter-device or inter-process communication.
4. Service Account – It is a user account that is created explicitly to provide a security context for services running on a Windows machine.

.

V. Guidelines

A. **Simplified Logons** – Provide an easy logon experience.

1. Identity Authentication for State Internal Communications and Computing Resources
    i. Employee and contractor identities for accessing state internal and back-end applications, systems and networks must be authenticated with the computing tenant called **ID.Delaware.gov**
2. Constituent; Residents and Visitors Identity Authentication for Public-Facing Digital Government Resources
    i. Constituent, resident and visitor identities for accessing state digital government services and applications must be authenticated, authorized and accounted for through the computing tenant called **My.Delaware.gov**

B. **Strong Passwords** – Meet or exceed the defined criteria for strong passwords.

1. All passwords used to access State of Delaware data must adhere to the following characteristics for strong passwords:
    i. Passwords must be at least ten characters long. The security of a password rises exponentially with the number of characters used in the password. Pass Phrases are recommended.
    ii. Passwords/phrases cannot contain whole or significant parts of the username, first name or last name of the user.
    iii. Active Directory (not K12) passwords (used for email, used for logging into Windows, etc) on the State network must be at least 10 characters long.
    iv. A password must not be repeated/reused within 8 resets.
    v. Passwords should not be a common word or name.
    vi. All personnel must treat passwords and other access credentials as confidential and should protect them from disclosure. Refer to the Standards and Policies and notably to the State of Delaware Information Security Policy for further insight.
2. Human/User accounts - These passwords must contain characters from at least three (3) of the following four (4) classes from the Acceptable Password Characters table below:

ACCEPTABLE PASSWORD CHARACTERS	
DESCRIPTION	**EXAMPLES**
English upper-case letters	A, B, C, ... Z
English lower-case letters	a, b, c, ... z
English (Arabic) numerals	0, 1, 2, ... 9
English Non-alphanumeric ("special characters")	#,$,%,& such as punctuation symbols etc.

3. Service/Resource Accounts - Passwords used to access State of Delaware data must adhere to the following characteristics for strong passwords:
    i. Passwords must be at least 32 characters long or the maximum number of characters available.
    ii. Passwords must contain characters from at least three (3) of the following four (4) classes from the Acceptable Password Characters table shown above.

    A different service/resource account must be used for different services.

    A named person must be designated as the owner of each service/resource account.

C. Self-Service Account Management – Provide a self-service capability.

1. State identity services must enable users to manage certain elements of their identity. This can include email address and phone number.
    i. Solution must support password reset and or changes to existing identities.
    ii. Solution must support notifications on account lockouts and enable self-service account unlock.
    iii. Solution must clearly present password complexity requirements and restrictions during creation, change, or updates.

D. Multi-factor Authentication (MFA) – Provide several methods to authenticate.

1. Adaptive multi-factor authentication is required for all applications, systems, and network access.
2. Adaptive multi-factor authentication must take into consideration the risk associated with login sessions to trigger additional validation. Suspicious activity must be reported to the account owner and the administrators of the solution.
3. Risk assessment considerations that should trigger reporting and MFA validation:

i. Geo-related information, such as unusual source country or region

ii. Bot-related or non-human connectivity activity

E. **Suspicious Activity** – Report unusual activities.

1. Suspicious activity must be reported to the account owner and the administrators of the solution. These include:
    i. Login from unknown asset
    ii. Login from unexpected location
    iii. Change of password
    iv. Change or addition of multi-factor authentication options

F. **Lifecycle Management** - The State's identity and access management system must track an employee or contract from position appointment, through position changes to eventual retirement or separation from state government services.

1. The State Chief Security Officer may recommend enhanced username schemas to mitigate authentication attacks where necessary. For instance, User IDs may be recommended to follow the naming schema below:
    i. User IDs must be unique across all branches of government and K12
2. The solution must allow new employees and contractors to be provided a digital identity to authenticate to state systems, applications, networks, and data
3. The State technology teams with oversight from the Chief Security Officer should periodically review user access rights to make sure that access is still required for assigned functions.
4. The State's identity and access management solution should ensure there is a clear separation of duties (SoD) process in place to:
    i. ensure granted access does not lead to conflict of interest combination, and
    ii. actively prohibit access levels that can lead to such situations.
5. The solution must enable the expedited and automated (where possible) removal of access for separating employees and contractors.
6. The State's identity lifecycle management solution must enable the identity proofing of new hires, using an approved identity proofing option, before access is provisioned within any internal directory store.

