Overarching Enterprise Information Security Policy

Table of Contents

1. OVERVIEW

It is the policy of the State of Illinois Department of Innovation & Technology (DoIT) to (i) support the business missions, goals, and objectives of the Governor and DoIT's client agencies, boards, and commissions, (ii) reduce the risk posed to the State of Illinois due to the loss, disruption, or corruption of information and Information Systems, and (iii) comply with applicable state, federal, and industry laws, rules, and regulations related to information security. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary. Any reference to "Agency" herein shall include both DoIT and Client Agencies.

2. PURPOSE

The Secretary of DoIT is committed to securing State of Illinois information, Information Systems, and technology assets. The Secretary has issued this State of Illinois Enterprise Information Security Policy and its corresponding policies, standards, procedures, and guidelines to prevent or limit the adverse effects of a failure, interruption, or security breach of State of Illinois Information Systems. This Policy is intended to focus on the core concepts of confidentiality, integrity, availability, and system resiliency.

This Policy and its subordinate policies and standards define the minimum-security controls that must be implemented for State of Illinois Information Systems. This Policy further establishes parameters and boundaries regarding the acceptable use of information and information technology assets.

Those who use, acquire, implement, and manage State of Illinois Information Systems must comply with this Policy. Individuals responsible for the implementation of Information Systems, including third parties, must address the security controls of this Policy and corresponding standards and procedures.

Executive Order 2016-01 created DoIT in recognition that thousands of state systems are redundant, outdated, and vulnerable to cyberattacks that place the private information of Illinois employees, residents, consumers, and businesses at risk. Public Act 100-0611, which codifies Executive Order 2016-01 and establishes DoIT by law, directs DoIT to (i) develop and implement data security policies and procedures that ensure the security of data that is confidential, sensitive, or protected from disclosure by privacy or other laws, and (ii) ensure compliance with applicable federal and state laws pertaining to information technology, data, and records of DoIT and the State of Illinois agencies, boards, and commissions that DoIT serves and that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

The Secretary of DoIT has established an information security program to address the requirements of Executive Order 2016-01 and Public Act 100-0611, to ensure a continued and deliberate effort to reduce the risk posed to the State by external cyberattacks, insider threats, and other incidents, and to ensure compliance with applicable state, federal, and industry laws, rules, and regulations. Focusing on the core information security concepts of confidentiality, integrity, availability, and system resiliency, the State of Illinois Overarching Enterprise Information Security Policy is established to help ensure that the risk posed to the State of Illinois due to the loss, disruption, or corruption of information is managed within acceptable limits.

3. SCOPE

The State of Illinois Overarching Enterprise Information Security Policy requires statewide compliance and applies to all State of Illinois agencies, boards, commissions, trusted partners, and information technology service providers that utilize State of Illinois information networks and information technology resources (IT Resources). This Policy applies to all Users and Employees, including contractors and third-party entities, of DoIT and its Client Agencies.

4. FRAMEWORK

To secure the State of Illinois enterprise information technology environment, DoIT has selected the information and cyber security frameworks published by the National Institute of Standards and Technology (NIST) as the foundation for the State of Illinois Overarching Enterprise Information Security Policy. The NIST Framework for Improving Critical Infrastructure Cybersecurity and NIST Special Publication 800-53, Assessing Security and Privacy Controls for Federal Systems and Organizations provide information security controls.

5. APPLICABLE LAWS, RULES, AND REGULATIONS

This Policy seeks to ensure compliance with applicable state and federal laws, rules, and regulations as well as to comply with industry-specific guidelines. The following non-exhaustive list of laws, rules, and regulations are applicable to the State of Illinois and are critical drivers to this Policy.

