



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-10-15-2014

DIVISION OF INFORMATION TECHNOLOGY

Network and Communications Security Policy

Date of Last Revision 07/31/2014

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Background

- a. Network security is critical to maintaining business data. However, many organizational networks are a patchwork of local area networks that run various technological platforms and require different solutions. As a result, maintaining an adequate information security posture is difficult. Because no single solution is able to provide absolute security against all types of threats, many organizations utilize the concept of defense in-depth to mitigate these limitations inherent within all security technologies. This strategy implements layers of security technologies to increase the odds that a security breach in one layer is caught within another layer and, thereby, reduce organizational risk.

2. Purpose

- a. To establish policy for implementing effective system and communications security over IT system resources and to ensure the confidentiality, integrity, and availability of transmitted data.

3. Scope

- a. This policy covers all State Executive Branch Departments¹ (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

4. Authority

- a. Executive Order 04-06 established the Division of Information Technology (DoIT) within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

- a. **Collaborative Computing** - A multifaceted group-oriented, and distributed environment with many users and shared resources and devices that enables multiple parties to

collaborate on textual and graphical documents. Examples include audio and visual conferencing capabilities and their networked devices, such as cameras, microphones, and white boards.

- b. Communication Session** - The entirety of a data transmission from start to end.
- c. Cryptography** - Securing information in such a manner that ensures its confidentiality and integrity (e.g. encryption).
- d. Domain Name Service (DNS)** - A hierarchal distributed naming system that provides domain name and address resolution, essentially translating a domain name to its numerical TCP/IP address, and is critical to the functionality of any IT system resource connected to the internet or within a private network.
- e. Internet Telephony** - Hardware and/or software that allow a broad range of services traditionally performed over telephone lines (e.g., transmitting voice, video, and data) to be performed over the internet.
- f. Mobile Code** - Software downloaded from remote systems and executed locally on servers and workstations, often without the user's explicit authorization, knowledge, or awareness. Mobile code is also referred to as executable or active content. Examples include Java Applets, ActiveX, Flash, JScript, VBScript, VBA, macros, content embedded within emails and web pages, etc.
- g. Public Key Infrastructure (PKI)** - Enables data to be transferred privately and securely over a public network (e.g., internet) through the use of public and private key certificates obtained from trusted authorities.
- h. Partitioning** - The process of separating and dividing roles, responsibilities, and functions.
- i. Perimeter Security** - Devices or systems that exist at the edge of infrastructure and are considered a first line of defense from external attack.
- j. Wireless** - Also known as "wifi", is an implementation of local area network over radio frequency.
- k. Waiver** - A dispensation from policy due to extenuating circumstances.

6. Policy

a. Partitioning

- (i.)** Information system management functionality will be partitioned and separate from non-privileged user functionality.
- (ii.)** Information system security functions will be isolated from non-security functions.
- (iii.)** Publicly accessible information system resources will be physically and logically separate from the internal network. The internal network will be secured and protected from untrusted external networks at all times.

b. Shared Resources

- (i.) Information systems will prevent the unauthorized or unintentional transfer of information via shared system resources.
- (ii.) Collaborative computing devices will be disabled and/or physically disconnected from the network until ready for use.
- (iii.) Information systems will prevent collaborative computing devices from being remotely activated without prior authorization.
- (iv.) Information systems will provide an explicit indication to local users that collaborative computing devices are active and in use.

c. Perimeter Security

- (i.) Information systems will connect to external networks only via managed perimeter security devices.
- (ii.) Communications at information system perimeters and critical internal boundaries will be monitored and controlled.
- (iii.) Information systems will protect against and limit the effects of denial of service attacks.

d. Data Security

- (i.) Data will be appropriately secured at all times, including when at rest, while processing, and during transmission, to ensure its confidentiality and integrity.
- (ii.) Cryptography controls will be implemented where appropriate and as required in accordance with applicable federal and State laws, Executive Orders, policies, regulations, compliance requirements, and standards.
- (iii.) Procedures will be developed for obtaining, issuing, and managing cryptographic keys and public key certificates.

e. Communications Sessions

- (i.) Network connections associated with communications sessions will automatically terminate at the end of the session or after a period of inactivity.
- (ii.) Information systems will protect the authenticity of communications sessions.

f. Domain Name Service (DNS)

- (i.) DNS will provide the security status of child subspaces. If the child supports secure resolution services, DNS will enable the verification of the chain of trust among parent and child domains.
- (ii.) DNS will be fault tolerant and have an internal/external role structure for processing name and address resolution requests.

g. Mobile Code

- (i.) Acceptable and unacceptable mobile code will be defined.
- (ii.) Mobile code access and usage restrictions will be established.

- (iii.) The use of mobile code within information system resources will be authorized, monitored, and controlled.
- h. Internet Telephony.** Internet telephony access will be authorized, monitored, and controlled, and usage restrictions will be established.
- i. Wireless Access.** Wireless access will be authorized, monitored, and controlled, and usage restrictions will be established.
- j. Policy Issuance.** This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be amended or revoked.
- k. Policy Reviews.** This policy will be reviewed annually and updated as required.
- l. Noncompliance.** Any/ person or entity that violates this policy may be subject to disciplinary action up to and including termination.
- m. Waivers.** The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason for the waiver, whichever occurs first, whereupon they must be renewed.

7. Roles and Responsibilities

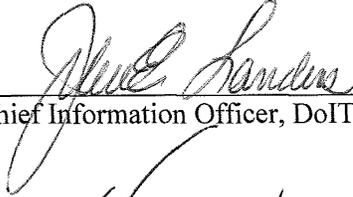
a. *Chief Information Security Officer*

- (i.) Periodically review this policy and update as required.
- (ii.) Perform periodic audits to ensure compliance with this policy.
- (iii.) Review requests for external connections to the internal network.

b. *Agencies*

- (i.) Comply with provisions documented in this policy.
- (ii.) Obtain approval from DoIT prior to connecting to the external network.
- (iii.) Periodically review external connections to the internal network.

8. Signatures



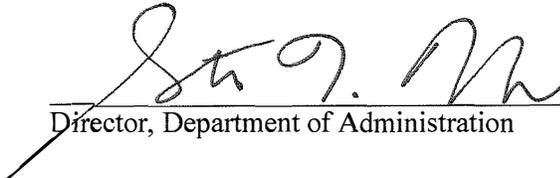
Chief Information Officer, DoIT

11/25/2014
Date



Chief Information Security Officer, DoIT

11/24/2014
Date



Director, Department of Administration

12-~~12~~3-14
Date