G. **Identity Proofing** – Utilize a service to verify identity.

1. The state partners with the approved identity proofing vendors below:
    i. Government ID Proofing - Onfido
    ii. Knowledge-based ID Proofing - Lexis/Nexis
2. Limited options for Manual identity proofing services will be offered through designated state service centers.

H. **Legacy identity and access management solutions** – Address legacy solutions.

1. Initiate plans and activities to transition to the State's Identity Management service and away from legacy solutions such as:
    i. ACF2
    ii. Oracle IAM
    iii. Microsoft ADFS

I. **User Authentication** – Provide adaptive multi-factor authentication.

1. Must utilize Claim-based authentication.
2. Must support Federation with other third-party identity providers.
3. Must be SAML2.0/OAuth/OpenID aware, compliant and supported.
4. Must demonstrate Multi-Factor Authentication (MFA).
5. Must utilize the state enterprise identity directory stores.
6. Use of Microsoft Active Directory for direct authentication or authorization is deprecated.

J. **Exceptions** – On a case-by-case basis, applications with validated technical limitations may be authorized by DTI to operate without full compliance.

VI. Development and Revision History

Date	Revision
6/14/2022	Rev 0 – Initial version
10/17/2023	Rev 1 – Added SAML2.0 awareness and removed User ID naming scheme

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

Doc Ref Number:	SE-IAM-001	**Revision Number:** 1
Document Type:	Enterprise Policy	**Page:** 1 of 5
Policy Title:	Identity and Access Management Policy	

Synopsis:	Management of identity and the authentication of users prior to obtaining access to State information is critical.
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 Technology Investment Council on an ongoing basis and 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:	6/14/2022
Reviewed:	7/18/2022
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

Section **Page**

I. POLICY

EXECUTIVE SUMMARY

Identity is the critical foundational element for the security and protection of state data and information systems. It must uniquely identify, validate, and confirm the user or system accessing state communications and computing resources with non-repudiation. Authenticating users and systems before they gain access to State information and resources has never been more important.

PURPOSE

All state applications, systems, networks, and data access must ensure they are using a State Chief Security Office designated directory store to effectively identify access to state data. This policy defines the requirements for authentication, authorization, and accounting for access to state applications, systems, networks, and data.

POLICY STATEMENT

1. State applications, systems, and networks controlling access to state constituent, employee, or financial data, must be authenticated, authorized, and accounted for through the state designated identity and access management solution.
2. State of Delaware internet facing applications that require the registration of constituent, resident, and/or visitors using their personally identifiable information, or

state applications that collect, store, or use personally identifiable information, must utilize the state designated identity and access management solution.

3. Identities used in the access to state applications, systems, networks, and data must be validated and proofed through a State Chief Security Office approved process or solution that ensures nonrepudiation of all activity.
4. The State identity and access management solution must protect the privacy of constituents', visitors', and residents' private identifiable information (PII). It must ensure they have:
   - The right to be forgotten and, to have their information deleted if they are no longer consuming state resources.
   - The right to know the applications accessing the identity information they have provided.
   - The right to not have their information sold or monetized.
   - The right to initiate the sharing or the transfer of their information to third party vendors.
5. All security-related activity must be logged with the required information (see standard/guideline) and upon request, the logs must be provided.
6. Identity and access management solutions must provide lifecycle management of all employees and contractors from position appointment, through position changes to eventual retirement or separation from State government.
7. Identity and access management solutions must enable the expedited and automated (where possible) removal of access for separating employees and contractors.
8. All Internet-facing applications must be compliant by 12/31/2023. All other state applications must be compliant by 12/31/2024.
9. The following areas are out of scope:
   - Authentication into mobile devices, legacy solutions like mainframes and Internet of Things (IOT) devices.
   - Authentication, authorization, and accounting requirements for ACF2 controlled applications, systems, and infrastructure.

II. DEFINITIONS

ACF2 –a security suite that is often used on mainframes.

Authentication (AuthN) – proving the person is who they say they are.

Authorization (AuthZ) – those things and only those things this authenticated person can do.

Directory store – a location or database of user account information.

Identity Access Management (IAM) – a centrally managed authentication service.