- Illinois Freedom of Information Act (5 ILCS 140)
- Illinois Identity Protection Act (5 ILCS 179)
- Illinois Personal Information Protection Act (815 ILCS 530)
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Federal Bureau of Investigations Criminal Justice Information Services (CJIS) Security Policy
- Federal Centers for Medicare & Medicaid Services (CMS) MARS-E Document Suite
- Federal Centers for Medicare & Medicaid Services Information Security Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements
- Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
- Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems
- Federal Internal Revenue Service (IRS) Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies
- Federal Information Security Modernization Act of 2014, which amends the Federal Information Security Management Act of 2002 (FISMA)
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law No.104-231, 110 Stat. 3048, Electronic Freedom of Information Act
- Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999
- Health Insurance Portability and Accountability Act (P.L. 104-191)
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy

Controls for Federal Information Systems and Organizations
- Payment Card Industry (PCI) Data Security Standard (DSS)
- Privacy Act of 1974 (P.L. 93-579)
- State Officials and Employees Ethics Act (5 ILCS 430)

6. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security establishes supplemental policies, standards, procedures, and guidelines and designates responsibility to specific personnel. To the extent necessary, each Client Agency and/or DoIT Division must establish procedures in order to achieve Policy compliance. It is the responsibility of Users to understand and adhere to this Policy.

Failure to comply with this Policy may result in the Chief Information Security Officer temporarily discontinuing or suspending the operation of the Information System, solution, and/or resource until such compliance is established as deemed solely by the Chief Information Security Officer. Failure to comply with this Policy could also result in the loss of access to State of Illinois IT Resources and/or discipline, up to and including discharge.

7. EXCEPTIONS TO POLICY

The State of Illinois Overarching Enterprise Information Security Policy establishes the security baseline for the State. Policy exceptions can adversely impact this baseline and increase information security risk. Some exceptions to this Policy and to related information security policies are inevitable due to ever-changing business and technology environments.

The acceptance of information security risk is not an information technology issue but is a business and public safety issue. Decisions to implement an Information System will be made by the executive level of State of Illinois government, and those decisions should be risk-informed.

If the head of an Agency determines that compliance with the provisions of this Policy or any related information security policies or standards would adversely impact the business of the Agency or the State, the head of the Agency should request approval to deviate from a specific requirement by submitting an exception request to the Chief Information Security Officer.

Each request shall be in writing to the Chief Information Security Officer and approved by the head of the Agency. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. Requests for exceptions shall be evaluated, discussed with the Agency, and decided by the Chief Information Security Officer. Should an information security policy exception be granted, the applicable Agency head will acknowledge the acceptance of the risk posed due to the policy exception. Denied exception requests may be appealed to the Secretary of DoIT.

8. INFORMATION SECURITY CONTROLS

Any data that is originated, entered, processed, transmitted, stored, or destroyed by or for the State of Illinois

shall be subject to the State of Illinois enterprise information security controls. These security controls must be implemented to protect information at the State of Illinois from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure the confidentiality, integrity, and availability of State of Illinois information. All State of Illinois Employees, trusted partners, or entities authorized to access, store, or transmit information at the State of Illinois shall protect the confidentiality, integrity, and availability of the information as set forth in this Policy and all State of Illinois information security policies. Information is not limited to data in computer systems and is included regardless of where it resides in an Agency, what form it takes, which technology is used to handle it, or which purposes itserves.

9. INFORMATION SECURITY POLICIES

The following State of Illinois information security policies are established based on NIST controls. State of Illinois agencies, boards, commissions, trusted partners, and third-party providers are bound to each policy. The policies establish the standards and procedures to effectively implement corresponding State of Illinois controls and establish an information security baseline for the State.

Enterprise security standards and procedures will be periodically reviewed and updated by DoIT. Policies will be reviewed by DoIT every three years, or more frequently when significant changes to the environment warrant an update.

Acceptable Use

The Acceptable Use Policy requires that all State of Illinois Users, contractors, and third parties understand the acceptable use of state information and Information Systems and the consequences of not adhering to the Acceptable Use Policy. The Acceptable Use Policy ensures that State of Illinois Authorizing Officials and all other associated personnel understand and communicate to Users the need for acceptable use of information assets to reduce the risks to Agency Information Systems due to disclosure, modification, or disruption, whether intentional or accidental.

Access Control

The Access Control Policy requires automated security controls, authorized access and use of Information Systems, special and limited access conditions, physical and automated process monitoring, and authorized system account activities by approved personnel. The Access Control Policy ensures that State of Illinois Authorizing Officials and all other associated personnel understand the responsibilities, access management requirements, and separation of duties necessary to effectively manage Information System accounts and coordinate, plan, and execute appropriate physical and account access control activities.

