Acceptable Use Policy

1 OVERVIEW

As State of Illinois employees, we have access to State information and State systems, technology and other information resources, including State-owned hardware, software, and computer network access. This Policy refers to all such information, data, systems, technology, and resources collectively as "Information Technology Resources (IT Resources)". As stewards of IT Resources, each of us is responsible for protecting those resources.

Inappropriate use exposes the State and its agencies to risks including cyber-attacks, compromise of network systems and services, information breaches and legal issues. Inappropriate personal use of IT Resources on State time also deprives the State of another valuable resource – your time and service.

To avoid these problems, every employee who accesses IT Resources (Users) must know and understand the following guidelines and conduct their activities accordingly.

2 GOAL

The goal of this Acceptable Use Policy is to establish appropriate and acceptable practices and responsibilities regarding the use of IT Resources, which will protect proprietary, personal, privileged, or otherwise sensitive data.

3 SCOPE

This Acceptable Use Policy requires statewide compliance, and it covers and applies to:

- All State agencies, boards, commissions, IT service providers, and any other entities that use IT Resources;
- All personnel, employees, and contractors, of the Illinois Department of Innovation & Technology ("DoIT"), and of all State agencies, boards and commissions that use IT Resources. All such personnel are referred to as a "User" or "Users" in this policy;
- All IT Resources, including systems and technology capabilities developed, acquired, or used as a service, whether the IT Resource is internally or externally developed, housed or maintained.

This policy establishes minimum guidelines for acceptable use. A User's agency policy may be more restrictive, and to that extent will supersede the minimum requirements of this policy.

4 REQUIREMENTS

4.1 General Use and Ownership

4.1.1 Every User must avoid all activity that compromises the security, performance or integrity of IT Resources, or that negatively impacts the IT Resources or other Users.

4.1.2 State employees, vendors, business partners, and other governmental agencies must first be authorized by DoIT or client agency designated staff before accessing IT Resources.

4.1.3 All individuals who access IT Resources may be required to undergo personnel screening. Such screening could include a background check, which shall be proportional to the data classification, business requirements, and acceptable risk, each based on the IT Resources being accessed.

4.1.4 Users must use IT Resources within the scope of their employment or contractual relationship with the State only, and must agree to abide by the terms of this policy. Such agreement will be evidenced by the User's acceptance of the terms and conditions of this policy.

4.1.5 Users shall promptly report to their supervisor and/or the service desk all security incidents, disruption of service, actual or suspected theft, loss and/or unauthorized disclosure of IT Resources.

4.1.6 The State audits IT Resources to secure its information systems and ensure compliance with this policy.

4.1.7 Limited, reasonable personal use of State Network Resources, in accordance with this Policy, is allowed. Users should be aware that all usage may be monitored and there is no reasonable expectation of privacy in the use of IT Resources.

4.2 Security and Information

4.2.1 All Users must undergo Cybersecurity Awareness Training, pursuant to 20 ILCS 450/25.

4.2.2 Users may access, use or share IT Resources only to the extent necessary to fulfill assigned job duties. All IT Resources must be handled with due care and confidentiality. Users who create, receive, process, edit, store, distribute or destroy IT Resources which are confidential, sensitive in nature, and/or governed by federal or state laws, rules or regulations must understand their responsibilities to protect such information.

4.2.3 All computing devices, which include personally owned devices, that connect to the State of Illinois internal network must first be authorized.

4.2.4 System and user level passwords must meet DoIT's password length and complexity requirements.

4.2.5 Use of another User's password or any other authentication capabilities is strictly prohibited.

4.2.6 User privileges must not be elevated without formal approval by authorized personnel.

4.2.7 Technical personnel must utilize accounts specified for elevated privileges.

4.2.8 Computing devices must be secured with a password-protected screensaver enabled, as applicable. Users must lock the screen or log off/sign out of the device when the device is unattended.

4.2.9 Users must use caution when opening e-mail attachments received from unknown senders, as attachments may contain malware. Users must also use caution when clicking on hyperlinks in email, as this could result in a successful cyber-attack.

4.3 Unacceptable Use

The following activities are prohibited. State Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access if it is disrupting production services).

Under no circumstances should any State resource be used to engage in any illegal activity.

The examples listed below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1 Prohibited System and Network Activities

4.3.1.1 Violations of any copyright, trade secret, patent or other intellectual property, or any similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or any other software products that are not licensed for use by the State.

4.3.1.2 Unauthorized copying, sharing and/or distribution of copyrighted material.

4.3.1.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate

management should be consulted prior to export of any material.

4.3.1.4 Careless introduction of malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, and e-mail bombs).

4.3.1.5 Revealing your account password to others or allowing others to use your account. This includes family and other household members. If the User losses control of their credentials they should report this to the helpdesk or their appropriate IT or Security staff and immediately change their network/email password.

4.3.1.6 Using IT Resources to obtain or transmit material that is in violation of sexual harassment or hostile workplace laws in the User's local jurisdiction, including but not limited to publishing, distributing, selling, displaying, possessing obscene materials such as pornography, child pornography, cyberbullying and threats of violence.

4.3.1.7 Effecting security breaches or disruptions of network communication.

4.3.1.8 Port scanning or security scanning is expressly prohibited unless prior notification to DoIT Division of Information Security is made. Security scanning conducted by or with express authorization from the Chief Information Security Officer ("CISO") is excluded from this prohibition.

4.3.1.9 Executing any form of network monitoring that will intercept data not intended for the User's host, unless this monitoring activity is a part of the User's normal job/duty.

4.3.1.10 Circumventing User authentication or security features of any host, network or account.

4.3.1.11 Installing password crackers, denial of service tools, key loggers or any other software or tools designed to acquire unauthorized access to data or IT Resources. Use of such tools can be acceptable, but only with express authorization from the CISO.

4.3.1.12 Utilizing tools such as unauthorized browsers to access the 'dark web' unless expressly authorized by the CISO.

4.3.1.13 Introducing honeypots, honeynets, or similar technology on the State network unless expressly authorized by the CISO.

4.3.1.14 Interfering with or denying service to any User (for example, a denial of service attack).

4.3.1.15 Using any program/script/command, or sending messages of any kind, with

the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.16 Providing information about, or lists of, State employees to parties outside of State established processes.

4.3.1.17 Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation, or which may compromise the security of the State, IT Resources, and/or DoIT Client Agencies.

4.3.1.18 Installing software that has not been authorized in writing by the requestor's manager and an appropriate service request submitted to designated IT staff or Help Desk for processing.

4.3.1.19 Attaching devices that have not been authorized in writing by the requestor's manager and then submit appropriate service request to designated IT staff or Help Desk for processing.

4.3.1.20 Using IT Resources to play or download games, music or videos that are not in support of business functions.

4.3.1.21 Using peer-to-peer or file sharing software must be authorized by the CISO.

4.3.1.22 Utilizing IT Resources for activities that violate policies established by State agencies, boards or commissions.

4.3.1.23 Moving, adding, or altering the security and/or security-related configurations of State owned workstations, mobile devices, network equipment, software or services.

4.3.1.24 Sharing or storing IT Resources via unauthorized cloud services.

4.3.2 Prohibited Email and Communication Activities

The purpose of the State's e-mail system is for correspondence relating to the mission of the agency, board or commission. E-mail is a resource provided to agencies, boards and commissions, and Users to enhance work performance and productivity, enable efficient communication, and to record and preserve the work performed in accordance with State law. The following are prohibited activities:

4.3.2.1 Sending "junk mail" or advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2 Any form of harassment via email, telephone, or instant messaging.

4.3.2.3 Unauthorized use, or forging, of email header information.

4.3.2.4 Solicitation of email for any other email address (other than that of the poster's account), with the intent to harass or to collect replies.

4.3.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6 Sending unsolicited email from within the State networks.

4.3.2.7 Users are not allowed to create or open archived .PST files unless first authorized in writing by the requestor's manager and then submit appropriate service request to designated IT staff or Help Desk for processing.

4.3.2.8 The Enterprise email system includes a disclaimer notification at the bottom of every email sent from the system. Additional disclaimers must be approved by the User's agency senior management or their legal department.

4.3.2.9 Sending broadcast messages to all agency email Users within the scope of the Enterprise Email system without appropriate authorization.

4.3.2.10 Misaddressed messages shall not be forwarded unless the User is familiar with both the sender and the recipient, and knows the message pertains to legitimate State business. In all other instances the sender should be notified, if possible, that the message was misaddressed or misdirected and the email deleted.

4.3.2.11 Users may not create email rules or other automated processes to forward any email to external email accounts; personal or otherwise. This includes carbon copying to personal accounts.

4.3.2.12 Users cannot retain or export a copy of email when terminating employment with the agency unless authorized by agency senior management or agency legal department.

4.3.3 Prohibited Activities When Using Collaboration Tools (Audio, Video, File Sharing, Group Chat, Remote tools and Online Meeting tools):

4.3.3.1 Using collaboration resources for monetary gain or for commercial, religious, or political purposes not directly related to State business.

4.3.3.2 Capturing, opening, intercepting or obtaining access to collaboration tools, except as otherwise permitted in the performance of assigned job responsibilities.

4.3.3.3 Giving the impression to others that the User is representing, giving opinions or otherwise making statements on behalf of DoIT, unless in the performance

of assigned job responsibilities.

4.3.3.4 Users will not directly or by implication employ a false identity.

4.3.4 Prohibited Blogging and Social Media Activities

4.3.4.1. Nothing in this Policy is intended to interfere with, restrain, or impinge upon any User's Constitutional rights, nor upon communications regarding wages, hours, or other terms and conditions of employment. Users have the right to engage in or refrain from such activities in accordance with any other applicable statues, rules, regulations or policies.

4.3.4.2. Users are prohibited from making comments or otherwise communicating about customers, residents, vendors, suppliers, coworkers, or supervisors in a manner that is vulgar, obscene, threatening, intimidating, harassing, libelous, or discriminatory on any grounds.

4.3.4.3. Privacy and confidential information requirements also apply to blogging and social media activities. As such, Users are prohibited from revealing any private, confidential or proprietary information, trade secrets or any other material protected from disclosure by applicable statutes, rules, standards, contracts and policies when engaged in blogging and/or social media activities.

4.3.4.4. When using social media in a non-official, or personal capacity:

- Users who identify themselves as a State employee or have a public-facing position should ensure their profile and related content conforms to applicable requirements, such as (but not limited to) the State Officials and Employees Ethics Act (5 ILCS 430).
- Users should add a disclaimer to their social networking profile, personal blog, or other online presences that clearly state that the opinions or views expressed are the User's alone, and do not represent the views of the User's employing agency or the State.
- In a publicly accessible forum, Users shall not discuss any agency or State-related information that is not already considered public information. The discussion of sensitive, proprietary, or confidential information is strictly prohibited. This rule applies even in circumstances where password or other privacy controls are implemented.

4.3.4.5. Users must comply with all applicable laws regarding trademarks, logos, intellectual property, rights of publicity, and any other third-party rights. Users

may not infringe on State-owned trademarks, logos, intellectual property, or rights of publicity.

4.4 Internet Access

Internet access is provided to meet informational needs and support the mission and goals of the State. All Internet usage utilizing IT Resources falls under this Acceptable Use Policy, regardless of equipment ownership. Misuse of Internet access may result in loss of Internet access privileges, or discipline, up to and including discharge.

Internet use is monitored by the State. Suspected misuse of the Internet should be reported to the applicable DoIT Client Agency for review and determination of appropriateaction.

5 POLICY COMPLIANCE

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

The DoIT Division of Information Security will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Policy owner.

All Users of DoIT and DoIT client agencies are required to complete the Ethics Training Program and Cyber Security Awareness training as part of the initial training for new users and annually thereafter. Any break in service, as defined by governing HR policy, will require retraining.

