INFORMATION TECHNOLOGY SECURITY POLICY

2400.25

4.0 OPERATIONAL POLICIES

4.1 Personnel

HUD systems face threats from many sources, including the actions of HUD employees, external users, and contractor personnel. The intentional and unintentional actions of these individuals can potentially harm or disrupt HUD systems and their facilities. These actions can result in the destruction or modification of the data being processed, denial of service (DoS) to the end users, and unauthorized disclosure of data, potentially jeopardizing HUD's mission. Therefore, it is highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

HUD Policy

a. Program Offices shall designate the position sensitivity level for all government positions that use, develop, operate, or maintain IT systems under their purview and shall determine risk levels for each contractor position in accordance with the Office of Personnel Management (OPM) policy and guidance. Position sensitivity levels and risk levels shall be reviewed periodically in accordance with OPM guidance.

b. Program Offices shall ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position's sensitivity levels. Screening shall be consistent with: (i) 5 Code of Federal Regulations (CFR) 731.106(a); (ii) OPM policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and its attendant SP 800-73 and 800-76; and (v) the criteria established for the risk designation of the assigned position.

c. Program Offices/System Owners shall ensure that no employee is granted access to HUD systems without having a favorably adjudicated Minimum Background Investigation (MBI), as defined in HUD's Personnel Security Program for systems under their purview.

d. Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems under their purview without having a favorably adjudicated background Investigation, as defined in HUD's Handbook 732.3, Personnel Security/Suitability. Exceptions may be granted by the CISO.

e. Program Offices/System Owners shall ensure that no government employee is granted access to HUD systems processing sensitive information under their purview who is not a citizen of the United States. Exceptions may be granted at the Program Office level and must be reported to the CISO and the security officer.

f. Program Offices/System Owners shall ensure that no contractor employee is granted access to HUD systems processing sensitive information under their purview who is not a citizen of the United States, a national of the United States (see 8 U.S.C. 1408), or an alien lawfully admitted to the United States for permanent residence. Exceptions may be granted at the Program Office level and reported to the CISO and the security officer.

4.1.1 Rules of Behavior

Rules of behavior are part of a comprehensive program to provide complete information security guidelines. The rules of behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful Information Security Program. These guidelines are established to hold users accountable for their actions and responsible for IT security.

HUD Policy

a. The CISO shall define generic rules of behavior for all IT systems.

b. Program Offices/System Owners shall define additional rules of behavior for all IT systems under their purview, when necessary.

c. ISSOs shall ensure that users of systems sign the rules of behavior and are given training regarding the rules of behavior and the disciplinary actions that may result if the rules are violated.

4.1.2 Access to Sensitive Information

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege must be applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed to perform authorized tasks (i.e., users should be able to access only the system resources needed to fulfill their job responsibilities).

The application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know.

HUD Policy

a. Program Offices/System Owners shall ensure that users of IT systems supporting their programs have a validated requirement to access these systems.

b. Program Offices/System Owners shall ensure that users of IT systems under their purview have approved access requests prior to granting access to the systems.

4.1.3 Separation of Duties Policy

Separation of duties is designed to prevent a single individual from being able to disrupt or corrupt a critical security process. This separation is necessary for adequate internal control of sensitive IT systems.

HUD Policy

a. Program Offices/System Owners shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

4.1.4 Training and Awareness

A key objective of an effective Information Security Program is to ensure that all employees and contractors understand their roles and responsibilities and are adequately trained to perform them. HUD cannot protect the confidentiality, integrity, and availability of its IT systems and the information they contain without the knowledge and active participation of its employees and contractors in the implementation of sound security principles.

