



GDOT Publications

Policies & Procedures

Policy: 8068-1- Network Security Controls and Remote Access

Section: Network Security

Office/Department: Information Technology

Reports To: Deputy Commissioner

Contact: 404-631-1000

PURPOSE

This document sets the IT policy to establish multiple layers of network security controls along with network security best practices for GDOT information systems to minimize the risks of attack or compromise while providing acceptable functionality and performance. It also sets the IT policy to implement security controls on public access, web facing systems.

SCOPE

This policy applies to all GDOT Offices and Districts.

RESPONSIBILITY

1. The IT Director/CIO retains authority for enforcement and monitoring of this policy.
2. The IT Director/CIO is responsible for designating a person to serve this function in case of absence or emergency.
3. The Administrator of the IT Office of Infrastructure is responsible for compliance with the policy, updates to the policy, monitoring, and enforcing the policy.
4. In the absence of the IT Office of Infrastructure administrator, the Assistant Administrator of the Office of Infrastructure is responsible for compliance with the policy and for reporting concerns to the IT Director/Chief Information Officer.

POLICY STATEMENT

- GDOT shall implement a defense-in-depth strategy and network security best practices for securing the information technology networks that they operate. These strategies shall provide protection for the network communications and infrastructure, network boundary, and access to the computing environment (hosts/servers, etc) while still providing acceptable functionality and performance
- GDOT's web facing public access systems shall provide desired services and functionality with security controls that protect the interests of the users and the confidentiality, integrity, and availability of web servers, applications and data as well as the network infrastructure that supports them.
- GDOT shall assess the risks and establish policies that explicitly define the architecture, methods, rules, procedures, and expectations for all forms of remote access to non-public state information systems, to include, but not limited to, wireless, mobile computing and teleworking systems.

Policy: 8068-1 - Network Security Controls and Remote Access

Date Last Reviewed: 8/22/2013

Page 1 of 12

Network Access and Session Control

- Unless specifically designated as a public information system, access to GDOT network and its resources shall require the use of agency issued identification and authentication credentials.
- Access and use of GDOT networks shall be in accordance with the appropriate use and access control related agency policies and standards.
- Only the minimum required network service access points shall be enabled and exposed.
- When allowing remote access to non-public state information systems, GDOT shall conduct a risk analysis to determine the access/connection methods that best supports the required security levels.
- Anti-virus protection and perimeter controls shall be properly configured
- GDOT shall ensure that remote users are aware of their roles and responsibilities for maintaining the security requirements of state information assets and adhering to security policies when they are away from GDOT controlled facilities. Users shall acknowledge (in writing) their understanding of these policies and be held accountable.
- GDOT shall establish and enforce network session controls that define rules and conditions for network connections
 - SESSION LOCK - All systems, network and/or applications, used to process, store, or transfer data with a security categorization of MODERATE or higher shall automatically initiate a session/screen lock after a limited period of inactivity, not to exceed 15 (fifteen) minutes, that remains in effect until the user re-establishes access using appropriate identification and authentication.
 - SESSION TERMINATE - All remote access networked sessions and public facing applications requiring a logon must automatically TERMINATE the connection after an inactivity timeout not to exceed 15 (fifteen) minutes. The user must provide appropriate identification and authentication to re-establish the connection.
- Access to and interconnections with State networks from external networks and systems shall occur through controlled interfaces.
- Network Access accounts will be managed as follows:
 - The Office of IT Infrastructure will generate a monthly report of all GDOT network accounts that have been inactive for 30 days and these accounts will be immediately disabled.
 - All passwords expire after 30 days.
 - State Of GDOT Employee:
 - State employee accounts will be neither disabled nor deleted until information technology receives a termination notification from PeopleSoft through EDW.
 - Consultant & Vendor AD Accounts in GDOT-AD and GADOT Domain:
 - The Office of IT Infrastructure will generate a periodic report on network accounts of all GDOT Consultant & Vendor AD Accounts in GDOT-AD and GADOT Domain that have been inactive for 45 days. Users of inactive accounts will be notified via email to remedy the disable status, and the accounts will be put on "pending disable action". Once notified, the user will have 15 days to remedy the disable status.
 - Accounts that have been inactive for over 60 days will be automatically disabled. Owners of disabled accounts will be notified via email to remedy the disable status, and the accounts will be put on "pending deletion action". Once notified, the user will have 15 days to remedy the disabled status.
 - Accounts that have been inactive for 75 days will be automatically deleted.
 - Administrative Special Circumstances.
 - Accounts will immediately be disabled when a vendor or consultant separates from GDOT.
 - The business unit will work closely with the Division of Information Technology to address and manage any business needs associated with accounts being disabled /deleted.

