

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 120

### **Title: Information Systems Security Audit and Compliance Procedures**

#### I. Applicability

These procedures establish a framework for conducting audit related reviews and compliance requirements of information resources at DHS in accordance with all applicable state and federal regulations. All DHS employees, contractors, and vendor partners must comply.

#### II. Scope

- (a) Security Audits can be conducted on any entity within DHS or any outside entity that has signed a Business Associate Agreement or Third Party Agreement with DHS. Security Audits can be conducted on any information system, to include applications, servers, networks, devices, and any process or procedure by which these systems are administered and/or maintained.
- (b) Employees, contractors, and vendor partners of DHS are subject to the policies and procedures of DHS and the Department of Information Systems. Some of those include manual or automated controls (where possible) that can result in a formal review by the DHS Chief Information Security Officer (CISO), an external auditor, or law enforcement, as appropriate.
- (c) This procedure plays a key role in security design, providing both preventative controls through alerts of suspicious activity and forensic security records of events essential for incident investigation. Capable components in the protected systems must record security relevant events, and will record events to either a local logging facility or by sending events to DHS authorized process.

#### III. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in restriction or suspension of all network access to DHS systems or applications. Employees who can't complete job duties or assignments without such access may be terminated or face disciplinary action as outlined in DHS Policies 4002 "Privacy and Security Sanctions" and 1084, "Employee Discipline."

#### IV. Procedures

- (a) All audits from external sources related to the security of systems, applications, or data are to be coordinated with the DHS IT Security Office and DHS Privacy Office prior to the audit.

- (b) The IT Security Office and the DHS Privacy Office will conduct security audits and reviews of identified systems and resources at least once a year as required by federal and state regulations and in support of assessing the security posture of the organization's critical and business systems. The IT Security Office will develop and maintain a review methodology to include the following:
  - (1) Audit/ Review approval procedures;
  - (2) Internal Inspections Plan;
  - (3) Preliminary risk analysis;
  - (4) Planning phase;
  - (5) Testing phase;
  - (6) Communicating results;
  - (7) Remediation validation; and,
  - (8) Final reporting.
- (c) Audits and reviews must be approved in writing by the DHS CISO and the CIO. In addition, detailed documentation of all audits must be produced and securely archived by the IT Security Office in compliance with DHS retention policies. Work may be performed completely in-house or by an outside firm. In addition, the IT Security Office will collect and monitor applicable log data to identify intrusion attempts and potential attacks. Audit logs will be maintained per the "Information Systems Change Management Procedure" (APM 124).
- (d) DHS entities and personnel will provide the appropriate divisions with timely and complete responses to all audit results, plans of action, milestones, and corrective action plans required.
- (e) Audits will be performed based on federal and state guidelines as needed. The baseline for compliance will be based on FISMA (NIST) and modified based on the federal and state laws that may apply to the application or division. Programs containing access to FTI data will follow the internal inspections plan at minimum of every eighteen (18) months in addition to the standard audit.
- (f) Log aggregation, correlation, alerting, and retention requirements will be met using a Security Information and Event Management (SIEM) tool. The IT Security Office includes a security component and continuity of operations component. These maintain an overview of the DHS' risks, operational issues, mitigating controls, and recovery methods including some audit related functions.

- (g) The IT Security Office will define procedures to include inspections for compliance with federal, state, and local laws and regulations based on alignment with Federal Information Management Security Act (FISMA), Internal Revenue Service (IRS) (**National Institute of Standards and Technology** (NIST) 800-53, IRS Publication 1075), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Social Security Administration (SSA), and any other system determined to hold, collect or modify protected information.
- (h) OST, Security, or System Support groups may request device specifics (such as Operating System (OS), version, and patch level) for review – especially for devices that cannot support any service account ID. The CISO must approve any additions to the system. The CIO shall be notified when operational issues may arise and before making changes within the change management process. All changes shall be approved by the CIO or designee.
- (i) Primary accounts shall be defined by the CISO and other applicable groups.
- (j) If the device supports login credentials (local or directory based [such as Active Directory or LDAP]), the entity responsible for configuring the device will include an audit service account on the device as specified below. The SIEM reports real-time events as they occur, escalating significant events to the SIEM administrators and security management. Logs from the enterprise intrusion prevention system, network class devices, server class devices, operating system related logs, application software logs and third party logs, including reputation services, are incorporated into the SIEM.
- (k) The inspection accounts shall be created on each applicable device with sufficient rights to allow review of all data on such a device via the device’s standard operating system access methods or physical environments necessary to ensure compliance. Audit and System logs will be maintained as documented per NIST requirements.
- (l) In order to meet state and federal guidelines, individuals will coordinate service accounts with the IT Security Office and other applicable support groups. All system components, including applications, databases, server operating systems, and network firewalls and proxies are required to record the following key security events to a local audit log, per the NIST security requirements for inspection:
  - (1) User account creation and deletion;
  - (2) User account enabled or disabled;
  - (3) User account modified;
  - (4) Security or audit configuration changed;
  - (5) Privileged task/command executed;
  - (6) Successful login and unsuccessful login;

- (7) Successful or unsuccessful access of protected data;
  - (8) Network packet blocked by firewall or access control list;
  - (9) System startup and shutdown;
  - (10) User permissions changed; and,
  - (11) Audit logging enabled and disabled.
- (m) For the events listed above in item (l), all systems will log the following data elements:
- (1) Event type;
  - (2) Time and date using the local system clock;
  - (3) Source of event, including source IP address, if available;
  - (4) Object of event, including destination IP address, if available;
  - (5) Outcome (success or failure); and,
  - (6) Users/subjects associated with the event (or system, if no user associated).
- (n) System components will log either to a local logging facility, or may send events to the SEIM for logging, following the format described in the SEIM section below. For local logging, use of the operating system logging facility (syslog, Windows Event log) is preferred.

## V. Vulnerability Assessment

- (a) The IT Security Office will perform vulnerability assessments on systems, applications, networks or devices where DHS data is located to the extent necessary to allow the IT Security Office or contracted company to perform the scans authorized by this procedure. DHS application owners shall provide protocols, addressing information, and network connections sufficient for auditing to utilize the software to perform network scanning.
- (b) Access may include:
  - (1) User level and/or system level access to any computing or communications device;
  - (2) Access to information (electronic, hard copy, etc.) that may be produced, transmitted or stored on DHS equipment or premise;

- (3) Access to work areas (labs, offices, cubicles, storage areas, etc.); and,
- (4) Access to interactively monitor and log traffic on DHS networks.

#### VI. Network Control

In the event DHS protected data is located outside of the DHS network, third parties will be required to perform a vulnerability assessment scan on an annual basis reporting findings to the DHS CISO and DHS Privacy Officer with a remediation plan and corrective action plan within thirty (30) days of finding the vulnerability. Failure to comply may result in loss of contract or connectivity. A risk evaluation will be performed as stated in “Information Systems Risk Management Procedures” (APM Chapter 121), to determine the risk and impact to DHS data, clients, and networks.

#### VII. Service Degradation and/or Interruptions

Network performance and/or availability may be affected by network scanning. The IT Security Office will plan accordingly to mitigate the impact to the network and the server.

#### VIII. Scanning Period

- (a) DHS Application owners and the IT Security Office shall identify in writing the allowable dates and times for audit scans and periodic scans to take place. Automated application scanning will be performed at a minimum of once every quarter. Alerts will be sent to the IT Security Office for any vulnerability found during automated alert which will be addressed per the incident response procedure.
- (b) DHS application owners shall identify in writing a person to be available if the IT Security Office or Privacy Office has questions regarding data discovered during the scan or if the offices require assistance in addressing an issue.

#### IX. Penetration Testing

Periodic penetration testing will be performed on DHS systems and applications. All scans will be non-intrusive unless approval is obtained from the application owner prior to testing. Exceptions may be made by the CIO or designee based on risk and known vulnerabilities.

#### X. Red/Blue Team Testing

DHS will build and train a group of engineers, security professionals, and developers to serve as active defense for cyber-attacks, breach evaluation, and vulnerability assessors. These teams will rotate responsibilities to build a strong skill set capable of protecting and evaluating the defense of DHS information systems. All actions will be coordinated with the divisions prior to the training or scenarios take place. Documentation of all actions will be recorded in a secured location for training purposes and all scenarios must be approved by the CIO and CISO prior to implementation.

## XI. External Audits

Audits managed by an external company will be performed annually, unless previous exclusion is given by the CIO for the fiscal year. Audits performed by other departments, agencies, or external parties shall be submitted to the IT Security Office to ensure issues are addressed to comply with state and federal regulations

## XII. Evaluation of Security and Privacy Policies and Procedures

Evaluation of Security and Privacy Policies and Procedures will be performed at minimum annually per federal and state guidelines unless significant changes are made within the annual timeframe. Policies and procedures will be evaluated based on information security measurements, performance, and documented activities.

## XIII. Other

- (a) This procedure does not replace the auditing and monitoring responsibilities of individual system administrators and data owners.
- (b) The DHS “Security Audit Process” is overseen by the IT Security Office. For information regarding the process, contact the IT Security Office.
- (c) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

## XIV. Definitions

- (a) “Entity” means any business unit, department, group, or third party, internal or external to DHS responsible for maintaining DHS assets.
- (b) “Risk” means those factors that could affect confidentiality, availability, and integrity of DHS’s key information assets and systems. The IT Security Office is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
- (c) “Security Audit” means formally testing and evaluating vulnerabilities and controls within the Information Technology environment, performed by an independent party, requiring independent corroboration (sampling in nature) to substantiate information provided by personnel.
- (d) “Security Review” means similar evaluation performed in a security audit but typically omits obtaining independent corroboration (non-sampling in nature) and testing to substantiate information provided by personnel. Security reviews may be performed in-house or outsourced to a third party.
- (e) “System Administrator” means an individual who performs network/system administration duties and or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of DHS and or third party vendors approved by IT may function as system/network administrators.
- (f) “Data Owners” means the person responsible for, or the person with administrative control over, granting access to an organization’s documents or electronic files while protecting the data as defined by the DHS

IT Security policies or standard IT practices. Data owners shall only be State Employees unless approved by the DHS CIO prior to receiving this responsibility.

- (g) “Application Owners” means the person responsible for development or management of an application containing DHS information.
- (h) “Resource” means one element of hardware, software or data that is part of a larger system.

## XV. References

- (a) Arkansas Data and System Security Classification  
[http://www.techarch.state.ar.us/domains/security/standards/SS-70-001\\_dataclass\\_standard.pdf](http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf)>
- (b) Arkansas Encryption Standard  
[http://www.techarch.state.ar.us/drafts/DRAFT\\_encryp\\_standardSS-70-006.pdf](http://www.techarch.state.ar.us/drafts/DRAFT_encryp_standardSS-70-006.pdf)>
- (c) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (d) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)  
<http://www.hhs.gov/ocr/privacy/>
- (e) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- (f) Social Security Administration Safeguards (SSA)  
<http://www.ssa.gov/dataexchange/security.html>
- (g) US Privacy Act of 1974 (Dept of State)  
<http://foia.state.gov/Learn/PrivacyAct.aspx>
- (h) Cybersecurity Enhancement Act of 2014  
<https://www.congress.gov/bill/113th-congress/senate-bill/1353>
- (i) Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/groups/SMA/fisma/>
- (j) IRS Publication 1075 (IRS), pertaining to Federal Tax Information (FTI)  
<http://www.irs.gov/pub/irs-pdf/p1075.pdf>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 121

### Title: Information System Risk Assessment and Management Procedures

#### I. Applicability

These procedures provide acceptable methods for DHS to perform required IT Security Risk Assessments for the purpose of determining areas of vulnerability and initiating appropriate remediation. These procedures are applicable to all employees, managers, and supervisors overseeing any resources owned, operated, or managed by DHS. All DHS users, employees, contractors, vendors, or others who utilize DHS IT resources are responsible for adhering to all DHS policies, including privacy and security policies (4000 and 5000 series).

#### II. Risk Assessment and Management

- (a) Risk Assessments can be conducted on any division or office within DHS and any outside entity that has signed a contract or Business Associate Agreement with DHS.
- (b) Risk Assessments can be conducted on any information system, including applications, servers and networks, and any process or procedure by which these systems are administered and/or maintained.
- (c) Any information not specifically identified as the property of other parties that is transmitted or stored on DHS IT resources, or includes information owned/managed by DHS (including e-mail, messages, files and federal or state data entrusted to DHS) is the property of DHS.
- (d) Employees are expected to cooperate fully with any Risk Assessments being conducted on systems for which they are held accountable.
- (e) Employees are further expected to work with the DHS IT Security Office and the DHS Privacy Office in the development of a remediation or corrective action plan and maintain a "Plan of Action" and "Milestone" for any issues discovered in the risk assessment process.
- (f) National Institute of Standards and Technology 800-37 framework will be complied with:
  - (1) Identification of a risk will be the responsibility of all DHS employees, contactors or third party vendors. Once a risk has been identified all individuals involved will follow the DHS Risk Management Procedure. The risk level will be defined by the Chief Information Security Officer (CISO) and the DHS Privacy Officer prior to mitigation or acceptance.

- (2) Mitigation plan for risk will be developed by the division's designee in conjunction with Security and Privacy teams and delivered to the CISO or the DHS Privacy Officer in writing for approval prior to implementation.
- (3) Acceptance of any risk with a severity level of Medium or higher will be evaluated by the Chief Information Officer (CIO) and division director of the affected divisions prior to final approval, documentation, and scheduling of periodic review of the risks.
- (g) The execution, development, and implementation of remediation programs are the joint responsibility of the CIO, CISO, the DHS Privacy Officer and the department or office responsible for the system area being assessed.
- (h) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

### III. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

### IV. Definitions

- (a) "Corrective Action Plan" means a defined process to mitigate and eliminate an identified risk.
- (b) "Entity" means any business unit, department, group, or third party, internal or external to the DHS, responsible for maintaining the DHS assets.
- (c) "Plan of Action and Milestone" means documentation to show all known issues and vulnerabilities based on criticality and impact.
- (d) "Risk" means those factors that could affect confidentiality, availability, and integrity of DHS' key information assets and systems. The Chief Information Security Officer is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

### V. References

- (a) DHS, Office of Systems and Technology, Information Technology Unit

- (b) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (c) Cybersecurity Enhancement Act of 2014  
<https://www.congress.gov/bill/113th-congress/senate-bill/1353>
- (d) FBI Criminal Justice Information Services (FBI CJIS)  
<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>
- (e) Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/groups/SMA/fisma/>
- (f) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)  
<http://www.hhs.gov/ocr/privacy/>
- (g) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- (h) IRS Publication 1075 (IRS) <http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- (i) Social Security Administration Safeguards (SSA)  
<http://www.ssa.gov/dataexchange/security.html>
- (j) US Privacy Act of 1994 (Dept of State) <http://foia.state.gov/Learn/PrivacyAct.aspx>.

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 122

### **Title: Information Systems Development & Acquisition Procedures**

#### I. Applicability

These procedures apply to all employees, divisions, offices, contractors, and vendors participating in the development and acquisition of information systems within DHS.