HUD Policy

a. The CISO shall establish an IT security awareness and training program in accordance with NIST 800 SP 800-50, Building an Information Technology Security Awareness and Training Program. The program shall be consistent with CFR 930.301.

b. Program Offices/System Owners shall establish additional system-specific security training for sensitive systems under their purview, when necessary.

c. Program Offices/System Owners shall ensure that HUD personnel and contractors accessing HUD IT systems receive initial training in security awareness and accepted security practices as part of their orientation. They shall sign the rules of behavior and receive refresher training by May 31 of each year.

d. Program Offices/System Owners shall ensure that HUD personnel and contractors with significant security responsibilities (e.g., ISSOs and system administrators) receive annual specialized training specific to their security responsibilities. The level of training shall be commensurate with the individual's duties and responsibilities and promote a consistent understanding of the principles and concepts of IT system security.

e. Program Offices shall maintain training records that include the individual names and positions, types of training received, and cost of training.

f. Unless a waiver is granted by the CISO, user accounts and access privileges, including access to email, will be disabled for those HUD employees who have not received annual refresher training.

g. Program Offices shall prepare and submit an IT Security Professional Training Plan to the CISO by September 1 of each year.

h. Program Offices shall prepare and submit awareness and training statistics semiannually to the CISO. These statistics shall include the (1) total number of personnel and the total number of personnel who received awareness training and (2) total number of IT security personnel and the total number who were trained.

4.1.5 Separation from Duty

This section addresses HUD's policy for an employee or contractor who terminates employment or transfers to another organization.

HUD Policy

a. Program Offices/System Owners shall implement procedures to ensure that system accesses are revoked or reassigned when HUD or contractor employees either change their employer or are reassigned to other duties. The procedures shall include:

Exit interviews

Process for returning all organizational information and system-related property (e.g., keys and ID cards)

Access by appropriate personnel to official records created by the terminated/transferred employee/contractor that are stored on organizational information systems

Formal notification to the facilities group or security officer

4.2 IT Physical Security

HUD security personnel and users must address physical security as an integral element in the effective implementation of an Information Security Program. Physical security represents the first line of defense against intruders and adversaries attempting to gain access to HUD facilities and or information systems.

4.2.1 General Physical Access

General physical access controls restrict the entry and exit of personnel from a protected area, such as an office building, data center, or room containing IT equipment. They include the protection of sensitive data and systems while in rest, as well as while away from the protection of HUD facilities. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business hours and at other times. Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

Homeland Security Presidential Directive 12 mandates government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees). Program Offices responsible for issuing ID badges at HUD shall consult FIPS 201 and its attendant SP 800-73 and SP 800-76 for specific guidance.

HUD Policy

a. The facilities group or security officer shall ensure that access to HUD buildings, rooms, work areas, and spaces is limited to authorized personnel. Controls shall be in place for deterring, detecting, monitoring, restricting, and regulating access to specific areas at all times.

b. The facilities group or security officer shall ensure that all visitors sign in and out when entering and leaving the facility. Visitor logs shall be reviewed at closeout, maintained on file, and available for further review for one year. Contractors' access shall be limited to those work areas requiring their presence. Records of their ingress and egress shall also be maintained for one year. For systems rated moderate or high, the maintenance and review of access logs shall use automated mechanisms.

c. For systems rated moderate or high, the facilities group or security officer shall ensure that all visitors are escorted.

d. For systems rated moderate or high, individuals within HUD shall employ appropriate security controls at alternate work sites in accordance with NIST SP 800-46, Security for Telecommuting and Broadband Communications. These individuals shall report security problems to HUD's Computer Security Incident Response Center (CSIRC).

e. Program Offices and users shall ensure that unattended laptops in offices are secured via a locking cable, locked office, or a locked cabinet or desk.

4.2.2 Facilities Housing Information Technology Assets

Facilities supporting large-scale IT operations (e.g., enterprise servers and telecommunication facilities) require additional environmental and physical controls as determined by a risk analysis. Section 4.2.1 provides policies for both general physical access and sensitive facilities. For facilities supporting large-scale IT operations, all of the following physical security controls also must be addressed. The risk assessment shall specifically document the rationale for not incorporating any such physical security controls.