Security Awareness and Training

The Security Awareness and Training Policy requires role-specific training on security controls, authorized access and use of Information Systems, physical and automated process monitoring, and authorized system activities and functions by approved personnel. The Security Awareness and Training Policy ensures that State of Illinois Authorizing Officials and all other associated personnel understand their responsibilities and training requirements necessary to reduce internal and external threats and prevent additional security-related

incidents.

Audit and Accountability

The Audit and Accountability Policy requires approved personnel to audit essential information, manage audit service devices and locations, integrate audit events, manage audit repositories, and process and generate audit reports. The Audit and Accountability Policy ensures that State of Illinois Authorizing Officials with auditing responsibilities understand the responsibilities required to successfully manage audit information, assign audit roles and tasks, and prevent the compromise of State of Illinois information.

Security Assessment and Authorization

The Security Assessment and Authorization Policy requires approved Agency personnel to conduct impartial security assessments, establish external system restrictions, and conduct penetration testing and other necessary vulnerability assessments. The Security Assessment and Authorization Policy ensures that State of Illinois Authorizing Officials and all other applicable personnel understand the responsibilities necessary to establish effective security assessment and authorization controls, prevent conflicts of interest, and maintain continuous monitoring strategies.

Configuration Management

The Configuration Management Policy requires approved Agency personnel to adequately manage the configuration of State of Illinois systems, including retaining previous system configurations, configuring approved devices for high-risk areas, tracking and documenting system changes, and assigning privileges to authorized personnel. The Configuration Management Policy ensures that State of Illinois Authorizing Officials and Information System support personnel understand the responsibilities necessary to maintain up-to-date system configuration, support rollbacks and system change requirements, and prevent unauthorized system changes, including software and program installs.

Contingency Planning

The Contingency Planning Policy requires approved Agency personnel to coordinate contingency plans with existing contingency development, designate key resumption activities, define service-level priorities, and define critical assets and offsite backup sites, including telecommunications, transaction systems, and operational separation measures. These standards ensure that State of Illinois Authorizing Officials and personnel responsible for contingency planning understand the responsibilities necessary to prevent conflicts with other contingency elements, effectively resume essential operations during and after a disruption, prevent loss or compromise of assets, and provide alternate methods to secure, store, and access State of Illinois information.

Identification and Authentication

The Identification and Authentication Policy requires approved Agency personnel to manage network systems that employ multifactor and public key information (PKI)-based authentication, replay-resistant mechanisms, identification of connected devices, and registration process requirements. The Identification and Authentication Policy ensures that State of Illinois Authorizing Officials and third parties understand the

responsibilities necessary to regulate non-privileged access of State of Illinois accounts, minimize authentication attacks, and prevent unauthorized devices and connections with State of Illinois networks.

Incident Response

The Incident Response Policy requires approved Agency personnel to apply incident response capabilities, including automated response and reporting processes, establish a test process for those incident response capabilities, and coordinate with existing State of Illinois contingency plans. The Incident Response Policy ensures that State of Illinois Authorizing Officials and all other associated personnel understand the responsibilities necessary to ensure that the State of Illinois' incident response capability (i) is effective, (ii) prevents conflicts with other contingency elements, and (iii) relies on automated system response, reporting, and support.

Maintenance Policy

The Maintenance Policy requires approved Agency personnel to employ adequate and approved information maintenance tools, inspect all maintenance tools entering State of Illinois facilities (including supporting media), and apply priority or time-sensitive maintenance procedures. The Maintenance Policy ensures that State of Illinois Authorizing Officials and personnel assigned to information technology maintenance-related activities understand the responsibilities necessary to effectively diagnose and repair State of Illinois Information Systems, ensure maintenance tools and supporting media are not modified beyond the State of Illinois' authorized specifications, and determine the levels of risk and priority for each Information System affected during an incident.

Media Protection

The Media Protection Policy requires all State of Illinois personnel to apply proper Information System media markings on all approved media, devices, and systems property; properly designate and control both physical and digital storage locations; execute approved and secure transport methods; ensure cryptographic protection is applied to required devices; and prohibit the use of unidentifiable devices. This Media Protection Policy ensures that State of Illinois Authorizing Officials and other applicable personnel understand the responsibilities necessary to ensure that all State of Illinois media is adequately used, handled, and distributed and properly protected, stored, and transported, including applying additional security mechanisms and restrictions on the use of unauthorized media devices.

