INFORMATION SECURITY PLAN GUIDELINES

Introduction

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

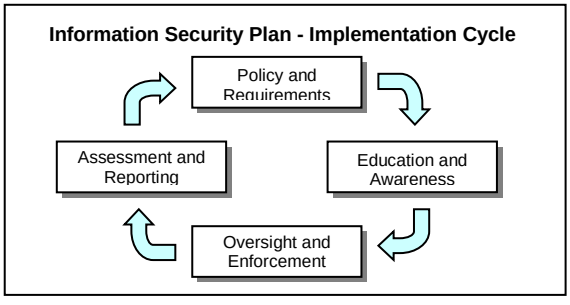
Information security is the protection of information from a wide range of threats in order to ensure business continuity, ensure privacy of information, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

The statewide Information Security policy (#107-004-052, effective date 7/30/2007) directs each agency to establish a plan to initiate and control the implementation of information security within the agency and manage risk associated with information assets. The plan will include:

- Processes to:
  - Identify agency information assets;
  - Determine information sensitivity;
  - Determine the appropriate levels of protection for that information;
- Applicable state directives and legal regulatory requirements;
- Identification of roles and responsibilities for information security within the agency;
- Identification of user security awareness and training elements; and,
- Information security policies that govern agency information security activities.

DAS adopted the ISO/IEC 27002:2005 international standard to guide creation of information security policy in state government. Agencies can use the ISO/IEC 27002 standard to identify best practices that will assist them in meeting the overall intent of information security. A summary of the ISO clauses and controls starts on page 13 of this guide.

Implementing an information security plan is not a one-time event. It is an ongoing cycle of identifying policy and requirements, training users, enforcing compliance, and assessing results.



This guide is offered as a tool to assist state agencies as they develop their information security plans. It ties together statewide information security policies, tools and resources created to assist in implementing various policies, ISO/IEC 27002 clauses, identification of appropriate roles and responsibilities, and best practices guidelines. Not all the elements identified in this guide will be applicable to all state agencies. An agency should develop a plan that supports its mission and business goals while considering the information assets it holds, their value to the organization, and the steps necessary to protect the information commensurate with its value.

Information Security Plan Requirements, Guidelines and Best Practices

The following elements are required by the statewide Information Security policy. Agencies are required to address these elements in their information security plans. The tables below detail policy requirements and offer guidance and best practice statements for each category. These lists are not intended to be all-inclusive. Agencies should apply the items presented and other elements available to them in a way that implements information security and manages risk while best meeting the business needs of the agency.

1. Processes to Identify Agency Information Assets	**Required**	**Guidance**	**Best Practice**
Establish processes to identify agency information assets	✓		
Where information is identified, consider legislation, regulations, policy compliance, and/or contractual obligations that affect the management of the information.	✓		
All information assets will have identified information owners established within the agency's lines of business.	✓		
Also see other applicable statewide policies: • Information Asset Classification, 107-004-050 (http://oregon.gov/DAS/OP/docs/policy/state/107-004-050_013108.pdf)	✓		
Information assets come in many forms, including but not limited to: • Paper • Electronic • Digital • Images • Voice mail		✓	
Examples of information assets include, but are not limited to: • Employee-related information including employee records, job applications, and records of interview; • Procurement records such as RFP specifications, evaluation of proposals, contracts, pricing details, and performance reports; • Agency information such as policies, strategic plans, correspondence, legal advice, financial and audit reports, system documentation, user manuals, training material, operational and support procedures, business continuity plans, system architecture drawings, and risk analyses; • Client information including service level agreements, service contracts, and client contact records; and • Customer information including personal identity information collected to issue licenses or certifications, report income, and track education credits.		✓	
Information owner questions: • What is the information? • Where is the information used? • When is the information needed and not needed? • Why is the information needed?		✓	

• How is the information used?			
In order to facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to group like information together. It is important to ensure that the grouping of information assets for classification is appropriate. A broad grouping may result in applying controls unnecessarily as the asset must be classified at the highest level necessitated by its individual data elements. A narrow grouping allows for more precise targeting of controls; however, as there are more information assets to classify, this increases the complexity of the classification and the management of controls.			✓
Where practical, leverage other business initiatives such as business continuity/disaster recovery planning, implementation of enterprise policies and initiatives, and implementation of new lines of business, and incorporate information asset identification, classification and handling methodologies to protect newly identified information assets.			✓
See ISO clause 7.1			✓

