



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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	1 of 45
Policy Title:	State of Delaware Information Security Policy		

Synopsis:	<p>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.</p> <p>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.</p> <p>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 27002:2005 (17799) (International Organization for Standardization Code of Practice for Information Security Management.) – the International Security Standard.</p>		
Authority:	<p>Title 29, Delaware Code, §9004C – General Powers, duties and functions of DTI “2) Implement statewide and interagency technology solutions, policies, standards and guidelines as recommended by the Technology Investment Council on an ongoing basis and the CIO, including, but not limited to, statewide technology and information architectures, statewide information technology plans, development life cycle methodologies, transportation facilities, communications protocols, data and information sharing considerations, the technique of obtaining grants involving the State's informational resources and the overall coordination of information technology efforts undertaken by and between the various State agencies;”</p>		
Applicability:	<p>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 School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.</p>		
Effective Date:	February 1, 2007	Expiration Date:	None
POC for Changes:	DTI Chief Security Officer		
Approval By:	Cabinet Secretary - State Chief Information Officer		
Approved On:	February 1, 2007		





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	2 of 45
Policy Title:	State of Delaware Information Security Policy		

TABLE OF CONTENTS

I.	Policy	4
	Policy Compliance	4
	General Security	5
	Related Documents	5
	Roles	5
	Asset Inventory and Data Classification	12
	Disaster Recovery/Continuity of Operations Plan (DR/COOP)	13
	Critically Classification	
	Policy Maintenance	13
	Consequences and Disciplinary Action	14
	Administrative Safeguards	14
	Privacy	14
	Security Clearances	15
	Authentication and Authorization	16
	Unique User Access Credentials	17
	Password Management	17
	Computing Resource Log Off and Screensavers	18
	Login Failure Lockout	18
	Disabling Inactive Accounts	19
	Review of System Access	20
	Roles Based	20
	Terminations and Transfers	20
	Segregation of Duties	20
	Segregation of Production and Test	21
	Change Control	21
	System Documentation	21
	Security Awareness and Training	21
	Protection from Malicious Software	22
	Security Incident Procedures	22
	Data Backup Plan	23
	Disaster Recovery Plan and Testing	24
	Continuity of Operations Planning	25
	Third-Party Business Contracts	25





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	3 of 45
Policy Title:	State of Delaware Information Security Policy		

	Software Copyright (Licensure)	26
	Technical Safeguards	28
	Transmission Security	28
	Integrity Controls	28
	Cryptography	28
	Cryptographic Controls	29
	General Cryptography	29
	Technical Cryptography Policy Statements	30
	Cryptography Key Management	30
	Monitoring	31
	Intrusion Detection	31
	Server Hardening	32
	Patch Management	33
	Security Reviews	33
	Network Security	33
	Equipment and System Setup and Configuration	34
	Remote Access	34
	Firewalls	34
	Internal Network Addresses and Designs	35
	Software Development and Intellectual Property	35
	Outsourced Software Development	36
	Procurement Security	36
	Physical Safeguards	37
	Facility Access Control	37
	Workstation & Computing Resource Access	38
	Equipment Security	39
	Disposal of Electronic Storage Media	39
	Hard Copy Information Handling	40
	Photography Controls	41
II.	Definitions	41
III.	Development and Revision History	45
IV.	Approval Signature Block	45
V.	Listing of Appendices	45





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	4 of 45
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 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 must be 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.

The DTI Chief Security Officer Team will periodically review compliance to 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 ISO for review and follow up.

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

- Delaware Security Breach Notification (Title 6, Commerce and Trade, Chapter 12B. Computer Security Breaches).
- Health Insurance Portability Accountability Act of 1996 (HIPAA).





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	5 of 45
Policy Title:	State of Delaware Information Security Policy		

- 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.

General Security

Related Documents

Related ISO 27002:2005 clause(s): **5.1.1**

Related published State, DTI policies, standards, and procedures can be reviewed at <http://dti.delaware.gov/information/standards-policies.shtml> and <http://intranet.state.de.us/dti/learnpolicies.htm>. In the event of any conflict between this policy and any other policy or standard referenced herein, the current version of the referenced policy or standard shall take precedence over this policy.