Internet-facing solution – a type of solution with an interface that is accessible to the Internet.

Internet of Things (IoT) devices – hardware devices that have the ability to collect and exchange information over the Internet.

Lifecyle Management – the discipline of ensuring that the information is current and relevant. In the context of this policy, it is confirming that new users are added and users, who are no longer with the State, are removed from the appropriate directory stores.

Mainframe – a large high-speed computer.

Non-repudiation – the process by which the sender must receive confirmation of delivery and the recipient must receive proof of sender's identity.

III. DEVELOPMENT AND REVISION HISTORY

Date	Revision
6/14/2022	Rev 0 – Initial version
7/18/2022	Rev 1 – Added definition section

IV. APPROVAL SIGNATURE BLOCK

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

V. RELATED POLICIES AND STANDARDS

Identity and Access Management Standard
Identity and Access Management Guidelines

Standard ID:	SE-IAM-002
Title:	**Identity and Access Management Standard**
Revision Number:	2
Domain:	Security
Discipline:	Identity and Access Management
Effective:	6/14/2022
Reviewed:	2/28/2024
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

I. Authority, Applicability and Purpose

A. 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 Technology Investment Council on an ongoing basis and the CIO"

B. Applicability: Applies to all 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 funding, access and continued use of these resources.

C. Purpose: Applications containing State data must address the requirements outlined in this document such as authorization, session management and logging.

II. Scope

A. Audience: This standard addresses applications and the requirements that must be met by the developers. This document is not intended for use by non-IT personnel.

B. Areas Covered: This standard covers applications containing State data.

C. Environments: This standard applies to all applications that process, store or display State data.

III. Process

A. Adoption: These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the state of Delaware.

B. Revision: Technology is constantly evolving; therefore, the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors: Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection of the proposed technology solution. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. Implementation responsibility: DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement: DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us: Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Declarations

A. Declarations

1. User authorization
   - Must be SAML2.0/OAuth/OpenID aware, compliant, and supported
   - Must be System for Cross-domain Identity (SCIM) compliant
   - Must support Role-based access authorization
   - Must follow a Least Privilege User Access model
   - Must demonstrate General Password and Authenticator Requirements
   - Must have credential storage requirements
   - Must have cryptographic Software and Device verifiers
   - Must have Service Authentication and Out of Band Verifiers
   - Must have Look-up Secret Verifiers and Credential Recovery requirements

2. Session Management
   - Custom session management must not store session parameters on the client side, even if encrypted
   - User sessions must be cancelled at the moment a user logs out of the web application
   - Sessions must have a timeout set after a specified period of inactivity
   - Sessions should have a secure flag set to prevent unauthorized viewing of session identifiers
   - Sessions must be invalidated on user log out
   - Session tokens must be sufficiently long and random
   - Session cookies must have appropriately restricted paths
   - Sessions must not permit duplicate concurrent user sessions from different machines
   - User must be able to see and terminate all sessions
   - User must be prompted for session termination on password change
3. All security related activity must be logged such as
   - Authentication
   - Authorization and privilege use
   - Create/Delete/Read/Change/Update
   - Successful and failed application authentication attempts
   - Application startups and shutdown
   - Major application configuration changes
4. Logs with security related activity must contain
   - Timestamp to NTP
   - Event, status, and error codes, event severity where possible
   - Service/command or application name
   - User or system account associated with event; where are service account is used, the true user account must be captured too
   - Connection source and destination
   - Session ID, terminal session ID and user-agent details of browser or tool used
   - Security Logs must not contain sensitive user information like PII (SSN, DOB) Bank Information (CC, Account information)
   - Source and destination IPs, source and destination ports
   - Payload size when possible

- The identity of the user should not be lost while traversing the web service, middleware or when calling the database for data
- Security logs should be separated from transaction logs wherever possible
- Ability to change, modify or delete logs must be restricted
- Systems must collect and retain at least 90 days' worth of logs
- Compliance related systems must collect and maintain 7 years' worth of logs
- Logs older than 90 days can be archived to less expensive storage

5. On a case-by-case basis, applications with validated technical limitations may be authorized by DTI to operate without full compliance.

V. Development and Revision History

Date	Revision
6/14/2022	Rev 0 – Initial version
10/17/2023	Rev 1 – Added SAML2.0 awareness and removed SCIM compliance
2/28/2024	Rev 2 – Added SCIM compliance