Any exception to this Policy must be approved by the DoIT Division of Information Security in writing and in advance of any action otherwise contrary to this Policy.

Failure to comply with this Policy may result in the CISO, or designee, temporarily discontinuing or suspending the operation of the information system, access, solution and/or resource until such compliance is established by the CISO or designee. Failure to comply with this Policy could also result in discipline, up to and including discharge.

Noncompliance with this Policy may constitute a legal risk to the State, an organizational risk to the State in terms of potential harm to employees or resident security, or a security risk to State Network Operations and the user community, and/or a potential personal liability.

The
presence of unauthorized data in the State network could lead to liability on the part of the State, in addition to the individuals responsible for obtaining it.

6 APPLICABLE LAWS, GUIDELINES OR SOURCES

Applicable laws, rules and regulations include, but are not limited to, those found in the State Enterprise Information Security Policy, and the State Officials and Employees Ethics Act, 5 ILCS 430 and 20 ILCS 450/25.

7 RELATED POLICIES, STANDARDS AND GUIDELINES

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

CERTIFICATION

I have been issued a copy of the Department of Innovation & Technology Acceptable Use Policy. I understand that compliance with the State's policies and regulations is a condition of employment and that it is my obligation to read, understand, and remain current with any new or amended policy, rule, directive or regulation. I further understand that a violation of any State policy, rule, directive or regulation may result in disciplinary action, up to and including discharge.

[Please sign below]

Signature **Date**

I UNDERSTAND THAT NO STATEMENT IN THIS POLICY SUPERSEDES THE PERSONNEL CODE OR ANY NEGOTIATED CONTRACT, NOR DOES THIS POLICY CONSTITUTE OR IMPLY ANY CONTRACTUAL OBLIGATIONS.

IT IS THE RESPONSIBILITY OF EACH EMPLOYEE TO COMPLETE THIS CERTIFICATION AND RETURN IT TO HIS OR HER IMMEDIATE SUPERVISOR. THE SUPERVISOR MUST FORWARD THE COMPLETED FORM TO THE PERSONNEL OFFICE FOR INCLUSION IN THE EMPLOYEE'S OFFICIAL PERSONNEL FILE.

PUBLICATION APPROVAL FORM

Publication Name(s):	Version #(s):
Acceptable Use Policy	03/22/2022
Overarching Enterprise Information Security Policy	03/22/2022

PROCESS, PROCEDURE, & STANDARD PUBLICATIONS

	Print Name	*Signature*	*Date*
APPROVER	Adam Ford		3/22/2022

Instructions:

1. **Complete signature process**
2. **Digitally scan signed Publication Approval Form**
3. **E-mail pdf version of Publication Approval Form and WORD version of document to:**
   DoIT.EUC.SVCMGMT@Illinois.Gov

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Access Control

1. OVERVIEW

It is the policy of the State of Illinois to protect State Information Systems against improper or unauthorized access that could result in the compromise of confidentiality, integrity, or availability of State of Illinois information, information technology (IT) assets, or technology-enabled capabilities. The establishment of appropriate and effective access controls helps to prevent accidental damage, disruption, physical tampering, eavesdropping, and other potential incidents. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to reduce the security risks posed to State of Illinois Information Systems due to unauthorized or unintentional access, while meeting the access requirements for authorized Users.

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Account Management

4.1.1 Agency shall identify Information System account types to support its mission and business functions. Account types could include, but are not limited to, group, system, application, guest/anonymous, emergency, and temporary accounts.

4.1.2 Agency account managers shall assign Information System accounts.

4.1.3 Agency shall establish conditions for group and role membership.

4.1.4 Agency shall specify required attributes for authorized Users, group and role membership, and access authorizations.

4.1.5 Accounts shall not be created without specific Agency approval. Information Owners shall approve User accounts, roles, and access levels based on need-to-know rules.

4.1.6 Privileged accounts shall be approved as appropriate by the DoIT-designated Information System Administrator(s).

4.1.7 Agency shall establish standards and/or procedures for creating, enabling, modifying, disabling, and removing Information System accounts for each account type.

4.1.8 Agency shall monitor Information System accounts commensurate with the level of privilege, risk, or other established standards.

4.1.9 Agency shall establish procedures for notifying appropriate account managers when accounts are no longer required or when access level requirements change. Triggers for these notifications

include but may not be limited to: User termination, User transfer, or changes to User job responsibilities.

4.1.10 Agency shall periodically review Information System accounts for compliance with established access rules.

4.2 Access Enforcement

4.2.1 Agency shall have the technical capability to enforce logical access to information and system resources in accordance with access control rules and policies.

4.3 Information Flow Enforcement

4.3.1 DoIT shall authorize and document business and security requirements for information flow between interconnected systems.

4.4 Separation of Duties

4.4.1 Agency shall address the potential for abuse of authorized privileges through the documentation and enforcement of separation of duties. Separation of duties includes but is not limited to: (i) dividing mission functions and Information System support functions; (ii) conducting Information System support functions with different individuals (e.g., system management, programming, and security); and (iii) ensuring that security personnel who administer access control functions do not also administer audit functions.

4.5 Least Privilege

4.5.1 Agency shall employ the principle of least privilege and allow only authorized access for Users (or processing actions on behalf of Users) that is necessary to accomplish assigned tasks.

4.6 Unsuccessful Logon Attempts

4.6.1 Information Systems must automatically lock an account after a maximum number of invalid or unsuccessful logon attempts.

4.7 System Use Notification

4.7.1 Internal Use Systems (State of Illinois Business Applications – Non-Public Use)

- An approved system use notification message or banner shall be displayed that provides privacy and security notices consistent with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance before granting access to the system. The notification message shall state that:
  - Users are accessing a State of Illinois Information System;
  - unauthorized use of the Information System is prohibited and subject to discipline and criminal and/or civil penalties; and

- use of the Information System indicates consent to monitoring and recording.

4.7.2 Publicly Available Information Systems

- A publicly available Information System shall display system use information that includes a description of authorized uses of the system before granting further access.
- A publicly available Information System shall display references, if any, to applicable monitoring, recording, or auditing that will be present with the use of the publicly available system.

4.7.3 System use notifications shall be retained on the screen until the User- acknowledges the usage conditions and takes explicit actions to log on to or further access the Information System.

4.7.4 Information Systems that are presented strictly for viewing publicly available information may be exempted from the system use notification requirement.

4.8 Session Lock

4.8.1 Information System sessions shall lock after a defined period of inactivity or upon receiving a request from the User.

4.8.2 A session lock shall remain in place until the User reconnects by using established identification and authentication.

4.8.3 Information Systems shall conceal information previously visible on the display with a publicly viewable image.

4.9 Session Termination

4.9.1 Information systems shall automatically terminate a User session after a defined period of inactivity.

4.10 Permitted Actions Without Identification and Authentication

4.10.1 Agency Information System security plans shall document any actions that will be permitted without identification or authentication and provide specific rationale for allowing these actions.

4.11 Remote Access

4.11.1 Usage restrictions and configuration/connection requirements for any planned or in-place remote access to the Information System shall be established and documented by DoIT. Implementation guidance for any remote access to Information Systems shall be developed by DoIT for each type of remote access allowed.

4.11.2 Remote access to Information Systems shall be authorized by the Information Owner prior to allowing such connections. Justification for remote access shall be provided and approved by the Employee's supervisor or designee.

4.11.3 Remote access to the State of Illinois network via virtual private network or similar technologies/connections shall be reviewed and approved by DoIT based on justified business

need as authorized by the User's supervisor. Remote access by third parties must also be approved by DoIT.

4.11.4 Remote access shall be monitored and controlled by DoIT. Cryptographic mechanisms shall be implemented by DoIT for access via virtual private network or similar technologies to further protect the confidentiality and integrity of remote access sessions.

4.11.5 Remote access shall be routed through a limited number of managed access control points by DoIT.

4.11.6 DoIT shall establish additional remote access controls such as geographic boundary, time of day usage, and/or other appropriate controls to further protect the confidentiality and integrity of remote access sessions.

4.12 Wireless Access

4.12.1 Usage restrictions, configuration and connection requirements, and implementation guidance shall be established by DoIT for wireless access to Information Systems and the State of Illinois network.

4.12.2 Wireless access policies and practices shall be authorized by Agency executive management with guidance from DoIT. Agency wireless access to State of Illinois IT assets and infrastructure shall be protected using encryption and authentication of both Users and devices.

4.12.3 Wireless access services provided by DoIT for use by the public and/or visitors shall not be enabled to provide access to the State of Illinois network. Sufficient security controls and technology must be in place to ensure public users have no path through a public network to the State of Illinois network.

4.13 Access Control for Mobile Devices

4.13.1 Usage restrictions and implementation guidance shall be established by DoIT for the use of mobile devices.

4.13.2 Mobile device access to Information Systems must be approved by Agency.

4.13.3 Full-device encryption, or container encryption, shall be utilized by Agency to protect the confidentiality and integrity of information on approved mobile devices.

4.14 Use of External Information Systems

4.14.1 Terms and conditions must be established by Agency prior to allowing external Information Systems to connect to State of Illinois Information Systems. Information System security plans must identify any and all external Information System connections that are planned or in place for the specific Information System. This requirement applies to: (i) any external Information Systems that will access a State of Illinois Information System; and (ii) the processing, storage, or transmission of State of Illinois information with/using external Information Systems.

4.14.2 State of Illinois employees, contractors, or third parties acting on behalf of the State of Illinois are prohibited from using external Information Systems to process, store, or transmit State of Illinois controlled information unless: (i) the Information System has been acquired for specific use by the State of Illinois and has been approved for use by DoIT; (ii) the Information System is being shared as part of a contract, interagency agreement, connection agreement, or other formal agreement; or (iii) the Information System has been explicitly approved by the Chief Information Security Officer.

4.14.3 The use of external systems shall only be approved by the Agency after verifying that the security controls of the external Information System comply with State of Illinois Enterprise Information Security Policies. The Agency authorized to utilize an external Information System must ensure that the external Information System has been properly added to the State of Illinois external Information System portfolio.

4.14.4 External Information System connection agreements shall be retained by the Agency that requires User or Information System access to the external Information System. Any connection agreements must be reviewed and renewed as stipulated in the connection agreements.

4.15 Information Sharing

4.15.1 Information that is restricted under applicable law (e.g., privileged medical information, personally identifiable information, criminal justice information, federal tax information, classified information, and/or other sensitive information) may only be shared following a formal review and authorization. Authorization for the sharing of restricted information may be provided by the Agency's Legal Counsel, the Agency's Privacy Officer, or similar authority.

4.15.2 Information sharing agreements shall be completed by Agency and should, at minimum, define the purpose and justification for the information sharing, the information being shared, the information sharing process, and the procedures for retrieving or disposing of the shared information when the information sharing process is no longer needed.

4.15.3 All information sharing must be in compliance with State of Illinois Enterprise Information Security Policies.

4.15.4 Information Owners shall provide training to authorized Information System Users to assist Users in making appropriate information sharing decisions.

4.16 Publicly Accessible Content

4.16.1 Information Owners shall designate individuals who are authorized to post information onto a publicly available Information System.

4.16.2 Information Owners shall provide training to ensure that authorized Users do not publicly post information that contains non-public information.

4.16.3 Processes shall be established by Agency to review proposed public content prior to public posting to help ensure that non-public information is not included.

4.16.4 Publicly accessible Information Systems shall be reviewed by Agency designated staff for non-public information. Any non-public information discovered will be removed by Agency as soon as reasonably practicable.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy

Audit and Accountability Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes this Enterprise Audit and Accountability Policy for managing risks from inadequate event logging and transaction monitoring. This Policy helps to identify accidental damage, disruption, physical tampering, eavesdropping, and other potential incidents and ensures the confidentiality, integrity, and availability of Information Systems and data within critical information technology (IT) assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

This Policy establishes an audit and accountability capability throughout DoIT and other State of Illinois agencies, boards, and commissions and their business units to implement security best practices for events, transaction logging, and retention of audit evidence.