2. Processes to Determine Information Sensitivity	**Required**	**Guidance**	**Best Practice**
Establish processes to determine information sensitivity	✓		
Once information assets are identified, conduct an impact assessment on the value of the asset to the organization and any risks associated with its disclosure. Include in the assessment any known legislation, regulations, policy compliance, and contractual obligations affecting the management or use of the information.	✓		
Published classification is low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients and partners. This includes information regularly made available to the public via electronic, verbal or hard copy media. Examples: • Press releases • Brochures • Pamphlets • Public access Web pages • Materials created for public consumption	✓		
Limited classification is sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, and/or partners. Each agency shall follow its disclosure policies and procedures before providing this information to external parties. Examples: • Enterprise risk management planning documents • Published internal audit reports • Names and addresses that are not protected from disclosure	✓		
Restricted classification is sensitive information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties. External parties requesting this information for authorized agency business must	✓		

be under contractual obligation of confidentiality with the agency (for example, confidential/non-disclosure agreement) prior to receiving it. Examples: • Network diagrams • Personally identifiable information • Other information exempt from public records disclosure			
Critical classification is information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners or cause major harm to the agency. Examples: • Regulated information with significant penalties for disclosure, such as information covered under HIPAA or IRS regulations • Information that is typically exempt from public disclosure	✓		
Also see other applicable statewide policies: • Information Asset Classification, 107-004-050 (http://oregon.gov/DAS/OP/docs/policy/state/107-004-050_013108.pdf)	✓		
Information assets should be classified according to business need and findings from the risk assessment. Business needs vary and similar information assets may be classified differently from agency to agency. One agency may classify their network diagrams as Level 3 – Restricted and another agency may classify their network diagrams as Level 2 – Limited based on the level of detail and the business need.		✓	
Information should be classified by the information owner or delegate at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset. Consideration must be given to stakeholders, users, and consumers of the information with regard to accessibility and business process changes that may adversely affect their respective business processes or consumer needs.			✓
Identifying risks means recognizing scenarios where threats may affect assets. This involves considering threats in terms of the impact on assets, assets in terms of their vulnerabilities and threats to them, and security objectives relevant to assets. • Risks should be initially identified as if there were no security measures in place; this is the inherent risk. Understanding an inherent risk facilitates risk management throughout the life of the system. • Risks should be explored to understand their causes, the extent of affected information assets, and possible consequences. • Identified risks should be expressed in the form of a triplet: Cause → Event → Consequences. Consequences should be expressed in a manner that reveals the affected security objectives. • Risks should be classified according to their business consequences. For examples of risk assessment tools, see http://oregon.gov/DAS/EISPD/ESO/IACCoP/RiskAssmtTool.doc and http://oregon.gov/DAS/EISPD/ESO/IACCoP/ThreatsConcerns.doc.			✓
See ISO clauses 6.2, 7.2.1			✓

3. Processes to Determine Appropriate Levels of Protection for Information	Required	Guidance	Best Practice
Establish processes to determine appropriate levels of protection for information	✓		
Also see other applicable statewide policies: • Information Asset Classification, 107-004-050 (http://oregon.gov/DAS/OP/docs/policy/state/107-004-050_013108.pdf) • Controlling Portable and Removable Storage Devices, 107-004-051 (http://oregon.gov/DAS/OP/docs/policy/state/107-004-051.pdf) • Transporting Information Assets, 107-004-100 (http://oregon.gov/DAS/OP/docs/policy/state/107-004-100_013108.pdf)	✓		
For an example of tips for handling classified information, see http://oregon.gov/DAS/EISPD/ESO/IACCoP/IACMatrix.doc			✓
For best practices related to safeguarding information, see http://oregon.gov/DAS/EISPD/ESO/IDTheft/Safeguard_bestpractices.pdf			✓
See ISO clauses 7.1.3, 7.2.2, 9.1, 9.2, 10.4, 10.7, 11.6			✓

4. Applicable Directives, Legal and Regulatory Requirements	Required	Guidance	Best Practice
Identify directives and legal and regulatory requirements affecting the agency	✓		
Regulations to consider: • Health Insurance Portability and Accountability Act (HIPAA) • Equal Employment Opportunity Act (EEOA) • Family Educational Rights and Privacy Act (FERPA) • Payment Card Industry (PCI) • Oregon Identity Theft Protection Act		✓	
See ISO clauses 15.1, 15.2			✓

5. Identification of Information Security Roles and Responsibilities	Required	Guidance	Best Practice
Identify roles and responsibilities for information security within the agency	✓		
Agency Director – Responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. Also responsible for ensuring compliance with state enterprise security policies, standards, and security initiatives, and with state and federal regulations.	✓		
Information Security Officer – Manages the agency information security program. Oversees compliance with policies and procedures regarding the security of information assets.	✓		
Information Owner – An individual or groups of individuals responsible to: • Create an initial information classification, including assigning classification levels to all data; • Approve decisions regarding controls, access privileges of users, and	✓		

ongoing decisions regarding information management; • Ensure the information will be regularly reviewed for value and controls updated to manage risks due to new threats, vulnerabilities, or changes in the environment; • Perform periodic reclassification based on business impact analysis, changing business priorities and/or new laws, regulations and security standards; • Follow state archive documentation retention rules regarding proper disposition of all information assets.			
Users – Responsible for complying with the provisions of policies, procedures and practices.	✓		
Incident Response Point of Contact – Responsible for communicating with State Incident Response Team and coordinating agency actions in response to an information security incident.		✓	
See ISO clauses 6.1, 7.1.2, 11.3, 13.1			✓

6. Identification of User Awareness and Training Elements	**Required**	**Guidance**	**Best Practice**
Identify user security awareness and training elements	✓		
Also see other applicable statewide policies: • Employee Security, 107-004-053 (http://oregon.gov/DAS/OP/docs/policy/state/107-004-053.pdf)	✓		