Physical and Environmental Protection

The Physical and Environmental Protection Policy requires definition of both physical facility and Information System management processes. All corresponding personnel will apply and manage security safeguards accordingly for facilities and Information System distribution and transmission lines; control and monitor physical information output devices and locations, including the use of safety, intrusion, and surveillance equipment; and implement appropriate power protection and alternate location practices and measures. The Physical and Environmental Protection Policy ensures that State of Illinois Authorizing Officials and personnel responsible for ensuring physical and environmental protection of information technology facilities and assets understand the responsibilities necessary to prevent unauthorized communication or transmission access.

Security Planning

The Security Planning Policy requires all assigned State of Illinois DoIT personnel to effectively coordinate security-related activities with Agencies and outside entities, provide and enforce social media and network rules and restrictions, and implement an adequate information security architecture. The Security Planning Policy ensures that State of Illinois Authorizing Officials, the Chief Information Security Officer, and other personnel responsible for security planning understand the responsibilities necessary to prevent security conflicts within and throughout the State of Illinois to ensure that a proper security architecture is in place and is continuously assessed.

Personnel Security

The Personnel Security Policy requires the employment of mechanisms to control employee transfers, as well as commencement and termination status, including disabling access for specific Information Systems, designating access levels for specific positions and roles, and conducting personnel screening before granting authorization or access. Furthermore, the Personnel Security Policy governs personnel security for both State of Illinois personnel and third-party providers. The Personnel Security Policy ensures that State of Illinois Authorizing Officials, management, human resources, and personnel assigned to access control functions understand the responsibilities necessary to ensure that (i) appropriate personnel have limited or appropriate access, (ii) changes in personnel status properly control further access or restriction to Information Systems, and (iii) appropriate documentation and processes are followed in order to track corresponding authorization changes and access.

Risk Assessment

The Risk Assessment Policy ensures that State of Illinois Authorizing Officials, management, information security personnel, business owners, and information technology support personnel understand the responsibilities necessary to readily identify and respond to system vulnerabilities. The Risk Assessment Policy requires that Agencies employ appropriate vulnerability scanning tools, maintain accurate updates of scanned vulnerabilities, and remediate legitimate vulnerabilities.

System and Services Acquisition

The System and Services Acquisition Policy requires Agency to apply visually functional security interface controls, controlled levels of systems design and implementation, and appropriate systems engineering, configuration, and service principles. The System and Services Acquisition Policy ensures that State of Illinois Authorizing Officials, management, and information technology personnel responsible for Information System design and engineering understand the responsibilities necessary to ensure that (i) State of Illinois sensitive information is excluded from open and unauthorized view, (ii) system functionality and requirements are defined during early development, and (iii) proper life-cycle strategies are in place.

System and Communications Protection

The System and Communications Protection Policy requires Agency to employ application, information, and functionality partitioning measures; limit external network connection points; properly manage external

telecommunications; prevent non-remote connections; and secure and monitor all transmitted and stored data, including all channeling networks. The System and Communications Protection Policy ensures that State of Illinois Authorizing Officials and personnel responsible for the management, maintenance, or development of Information Systems understand the responsibilities necessary to prevent unauthorized system management access and control information flow via shared information sources, connections, networks, and other data sources.

System and Information Integrity

The System and Information Integrity Policy requires Agency to employ alert mechanisms to identify Information System flaws during malfunction or failure; designate central management for automated malicious code protection measures; apply real-time event analysis, validation, and verification tools, including traffic communications monitoring; and log detection events. The System and Information Integrity Policy ensures that State of Illinois Authorizing Officials, information security management and personnel, and other personnel assigned to system and information integrity roles understand the responsibilities necessary to effectively determine changing states within the State of Illinois' Information Systems, obtain accurate event-based system information, and determine suitable corrective actions for security-relevant events.

10. SUPPLEMENTAL INFORMATION SECURITY POLICIES

The State of Illinois has developed and published supplemental policies to ensure the appropriate protection of information and Information Systems that require the establishment of enhanced information security controls due to the sensitivity or criticality of the data, and/or the existence of enhanced security requirements established by state or federal law, rule, regulation, or industry-specific guidelines.