Roles

Related ISO 27002:2005 clause(s): **6.1.1, 6.1.2, 6.1.3, 6.1.5, 6.1.6, 7.1.1, 7.1.2, 8.1, 15.2.1**

Data Owner

Data in use by State of Delaware Organizations, in transit through, or residing within the computing infrastructure shall be considered State property and owned and controlled by the State of Delaware according to statute. This fact of law results in differing definitions when considering the ISO 27002 standard for roles in name only. The responsibilities for data protection are clarified in the roles presented below.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	6 of 45
Policy Title:	State of Delaware Information Security Policy		

Data Steward

A Data Steward is a business unit/departmental manager with the authority for acquiring, creating, and maintaining data within their assigned area of control. The Data Steward must be a State employee with a cleared background check. They are designated by Organization Head to perform this function. However, the Organization Head will bear final responsibility for compliance. The Data Steward is responsible for ensuring that:

- 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](#).
- Appropriate continuity of operations planning efforts exist including a defined State organization liaison to work with authorities.
- COOP planning efforts must be aligned with the appropriate State of Delaware BC/DR criticality recovery requirements.
- Data (or specific application systems) is categorized according to a criticality scale defined by the business unit/department according to the Disaster Recovery/Continuity of Operations Plan (DR/COOP) criticality levels.
- Assets are inventoried and custody is officially assigned.
- User and system administrator access to data is on a need-to-know basis rather than by rank, position, or affiliation-based. Personnel have undergone a prescribed screening process/background check and completed appropriate non-disclosure agreements as relevant to their position and level of access.
- Appropriate privacy regulations are addressed in the classification of data.
- Employees, casual seasonal employees, temporary personnel, contractors, vendors and all State third party associates shall report any violation of this policy to a supervisor/manager, Human Resources, the DTI Chief Security Officer Team, or contracting representative.
- Checks are periodically made to ensure that data continues to be classified appropriately and that safeguards remain valid and operative.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	7 of 45
Policy Title:	State of Delaware Information Security Policy		

- Requesting deviations and clarifications as necessary in accordance with the [Data Classification Policy](#).
- Data Steward can delegate the responsibility of submitting security access requests to specific Data Custodians as needed.

Data Custodian

Data Custodians are individuals responsible for overseeing and implementing the necessary safeguards to protect the data assets at the level classified by the Data Steward. The Data Custodian for a local database could be the same as the Data User, a system administrator, Information Resource Manager (IRM), or Information Security Officer (ISO).

Data Custodians are charged with the provision of information systems services 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, Data Custodians must protect the data in their possession from unauthorized access, alteration, destruction, or usage.

Data Custodians shall operate information systems based on procedures indicated by management direction to ensure the confidentiality, integrity, and availability of data in their care.

A Data Custodian is the person responsible for viewing/amending/updating the content of the data assets. This can be any authorized user of the data. Data Custodians are individuals who have been granted explicit authorization to access, modify, delete, and/or utilize data by the relevant Data Steward.

Data Custodians for all data are identified and responsible for implementing and maintaining requisite security controls prescribed in relevant policies, procedures, guidelines, and standards.

Data Custodians, at the appointment of the Data Steward, can approve security access requests as needed.

Data Custodians must use the information only for the purposes specifically approved by the Data Steward. Data Custodians must also comply with all security measures defined by the Data Steward. Additionally, Data Custodians must refrain from disclosing data in their possession (unless it has been designated as State of Delaware Public) without first obtaining permission from the Data Steward. Data Custodians must, additionally, report to their manager, ISO, or IRM all situations





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	8 of 45
Policy Title:	State of Delaware Information Security Policy		

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

Authorized users who access and use the State's data. This also includes the use of data on an individual's State personal computer and related files shares. A Data user could be an employee, casual seasonal employee, temporary personnel, contractor, or vendor. All Data users must understand and abide by this policy. As well as sign and acknowledge an applicable acceptable use policy declaration to this end.

Changes in Status

Any changes to employment status of personnel must be reported to the organization ISO within two (2) days prior to the last day of employment or the day of employment termination. The ISO must then notify the DTI Chief Security Officer Team or the CSO's designee 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. This notification shall be required for all data that is hosted or co-located at DTI. Data Stewards must maintain access control systems so that previously provided access privileges are no longer provided whenever there has been a Data Custodian status change. When a Data Steward has a change in status, it is the responsibility of the Organization Head to promptly designate a new Data Steward and notify affected parties. This policy applies to all employees, casual seasonal employees, temporary personnel, contractors, vendors, outsourcers, and/or all others who have access to the State's data.

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

State Chief Information Officer

The Chief Information Officer (CIO) in Delaware is an Organization Head and the CIO 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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	9 of 45
Policy Title:	State of Delaware Information Security Policy		

government. The CIO is responsible to establish State of Delaware Information Technology Policy.