#### II. Procedures

- (a) The development of all requests for the acquisition of information systems technology or services (hardware, communications equipment, professional services and open market software acquisitions) will be coordinated with the DHS Chief Information Officer (CIO). The development process shall include a business evaluation and systematic selection based on defined system requirements. All such acquisitions will be reviewed by the CIO or designee and will be subject to the CIO's approval.
- (b) To ensure the security and integrity of DHS data, all software purchased or used within DHS systems shall be within the current version and two (2) revisions and updated as released. This includes supporting software such as Java, Silverlight and web browsers.
- (c) All DHS project managers and application owners will work with the DHS IT Security Office and the DHS Privacy Office during the planning, purchasing, and development phases to ensure compliance with all applicable state and federal laws. The CIO must approve all protected data integration with the system to ensure the confidentiality and integrity of the data and network.
- (d) The DHS Office of Systems Technology (OST) will coordinate the acquisition, evaluation, and selection process. The purpose of coordination is to ensure effective utilization of available DHS information hardware and network resources, to assess compatibility with current systems and architectures, and to determine the acquisition's conformance with the IT Plan and DHS' technology strategy.
- (e) There is to be no use of live data in development environments due to the significant risk involved. DHS will minimize such risk by using test data (fictional data) during the development of information systems, information system components, and information system services. Should any testing require the use of live data, the appropriate security controls (as determined by OST) must be in place to protect the data.
- (f) The IT Security Office will include safeguards including secure coding practices, configuration management and control, trusted procurement processes, and

monitoring practices to help ensure that software does not perform functions other than the functions intended.

- (g) The CIO or designee will assist the division with the business evaluation, as needed. At the CIO's discretion, Joint Application Development sessions may be required to facilitate or inform the system selection process. The CIO or designee will manage, with the requesting division's participation, the system selection process and any required Joint Application Development sessions.
- (h) The requesting division shall ensure the selected system solution is included in the current biennial IT Plan and that the planned solution does not exceed the planned cost estimate in the IT Plan. If not included in the current IT Plan or if the solution exceeds the IT Plan cost estimate, the requesting division must submit to the CIO supporting documents required to amend the IT Plan. The Department of Information Systems (DIS) shall provide technical assistance, as needed, in addressing IT Plan requirements.
- (i) Upon completion of the evaluation and selection process and obtaining the CIO's approval, OST will process the acquisition request as follows:
  - (1) OST will submit items not included within the IT Plan that require approval by the Department of Information Systems (DIS); and,
  - (2) Items approved for acquisition by DIS, and those items covered within the IT Plan, but not requiring DIS approval, will be processed by OST's purchasing agent.
- (j) The requesting division shall submit the approved acquisition request from the CIO to the DHS Office of Finance and Administration's Contract Support Section for review to ensure compliance with state contract and purchasing requirements.

### III. Service Agreements

Any service agreements with outside vendors and contractors that may require the release of protected health information requires the approval of the DHS Privacy Officer prior to activation.

### IV. Other

- (a) All requests for application development must be submitted to the CIO, with a DHS-357 "Application Development Request" form located on DHS Share at <https://dhsshare.arkansas.gov/DHS%20Forms/DHS-357.doc>.
- (b) Only Voice-over Internet Protocol (VoIP) devices that are purchased through OST shall be connected to any part of DHS' Information Systems. Before any VoIP device is purchased, it must either be on a list of DHS approved devices or must be reviewed and approved by the CIO. After a VoIP device has been purchased, it

must be registered with Unified Communications Services and connected to DHS Information Systems according to established network and security procedures. Use of VoIP devices will adhere to OST's applicable policy and procedures.

- (c) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

## V. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in restriction or suspension of all network access to DHS systems or applications. Employees who can't complete job duties or assignments without such access may be terminated or face disciplinary action as outlined in DHS Policies 4002 "Privacy and Security Sanctions" and 1084, "Employee Discipline."

## VI. Definitions

- (a) "Hardware" means desktop and laptop computer equipment, other electronic data processing equipment and peripherals, and all devices attached to the state network. This applies to leased or purchased hardware.
- (b) "Communications Hardware" means all information transmission and switching equipment and all devices attached to the state network. This applies to leased or purchased communications hardware. (Excluded for the purposes of this policy are telephones, cell phones, pagers and similar mobile devices.)
- (c) "Open Market Software" means all information technology applications and system architectures acquired from sources outside of the Department of Human Services.
- (d) "Internally Developed Applications" means all software applications developed by Department of Human Services employees and not acquired through contract or state purchasing procedures. Provisions of this policy apply explicitly to those applications developed for multi-user environments.
- (e) "Internally Developed Applications-Web Based" means all web-based applications developed by Department of Human Services employees and not acquired through contract or state purchasing procedures. For the purposes of this policy, a web-based application is defined as any file or collection of files created for live internet or intranet functionality beyond the simple posting of content.
- (f) "Software Produced by Contracted Vendor" means all software applications and system architectures developed by a vendor under the terms of an approved contract.

- (g) “Professional Services” means all Information Systems Technology professional and consulting services acquired from sources outside the requesting DHS division. (Excluded for the purposes of this policy are hardware repair services and maintenance agreement renewals.)

## VI. References

- (a) State of Arkansas Policies and Standards:  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>
- (b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001\\_dataclass\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf)
- (c) Arkansas State Security Office Data and System Classification Grid Guidelines:  
<http://www.dis.arkansas.gov/policiesStandards/Documents/DataClassificationGuide.pdf>
- (d) Arkansas State Security Office Data Classification Grid Form:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/data\\_grid.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/data_grid.pdf)
- (e) State of Arkansas Standard Statement-Encryption -Document Number: SS-70-006:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT\\_encryption\\_standard\\_2011.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT_encryption_standard_2011.pdf)
- (f) State of Arkansas Security Office Financial and Risk Impact Statement for Proposed Encryption Standard:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryption\\_financial.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryption_financial.pdf)
- (g) State of Arkansas Security Office Information on Backup Encryption Methods:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryp\\_impactinfo.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryp_impactinfo.pdf)
- (h) State of Arkansas Security Office Encryption Standard Guidelines:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/comply\\_encryp\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/comply_encryp_standard.pdf)
- (i) Department of Human Services Policy 4006: HIPAA Privacy Requirements in the Use of eMail and Facsimile Services:  
<https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx>
- (j) Department of Human Services Policy 5009: Mobile Computing and Teleworking:  
<https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx>
- (k) Department of Human Services Policy 5012: Data Classification:  
<https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx>
- (l) National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP): <http://csrc.nist.gov/groups/STM/cmvp/index.html>
- (m) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications: <http://csrc.nist.gov/publications/PubsSPs.html>
- (n) Federal Information Processing Standards Publications (FIPS PUBS):  
<http://itl.nist.gov/fipspubs/>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 123

### Title: Data Classification Procedure

#### I. Applicability

This procedure establishes and maintains a data classification mechanism that includes the determination of sensitivity, labeling, and access control of data to ensure that all DHS data is evaluated and properly classified as mandated by various federal and state regulations. This procedure applies to all employees and users granted access to DHS Information Systems or who handle DHS data.

#### II. Procedure

- (a) Data owned and maintained by DHS shall be put into appropriate classification levels according to its confidentiality, integrity, and availability. The level of security controls implemented shall be commensurate with the classification of sensitivity of the information and magnitude of loss or harm that could result from improper access.
- (b) The assigned security classifications shall be maintained by the DHS IT Security Office in a central “DHS Information Technology Information Resource Inventory.”
- (c) Procedures developed and maintained by the IT Security Office will enable the system owner, data custodian, and other key individuals to make decisions regarding the confidentiality of data. The classification will establish the general requirements for the implementation of security controls. The determination of confidentiality will be documented and maintained on file with the system owner.
- (d) The availability classification shall be determined by the system owner, based upon the overall needs of the system to be available to the department’s critical business functions. The recovery category determines how soon the application and the network should be available and online after disaster or other malfunction.

#### III. Data Classification Labeling and Access Controls

- (a) DHS divisions and offices shall implement the appropriate safeguards based on the confidentiality level of the data to include “Unrestricted,” “Sensitive,” and “Confidential.”
  - (1) “Unrestricted Data” is characterized as public data with no distribution limitations. These data elements are from information that is actively made public by the state government. It is published and distributed without restriction. It is available in the form of physical documents such as brochures, formal statements, press releases, reports and in electronic forms such as internet web pages and bulletin boards. This information is accessible

with anonymous access. The greatest security threat to this data is from unauthorized or unintentional alteration, distortion or destruction of the data. Security efforts appropriate to the criticality of systems containing this data must be taken to maintain its integrity (e.g. DHS Public Websites);

- (2) “Sensitive Data” is data elements of information that is made available through open records requests, formal or legal processes. Sensitive data is intended for use only by individuals who require the information in the course of performing their duties. Redaction of data elements is required for this level of information if released. Security threats to this data include violations of privacy statutes or federal regulations, in addition to unauthorized alteration or destruction. If this data was accessed by unauthorized persons, it could cause financial loss, identity theft, or breach of protected information (e.g. Personnel Records, IP Addresses, Emergency Contact Information, Application Source Code, Security Video Footage, Communications Systems, and Competitive Bids); and,
  - (3) “Confidential Information” is data whose disclosure could be hazardous to the health of citizens or a breach to DHS applications or network. This category includes the majority of the data contained within the DHS network. These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health, or safety repercussions. Strict rules must be followed in the usage of this data (e.g. Health Information, Personally Identifiable Information, Law Enforcement Investigative records, Educational Records, Audit responses, Social Security Numbers, Federal Tax Information and Adoption Records).
- (b) DHS divisions and offices shall implement the appropriate classification level for data and systems according to these criticality levels:
- (1) Non-Critical: These systems are necessary to state government but short-term interruptions or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of the citizens. They could be easily offset with manual procedures;
  - (2) Critical: These systems are required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data and systems can be restored; and
  - (3) Extremely Critical: These data and systems are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business.

- (c) Each DHS division and office shall utilize more stringent security control requirements when the security level of an information system, facility, or network is designated at the “Sensitive” or “Confidential” level. In all instances, the minimum security requirements of a system should be appropriate for the highest security level designation of any data the DHS division and office processes within that system, including data received from other agencies.
- (d) For each security level classification, there are controls that define the protection of information being processed for these types of activities:
  - (1) Copying and storage;
  - (2) Destruction; and,
  - (3) Transmission by mail, electronic email, fax, internet, intranet, and storage media.
- (e) Output from systems containing DHS information shall carry an appropriate classification label on the output. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CDs, cassettes), electronic messages, and file transfers.
- (f) Physical labels are generally appropriate; however, data in electronic form cannot be physically labeled. An electronic means of labeling must be implemented, as applicable.
- (g) The IT Security Office shall:
  - (1) Develop and maintain enterprise-wide procedures to assist divisions and offices on labeling data;
  - (2) Provide guidelines for access control to that data including electronic marking and physical labeling; and,
  - (3) Provide assistance in determining the integrity classification of each business application used.
- (h) For an illustration on how the classification works, utilize the “Data Classification Matrix” attached to this procedure.

#### IV. Application and System Security Controls

All DHS Applications and Systems shall implement the appropriate security controls to minimize risk in the production or operating environment. The type of controls necessary will be appropriate with the determination of data confidentiality, integrity, and availability levels. The DHS Chief Information Security Officer (CISO) shall certify the controls as appropriate, based on the classification of the data or system.

## V. Data Transfers

- (a) The use of non-encrypted mobile devices for transfer of confidential information such as PII, PHI, and FTI is restricted. This includes but is not limited to: text messaging, external applications, and non-DHS email. DHS will maintain acceptable standards for delivery of protected information. This means DHS employees or contractors cannot use personal phones or devices that are unencrypted for DHS business related tasks such as taking pictures for investigations or the use of text messaging DHS or client related data.
- (b) The record of transfer of any data containing Protected Health Information (PHI) and Federal Tax Information (FTI) will be logged separately. The logs will be maintained by the DHS Privacy Office. PHI logs will be reviewed and approved by the DHS Privacy Officer. The FTI log will be reviewed and approved by the CISO and Privacy Officer.
- (c) DHS shall utilize the three tiered architecture for the storage of data for the Demilitarized, Middleware, and Private zones. All protected data shall be located in a Private Zone, public access will be located in Demilitarized Zone, and all other data located in Middleware Zone.

## VI. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

## VII. Exceptions

Any requests for exceptions to this procedure must be submitted in writing and approved by the DHS Chief Information Officer. Exceptions shall be reviewed annually and require approval on an annual basis. Exceptions will not violate compliance with any federal or state law, rule, or regulation.

## VIII. Definitions

- (a) "DHS Data" means any information which is maintained in any form within DHS. Any grouping of data is classified based on data confidentiality, integrity, and availability.
- (b) "DHS Information Systems" means the DHS Network services, Network Access, including e-mail and internet access, DHS applications including client-server, web-based and mainframe applications or any third-party software legally acquired and installed on DHS devices. This also includes any computer file on any device in use

- by DHS or its agents that is shared across the DHS network and requires DHS support or that contains DHS-related information.
- (c) “Demilitarized Zone” means in computer networks, a Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network.
  - (d) “Middleware Zone” Zone where computers and devices are located and systems not containing protected data.
  - (e) “Private Zone” means a restricted access location designed to protect data.
  - (f) “Protected Information” means any data classified as Sensitive or Confidential.
  - (g) “Protected Health Information” means as defined in the HIPAA, 45 CFR 160.103.
  - (h) “Personally Identifiable Information” means information that can be used on its own or with other information to identify, contact or locate a single person to identify an individual in context as defined by the U.S. Privacy Act and Arkansas Personal Information Protection Act (PIPA).
  - (i) “Federal Tax Information” means any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information as defined by IRS Publication 1075. FTI data may not be masked to change the character of information to circumvent requirements.

## IX. References

- (a) Arkansas Data and System Security Classification  
[http://www.techarch.state.ar.us/domains/security/standards/SS-70-001\\_dataclass\\_standard.pdf](http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf)
- (b) Cybersecurity Enhancement Act of 2014  
<https://www.congress.gov/bill/113th-congress/senate-bill/1353>
- (c) Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/groups/SMA/fisma/>
- (d) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (e) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)  
<http://www.hhs.gov/ocr/privacy/>
- (f) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- (g) Social Security Administration Safeguards (SSA)  
<http://www.ssa.gov/dataexchange/security.html>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 124

### Title: DHS Information Systems Change Management Procedures

#### I. Applicability

These procedures apply to all employees and authorized users who install, operate, or maintain DHS information resources.

#### II. Scope

This procedure ensures that changes to information systems are deployed in a controlled manner so that DHS users and clients can plan accordingly. Changes require careful evaluation, prioritization, planning, testing, implementation and documentation to reduce negative impact to DHS' business and user community. Management of these changes is a critical part of providing strong and valuable information systems throughout the agency.