HUD Policy

a. The Deputy CIO for IT Operations shall ensure that facilities processing, transmitting, or storing sensitive information incorporate physical protection measures. These facilities include data centers, wiring closets, server rooms at non-HUD facilities, contractor facilities housing HUD IT systems, and in some cases, areas designated as publicly accessible inside HUD facilities.

b. The facilities group or security officer shall ensure that lists of personnel authorized to access these facilities are current and shall issue appropriate credentials. Access shall be promptly removed for personnel no longer needing it.

c. The Official responsible for approving initial access to these facilities shall review and approve access lists and authorization credentials once a year.

d. The facilities group or security officer shall control all access points with physical access devices and/or guards. Keys, combinations, and other access devices shall be secured and inventoried every six months and changed any time the keys are lost, combinations are compromised, or individuals are terminated or transferred.

e. The facilities group or security officer shall develop and implement procedures to ensure that only authorized individuals can reenter the facility after emergency-related events.

f. For systems rated moderate or high, the Program Offices/System Owners shall ensure that physical access to devices displaying information is controlled to prevent unauthorized disclosure.

g. The facilities group or security officer shall monitor physical access to detect and respond to incidents. Logs shall be reviewed daily for apparent security violations or suspicious activities and responded to accordingly. For systems rated moderate or high, the monitoring shall be in real-time for intrusion alarms and surveillance equipment. For systems rated high, the monitoring shall use automated mechanisms to recognize intrusions and to take appropriate action.

h. For systems rated moderate or high, the facilities group or security officer shall ensure that power equipment and cabling are protected from damage and destruction.

i. For specific locations within a facility containing concentrations of information system resources (e.g., data centers and server rooms), the facilities group or security officer shall provide for the capability of shutting off power to any IT component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

j. For specific locations within a facility containing concentrations of information system resources (e.g., data centers and server rooms), the facilities group or security officer shall maintain a redundant air-cooling system.

k. The facilities group or security officer shall provide short-term UPS to facilitate an orderly shutdown in the event of a primary power source loss.

l. The facilities group or security officer shall provide a long-term alternate power supply to maintain minimal operational capability for systems rated moderate or high in the event of an extended loss of the primary power source.

m. The facilities group or security officer shall provide automatic emergency lighting systems that activate in the event of a power outage or disruption and cover emergency exits and evacuation routes.

n. The facilities group or security officer shall provide fire suppression and detection devices/systems that can be activated in the event of fire. The devices/systems shall include, but are not limited to:

- Sprinkler systems
- Handheld fire extinguishers
- Fixed fire hoses
- Smoke detectors

o. For systems rated moderate or high, the facilities group or security officer shall provide fire suppression devices/systems that activate automatically in the event of fire.

p. For systems rated high, the facilities group or security officer shall provide fire suppression devices/systems that automatically notify any activation to the organization and emergency responders in the event of fire.

q. The facilities group or security officer shall ensure that facilities containing information systems monitor and maintain acceptable levels of temperature and humidity.

r. The facilities group or security officer shall ensure that the information systems contained in the facility are protected from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. For systems rated high, the shutoff shall use automatic mechanisms in the event of a significant water leak.

s. The facilities group or security officer shall ensure that the facility has procedures to control the entering and exiting of information system-related items and maintains appropriate records. Delivery and removal of these items shall be authorized by an appropriate HUD official. If possible, the delivery area shall be separate from the system and media library area.

4.3 Media Controls

Information resides in many forms and can be stored in many different ways. Media controls are protective measures specifically designed to safeguard electronic data and hardcopy information. This policy addresses the protection, marking, sanitization, production input/output, and disposal of media containing sensitive information. Media destruction and disposal should be accomplished in an environmentally approved manner. The National Security Agency (NSA) provides media destruction guidance at http://www.nsa.gov/ia/government/mdg.cfm.

Proper storage of hardcopy and magnetic media enhances protection against unauthorized disclosure. There are additional security risks associated with the portability of removable storage media. Loss, theft, or physical damage to disks and other removable media can compromise the confidentiality, integrity, or availability of the data contained in these devices.