Network Security-Boundary Protection

- GDOT shall establish controls that monitor and control the flow of information within and at the external boundary of the information systems and networks they operate. GDOT shall designate an individual responsible for managing and administering network boundary protection strategies (e.g. firewalls and other boundary protection devices).
- Boundary Protection strategies shall include but are not limited to:
 - **Physical Security:** GDOT shall employ due diligence in ensuring physical security at any location where boundary protection devices are installed.
 - **Access Control:** All access to GDOT information systems and networks shall be controlled and monitored in accordance with GDOT access control policies and standards.
 - **Interconnections:** All connections to information systems outside the security boundary of GDOT's information system or the state backbone (internet, or other external network or information system) shall be fully documented, authorized, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) and be continuously monitored. Network traffic filtering rules that traverses the internet shall include the following:
 1. An incoming packet shall not have a source address of the internal network
 2. An incoming packet shall not contain Internet Control Message Protocol (ICMP) traffic
 3. An incoming packet shall have a publicly registered destination address associated with the internal network if using static or dynamic Network Address Translation (NAT)
 4. An incoming packet should not contain Simple Network Management Protocol (SNMP) traffic
 5. An outgoing packet shall have a source address of the internal network
 6. An outgoing packet shall not have a destination address of the internal network
 7. An incoming or outgoing packet shall not have a source or destination address that is private or listed in RFC 1918-reserved space
 8. Sources of traffic from Internet sites that are known to contain spam, offensive material, etc., shall be blocked
- **Least Functionality:** Network boundary control devices shall be configured to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services. When required to allow converged services, such as voice (VoIP), instant messaging, presence, mobility services, multimedia (MoIP), etc., to securely traverse network borders and NAT functionality, firewall technologies shall be one of the following:
 - Use a SIP proxy server or H.323 gatekeeper outside the firewall, with the firewall configured to allow communication of endpoints only with the proxy server
 - Be configured to function as application-layer gateways that monitor all SIP and H.323 traffic in order to open and close restricted ports as required and rewrite the IP addresses within the unencrypted application-layer messages
 - Use a Session Border Controller, also known as an application router, to allow for end-to-end VoIP communications across multiple IP networks while allowing VoIP endpoints such as VoIP gateways, IP phones, and IP soft phones; which are behind a Network Address Translation (NAT) firewall, to communicate with VoIP endpoints on external IP networks.
- **Default Denial:** GDOT firewalls shall block every network connectivity path and network service not explicitly authorized by the Agency CIO.
 - Any source routed packets or any packets with the IP options field set shall be blocked.
 - Inbound or outbound traffic containing source or destination addresses of 127.0.0.1 or 0.0.0.0, or directed broadcast addresses should be blocked.

- **Configuration Changes and Documentation:** All changes to firewall configuration parameters, enabled services, and permitted connectivity shall be authorized by the CIO, and documented in accordance with change control policies and procedures. Privileges to modify the functionality, connectivity, configuration and services supported by firewalls shall be restricted to the designated firewall administrator(s); GDOT ISO and/or other authorized designee(s).

Destruction of hardcopy and electronic documentation of network device configurations, network diagrams, etc., shall be destroyed, when superseded, or no longer needed. Such destruction may be completed on-site by the use of a commercial strength document shredder and/or the use of a secure recycling container. The secure container shall contain a pad lock or other similar locking mechanism and the contents of the container must be securely disposed of either through the document shredder and/or recycled by a third party contractor to destroy such documentation.