#### III. Procedures

- (a) All changes to the DHS information systems or resources shall comply with this procedure.
- (b) All changes affecting DHS' computing environmental facilities (for example, air conditioning, water, heat, plumbing, electricity, and alarms) need to be reported and coordinated with the DHS Chief Information Officer (CIO) or Chief Information Security Officer (CISO). These changes shall adhere to any applicable state regulations.
- (c) All change requests must be submitted in writing to the CIO or designee by the end of business on Wednesday to be reviewed by the DHS Change Management Committee on Friday.
- (d) The members of the DHS Change Management Committee meets with the appropriate agency systems managers to review, assess, and evaluate all change requests.
- (e) If the proposed change is authorized, the committee plans the update and coordinates the implementation of the change, then after the final review, the change process is closed.
- (f) The CIO or CISO and the DHS Change Management Committee may deny the standard change or an emergency change for the following reasons:
  - (1) Planning (for example, inadequate planning related to implementation, risk assessment, testing, back-out);

- (2) Timing (for example, timing of a change that would negatively impact a key business process such as year-end accounting);
  - (3) Documentation (for example, inadequate documentation related to disaster recovery, security testing methodology/data); or
  - (4) Resources (for example, adequate resources may particularly be a problem on weekends, holidays, or during special events).
- (g) DHS user notification (located on the DHS Sharepoint site) must be completed for each Standard and Emergency Change by utilizing these procedures included in this section.
- (h) A Change Management log must be maintained for all changes. The log must contain, but is not limited to:
- (1) Date of submission and date of Change;
  - (2) Owner and custodian contact information;
  - (3) Nature of the Change; and,
  - (4) Indication of success or failure.
- (i) A change review must be completed and documented for all changes, whether the change is successful or not.
- (j) All DHS Information Systems, network devices, and databases will use approved baseline configurations and hardening per the DHS Configuration Standards and National Institute of Standards Technology guidelines. Any deviation from the standard baseline configuration must be approved by the CIO or CISO prior to implementation.
- (k) The DHS IT Security Office ensures that DHS maintains information and system integrity through intrusion detection systems that facilitate notification of unauthorized changes.

#### IV. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

#### V. Definitions

- (a) "Back-out Plan" means a plan that documents all actions to be taken to restore a service or service component if the associated Change or Release fails or partially fails. Back-out plans may provide for a full or partial reversal.

- (b) “Change” means the addition, modification or removal of an authorized, planned or supported service or service component and its associated documentation. All Changes must be registered by the Change Management process.
- (c) “Emergency Change” means an authorized modification that is intended to repair a failure in an Information Technology service that may have a significant negative impact on DHS business.
- (d) “Standard Change” means an authorized, planned modification or upgrade of a service or infrastructure component that is of low risk.
- (e) “Change Management” means the process responsible for the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to DHS Information Systems. The process includes the management and coordination of the processes, systems and functions required for the packaging, building, testing and deployment of a release into production, and establish the service specified in the customer and stakeholder requirements.
- (f) “DHS Information Systems” means the DHS Network services (Network access, Email, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS device for which they were intended. A DHS Information System also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or that requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.
- (g) “DHS User” means a person whose identity has been validated, whose association with DHS has been certified by the division with whom the person is affiliated, who has been granted access to any DHS Information Systems, and who is held accountable for the security of such access. A DHS User may or may not be a DHS employee.
- (h) “Information Resources” means any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA) devices, pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- (i) “Release” means a collection of hardware, software, documentation, processes or other components required to implement one or more approved Changes to DHS Information Services. The contents of each Release are managed, tested, and deployed as a single entity.

- (j) “Request for Change (RFC)” means a formal proposal for a change to be made. A Request for Change includes details of the proposed change.
- (k) “DHS System Manager” means the persons exercising management authority for a DHS-supported network service or application system. The role of such persons provides DHS ownership for the DHS service or system.

## VI. References:

- (a) Arkansas Physical and Logical Security Standard for Information Technology Resources (SS-70-008) [http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-008\\_phys\\_log\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-008_phys_log_standard.pdf)
- (b) Arkansas Physical and Logical Security Standard Guidelines Document Number SS-70-008 [http://www.dis.arkansas.gov/poli stan\\_bestpract/pdf/PhyLogGuidelines.pdf](http://www.dis.arkansas.gov/poli stan_bestpract/pdf/PhyLogGuidelines.pdf)
- (c) Health Insurance Portability and Accountability Act of 1996 (HIPAA) <http://www.hhs.gov/ocr/privacy> And Patient Protection and Affordable Care Act of 2010
- (d) Information Technology Infrastructure Library version 3 (ITIL v3) <http://www.itil-officialsite.com/home/home.asp>
- (e) Copyright Act of 1976; U.S. Copyright Law of 2007; Enactments to amend U.S. Copyright Law, 2008; <http://www.copyright.gov/title17>
- (f) Foreign Corrupt Practices Act of 1977, as amended [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/47mcrm.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/47mcrm.htm)
- (g) Computer Fraud and Abuse Act of 1986 [http://www.justice.gov/criminal/cybercrime/1030\\_new.html](http://www.justice.gov/criminal/cybercrime/1030_new.html)
- (h) Computer Security Act of 1987 <http://www.csp.noaa.gov/policies/csa-1987.htm>
- (i) Critical infrastructure Executive Order 13636
- (j) IRS Publication 1075
- (k) Federal Information Security Management Act of 2002
- (l) The Health Information Technology for Economic and Clinical Health Act of 2009
- (m) The Privacy Act of 1974
- (n) Act 339 of 2007, State of Arkansas, PIPA, ACA 4-110-104
- (o) The e-Government Act of 2002
- (p) HHS Final Rule 155.260 Privacy and Security of Personally Identifiable Information
- (q) 26 U.S.C. §6103 Safeguards for Protecting Federal Tax Returns and Return Information
- (r) USA Patriot Act of 2001, USA Cyber Security Enhancement Act of 2002, USA Computer Fraud and Abuse Act of 1986
- (s) 18 U.S.C. § 1029. (Fraud and Related Activity in Connection with Access Devices); 18 U.S.C. § 1030. (Fraud and Related Activity in Connection with Computers); and 18 U.S.C. § 1362. (Communication Interference)

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 125

### Title: Information Systems Access Procedures

#### I. Applicability

These procedures apply to Authorized DHS Approving Managers (ADAMs) and users attempting to gain access to DHS Information Systems and describe the procedures needed to obtain access.

#### II. Procedure

- (a) All persons requiring access to DHS Information Systems must obtain permission from their divisions' ADAM and be authenticated through the Chief Information Officer's (CIO) designated Systems Administrators. ADAMs and new users must complete and sign DHS Form 359 (for employees) or 5002 (for contractors), "DHS Systems Security Access Request."
- (b) Hiring Supervisors are responsible for notifying their division or office's ADAM of a new employee and when an employee leaves or transfers. Hiring supervisors must complete a Form 359 or 5002 and submit to their division or office's ADAM for a change in a user's status (demographic data or type of access, etc.), the termination of a user, and when a user transfers to another location or division. In the case of a transfer, only the user's network account and email transfer. All other access will be based on the new permissions.
- (c) By signing DHS Form 359 or 5002, ADAMS certify that:
  - (1) Access requests are made on behalf of persons who are DHS employees in good standing or non-DHS users who are members of an organization with whom a formal agreement is in place to permit access to DHS systems and safeguard protected information;
  - (2) Users have provided accurate identifying information and have a legitimate and official purpose for the requested level of access;
  - (3) Users have been notified of DHS policies pertaining to the appropriate use of state equipment and systems and the safeguarding of private information and that users have completed the required DHS Security and Privacy training; and,
  - (4) He or she agrees to notify the DHS Systems Security Gateway of material changes in a user's employment status as it relates to the DHS network services or systems applications to which the user has been granted access.

- (d) By signing DHS Form 359 or 5002, DHS Information System users certify that he or she:
- (1) understands that access to state-furnished equipment, software, and data is restricted to authorized persons only and may be used for official business purposes only;
  - (2) accepts responsibility for appropriate utilization of state-furnished equipment and understands that computer devices, network activity, email, and internet access may be monitored to detect improper or illicit activity;
  - (3) has no expectation of privacy in the use of state-furnished computer equipment and services;
  - (4) agrees to take all necessary measures to safeguard the security of his/her access credentials (username, password, smart card) and is accountable for any unauthorized usage of access credentials that results from his/her negligence or purposeful action; the user agrees to immediately report any compromise of access credentials;
  - (5) understands it is a violation of state and federal law to use, permit the use of, or fail to safeguard the security of client information in any way that jeopardizes its confidentiality;
  - (6) is subject to DHS policies pertaining to safeguarding confidential or sensitive information, penalties for inappropriate use of state equipment and electronic communication services, and sanctions for violations of related DHS Conduct Standards; and,
  - (7) understands penalties for unauthorized access or inappropriate usage, for DHS or non-DHS users, may include discipline and/or prosecution.

### III. Integrated Systems Security Gateway

- (a) Upon receipt of DHS Form 359 or 5002 from the ADAM, the Security Gateway Administrator will match identity data against validation data sources. DHS users may be contacted by phone and verbally challenged for their AASIS number. The confirmation of other demographic information may be obtained at that time if the Gateway Administrator deems it appropriate. For non-DHS users, the ADAM will be contacted by phone and will be verbally challenged to verify collected information about the user and the request for new user access.
- (b) When validation of identity is not successful, the Gateway Administrator will notify the requesting ADAM that the access request was denied. When validation of identity is successful, the Gateway Administrator will re-direct the request to the appropriate Systems Administrators for processing.

#### IV. User Credentials and Security

- (a) Users are assigned a unique personal identifier (username) which must be authenticated in conjunction with a valid password or smart card to gain access to DHS Information Systems. ADAMs should instruct users to safeguard credentials with respect to both physical security and access to DHS Information Systems. The structuring of passwords will meet or exceed prevailing state government standards of at least eight characters with a mixture of alpha, numeric, and special characters.
- (b) All Windows or Active Directory based passwords will expire in 60 days and Mainframe based passwords will expire in 90 days, or earlier if changed by user. Users will receive system prompts to change passwords before they expire. Users may not reuse any of their last five passwords for DHS Network access or their last four passwords for Mainframe access. A password should be changed if a user suspects its security has been compromised.
- (c) Sharing of credentials is strictly forbidden. Written recording of credentials is discouraged but if recorded, the following rules should be observed:
  - (1) Never openly post User Credentials, particularly in proximity to the user's PC.
  - (2) Store recording of credentials in a secure location.
  - (3) Do not identify the recording as a password.
  - (4) Do not include User Name with password.
  - (5) Mix in false characters or scramble the password recording in a manner you will remember so the written version is different from the real password.
  - (6) Never record a password on-line or include it in an email message.

#### V. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policy 4002, "Privacy and Security Sanctions" and the DHS Employee Discipline policy.

#### VI. Systems Security Roles Defined

- (a) User: A person whose identity has been validated, whose association with DHS has been certified by the division with whom the person is affiliated, who has been granted access to any Department of Human Services information system, and who is held accountable for the security of such access. A user may or may not be a Department of Human Services employee.

- (b) Department of Human Services User: A person, Department of Human Services employee, who has been granted access to any Department of Human Services information system and is accountable for the security of such access.
- (c) Non-Department of Human Services User: A person, not a Department of Human Services employee, who has been granted access to any Department of Human Services information system and is accountable for the security of such access.
- (d) System Administrator: Collectively refers to persons exercising the following systems security roles: Security Gateway Administrator, Network Services Administrator, Mainframe Services Administrator, Windows Application Security Administrator, Mainframe Application Security Administrator, Systems Administrators for division supported applications, DHS CIO. The role of such persons is to provide technical support and access management for DHS network services and applications.
- (e) Security Gateway Administrator: Persons performing this role serve as the common point of entry for all user access requests. Primary functions include initial evaluation of received access requests, validation of identity, and re-directing of requests for additional processing.
- (f) ADAM: Authorized DHS Approving Manager – a class of DHS managers who have been authorized by each division’s ADAM administrator to certify user access requests. An ADAM must be a DHS employee. The role of the ADAM is to authorize the submission of security access requests for (1) employees within the manager’s division, and (2) non-DHS users affiliated with the manager’s division. ADAMs are responsible for the validity of both DHS User and non-DHS User information in all User Access Account records they have authorized (DHS Form 359 or DHS Form 5002, DHS Systems Access Request, available on DHS Share). ADAMs are responsible for notifying the Gateway Administrator of material changes that affect both DHS User and non-DHS User access privileges.
- (g) ADAM Administrator: A designee appointed by each division’s director to assume the role of managing and maintaining the currency of the division’s list of ADAMs. Only those managers appearing in each division’s list will be recognized by the Security Gateway Administrator for the purpose of submitting user access requests.

VII. References:

- (a) State of Arkansas Policies and Standards  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>
- (b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001  
[http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001\\_dataclass\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf)
- (c) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications <http://csrc.nist.gov/publications/PubsSPs.html>
- (d) Federal Information Processing Standards Publications (FIPS PUBS) <http://itl.nist.gov/fipspubs/>

- (e) Federal Information Security Management Act of 2002 (FISMA) <http://csrc.nist.gov/groups/SMA/fisma/>
- (f) Social Security Administration Safeguards (SSA) <http://www.ssa.gov/dataexchange/security.html>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 126

### Title: Acceptable Encryption Procedures

#### I. Applicability

This procedure applies to all DHS employees and affiliates authorized to use DHS Information Systems.

#### II. Scope

The DHS IT Security Office and the Office of Systems Technology (OST) will identify and classify the owners and locations of DHS' confidential, sensitive, or other critical data which requires encryption through its annual risk assessment process using tools and/or documented methodology approved by the DHS Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

#### II. Procedure

- (a) Proven, standard algorithms listed in the National Institute of Standards and Technology (NIST) cryptographic module validation list and validated to the current Federal Information Processing Standards (FIPS) standard shall be used as the basis for encryption technologies.
- (b) The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the DHS CIO or CISO.
- (c) DHS data to be encrypted includes, but is not limited to, the following:
  - (1) Data classified as "Sensitive Data" or "Confidential Information" (as detailed in "Data Classification Procedures" (APM 123));
  - (2) DHS Information Systems users' login credentials;
  - (3) All portable media/mobile computing devices;
  - (4) Data at rest;
  - (5) Data in motion; and,
  - (6) Offsite data storage.
- (d) Non-approved protocols such as FTP and Telnet will not be permitted without prior approval by the CIO or CISO. A list of non-approved protocols will be

maintained in the DHS encryption standard, as kept by OST. Encryptions will be audited per the “IT Security Audit Compliance Procedure” (APM 120).

#### IV. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can’t complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, “Privacy and Security Sanctions” and 1084, “Employee Discipline: Conduct/Performance.”

#### V. Definitions

- (a) “Proprietary Encryption” means an algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or a government.
- (b) “Symmetric Cryptosystem” means a method of encryption in which the same key is used for both encryption and decryption of the data.
- (c) “Asymmetric Cryptosystem” means a method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).
- (d) “Mobile Computing Device” means a term used to describe portable and/or pocket-sized computing devices, typically having a display screen with touch input and/or a miniature keyboard; examples include mobile tablet/laptop computers, personal digital assistants (PDAs), and smartphones.
- (e) “Data at Rest” means a term used to describe all data in storage but excludes any data that frequently traverses the network or that which resides in temporary memory. Data at rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, USB flash drives, files stored on backup tape and disks, and also files stored off-site or on a storage area network (SAN).
- (f) “Data in Motion” means a term used to refer to the transfer of that data between all copies and versions of the original file, such as data traversing a local area or wide area network (such as the Internet).
- (g) “Offsite Data Storage” means a term used to describe data stored for backup and restore at a separate geographic location from where that data is actually being created or accessed.