All information and Information Systems governed by supplemental information security policies adopt the requirements of all minimum-standard information security policies detailed above, unless otherwise specified. The additional required security controls and standards are included in each supplemental information security policy.

Should a conflict be identified between a State of Illinois supplemental information security policy and the laws, rules, regulations, or guidelines that have been published by the governing authority, the requirements stipulated and published by the governing authority shall apply.

Criminal Justice Information System Security

The security of criminal justice information is governed by the Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS) Security Policy. Criminal justice information is the term used to refer to all the FBI CJIS-provided data necessary for law enforcement and civil agencies to perform their missions, including but not limited to biometric, identity history, biographic, property, and case/incident history data. Illinois criminal justice agencies, as well as DoIT, have specific responsibilities and security requirements identified by the CJIS Security Policy. The CJIS Security Policy ensures that State of Illinois Authorizing Officials and other personnel who are responsible for ensuring the security of criminal justice information understand the expanded security and compliance requirements.

Federal Tax Information Security

Federal law specifically names state Employees among those who may not disclose federal tax returns and return information unless permitted by an exception in the statute. (See Internal Revenue Service Publication 1075.) Tax Information Security Guidelines provide safeguards for the protection of federal tax returns and return information. The expanded security and compliance requirements that must be established and maintained apply to all State of Illinois personnel, but are especially relevant to those Agencies that deal with federal tax returns and return information on an ongoing basis. Federal Tax Information (FTI) that is transmitted across Information Systems must also be specifically addressed. The Federal Tax Information Security Policy ensures that State of Illinois Authorizing Officials who oversee and/or authorize the use of Information Systems that contain or process FTI understand the expanded security and compliance requirements of FTI. State personnel who process, use, or otherwise access FTI must also understand the requirements and, specifically, the limitations on the release and/or sharing of FTI.

Payment Card Data Protection

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance the security of cardholder data and to facilitate the broad adoption of consistent data security measures globally. The PCI DSS provides a baseline of technical and operational requirements designed to protect account data. The PCI DSS applies to all entities involved in payment card processing, which includes many State of Illinois agencies, boards, and commissions. State of Illinois agencies, boards, and commissions that process electronic payment card transactions are expected to meet the supplemental requirements associated with protecting

themselves from PCI fines, credit card misuse, consumer identity theft, and cyber-crimes.

Protected Health Information Security

The United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, in 1996. This law addresses a variety of issues related to health care. HIPAA required the U.S. Department of Health and Human Services to adopt standards regarding the electronic exchange, privacy, and security of health information. The HIPAA Privacy Rule sets standards with respect to the rights of individuals to their health information, procedures for exercising those rights, and the authorized and required uses and disclosures of such information. The HIPAA Privacy Rule defines what information needs to be protected and who is authorized to access the Protected Health Information (PHI), and it also delineates individuals' rights to control and access their own protected information.

The security standards in HIPAA (the HIPAA Security Rule) were developed for two primary purposes. First and foremost, the implementation of appropriate security safeguards protects certain electronic health information that may be at risk. Second, protecting an individual's health information, while permitting the appropriate access and use of that information, ultimately promotes the use of electronic health information in the industry—an important goal of HIPAA.

Agencies shall establish reasonable measures to limit the use and disclosure of electronic PHI to accomplish the intended purpose of business requests and to ensure compliance with applicable state and federal laws. Agencies must set baselines to effectively limit access and protect the confidentiality, availability, and integrity

of electronic health information.

Protection of Personally Identifiable Information

The State of Illinois is entrusted with the personal information of millions of its residents and other constituents. Personally Identifiable Information (PII) is held in myriad State of Illinois Information Systems and must be protected. Agencies shall establish appropriate and effective privacy security controls to protect the identity of individuals by defining permissible and prohibited practices in the collection, access, use, sharing, and destruction of PII. Agencies shall manage PII utilized by State of Illinois resources and shall promote compliance with local, state, and federal regulations regarding privacy and confidentiality in accordance with the Illinois Identity Protection Act (5 ILCS 179) and the Illinois Personal Information Protection Act (815 ILCS 530).