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 directs and supports DTI security professionals in the attainment of objectives. The CSO is responsible for developing, communicating, and enforcing the State of Delaware Information Security Policy, and local management is responsible for execution of the policy. This involves the management of the overall Statewide Information Security Program to include logical and physical controls, as well as coordination of efforts between DTI staff and other State organizations. The CSO is responsible for:

- Developing and managing the statewide direction for information security.
- 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 security and COOP education and awareness program.
- Protecting the physical and 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, communicating, 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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	10 of 45
Policy Title:	State of Delaware Information Security Policy		

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 should be independent of both development and operations staff.

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

- Maintain statewide information security policies, procedures, guidelines, and standards.
- Communicate information security policies to the general user population.
- Assist State organizations in developing and implementing their own disaster recovery and continuity of operation plans.
- Periodically test information security, disaster recovery, and COOP controls.
- Execute appropriate training and awareness programs for information security, disaster recovery, and COOP.
- Perform administration of the information security exception process.
- Participate in the investigation of information security incidents or violations of State security policies and report them to management.
- 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.
- Call upon 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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	11 of 45
Policy Title:	State of Delaware Information Security Policy		

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:

- Inventorying, tracking and classifying department’s data assets.
- Identifying authorized users for each document type, file, and report.
- Conducting regular risk assessments of sensitive data.
- Communicating to the DTI CSO Team on security-related issues.
- Investigating and reporting security violations.
- Conducting periodic reviews to ensure compliance with security standards and policies.
- Initiating incident reporting or issues of non-compliance to the organization head and to DTI.
- Preparing and submitting security reports to the organization head and to DTI.

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. They could formally delegate completing these tasks and activities, although overall accountability cannot be delegated. Key responsibilities include the following:

- Ensuring that information risk is assessed monitored and managed in compliance with regulatory requirements and Policies and Standards for Information Security.
- Ensuring that an asset inventory is maintained and that there is clear ownership of the major information assets in their organization.
- Ensuring that regular reporting occurs on the status of information security across the organization.
- Ensuring that information security requirements for services provided from outside providers are defined, implemented, maintained and supported with appropriate agreements.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	12 of 45
Policy Title:	State of Delaware Information Security Policy		

All Staff

All staff, of whatever level and in whatever role, will have specific personal responsibilities for information security. These should be included in local policies and procedures, and incorporated into the staff orientation process. All staff has responsibility for the following:

- Complying with the State of Delaware Information Security policies, procedures and standards to maintain the confidentiality, integrity and availability of State data.
- Activities associated with assigned accounts, as well as assigned equipment and removable media.
- Protecting the secrecy of their passwords.
- Participating in risk assessment processes as requested.
- Reporting known or suspected security incidents.
- Participate in information security awareness training.

Asset Inventory and Data Classification

Related ISO 27002:2005 clause(s): **7.1.1, 7.2.1**

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

All assets should be clearly documented in a single repository and updated at least two (2) times per year. The inventory shall include the type of asset, format, steward of the asset, Information Security Officer, data classification, DR criticality level, location, backup information, license information, and a business value.

Data shall be broken into four (4) sensitivity classifications with separate handling requirements (State of Delaware Top Secret, State of Delaware Secret, State of Delaware Confidential, and State of Delaware Public). This State-established standard of data sensitivity classification system shall be used throughout the State enterprise. These classifications are defined in the [Data Classification Policy](#). Caveats exist in that these categorizations are State-derived and are not aligned with similar classifications for National Security Information (NSI). Care shall be taken to





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	13 of 45
Policy Title:	State of Delaware Information Security Policy		

ensure that NSI is not mistaken for State-derived information and, consequently, not afforded inappropriate safeguards in storage and transmission.

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

Related ISO 27002:2005 clause(s): **7.2.1**

Production systems shall be characterized based on a Business Impact Analysis each with separate handling requirements. This criticality classification system shall be used statewide, and shall form an integral part of the system contingency planning process.

Critical (1)

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

Significant (2)

Loss of business function significantly reduces the effectiveness of the State's operations. Loss of business function 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. Loss of business function 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. Loss of this business function has little or no effect on the State's ability to carry out business.

Minimal (5)

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

Policy Maintenance

Related ISO 27002:2005 clause(s): **5.1.2, 15.1.1**

Periodic Policy Review and Evaluation

The State of Delaware Information Security Policy is subject to 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. For more information, see the [Establishment and Promulgation of DTI Enterprise Policies, Procedures, Standards and Best Practices Guidelines Policy](#).