#### VI. References

- (a) State of Arkansas Policies and Standards  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>

- (b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001  
[http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001\\_dataclass\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf)
- (c) Arkansas State Security Office Data and System Classification Grid Guidelines  
[http://www.dis.arkansas.gov/policiesStandards/Documents/DataClassification\\_Guide.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/DataClassification_Guide.pdf)
- (d) Arkansas State Security Office Data Classification Grid Form  
[http://www.dis.arkansas.gov/policiesStandards/Documents/data\\_grid.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/data_grid.pdf)
- (e) State of Arkansas Standard Statement-Encryption -Document Number: SS-70-006  
[http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT\\_encryption\\_standard\\_2011.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT_encryption_standard_2011.pdf)
- (f) State of Arkansas Security Office Financial and Risk Impact Statement for Proposed Encryption Standard  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryption\\_financial.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryption_financial.pdf)
- (g) State of Arkansas Security Office Information on Backup Encryption Methods  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryp\\_impactinfo.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryp_impactinfo.pdf)
- (h) State of Arkansas Security Office Encryption Standard Guidelines  
[http://www.dis.arkansas.gov/policiesStandards/Documents/comply\\_encryp\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/comply_encryp_standard.pdf)
- (i) National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP)  
<http://csrc.nist.gov/groups/STM/cmvp/index.html>
- (j) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications  
<http://csrc.nist.gov/publications/PubsSPs.html>
- (k) Federal Information Processing Standards Publications (FIPS PUBS)  
<http://itl.nist.gov/fipspubs/>
- (l) IRS Publication 1075 (IRS)  
<http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- (m) FBI Criminal Justice Information Services (FBI CJIS)  
<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>
- (n) CMS Minimum Acceptable Risk Standards (CMS MARS-E 2.0)  
<https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf>
- (o) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 127

### Title: Voice-over Internet Protocol Procedures

#### I. Applicability

This procedure applies to all DHS users who are authorized to purchase and connect voice over internet protocol (VOIP) devices to DHS Information Systems. VOIP is a technology that enables voice conversations over data networks and between those networks and legacy phone networks. VOIP consists of a number of hardware and software components that provide the voice services required by DHS.

#### II. Procedure

- (a) All VOIP components purchased by DHS divisions and offices will have the features needed by the agency and will adhere to the VOIP network and security standards that DHS implements.
- (b) Only VOIP devices that are purchased through DHS Office of System and Technology (OST) shall be connected to any part of the DHS Information Systems. Before any VOIP device is purchased, it must either be on a list of DHS approved devices or must be reviewed and approved by the DHS Chief Information Officer (CIO) or designee. After a VOIP device has been purchased, it must be registered with Unified Communications Services and connected to DHS Information Systems according to established network and security procedures.
- (c) OST will be responsible for:
  - (1) maintaining a list of approved VOIP devices;
  - (2) approving unlisted devices; and,
  - (3) maintaining a registry of connected VOIP devices.
- (d) The DHS IT Security Office is responsible for:
  - (1) developing, certifying, and clarifying VOIP device network and security procedures; and,
  - (2) investigating and notifying any DHS user attempting to violate the DHS VOIP Device Procedure.

### III. Review and Measurement

- (a) OST will periodically review the VOIP registry to verify devices are within compliance.
- (b) If a DHS division or office purchases a VOIP device that is not on the approved list or has not been approved by the DHS CIO or designee, it will not be allowed to connect to DHS Information Systems.

### IV. Other

Although there are a number of national and international standards (along with proprietary features) that voice over internet protocol vendors implement in their products, adoption of these standards do not guarantee multi-vendor voice over internet protocol interoperability. Some voice over internet protocol standards compete with one another and others are still maturing. In addition, not all VOIP vendors implement the features that DHS users need.

### V. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

### VI. References

- (a) Security Considerations for Voice Over Internet Protocol Systems (National Institute of Standards and Technology Special Publication 800-58,) <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- (b) IRS Publication 1075 (IRS) <http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- (c) Federal Information Security Management Act of 2002 (FISMA) <http://csrc.nist.gov/groups/SMA/fisma/>
- (d) CMS Minimum Acceptable Risk Standards (CMS MARS-E) <http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 128

### Title: Information Systems Disaster Recovery and Continuity Procedure

#### I. Applicability

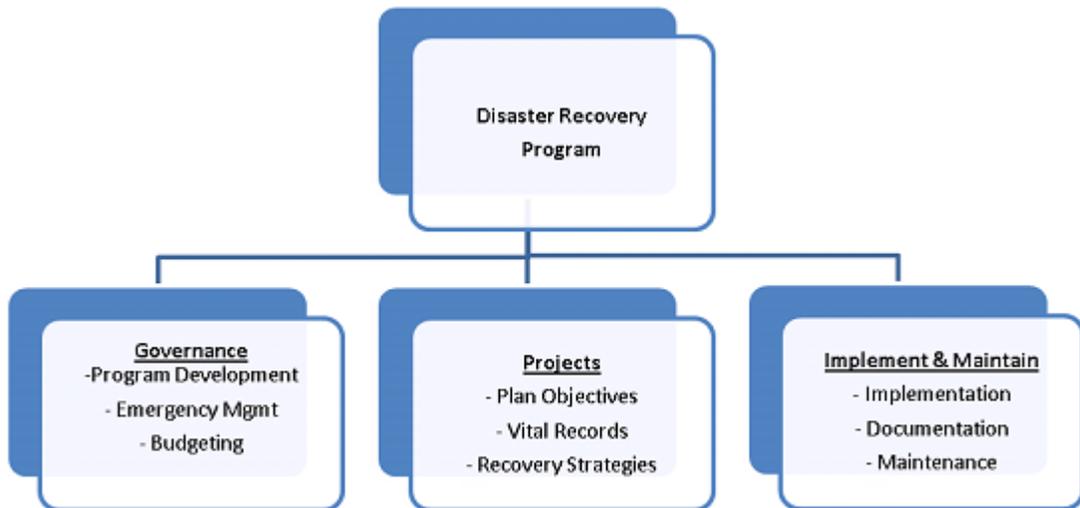
The Disaster Recovery and Continuity Procedures apply to all DHS users, managers, and contractors with critical systems managing or hosting DHS data, processing and/or services. All IT-managed systems must comply with this procedure.

#### II. Scope

This procedure defines acceptable methods for disaster recovery planning, preparedness, management, and mitigation of IT systems and services at DHS. The disaster recovery standards in this procedure provide a systematic approach for safeguarding the vital technology and data managed by the Office of Systems Technology (OST). It also provides a framework for the management, development, and implementation and maintenance of a disaster recovery program for the systems and services managed by OST.

#### III. Procedure

- (a) DHS Disaster Recovery Planning is a program that has a continuous lifecycle. The high-level processes for DHS Disaster Recovery (DR) Cycle steps are detailed in a flowchart below:



- (b) The Chief Information Officer (CIO) and Chief Information Security Officer (CISO) are responsible for IT DR program coordination and project management: including reporting status of IT DR planning, testing, and auditing activity on a regular basis; annually.

- (c) The CIO is responsible for ensuring sufficient financial, personnel and other resources are available as needed.
- (d) The CIO and CISO will review and update the DR Procedure as necessary at minimum annually. All modifications must be approved by the CIO and the CISO.
- (e) The IT Disaster Recovery Program (DRP) addresses the protection and recovery of DHS IT services so that critical operations and services are recovered in a timeframe that ensures the survivability of DHS and is commensurate with client obligations, business necessities, industry practices, and regulatory requirements.
- (f) Plans must be developed, tested, and maintained to support the objectives of the Program, and those plans should include relevant IT infrastructure, computer systems, network elements, and applications. At minimum, annual updating is required.
- (g) The CIO or designee is responsible for conducting Business Impact Analyses (BIA) to identify the critical business processes, determine standard recovery timeframes, and establish the criticality ratings for each; at least annually or when a significant change occurs.
- (h) The CIO or designee is responsible for conducting Capability Analyses (CA) to determine IT's capacity to recover critical IT services that support defined critical business processes and recovery objectives; at least annually.
- (i) The CIO or designee is responsible for maintaining the Recovery Tier Chart, which defines the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of all IT-managed systems. The application managers are required to prioritize their IT processes and associated assets based upon the potential detrimental impacts to the defined critical business processes.
- (j) Application managers required to create disaster recovery plans for the IT portion - including services, systems, and assets - of critical business processes. These IT services, systems, and assets must be inventoried and correlated according to the technical service catalog, prioritized based upon results of the business impact analysis, and ranked according to their RTO and RPO.
- (k) A risk assessment must be conducted annually to determine threats to disaster recovery and their likelihood of impacting the IT infrastructure.
- (l) For each risk or vulnerability identified in the risk assessment, a mitigation or preventive solution must be identified and a corrective action plan must be developed and sent to IT Security for review.
- (m) The IT DRP must include a change management and quality assurance process.

#### IV. Emergency Management

- (a) DHS Divisions will assign a Disaster Recovery Manager.

- (b) The IT Disaster Recovery Manager is responsible for overseeing IT DR activities, for their divisions, in the event of an emergency -i.e., an unplanned outage where RTO is in jeopardy.
- (c) The IT Disaster Recovery Manager should be part of the IT representation within the institution's Emergency Management Team.
- (d) Each division must develop and maintain a documented emergency plan including notification procedures.
- (e) Each division shall account for its associates when a building evacuation is ordered. Supervisory personnel are responsible to account for the associates they supervise.
- (f) The IT Disaster Recovery Team/Manager is required to complete a post-mortem report documenting outages and recovery responses within forty-five (45) days after the occurrence of a disaster recovery event.

#### V. Plan Objective

- (a) Division DR Plans must provide information on Business Impact Analysis, Data Backup, Recovery, Business Resumption, Administration, Organization Responsibilities, Emergency Response & Operations, Training and Awareness and Testing.
- (b) Plans must contain Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
- (c) Technological solutions for data availability, data protection, and application recovery must be considered by data gathered by the BIA and CA.

#### VI. Vital Records

- (a) OST shall maintain a single, comprehensive electronic inventory of all servers, network equipment, relevant configuration, and model information, and the applications they support. This inventory should be aligned with the service catalog and the technical service catalog.
- (b) All physical backup data must be labeled and logged, and are available for use during an emergency within stated recovery time objectives. A documented decision making process will be used to determine what subset of backup data will be additionally encrypted, and stored off-site in a secured location outside of the geographical area of the system they are backups of.
- (c) DR plans must be stored in a single, comprehensive database.
- (d) DR plan owners need to be able to access a copy of emergency and recovery plan(s) independent of IT services and/or network.

- (e) Upon completion or update, DR plans must be sent to the CIO and CISO for review.
- (f) Plan information must be reviewed and updated as warranted by business and/or information systems environment changes, at least annually.

#### VII. Plan Attributes

- (a) Plans must address an outage that could potentially last for a period of up to six weeks.
- (b) Plans must identify risk exposure and either accept the risk or propose mitigation solution(s).
- (c) Backup strategies must comply with predefined businesses continuity requirements, including defined recovery time and point objectives. Backup strategies must be reviewed at least annually or whenever any significant change occurs.
- (d) Recovery strategies must meet recovery objectives defined in the “DR Tier Chart.”
- (e) Approved recovery strategies must be tested to ensure they meet required recovery time and recovery point objectives.
- (f) Recovery strategies must be implemented within a previously agreed upon period of time, generally not more than one hundred and eighty (180) days after management approval.
- (g) The CIO or designee is required to provide DR training and awareness activities at least annually.

#### VIII. Maintenance

- (a) Plans must contain current and accurate information.
- (b) Planning must be integrated into all phases of the IT system life cycle.
- (c) IT DR tests that demonstrate recoverability commensurate with documented IT DR plans must be conducted regularly; as well as when warranted by changes in the business and/or information systems environment.
- (d) Backup media supporting critical business processes must be tested semi-annually. Reviews are required within sixty (60) days after a test to correct exposed deficiencies.
- (e) Plan revisions must be completed within sixty (60) days after a DR test is completed.
- (f) The following maintenance activities must be conducted annually:

- (1) Update the documented DR plan;
  - (2) Review the DR objectives and strategy;
  - (3) Update the internal and external contacts lists;
  - (4) Conduct a simulation/desktop exercise;
  - (5) Conduct a telecommunication exercise;
  - (6) Conduct an application recovery test;
  - (7) Verify the alternate site technology;
  - (8) Verify the hardware platform requirements; and,
  - (9) Submit the DR Status and Recoverability Report.
- (g) IT managers in DHS divisions and offices are responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.

#### IX. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in termination or disciplinary action as outlined in DHS Policies 4002 “Privacy and Security Sanctions” and 1084, “Employee Discipline.”

#### X. References

- (a) DHS, Office of Systems and Technology, Information Technology Unit
- (b) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (c) IRS Publication 1075 (IRS) <http://www.irs.gov/pub/irs-pdf/p1075.pdf>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 129

### Title: Data Destruction and Information Processing Equipment End of Life Procedures

#### I. Applicability

These procedures specify the steps for the safe retirement and/or disposal of Data Storage Media and Information Processing Equipment from agency use as required by Ark. Code Ann. §25-34-102, and ensures compliance with all applicable federal (HIPAA) regulations regarding the security of confidential information. This chapter applies to all DHS employees, volunteers, and contractors or entities that handle DHS information or interact with Information Processing Equipment or Data Storage Media.

#### II. Document Destruction

Use only the locked shred bins to destroy confidential documents when they are no longer needed. Do not use the recycling bins to dispose of documents that contain Protected Health Information (PHI), Personal Identifying Information (PII), Federal Tax Information (FTI), or Social Security Administration (SSA) data. All DHS Divisions and Offices will work with the DHS IT Security Office and the DHS Privacy Office during the planning, purchasing, and development phases of shredding contracts to ensure the destruction of confidential documents is handled appropriately.

#### III. Media Destruction

- (a) The DHS Office of Systems Technology (OST) provides a secure method for the physical destruction of media. Shredders capable of destroying media in accordance with state and federal rules and regulations may be used by divisions.
- (b) Physical destruction is the preferred method of media disposal as outlined below in the Destruction Matrix. However, media overwrites may be utilized by using secure deletion software that's authorized and provided by the DHS Chief Information Officer (CIO) or designee.
- (c) Media disposal, physical destruction, wipes and sanitizing, must follow the Destruction Matrix below:

Media	Clear/Wipe	Sanitize
Tape	a	a or d
Floppies	a, b	d
Non-Removable Rigid Disk (hard drive)	b	a, c, or e
Removable Rigid Disk (Zip, Jaz, other)	a, b	a, c or d
<b><i>Optical Disk (CD-R, CD-RW, DVD+R, DVD-R, DVD+RW, DVD-RW, etc.)</i></b>		
Read Many, Write Many (CD-RW)	b	d
Read Only (CD-ROM)	d	d

Write Once, Read Many (CD-R)	d	d
a. Degauss (do not degauss hard drives)		
b. Overwrite all addressable locations with a single character. (single pass overwrite)		
c. Overwrite all addressable locations with a character, its complement, then a random character and verify. (multiple pass / DoD secure overwrite)		
d. Destroy - Disintegrate, incinerate, pulverize, shred, or melt		
e. Destruction required only if restricted information is contained.		