HUD Policy

a. Program Offices/System Owners shall establish procedures to ensure that sensitive information in printed form or digital media cannot be accessed, removed, or stolen by unauthorized individuals.

b. Program Offices/System Owners and users shall ensure that all media containing sensitive information rated moderate or high is appropriately marked with the sensitivity of the information stored on the media. At a minimum, printed output that is not otherwise appropriately marked shall have a cover sheet and digital media shall be labeled with the distribution limitations, handling caveats, and applicable security markings, if any, of the information. Systems rated high shall use an automated marking mechanism.

c. Program Offices/System Owners and users shall control access to and securely store all information system media (i.e., both paper and digital) containing sensitive information rated moderate or high, including backup and removable media, in a secure location when not in use.

The following policy statements apply only to media that contain information that has been rated moderate or high.

d. Program Offices/System Owners shall ensure that any sensitive information stored on media that will be surplused or returned to the manufacturer shall be purged from the media before disposal.

e. Disposal shall be performed using approved sanitization methods in accordance with NIST SP 800-36, Guide to Selecting Information Security Products.

f. Program Offices/System Owners shall maintain records certifying that such sanitization was performed.

g. Program Offices/System Owners shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor.

h. Program Offices/System Owners shall ensure that sensitive information is purged from the hard drives of any workstation or server returned to the equipment surplus pool or transferred to another individual.

i. Program Offices/System Owners shall ensure that media (e.g., paper, diskettes, and removable disk drives) containing sensitive information is destroyed in such a manner that all sensitive information on that media cannot be recovered by ordinary means. Examples of appropriate methods are crosscut shredders, degaussing, and approved disk-wiping software.

j. Program Offices/System Owners shall maintain records certifying that such destruction was performed.

k. Program Offices/System Owners shall establish procedures to ensure that sensitive information in printed form or digital media can only be picked up, received, transferred, or delivered to authorized individuals.

The following policy statements apply only to media that contain information that has been rated high.

l. Program Offices/System Owners shall ensure that access to media storage areas is controlled through guard stations or automated mechanisms that ensure only authorized access. All access and access attempts shall be audited.

4.4 Data Communications

4.4.1 Telecommunications Protection Techniques

Extreme caution should be exercised when telecommunications protection techniques (e.g., protective distribution systems) are being considered as alternatives to the use of encryption. While such technologies may represent a lower-cost approach, they may not provide an adequate level of protection.

The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

HUD Policy

a. Program Offices/System Owners shall ensure that the integrity of the information in systems under their purview is protected during transmission. For systems rated high, the system shall employ cryptographic mechanisms to ensure recognition of changes to information during transmission, unless adequately protected by alternative physical measures (e.g., protective distribution systems).

b. Program Offices/System Owners shall ensure that the confidentiality of the information in systems under their purview is protected during transmission. For systems rated high, the system shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission, unless otherwise protected by adequately physical measures (e.g., protective distribution systems).

4.5 Wireless Communications

Wireless communications are inherently insecure. Program Offices/System Owners implementing wireless capabilities must ensure that the transmission and storage of sensitive information are protected from compromise.

4.5.1 Wireless Local Area Networks

HUD Policy

a. The CISO shall approve the implementation and use of all Wireless Local Area Networks (WLAN) and wireless Access Points (AP) at a specified risk level and only after they have been certified and accredited.

b. The Deputy CIO for IT Operations shall ensure that all WLANs and WAPs have been configured in accordance with NIST SP 800-48, Wireless Network Security.

c. The Deputy CIO for IT Operations shall implement encryption and strong identification and authentication (e.g., Extensible Authentication Protocol with Wi-Fi Access Protection (WAP) or IEEE 802.11i) on WLANs and APs that have been rated moderate or high.

d. The CISO shall scan for rogue access points on HUD's network annually.

4.6 Hardware and Software

This section addresses the use and maintenance of computer equipment. It stresses the importance of individual accountability in protecting these resources. Equipment security encompasses workstations, laptops, other mobile computing devices, personally-owned equipment, and the maintenance of these items.

4.6.1 Workstations

All users must be instructed to log off or lock their workstations any time the workstations are left unattended. As an added precaution, users should also use a password-protected screensaver.