In response to a gap analysis conducted in 2006, a multi-agency workgroup identified several information security awareness topics that have been developed into on-line training modules available to all government agencies. While agencies are not required to use this content, they do meet the requirements of information security training as established in the statewide Employee Security policy. The modules are currently available at the state intranet. Contact the Enterprise Security Office for access to the source programs.
• IS101 – Introduction
  ○ What is Information Security
  ○ Basic Principles
  ○ Policies, Standards and Procedures
• IS201 – Securing Your Computer – Part 1
  ○ Computer Viruses
  ○ Spyware
• IS202 – Securing Your Computer – Part 2
  ○ Choosing Strong Passwords
  ○ Protecting Your Passwords
  ○ Safe Use of the Internet
  ○ Physically Secure Your Computer
• IS203 – Using E-Mail
  ○ Introduction
  ○ E-Mail Content and Etiquette
		✓	

○ Keeping Your E-Mail Private ○ E-Mail from Other People • IS204 – Dealing with Documents ○ Basic Document Security ○ Requests for Information ○ Retaining Documents ○ Destroying Documents • IS205 – When You're Out of the Office ○ Introduction ○ General Guidelines ○ Laptop Computers ○ USB Flash Drives ○ Cell Phones			
Employees should be tested on their understanding of the content of training sessions.			✓
Employees should go through annual refresher courses on information security basics and applicable policies and procedures.			✓
See ISO clause 8.2.2			✓

7. Information Security Policies That Govern Information Security Activities	**Required**	**Guidance**	**Best Practice**
Identify information security policies that govern agency information security activities	✓		
Matrix – See matrix of statewide information security policies and their requirements (starting on page 8).	✓		
See ISO clauses 5.1, 15.1, 15.2			✓

Statute and Rule Requirements

Oregon Revised Statute 182.122

	Enterprise Security Office	State Data Center	Agency
Information Systems Security			
Plans, standards, policies, procedures	Develop enterprise information security plans, standards, and policies.	Information systems security for state network and systems under SDC control. Develop plans, standards, policies, and procedures.	
Review/verify security of information systems	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessments of systems security under SDC control.	Conduct self assessments, third party assessments, or assessments using ESO staff.
Monitor network traffic		Monitor state network traffic.	
Identify and react to threats		Mitigate threats, work with agencies and ESO to address vulnerabilities.	
Conduct vulnerability assessments	Conduct security assessments using ESO staff or third parties.	Information systems security for state network and systems under SDC control.	Conduct self assessments, third party assessments, or assessments using ESO staff.
Incident Response			
Policies	Develop enterprise level policies.		Develop agency policies.
Respond to events	Respond through SIRT or at the request of SDC or agency.	Respond for state network and systems under SDC control and at the request of ESO or agency.	Respond if capable, or request SDC or ESO assistance.
Alert appropriate parties	Through SIRT.	Advise ESO and agencies of issues identified through monitoring.	Advise ESO of incidents.
Implement forensic techniques	Trained staff, procedures, and forensics lab.		Develop capability or request ESO assistance.
Evaluate event; lessons learned	Document through SIRT or ESO working with agency.	Document work in conjunction with ESO and agency.	Work in conjunction with ESO and SDC.

	Enterprise Security Office	State Data Center	Agency
Communicate; track trends	Track/trend incidents and communicate to agencies.		
Remedial Action	Work with agencies and provide recommendations; review agency follow-up actions.	Implement remedial action and report back to the ESO.	Implement remedial action and report back to the ESO.
Agencies			
Security of computers, hardware, software, storage media, networks, operations procedures and processes outside the control of the SDC.			Agencies are responsible for information security and security of their systems, applications, desktops, LANs, etc.
Follow enterprise policies, standards, and procedures			Develop and implement policies, procedures based on enterprise policies.
Report results of any assessments, evaluations, or audits.		Provide assessment and audit results to the ESO.	Provide assessment and audit results to the ESO.

Oregon Administrative Rule 125-800-005 through 125-800-0020

	Enterprise Security Office	State Data Center	Agency
State Information Security			
Protect shared computing and network infrastructure		Information systems security for state network and systems under SDC control. Monitor state network traffic. Mitigate threats, work with agencies and the ESO to address vulnerabilities.	Protect agency systems, applications, desktops, LANs, etc.

	Enterprise Security Office	State Data Center	Agency
Leadership	Direct and coordinate all enterprise information security activities.		Develop and implement information security activities based on enterprise direction.
Policies and architecture	Develop enterprise level policies and architecture.	Develop architecture for SDC controlled systems.	Develop agency policies.
Conduct vulnerability assessments	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessment of the state network and systems under SDC control.	Conduct security assessments using ESO staff, third parties, or self assessments.
Manage information systems	Develop enterprise policies and provide consultation on systems management.	Develop enterprise systems and management standards.	Develop and implement policies and procedures based on enterprise policies.
Awareness and training	Develop information security awareness and training tools.		
Reporting	Track/trend information security.		
Performance management	Identify and measure information security performance measures.		
Compliance	Conduct compliance reviews using ESO staff or third party.		Conduct compliance reviews using ESO staff, third party, or through self assessments.
Evaluation	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessment of the state network and systems under SDC control.	Conduct security assessments using ESO staff, third parties, or self assessments.
Collaboration		Work with other governmental jurisdictions within Oregon for appropriate cost sharing.	