#### IV. End of Life Procedures

- (a) A division designee shall make the initial determination that a computer or computer peripheral meets the conditions of being obsolete. Obsolete means the equipment is no longer under warranty or is no longer fit for use because it uses components that are no longer adequate to achieve the equipment's intended purpose or because the cost of the repair or replacement would be greater than the equipment's residual market value.
- (b) The division designee will email the following information for each item of obsolete equipment to the DHS CIO or designee:
  - (1) Brand;
  - (2) Model;
  - (3) Serial number;
  - (4) Inventory tag number (if any);
  - (5) Purchase date and price (if available); and,
  - (6) Service warranty expiration date (if available).
- (c) The CIO or designee will make arrangements to determine if the obsolete equipment is suitable for other purposes within DHS. This determination will be based on an estimate of the equipment's remaining useful life and knowledge of existing needs elsewhere within DHS where the equipment can be used with minimal support cost. If the equipment is redeployed within DHS, the originating division will arrange for the delivery of the equipment to the new site. If the equipment cannot be redeployed, the originating division will arrange for the equipment to be delivered to the DHS Warehouse.
- (d) All transportation of equipment to new locations will be performed in a secure manner using a CIO-approved transport provider. The sender is responsible for creating a manifest and tracking the shipment by item and description. The manifest should be maintained until the equipment arrives at the intended destination. The CIO or designee must be notified in writing of all equipment to be transported.
- (e) In accordance with the procedures listed here, the DHS CIO or designee will deliver media to the DHS IT Security Office for destruction of all data from equipment not being redeployed. The CIO or designee will document compliance by affixing a release tag or documentation to the equipment. The DHS Warehouse must ensure that equipment delivered to Marketing and Redistribution (M&R) has the appropriate OST release

documentation and media such as hard drives has been removed before the transfer of possession can be completed.

- (f) The CIO or designee must make the appropriate modifications to the AASIS inventory record for each device to be transported.
- (g) When equipment arrives at the storage facility, OST will remove all portions of the equipment that had the potential to store sensitive and/or protected DHS information. All hard drives will be wiped and sanitized according to the media destruction procedures in this APM.

#### V. Computer and electronic equipment recycling grants

- (a) Electronic equipment recycling grants must be awarded on the basis of written grant-request proposals submitted to and approved by the Arkansas Department of Environmental Quality (See AR Code Ann. § 25-34-110).
- (b) Grant requests shall be considered based upon the following criteria:
  - (1) The development of sustained processes for recovery, recycling, and remanufacturing of scrap computers and electronics;
  - (2) Minimization and elimination of substantial volumes of this material as waste;
  - (3) Creation of Arkansas jobs;
  - (4) Return of investment analysis; and,
  - (5) Available funds.
- (c) DHS Office of System and Technology may keep a back stock of computer hardware and electronics for the purpose of parts harvesting for the repair, maintenance, and upgrade of computers in use. Back stock shall not exceed 10% of the number of state employee computers in the agency.

#### VI. Other

- (a) The DHS CISO can be contacted for assistance with secure removal of DHS information from information processing equipment, printed materials, and data storage media.
- (b) DHS divisions will ensure compliance with procedures published by the DHS CISO for the secure removal of DHS information from Information Processing Equipment and Data Storage Media.

#### VII. Failure to Comply

- (a) Any violations of these procedures must be reported as a security incident on DHS Share. The DHS IT Security Office or Privacy Office must be alerted to all possible violations of privacy or security in the handling of confidential information.
- (b) Failure to comply with this, or any IT security procedure or policy will result in disciplinary action as outlined in DHS Policies 4002, “DHS Privacy and Security Sanctions” and 1084, “Employee Discipline: Conduct Performance.”

#### VIII. References

- (a) Arkansas Data and System Security Classification  
[http://www.techarch.state.ar.us/domains/security/standards/SS-70-001\\_dataclass\\_standard.pdf](http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf)>
- (b) Act 1526 of 2005, State of Arkansas
- (c) Health Insurance Portability and Privacy Act of 1996, United States of America
- (d) ISACA COBIT Standards <http://www.isaca.org/cobit>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 120

### **Title: Information Systems Security Audit and Compliance Procedures**

#### I. Applicability

These procedures establish a framework for conducting audit related reviews and compliance requirements of information resources at DHS in accordance with all applicable state and federal regulations. All DHS employees, contractors, and vendor partners must comply.

#### II. Scope

- (a) Security Audits can be conducted on any entity within DHS or any outside entity that has signed a Business Associate Agreement or Third Party Agreement with DHS. Security Audits can be conducted on any information system, to include applications, servers, networks, devices, and any process or procedure by which these systems are administered and/or maintained.
- (b) Employees, contractors, and vendor partners of DHS are subject to the policies and procedures of DHS and the Department of Information Systems. Some of those include manual or automated controls (where possible) that can result in a formal review by the DHS Chief Information Security Officer (CISO), an external auditor, or law enforcement, as appropriate.
- (c) This procedure plays a key role in security design, providing both preventative controls through alerts of suspicious activity and forensic security records of events essential for incident investigation. Capable components in the protected systems must record security relevant events, and will record events to either a local logging facility or by sending events to DHS authorized process.

#### III. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in restriction or suspension of all network access to DHS systems or applications. Employees who can't complete job duties or assignments without such access may be terminated or face disciplinary action as outlined in DHS Policies 4002 "Privacy and Security Sanctions" and 1084, "Employee Discipline."

#### IV. Procedures

- (a) All audits from external sources related to the security of systems, applications, or data are to be coordinated with the DHS IT Security Office and DHS Privacy Office prior to the audit.

- (b) The IT Security Office and the DHS Privacy Office will conduct security audits and reviews of identified systems and resources at least once a year as required by federal and state regulations and in support of assessing the security posture of the organization's critical and business systems. The IT Security Office will develop and maintain a review methodology to include the following:
- (1) Audit/ Review approval procedures;
  - (2) Internal Inspections Plan;
  - (3) Preliminary risk analysis;
  - (4) Planning phase;
  - (5) Testing phase;
  - (6) Communicating results;
  - (7) Remediation validation; and,
  - (8) Final reporting.
- (c) Audits and reviews must be approved in writing by the DHS CISO and the CIO. In addition, detailed documentation of all audits must be produced and securely archived by the IT Security Office in compliance with DHS retention policies. Work may be performed completely in-house or by an outside firm. In addition, the IT Security Office will collect and monitor applicable log data to identify intrusion attempts and potential attacks. Audit logs will be maintained per the "Information Systems Change Management Procedure" (APM 124).
- (d) DHS entities and personnel will provide the appropriate divisions with timely and complete responses to all audit results, plans of action, milestones, and corrective action plans required.
- (e) Audits will be performed based on federal and state guidelines as needed. The baseline for compliance will be based on FISMA (NIST) and modified based on the federal and state laws that may apply to the application or division. Programs containing access to FTI data will follow the internal inspections plan at minimum of every eighteen (18) months in addition to the standard audit.
- (f) Log aggregation, correlation, alerting, and retention requirements will be met using a Security Information and Event Management (SIEM) tool. The IT Security Office includes a security component and continuity of operations component. These maintain an overview of the DHS' risks, operational issues, mitigating controls, and recovery methods including some audit related functions.

- (g) The IT Security Office will define procedures to include inspections for compliance with federal, state, and local laws and regulations based on alignment with Federal Information Management Security Act (FISMA), Internal Revenue Service (IRS) (**National Institute of Standards and Technology** (NIST) 800-53, IRS Publication 1075), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Social Security Administration (SSA), and any other system determined to hold, collect or modify protected information.
- (h) OST, Security, or System Support groups may request device specifics (such as Operating System (OS), version, and patch level) for review – especially for devices that cannot support any service account ID. The CISO must approve any additions to the system. The CIO shall be notified when operational issues may arise and before making changes within the change management process. All changes shall be approved by the CIO or designee.
- (i) Primary accounts shall be defined by the CISO and other applicable groups.
- (j) If the device supports login credentials (local or directory based [such as Active Directory or LDAP]), the entity responsible for configuring the device will include an audit service account on the device as specified below. The SIEM reports real-time events as they occur, escalating significant events to the SIEM administrators and security management. Logs from the enterprise intrusion prevention system, network class devices, server class devices, operating system related logs, application software logs and third party logs, including reputation services, are incorporated into the SIEM.
- (k) The inspection accounts shall be created on each applicable device with sufficient rights to allow review of all data on such a device via the device's standard operating system access methods or physical environments necessary to ensure compliance. Audit and System logs will be maintained as documented per NIST requirements.
- (l) In order to meet state and federal guidelines, individuals will coordinate service accounts with the IT Security Office and other applicable support groups. All system components, including applications, databases, server operating systems, and network firewalls and proxies are required to record the following key security events to a local audit log, per the NIST security requirements for inspection:
  - (1) User account creation and deletion;
  - (2) User account enabled or disabled;
  - (3) User account modified;
  - (4) Security or audit configuration changed;
  - (5) Privileged task/command executed;
  - (6) Successful login and unsuccessful login;

- (7) Successful or unsuccessful access of protected data;
  - (8) Network packet blocked by firewall or access control list;
  - (9) System startup and shutdown;
  - (10) User permissions changed; and,
  - (11) Audit logging enabled and disabled.
- (m) For the events listed above in item (l), all systems will log the following data elements:
- (1) Event type;
  - (2) Time and date using the local system clock;
  - (3) Source of event, including source IP address, if available;
  - (4) Object of event, including destination IP address, if available;
  - (5) Outcome (success or failure); and,
  - (6) Users/subjects associated with the event (or system, if no user associated).
- (n) System components will log either to a local logging facility, or may send events to the SEIM for logging, following the format described in the SEIM section below. For local logging, use of the operating system logging facility (syslog, Windows Event log) is preferred.

## V. Vulnerability Assessment

- (a) The IT Security Office will perform vulnerability assessments on systems, applications, networks or devices where DHS data is located to the extent necessary to allow the IT Security Office or contracted company to perform the scans authorized by this procedure. DHS application owners shall provide protocols, addressing information, and network connections sufficient for auditing to utilize the software to perform network scanning.
- (b) Access may include:
  - (1) User level and/or system level access to any computing or communications device;
  - (2) Access to information (electronic, hard copy, etc.) that may be produced, transmitted or stored on DHS equipment or premise;

- (3) Access to work areas (labs, offices, cubicles, storage areas, etc.); and,
- (4) Access to interactively monitor and log traffic on DHS networks.

#### VI. Network Control

In the event DHS protected data is located outside of the DHS network, third parties will be required to perform a vulnerability assessment scan on an annual basis reporting findings to the DHS CISO and DHS Privacy Officer with a remediation plan and corrective action plan within thirty (30) days of finding the vulnerability. Failure to comply may result in loss of contract or connectivity. A risk evaluation will be performed as stated in “Information Systems Risk Management Procedures” (APM Chapter 121), to determine the risk and impact to DHS data, clients, and networks.

#### VII. Service Degradation and/or Interruptions

Network performance and/or availability may be affected by network scanning. The IT Security Office will plan accordingly to mitigate the impact to the network and the server.

#### VIII. Scanning Period

- (a) DHS Application owners and the IT Security Office shall identify in writing the allowable dates and times for audit scans and periodic scans to take place. Automated application scanning will be performed at a minimum of once every quarter. Alerts will be sent to the IT Security Office for any vulnerability found during automated alert which will be addressed per the incident response procedure.
- (b) DHS application owners shall identify in writing a person to be available if the IT Security Office or Privacy Office has questions regarding data discovered during the scan or if the offices require assistance in addressing an issue.

#### IX. Penetration Testing

Periodic penetration testing will be performed on DHS systems and applications. All scans will be non-intrusive unless approval is obtained from the application owner prior to testing. Exceptions may be made by the CIO or designee based on risk and known vulnerabilities.

#### X. Red/Blue Team Testing

DHS will build and train a group of engineers, security professionals, and developers to serve as active defense for cyber-attacks, breach evaluation, and vulnerability assessors. These teams will rotate responsibilities to build a strong skill set capable of protecting and evaluating the defense of DHS information systems. All actions will be coordinated with the divisions prior to the training or scenarios take place. Documentation of all actions will be recorded in a secured location for training purposes and all scenarios must be approved by the CIO and CISO prior to implementation.

## XI. External Audits

Audits managed by an external company will be performed annually, unless previous exclusion is given by the CIO for the fiscal year. Audits performed by other departments, agencies, or external parties shall be submitted to the IT Security Office to ensure issues are addressed to comply with state and federal regulations

## XII. Evaluation of Security and Privacy Policies and Procedures

Evaluation of Security and Privacy Policies and Procedures will be performed at minimum annually per federal and state guidelines unless significant changes are made within the annual timeframe. Policies and procedures will be evaluated based on information security measurements, performance, and documented activities.

## XIII. Other

- (a) This procedure does not replace the auditing and monitoring responsibilities of individual system administrators and data owners.
- (b) The DHS “Security Audit Process” is overseen by the IT Security Office. For information regarding the process, contact the IT Security Office.
- (c) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

## XIV. Definitions

- (a) “Entity” means any business unit, department, group, or third party, internal or external to DHS responsible for maintaining DHS assets.
- (b) “Risk” means those factors that could affect confidentiality, availability, and integrity of DHS’s key information assets and systems. The IT Security Office is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
- (c) “Security Audit” means formally testing and evaluating vulnerabilities and controls within the Information Technology environment, performed by an independent party, requiring independent corroboration (sampling in nature) to substantiate information provided by personnel.
- (d) “Security Review” means similar evaluation performed in a security audit but typically omits obtaining independent corroboration (non-sampling in nature) and testing to substantiate information provided by personnel. Security reviews may be performed in-house or outsourced to a third party.
- (e) “System Administrator” means an individual who performs network/system administration duties and or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of DHS and or third party vendors approved by IT may function as system/network administrators.
- (f) “Data Owners” means the person responsible for, or the person with administrative control over, granting access to an organization’s documents or electronic files while protecting the data as defined by the DHS

IT Security policies or standard IT practices. Data owners shall only be State Employees unless approved by the DHS CIO prior to receiving this responsibility.

- (g) “Application Owners” means the person responsible for development or management of an application containing DHS information.
- (h) “Resource” means one element of hardware, software or data that is part of a larger system.