HUD Policy

a. All users shall ensure that their unattended workstations are either logged off or locked, or that a password-protected screensaver is used.

b. The Deputy CIO for IT Operations shall provide and implement password-protected screen savers on all workstations owned/leased by HUD. The screen saver shall automatically lock the workstation after ten minutes of inactivity. Program Offices/System Owners of systems rated moderate to high shall require that contractors and business partners who connect to the systems implement such a screen saver.

4.6.2 Copyrighted Software

Computer software purchased using HUD funds is HUD property and shall be protected as such. Only licensed and approved operating systems and applications may be used on HUD equipment.

HUD Policy

a. Program Offices/System Owners shall ensure that users abide by copyright and contract agreements related to HUD-provided software. For software and associated documentation protected by quantity licenses, the Program Offices/System Owners shall use tracking systems to control copying and distribution.

b. Program Offices/System Owners that use peer-to-peer file sharing technology on their information system shall control and monitor its use to ensure that this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

4.6.3 User-Installed Software/Downloads

User-installed software, including downloaded software, can contain viruses and other types of malicious code. In addition, such software can alter the HUD equipment configuration causing malfunctions and costly support calls. Users should be warned about such risks and instructed to refrain from installing any software on HUD equipment without proper approval.

HUD Policy

a. Users shall not install any software on HUD-owned or leased equipment without prior written approval from the Deputy CIO for IT Operations.

4.6.4 Personally-Owned Equipment and Software

Users shall not use personally owned equipment (e.g., laptop computers or personal digital devices [PDA]) or software to process, access, or store sensitive information. Such equipment also includes plug-in and wireless peripherals (e.g., Blackberry) that may employ removable media (e.g., CDs and DVDs), Universal Serial Bus (USB) flash (thumb) drives, external drives, and diskettes.

HUD Policy

a. Users shall not use personally-owned equipment and software to process, access, or store sensitive information without prior written approval from the Program Offices/System Owners.

b. Employees and contractors shall not connect equipment not owned or leased by HUD-to-HUD equipment or networks without prior written approval from the CISO.

c. The written approval shall include a terms and conditions statement that addresses at a minimum: (i) the types of applications that can be accessed from personally-owned information systems; (ii) the maximum FIPS 199 security category of information that can processed, stored, and transmitted; (iii) how other users of the personally-owned information system will be prevented from accessing federal information; (iv) the use of virtual private network (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, and spyware definitions).

4.6.5 Hardware and Software Maintenance

Program Offices/System Owners must be cognizant of the threats and vulnerabilities associated with hardware or software maintenance on IT systems. System maintenance requires either physical or logical access to the system. One of the most common methods hackers use to break into systems is through maintenance accounts that still have factory-set or easily guessed passwords. War-dialing techniques will also reveal maintenance ports that are not protected.

HUD Policy

a. Program Offices/System Owners shall confine access to system software and hardware to authorized personnel.

b. The Deputy CIO for IT Operations shall ensure that routine preventive and regular maintenance are performed on software and hardware according to manufacturer/vendor specifications and/or organizational requirements. For systems that have been rated moderate or high a log shall be maintained for such maintenance and include the following:

  Date and time of maintenance
  Name of individual performing the maintenance

Name of escort, if necessary

Description of maintenance performed

A list of equipment removed or replaced (including identification numbers, if applicable).

For systems rated high, the Deputy CIO for IT Operations shall use an automated mechanism to ensure that the maintenance is scheduled and conducted, as required.

c. The Deputy CIO for IT Operations shall ensure that an appropriate organizational official approves the removal of the information system or its components from the facility when repairs are necessary. The Deputy CIO for IT Operations shall ensure that the security features of the system are checked to ensure proper functioning when it is returned.

d. The Deputy CIO for IT Operations shall ensure that appropriate organization officials approve, control, and monitor the use of information system maintenance tools and maintain such tools on an ongoing basis.

e. The Deputy CIO for IT Operations shall ensure that maintenance ports are disabled by default and enabled only during maintenance.