	Enterprise Security Office	State Data Center	Agency
Agency			
Information security			Chief executive is responsible for agency's information security. Develop and implement policies and procedures based on enterprise policies. Designate an agency security liaison. Develop and implement information security activities based on enterprise direction.
Plans and standards	Develop standards for security plans. Review and approve agency security plans.		Develop a security plan based on the enterprise standards. Submit security plan to ESO for certification and revise security plans to meet certification requirements.
Security Assessments			
Conduct vulnerability assessments	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessment of the state network and systems under SDC control.	Conduct security assessments using ESO staff, third parties, or self assessments.
Identify and react to threats		Mitigate threats, work with agencies and ESO to address vulnerabilities.	Mitigate threats, work with SDC and ESO to address vulnerabilities.
Report results of any assessments, evaluations, or audits		Provide assessment and audit results to the ESO.	Provide assessment and audit results to the ESO.
Incident Response			
Policies	Develop enterprise level policies.		Develop agency policies.
Respond to events	Respond through SIRT or at the request of SDC or agency.	Respond for state network and systems under SDC control and at the request of ESO or agency.	Respond if capable or request SDC or ESO assistance.

	Enterprise Security Office	State Data Center	Agency
Alert appropriate parties	Through SIRT.	Advise ESO and agencies of issues identified through monitoring.	Advise ESO of incidents.
Implement forensic techniques	Trained staff, procedures, and forensic lab.		Develop capability or request ESO assistance.
Evaluate event, lessons learned	Document through SIRT or ESO working with agency.	Document work in conjunction with ESO and agency.	Work in conjunction with ESO and SDC.
Communication, track trends	Track, identify trends of incidents and communicate to agencies.		
Remedial actions	Work with agencies and provide recommendations; review agency follow-up actions.	Take remedial action as appropriate and report back to the ESO.	Implement remedial action and report back to the ESO.

Statewide Policy Summary Matrix

Policy No.	Subject	Agency Policy	Agency Procedures / Processes	Agency Plan	Information Classification	Designate Information Owner	Apply Information Protection	Assess Risk	Monitoring / Tracking	Training
107-004-110	Acceptable Use of State Information Assets	✓	✓						✓	
107-004-051	Controlling Portable and Removable Storage Devices	✓	✓				✓		✓	
107-004-053	Employee Security	✓	✓							✓
107-004-050	Information Asset Classification			✓	✓	✓	✓	✓	✓	
107-004-052	Information Security	✓	✓	✓			✓	✓		✓
107-004-100	Transporting Information Assets			✓	✓		✓	✓	✓	

Policy No.	Subject	Effective Date	Compliance Date
107-004-110	Acceptable Use of State Information Assets	10/16/2007	n/a
Purpose: To inform authorized users of state agency information assets of the appropriate and acceptable use of information, computer systems and devices.			
Requirements: Any use of information, computer systems and devices will comply with the policy. Agencies will put in place policies, procedures and practices that enable compliance, deter misuse, and detect policy violations. Users of state information assets are responsible for complying with the provisions of the policy and agency-promulgated supporting policies, procedures and practices.			

Agencies will monitor use of information systems and assets. Agencies will, at a minimum, monitor on a random basis and for cause.

Monitoring systems or processes will be used to create usage reports and resulting reports will be reviewed by agency management for compliance.

See policy for specific restrictions and areas of discretionary use.

☒ **Agency Policy** ☒ **Agency Procedures/Processes** ☐ **Agency Plan** ☐ **Information Classification** ☐ **Training**
☐ **Designated Information Owner** ☐ **Application of Information Protection** ☐ **Risk Assessment** ☒ **Monitoring / Tracking**

Policy No.	Subject	Effective Date	Compliance Date
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007	7/30/2008

Purpose: To ensure the confidentiality, integrity, and availability of state information assets stored on portable or removable storage devices.

Requirements: Each agency will physically control and protect portable and removable storage devices, and protect and manage any sensitive information stored on them.

Agencies will adopt policy and procedures identifying types of approved devices, govern use of personally-owned devices, and establish methods for tracking the devices.

Agencies will adopt policy and procedures identifying what agency information assets may or may not be stored on portable or removable devices and approved methods for securing that information, as needed, appropriate to the information's sensitivity.

☒ **Agency Policy** ☒ **Agency Procedures/Processes** ☐ **Agency Plan** ☐ **Information Classification** ☐ **Training**
☐ **Designated Information Owner** ☒ **Application of Information Protection** ☐ **Risk Assessment** ☒ **Monitoring / Tracking**

Policy No.	Subject	Effective Date	Compliance Date
107-004-053	Employee Security	7/30/2007	1/31/2008

Purpose: To protect information assets and reduce the risk of human error and misuse of enterprise information and equipment.