- **Firewall Monitoring and Logs:** GDOT shall continuously monitor boundary protection devices for suspicious activity and inappropriate use, and utilize the firewall logging capabilities in accordance with the log management policies and standards.
 - Firewall technologies shall have security logging turned on. Logs should be reviewed, on a frequency determined and documented by the GDOT authorized personnel and all incidents and violations reported shall be resolved in a timely manner.
 - Remote management of firewall technologies shall be via encrypted communications.
- **Denial of Service; intrusion detection and malicious code:** GDOT shall ensure boundary protection controls protect and monitor the network against malicious code, denial of service, intrusions, and other hacking attacks. Systems categorized as MODERATE or higher shall alert parties responsible for monitoring or responding when these suspicious conditions exist.
- **Record Retention:** All documentation and/or firewall logs shall be retained in accordance with GDOT's respective retention policies and schedules. No specific retention requirements are set forth by these Standards.
- **Periodic Review:** Firewall configurations shall be reviewed to ensure compliance to agency or State security policies. Supporting documentation shall exist for all enabled services. GDOT is responsible for testing their firewall configurations for effectiveness.
- **Security Updates:** GDOT personnel responsible for managing firewalls will subscribe to security advisories and other relevant sources providing up-to-date information about firewall vulnerabilities and apply relevant patches, updates and/or other recommended protective actions.
- **Contingency Planning:** GDOT shall take appropriate measures to ensure that operational failures of boundary protection mechanisms do not result in unauthorized releases of information outside the information system boundary. Firewall configurations shall be backed up fully, a redundancy and failover strategy shall be employed and alternate processing sites shall provide the same levels of protection as the primary site.
- **Access to Internetworking Devices and Shared Platforms:** Internetworking devices (including routers, firewalls, switches, etc.) and shared platforms (including mainframes, servers, etc.) provide both access to and information about networks. They shall be controlled to prevent unauthorized access.
 - Access to Internetworking devices and shared platforms shall be restricted to authorized employees and contractors in accordance with GDOT personnel policy.
 - Access to network management tools such as Simple Network Management Protocol (SNMP), Secure Socket Shell (SSH), and Remote Monitoring (RMON), etc., as well as telnet access, shall be controlled.
 - Internetworking devices connected to the Internet shall have RFC 1918 and RFC 2827 implemented for inbound traffic.
 - If dial-in access is required to access and manage routers, RADIUS should be used.

- Internetworking devices shall have unneeded services turned off, unused ports disabled, and logging capability turned on. Logs should be reviewed, on a frequency determined and documented by the GDOT authorized personnel, and all incidents and violations reported shall be resolved in a timely manner.
- Internetworking device passwords shall be immediately changed before or upon device installation and shall conform to GDOT specific password criteria.
- Internetworking devices shall be configured to retain their current configuration, security settings, passwords, etc., during a reset or reboot process.
- When disposing of internetworking devices that are no longer used by the GDOT, all configuration information shall be cleared to prevent disclosure of network configuration, keys, passwords, etc.
- Designated networking, server and application unit employees or contractors shall proactively monitor and address software vulnerabilities of all internetworking devices (routers, firewalls, switches, servers, etc) by ensuring that applicable patches are acquired, tested, and installed in a timely manner.
- Patches make changes to the configuration of an internetworking device designed to protect and secure internetworking devices and attached IT devices and systems from attack, and shall be controlled and documented in accordance with GDOT Configuration Management procedures.
- GDOT shall provide tele-workers (remote) users with secure login, connection procedures and instructions to securely access internal systems.
- GDOT shall provide teleworkers and remote users with the requirements, guidance and recommendations for ensuring that remote/telework sites, remote access devices and user behavior uphold the physical and technical security requirements and policies for internal systems and mobile data.
- When teleworking and remote access to internal, non-public state information systems is permitted, GDOT shall develop remote access security plans that explicitly define the architecture, methods, rules, procedures, and expectations for all forms of remote access to non-public state information systems.

Web and E-Commerce Security

- GDOT shall properly plan for and address information security requirements prior to deploying an internet based web server and/or web services.
- GDOT shall have a secure network infrastructure that physically allocates publicly accessible information system components (e.g., public web servers) to separate sub-networks, each of which will have separate, physical network interfaces and prevents public access into the organization's internal networks (e.g. DMZ).
 - Services provided through the Internet (Web-enabled applications, FTP, Mail, DNS, VoIP, etc.) shall be deployed on a Demilitarized Zone (DMZ) or proxied from the DMZ.
 - All communication from servers on the DMZ to internal applications and services shall be controlled.
 - Remote or dial-in access to networks shall be authenticated at the firewall, or through services placed on the DMZ.
 - The DMZ is the appropriate location for web servers, external DNS servers, Virtual Private Networks (VPNs), and dial-in servers.
 - GDOT's external DNS servers should neither be primary servers nor permit zone transfers to DNS servers outside of the GDOT.
 - All remote access users shall be considered external and therefore should be subjected to the firewall rule set. VPNs should terminate on the external segment or outside of the firewall.