f. The Deputy CIO for IT Operations shall ensure that the appropriate organizational officials approve, control, and monitor remotely executed maintenance and diagnostic activities. The Deputy CIO for IT Operations shall ensure that all sessions are terminated when remote maintenance is completed. If password-based authentication is used, the Deputy CIO for IT Operations shall ensure that passwords are changed following each maintenance service. For high-impact systems, the Deputy CIO for IT Operations shall ensure that logs for such activities are maintained and periodically reviewed.

g. The Deputy CIO for IT Operations shall ensure that only authorized individuals perform maintenance on information systems. If maintenance personnel need access to organizational information, they must be supervised by organizational personnel with authorized access to such information.

h. The Deputy CIO for IT Operations shall identify critical components that support systems rated moderate or high and ensure that maintenance support and parts are provided within 48 hours of failure.

i. The Deputy CIO for IT Operations shall ensure that all default vendor or factory-set administrator accounts and passwords shall be changed before installation or use on all systems owned or operated on behalf of HUD.

j. Program Offices/System Owners of information systems that have been rated high shall address the installation and use of remote diagnostic links in the system security plan.

k. The Deputy CIO for IT Operations shall ensure that remote diagnostic or maintenance services for information systems that have been rated high are only performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

4.6.6 Personal Use of Government Office Equipment and HUD Information Systems/Computers

This section discusses HUD policies applicable to the personal use of government office equipment and HUD information systems. Policies governing personal use may be contained in several HUD management directives.

HUD Policy

a. HUD employees may use government office equipment and HUD information systems/computers for authorized purposes only. "Authorized use" includes limited personal use of HUD email and Internet services, so long as use does not interfere with official duties, cause degradation of network services, or violate the rules of behavior.

b. Contractors and other non-HUD employees are not authorized to use government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the governing contract or Memorandum of Agreement (MOA).

4.7 General IT Security

This section provides guidance in the areas of incident reporting, contingency planning, documentation, and backup procedures. It stresses the role of the user, as well as the security professional, in the implementation of the operational controls associated with these areas.

4.7.1 Security Incident and Violation Handling

Incidents can be accidental or malicious, can be caused by outside intruders or internal employees, and can cause significant disruptions to mission-critical business processes. These incidents can severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data.

To help combat the disruptive short- and long-term effects of security incidents, direction from higher authority (e.g., OMB, FISMA, and Presidential directives) requires that each government agency implement and maintain a security incident reporting and handling capability.

The HUD Security Incident Reporting and Handling Program requires participation by all Program Offices/System Owners; thus, a CSIRC has been established. The CSIRC is the focal point for the implementation of HUD's incident response capability.

HUD Policy

a. The CISO shall establish and maintain a HUD CSIRC to prevent, detect, track, and respond to information security incidents and alerts in accordance with NIST SP 800-61, Computer Security Incident Handling Guide. Lessons learned from ongoing incident handling activities shall be incorporated into the procedures and implemented accordingly. For systems rated moderate or high, the CISO shall provide automated mechanisms to support the incident handling process.

b. Program Offices/System Owners of systems rated moderate or high shall ensure that security alerts, advisories, Intrusion Detection System (IDS) alerts, and vulnerabilities identified during vulnerability scans and penetration tests are tracked and responded to as security incidents.

c. The Deputy CIO for IT Operations shall test patches, service packs, and hot fixes for effectiveness and potential side effects prior to installation in accordance with NIST SP 800-40, Procedures for Handling Security Patches. The Deputy CIO for IT Operations shall use automated mechanisms that require no user intervention to manage and install updates. The Deputy CIO for IT Operations shall employ an automated mechanism to determine periodically and upon demand the state of information system components with regard to flaw remediation.

d. The CSIRC, in conjunction with the Deputy CIO for IT Operations, shall provide a process to track and document information system security incidents on an ongoing basis. For systems rated high, the tracking of security incidents and the collection and analysis of incident information shall employ automated mechanisms.

e. Program Offices/System Owners shall ensure that personnel with incident response responsibilities receive training at least once a year. Incident response training for systems rated high shall incorporate simulated events to facilitate effective response by personnel in a crisis and employ automated mechanisms.