Requirements: Each agency will develop and enforce a policy that:

- Requires pre-employment screening of employees commensurate with the value and risk of the information assets they will have access to;
- Establishes accountability and responsibility to all employees having access to the agency's information assets;
- Establishes processes for timely removal of all permissions for employees having access to information assets and return of agency

assets at termination or reassignment; and

- Establishes user awareness training for employees.

☒ **Agency Policy** ☒ **Agency Procedures/Processes** ☐ **Agency Plan** ☐ **Information Classification** ☒ **Training**
☐ **Designated Information Owner** ☐ **Application of Information Protection** ☐ **Risk Assessment** ☐ **Monitoring / Tracking**

Policy No.	Subject	Effective Date	Compliance Date
107-004-050	Information Asset Classification	1/31/2008	6/30/2009 12/31/2009 7/30/2010

Purpose: To ensure State of Oregon information assets are identified, properly classified, and protected throughout their lifecycles.

Requirements: All state agency information will be classified and managed based on its confidentiality, sensitivity, value and availability requirements.

Each agency will identify and classify its information assets.

Proper levels of protection will be implemented to protect assets relative to the classification.

All information will have an information owner or owners established within the agency's line of business. Information owners are responsible to:

- Create an initial information classification, including assigning classification levels to all data;
- Approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management;
- Ensure the information will be regularly reviewed for value and updated to manage changes to risk due to new threats, vulnerabilities, or changes in the environment;
- Perform periodic reclassification based on business impact analysis, changing business priorities and/or new laws, regulations and security standards;
- Follow state archive document retention rules regarding proper disposition of all information assets.

Each agency will identify its information assets for the purpose of defining its value, criticality, sensitivity and legal importance.

Agencies will use the classification schema included in the policy to differentiate between various levels of sensitivity and value:

- Level 1 – Published
- Level 2 – Limited

- Level 3 – Restricted
- Level 4 – Critical

Each information asset will have a range of controls, designed to provide the appropriate level of protection of the information commensurate with the value of the information in that classification.

Agencies will properly identify and protect information meeting the definitions, requirements and effective dates outlined in the Oregon Consumer Identity Theft Protection Act (Senate Bill 583, 2007 Legislative Session) as they relate to personal information.

Agencies will develop a plan for identifying, classifying and protecting information assets no later than 6/30/2009.

All Level 4 – Critical information assets will be identified and protected no later than 12/31/2009.

Agencies will comply with all other provisions of the policy, including identification, classification and protection of all information assets, by 6/30/2010.

☐ **Agency Policy** ☐ **Agency Procedures/Processes** ☒ **Agency Plan** ☒ **Information Classification** ☐ **Training**
☒ **Designated Information Owner** ☒ **Application of Information Protection** ☒ **Risk Assessment** ☒ **Monitoring / Tracking**

Policy No.	Subject	Effective Date	Compliance Date
107-004-052	Information Security	7/30/2007	7/30/2009

Purpose: To emphasize the state's commitment to information security and provide direction and support for information security in accordance with business requirements and relevant laws and regulations. Names state standard to guide policy development.

Requirements: Each agency will develop and implement information security plans, policies and procedures that protect its information assets from the time of creation, through useful life and through proper disposal.

Each State Agency Head is responsible for information security in his/her agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. Each State Agency Head also is responsible for ensuring his/her agency's compliance with state enterprise security policies, standards, and security initiatives, and with state and federal security regulations.

All agency employees are responsible for protecting the confidentiality, integrity and availability of the agency's information assets.

Each agency will establish a plan to initiate and control the implementation of information security within the agency and manage risk associated with information assets. The plan will include:

- Processes to:
  - Identify agency information assets;
  - Determine information sensitivity;
  - Determine the appropriate levels of protection for that information;

- Applicable state directives and legal and regulatory requirements;
- Identification of roles and responsibilities for information security within the agency;
- Identification of user security awareness and training elements; and,
- Information security policies that govern agency information security activities.

Each agency will ensure that new business needs and risks are reflects in its information security plans and policies.

Agency information security plans, policies, standards and procedures will be reviewed and revised, as needed, by the agency no less frequently than every five years.

☒ **Agency Policy** ☒ **Agency Procedures/Processes** ☒ **Agency Plan** ☐ **Information Classification** ☒ **Training**
☐ **Designated Information Owner** ☒ **Application of Information Protection** ☒ **Risk Assessment** ☐ **Monitoring / Tracking**

Policy No.	Subject	Effective Date	Compliance Date
107-004-100	Transporting Information Assets	1/31/2008	n/a

Purpose: To ensure the security of state information assets when in transit.

Requirements: Each agency must use appropriate security controls for transportation of sensitive information assets (physical media – e.g. tape, disk, paper) during transit and beyond the physical boundaries of a facility from loss, destruction or unauthorized access.

Each agency that sends, receives or transports confidential or sensitive information to or from another facility or agency/entity is responsible to assure that the information is protected appropriately during transit.

The determination of the sensitivity level of an asset is governed by the statewide Information Asset Classification policy, in which it is the responsibility of the information owner to identify sensitive information and ensure appropriate protection.