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Audit Events

4.1.1 Agency shall develop a standard that defines which security events to audit and the frequency of each audit. Agency shall review the list of events based on a defined frequency.

4.1.2 Agency shall determine auditable events in coordination with other entities requiring audit-related information.

4.1.3 Agency shall provide an explanation as to how audit events support investigations of security incidents when applicable.

4.1.4 Agency shall determine which events should be audited within the Information System.

4.2 Content of Audit Records

4.2.1 Audit records shall contain the following information:

- What type of event occurred
- When the event occurred
- Where the event occurred
- Source of the event
- Outcome of the event
- Identity of any individuals associated with the event

4.3 Audit Storage Capacity

4.3.1 DoIT shall allocate an adequate amount of storage capacity to ensure audit records can be retained for the required audit retention period.

4.4 Response to Audit Processing Failures

4.4.1 DoIT shall alert designated personnel when there is an audit processing failure.

4.4.2 DoIT shall create standards to define additional actions to follow in the event of an audit processing failure.

4.5 Audit Review, Analysis, and Reporting

4.5.1 DoIT shall review and analyze Information System audit records for indications of unusual activity related to potential unauthorized access.

4.5.2 DoIT shall report findings to designated personnel.

4.6 Audit Reduction and Report Generation

4.6.1 Agency shall employ audit reduction and reporting capability that supports on-demand audit review, analysis and reporting, and after-the-fact investigations of security incidents.

4.6.2 Agency shall not alter original content and time marking of audit records.

4.7 Time Stamps

4.7.1 State of Illinois Information Systems shall use internal Information System clocks to generate time stamps for audit records.

4.7.2 State of Illinois Information Systems shall record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and shall synchronize internal Information System clocks to an enterprise-wide authoritative time source.

4.8 Protection of Audit Information

4.8.1 Agencies shall protect audit information and audit tools from unauthorized access, modification, and deletion.

4.9 Audit Record Retention

4.9.1 Agencies shall retain audit records to provide support for security incident investigations and to meet regulatory and Agency-specified requirements.

4.10 Audit Generation

4.10.1 The Information System(s) of DoIT and/or its Client Agencies shall provide audit record generation capability for all suitable events that are defined in this Policy or in the associated implementation standards and procedures.

4.10.2 Agencies shall designate personnel to select which events are to be audited by specific components of the Information System.

4.10.3 The Information System(s) of DoIT and/or its Client Agencies shall generate audit records for events defined by regulatory or Agency-specified requirements.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Awareness and Training Policy

1. OVERVIEW

Pursuant to 20 ILCS 450/25, the State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of cybersecurity awareness and training. This training educates Employees how to safeguard the confidentiality, integrity, and availability of State information technology (IT) assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to reduce security risks by educating State of Illinois Employees to help protect and appropriately use IT Resources and data.

3. SCOPE

This Policy applies to all Employees, as defined by the State Officials and Employees Ethics Act (5 ILCS 430/1-5), of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems.

4.1 Security Awareness Training (Content Provided by DoIT)

4.1.1 Security awareness training shall be provided by Client Agencies as part of initial training for new Employees.

4.1.2 Security awareness training shall occur when required by Information System changes as deemed necessary by DoIT.

4.1.3 Security awareness training shall occur on an annual basis as required by 20 ILCS 450/25.

4.2 Role-Based Security Training

4.2.1 Role-based security training is special training for Employees with assigned administrative or technical roles and responsibilities involving access to sensitive information, including but not limited to Federal Tax Information, Protected Health Information, and Personally Identifiable Information.

4.2.2 Role-based security training shall be administered by the Client Agency before granting Employees privileged access to the Information System or before Employees begin performing assigned duties.

4.2.3 Role-based security training shall occur on a defined frequency, whenever there is a significant change in the Client Agency's Information System environment or procedures, and whenever an Employee enters a new position that requires additional role-specific training.

4.3 Security Training Records

4.3.1 Client Agencies shall document and monitor individual Information System security training

activities, including basic security awareness training and specific Information System security training.

4.3.2 Client Agencies shall retain training records for appropriate periods as defined by law.

5. POLICY COMPLIANCE

To implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate responsibility to specific personnel. To the extent necessary, each Client Agency and/or DoIT Division must establish procedures to achieve Policy compliance. It is the responsibility of Employees 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy

Configuration Management

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of appropriate configuration management controls that safeguard the confidentiality, integrity, and availability of Information Systems. This Policy alleviates security risks through configuration management processes. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to create a prescriptive set of process and procedures, aligned with applicable DoIT information technology (IT) security policies and standards, to ensure that DoIT develops, disseminates, and updates its configuration management practices. This Policy establishes the minimum requirements for configuration management.

Executive agencies, boards, and commissions are required to implement necessary controls to maintain proper documentation of IT Resources and information assets on the basis of business and security requirements.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Baseline Configuration

4.1.1 DoIT shall develop, document, and maintain under configuration control a current baseline configuration of the Information System that:

- maintains baseline configurations of the Information System to be consistent with State of Illinois Agencies' enterprise architecture;
- maintains records that document the application of baseline security configurations;
- monitors systems for security baselines and policy compliance;
- reapplies all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade; and
- modifies individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

4.1.2 Agency shall create and periodically review a list of Agency hardware and software assets.

4.1.3 DoIT shall review and update the baseline configuration of the Information System:

- based on a defined frequency;
- when required due to a significant configuration change, such as an operating system upgrade or hardware change, or due to a demonstrated vulnerability; and

- as an integral part of Information System component installations and upgrades.

4.2 Configuration Change Control

4.2.1 DoIT shall determine the types of changes to the Information System that are configuration-controlled.

4.2.2 DoIT shall review and approve configuration-controlled changes to the system with explicit consideration for security impact analyses.

4.2.3 DoIT shall document approved configuration-controlled changes to the system.

4.2.4 DoIT shall retain and review records of configuration-controlled changes to the system.

4.2.5 DoIT shall audit and review activities associated with configuration-controlled changes to the Information System.

4.2.6 DoIT shall coordinate and provide oversight for configuration change control activities through a committee that convenes based on an approved frequency to review changes prior to implementation.

4.3 Security Impact Analysis

4.3.1 Agency shall analyze changes to the Information System to determine potential security impacts prior to change implementation.

4.4 Access Restrictions for Configuration Changes

4.4.1 Agency shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the Information System.

4.4.1.1 Only qualified and authorized individuals are allowed to obtain access to Information System components for purposes of initiating changes, including upgrades and modifications.

4.4.1.2 Maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the Agency become aware of an unauthorized change to the Information System.

4.4.1.3 Logical and physical access control lists that authorize qualified individuals to make changes to an Information System or component must be created and maintained by the Agency.

4.4.1.4 Access to software libraries is restricted to authorized individuals.

4.4.2 Agency shall limit Information System developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment.

4.4.3 Agency shall review and update Information System developer/integrator privileges annually.

4.5 Configuration Settings

4.5.1 DoIT shall establish, document, and implement the configuration settings for IT services.

4.5.2 DoIT shall identify, document, and approve exceptions from the established configuration settings for individual components within the Information System based on operational requirements.

4.5.3 DoIT shall monitor and control changes to the configuration settings in accordance with relevant policies and procedures.

4.6 Least Functionality

4.6.1 DoIT shall verify that the Information System is configured to provide only essential capabilities.

4.7 Information System Component Inventory

4.7.1 DoIT shall develop, document, and maintain an inventory of Information System components that:

- accurately reflects the current Information System;
- includes components within the authorization boundary of the Information System;
- is at the level of granularity deemed necessary for tracking and reporting; and
- includes Agency-defined information deemed necessary to achieve effective property accountability.

4.7.2 DoIT shall review and update the Information System component inventory annually.

4.8 Configuration Management Plan

4.8.1 DoIT shall develop, document, and implement a configuration management plan for the Information System.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 Employees 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

Enterprise Information Security Policy
Contingency Planning Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) Contingency Planning Policy ensures that Information Systems that are determined to be critical and essential to DoIT and Client Agencies' missions have recovery objectives defined, documented, and tested in the case of a catastrophic failure. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to reduce the security risks and establish enterprise contingency planning measures and procedures. Contingency planning helps DoIT execute a coherent, organized, planned, and strategic response to Information System emergencies and other disruptive Information System events.

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Contingency Planning

4.1.1 Information System contingency plans shall:

- 4.1.1.1 identify essential missions and business functions and associated contingency requirements.
- 4.1.1.2 provide recovery objectives and restoration priorities.
- 4.1.1.3 address contingency roles, responsibilities, and contact information of assigned individuals, as well as delegations of authority, orders of succession, and notification procedures.
- 4.1.1.4 address maintaining essential missions and business functions despite an Information System disruption, compromise, or failure.
- 4.1.1.5 address eventual, full Information System restoration without deterioration of the security safeguards originally planned and implemented.
- 4.1.1.6 be reviewed and approved by designated officials within DoIT.

4.1.2 Agency shall distribute copies of the contingency plan to key contingency personnel.

4.1.3 Agency shall coordinate contingency planning activities with incident handling activities.

4.1.4 Agency shall review the contingency plan for the Information System at a DoIT-defined frequency.

4.1.5 Agency shall update the contingency plan to address changes to the Information System or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

4.1.6 Agency shall communicate contingency plan changes to the key contingency personnel.
4.1.7 Agency shall protect the contingency plan from unauthorized disclosure and modification.

4.2 Contingency Training

4.2.1 Agency shall provide training for personnel in their contingency roles and responsibilities with respect to the Information System on a defined frequency, and Agency shall provide refresher training when changes occur.

4.3 Contingency Plan Testing

4.3.1 Information System contingency plans must be tested by the Client Agency with the assistance of DoIT resources on a defined frequency to determine the plan's effectiveness and the Agency's readiness to execute the plan.
4.3.2 The contingency plan test results must be reviewed, and issues must be noted and mitigated to an acceptable level, by the respective Client Agency's designated personnel to ensure the validity of the plan.

4.4 Alternate Storage Site

4.4.1 DoIT shall establish an alternate storage site, including necessary agreements to permit the storage and recovery of Information System backup information.
4.4.2 Agency shall ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

4.5 Alternate Processing Site

4.5.1 Agency shall establish an alternate processing site, including necessary agreements to permit the resumption of Information System operations for essential missions and business functions within a defined time period consistent with recovery time objectives when the primary processing capabilities are unavailable.
4.5.2 Agency shall ensure that equipment and supplies required to resume operations are available at the alternate site to support delivery to the site in time to support the defined time period for resumption.
4.5.3 Agency shall identify an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.
4.5.4 DoIT shall configure the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.
4.5.5 Agency shall ensure that the alternate processing site provides information security measures equivalent to that of the primary site.

4.6 Telecommunications Services

4.6.1 DoIT shall establish alternate telecommunications service plans, including necessary agreements to permit the resumption of Information System operations for essential missions and business functions within a defined time period when the primary telecommunications capabilities are unavailable.

4.7 Information System Backup

4.7.1 Agency shall conduct periodic backups of User information contained in the Information System within a defined frequency consistent with recovery time and recovery point objectives.

4.7.2 Agency shall conduct periodic backups of system-level information contained in the Information System in accordance with a defined frequency consistent with recovery time and recovery point objectives, including system-state information, operating system, application software, and licenses.

4.7.3 Agency shall conduct periodic backups of Information System documentation, including security-related documentation in accordance with a defined frequency consistent with recovery time and recovery point objectives.

4.7.4 Agency shall protect the confidentiality and integrity of backup information at the storage locations.

4.7.5 Agency shall test backup information within a defined frequency to verify media reliability and information integrity.