f. Program Offices/System Owners shall test the incident response capability for systems under their purview rated moderate or high once a year and document the test results. For high-impact systems the tests shall employ automated mechanisms.

g. ISSOs shall report significant computer security incidents to the CSIRC immediately upon identification and validation of the incident occurrence.

h. ISSOs shall report all incidents to the CSIRC in a Weekly Incident Report.

i. The CSIRC shall report significant computer security incidents to appropriate authorities, including the United States Computer Emergency Readiness Team (USCERT), upon identification and validation of the incident occurrence. The CSIRC shall use automated mechanisms to assist in the reporting of security incidents for systems rated moderate or high. The CSIRC shall report incident-related information to OMB, as required by FISMA.

j. The CSIRC, in conjunction with the Deputy CIO for IT Operations, shall provide users of information systems with support and assistance (e.g., help desk) for the handling and reporting of security incidents. For systems rated moderate or high, the CSIRC and the Deputy CIO for IT Operations shall employ automated mechanisms to increase the availability of incident response-related information and support.

4.7.2 Documentation

Documentation of IT systems involves the collection of detailed information, such as functionality, system mission, unique personnel requirements, type of data processed, architectural design, system interfaces, system boundaries, hardware and software components, system and network diagrams, asset costs, and system communications and facilities. This information is part of the configuration baseline of the system.

HUD Policy

a. Program Offices/System Owners shall ensure that adequate documentation for the information system and its constituent components is available, current, protected when required, and distributed to authorized personnel. Documentation includes but is not limited to:

- C&A and SDLC documentation
- Vendor-supplied documentation of purchased software and hardware
- Network diagrams
- Application documentation for in-house applications
- System build and configuration documentation, which includes

optimization of system security settings, when applicable

- User manuals
- Standard operating procedures

For systems that have been rated moderate or high, the documentation shall describe the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. For systems that have been rated high, the documentation shall describe the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls, including functional interfaces among control components.

4.7.3 Information and Data Backup

Adhering to requirements regarding data backups can significantly reduce the risk that data will be compromised or lost in the event of a disaster or other interruption of service. A Backup Operations Plan should be included in the Contingency Plan.

The development of a data backup strategy begins early in the life cycle when the security categorization of the system is first considered. Several factors derived from the risk assessment and documented in the Contingency Plan will drive the data backup strategy. Frequency of backups will depend upon how often the data processed by the system(s) changes and how important those changes are. The risk assessment will drive this element of the backup strategy. Data backups need to be stored, both onsite and offsite, in a secure facility in fireproof and waterproof containers.

HUD Policy

a. Program Offices/System Owners shall ensure that a backup strategy and procedures are established, implemented, and tested in accordance with the Contingency Plan.

b. The Deputy CIO for IT Operations shall implement and enforce backup procedures for all sensitive IT systems, data, and information. The backups shall include user-level and system-level information.

c. The Deputy CIO for IT Operations shall store backups at a secure offsite location in accordance with the Contingency Plan.

d. The Deputy CIO for IT Operations shall test backup information quarterly for systems rated moderate and high.

e. The Deputy CIO for IT Operations shall test backup information as part of contingency planning for systems rated high.

f. For systems rated high, the Deputy CIO for IT Operations shall store backup copies of the operating system and other critical information systems software in a fire-rated container that is not collocated with the operational software or in a separate facility.

4.7.4 Input/Output Controls

Many security problems start with input validation issues. Information systems that fail to validate input can introduce "buffer overflow" vulnerabilities that could be exploited by an attacker. Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, and acceptable values) should be in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure that the content is not unintentionally interpreted as commands.

On the output side, the structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators and maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages.

HUD Policy

a. For systems rated moderate or high, the Program Offices/System Owners shall ensure that the information system checks information inputs for accuracy, completeness, and validity.

b. For systems rated moderate or high, the Program Offices/System Owners shall ensure the information system identifies and handles error conditions in an expeditious manner.