- GDOT shall standardize secure operating system and application configurations, deployment and maintenance strategies. External connections to networks shall be routed through secure gateways and protected by at least one of the following encryption methods, as appropriate:
 - Secure Socket Layer (SSL) shall be employed between a web server and browser to authenticate the web server and, optionally, the user's browser. Implementation of SSL shall allow for client authentication support using the services provided by Certificate Authorities.
 - Wireless Transaction Layer Security (WTLS) with strong authentication and encryption shall be used between a web server and the browser of a wireless mobile device, such as a cellular telephone, PDA, etc., to provide sufficient levels of security during data transmission. WTLS currently supports X.509, X9.68 and WTLS certificates.
 - IP Security (IPSec) shall be used to extend the IP communications protocol, providing end-to-end confidentiality for data packets traveling over the Internet. The appropriate mode of IPSec shall be used commensurate with the level of security required for the data being transmitted: sender authentication and integrity without confidentiality or sender authentication and integrity with confidentiality.
 - VPNs shall be used to connect two networks or trading partners that must communicate over insecure networks, such as the public Internet, by establishing a secure link, typically between firewalls, using a version of the IPSec security protocol. VPNs are recommended for use in remote access.
 - Remote Authentication Dial-In User Service (RADIUS) is a client/ server software protocol that enables network access servers to communicate with a central server to authenticate and authorize remote users to access systems or services; strong authentication shall be used for dial-up modem systems.
 - Dial-up desktop workstation modems should be disabled and removed. Hardware and inventory scanning tools shall be used to verify the presence and configuration of dial utilities and modems. If GDOT is using dial-up modem systems, it shall establish modem use policies which include:
 - A complete, current list of all authorized personnel having modem access privileges.
 - Automatic disconnection after a specified period of inactivity.
 - Inactivity parameters shall be determined by the GDOT client support.
 - The recommended use of security tokens.
 - Immediate termination of modem access privileges upon employment transfer, re-assignment, or termination.
 - Strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, and smart cards, shall be used once permission to connect has been granted.
 - External connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.
 - Based on GDOT's business requirements, commercially available transport services, commonly referred to as carrier services shall be configured and implemented to allow for automatic re-routing of communications when critical nodes or links fail, or fallback to alternate transport services, including the provision of duplicate or alternate secure gateways and external exchanges or switching centers.
- Web application developer's and web master's design shall use security engineering principles in accordance with guidance provided in NIST SP 800-27 Engineering Principles for Information Technology Security.
- Ensure that only appropriate/authorized web server content is published and accessed.
- Limit user activity that does not require identification and authentication, and implement authentication and cryptographic technologies as appropriate to meet data security/privacy requirements.
- Perform logging and implement controls to prevent, monitor and respond to unauthorized modifications to web server content and applications, intrusions, malicious code, system failure or other forms of compromise. Intrusion detection

mechanisms or intrusion prevention tools shall be incorporated into all servers connected to WANs and to all internetworking devices that serve as gateways between WAN network segments

- When used, intrusion detection systems shall be installed both external and internal to firewall technology protecting the network to monitor, block, and report unauthorized activity. Logs should be reviewed by GDOT authorized personnel and all incidents and violations reported shall be resolved in a timely manner.
- Intrusion detection mechanisms for servers shall include the use of software and review procedures that scan for unauthorized changes to files, including system files.
- Software and review procedures shall examine network traffic for known, suspicious attack signatures or activities and look for network traffic indicative of devices that have been misconfigured.
- Violations of set parameters shall trigger appropriate notification to security administrators, allowing a response to be undertaken.
- Intrusion prevention tools combine user-defined security parameters with the ability to learn how software applications and operating systems should perform in their normal states to generate an appropriate set of security policies. Violations of these security policies produced through network penetration and changes in the normal state result in recognition of an attack with corresponding adjustments to stop it.
- Application Vulnerability Description Language (AVDL) is a security interoperability standard being proposed as an OASIS standard. AVDL creates a uniform way of describing application security vulnerabilities using XML. The XML-based technology will allow communication between products that find, block, fix, and report application security holes.
- Intrusion prevention technologies reduce the number of false alarms by focusing on real-time behavior rather than using signature matching technology to identify a potential network attack. Intrusion prevention technologies can also prevent attacks, which exploit previously unknown weaknesses, because they respond to a change in the normal state of operation.
- When manufacturer recommended updates/patches are applied to IDS/IPS systems that may impact end-user connectivity, notification to all impacted entities/users as to date and time shall occur prior to any updates.
- Be Payment Card Industry Data Security Standard (PCI DSS) compliant when providing on-line customer payment processing services or shall validate the PCI compliance of third-party service providers outsourced to store, process, or transmit credit card data on their behalf.