11. KEY ROLES AND RESPONSIBILITIES

State of Illinois information security is a shared responsibility that must be integrated into all aspects of the State of Illinois information technology enterprise. This section focuses on the specific roles and responsibilities involved in securing information. (The below subpart headings do not necessarily reflect actual job titles.)

Authorizing Official (Agency Role)

- Senior official or executive with the authority to formally assume responsibility for operating an Information System at an acceptable level of risk to operations, assets, individuals, and other organizations
- Reviews and approves the data classification and system categorization assigned to the information types and Information System
- Approves security plans and Plans of Actions and Milestones (POAMs)
- Determines whether significant changes require reauthorization

Business System Owner (Agency Role)

- Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an Information System
- Ensures system Users and support personnel receive requisite training
- Responsible for addressing the operational interest of the User community and for ensuring compliance with information security requirements
- Assigns and documents initial information classification and periodically reviews the classification to ensure it accurately reflects the risks associated with the potential loss of the confidentiality, integrity, and availability of the information and Information System
- Responsible for integrating the minimum baseline security controls based on the categorization of the information
- Works with appropriate staff to remediate control deficiencies
- Establishes and maintains Information System resiliency requirements based on business impact analyses

- Serves as the approval authority for access requests from other business units or delegates approval authority to a representative in the same business unit

Chief Executive Officer (Agency Role)

- Ensures that information security management processes are integrated with strategic and operational planning processes
- Ensures Chief Information Officers provide information security support for operations and assets under their control
- Ensures personnel are sufficiently trained to assist in complying with the information security requirements
- Ensures all Employees, contractors, and third parties who will access the State of Illinois network and/or otherwise have access to sensitive State of Illinois information are appropriately screened in line with Agency and information security policies and standards
- Ensures all Employees, contractors, and third parties who will access the State of Illinois network and/or otherwise have access to sensitive State of Illinois information receive information security awareness training

Chief Information Officer (DoIT Role)

- Ensures that all IT projects and procurements go through Governance
- Ensures the periodic assessment of risk posed to the confidentiality, integrity, and availability of information and Information Systems and ensures the development and execution of risk remediation plans
- Responsible for remediation of identified vulnerabilities
- Ensures that data is classified, Information Systems are categorized, and resiliency requirements are established based on the mission and business objectives of the Agency
- Designates or otherwise identifies an Information Systems Security Officer (ISSO) who will be responsible for ensuring the adherence to State of Illinois information security policies, standards, and procedures for all Information Systems
- Ensures the completion, execution, and maintenance of Information System security plans that address Information System security requirements for all Information Systems developed, acquired, or utilized as a service
- Ensures that all Information System security requirements are met prior to Information System implementation
- Ensures personnel are adequately trained in information security roles and responsibilities
- Assists senior Agency officials concerning their security responsibilities
- Facilitates the sharing of security-related information among appropriate staff
- Designates an Agency Information System Security Officer
- Designates a Technical System Owner for each Information System

Chief Information Security Officer (DoIT Role)

- Ensures the alignment of information and cyber security programs with the business missions, goals, and objectives of the Governor and agencies, boards, and commissions
- Establishes information security governance and communication plans
- Conducts information and cyber security strategic, operational, and resource planning and facilitates an effective enterprise information security architecture capable of protecting the State of Illinois in the ever-changing cybersecurity threat landscape
- Facilitates development of subordinate plans for providing adequate information security for networks and systems or groups of Information Systems
- Develops and maintains risk-based, cost-effective information security programs, policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each Agency Information System to ensure compliance with applicable security and regulatory requirements
- Establishes DoIT's capability to sufficiently protect the security of data through effective Information System security planning, secure system development, acquisition and deployment, the application of protective technologies, and Information System certification, accreditation, and assessments
- Ensures that Agency personnel, including contractors, are appropriately screened and receive information security awareness training
- Oversees personnel with significant responsibilities for information security and ensures a competent workforce
- Supports the DoIT Secretary in annual reporting to the Governor and the General Assembly on the effectiveness of the State of Illinois information security programs
- Establishes the policies, procedures, processes, and technologies to rapidly and effectively identify threats, risks, and vulnerabilities to Agency Information Systems, and ensures the prioritization of the remediation of vulnerabilities that pose risk to the enterprise
- Develops and implements capabilities and procedures for detecting, reporting, and responding to security incidents
- Establishes proactive capabilities to identify, protect, detect, respond, and recover from information and cyber security threats and attacks
- Periodically assesses and communicates risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and Information Systems that support the operations and assets of Agencies and the enterprise
- Establishes and periodically tests security policies, standards, procedures, guidelines, and plans that provide the framework for reducing information security risk and enable regulatory compliance
- Establishes and maintains a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and Agency practices
- Develops the policies, standards, and monitoring capabilities to enable effective information security asset management, including asset classification, prioritization, and secure configuration monitoring
- Manages and prioritizes the acquisition of security services and products
- Facilitates secure system and information access through the establishment of effective identity and

