	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

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:** 2 of 61
Policy Title:	State of Delaware Information Security Policy	

TABLE OF CONTENTS

	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:** 3 of 61
Policy Title:	State of Delaware Information Security Policy	

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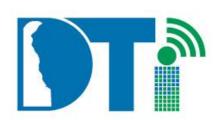**DEPARTMENT OF TECHNOLOGY AND INFORMATION**
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-ESP-001		**Revision Number:** 7
Document Type:	Enterprise Policy		**Page:** 5 of 61
Policy Title:	State of Delaware Information Security Policy		

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:

"Delivering Technology that Innovates"

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:	6 of 61
Policy Title:	State of Delaware Information Security Policy		

- 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.

| 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:** 8 of 61
Policy Title:	State of Delaware Information Security Policy	

- **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.

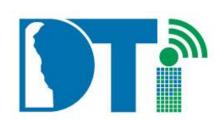9. Ensures appropriate backups are taken and tested.

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:** 9 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

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

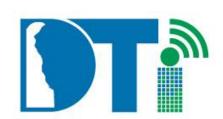| **Doc Ref Number:** SE-ESP-001		**Revision Number:** 7
Document Type: Enterprise Policy		**Page:** 10 of 61
Policy Title: State of Delaware Information Security Policy		

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

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

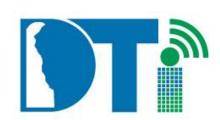| Doc Ref Number:	SE-ESP-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 11 of 61
Policy Title:	State of Delaware Information Security Policy	

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 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:	12 of 61
Policy Title:	State of Delaware Information Security Policy			

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.

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: 13 of 61
Policy Title:	State of Delaware Information Security Policy		

- 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.

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: 14 of 61
Policy Title:	State of Delaware Information Security Policy	

- 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.

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: 15 of 61
Policy Title:	State of Delaware Information Security Policy	

- 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.

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:** 17 of 61
Policy Title:	State of Delaware Information Security Policy	

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)

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:	18 of 61
Policy Title:	State of Delaware Information Security Policy		

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**

	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:**	20 of 61
Policy Title:	State of Delaware Information Security Policy		

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

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:** 21 of 61
Policy Title:	State of Delaware Information Security Policy	

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**

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:** 22 of 61
Policy Title:	State of Delaware Information Security Policy		

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.

Doc Ref Number:	SE-ESP-001	**Revision Number:**	7
Document Type:	Enterprise Policy	**Page:**	23 of 61
Policy Title:	State of Delaware Information Security Policy		

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

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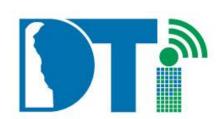
Administrator Accounts require special protection commensurate with the data that is accessed/controlled. This is also known as a privileged account. See Data Classification Policy.

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)

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: 24 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

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

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**

	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:** 26 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

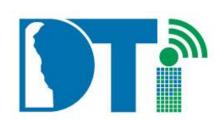Accounts on all platforms are reviewed at least twice a year for usage and activity and the status evaluated by the ISO and Data Steward. Where applicable, a list of unused and inactive user IDs is sent to the Organization ISOs by DTI. Accounts that are dormant over ninety (90) calendar days are evaluated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

	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:** 27 of 61
Policy Title:	State of Delaware Information Security Policy	

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**

Doc Ref Number:	SE-ESP-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 28 of 61
Policy Title:	State of Delaware Information Security Policy	

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

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.

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: 29 of 61
Policy Title:	State of Delaware Information Security Policy	

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
    - o Determine if there has been a security breach
    - o 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
    - o Central communication point to receive information on security incidents and to disseminate vital information to appropriate State entities about the incidents
    - o Ability to quickly notify organization management and the DTI Service Desk of the security incident
- Containment, Eradication, and Recovery
- Post-incident Activity
    - o Document and catalog security incidents.
    - o Continually update current systems and procedures
    - o Analyze event information and reports to determine trends and patterns of intruder activity

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: 31 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

	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:** 33 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

"Delivering Technology that Innovates"

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:** 34 of 61
Policy Title:	State of Delaware Information Security Policy	

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

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: 35 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

Doc Ref Number:	SE-ESP-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 36 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

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: 37 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

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:** 38 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

	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:** 39 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

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: 41 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

"Delivering Technology that Innovates"

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: 42 of 61
Policy Title:	State of Delaware Information Security Policy	

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

"Delivering Technology that Innovates"

Doc Ref Number: SE-ESP-001	**Revision Number:** 7
Document Type: Enterprise Policy	**Page:** 43 of 61
Policy Title: State of Delaware Information Security Policy	

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

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.

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: 44 of 61
Policy Title:	State of Delaware Information Security Policy	

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

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: 45 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

Doc Ref Number:	SE-ESP-001	Revision Number: 7
Document Type:	Enterprise Policy	Page: 46 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

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: 47 of 61
Policy Title:	State of Delaware Information Security Policy	

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.

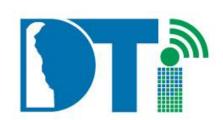## Workstation & Computing Resource Access
Related ISO 27002:2013 clause(s): **6.2, 8.3.1, 9.1.1, 9.3, 9.4.2, 11.1, 11.1.5, 11.2.1, 11.2.8, 11.2.9, 14.1.2**

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,

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:** 48 of 61	
Policy Title:	State of Delaware Information Security Policy		

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

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: 49 of 61
Policy Title:	State of Delaware Information Security Policy	

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

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: 51 of 61
Policy Title:	State of Delaware Information Security Policy	

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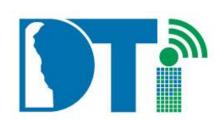
It is those things and only those things this authenticated person can do.

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.

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: 52 of 61
Policy Title:	State of Delaware Information Security Policy	

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)
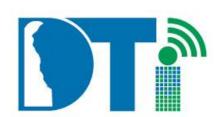
Service Models:

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.

	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:** 53 of 61
Policy Title:	State of Delaware Information Security Policy	

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).
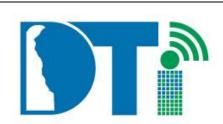
Deployment Models:

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

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:**	54 of 61
Policy Title:	State of Delaware Information Security Policy		

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

	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:** 55 of 61
Policy Title:	State of Delaware Information Security Policy	

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

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:	56 of 61
Policy Title:	State of Delaware Information Security Policy		

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.
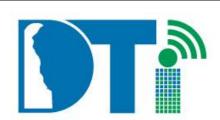
Information remnance control

Control of information remnance prevents unauthorized and unintended information transfer.

Information Resource Manager (IRM)

Information Resource Managers are organization IT managers or administrators.

	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:** 57 of 61
Policy Title:	State of Delaware Information Security Policy	

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

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:**	58 of 61
Policy Title:	State of Delaware Information Security Policy		

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.

"Delivering Technology that Innovates"

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:	59 of 61
Policy Title:	State of Delaware Information Security Policy		

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.

"Delivering Technology that Innovates"

	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:** 61 of 61
Policy Title:	State of Delaware Information Security Policy		

IV. Approval Signature Block

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

V. Listing of Appendices

None.