Wireless Networks Access

- The 802.1x security standards having centralized user authentication and encryption technologies with automated key distribution, and VPN technologies shall be used as appropriate with standard wireless networks: IEEE 802.11x (Wireless Local Area Network (WLAN)), IEEE 802.15 (Wireless Personal Area Network (WPAN)), and IEEE 802.16 (Wireless Metropolitan Area Network (WMAN)).
- WLAN security is being addressed in the transmission layer with the IEEE 802.11i draft standard and at the IP applications layer with standards- and policy-based authentication and access control.
- The Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11 standard, is susceptible to compromise; therefore, improved security methods should be considered through the use of AES, EAP and IPsec. All wireless data shall be encrypted.
- The Wireless Application Protocol (WAP) standard and Protected Extensible Authentication Protocol (PEAP) with the IEEE 802.1x Network Port Authentication standard provides interim, improved security until approval and widespread adoption of 802.11i.

- 802.11i also allows for automatically generated per user, per session keys through 802.1x. In addition, keys can be regenerated (re-keying) periodically to increase security.
- Vendor-specific, proprietary, security solutions may provide more enhanced interim security prior to approval and widespread adoption of 802.11i.
- Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Therefore, it is important that GDOT IT assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

Wireless Access Point Device Security:

- The service set identifier (SSID) shall be changed from the factory default setting and limit their identifying information. The broadcast SSID feature should be disabled, requiring wireless clients to scan for a specific access point.
- Management access passwords must be changed from their default and default cryptographic keys shall be changed from the factory default setting. Cryptographic keys should be changed often.
 - Access point devices shall be managed via network management tools
 - Access point devices that operate with a central controller is recommended and should be turned off during off-hours when not in use.
 - Access points that access the Internet by default must reside on a VLAN. The use of VPN shall be employed when accessing internal resources.
 - Signal strength (signal-to-noise ration) of Wireless Access Points should be audited and reduced to encompass only desired areas.
- WLAN wireless client platforms connecting to GDOT networks using public access points and the Internet shall use VPN technologies and should use centrally managed individual firewall software solutions. Wireless client platforms utilizing VPN technologies to access internal networks and mission-critical software applications improve security and decrease certain vulnerabilities inherent in unprotected wireless connectivity.
- WPAN client devices used for network access, internal network-based Internet access, and application software access shall:
 - Be required to adhere to the same range of security requirements as WLAN client devices
 - Require PIN entry or similar authentication for all access
 - Require device-mutual authentication for all accesses
 - Invoke link encryption for all connections in the communication chain and encryption for all broadcast transmissions
 - Be set to the lowest necessary and sufficient power level so that transmissions remain localized
 - Require device passwords to prevent unauthorized use if lost or stolen
 - Use application-level encryption, authentication and VPN technologies
 - Be turned off during off-hours when not in use
- WMAN connectivity, commonly used to interconnect buildings, to internal networks that include transmissions to access internal networks and mission-critical software applications shall be encrypted and use VPN technologies.
- Passwords for wireless devices shall conform to GDOT specific password criteria.
- Firewall technologies implemented at wireless application gateways and connection points between wireless and wire-based LANs additionally reduce unauthorized access to internal networks.

SUPPORTING DOCUMENTS

<http://csrc.nist.gov/publications/nistpubs>

Doc ID: GTA Policy No. P-08-027.01 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Network Security Controls

Effective Date: 03/20/2008

Doc ID: GTA Policy No. P-08-028.01 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Public Access Systems

Effective Date: 03/20/2008

Doc ID: GTA Policy No. P-08-023.01 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Remote Access

Effective Date: 03/20/2008

Doc ID: GTA Standard No. S-08-048.01 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Network Security Controls

Effective Date: 03/31/2008

Doc ID: GTA Standard No. S-08-047.01 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Network Security Controls

Effective Date: 03/31/2008

Doc ID: GTA Standard No. S-08-049.01 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Network Security Controls