☐ **Agency Policy** ☐ **Agency Procedures/Processes** ☒ **Agency Plan** ☒ **Information Classification** ☐ **Training**
☐ **Designated Information Owner** ☒ **Application of Information Protection** ☒ **Risk Assessment** ☒ **Monitoring / Tracking**

Information Security Control Objectives and Controls

These control objectives and controls are derived from and aligned with those listed in the ISO/IEC 27002:2005 code of practice for information security management (© ISO/IEC 2005) and the ISO/IEC 27001:2005(© ISO/IEC 2005) information management systems requirements, the recognized state standards for information security. The numbers cited align with clauses 5 to 15 of the 27002 standard. These objectives and controls are offered as best practices for information security. This is not an exhaustive list and agencies may determine additional control objectives and controls are necessary. ISO/IEC 27002:2005 provides implementation advice and guidance on best practices in support of the controls listed here. (Contact the DAS Enterprise Security Office for access to the ISO/IEC 27002:2005 and ISO/IEC 27001:2005 standards documents.)

5. Security policy	
5.1 Information Security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	
5.1.1 Information security policy document	*Control:* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
5.1.2 Review of the information security policy	*Control:* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

6. Organization of information security	
6.1 Internal organization *Objective:* To manage information security within the organization.	
6.1.1 Management commitment to information security	*Control:* Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
6.1.2 Information security coordination	*Control:* Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.
6.1.3 Allocation of information security responsibilities	*Control:* All information security responsibilities shall be clearly defined.

6.1.4 Authorization process for information processing facilities	*Control:* A management authorization process for new information processing facilities shall be defined and implemented.
6.1.5 Confidentiality agreements	*Control:* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
6.1.6 Contact with authorities	*Control:* Appropriate contacts with relevant authorities shall be maintained.
6.1.7 Contact with special interest groups	*Control:* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
6.1.8 Independent review of information security	*Control:* The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
6.2 External parties *Objective:* To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties	
6.2.1 Identification of risks related to external parties	*Control:* The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
6.2.2 Addressing security when dealing with customers	*Control:* All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
6.2.3 Addressing security in third party agreements	*Control:* Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

7. Asset management	
7.1 Responsibility for assets *Objective:* To achieve and maintain appropriate protection of organizational assets.	
7.1.1 Inventory of assets	*Control:* All assets shall be clearly identified and an inventory of all important assets

	drawn up and maintained.
7.1.2 Ownership of assets	*Control:* All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organization. The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset.
7.1.3 Acceptable use of assets	*Control:* Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
7.2 Information classification *Objective:* To ensure that information receives an appropriate level of protection.	
7.2.1 Classification guidelines	*Control:* Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
7.2.2 Information labeling and handling	*Control:* An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.

8. Human resources security	
8.1 Prior to employment *Objective:* To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.	
8.1.1 Roles and responsibilities	*Control:* Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.
8.1.2 Screening	*Control:* Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
8.1.3 Terms and conditions of employment	*Control:* As part of their contractual obligation, employees, contractors and third party

	users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
8.2 During employment *Objective:* To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.	
8.2.1 Management responsibilities	*Control:* Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
8.2.2 Information security awareness, education and training	*Control:* All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
8.2.3 Disciplinary process	*Control:* There shall be a formal disciplinary process for employees who have committed a breach of security
8.3 Termination or change of employment *Objective:* To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.	
8.3.1 Termination responsibilities	*Control:* Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
8.3.2 Return of assets	*Control:* All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
8.3.3 Removal of access rights	*Control:* The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

9. Physical and environmental security	
9.1 Secure areas *Objective:* To prevent unauthorized physical access, damage and interference to the organization's premises and information.	
9.1.1 Physical security perimeter	*Control:* Security perimeters (barriers such as walls, card controlled entry gates or

	manned reception desks) shall be used to protect areas that contain information and information processing facilities.
9.1.2 Physical entry controls	*Control:* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
9.1.3 Securing offices, rooms and facilities	*Control:* Physical security for offices, rooms, and facilities shall be designed and applied.
9.1.4 Protecting against external and environmental threats	*Control:* Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
9.1.5 Working in secure areas	*Control:* Physical protection and guidelines for working in secure areas shall be designed and applied.
9.1.5 Public access, delivery and loading areas	*Control:* Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
9.2 Equipment security *Objective:* To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.	
9.2.1 Equipment siting and protection	*Control:* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
9.2.2 Supporting utilities	*Control:* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
9.2.3 Cabling security	*Control:* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
9.2.4 Equipment maintenance	*Control:* Equipment shall be correctly maintained to ensure its continued availability and integrity.
9.2.5 Security of equipment off-premises	*Control:* Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
9.2.6 Secure disposal or re-use of equipment	*Control:* All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

9.2.7 Removal of property	*Control:* Equipment, information or software shall not be taken off-site without prior authorization.