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	14 of 45
Policy Title:	State of Delaware Information Security Policy		

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

Exception Process

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

Consequences and Disciplinary Action

Related ISO 27002:2005 clause(s): **8.2.3**

Failure to comply with the policy is a serious matter, whether through intentional act or negligence, and may be grounds for discipline up to and including dismissal based on the just cause standard set forth by Merit Rules, or collective bargaining agreement, whichever is applicable to the subject employee. Exempt employees shall be subject to appropriate discipline without recourse, except as provided by law. While DTI has no authority to discipline employees 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 27002:2005 clause(s): **7.1.3, 8.1.3, 8.2.1, 13.1.1, 13.1.2**

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. 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 may be accessed by authorized DTI employees 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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	15 of 45
Policy Title:	State of Delaware Information Security Policy		

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 shall be reported to the Organization’s ISO within four (4) business days.

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 thought to be a threat to State infrastructure must be 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.

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 27002:2005 clause(s): **6.2.3, 8.1.2**

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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	16 of 45
Policy Title:	State of Delaware Information Security Policy		

A criminal background check consists of providing fingerprints for a full State Bureau of Identification (SBI) and Federal Bureau of Investigation (FBI) check. 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 may be 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 may be 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 can be performed. See [DTI Security Clearance Policy](#).

The Organization ISO is responsible for ensuring compliance with the criminal background check requirement for its users and employees and the affected Organizations are responsible for processing these checks through the State Bureau of Identification (SBI) and responsible for the costs associated with these checks. With respect to IT contractors, IT vendors and other IT third-party service providers requiring a criminal background check, Organizations reserve the right to require vendors, contractors and third-party providers to assume responsibility for the costs associated with processing criminal background checks.

Information collected will be 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 27002:2005 clause(s): **11.1.1, 11.5.1**

Access to all information must be authorized by the Data Steward on a need-to-know basis.



“Enabling Excellence In Delaware State Government”



Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	17 of 45
Policy Title:	State of Delaware Information Security Policy		

All business applications or systems must be secured by an access control system compliant with approved standards.

It is strongly recommended that all Internet facing business applications or systems use the State's enterprise identity access management solution for authentication.

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

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

Unique User Access Credentials

Related ISO 27002:2005 clause(s): **11.2.1, 11.5.2**

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 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 may not 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 approved security access request.

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 shall be 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.

Password Management

Related ISO 27002:2005 clause(s): **11.2.3, 11.5.3**

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	18 of 45
Policy Title:	State of Delaware Information Security Policy		

User IDs and passwords (access credentials) for new users must be distributed in a secure manner. User credentials shall not be sent by email unless it is encrypted. Initial passwords shall be set up in a way so non-authorized individuals cannot gain access. Initial passwords shall require changing on initial login and after requesting a password reset.

Passwords shall conform to guidelines presented in the [Strong Password Standard](#) documentation.

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

For additional information, consult the [Strong Password Standard](#).

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 27002:2005 clause(s): **11.3.2, 11.3.3**

Data Custodians 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 27002:2005 clause(s): **11.5.1**

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	19 of 45
Policy Title:	State of Delaware Information Security Policy		

After a specified number of consecutive authentication failures, users shall be 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 shall be reviewed by a data custodian within a 24-hour period.

Disabling Inactive Accounts

Related ISO 27002:2005 clause(s): **8.3.3**

User accounts that have not been used for at least ninety (90) days shall be disabled.

Accounts on all platforms will be 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 will be sent to the Organization ISOs by DTI. Accounts that are dormant over ninety (90) calendar days shall be 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 shall be conducted at least twice per year for usage and activity. Stale accounts (accounts that have not been logged into for over ninety (90) days) shall be evaluated and if appropriate deleted by the Agency's AD Organizational Unit (OU) manager. If required, the mail associated with this account can be transferred to an agency appointed person by submitting an [eRecords Request Form](#) to the DTI Executive Branch. An "Out of Office" response can be configured for a period of two (2) weeks prior to deleting the account for notification purposes. AD policies are in place to automatically purge the associated mailbox thirty (30) days after the AD account has been deleted.

The organization ISO shall follow DTI's policies, standards, and directives to exercise sound judgment through the life cycle of accounts. The organization ISOs are required to monitor and maintain control over the accounts he/she requests for approval, creation, modification, and deletion on all State platforms. All activities related to accounts will be submitted through the current process.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	20 of 45
Policy Title:	State of Delaware Information Security Policy		

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

Review of System Access

Related ISO 27002:2005 clause(s): **11.2.4**

System access and privileges are to be 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 27002:2005 clause(s): **11.2.2**

Profiles must be 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 DTI CSO Team is available to provide additional guidance.