## XV. References

- (a) Arkansas Data and System Security Classification  
[http://www.techarch.state.ar.us/domains/security/standards/SS-70-001\\_dataclass\\_standard.pdf](http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf)>
- (b) Arkansas Encryption Standard  
[http://www.techarch.state.ar.us/drafts/DRAFT\\_encryp\\_standardSS-70-006.pdf](http://www.techarch.state.ar.us/drafts/DRAFT_encryp_standardSS-70-006.pdf)>
- (c) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (d) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)  
<http://www.hhs.gov/ocr/privacy/>
- (e) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- (f) Social Security Administration Safeguards (SSA)  
<http://www.ssa.gov/dataexchange/security.html>
- (g) US Privacy Act of 1974 (Dept of State)  
<http://foia.state.gov/Learn/PrivacyAct.aspx>
- (h) Cybersecurity Enhancement Act of 2014  
<https://www.congress.gov/bill/113th-congress/senate-bill/1353>
- (i) Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/groups/SMA/fisma/>
- (j) IRS Publication 1075 (IRS), pertaining to Federal Tax Information (FTI)  
<http://www.irs.gov/pub/irs-pdf/p1075.pdf>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 121

### Title: Information System Risk Assessment and Management Procedures

#### I. Applicability

These procedures provide acceptable methods for DHS to perform required IT Security Risk Assessments for the purpose of determining areas of vulnerability and initiating appropriate remediation. These procedures are applicable to all employees, managers, and supervisors overseeing any resources owned, operated, or managed by DHS. All DHS users, employees, contractors, vendors, or others who utilize DHS IT resources are responsible for adhering to all DHS policies, including privacy and security policies (4000 and 5000 series).

#### II. Risk Assessment and Management

- (a) Risk Assessments can be conducted on any division or office within DHS and any outside entity that has signed a contract or Business Associate Agreement with DHS.
- (b) Risk Assessments can be conducted on any information system, including applications, servers and networks, and any process or procedure by which these systems are administered and/or maintained.
- (c) Any information not specifically identified as the property of other parties that is transmitted or stored on DHS IT resources, or includes information owned/managed by DHS (including e-mail, messages, files and federal or state data entrusted to DHS) is the property of DHS.
- (d) Employees are expected to cooperate fully with any Risk Assessments being conducted on systems for which they are held accountable.
- (e) Employees are further expected to work with the DHS IT Security Office and the DHS Privacy Office in the development of a remediation or corrective action plan and maintain a "Plan of Action" and "Milestone" for any issues discovered in the risk assessment process.
- (f) National Institute of Standards and Technology 800-37 framework will be complied with:
  - (1) Identification of a risk will be the responsibility of all DHS employees, contactors or third party vendors. Once a risk has been identified all individuals involved will follow the DHS Risk Management Procedure. The risk level will be defined by the Chief Information Security Officer (CISO) and the DHS Privacy Officer prior to mitigation or acceptance.

- (2) Mitigation plan for risk will be developed by the division's designee in conjunction with Security and Privacy teams and delivered to the CISO or the DHS Privacy Officer in writing for approval prior to implementation.
- (3) Acceptance of any risk with a severity level of Medium or higher will be evaluated by the Chief Information Officer (CIO) and division director of the affected divisions prior to final approval, documentation, and scheduling of periodic review of the risks.
- (g) The execution, development, and implementation of remediation programs are the joint responsibility of the CIO, CISO, the DHS Privacy Officer and the department or office responsible for the system area being assessed.
- (h) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

### III. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

### IV. Definitions

- (a) "Corrective Action Plan" means a defined process to mitigate and eliminate an identified risk.
- (b) "Entity" means any business unit, department, group, or third party, internal or external to the DHS, responsible for maintaining the DHS assets.
- (c) "Plan of Action and Milestone" means documentation to show all known issues and vulnerabilities based on criticality and impact.
- (d) "Risk" means those factors that could affect confidentiality, availability, and integrity of DHS' key information assets and systems. The Chief Information Security Officer is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

### V. References

- (a) DHS, Office of Systems and Technology, Information Technology Unit

- (b) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (c) Cybersecurity Enhancement Act of 2014  
<https://www.congress.gov/bill/113th-congress/senate-bill/1353>
- (d) FBI Criminal Justice Information Services (FBI CJIS)  
<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>
- (e) Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/groups/SMA/fisma/>
- (f) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)  
<http://www.hhs.gov/ocr/privacy/>
- (g) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- (h) IRS Publication 1075 (IRS) <http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- (i) Social Security Administration Safeguards (SSA)  
<http://www.ssa.gov/dataexchange/security.html>
- (j) US Privacy Act of 1994 (Dept of State) <http://foia.state.gov/Learn/PrivacyAct.aspx>.

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 122

### **Title: Information Systems Development & Acquisition Procedures**

#### I. Applicability

These procedures apply to all employees, divisions, offices, contractors, and vendors participating in the development and acquisition of information systems within DHS.

#### II. Procedures

- (a) The development of all requests for the acquisition of information systems technology or services (hardware, communications equipment, professional services and open market software acquisitions) will be coordinated with the DHS Chief Information Officer (CIO). The development process shall include a business evaluation and systematic selection based on defined system requirements. All such acquisitions will be reviewed by the CIO or designee and will be subject to the CIO's approval.
- (b) To ensure the security and integrity of DHS data, all software purchased or used within DHS systems shall be within the current version and two (2) revisions and updated as released. This includes supporting software such as Java, Silverlight and web browsers.
- (c) All DHS project managers and application owners will work with the DHS IT Security Office and the DHS Privacy Office during the planning, purchasing, and development phases to ensure compliance with all applicable state and federal laws. The CIO must approve all protected data integration with the system to ensure the confidentiality and integrity of the data and network.
- (d) The DHS Office of Systems Technology (OST) will coordinate the acquisition, evaluation, and selection process. The purpose of coordination is to ensure effective utilization of available DHS information hardware and network resources, to assess compatibility with current systems and architectures, and to determine the acquisition's conformance with the IT Plan and DHS' technology strategy.
- (e) There is to be no use of live data in development environments due to the significant risk involved. DHS will minimize such risk by using test data (fictional data) during the development of information systems, information system components, and information system services. Should any testing require the use of live data, the appropriate security controls (as determined by OST) must be in place to protect the data.
- (f) The IT Security Office will include safeguards including secure coding practices, configuration management and control, trusted procurement processes, and

monitoring practices to help ensure that software does not perform functions other than the functions intended.

- (g) The CIO or designee will assist the division with the business evaluation, as needed. At the CIO's discretion, Joint Application Development sessions may be required to facilitate or inform the system selection process. The CIO or designee will manage, with the requesting division's participation, the system selection process and any required Joint Application Development sessions.
- (h) The requesting division shall ensure the selected system solution is included in the current biennial IT Plan and that the planned solution does not exceed the planned cost estimate in the IT Plan. If not included in the current IT Plan or if the solution exceeds the IT Plan cost estimate, the requesting division must submit to the CIO supporting documents required to amend the IT Plan. The Department of Information Systems (DIS) shall provide technical assistance, as needed, in addressing IT Plan requirements.
- (i) Upon completion of the evaluation and selection process and obtaining the CIO's approval, OST will process the acquisition request as follows:
  - (1) OST will submit items not included within the IT Plan that require approval by the Department of Information Systems (DIS); and,
  - (2) Items approved for acquisition by DIS, and those items covered within the IT Plan, but not requiring DIS approval, will be processed by OST's purchasing agent.
- (j) The requesting division shall submit the approved acquisition request from the CIO to the DHS Office of Finance and Administration's Contract Support Section for review to ensure compliance with state contract and purchasing requirements.

### III. Service Agreements

Any service agreements with outside vendors and contractors that may require the release of protected health information requires the approval of the DHS Privacy Officer prior to activation.

### IV. Other

- (a) All requests for application development must be submitted to the CIO, with a DHS-357 "Application Development Request" form located on DHS Share at <https://dhsshare.arkansas.gov/DHS%20Forms/DHS-357.doc>.
- (b) Only Voice-over Internet Protocol (VoIP) devices that are purchased through OST shall be connected to any part of DHS' Information Systems. Before any VoIP device is purchased, it must either be on a list of DHS approved devices or must be reviewed and approved by the CIO. After a VoIP device has been purchased, it

must be registered with Unified Communications Services and connected to DHS Information Systems according to established network and security procedures. Use of VoIP devices will adhere to OST's applicable policy and procedures.

- (c) Requests for exceptions to this procedure must be submitted in writing and approved in writing by the DHS CIO. Exceptions, if granted, will not violate compliance with any federal or state law, rule, or regulation and must be renewed by the CIO annually.

## V. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in restriction or suspension of all network access to DHS systems or applications. Employees who can't complete job duties or assignments without such access may be terminated or face disciplinary action as outlined in DHS Policies 4002 "Privacy and Security Sanctions" and 1084, "Employee Discipline."

## VI. Definitions

- (a) "Hardware" means desktop and laptop computer equipment, other electronic data processing equipment and peripherals, and all devices attached to the state network. This applies to leased or purchased hardware.
- (b) "Communications Hardware" means all information transmission and switching equipment and all devices attached to the state network. This applies to leased or purchased communications hardware. (Excluded for the purposes of this policy are telephones, cell phones, pagers and similar mobile devices.)
- (c) "Open Market Software" means all information technology applications and system architectures acquired from sources outside of the Department of Human Services.
- (d) "Internally Developed Applications" means all software applications developed by Department of Human Services employees and not acquired through contract or state purchasing procedures. Provisions of this policy apply explicitly to those applications developed for multi-user environments.
- (e) "Internally Developed Applications-Web Based" means all web-based applications developed by Department of Human Services employees and not acquired through contract or state purchasing procedures. For the purposes of this policy, a web-based application is defined as any file or collection of files created for live internet or intranet functionality beyond the simple posting of content.
- (f) "Software Produced by Contracted Vendor" means all software applications and system architectures developed by a vendor under the terms of an approved contract.

- (g) “Professional Services” means all Information Systems Technology professional and consulting services acquired from sources outside the requesting DHS division. (Excluded for the purposes of this policy are hardware repair services and maintenance agreement renewals.)

## VI. References

- (a) State of Arkansas Policies and Standards:  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>
- (b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001\\_dataclass\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf)
- (c) Arkansas State Security Office Data and System Classification Grid Guidelines:  
<http://www.dis.arkansas.gov/policiesStandards/Documents/DataClassificationGuide.pdf>
- (d) Arkansas State Security Office Data Classification Grid Form:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/data\\_grid.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/data_grid.pdf)
- (e) State of Arkansas Standard Statement-Encryption -Document Number: SS-70-006:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT\\_encryption\\_standard\\_2011.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT_encryption_standard_2011.pdf)
- (f) State of Arkansas Security Office Financial and Risk Impact Statement for Proposed Encryption Standard:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryption\\_financial.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryption_financial.pdf)
- (g) State of Arkansas Security Office Information on Backup Encryption Methods:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryp\\_impactinfo.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryp_impactinfo.pdf)
- (h) State of Arkansas Security Office Encryption Standard Guidelines:  
[http://www.dis.arkansas.gov/policiesStandards/Documents/comply\\_encryp\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/comply_encryp_standard.pdf)
- (i) Department of Human Services Policy 4006: HIPAA Privacy Requirements in the Use of eMail and Facsimile Services:  
<https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx>
- (j) Department of Human Services Policy 5009: Mobile Computing and Teleworking:  
<https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx>
- (k) Department of Human Services Policy 5012: Data Classification:  
<https://dhsshare.arkansas.gov/DHS%20Policies/Forms/By%20Policy.aspx>
- (l) National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP): <http://csrc.nist.gov/groups/STM/cmvp/index.html>
- (m) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications: <http://csrc.nist.gov/publications/PubsSPs.html>
- (n) Federal Information Processing Standards Publications (FIPS PUBS):  
<http://itl.nist.gov/fipspubs/>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 123

### Title: Data Classification Procedure

#### I. Applicability

This procedure establishes and maintains a data classification mechanism that includes the determination of sensitivity, labeling, and access control of data to ensure that all DHS data is evaluated and properly classified as mandated by various federal and state regulations. This procedure applies to all employees and users granted access to DHS Information Systems or who handle DHS data.

#### II. Procedure

- (a) Data owned and maintained by DHS shall be put into appropriate classification levels according to its confidentiality, integrity, and availability. The level of security controls implemented shall be commensurate with the classification of sensitivity of the information and magnitude of loss or harm that could result from improper access.
- (b) The assigned security classifications shall be maintained by the DHS IT Security Office in a central “DHS Information Technology Information Resource Inventory.”
- (c) Procedures developed and maintained by the IT Security Office will enable the system owner, data custodian, and other key individuals to make decisions regarding the confidentiality of data. The classification will establish the general requirements for the implementation of security controls. The determination of confidentiality will be documented and maintained on file with the system owner.
- (d) The availability classification shall be determined by the system owner, based upon the overall needs of the system to be available to the department’s critical business functions. The recovery category determines how soon the application and the network should be available and online after disaster or other malfunction.

#### III. Data Classification Labeling and Access Controls

- (a) DHS divisions and offices shall implement the appropriate safeguards based on the confidentiality level of the data to include “Unrestricted,” “Sensitive,” and “Confidential.”
  - (1) “Unrestricted Data” is characterized as public data with no distribution limitations. These data elements are from information that is actively made public by the state government. It is published and distributed without restriction. It is available in the form of physical documents such as brochures, formal statements, press releases, reports and in electronic forms such as internet web pages and bulletin boards. This information is accessible

with anonymous access. The greatest security threat to this data is from unauthorized or unintentional alteration, distortion or destruction of the data. Security efforts appropriate to the criticality of systems containing this data must be taken to maintain its integrity (e.g. DHS Public Websites);

- (2) “Sensitive Data” is data elements of information that is made available through open records requests, formal or legal processes. Sensitive data is intended for use only by individuals who require the information in the course of performing their duties. Redaction of data elements is required for this level of information if released. Security threats to this data include violations of privacy statutes or federal regulations, in addition to unauthorized alteration or destruction. If this data was accessed by unauthorized persons, it could cause financial loss, identity theft, or breach of protected information (e.g. Personnel Records, IP Addresses, Emergency Contact Information, Application Source Code, Security Video Footage, Communications Systems, and Competitive Bids); and,
  - (3) “Confidential Information” is data whose disclosure could be hazardous to the health of citizens or a breach to DHS applications or network. This category includes the majority of the data contained within the DHS network. These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health, or safety repercussions. Strict rules must be followed in the usage of this data (e.g. Health Information, Personally Identifiable Information, Law Enforcement Investigative records, Educational Records, Audit responses, Social Security Numbers, Federal Tax Information and Adoption Records).
- (b) DHS divisions and offices shall implement the appropriate classification level for data and systems according to these criticality levels:
- (1) Non-Critical: These systems are necessary to state government but short-term interruptions or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of the citizens. They could be easily offset with manual procedures;
  - (2) Critical: These systems are required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data and systems can be restored; and
  - (3) Extremely Critical: These data and systems are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business.

- (c) Each DHS division and office shall utilize more stringent security control requirements when the security level of an information system, facility, or network is designated at the “Sensitive” or “Confidential” level. In all instances, the minimum security requirements of a system should be appropriate for the highest security level designation of any data the DHS division and office processes within that system, including data received from other agencies.
- (d) For each security level classification, there are controls that define the protection of information being processed for these types of activities:
  - (1) Copying and storage;
  - (2) Destruction; and,
  - (3) Transmission by mail, electronic email, fax, internet, intranet, and storage media.
- (e) Output from systems containing DHS information shall carry an appropriate classification label on the output. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CDs, cassettes), electronic messages, and file transfers.
- (f) Physical labels are generally appropriate; however, data in electronic form cannot be physically labeled. An electronic means of labeling must be implemented, as applicable.
- (g) The IT Security Office shall:
  - (1) Develop and maintain enterprise-wide procedures to assist divisions and offices on labeling data;
  - (2) Provide guidelines for access control to that data including electronic marking and physical labeling; and,
  - (3) Provide assistance in determining the integrity classification of each business application used.
- (h) For an illustration on how the classification works, utilize the “Data Classification Matrix” attached to this procedure.