10. Communications and operations management	
10.1 Operational procedures and responsibilities *Objective:* To ensure the correct and secure operation of information processing facilities.	
10.1.1 Documented operating procedures	*Control:* Operating procedures shall be documented, maintained, and made available to all users who need them.
10.1.2 Change management	*Control:* Changes to information processing facilities and systems shall be controlled.
10.1.3 Segregation of duties	*Control:* Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
10.1.4 Separation of development, test and operational facilities	*Control:* Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.
10.2 Third party service delivery management *Objective:* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.	
10.2.1 Service delivery	*Control:* It shall be ensured that the security controls, service definitions and delivery levels included in third party service delivery agreements are implemented, operated, and maintained by the third party.
10.2.2 Monitoring and review of third party services	*Control:* The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
10.2.3 Managing changes to third party services	*Control:* Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
10.3 System planning and acceptance *Objective:* To minimize the risk of systems failure.	
10.3.1 Capacity management	*Control:* The use of resources shall be monitored, tuned, and projections made of

	future capacity requirements to ensure the required system performance.
10.3.2 System acceptance	*Control:* Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
10.4 Protection against malicious and mobile code *Objective:* To protect the integrity of software and information.	
10.4.1 Controls against malicious code	*Control:* Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
10.4.2 Controls against mobile code	*Control:* Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
10.5 Back-up *Objective:* To maintain the integrity and availability of information and information processing facilities.	
10.5.1 Information back-up	*Control:* Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.
10.6 Network security management *Objective:* To ensure the protection of information in networks and the protection of the supporting infrastructure.	
10.6.1 Network control	*Control:* Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
10.6.2 Security of network services	*Control:* Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
10.7 Media handling *Objective:* To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.	
10.7.1 Management of removable media	*Control:* There shall be procedures in place for the management of removable media.
10.7.2 Disposal of media	*Control:* Media shall be disposed of securely and safely when no longer required, using formal procedures.
10.7.3 Information handling procedures	*Control:* Procedures for the handling and storage of information shall be established to

	protect this information from unauthorized disclosure or misuse.
10.7.4 Security of system documentation	*Control:* System documentation shall be protected against unauthorized access.
10.8 Exchange of information *Objective:* To maintain the security of information and software exchanged within an organization and with any external entity.	
10.8.1 Information exchange policies and procedures	*Control:* Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
10.8.2 Exchange agreements	*Control:* Agreements shall be established for the exchange of information and software between the organization and external parties.
10.8.3 Physical media in transit	*Control:* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
10.8.4 Electronic messaging	*Control:* Information involved in electronic messaging shall be appropriately protected.
10.8.5 Business information systems	*Control:* Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
10.9 Electronic commerce activities *Objective:* To ensure the security of electronic commerce services and their secure use.	
10.9.1 Electronic commerce	*Control:* Information in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
10.9.2 On-line transactions	*Control:* Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
10.9.3 Publicly available information	*Control:* The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
10.10 Monitoring *Objective:* To detect unauthorized information processing activities.	
10.10.1 Audit logging	*Control:* Audit logs recording user activities, exceptions, and information security

	events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
10.10.2 Monitoring system use	*Control:* Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
10.10.3 Protection of log information	*Control:* Logging facilities and log information shall be protected against tampering and unauthorized access.
10.10.4 Administrator and operator logs	*Control:* System administrator and system operator activities shall be logged.
10.10.5 Fault logging	*Control:* Faults shall be logged, analyzed, and appropriate action taken.
10.10.6 Clock synchronization	*Control:* The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

11. Access control	
11.1 Business requirement for access control *Objective:* To control access to information.	
11.1.1 Access control policy	*Control:* An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
11.2 User access management *Objective:* To ensure authorized user access and to prevent unauthorized access to information systems.	
11.2.1 User registration	*Control:* There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
11.2.2 Privilege management	*Control:* The allocation and use of privileges shall be restricted and controlled.
11.2.3 User password management	*Control:* The allocation of passwords shall be controlled through a formal management process.
11.2.4 Review of user access rights	*Control:* Management shall review users' access rights at regular intervals using a formal process.
11.3 User responsibilities	

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.	
11.3.1 Password use	*Control:* Users shall be required to follow good security practices in the selection and use of passwords.
11.3.2 Unattended user equipment	*Control:* Users shall ensure that unattended equipment has appropriate protection.
11.3.3 Clear desk and clear screen policy	*Control:* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
11.4 Network access control *Objective:* To prevent unauthorized access to network services.	
11.4.1 Policy on use of network services	*Control:* Users shall only be provided with access to the services that they have been specifically authorized to use.
11.4.2 User authentication for external connections	*Control:* Appropriate authentication methods shall be used to control access by remote users.
11.4.3 Equipment identification in networks	*Control:* Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
11.4.4 Remote diagnostic and configuration port protection	*Control:* Physical and logical access to diagnostic and configuration ports shall be controlled.
11.4.5 Segregation in networks	*Control:* Groups of information services, users, and information systems shall be segregated on networks.
11.4.6 Network connection control	*Control:* For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with access control policy and requirements of the business applications.
11.4.7 Network routing control	*Control:* Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
11.5 Operating system access control *Objective:* To prevent unauthorized access to operating systems.	
11.5.1 Secure log-on procedures	*Control:* Access to operating systems shall be controlled by a secure log-on procedure.
11.5.2 User identification and authentication	*Control:* All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed

	identity of a user.
11.5.3 Password management system	*Control:* Systems for managing passwords shall be interactive and shall ensure quality passwords.
11.5.4 Use of system utilities	*Control:* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
11.5.5 Session time-out	*Control:* Inactive sessions shall shut down after a defined period of inactivity.
11.5.6 Limitation of connection time	*Control:* Restrictions on connection times shall be used to provide additional security for high-risk applications.
11.6 Application and information access control *Objective:* To prevent unauthorized access to information held in application systems.	
11.6.1 Information access restriction	*Control:* Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
11.6.2 Sensitive system isolation	*Control:* Sensitive systems shall have a dedicated (isolated) computing environment.
11.7 Mobile computing and teleworking *Objective:* To ensure information security when using mobile computing and teleworking facilities.	
11.7.1 Mobile computing and communications	*Control:* A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risk of using mobile computing and communication facilities.
11.7.2 Teleworking	*Control:* A policy, operational plans and procedures shall be developed and implemented for teleworking activities.

12. Information systems acquisition, development and maintenance	
12.1 Security requirements of information systems *Objective:* To ensure that security is an integral part of information systems.	
12.1.1 Security requirements analysis and specification	*Control:* Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

12.2 Correct processing in applications *Objective:* To prevent errors, loss, unauthorized modification or misuse of information in applications.	
12.2.1 Input data validation	*Control:* Data input to applications shall be validated to ensure that the data is correct and appropriate.
12.2.2 Control of internal processing	*Control:* Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
12.2.3 Message integrity	*Control:* Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
12.2.4 Output data validation	*Control:* Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
12.3 Cryptographic controls *Objective:* To protect the confidentiality, authenticity or integrity of information by cryptographic means.	
12.3.1 Policy on the use of cryptographic controls	*Control:* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
12.3.2 Key management	*Control:* Key management shall be in place to support the organization's use of cryptographic techniques.
12.4 Security of system files *Objective:* To ensure the security of system files.	
12.4.1 Control of operational software	*Control:* There shall be procedures in place to control the installation of software on operational systems.
12.4.2 Protection of system test data	*Control:* Test data shall be selected carefully, and protected and controlled.
12.4.3 Access control to program source code	*Control:* Access to program source code shall be restricted.
12.5 Security in development and support processes *Objective:* To maintain the security of application system software and information.	
12.5.1 Change control procedures	*Control:* The implementation of changes shall be controlled by the use of formal change control procedures.
12.5.2 Technical review of applications after operating system changes	*Control:* When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations

	or security.
12.5.3 Restrictions on changes to software packages	*Control:* Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
12.5.4 Information leakage	*Control:* Opportunities for information leakage shall be prevented.
12.5.5 Outsourced software development	*Control:* Outsourced software development shall be supervised and monitored by the organization.
12.6 Technical vulnerability management *Objective:* To reduce risks resulting from exploitation of published technical vulnerabilities.	
12.6.1 Control of technical vulnerabilities	*Control:* Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

13. Information security incident management	
13.1 Reporting information security events and weaknesses *Objective:* To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	
13.1.1 Reporting information security events	*Control:* Information security events shall be reported through appropriate management channels as quickly as possible.
13.1.2 Reporting security weaknesses	*Control:* All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
13.2 Management of information security incidents and improvements *Objective:* To ensure a consistent and effective approach is applied to the management of information security incidents.	
13.2.1 Responsibilities and procedures	*Control:* Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
13.2.2 Learning from information security incidents	*Control:* There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
13.2.3 Collection of evidence	*Control:* Where a follow-up action against a person or organization after an

	information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

14. Business continuity management	
14.1 Information security aspects of business continuity management *Objective:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.	
14.1.1 Including information security in the business continuity management process	*Control:* A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
14.1.2 Business continuity and risk assessment	*Control:* Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
14.1.3 Developing and implementing continuity plans including information security	*Control:* Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
14.1.4 Business continuity planning framework	*Control:* A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
14.1.5 Testing, maintaining and reassessing business continuity plans	*Control:* Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

15. Compliance	
15.1 Compliance with legal requirements *Objective:* To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.	
15.1.1 Identification of applicable legislation	*Control:* All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined,

	documented, and kept up to date for each information system and the organization.
15.1.2 Intellectual property rights	*Control:* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
15.1.3 Protection of organizational records	*Control:* Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
15.1.4 Data protection and privacy of personal information	*Control:* Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
15.1.5 Prevention of misuse of information processing facilities	*Control:* Users shall be deterred from using information processing facilities for unauthorized purposes.
15.1.6 Regulation of cryptographic controls	*Control:* Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
15.2 Compliance with security policies and standards, and technical compliance *Objective:* To ensure compliance of systems with organizational security policies and standards.	
15.2.1 Compliance with security policies and standards	*Control:* Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
15.2.2 Technical compliance checking	*Control:* Information systems shall be regularly checked for compliance with security implementation standards.
15.3 Information systems audit considerations *Objective:* To maximize the effectiveness of and to minimize interference to/from the information systems audit process.	
15.3.1 Information systems audit controls	*Control:* Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
15.3.2 Protection of information systems audit tools	*Control:* Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.