Terminations and Transfers

Related ISO 27002:2005 clause(s): **8.3.1, 8.3.2, 8.3.3**

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 have been 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 27002:2005 clause(s): **10.1.3**

No person shall be responsible for completing a task involving non-public, valuable, or critical information from beginning to end of said process in order to achieve a segregation of duties. Likewise, a single person must not be responsible for approving his or her own work. To the extent possible, at least two (2) people must





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	21 of 45
Policy Title:	State of Delaware Information Security Policy		

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 be permitted to modify production data, production programs, or the operating system.

Segregation of Production and Test

Related ISO 27002:2005 clause(s): **10.1.4**

Production, development, and test environments shall be kept strictly separate (computer systems or separate directories or libraries), with strictly enforced access controls. See [System Environments Standard](#).

Change Control

Related ISO 27002:2005 clause(s): **10.1.2, 12.1.1, 12.4, 12.5**

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 27002:2005 clause(s): **10.7.4, 10.1.1**

System documentation is a necessary part of the State's information system management. Such documentation must be 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 27002:2005 clause(s): **8.2.2, 6.1.7**

DTI provides regular information security awareness communications to all staff, including contractors, by various means, such as webcasts, briefings, newsletters, advisories, etc. in direct support of the ISOs and IRMs, and System Administrators. Furthermore, DTI embraces its responsibility to assist managers and ISO personnel in conducting relevant training for their users and their involvement with relevant industry special interest groups.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	22 of 45
Policy Title:	State of Delaware Information Security Policy		

Protection from Malicious Software

Related ISO 27002:2005 clause(s): **10.4**

All computing resources must be current with operating system and software security patches and virus protection software before connecting to the network, and be configured to stay current as new patches are released. More guidance can be located within the [Generally Available Software Policy](#)

All computing resources must run State standard virus protection software. The virus protection software must not be disabled or altered in a manner that shall reduce the effectiveness of the software. The software's virus definitions must be kept current.

For users who access the network from home or other remote locations, the [VPN policy](#) provides further instruction.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Organization ISO. (See Security Incident Procedures, below.) More guidance can be located within [Virus Protection Standard](#) documentation.

Security Incident Procedures

Related ISO 27002:2005 clause(s): **13.2**

All information security breaches must be reported without delay to the relevant ISO and the DTI Chief Security Officer Team. Prompt reporting will speed the identification of any damage caused, effect any restoration and repair, prevent further contamination, and facilitate the gathering of any associated evidence.

The ISO shall follow pre-defined incident response procedures. Incidents shall 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.

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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	23 of 45
Policy Title:	State of Delaware Information Security Policy		

Data Backup Plan

Related ISO 27002:2005 clause(s): **10.5, 9.2.5, 6.2.3**

A backup of the organization's data files and the ability to recover such data is a top priority. Organizations local management must assess the business process by the supported data and/or systems and assign a Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The backup of the associated media must correlate to the RPO/RTO. The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements, such as Delaware Public Records Law (29 Delaware Code §501-526) and the Delaware Freedom of Information Act (29 Delaware Code Ch. 100 *et seq.*). The archiving of electronic data should be consistent with the Delaware Public Records Law's requirements for records retention and disposition schedules, and use the procedures of the Delaware Public Archives (DPA) for authorizing records disposition.

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved. Data backups on removable media must be encrypted for State of Delaware confidential, secret and top secret data. Furthermore, State of Delaware confidential, secret and top secret data may only reside at rest on State owned or DTI approved systems or devices.

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

The vendor(s) providing offsite backup storage for State data must be cleared to handle the highest level of information stored. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest State sensitivity levels for information stored.

Storage media protection and authentication controls at the storage system and media levels can provide strong barriers against unauthorized stored data disclosure, theft, and corruption.

Backup media shall be stored in a locked, fireproof container (UL-rated for media protection) during transport and while being retained at a pre-determined offsite location, far enough away in the event of a localized disaster (tornado, fire, etc.).





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	24 of 45
Policy Title:	State of Delaware Information Security Policy		

A process must be implemented to verify the success of the electronic information backup. Backups must be periodically tested to ensure that they are recoverable within the expected timeframe. Testing helps to identify if:

- Backups are incomplete.
- Backup software was wrongly configured.
- Encryption has caused a lockout (unknown password).
- Backup can only be read by an earlier version of your software.
- Backup cannot perform the restore from backup media which is several months old.
- Dormant backup software bugs now plague your newly upgraded operating system.
- The tape breaks during backup process.
- Unexplained reboots could have caused a system crash and tape rewind during the backup process.