#### IV. Application and System Security Controls

All DHS Applications and Systems shall implement the appropriate security controls to minimize risk in the production or operating environment. The type of controls necessary will be appropriate with the determination of data confidentiality, integrity, and availability levels. The DHS Chief Information Security Officer (CISO) shall certify the controls as appropriate, based on the classification of the data or system.

## V. Data Transfers

- (a) The use of non-encrypted mobile devices for transfer of confidential information such as PII, PHI, and FTI is restricted. This includes but is not limited to: text messaging, external applications, and non-DHS email. DHS will maintain acceptable standards for delivery of protected information. This means DHS employees or contractors cannot use personal phones or devices that are unencrypted for DHS business related tasks such as taking pictures for investigations or the use of text messaging DHS or client related data.
- (b) The record of transfer of any data containing Protected Health Information (PHI) and Federal Tax Information (FTI) will be logged separately. The logs will be maintained by the DHS Privacy Office. PHI logs will be reviewed and approved by the DHS Privacy Officer. The FTI log will be reviewed and approved by the CISO and Privacy Officer.
- (c) DHS shall utilize the three tiered architecture for the storage of data for the Demilitarized, Middleware, and Private zones. All protected data shall be located in a Private Zone, public access will be located in Demilitarized Zone, and all other data located in Middleware Zone.

## VI. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

## VII. Exceptions

Any requests for exceptions to this procedure must be submitted in writing and approved by the DHS Chief Information Officer. Exceptions shall be reviewed annually and require approval on an annual basis. Exceptions will not violate compliance with any federal or state law, rule, or regulation.

## VIII. Definitions

- (a) "DHS Data" means any information which is maintained in any form within DHS. Any grouping of data is classified based on data confidentiality, integrity, and availability.
- (b) "DHS Information Systems" means the DHS Network services, Network Access, including e-mail and internet access, DHS applications including client-server, web-based and mainframe applications or any third-party software legally acquired and installed on DHS devices. This also includes any computer file on any device in use

- by DHS or its agents that is shared across the DHS network and requires DHS support or that contains DHS-related information.
- (c) “Demilitarized Zone” means in computer networks, a Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network.
  - (d) “Middleware Zone” Zone where computers and devices are located and systems not containing protected data.
  - (e) “Private Zone” means a restricted access location designed to protect data.
  - (f) “Protected Information” means any data classified as Sensitive or Confidential.
  - (g) “Protected Health Information” means as defined in the HIPAA, 45 CFR 160.103.
  - (h) “Personally Identifiable Information” means information that can be used on its own or with other information to identify, contact or locate a single person to identify an individual in context as defined by the U.S. Privacy Act and Arkansas Personal Information Protection Act (PIPA).
  - (i) “Federal Tax Information” means any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information as defined by IRS Publication 1075. FTI data may not be masked to change the character of information to circumvent requirements.

## IX. References

- (a) Arkansas Data and System Security Classification  
[http://www.techarch.state.ar.us/domains/security/standards/SS-70-001\\_dataclass\\_standard.pdf](http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf)
- (b) Cybersecurity Enhancement Act of 2014  
<https://www.congress.gov/bill/113th-congress/senate-bill/1353>
- (c) Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/groups/SMA/fisma/>
- (d) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (e) Health Insurance Portability and Accountability Act CFR parts 160, 162 and 164 (HHS HIPAA)  
<http://www.hhs.gov/ocr/privacy/>
- (f) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- (g) Social Security Administration Safeguards (SSA)  
<http://www.ssa.gov/dataexchange/security.html>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 124

### Title: DHS Information Systems Change Management Procedures

#### I. Applicability

These procedures apply to all employees and authorized users who install, operate, or maintain DHS information resources.

#### II. Scope

This procedure ensures that changes to information systems are deployed in a controlled manner so that DHS users and clients can plan accordingly. Changes require careful evaluation, prioritization, planning, testing, implementation and documentation to reduce negative impact to DHS' business and user community. Management of these changes is a critical part of providing strong and valuable information systems throughout the agency.

#### III. Procedures

- (a) All changes to the DHS information systems or resources shall comply with this procedure.
- (b) All changes affecting DHS' computing environmental facilities (for example, air conditioning, water, heat, plumbing, electricity, and alarms) need to be reported and coordinated with the DHS Chief Information Officer (CIO) or Chief Information Security Officer (CISO). These changes shall adhere to any applicable state regulations.
- (c) All change requests must be submitted in writing to the CIO or designee by the end of business on Wednesday to be reviewed by the DHS Change Management Committee on Friday.
- (d) The members of the DHS Change Management Committee meets with the appropriate agency systems managers to review, assess, and evaluate all change requests.
- (e) If the proposed change is authorized, the committee plans the update and coordinates the implementation of the change, then after the final review, the change process is closed.
- (f) The CIO or CISO and the DHS Change Management Committee may deny the standard change or an emergency change for the following reasons:
  - (1) Planning (for example, inadequate planning related to implementation, risk assessment, testing, back-out);

- (2) Timing (for example, timing of a change that would negatively impact a key business process such as year-end accounting);
  - (3) Documentation (for example, inadequate documentation related to disaster recovery, security testing methodology/data); or
  - (4) Resources (for example, adequate resources may particularly be a problem on weekends, holidays, or during special events).
- (g) DHS user notification (located on the DHS Sharepoint site) must be completed for each Standard and Emergency Change by utilizing these procedures included in this section.
- (h) A Change Management log must be maintained for all changes. The log must contain, but is not limited to:
- (1) Date of submission and date of Change;
  - (2) Owner and custodian contact information;
  - (3) Nature of the Change; and,
  - (4) Indication of success or failure.
- (i) A change review must be completed and documented for all changes, whether the change is successful or not.
- (j) All DHS Information Systems, network devices, and databases will use approved baseline configurations and hardening per the DHS Configuration Standards and National Institute of Standards Technology guidelines. Any deviation from the standard baseline configuration must be approved by the CIO or CISO prior to implementation.
- (k) The DHS IT Security Office ensures that DHS maintains information and system integrity through intrusion detection systems that facilitate notification of unauthorized changes.

#### IV. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

#### V. Definitions

- (a) "Back-out Plan" means a plan that documents all actions to be taken to restore a service or service component if the associated Change or Release fails or partially fails. Back-out plans may provide for a full or partial reversal.

- (b) “Change” means the addition, modification or removal of an authorized, planned or supported service or service component and its associated documentation. All Changes must be registered by the Change Management process.
- (c) “Emergency Change” means an authorized modification that is intended to repair a failure in an Information Technology service that may have a significant negative impact on DHS business.
- (d) “Standard Change” means an authorized, planned modification or upgrade of a service or infrastructure component that is of low risk.
- (e) “Change Management” means the process responsible for the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to DHS Information Systems. The process includes the management and coordination of the processes, systems and functions required for the packaging, building, testing and deployment of a release into production, and establish the service specified in the customer and stakeholder requirements.
- (f) “DHS Information Systems” means the DHS Network services (Network access, Email, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS device for which they were intended. A DHS Information System also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or that requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.
- (g) “DHS User” means a person whose identity has been validated, whose association with DHS has been certified by the division with whom the person is affiliated, who has been granted access to any DHS Information Systems, and who is held accountable for the security of such access. A DHS User may or may not be a DHS employee.
- (h) “Information Resources” means any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA) devices, pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- (i) “Release” means a collection of hardware, software, documentation, processes or other components required to implement one or more approved Changes to DHS Information Services. The contents of each Release are managed, tested, and deployed as a single entity.

- (j) “Request for Change (RFC)” means a formal proposal for a change to be made. A Request for Change includes details of the proposed change.
- (k) “DHS System Manager” means the persons exercising management authority for a DHS-supported network service or application system. The role of such persons provides DHS ownership for the DHS service or system.

## VI. References:

- (a) Arkansas Physical and Logical Security Standard for Information Technology Resources (SS-70-008) [http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-008\\_phys\\_log\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-008_phys_log_standard.pdf)
- (b) Arkansas Physical and Logical Security Standard Guidelines Document Number SS-70-008 [http://www.dis.arkansas.gov/poli stan\\_bestpract/pdf/PhyLogGuidelines.pdf](http://www.dis.arkansas.gov/poli stan_bestpract/pdf/PhyLogGuidelines.pdf)
- (c) Health Insurance Portability and Accountability Act of 1996 (HIPAA) <http://www.hhs.gov/ocr/privacy> And Patient Protection and Affordable Care Act of 2010
- (d) Information Technology Infrastructure Library version 3 (ITIL v3) <http://www.itil-officialsite.com/home/home.asp>
- (e) Copyright Act of 1976; U.S. Copyright Law of 2007; Enactments to amend U.S. Copyright Law, 2008; <http://www.copyright.gov/title17>
- (f) Foreign Corrupt Practices Act of 1977, as amended [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/47mcrm.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/47mcrm.htm)
- (g) Computer Fraud and Abuse Act of 1986 [http://www.justice.gov/criminal/cybercrime/1030\\_new.html](http://www.justice.gov/criminal/cybercrime/1030_new.html)
- (h) Computer Security Act of 1987 <http://www.csp.noaa.gov/policies/csa-1987.htm>
- (i) Critical infrastructure Executive Order 13636
- (j) IRS Publication 1075
- (k) Federal Information Security Management Act of 2002
- (l) The Health Information Technology for Economic and Clinical Health Act of 2009
- (m) The Privacy Act of 1974
- (n) Act 339 of 2007, State of Arkansas, PIPA, ACA 4-110-104
- (o) The e-Government Act of 2002
- (p) HHS Final Rule 155.260 Privacy and Security of Personally Identifiable Information
- (q) 26 U.S.C. §6103 Safeguards for Protecting Federal Tax Returns and Return Information
- (r) USA Patriot Act of 2001, USA Cyber Security Enhancement Act of 2002, USA Computer Fraud and Abuse Act of 1986
- (s) 18 U.S.C. § 1029. (Fraud and Related Activity in Connection with Access Devices); 18 U.S.C. § 1030. (Fraud and Related Activity in Connection with Computers); and 18 U.S.C. § 1362. (Communication Interference)

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 125

### Title: Information Systems Access Procedures

#### I. Applicability

These procedures apply to Authorized DHS Approving Managers (ADAMs) and users attempting to gain access to DHS Information Systems and describe the procedures needed to obtain access.

#### II. Procedure

- (a) All persons requiring access to DHS Information Systems must obtain permission from their divisions' ADAM and be authenticated through the Chief Information Officer's (CIO) designated Systems Administrators. ADAMs and new users must complete and sign DHS Form 359 (for employees) or 5002 (for contractors), "DHS Systems Security Access Request."
- (b) Hiring Supervisors are responsible for notifying their division or office's ADAM of a new employee and when an employee leaves or transfers. Hiring supervisors must complete a Form 359 or 5002 and submit to their division or office's ADAM for a change in a user's status (demographic data or type of access, etc.), the termination of a user, and when a user transfers to another location or division. In the case of a transfer, only the user's network account and email transfer. All other access will be based on the new permissions.
- (c) By signing DHS Form 359 or 5002, ADAMS certify that:
  - (1) Access requests are made on behalf of persons who are DHS employees in good standing or non-DHS users who are members of an organization with whom a formal agreement is in place to permit access to DHS systems and safeguard protected information;
  - (2) Users have provided accurate identifying information and have a legitimate and official purpose for the requested level of access;
  - (3) Users have been notified of DHS policies pertaining to the appropriate use of state equipment and systems and the safeguarding of private information and that users have completed the required DHS Security and Privacy training; and,
  - (4) He or she agrees to notify the DHS Systems Security Gateway of material changes in a user's employment status as it relates to the DHS network services or systems applications to which the user has been granted access.

- (d) By signing DHS Form 359 or 5002, DHS Information System users certify that he or she:
- (1) understands that access to state-furnished equipment, software, and data is restricted to authorized persons only and may be used for official business purposes only;
  - (2) accepts responsibility for appropriate utilization of state-furnished equipment and understands that computer devices, network activity, email, and internet access may be monitored to detect improper or illicit activity;
  - (3) has no expectation of privacy in the use of state-furnished computer equipment and services;
  - (4) agrees to take all necessary measures to safeguard the security of his/her access credentials (username, password, smart card) and is accountable for any unauthorized usage of access credentials that results from his/her negligence or purposeful action; the user agrees to immediately report any compromise of access credentials;
  - (5) understands it is a violation of state and federal law to use, permit the use of, or fail to safeguard the security of client information in any way that jeopardizes its confidentiality;
  - (6) is subject to DHS policies pertaining to safeguarding confidential or sensitive information, penalties for inappropriate use of state equipment and electronic communication services, and sanctions for violations of related DHS Conduct Standards; and,
  - (7) understands penalties for unauthorized access or inappropriate usage, for DHS or non-DHS users, may include discipline and/or prosecution.

### III. Integrated Systems Security Gateway

- (a) Upon receipt of DHS Form 359 or 5002 from the ADAM, the Security Gateway Administrator will match identity data against validation data sources. DHS users may be contacted by phone and verbally challenged for their AASIS number. The confirmation of other demographic information may be obtained at that time if the Gateway Administrator deems it appropriate. For non-DHS users, the ADAM will be contacted by phone and will be verbally challenged to verify collected information about the user and the request for new user access.
- (b) When validation of identity is not successful, the Gateway Administrator will notify the requesting ADAM that the access request was denied. When validation of identity is successful, the Gateway Administrator will re-direct the request to the appropriate Systems Administrators for processing.

#### IV. User Credentials and Security

- (a) Users are assigned a unique personal identifier (username) which must be authenticated in conjunction with a valid password or smart card to gain access to DHS Information Systems. ADAMs should instruct users to safeguard credentials with respect to both physical security and access to DHS Information Systems. The structuring of passwords will meet or exceed prevailing state government standards of at least eight characters with a mixture of alpha, numeric, and special characters.
- (b) All Windows or Active Directory based passwords will expire in 60 days and Mainframe based passwords will expire in 90 days, or earlier if changed by user. Users will receive system prompts to change passwords before they expire. Users may not reuse any of their last five passwords for DHS Network access or their last four passwords for Mainframe access. A password should be changed if a user suspects its security has been compromised.
- (c) Sharing of credentials is strictly forbidden. Written recording of credentials is discouraged but if recorded, the following rules should be observed:
  - (1) Never openly post User Credentials, particularly in proximity to the user's PC.
  - (2) Store recording of credentials in a secure location.
  - (3) Do not identify the recording as a password.
  - (4) Do not include User Name with password.
  - (5) Mix in false characters or scramble the password recording in a manner you will remember so the written version is different from the real password.
  - (6) Never record a password on-line or include it in an email message.