4.8 Information System Recovery and Reconstitution

4.8.1 Agency shall provide for the recovery and reconstitution of the Information System to a known state after a disruption, compromise, or failure.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Criminal Justice Information Services (CJIS)
Security Supplemental Policy

1. **OVERVIEW**

The State of Illinois Department of Innovation & Technology (DoIT) has published this Supplemental Policy to ensure the appropriate protection of criminal justice information, which requires the establishment of enhanced information security controls due to the sensitivity or criticality of the data. This Policy provides personnel who are responsible for ensuring the security of criminal justice information with an understanding of the expanded security and compliance requirements. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. **GOAL**

The goal of this Supplemental Policy is to secure and control criminal justice information. This minimum standard of security requirements ensures continuity of information protection.

3. **SCOPE**

This Policy applies to all entities with access to, or who operate in support of, the Federal Bureau of Investigation (FBI) Crimination Justice Information Services (CJIS) Division's services and information. These entities include personnel, contractors, and third-parties of the State of Illinois agencies, boards, and commissions that access, transmit, store, and/or process criminal justice information.

4. **REQUIREMENTS**

The State of Illinois adopts the FBI's Criminal Justice Information Services (CJIS) Security Policy as its minimum-security requirement for criminal justice information. All Information Systems developed, acquired, or utilized as a service by DoIT and/or its Client Agencies containing CJIS-regulated information will incorporate this security standard. Entities may develop local security policies; however, the CJIS Security Policy shall be the minimum applicable standard, and local policy shall notdetract from this baseline.

5. **POLICY COMPLIANCE**

Compliance with this Policy is accomplished through established procedures and designation of responsibility to specific personnel/job titles. To the extent necessary, each agency, board, and commission shall establish policies, standards, and procedures in accordance with this Policy.

All Employees are responsible for Policy adherence and understanding. Failure to comply with this Policy could result in discipline, up to and including discharge.

6. **APPLICABLE LAWS, GUIDELINES, OR SOURCES**

Criminal Justice Information Services (CJIS) Security Policy

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Federal Tax Information (FTI) Supplemental Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) has published this Supplemental Policy to ensure the appropriate protection of Federal Tax Information (FTI), which requires the establishment of enhanced information security controls due to the sensitivity or criticality of the data. This Policy provides personnel who are responsible for safeguarding and protecting FTI with required expanded security and compliance guidelines. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Supplemental Policy is to secure and control FTI. This Policy establishes a minimum standard for security requirements that will ensure the continuity of information protection.

3. SCOPE

This Policy applies to all entities with physical and/or logical access to FTI. These entities include personnel, contractors, and third-party State of Illinois agencies, boards, and commissions that access, transmit, store, and/or process FTI. This Policy applies to all Information Systems containing FTI, regardless of whether the Information System is internally or externally developed, acquired from third-party entities, or utilized as a service.

4. REQUIREMENTS

The State of Illinois adopts the Internal Revenue Service's Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies (Publication 1075) as its minimum-security requirement for FTI. All Information Systems developed, acquired, or utilized as a service by DoIT and/or its Client Agencies containing regulated tax information will incorporate the security standards of Publication 1075.

5. POLICY COMPLIANCE

Compliance with this Policy is accomplished through established procedures and designation of responsibility to specific personnel/job titles. To the extent necessary, each agency, board, and commission shall establish policies, standards, and procedures in accordance with this Policy.

All authorized Users of Information Technology (IT) Resources are responsible for Policy adherence and understanding. Failure to comply with this Policy could result in discipline, up to and including discharge.

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Identification and Authentication

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of appropriate identification and authentication controls that safeguard the confidentiality, integrity, and availability of Information Systems. This Policy alleviates security risks by managing risks from User access and authentication to Information Systems through the establishment of effective identification and authentication processes. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to protect State of Illinois Information Systems by creating processes and procedures for securely identifying and authenticating State of Illinois Users.

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

4.1 Identification and Authentication

4.1.1 The Information System shall uniquely identify and authenticate the User.

4.2 Device Identification and Authentication

4.2.1 The Information System shall uniquely identify and authenticate State of Illinois devices before establishing a network connection.

4.3 Identifier Management

4.3.1 The Information System shall receive authorization from authorized personnel to assign an individual, group, role, or device identifier.

4.3.2 The Information System shall select and assign an identifier that identifies an individual, group, role, or device.

4.3.3 The Information System shall prevent the reuse of identical identifiers for a defined time period.

4.3.4 The Information System shall disable the identifier after a defined time period ofinactivity.

4.4 Authenticator Management

4.4.1 The Information System shall verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

4.4.2 The Information System shall establish initial authenticator content for authenticators defined by the Agency.

4.4.3 The Information System shall ensure that authenticators have sufficient strength of mechanism for their intended use.

4.4.4 The Information System shall establish and implement administrative procedures for distributing initial authenticators, for handling lost/compromised or damaged authenticators, and for revoking authenticators.

4.4.5 The Information System shall change default content of authenticators prior to Information System installation.

4.4.6 The Information System shall contain minimum and maximum lifetime restrictions and reuse conditions for authenticators.

4.4.7 The Information System shall change/refresh authenticators on a defined time period.

4.4.8 The Information System shall protect authenticator content from unauthorized disclosure and modification.

4.4.9 The Information System shall require Users to take, and have devices implement, specific security safeguards to protect authenticators.

4.4.10 The Information System shall change authenticators for group/role accounts when membership to those accounts changes.

4.5 Authenticator Feedback

4.5.1 The Information System shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

4.6 Cryptographic Module Authentication

4.6.1 The Information System shall implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Information Security Incident Management

1. OVERVIEW

The ever-increasing number and diversity of cybersecurity-related attacks, as well as the State of Illinois' growing reliance on information and Information Systems for critical functions and services, requires a robust Information Security Incident response capability. While attacks from myriad threat sources place the State at risk, Information Security Incidents can also be caused by human error, lost or stolen equipment, environmental conditions, or other factors. Effective Information Security Incident Management capabilities must be in place to address any type of Information Security Incident that can significantly affect the State's ability to operate or that may cause damage.

This Policy defines management intent, expectations, and direction for the establishment of an Information Security Incident Management capability. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to control the impact of State of Illinois Information Security Incidents within acceptable levels.

3. SCOPE

This Policy applies to Employees of the State of Illinois Department of Innovation & Technology (DoIT) and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. POLICY

DoIT will develop and maintain an Information Security Incident Management capability that:

- detects incidents quickly;
- diagnoses incidents accurately;
- manages incidents properly;
- completes timely and appropriate notifications;
- contains and minimizes damage of incidents;
- restores services affected by incidents;
- determines root causes of incidents;
- implements improvements to prevent recurrence; and
- appropriately documents incidents.

5. DEFINITIONS

5.1 Information Security Incident: A violation or imminent threat of a violation of information security policies, acceptable use policies, or standard security practices. The definition of an Information Security Incident includes but is not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data;
- an unwanted disruption or denial of service;
- a discovery of network intrusions including bot-nets;
- malware events;
- the unauthorized use of a system for the processing or storage of data;
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent;
- an unplanned, unauthorized, or unexpected change to security baselines, including an unauthorized change to security controls, technologies, or processes;
- the inappropriate release of personally identifiable or other confidential information;
- a theft or loss of information technology (IT) equipment that could contain non-public information; and
- a violation of information security policies.

5.2 Information Security Incident Management: The capability to effectively manage Information Security Incidents with the objective of minimizing impacts and maintaining or restoring normal operations.

5.3 Information Security Incident Response Plan: A predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against State of Illinois Information Systems.

6. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

6.1 Information Security Incident Response Training

6.1.1 Information Security Incident response training will be provided to Employees by DoIT on an annual basis.

6.1.2 Information Security Incident response Employees will be trained regarding their specific roles and responsibilities. Incident response Employee training will be conducted by DoIT on at least an annual basis to address any changes to the Information Security Incident Response Plan and to ensure currency of training.

6.2 Information Security Incident Handling

6.2.1 An Information Security Incident handling capability will be developed and maintained by DoIT that includes preparation, detection and analysis, containment, eradication, and recovery processes.

6.2.2 Agency shall coordinate incident handling activities with contingency planning activities.

6.2.3 DoIT shall incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing.

6.3 Information Security Incident Monitoring

6.3.1 Agency shall document and track Information Security Incidents.

6.4 Information Security Incident Reporting

6.4.1 All Employees, contractors, and third-party providers of State of Illinois shall report any and all Information Security Incidents to the DoIT Division of Information Security.

6.4.2 Information Security Incidents shall be reported to the DoIT Division of Information Security without delay, but no later than 24 hours following the discovery of an Information Security Incident.

6.4.3 The DoIT Division of Information Security shall work collaboratively with Employees of impacted or involved agencies, boards, and commissions to help ensure the appropriate reporting of Information Security Incidents to the Governor's Office, the General Assembly, the Attorney General, and/or other entities as required by policies, regulations, or laws.

6.4.4 The DoIT Division of Information Security shall provide guidance and input to executive management of agencies, boards, and commissions regarding potential reporting of Information Security Incidents to law enforcement.

6.4.5 The DoIT Division of Information Security may share information regarding Information Security Incidents with the Illinois State Police Statewide Terrorism and Intelligence Center (STIC), Multi-State Information and Analysis Center (MS-ISAC), and other trusted partners to help resolve, mitigate, or reduce the impact of cyber events on the State or the nation. External information sharing will not include Agency-specific information without the authorization of Agency executive management.

6.5 Information Security Incident Response

6.5.1 The DoIT Division of Information Security shall lead, manage, and coordinate the response to all Information Security Incidents. Information Security Incident responses will be conducted collaboratively with DoIT Divisions and the appropriate Employees from the impacted or involved agencies, boards, or commissions.

6.5.2 The DoIT Division of Information Security shall provide Information Security Incident response support resources, guidance, advice, and assistance to agencies, boards, and commissions to help ensure the effective handling and reporting of Information Security Incidents.

6.5.3 Third-party providers of Information Systems will provide Information Security Incident response cooperation and assistance relating to any Information Security Incidents that involve Information Systems provided by the third-party entity.

6.6 Information Security Incident Response Plan

6.6.1 The DoIT Division of Information Security shall develop and maintain an Information Security Incident Response Plan, subordinate plans, policies, procedures, and guidelines that:

- provide the State of Illinois with a roadmap for implementing its incident response capability;
- describe the structure and organization of the incident response capability;
- provide a high-level approach to the Agency's incident response capability;
- meet the unique requirements for the State of Illinois;
- define reportable incidents;
- provide metrics for measuring the incident response capability within the State of Illinois;
- define the resources and management support needed to effectively maintain and mature an incident response capability; and
- are reviewed and approved by the Chief Information Security Officer.

6.6.2 Third-party providers of State of Illinois Information Systems will develop and maintain as applicable information security incident response plans that meet or exceed the requirements defined in this Policy.

6.6.3 The Information Security Incident Response Plan and subordinate plans shall be protected from unauthorized public disclosure and modification.

6.6.4 The Information Security Incident Response Plan and subordinate plans shall be reviewed on a defined frequency by DoIT. The plans shall be updated by Agencies as appropriate to address system changes or problems encountered during plan implementation, execution, or testing.

6.6.5 Changes to the Information Security Incident Response Plan and subordinate plans shall be communicated to incident response Employee by designated DoIT staff.

7. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 Employees 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.

8. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security

(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

1. OVERVIEW

The State of Illinois Department of Innovation and Technology (DoIT) is responsible for the establishment and implementation of media protection controls to protect electronic and physical media containing State information while at rest, stored, in transit, or actively being accessed. State Information Systems must be protected against improper or unauthorized access that could result in the compromise of confidentiality, integrity, or availability of State of Illinois information assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to reduce the security risk to electronic or physical media containing State of Illinois information and to limit potential mishandling or loss while being stored, accessed, or transported to and from the Information Systems.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Media Access

4.1.1 Agency shall restrict access to sensitive information residing on electronic and physical media to authorized individuals.