Effective Date: 03/31/2008

Doc ID: NIST SP 800-44 <http://csrc.nist.gov/publications/nistpubs>

Title: Guide for Securing Public Web Servers

Effective Date: 09/01/ 2007

Doc ID: GTA Policy No. 9.4.2 9.8.1 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Access Control Wireless Network

Effective Date: 09/10/02 revised 04/13/04

Doc ID: GTA Policy No. 10.5.4 <http://gta.georgia.gov/egap/search-current-psgs>

Title: Security in Development and Support Process

Effective Date: 09/10/02 revised 04/13/04

Doc ID: NIST SP 800-96 <http://csrc.nist.gov/publications/nistpubs>

Title: Guide to Secure Web Services

Effective Date: 09/01/2006

Policy: 8068-1 - Network Security Controls and Remote Access

Date Last Reviewed: 8/22/2013

Doc ID: NIST SP 800-28 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Guidelines for Active Content and Mobile Code

Effective Date: 03/01/2008

Doc ID: NIST SP 800-27

Title: Engineering Principles for Information Technology Security

Effective Date: 06/01/2004

Doc ID: NIST SP 800-52 <https://www.pcisecuritystandards.org/>

Title: Guideline for Selection and Use of Transport Layer Security Implementation (SSL) PCI Data Security Standard

Effective Date: 06/01/2005

Doc ID: NIST SP 800-41 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Guidelines on Firewalls and Firewall Policy

Effective Date: 01/01/2002

Doc ID: NIST SP 800-94 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Guideline to Intrusion Detection and Prevention Systems

Effective Date: 02/01/2007

Doc ID: NIST SP 800-47 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Interconnecting Information Technology Systems

Effective Date: 08/01/ 2002

Doc ID: NIST SP 800-46 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Security for Telecommuting and Broadband Communications

Effective Date: 08/01/ 2002

Doc ID: NIST SP 800-114 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: User's Guide to Securing External Devices for Telework and Remote Access

Effective Date: 11/01/2007

Doc ID: NIST SP800-48 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Wireless Network Security

Effective Date: 11/01/2002

Doc ID: NIST SP800-97 <http://csrc.nist.gov/publications/PubsSPs.html>

Title: Establishing Wireless Robust Security Networks

Effective Date: 02/01/2007

Policy: 8068-1 - Network Security Controls and Remote Access

Date Last Reviewed: 8/22/2013

DEFINITIONS

Defense-in Depth – An Information Assurance (IA) “best practices” strategy for protecting networked environments where multiple layers of security defenses (policy, personnel, technology and operations) are placed throughout a network infrastructure to protect internal data, systems, networks, and users such that if one mechanism fails, another will already be in place to continue to protect the assets.

Controlled Interfaces - Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels).

Demilitarized Zone (DMZ) - A host or network segment inserted as a “neutral zone” between an organization’s private network and the Internet.

Web Server - A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an “intranet server”

Webmaster - A person responsible for the implementation of a Web site. Webmasters should be proficient in HTML and one or more scripting and interface languages, such as JavaScript and Perl. They may or may not be responsible for the underlying server.

Information System (hereafter referred to as ‘system’) - A discrete set of information resources (workstations, servers, applications, network, etc) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

System Boundary – All the components of an information system or an interconnected set of information resources under the same direct management control and security support structure, that share common functionality (normally includes hardware, software, information, data, applications, communications, and people).

Boundary Protection (or perimeter defense) – Tools and techniques used to manage, control and protect the security objectives of information stored, processed and transmitted within and between network boundaries; such as but not limited to controlled interfaces, intrusion detection, anti-virus, network forensic analysis, log monitoring.

Controlled Interfaces - Mechanisms that facilitate the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels).

Network Session – Refers to a lasting connection in a network protocol or between a user (or user agent) and a peer, typically a server, usually involving the exchange of many packets between the user’s computer and the server.

Remote Access - The ability of an organization’s users to access its non-public computing resources from locations other than the organization’s facilities.

Telework or Telecommute - The ability of an organization's employees and contractors to conduct work from locations other than the organization's facilities.

Mobile Computing - A generic term describing one's ability to use technology 'untethered', that is not physically connected, or in remote or mobile (non-static) environments.

References:

History:

Policy approval error out--restarted workflow 8/20/13

Updated policy content on 8/12/13

Reviewed: 8/22/2013