access management controls, processes, and technologies; privileged identity management and monitoring; and the management of digital certificates
- Ensures preparation and maintenance of plans and procedures to provide cyber-resilience and continuity of operations for Information Systems that support the operations and assets of the State
- Establishes and implements the data classification, system categorization, and resiliency programs
- Reviews and processes information security policy exception requests

Risk Officer (DoIT Role)

- Ensures risk-related considerations are viewed from an Agency-wide perspective regarding the Agency's overall strategies, goals, and objectives
- Ensures that the management of Information System-related security risks is consistent across the Agency
- Provides oversight to the data classification and system categorization process to ensure that Agency risk to mission and business success is considered in decision-making
- Considers all sources of risk, including aggregated risk from individual Information Systems
- Promotes collaboration and cooperation with other Agencies and external entities
- Identifies risks and assists with the development of suitable loss control and intervention strategies
- Facilitates the sharing of security risk-related information among authorizing officials

Information Security Architect (DoIT Role)

- Responsible for ensuring the identification of Information System security requirements necessary to protect the Agency's core mission and business processes
- Addresses all aspects of enterprise architecture, including reference models, segments and solutions architectures, and the resulting Information System supporting the business mission
- Serves as the liaison between the Enterprise Architect and Information System Security Engineer

Information Security Risk Assessor (DoIT Role)

- Facilitates the classification of data and categorization of Information Systems
- Conducts Information System security risk assessments
- Facilitates the development of risk treatment plans

Information System Security Controls Assessor (DoIT Role)

- Conducts assessments of management, operational, and technical security controls of an Information System to ensure compliance with Information System security plans and to determine the overall effectiveness of the controls
- Provides specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities
- Provides recommendations and findings related to Information System security controls to assist with the Information System accreditation and authorization process
- Tracks compliance with Information System security control Plans of Action and Milestones (POAMs)

Information System Security Engineer (DoIT Role)

- Reviews and refines security requirements, provides recommendations, and assists with the integration of appropriate security technologies into Information Systems
- Provides guidance in the establishment or validation of the system boundary of Information Systems
- Serves as advisor to solution development teams and/or providers to assist with the design, development, and implementation of Information Systems or the upgrade of legacy systems

Information System Security Officer (DoIT Role)

- Develops, executes, and controls the changes to Information System security plans for systems
- Ensures that Information System security plans address Information System security requirements for assigned Information Systems
- Coordinates and facilitates applicable security requirements for assigned Information Systems
- In close collaboration with the Business System Owner, ensures that the appropriate operational security posture is maintained for an Information System
- Serves as a principal advisor on all matters, technical and otherwise, involving the security of assigned Information Systems
- Assists in the development of security controls and procedures

Resiliency Planner (DoIT Role)

- Facilitates the completion of business impact analyses for Agency functions that are supported by Information Systems
- Provides findings to chief executive officers, Business System Owners, and other key personnel Develops and assists with the training, testing, and execution of Information System and critical infrastructure contingency plans and disaster recovery plans

Technical Business Owner (DoIT Role)

- Responsible for the technical implementation, development, integration, modification, operation, maintenance, and disposal of an Information System as requested by the Business System Owner
- Responsible for ensuring technical compliance with information security requirements
- Responsible for integrating the minimum technical baseline security controls based on the categorization of the information
- Works with appropriate staff to remediate information system deficiencies

Revision history and approvals are reflected in ServiceNow.