#### V. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policy 4002, "Privacy and Security Sanctions" and the DHS Employee Discipline policy.

#### VI. Systems Security Roles Defined

- (a) User: A person whose identity has been validated, whose association with DHS has been certified by the division with whom the person is affiliated, who has been granted access to any Department of Human Services information system, and who is held accountable for the security of such access. A user may or may not be a Department of Human Services employee.

- (b) Department of Human Services User: A person, Department of Human Services employee, who has been granted access to any Department of Human Services information system and is accountable for the security of such access.
- (c) Non-Department of Human Services User: A person, not a Department of Human Services employee, who has been granted access to any Department of Human Services information system and is accountable for the security of such access.
- (d) System Administrator: Collectively refers to persons exercising the following systems security roles: Security Gateway Administrator, Network Services Administrator, Mainframe Services Administrator, Windows Application Security Administrator, Mainframe Application Security Administrator, Systems Administrators for division supported applications, DHS CIO. The role of such persons is to provide technical support and access management for DHS network services and applications.
- (e) Security Gateway Administrator: Persons performing this role serve as the common point of entry for all user access requests. Primary functions include initial evaluation of received access requests, validation of identity, and re-directing of requests for additional processing.
- (f) ADAM: Authorized DHS Approving Manager – a class of DHS managers who have been authorized by each division’s ADAM administrator to certify user access requests. An ADAM must be a DHS employee. The role of the ADAM is to authorize the submission of security access requests for (1) employees within the manager’s division, and (2) non-DHS users affiliated with the manager’s division. ADAMs are responsible for the validity of both DHS User and non-DHS User information in all User Access Account records they have authorized (DHS Form 359 or DHS Form 5002, DHS Systems Access Request, available on DHS Share). ADAMs are responsible for notifying the Gateway Administrator of material changes that affect both DHS User and non-DHS User access privileges.
- (g) ADAM Administrator: A designee appointed by each division’s director to assume the role of managing and maintaining the currency of the division’s list of ADAMs. Only those managers appearing in each division’s list will be recognized by the Security Gateway Administrator for the purpose of submitting user access requests.

VII. References:

- (a) State of Arkansas Policies and Standards  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>
- (b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001  
[http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001\\_dataclass\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf)
- (c) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications <http://csrc.nist.gov/publications/PubsSPs.html>
- (d) Federal Information Processing Standards Publications (FIPS PUBS) <http://itl.nist.gov/fipspubs/>

- (e) Federal Information Security Management Act of 2002 (FISMA) <http://csrc.nist.gov/groups/SMA/fisma/>
- (f) Social Security Administration Safeguards (SSA) <http://www.ssa.gov/dataexchange/security.html>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 126

### Title: Acceptable Encryption Procedures

#### I. Applicability

This procedure applies to all DHS employees and affiliates authorized to use DHS Information Systems.

#### II. Scope

The DHS IT Security Office and the Office of Systems Technology (OST) will identify and classify the owners and locations of DHS' confidential, sensitive, or other critical data which requires encryption through its annual risk assessment process using tools and/or documented methodology approved by the DHS Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

#### II. Procedure

- (a) Proven, standard algorithms listed in the National Institute of Standards and Technology (NIST) cryptographic module validation list and validated to the current Federal Information Processing Standards (FIPS) standard shall be used as the basis for encryption technologies.
- (b) The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the DHS CIO or CISO.
- (c) DHS data to be encrypted includes, but is not limited to, the following:
  - (1) Data classified as "Sensitive Data" or "Confidential Information" (as detailed in "Data Classification Procedures" (APM 123));
  - (2) DHS Information Systems users' login credentials;
  - (3) All portable media/mobile computing devices;
  - (4) Data at rest;
  - (5) Data in motion; and,
  - (6) Offsite data storage.
- (d) Non-approved protocols such as FTP and Telnet will not be permitted without prior approval by the CIO or CISO. A list of non-approved protocols will be

maintained in the DHS encryption standard, as kept by OST. Encryptions will be audited per the “IT Security Audit Compliance Procedure” (APM 120).

#### IV. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can’t complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, “Privacy and Security Sanctions” and 1084, “Employee Discipline: Conduct/Performance.”

#### V. Definitions

- (a) “Proprietary Encryption” means an algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or a government.
- (b) “Symmetric Cryptosystem” means a method of encryption in which the same key is used for both encryption and decryption of the data.
- (c) “Asymmetric Cryptosystem” means a method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).
- (d) “Mobile Computing Device” means a term used to describe portable and/or pocket-sized computing devices, typically having a display screen with touch input and/or a miniature keyboard; examples include mobile tablet/laptop computers, personal digital assistants (PDAs), and smartphones.
- (e) “Data at Rest” means a term used to describe all data in storage but excludes any data that frequently traverses the network or that which resides in temporary memory. Data at rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, USB flash drives, files stored on backup tape and disks, and also files stored off-site or on a storage area network (SAN).
- (f) “Data in Motion” means a term used to refer to the transfer of that data between all copies and versions of the original file, such as data traversing a local area or wide area network (such as the Internet).
- (g) “Offsite Data Storage” means a term used to describe data stored for backup and restore at a separate geographic location from where that data is actually being created or accessed.

#### VI. References

- (a) State of Arkansas Policies and Standards  
<http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx>

- (b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001  
[http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001\\_dataclass\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf)
- (c) Arkansas State Security Office Data and System Classification Grid Guidelines  
[http://www.dis.arkansas.gov/policiesStandards/Documents/DataClassification\\_Guide.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/DataClassification_Guide.pdf)
- (d) Arkansas State Security Office Data Classification Grid Form  
[http://www.dis.arkansas.gov/policiesStandards/Documents/data\\_grid.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/data_grid.pdf)
- (e) State of Arkansas Standard Statement-Encryption -Document Number: SS-70-006  
[http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT\\_encryption\\_standard\\_2011.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/DRAFT_encryption_standard_2011.pdf)
- (f) State of Arkansas Security Office Financial and Risk Impact Statement for Proposed Encryption Standard  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryption\\_financial.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryption_financial.pdf)
- (g) State of Arkansas Security Office Information on Backup Encryption Methods  
[http://www.dis.arkansas.gov/policiesStandards/Documents/encryp\\_impactinfo.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/encryp_impactinfo.pdf)
- (h) State of Arkansas Security Office Encryption Standard Guidelines  
[http://www.dis.arkansas.gov/policiesStandards/Documents/comply\\_encryp\\_standard.pdf](http://www.dis.arkansas.gov/policiesStandards/Documents/comply_encryp_standard.pdf)
- (i) National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP)  
<http://csrc.nist.gov/groups/STM/cmvp/index.html>
- (j) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications  
<http://csrc.nist.gov/publications/PubsSPs.html>
- (k) Federal Information Processing Standards Publications (FIPS PUBS)  
<http://itl.nist.gov/fipspubs/>
- (l) IRS Publication 1075 (IRS)  
<http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- (m) FBI Criminal Justice Information Services (FBI CJIS)  
<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>
- (n) CMS Minimum Acceptable Risk Standards (CMS MARS-E 2.0)  
<https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf>
- (o) Health Information Technology for Economic and Clinical Health Act (HHS HITEC)  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 127

### Title: Voice-over Internet Protocol Procedures

#### I. Applicability

This procedure applies to all DHS users who are authorized to purchase and connect voice over internet protocol (VOIP) devices to DHS Information Systems. VOIP is a technology that enables voice conversations over data networks and between those networks and legacy phone networks. VOIP consists of a number of hardware and software components that provide the voice services required by DHS.

#### II. Procedure

- (a) All VOIP components purchased by DHS divisions and offices will have the features needed by the agency and will adhere to the VOIP network and security standards that DHS implements.
- (b) Only VOIP devices that are purchased through DHS Office of System and Technology (OST) shall be connected to any part of the DHS Information Systems. Before any VOIP device is purchased, it must either be on a list of DHS approved devices or must be reviewed and approved by the DHS Chief Information Officer (CIO) or designee. After a VOIP device has been purchased, it must be registered with Unified Communications Services and connected to DHS Information Systems according to established network and security procedures.
- (c) OST will be responsible for:
  - (1) maintaining a list of approved VOIP devices;
  - (2) approving unlisted devices; and,
  - (3) maintaining a registry of connected VOIP devices.
- (d) The DHS IT Security Office is responsible for:
  - (1) developing, certifying, and clarifying VOIP device network and security procedures; and,
  - (2) investigating and notifying any DHS user attempting to violate the DHS VOIP Device Procedure.

### III. Review and Measurement

- (a) OST will periodically review the VOIP registry to verify devices are within compliance.
- (b) If a DHS division or office purchases a VOIP device that is not on the approved list or has not been approved by the DHS CIO or designee, it will not be allowed to connect to DHS Information Systems.

### IV. Other

Although there are a number of national and international standards (along with proprietary features) that voice over internet protocol vendors implement in their products, adoption of these standards do not guarantee multi-vendor voice over internet protocol interoperability. Some voice over internet protocol standards compete with one another and others are still maturing. In addition, not all VOIP vendors implement the features that DHS users need.

### V. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

### VI. References

- (a) Security Considerations for Voice Over Internet Protocol Systems (National Institute of Standards and Technology Special Publication 800-58,) <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- (b) IRS Publication 1075 (IRS) <http://www.irs.gov/pub/irs-pdf/p1075.pdf>
- (c) Federal Information Security Management Act of 2002 (FISMA) <http://csrc.nist.gov/groups/SMA/fisma/>
- (d) CMS Minimum Acceptable Risk Standards (CMS MARS-E) <http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 128

### Title: Information Systems Disaster Recovery and Continuity Procedure

#### I. Applicability

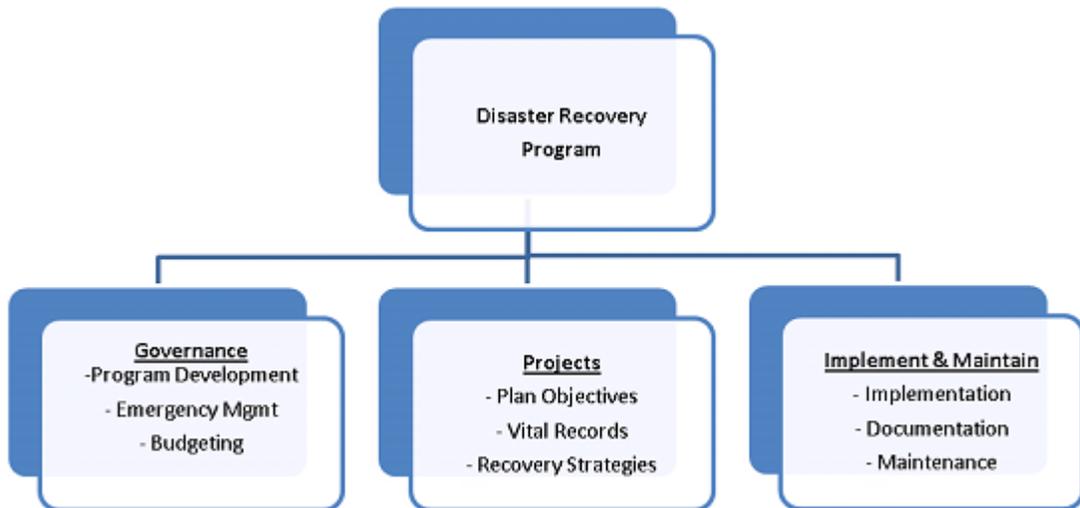
The Disaster Recovery and Continuity Procedures apply to all DHS users, managers, and contractors with critical systems managing or hosting DHS data, processing and/or services. All IT-managed systems must comply with this procedure.

#### II. Scope

This procedure defines acceptable methods for disaster recovery planning, preparedness, management, and mitigation of IT systems and services at DHS. The disaster recovery standards in this procedure provide a systematic approach for safeguarding the vital technology and data managed by the Office of Systems Technology (OST). It also provides a framework for the management, development, and implementation and maintenance of a disaster recovery program for the systems and services managed by OST.

#### III. Procedure

- (a) DHS Disaster Recovery Planning is a program that has a continuous lifecycle. The high-level processes for DHS Disaster Recovery (DR) Cycle steps are detailed in a flowchart below:



- (b) The Chief Information Officer (CIO) and Chief Information Security Officer (CISO) are responsible for IT DR program coordination and project management: including reporting status of IT DR planning, testing, and auditing activity on a regular basis; annually.

- (c) The CIO is responsible for ensuring sufficient financial, personnel and other resources are available as needed.
- (d) The CIO and CISO will review and update the DR Procedure as necessary at minimum annually. All modifications must be approved by the CIO and the CISO.
- (e) The IT Disaster Recovery Program (DRP) addresses the protection and recovery of DHS IT services so that critical operations and services are recovered in a timeframe that ensures the survivability of DHS and is commensurate with client obligations, business necessities, industry practices, and regulatory requirements.
- (f) Plans must be developed, tested, and maintained to support the objectives of the Program, and those plans should include relevant IT infrastructure, computer systems, network elements, and applications. At minimum, annual updating is required.
- (g) The CIO or designee is responsible for conducting Business Impact Analyses (BIA) to identify the critical business processes, determine standard recovery timeframes, and establish the criticality ratings for each; at least annually or when a significant change occurs.
- (h) The CIO or designee is responsible for conducting Capability Analyses (CA) to determine IT's capacity to recover critical IT services that support defined critical business processes and recovery objectives; at least annually.
- (i) The CIO or designee is responsible for maintaining the Recovery Tier Chart, which defines the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of all IT-managed systems. The application managers are required to prioritize their IT processes and associated assets based upon the potential detrimental impacts to the defined critical business processes.
- (j) Application managers required to create disaster recovery plans for the IT portion - including services, systems, and assets - of critical business processes. These IT services, systems, and assets must be inventoried and correlated according to the technical service catalog, prioritized based upon results of the business impact analysis, and ranked according to their RTO and RPO.
- (k) A risk assessment must be conducted annually to determine threats to disaster recovery and their likelihood of impacting the IT infrastructure.
- (l) For each risk or vulnerability identified in the risk assessment, a mitigation or preventive solution must be identified and a corrective action plan must be developed and sent to IT Security for review.
- (m) The IT DRP must include a change management and quality assurance process.

#### IV. Emergency Management

- (a) DHS Divisions will assign a Disaster Recovery Manager.

- (b) The IT Disaster Recovery Manager is responsible for overseeing IT DR activities, for their divisions, in the event of an emergency -i.e., an unplanned outage where RTO is in jeopardy.
- (c) The IT Disaster Recovery Manager should be part of the IT representation within the institution's Emergency Management Team.
- (d) Each division must develop and maintain a documented emergency plan including notification procedures.
- (e) Each division shall account for its associates when a building evacuation is ordered. Supervisory personnel are responsible to account for the associates they supervise.
- (f) The IT Disaster Recovery Team/Manager is required to complete a post-mortem report documenting outages and recovery responses within forty-five (45) days after the occurrence of a disaster recovery event.

#### V. Plan Objective

- (a) Division DR Plans must provide information on Business Impact Analysis, Data Backup, Recovery, Business Resumption, Administration, