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.