Signing Authorities held by the offsite backup storage vendor(s) for access to State backup media must be reviewed annually or when an authorized individual leaves or changes job responsibilities.

Procedures between organization and the offsite backup storage vendor(s) must be reviewed at least annually.

Backup tapes and/or containers must be readily identified by labels and/or a bar-coding system.

Disaster Recovery Plan and Testing

Related ISO 27002:2005 clause(s): **14.1.2, 14.1.3, 14.1.5**

Data Stewards must evaluate, by using a risk assessment model, prepare, periodically update, and regularly test a disaster recovery plan that shall allow all designated critical computer and communication systems to be available in the event of a major loss, such as a flood, earthquake, or tornado, on a predefined priority basis.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	25 of 45
Policy Title:	State of Delaware Information Security Policy		

Continuity of Operations Planning

Related ISO 27002:2005 clause(s): **14.1**

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 shall be 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 be able to be performed as normal. A disaster declaration enacts IT and business recovery plans coordinated by the Disaster Management Team. Emergency Response and Disaster Declaration stand-downs shall be 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 shall be executed to assure minimum disruption. All COOP plans must be reviewed and updated to include, but not be limited to, employee contact information at least once every two years. However, it is highly recommended that plans be updated as change occurs within the organization.

Third-Party Business Contracts

Related ISO 27002:2005 clause(s): **6.2, 10.2, 10.8**

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 should 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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	26 of 45
Policy Title:	State of Delaware Information Security Policy		

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 27002:2005 clause(s): **15.1.2**

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

Third-party copyrighted information or software that the organization or district does not have specific approval to store and/or use must not be 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 can be 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 should be noted, but not be 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 can be found in the [Acceptable Use Policy](#) and [Generally Available 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



"Enabling Excellence In Delaware State Government"



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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	27 of 45
Policy Title:	State of Delaware Information Security Policy		

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 can be held accountable for any breaches of security or confidentiality resulting from their use of the State Internet connection.

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

Only voice including VOIP solutions owned and managed by the State are permitted for use on the State network. 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 shall not be used to communicate confidential and/or sensitive information unless they are configured to include security features with encryption.
3. Only State internal contacts shall be loaded in your contact list or "buddy list".
4. Be aware that IM messages are no different than other electronic communication and can be monitored, retrieved and archived. The same privacy principles described on page 14 (privacy section) of this policy apply.
5. Keep messages simple and to the point.
6. Contact names should be 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 shall be taken when speaking on any type of voice device whether inside or outside of department facilities, so that others cannot overhear conversations of a sensitive nature.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	28 of 45
Policy Title:	State of Delaware Information Security Policy		

Wireless and Mobile LAN Computing

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

- [Wireless 802.11 Architecture Standard](#)
- [Acceptable Use Policy](#)
- [Data Classification Policy](#)

Technical Safeguards

Transmission Security

Related ISO 27002:2005 clause(s): **10.8, 10.9**

All electronic data transmitted shall 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 shall be appropriately secured over electronic communications networks in accordance with the [Data Classification Policy](#) and all applicable published standards.

Integrity Controls

Related ISO 27002:2005 clause(s): **12.2**

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 must be notified of these facts each time they are presented with the involved information.

Cryptography

Related ISO 27002:2005 clause(s): **15.1.6**

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	29 of 45
Policy Title:	State of Delaware Information Security Policy		

In addition to following the cryptography and encryption policies contained herein, organizations should 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 27002:2005 clause(s): **12.3**

To protect the confidentiality, authenticity or integrity of information, cryptographic techniques shall be 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 27002:2005 clause(s): **12.3.1, 12.3.2**

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 must be encrypted at the file level where practical.

Encryption shall be applied to protect the confidentiality of information and shall follow the rules outlined in the [Data Classification Policy](#) and [Secure File Transport](#) and [Secure Email Standard](#) and [Mobile Device Encryption Standard](#).

Encryption keys, encryption procedures, and encryption software must not be disclosed to anyone that does not need to know.

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

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

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

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	30 of 45
Policy Title:	State of Delaware Information Security Policy		

Technical Cryptography Policy Statements

Related ISO 27002:2005 clause(s): **12.3.1**

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 not be 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. See [VPN Policy](#).

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.

Cryptography Key Management

Related ISO 27002:2005 clause(s): **12.3.2**

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

Secret encryption keys, if approved (see [Secure File Transport](#)), used for file encryption must be 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 must not be stored in an insecure manner.