4.2 Media Storage

4.2.1 Agency shall:

- physically control and securely store all media in a secure area.
- encrypt digital media according to the classification of the data and secure non-digital media in secured environments.
- protect all Information System media until destroyed or sanitized using approved procedures.

4.3 Media Transport

4.3.1 Agency shall maintain accountability, protect Information System media during transport outside of controlled areas, and document associated activities. To protect the confidentiality and integrity of information stored on digital media and cryptographic mechanisms, Agency must implement FIPS 140-2 during transport outside of controlled areas.

4.4 Media Sanitization

4.4.1 Agency shall sanitize Information System media prior to disposal or release for reuse in accordance with applicable federal and state laws and regulations and Agency standards and policies. Agency shall use sanitation mechanisms that have the strength and integrity equivalent to the security category or classification of the information. Agency shall review, approve, track, document, and verify media sanitization and disposal actions.

4.5 Media Use

4.5.1 Agency shall restrict the use of personally owned media on Agency Information Systems or system components utilizing defined security safeguards.

5. 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 all Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

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.

PUBLICATION APPROVAL FORM

Publication Name(s):	Version #(s):
Acceptable Use Policy	03/22/2022
Overarching Enterprise Information Security Policy	03/22/2022

PROCESS, PROCEDURE, & STANDARD PUBLICATIONS

	Print Name	*Signature*	*Date*
APPROVER	Adam Ford		3/22/2022

Instructions:

1. **Complete signature process**
2. **Digitally scan signed Publication Approval Form**
3. **E-mail pdf version of Publication Approval Form and WORD version of document to:**
   DoIT.EUC.SVCMGMT@Illinois.Gov

State of Illinois
Department of Innovation & Technology
PCI Data Security Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes this Policy to encourage and enhance the security of cardholder data and facilitate the broad adoption of consistent data security measures. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure that State of Illinois agencies, boards, and commissions securely store, process, or transmit cardholder data in compliance with established Payment Card Industry Data Security Standards (PCI DSS).

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT in collaboration with Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Build and Maintain a Secure Network and Systems

- 4.1.1 Agency shall install and maintain a firewall configuration to protect cardholder data.
- 4.1.2 Agency shall change all vendor-supplied defaults for system passwords and other security parameters.
- 4.1.3 Agency shall protect stored cardholder data from unauthorized access.
- 4.1.4 Agency shall encrypt transmission of cardholder data across open, public networks.

4.2 Maintain a Vulnerability Management System

- 4.2.1 Agency shall protect all systems against malware and shall regularly update anti-virus software or programs.
- 4.2.2 Agency shall develop and maintain systems and applications that are secure from unauthorized access.

4.3 Implement Strong Access Control Measures

- 4.3.1 Agency shall restrict access to cardholder data on a business need-to-know basis.
- 4.3.2 Agency shall identify and authenticate access to system components.
- 4.3.3 Agency shall restrict physical access to cardholder data.

4.4 Regularly Monitor and Test Networks

4.4.1 Agency shall track and monitor all access to network resources and cardholder data.

4.4.2 Agency shall regularly test security systems and processes.

4.5 Maintain an Information Security Policy

4.5.1 Agency shall maintain policies that clearly define information security responsibilities for all personnel.

5. POLICY COMPLIANCE

Compliance with this Policy is accomplished through established procedures and designation of responsibility to specific personnel/job titles. To the extent necessary, each Client Agency shall establish policy, standards, and procedures in accordance with this Policy. Exceptions to this Policy are approved through DoIT where justified in maintaining acceptable levels of assurance.

All authorized Users are responsible for Policy adherence and understanding. Failure to comply with this Policy could result in discipline, up to and including discharge.

Revision history and approvals are reflected in ServiceNow.

Enterprise Information Security Policy
Personnel Security

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for establishing appropriate personnel security controls to ensure that safeguards are applied for access and use of Information Technology (IT) Resources and data. Such safeguards include, but are not limited to, conducting appropriate personnel screening and background checks, conducting security awareness training, and executing non-disclosure agreements for individuals needing access to sensitive, confidential, or regulated information. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

It is the policy of the State of Illinois that access to State of Illinois IT Resources will be limited to only those persons who have been appropriately screened and authorized. Agency will ensure that individuals occupying positions of responsibility (including third-party providers) (i) meet established security criteria for those positions, (ii) protect IT Resources during and after personnel actions, and (iii) comply with state and federal laws, rules, and regulations.

2. GOAL

The goals of this Policy are to (i) mitigate the risk of personnel intentionally or inadvertently exploiting their legitimate access to information assets for unauthorized purposes, which may have negative impacts, and (ii) secure the confidentiality, integrity, and availability of information.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Information Security - Position Risk Designation

4.1.1 Agencies shall establish and maintain standards to ensure appropriate levels of personnel screening for all personnel accessing State of Illinois IT Resources. Standards will include:

- defined risk designation levels based on the sensitivity of the information that the individual is required to access for legitimate position responsibilities;
- screening criteria for each risk designation level; and
- periodic reviews and updates to position risk designations.

4.2 Personnel Screening

4.2.1 Individuals will be screened by Agencies prior to being granted access to the applicable information and system(s).

4.2.2 Personnel will be screened by Agencies (i) as part of the establishment of access to the State of Illinois network, (ii) when a change in policies, laws, rules, and/or regulations warrants additional or renewed screening, and (iii) when changes in position and/or responsibilities require access to information that would place the individual into a different risk designation.

4.2.3 Personnel requesting access to State of Illinois IT Resources must comply with the submission of required documentation.

4.3 Personnel Termination

4.3.1 It is the responsibility of Agencies to notify DoIT of personnel employment terminations without delay following the employment termination.

4.3.2 Exit interviews will be conducted by the individual's Agency to review the terms of any applicable non-disclosure agreements and to ensure that the individual separating is informed that State of Illinois confidential and sensitive information shall not be removed, retained, or communicated to third parties.

4.3.3 Agency will terminate, revoke, or render inoperable the terminated individual's access credentials.

4.3.4 Agency will ensure that all Information System devices and authentication devices or tools are obtained from the individual and either returned to DoIT or re-allocated to appropriate personnel.

4.3.5 Agency information and Information Systems formerly controlled by the terminated individual will be retained by Agency, as appropriate.

4.4 Personnel Transfer

4.4.1 Agency will review and confirm ongoing operational need for current logical and physical access authorizations to Information Systems/facilities when individuals are reassigned or transferred to other positions within the Agency.

4.4.2 Agencies must notify DoIT when an individual is transferring to another state Agency.

4.4.3 DoIT will make appropriate changes to required access following the transfer or when DoIT is advised of the transfer.

4.5 Access Agreements

4.5.1 Agencies must develop and document access agreements for their Information Systems in compliance with established policies, laws, rules, and regulations.

4.5.2 Agencies must review and update access agreements in line with applicable laws, rules, and regulations.

4.5.3 Agencies must ensure that individuals requiring access to information and Information Systems:
(1) sign appropriate access agreements prior to being granted access; and

(2) re-sign said agreements to maintain access to Information Systems when access agreements have been materially updated or when access requirements change.

4.6 Third-Party Personnel Security

4.6.1 Third-party providers and third-party personnel must comply with this Policy and all other information security policies.

4.6.2 It is the responsibility of third-party providers to submit any and all documentation as identified in applicable standards as assurance of compliance with this Policy.

4.6.3 Third-party providers must notify the employing Agency of any transfers or terminations of personnel who possess Agency credentials and/or badges, or who have Information System privileges.

4.6.4 DoIT will periodically review compliance regarding third-party personnel security. Third-party providers must provide DoIT with requested information to help ensure compliance with this Policy.

4.7 Denial and/or Termination of Access

DoIT's Office of the Chief Information Security Officer and/or other Agency-designated senior management may deny or terminate access to State of Illinois information and systems by personnel who have not been appropriately screened in accordance with this Policy and/or who are deemed ineligible for information access based on personnel screening criteria.

4.7.1 Should the DoIT Chief Information Security Officer (CISO) or authorized delegate determine that denial or termination of access is warranted, the CISO will notify the impacted Agency-designated senior management of the intent to deny or terminate access. The notification to Agency-designated senior management shall be in writing. Electronic mail may be utilized to provide the notification.

4.7.2 In the case of an imminent threat as determined by the CISO or authorized delegate, termination of access may take place immediately.

4.7.3 The Agency-designated senior management may request an exception to the access denial/termination decision. The exception request shall be in writing to the CISO and/or other Agency-designated senior management. Electronic mail may be utilized to request the exception.

4.8 Information Security Training

4.8.1 Employees seeking or retaining access to State of Illinois IT Resources must undergo information security awareness training in compliance with applicable laws, rules, and regulations.

4.8.2 Information security training must be completed within 30 days of acquiring access to State of Illinois IT Resources.

4.8.3 Employees must undergo information security training on an annual basis between January 1 and December 31 of each year.

4.8.4 DoIT is responsible for providing information security training in compliance with State of Illinois statute 20 ILCS 450/25 and any adopted rules and standards.

4.8.5 Agencies are responsible for ensuring Employee compliance with this Policy.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security establishes supplemental policies, standards, procedures, and guidelines and may designate 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 all authorized Employees of IT Resources 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Protected Health Information (PHI) Supplemental Policy

1. **OVERVIEW**

The State of Illinois has published this Supplemental Policy to ensure the appropriate protection of Protected Health Information (PHI), which requires the establishment of enhanced information security controls due to the sensitivity or criticality of the data. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. **GOAL**

The goal of this Supplemental Policy is to secure and control PHI. This minimum standard of security requirements ensures continuity of information protection.

3. **SCOPE**

This Policy applies to all entities with access to, or who operate in support of information regulated by the Federal Centers for Medicare and Medicaid Services (CMS). These entities include personnel, contractors, and third-party State of Illinois agencies, boards, and commissions that access, transmit, store, and/or process PHI subject to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

4. **REQUIREMENTS**

The State of Illinois adopts the HIPAA Security Rule as its minimum-security requirement for those serving as a HIPAA Exchange. All Information Systems developed, acquired, or utilized as a service by DoIT and/or its Client Agencies containing HIPAA regulated information will incorporate this security standard. Entities may develop local security policy; however, the HIPAA Security Rule shallbe the minimum applicable standard, and local policy shall not detract from this baseline.

5. **POLICY COMPLIANCE**

Compliance with this Policy is accomplished through established procedures and designation of responsibility to specific personnel/job titles. To the extent necessary, each agency, board, and commission shall establish policies, standards, and procedures in accordance with this Policy.

6. **APPLICABLE LAWS, GUIDELINES, OR SOURCES**

HIPAA Security Rule

Revision history and approvals are reflected in ServiceNow.

Enterprise Information Security Policy
Physical and Environmental Protection Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for protecting information technology (IT) assets and the premises in which they reside. This Policy addresses the establishment and implementation for protecting IT assets from physical and environmental threats in order to reduce the risk of loss, theft, accidental damage, or unauthorized access to those IT assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to protect IT assets by limiting and controlling physical access and implementing controls to protect the physical environment in which State of Illinois IT assets are housed.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Physical Access Authorization

- 4.1.1 Agency shall develop, approve, and maintain an authorized access list of individuals with authorized access to the facility where the Information System resides.
- 4.1.2 Agency shall issue authorization credentials for access to the facility.
- 4.1.3 Agency shall review the access list detailing authorized facility access by individuals.
- 4.1.4 Agency shall remove individuals from the facility access list when access is no longer required.

4.2 Physical Access Control

- 4.2.1 Agency shall enforce physical access authorizations at defined entry/exit points to facilities where the Information Systems reside.
- (1) Agency shall verify individual access authorization before granting access to the facility.
- (2) Agency shall control ingress/egress to the facility.
- 4.2.2 Agency shall maintain physical access audit logs for defined entry/exit points.
- 4.2.3 Agency shall provide defined security safeguards to control access to areas within the facility officially designated as publicly accessible.
- 4.2.4 Agency shall monitor visitor activity.
- 4.2.5 Agency shall secure keys, combinations, and other physical access devices.
- 4.2.6 Agency shall inventory defined physical access devices on a defined frequency.
- 4.2.7 Agency shall change combinations and keys on a defined frequency and/or when keys are lost,

combinations are compromised, or individuals are transferred or terminated.

4.3 Access Control for Transmission Medium

4.3.1 Agency shall control physical access to defined Information System distribution and transmission lines within facilities using physical safeguards.

4.4 Access Control for Output Devices

4.4.1 Agency shall control physical access to Information System output devices to prevent unauthorized individuals from obtaining the output.

4.5 Monitoring Physical Access

4.5.1 Agency shall monitor physical access to the facility where information resides to detect and respond to physical security incidents.

4.5.2 Agency shall review physical access logs on a defined frequency and upon the occurrence and/or indication of adverse events.

4.5.3 Agency shall review and investigate physical security incidents through a formally developed response process.

4.6 Visitor Access Records

4.6.1 Agency shall maintain visitor access records to the facility where the Information System resides for a defined time period.

4.6.2 Agency shall review access records on a defined frequency.

4.7 Power Equipment and Cabling

4.7.1 Agency shall protect power equipment and power cabling for the Information System from damage and destruction.

4.8 Emergency Shutoff

4.8.2 Agency shall provide the capability of shutting off power to the Information System or individual system components in emergency situations.

4.8.3 Agency shall place emergency shutoff switches or devices to facilitate safe and easy access for personnel.

4.8.4 Agency shall protect emergency power shutoff capability from unauthorized activation.

4.9 Emergency Power

4.9.1 Agency shall provide short-term, uninterruptible power supply to allow for an orderly shutdown of the Information System in the event of a primary power source failure.

4.9.2 Agency shall provide long-term, alternate power supply for the Information System that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

4.10 Emergency Lighting

4.10.1 Agency shall employ and maintain automatic emergency lighting that activates in the event of a power disruption and covers emergency exits and evacuation routes within the facility.

4.11 Fire Protection

4.11.1 Agency shall employ and maintain system fire suppression and detection devices/systems for facilities containing concentrations of Information System resources that are supported by an independent energy source.

4.12 Temperature and Humidity Controls

4.12.1 Agency shall maintain appropriate temperature and humidity levels within the facility where the Information System resides.

4.12.2 Agency shall monitor temperature and humidity levels.

4.13 Water Damage Protection

4.13.1 Agency shall protect facilities containing concentrations of Information System resources from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

4.14 Delivery and Removal

4.14.1 Agency shall authorize, monitor, and control defined types of Information System components entering and exiting the facility and shall maintain records of those items.

4.15 Alternate Work Site

4.15.1 Agency shall employ defined security controls at alternate work sites.

4.15.2 Agency shall assess, as feasible, the effectiveness of security controls at alternate work sites.

4.15.3 Agency shall provide a means for Employees to communicate with information security personnel in case of security incidents or problems.

4.16 Location of Information System Components

4.16.1 Agency shall position Information System components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 Employees 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Privacy: Accountability, Audit, and Risk Management

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will protect the confidentiality of Personally Identifiable Information (PII) by establishing minimum baseline controls that reduce the risk of adverse events associated with privacy and confidentiality. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to integrate the privacy, accountability, audit, and risk management requirements as part of data collection to mitigate risk and effectively manage information.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1. Governance & Privacy Program

Agency shall:

- appoint individuals accountable for developing, implementing, and maintaining an Agency-wide governance and privacy program to ensure compliance with applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII.
- monitor privacy laws and Agency policies for changes that affect the privacy program.
- allocate sufficient resources to implement and operate the Agency-wide privacy program.
- develop a strategic privacy plan for implementing applicable privacy controls, policies, and procedures.
- develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, Information Systems, or technologies involving PII.
- update privacy plan, policies, and procedures on a defined frequency.

4.2. Privacy Impact and Risk Assessment

4.2.1. Agency shall develop and implement a privacy risk management process that assesses privacy risk for the collection, sharing, storing, transmitting, use, and disposal of PII.

4.2.2. Agency shall conduct Privacy Impact Assessments (PIAs) for Information Systems, programs, or other activities that pose a privacy risk in accordance with applicable law or respective Agencies' policies and procedures.

4.3. Privacy Requirements for Contractors And Service Providers

4.3.1. Agency shall include privacy requirements within contractual agreements for contractors and service providers.

4.4. Privacy Monitoring and Auditing

4.4.1. Agency shall monitor and audit privacy controls and internal privacy policies to ensure effective implementation.

4.5. Privacy Awareness and Training

4.5.1. Agency shall develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that Employees understand privacy responsibilities and procedures.

4.5.2. Agency shall administer basic privacy training annually.

4.5.3. Agency shall administer additional role-based training as required by federal, state, and Agency guidelines.

4.5.4. Agency shall ensure that Employees certify (manually or electronically) acceptance of responsibilities for privacy requirements.

4.6. Privacy Reporting

4.6.1. Agency shall develop, disseminate, and update reports to senior management and other Employees with responsibility for monitoring privacy program progress and compliance to demonstrate accountability with specific statutory and regulatory privacy program mandates.

4.7. Privacy-Enhanced System Design and Development

4.7.1. Agency shall design Information Systems to support privacy by automating privacy controls.

4.8. Accounting of Disclosures

4.8.1. Agency shall keep an accurate accounting of disclosures of information held in each system of records under its control, including:

- date, nature, and purpose of each disclosure of a record; and
- name and address of the person or Agency to which the disclosure was made.

4.8.2. Agency shall retain the accounting of disclosures according to defined retention requirements.

4.8.3. Agency shall make the accounting of disclosures available to the person named in the record upon request.

5. 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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Privacy: Data Minimization and Retention

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will protect the integrity of Personally Identifiable Information (PII) from unnecessary collection and will ensure that all collected PII is disposed of in a secure and timely manner. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to implement data minimization and retention standards for the collection, use, and retention of PII.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Minimization of PII

4.1.1 Agency shall identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.

4.1.2 Agency shall limit the collection and retention of PII to the minimum elements identified for the purposes described in an applicable privacy notice and for which the individual has provided consent.

4.1.3 Agency shall conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings to ensure that (i) only PII identified in an applicable privacy notice is collected and retained, and (ii) the PII continues to be necessary to accomplish the legally authorized purpose.

4.2 Data Retention and Disposal

4.2.1 Agency shall retain each collection of PII for a time period that fulfills the purpose(s) identified in an applicable privacy notice or as required by law.

4.2.2 Agency shall dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with an approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

4.2.3 Agency shall use defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

4.3 Minimization of PII Used in Testing, Training, and Research

4.3.1 Agency shall develop policies and procedures that minimize the use of PII for testing, training, and research.

4.3.2 Agency shall implement controls to protect PII used for testing, training, and research.

5. 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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy

Privacy: Data Quality and Integrity Policy

1. **OVERVIEW**

The State of Illinois Department of Innovation & Technology (DoIT) strives to enhance public confidence that any Personally Identifiable Information (PII) collected and maintained by the State of Illinois and its agencies, boards, and commissions is accurate, relevant, timely, and complete for the purpose for which the information is to be used. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. **GOAL**

The goal of this Policy is to maximize the quality, value, objectivity, and integrity of PII that the State of Illinois and its agencies, boards, and commissions collect.

3. **SCOPE**

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. **REQUIREMENTS**

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Data Quality

- 4.1.1 Agency shall confirm, to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.
- 4.1.2 Agency shall collect PII directly from the individual to the greatest extent practicable.
- 4.1.3 Agency shall check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems on a defined frequency.
- 4.1.4 Agency shall issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

4.2 Data Integrity

- 4.2.1 Agency shall document processes to ensure the integrity of PII through existing security controls.
- 4.2.2 Agency's Legal Office shall review and approve Computer Matching Agreements.

5. **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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Privacy: Security

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes appropriate and effective privacy security controls to protect, limit, or contain the impact of any incident involving a breach of Personally Identifiable Information (PII). Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

This Policy protects and ensures the proper handling of PII and provides effective responses to privacy incidents and breaches.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Inventory of Personally Identifiable Information (PII)

4.1.1 Agency shall establish, maintain, and update, on a defined frequency, an inventory that contains a listing of all programs and Information Systems identified as collecting, using, maintaining, or sharing PII.

4.1.2 Agency shall provide updates of the PII inventory to its Agency Chief Information Officer or information security official to support the establishment of information security requirements for all new or modified Information Systems containing PII.

4.2 Privacy Incident Response

4.2.1 Agency shall develop and implement a Privacy Incident Response Plan.

4.2.2 Agency shall provide an organized and effective response to privacy incidents and breaches in accordance with the Privacy Incident Response Plan.

5. 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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

Revision history and approvals are reflected in ServiceNow.

Enterprise Information Security Policy

Privacy: Transparency, Authority, and Purpose

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes and maintains transparency standards to provide public notice of its information practices of its programs and activities. This Policy provides Employees with an understanding of their role in communicating and notifying various audiences how Personally Identifiable Information (PII) is created, managed, and stored in the DoIT environment. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

This Policy ensures that the State of Illinois provides public notice of its information practices of its programs and activities.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Purpose Specification

4.1.1 Agency shall describe in its privacy notices the purpose(s) for which PII is collected, used, maintained, and shared.

4.2 Privacy Notice

4.2.1 Agency shall provide notice to the public and to individuals regarding:

- its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
- its authority for collecting PII;
- the choices, if any, individuals may have regarding how the State of Illinois uses PII, as well as the consequences of exercising or not exercising those choices;
- the ability to access PII and to have PII amended or corrected, if necessary;
- the PII that the State of Illinois collects and the purpose(s) for which it collects that information;
- how the State of Illinois uses PII internally;

- whether the State of Illinois shares PII with external entities, the categories of those entities, and the purposes for such sharing;
- whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
- how individuals may obtain access to PII; and
- how the PII will be protected.

4.2.2 Agency shall revise public notices to reflect changes in practice or policy that affect PII or changes in Agency activities that impact privacy, before or as soon as practicable after the change.

4.3 Privacy Statements and System of Record Notification

4.3.1 Agencies shall have an indexing or retrieval capability built into the systems containing PII.

4.3.2 Agency shall include privacy statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

4.4 Dissemination of Privacy Program Information

4.4.1 Agency shall ensure that the public has access to information about the Agency's privacy activities, and Agency shall ensure that the public is able to communicate with its Agency Privacy Officer.

4.4.2 Agency shall ensure that its privacy practices are publicly available through Agency websites or otherwise.

5. 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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Privacy: Use Limitation

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) ensures that the Personally Identifiable Information (PII) that it collects is only used in a manner that is compatible with the specific purposes for which it was collected, or as permitted by law. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure that PII collected by the State of Illinois is only used for the intended, authorized purpose(s).

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Internal Use

4.1.1 Agency shall use PII internally only in the following manners: (i) for the authorized purpose(s) identified in federal and state laws and regulations; (ii) as described in the Agency's notice(s); and/or (iii) for a purpose compatible with the purposes in 4.1.1(i) and 4.1.1(ii).

4.2 Information Sharing with Third Parties

4.2.1 Agency shall share PII externally only in the following manners: (i) for the authorized purposes identified in federal and state laws and regulations; (ii) as described in the Agency's notice(s); and/or (iii) for a purpose compatible with the purposes in 4.2.1(i) and 4.2.1(ii).

4.2.2 Where appropriate, Agency shall enter into agreements with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.

4.2.3 Agency shall monitor, audit, and train staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

4.2.4 Agency shall evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

5. 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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Program Management Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) Program Management Policy coordinates activities to manage risk to an acceptable level and to provide protection of State of Illinois information assets utilizing Defense in Depth. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to protect State of Illinois information and Information Systems, to reduce cyber risk through sound risk management practices, and to provide best-in-class enterprise information security program capabilities to Illinois agencies, boards, and commissions.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Information Security Program Plan

4.1.1 Agency shall develop and disseminate an information security program plan that:

(1) provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

(2) includes the identification and assignment of roles, responsibilities, management commitment, coordination, and compliance;

(3) reflects coordination and responsibility for the different aspects of information security (i.e., technical, physical, personnel, and cyber-physical); and

(4) is approved by senior officials with responsibility and accountability for the reduction of risk to operations and mission objectives.

4.1.2 Agency shall review the security program plan based on a defined frequency.

4.1.3 Agency shall update the plan to address changes and problems identified during plan implementation or security control assessments.

4.1.4 Agency shall protect the information security program plan from unauthorized disclosure and modification.

4.2 Senior Information Security Officer

4.2.1 Agency shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an information security program.

4.3 Information Security Resources

4.3.1 Agency shall ensure that appropriate information security resources are allocated to implement the information security program.

4.4 Plan of Action and Milestones Process

4.4.1 Agency shall implement a process for ensuring that a Plan of Action and Milestones (POAM) or a Corrective Action Plan (CAP) is developed and maintained for the security program and associated Information Systems.

(1) Agency shall document the remedial information security actions to adequately respond to risk to operations and assets, individuals, and other organizations.

4.4.2 Agency shall review POAMs and CAPs for consistency with the risk management strategy and priorities for risk response.

4.5 Information System Inventory

4.5.1 Agency shall develop and maintain an inventory of Information Systems.

4.6 Information Security Measures of Performance

4.6.1 Agency shall develop, monitor, and report on the results of information security measures of performance.

4.7 Enterprise Architecture

4.7.1 Agency shall develop enterprise architecture with consideration for information security and the resulting risk to operations, assets, individuals, and other organizations.

4.8 Critical Infrastructure Plan

4.8.1 Agency shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resource continuity plan.

4.9 Risk Management Strategy

4.9.1 Agency shall develop a comprehensive strategy to manage risk.

(1) Agency shall implement the risk management strategy.

(2) Agency shall review and update the risk management strategy based on a defined frequency or as necessary to address risk.

4.10 Security Authorization Process

4.10.1 Agency shall manage (i.e., document, track, and report) the level of security on Information Systems and the environments in which those systems operate through security authorization processes.

(1) Agency shall designate individuals to fulfill specific roles and responsibilities within the risk management process.

(2) Agency shall fully integrate the security authorization processes into its management program.

4.11 Mission/Business Process Definition

4.11.1 Agency shall define mission/business processes with consideration for information security and the resulting risk to operations, assets, individuals, and other organizations.

4.11.2 Agency shall determine information protection needs arising from the defined mission/business processes and shall revise the processes as necessary, until achievable protection needs are obtained.

4.12 Insider Threat Program

4.12.1 Agency shall implement an insider threat program that includes a cross-discipline, insider threat incident handling team.

4.13 Information Security Workforce

4.13.1 Agency shall establish an information security workforce development and improvement program.

4.14 Testing, Training, and Monitoring

4.14.1 Agency shall implement a process for ensuring that Agency plans for conducting security testing, training, and monitoring activities associated with Information Systems are developed and maintained, and that they continue to be executed in a timely manner.

4.14.2 Agency shall review testing, training, and monitoring plans for consistency with the Agency's risk management strategy and priorities for risk response actions.

4.15 Contacts with Security Groups and Associations

4.15.1 Agency shall establish and institutionalize contact with selected groups and associations within the security community to facilitate ongoing security education and training for personnel.

4.15.2 Agency shall remain current with recommended security practices, techniques, and technologies.

4.15.3 Agency shall share current security-related information including threats, vulnerabilities, and incidents.

4.16 Threat Awareness Programs

4.16.1 Agency shall implement a threat awareness program that includes information-sharing capabilities.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 all Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Risk Assessment

1. Overview

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for securing State of Illinois information technology (IT) assets from unauthorized access, modification, disclosure, and destruction. This Risk Assessment Policy addresses the establishment of policies and procedures for the effective implementation of selected security controls and control enhancements in the Risk Management Program. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure that State of Illinois Information Systems are categorized and vulnerabilities are identified in order to allow management to make informed decisions.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

DoIT shall conduct all risk assessments.

4.1 Security Categorization

4.1.1 DoIT shall categorize information and the Information System in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.1.2 DoIT shall document the security categorization results (including supporting rationale) in the security plan for the Information System.

4.1.3 DoIT shall ensure that Agency senior management and appropriate designees review and approve the security categorization decision.

4.2 Risk Assessment

4.2.1 DoIT shall conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the Information System and the information it processes, stores, or transmits.

4.2.2 DoIT shall document risk assessment results and prepare a risk assessment report.

4.2.3 DoIT shall review risk assessment results.

4.2.4 DoIT shall disseminate risk assessment results to Agency senior management and appropriate designees.

4.2.5 DoIT shall update the risk assessment whenever there are significant changes to the Information System or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

4.3 Vulnerability Scanning

4.3.1 DoIT shall obtain authorization to scan for vulnerabilities in the Information Systems and hosted applications to identify threats.

4.3.2 DoIT shall employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
(1) enumerating platforms, software flaws, and improper configurations;
(2) formatting checklists and test procedures; and
(3) measuring vulnerability impact.

4.3.3 DoIT shall analyze vulnerability scan reports and results from security control assessments.

4.3.4 DoIT shall remediate legitimate vulnerabilities in accordance with an Agency assessment of risk.

4.3.5 DoIT shall share information obtained from the vulnerability scanning process and security control assessments with Agency senior management and appropriate designees to help eliminate similar vulnerabilities in other Information Systems (i.e., systemic weaknesses or deficiencies).

5. 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 Employees 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes the requirements for security assessment and authorization to ensure that necessary security controls are integrated into systems and processes. Security assessments allow management to assess existing risk and ensure that security and privacy controls have been implemented. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to establish a security assessment and authorization capability throughout State of Illinois agencies, boards and commissions. Specifically, this Policy will support the implementation of security best practices.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Security Assessments

4.1.1. Agency shall develop a security assessment plan that describes the scope of the assessment, including:

- security and privacy controls and control enhancements under assessment;
- assessment procedures to be used to determine control effectiveness; and
- assessment environment, assessment team, and assessment roles and responsibilities.

4.1.2. Agency shall assess the security controls in the Information System and its environment of operation within an established timeframe to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

4.1.3. Agency shall produce a security assessment report that documents the results of the assessment.

4.1.4. Agency shall formally provide the results of the security control assessment to Agency senior management.

4.2. Information System Connections

This control applies to dedicated connections between Information Systems and does not apply to transitory, user-controlled connections such as email and website browsing.

4.2.1. Connections from the Information System to other Information Systems outside of the authorization boundary must be authorized by Agency senior management through the use of Interconnection Security Agreements (ISAs).

- If the connecting systems have the same Authorizing Official, an ISA is not required.

Rather, the interface characteristics between the connecting Information Systems must be described in the security plans for the respective systems. Instead of developing an ISA, Agencies may choose to incorporate this information into a formal contract.

- If the connecting systems have different Authorizing Officials, but the Authorizing Officials are in the same Agency, DoIT shall determine whether an ISA is required, or alternatively, the interface characteristics between the connecting Information Systems must be described in the security plans for the respective systems.

4.2.2. For every Sensitive Agency Information System that shares data with non-State of Illinois entities, the Agency shall require or shall specify via written agreement (an ISA) that its service provider comply with the following requirements:

- The System Owner, in consultation with the Business Owner, shall document Information Systems with which data is shared. This documentation must include:
  i. the types of shared data;
  ii. the direction(s) of data flow; and
  iii. contact information for the Agency that owns the Information System with which data is shared, including the System Owner, the Information System Security Officer (ISSO), or equivalent, and the System Administrator.
- The System Owners of interconnected systems must inform one another of connections with other systems.
- The ISA shall specify if and how the shared data will be stored on each Information System.
- The ISA shall specify that System Owners of the Information Systems that share data acknowledge and agree to abide by any legal and/or regulatory requirements.
- The ISA shall specify each Business Owner's authority to approve access to the shared data.
- The System Owners shall approve and enforce the written agreement.
- Risks that may be introduced when Information Systems are connected to other systems with different security requirements and security controls must be carefully considered. The Authorizing Official shall determine the risk associated with each connection and the appropriate controls to be employed.

4.3. Security Authorization

Security authorization is the official management decision, conveyed through the authorization decision document of an Information System, explicitly accepting the risk to Agency operations.

4.3.1. For each Information System, the ISO or equivalent designee shall:

- assign a State of Illinois employee in an existing senior-level executive or managerial position to serve as the Authorizing Official;
- ensure that the Authorizing Official authorizes the Information System for processing before commencing operations; and
- update the security authorization based on a defined frequency.

4.4. Continuous Monitoring

A continuous monitoring program maintains the security authorization of an Information System.

4.4.1. The ISO or equivalent designee shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:

- a configuration management process for the Information System and its components;
- a determination of the security impact of changes to the Information System and environment of operation;
- ongoing security control assessments in accordance with the Agency's continuous monitoring strategy; and
- reporting the security state of the Information System to appropriate Agency officials.

4.4.2. The implementation of a continuous monitoring program results in ongoing updates to the security plan.

5. 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 Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Security Planning

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will ensure the protection of State of Illinois information technology (IT) assets from unauthorized access, modification, disclosure, and destruction. This Policy establishes the minimum-security requirements to ensure a consistent security baseline. This Policy also provides direction to coordinate information security program planning activities to effectively manage risk and to protect the State of Illinois information assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure that planning activities are accomplished to provide protection to the confidentiality, integrity, and availability of State of Illinois information assets.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 System Security Plan

4.1.1 Agency shall develop a security plan for the Information System that:

- is consistent with the enterprise architecture;
- explicitly defines the authorization boundary for the system;
- describes the operational context of the Information System in terms of missions and business processes;
- provides the security categorization of the Information System including supporting rationale;
- describes the operational environment for the Information System and relationships with or connections to other Information Systems;
- provides an overview of the security requirements for the system;
- identifies any relevant overlays, if applicable;
- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
- is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

4.1.2 Agency shall distribute copies of the security plan and communicate subsequent changes to the plan to the State of Illinois Chief Information Security Officer.

4.1.3 Agency shall review the security plan for the Information Systems at a defined frequency based on risk.

4.1.4 Agency shall update the plan to address changes to:

- the Information System;
- environment of operation;
- problems identified during plan implementation; and
- security control assessments.

4.1.5 Agency shall utilize Least Privilege protocol to protect the security plan from unauthorized disclosure and modification.

4.2 Information Security Architecture

4.2.1 Agency shall develop an Information Security architecture plan that:

- describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of information;
- describes how the information security architecture is integrated into and supports the enterprise architecture; and
- describes any information security assumptions about, and dependencies on, external services.

4.2.2 Agency shall review and update the information security architecture plan on a defined frequency to reflect updates in the enterprise architecture.

4.2.3 Agency shall ensure that information security architecture changes are reflected in the security plan and procurements.

5. 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 Employees 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

Enterprise Information Security Policy
System and Communications Protection

1. **OVERVIEW**

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for securing State of Illinois information technology (IT) assets from unauthorized access, modification, disclosure, and destruction. This Policy ensures Information Systems and communications are protected against security threats in transit and at rest. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. **GOAL**

The goal of this Policy is to ensure that system communications security activities are accomplished to provide protection to the confidentiality, integrity, and availability of State of Illinois information assets.

3. **SCOPE**

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. **REQUIREMENTS**

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Application Partitioning

4.1.1 Agency shall separate User functionality (including User interface services) from Information System management functionality.

4.2 Information in Shared Resources

4.2.1 Agency shall prevent unauthorized and unintended information transfer via shared system resources.

4.3 Denial of Service Protection

4.3.1 Agency shall protect against or limit the effects of denial of service attacks.

4.4 Boundary Protection

4.4.1 Agency shall monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

4.4.2 Agency shall implement subnetworks for publicly accessible system components that are separated from internal Agency networks.

4.4.3 Agency shall connect to external networks or Information Systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an Agency security architecture.

4.5 Transmission Confidentiality and Integrity

4.5.1 Agency Information System shall protect the confidentiality and integrity of transmitted information.

4.6 Network Disconnect

4.6.1 Agency Information System shall terminate the network connection associated with a communications session at the end of the session or after a defined time period of inactivity.

4.7 Cryptographic Key Establishment and Management

4.7.1 Agency shall establish and manage cryptographic keys for required cryptography employed within the Information System.

4.8 Cryptographic Protection

4.8.1 Agency shall implement cryptographic protection in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.

4.9 Collaborative Computing Devices

4.9.1 Agency shall prohibit remote activation of collaborative computing devices unless otherwise authorized.

4.9.2 Agency shall provide an explicit indication of use to Users physically present at the devices.

4.10 Public Key Infrastructure Certificates

4.10.1 Agency shall obtain and issue public key certificates from an approved service provider.

4.11 Mobile Code

4.11.1 Agency shall define acceptable and unacceptable mobile code and mobile code technologies.

4.11.2 Agency shall establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

4.11.3 Agency shall authorize, monitor, and control the use of mobile code within the Information System.

4.12 Voice Over Internet Protocol

4.12.1 Agency shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the Information System if used maliciously.

4.12.2 Agency shall authorize, monitor, and control the use of VoIP within the Information System.

4.13 Secure Name / Address Resolution Service (Authoritative Source)

4.13.1 Agency Information System shall provide additional data origin authentication and integrity verification.

4.13.2 Agency Information System shall provide the means to indicate the security status to enable verification of a chain of trust among parent and child domains.

4.14 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

4.14.1 Agency Information System shall request and perform data origin authentication and data integrity verification on the name/address resolution responses that the system receives from authoritative sources.

4.15 Architecture and Provisioning for Name / Address Resolution Service

4.15.1 Agency shall ensure that Information Systems that collectively provide name/address resolution service are fault-tolerant and implement internal/external role separation.

4.16 Session Authenticity

4.16.1 Agency Information System shall protect the authenticity of communications sessions.

4.17 Protection of Information at Rest

4.17.1 Agency Information System shall protect the confidentiality and integrity of information at rest.

4.18 Process Isolation

4.18.1 Agency Information System shall maintain a separate execution domain for each executing process.

5. 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.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
System and Information Integrity

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for protecting the integrity of systems and information through the development, implementation, documentation, and maintenance of system and information integrity controls. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure the integrity of State of Illinois data and Information Systems and to establish a consistent and enterprise-wide information security baseline.

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Flaw Remediation

4.1.1 Agency shall identify, report, and correct Information System flaws.

4.1.2 Agency shall test software and firmware updates related to flaw remediation for effectiveness and potential side effects prior to implementation.

4.1.3 DoIT shall install applicable security-related software and firmware updates in compliance with standards established by the DoIT Division of Information Security.

4.1.4 DoIT shall incorporate flaw remediation into the Information System configuration processes.

4.2 Malicious Code Protection

4.2.1 DoIT shall employ malicious code protection mechanisms at Information System entry and exit points to detect and eradicate malicious code.

4.2.2 DoIT shall update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policies, standards, and/or procedures.

4.2.3 DoIT shall configure malicious code protection mechanisms to:

- perform periodic scans of the Information Systems;
- perform real-time scans of files from external sources at endpoints;
- block and quarantine malicious code;
- alert the DoIT Division of Information Security when suspected malicious code is detected;

- address the potential impact on the confidentiality, integrity, and availability of the impacted system and information; and
- address the receipt of false positives during malicious code detection and eradication.

4.3 Information System Monitoring

4.3.1 DoIT shall monitor Information Systems to detect:
- attacks and indicators of potential attacks in accordance with continuous monitoring policies, standards, and procedures; and
- unauthorized local, network, and remote connections.

4.3.2 DoIT shall identify unauthorized use of Information System(s) through system alerts and monitoring of system events/transactions.

4.3.3 DoIT shall deploy monitoring devices and/or capabilities strategically to collect essential information and at ad hoc locations to track specific types of transactions in support of attack detection and incident response.

4.3.4 DoIT shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

4.3.5 DoIT shall heighten the level of Information System monitoring activity whenever there is an indication of increased risk to Agency operations and assets, individuals, the State of Illinois, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

4.3.6 DoIT shall perform Information System monitoring activities in accordance with applicable laws, regulations, orders, directives, or policies.

4.3.7 Agency shall alert information security response personnel in line with established policies, standards, and plans when indications of compromise occur.

4.3.8 DoIT shall monitor inbound and outbound communications traffic on an ongoing basis to guard against unusual or unauthorized activities or conditions.

4.4 Security Alerts, Advisories, and Directives

4.4.1 Agency shall receive information security alerts, advisories, and directives on an ongoing basis from external organizations such as the Illinois Statewide Terrorism Intelligence Center, the United States Computer Emergency Readiness Team (US-CERT), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Department of Homeland Security (DHS).

4.4.2 Agency shall review the information security alerts or advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

4.4.3 Agency shall generate internal security alerts, advisories, and directives as deemed necessary.

4.4.4 Agency shall disseminate security alerts, advisories, and directives to personnel responsible for implementing, monitoring, and managing the Information System.

4.5 Spam Protection

4.5.1 DoIT shall employ spam protection mechanisms at Information System entry and exit points to detect and take action on unsolicited messages.

4.5.2 DoIT shall automatically update spam protection mechanisms when new releases are available.

4.6 Information Input Validation

4.6.1 Agency's Information Systems shall validate inputs to match specified definitions for format and content to ensure the confidentiality, integrity, and availability of the data.

4.7 Error Handling

4.7.1 Agency's Information Systems shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

4.7.2 Agency's Information Systems shall reveal error messages only to authorized personnel.

4.8 Information Handling and Retention

4.8.1 Agency's Information Systems shall handle and retain information within the system and output from the system in accordance with applicable laws, regulations, orders, directives, or policies.

5. 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
System and Services Acquisition

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will protect the integrity of systems and information through the development, implementation, documentation, and maintenance of the below system and services acquisition requirements. This Policy defines the criteria and methods for managing risks associated with third-party products and service providers. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure consistent application of security controls across all State of Illinois systems during the procurement process.

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Allocation of Resources

4.1.1 Agency shall determine information security requirements for the Information System or Information System service in mission/business process planning.

4.1.2 Agency shall determine, document, and allocate the resources required to protect the Information System or Information System service as part of its capital planning and investment control process.

4.1.3 Agency shall establish a discrete line item for information security in programming and budgeting documentation.

4.2 System Development Lifecycle

4.2.1 Agency shall manage the Information System using the DoIT-defined system development life cycle methodology that incorporates information security considerations.

4.2.2 Agency shall define and document information security roles and responsibilities throughout the system development life cycle.

4.2.3 Agency shall identify individuals having information security roles and responsibilities.

4.2.4 Agency shall integrate the information security risk management process into system development life cycle activities.

4.3 Acquisition Process

4.3.1 The following requirements, descriptions, and criteria, explicitly or by reference, will be included in the acquisition contract for the Information System, system component, or Information System service in accordance with applicable laws, executive orders, directives, policies, regulations, standards, guidelines, and as applicable to the Agency's mission/business needs:

- security functional requirements;
- security strength requirements;
- security assurance requirements;
- security-related documentation requirements;
- requirements for protecting security-related documentation;
- description of the Information System development environment and environment in which the system is intended to operate; and
- acceptance criteria.

4.4 Information System Documentation

4.4.1 Agency shall obtain administrator documentation for the Information System, system component, or Information System service that describes:

- secure configuration, installation, and operation of the system, component, or service;
- effective use and maintenance of security functions/mechanisms; and
- known vulnerabilities regarding configuration and use of administrative functions.

4.4.2 Agency shall obtain user documentation for the Information System, system component, or Information System service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
- User responsibilities in maintaining the security of the system, component, or service.

4.4.3 Agency shall document each attempt to obtain Information System, component, or Information System service documentation, when unavailable.

4.4.4 Agency shall protect documentation as required, in accordance with Least Privilege risk management strategy.

4.4.5 Agency shall distribute documentation to appropriate personnel.

4.5 Security Engineering Principles

4.5.1 DoIT shall apply Information System security engineering principles in the specification, design, development, implementation, and modification of the Information System.

4.6 External Information System Services

4.6.1 Agency shall require that providers of external Information System services comply with DoIT information security requirements and employ security controls in accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.

4.6.2 Agency shall define and document oversight, User roles, and responsibilities.

4.6.3 Agency shall employ DoIT processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

4.7 Developer Configuration Management

4.7.1 Agency shall require the developer of the Information System, system component, or Information System service to:

- perform configuration management during system, component, or service for design, development, implementation, and operation;
- document, manage, and control the integrity of changes to configuration items under configuration management;
- implement only approved changes to the system, component, or service;
- document approved changes to the system, component, or service and the potential security impacts of such changes; and
- track security flaws and flaw resolution within the system, component, or service and report findings to appropriate personnel.

4.8 Developer Security Testing and Evaluation

4.8.1 Agency shall require the developer of the Information System, system component, or Information System service to:

- create and implement a security assessment plan;
- perform testing/evaluation per business requirements;
- produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- implement a verifiable flaw remediation process; and
- correct flaws identified during security testing/evaluation.

5. 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.

State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
System Maintenance

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of appropriate system maintenance controls that safeguard the confidentiality, integrity, and availability of Information Systems. This Policy alleviates security risks by managing risks from information asset maintenance and repairs through the establishment of an effective system maintenance program. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to protect State of Illinois Information Systems by establishing the minimum requirements for system maintenance.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Controlled Maintenance

4.1.1 Agency shall schedule, perform, document, and review records of maintenance and repairs on Information System components in accordance with manufacturer or vendor specifications and/or Agency requirements.

4.1.2 Agency shall approve and monitor all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.

4.1.3 Agency shall require that defined personnel explicitly approve the removal of the Information System or system components from Agency facilities for off-site maintenance or repairs.

4.1.4 Agency shall sanitize equipment to remove all information from associated media prior to removal from Agency facilities for off-site maintenance or repairs.

4.1.5 DoIT shall test potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

4.1.6 Agency shall maintain system maintenance records.

4.2 Maintenance Tools

4.2.1 DoIT shall approve, control, and monitor Information System maintenance tools.

4.3 Non-Local Maintenance

4.3.1 Agency shall approve and monitor non-local maintenance and diagnostic activities.
4.3.2 DoIT shall approve the use of non-local maintenance and diagnostic tools.
4.3.3 DoIT shall employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.
4.3.4 DoIT shall maintain records for non-local maintenance and diagnostic activities.
4.3.5 DoIT shall terminate session and network connections when non-local maintenance is completed.

4.4 Maintenance Personnel

4.4.1 Agency shall establish a process for maintenance personnel authorization and shall maintain a list of authorized maintenance organizations or personnel.
4.4.2 Agency shall ensure that personnel performing maintenance on the Information System have required access authorizations and are supervised.

4.5 Timely Maintenance

4.5.1 Agency shall obtain maintenance support and/or spare parts for key components as defined in service agreements.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 all Employees 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 Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.