Approved Encryption Techniques

Approved algorithms and standards shall be established through DTI published standards.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	31 of 45
Policy Title:	State of Delaware Information Security Policy		

Monitoring

Related ISO 27002:2005 clause(s): **10.10**

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 shall be 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 shall be synchronized on a regular basis, and audit logs must be protected as classified information.

Intrusion Detection

Related ISO 27002:2005 clause(s): **10.10.1, 10.6**

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

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

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

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

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

Audit logs for servers and hosts on the internal, protected network must be 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 shall be used to check systems on a routine basis.

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	32 of 45
Policy Title:	State of Delaware Information Security Policy		

All suspected and/or confirmed instances of successful and/or attempted intrusions must be 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 shall be retained for a period of time in accordance with current document retention schedule(s).

Server Hardening

Related ISO 27002:2005 clause(s): **12.6, 15.2.2, 11.4.4, 11.5.4**

All servers must be 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 must be 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 [Server OS Standard](#).
- Host based firewall for servers.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	33 of 45
Policy Title:	State of Delaware Information Security Policy		

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.

Patch Management

Related ISO 27002:2005 clause(s): **12.6, 15.2.2, 10.1.2**

Security patches must be implemented via change control within a specified timeframe of notification of available patches as defined by organization management. Patches must be tested appropriately prior to implementation.

Security Reviews

Related ISO 27002:2005 clause(s): **6.1.8, 15.2.2, 15.3**

Independent Baseline Security Reviews, Vulnerability Testing, and Penetration Testing shall be periodically completed to determine the minimum set of controls required to reduce and maintain risk at an acceptable level. Furthermore, audit tools and results must be safeguarded to prevent any possible misuse or compromise. Audit findings must be reported to organization management for mitigation and corrective actions.

Network Security

Related ISO 27002:2005 clause(s): **11.4**

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 may not be 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 shall be required to comply with the authentication and authorization policy, the [Remote Access Standard](#) and the [VPN Policy](#).

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	34 of 45
Policy Title:	State of Delaware Information Security Policy		

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.

Equipment and System Setup and Configuration

Related ISO 27002:2005 clause(s): **10.1.1**

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

Remote Access

Related ISO 27002:2005 clause(s): **11.7**

All remote access to the State network shall be in accordance with the [Remote Access Standard](#), the [Remote Access Policy](#), the [VPN Policy](#), and the [Acceptable Use Policy](#).

Firewalls

Related ISO 27002:2005 clause(s): **10.6.1, 11.4**

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 must be 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 must only be used by the appropriate well known service.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	35 of 45
Policy Title:	State of Delaware Information Security Policy		

Internal Network Addresses and Designs

Related ISO 27002:2005 clause(s): **10.6, 11.4**

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

Software Development and Intellectual Property

Related ISO 27002:2005 clause(s): **6.2.3, 15.1.2, 12.4, 8.1.2**

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 have been evaluated and have been purchased from reputable sources, testing the source code to ensure the source code is harmless.

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

Special attention shall be given to input validation on web-based applications. Careful input validation is a vital step to prevent malicious users from attacking applications. Applications shall make use of centralized logging and log analysis which includes failed and successful authentication attempts, administrative changes, error messages, and exception handling.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	36 of 45
Policy Title:	State of Delaware Information Security Policy		

Vulnerability scans and/or penetration tests shall be performed on systems before they are connected to the network and on a regular schedule thereafter.

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 27002:2005 clause(s): **12.5.5**

All outsourced software development shall follow the same policy as shown above. In addition, the source code ownership, licensing arrangements, and quality assurance processes shall 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 27002:2005 clause(s): **10.3, 6.1.4**

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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	37 of 45
Policy Title:	State of Delaware Information Security Policy		

Physical Safeguards

Facility Access Control

Related ISO 27002:2005 clause(s): **8.3.3, 9.1.1, 9.1.2, 9.1.3, 9.2.4, 10.10.2, 11.1.1, 11.2.4, 15.1.5**

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 shall be documented and managed.

All data center facilities must be physically protected in proportion to the criticality of the business functions and associated systems, assets and infrastructure. See the [Data Classification Policy](#), the [Data Center Policy](#), and the [DTI Physical Security Policy](#).

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

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

Any Data Center must use appropriate tracking process and procedures to track visitor access.

Keycard access records and visitor logs for the Data Center must be kept for routine review.

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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	38 of 45
Policy Title:	State of Delaware Information Security Policy		

Visitors shall be 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 on a regular basis 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) shall be maintained.

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

Workstation & Computing Resource Access

Related ISO 27002:2005 clause(s): **9.2.1, 11.1.1, 11.3, 11.5.5, 11.7, 15.1.5, 9.1.5**

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 must be 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. User 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 must be hardened when used or connected to the network. They should be configured to harden the network protocols used, management services, processing services (print, copy, fax, and scan), logging, and physical security. Care shall be 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](#)





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	39 of 45
Policy Title:	State of Delaware Information Security Policy		

[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, Blackberry, iPod, etc.) that is not owned by the State cannot be connected from an internal source (inside the firewall) to the State's network. By not allowing such an event, it eliminates unnecessary risk to the State's network via an unauthorized internal source. This action of not allowing personally owned electronic equipment 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 27002:2005 clause(s): **9.1.4, 9.2, 9.1.6**

Data Stewards must ensure that computer resources and facilities are afforded appropriate security and protection from environmental threats. Considerations for resource security extend to supporting infrastructure, such as utilities and cabling, to ensure the availability of information.

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

Special care should be 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 [Data Center Policy](#), and the [DTI Physical Security Policy](#).

Disposal of Electronic Storage Media

Related ISO 27002:2005 clause(s): **9.2.6, 10.7.2**

Whenever any State-owned or leased computing resource is released from use, State information and/or software must be 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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	40 of 45
Policy Title:	State of Delaware Information Security Policy		

Electronic information storage devices (hard drives, tapes, diskettes, compact disks, USB, multifunction peripherals, etc.) shall be 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.

For further information, consult the [Disposal of Electronic Equipment and Storage Media Policy](#) and the [Non-Disclosure Policy](#).

Hard Copy Information Handling

Related ISO 27002:2005 clause(s): **15.1.3, 15.1.4, 7.2.2**

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

Hard copies containing State non-public information classified per the [Data Classification Policy](#) shall be 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 must be 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 shall be 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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	41 of 45
Policy Title:	State of Delaware Information Security Policy		

Photography Controls

Related ISO 27002:2005 clause(s): **9, 11.3.3, 11.7**

Cameras and camera-equipped mobile devices are generally allowed in State facilities. Data Stewards have the authority to restrict certain areas from photography or the presence of camera and recording-equipped resources. Organization management shall restrict the use of photography within Data Centers, except of course for the purpose of physical security surveillance. Any exception requires the express consent of the Organization ISO. Vendors and contractors may be asked not to bring camera-equipped devices into facilities. Any media or prints containing images of facilities shall be considered State of Delaware Secret unless released by the Organization ISO or executive management.

II. Definitions

Availability

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

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.¹

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),

¹ "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:	1
Document Type:	Enterprise Policy	Page:	42 of 45
Policy Title:	State of Delaware Information Security Policy		

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.

Criminal Background Check

This consists of providing fingerprints for a full State Bureau of Identification (SBI) and Federal Bureau of Investigation (FBI) check.

Data Custodian

Data Custodians are individuals responsible for overseeing and implementing the necessary safeguards to protect the information assets at the level classified by the Data Steward.

Data Owner

Data in use by State of Delaware Organizations, in transit through, or residing within the computing infrastructure shall be considered State property and owned and controlled by the State of Delaware.

Data Steward

Data Stewards are business unit/departmental managers with the authority for acquiring, creating, and maintaining information within their assigned area of control.

Data User

Data User is an individual who accesses and uses the State's data.

Display

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





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	43 of 45
Policy Title:	State of Delaware Information Security Policy		

Document

Document pertains to any kind of file that can be read on a computer screen as if it were a printed page, including HTML files read in an Internet browser; any file meant to be 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.

DTI Technical Team(s)

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

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.

Graphics

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

Information Resource Manager (IRM)

Information Resource Managers are organization IT managers or administrators.

Information Security Officer (ISO)

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

Integrity

Integrity is assurance that information is authentic and complete. Ensuring that information can be relied upon to be 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 can be 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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	44 of 45
Policy Title:	State of Delaware Information Security Policy		

Intellectual Property

Intellectual property is information that can be 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.

Recovery Point Objective (RPO)

The recovery point objective (RPO) is an important consideration in disaster recovery planning. It represents the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a failure.

Recovery Time Objective (RTO)

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

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 must be 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.





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

Doc Ref Number:	SE-ESP-001	Revision Number:	1
Document Type:	Enterprise Policy	Page:	45 of 45
Policy Title:	State of Delaware Information Security Policy		

Sanitization

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

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 are 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

Initial version established February 1, 2007.

Revised version published December 5, 2008.

IV. Approval Signature Block

Name & Title: Cabinet Secretary - State Chief Information Officer	Date

V. Listing of Appendices

None.

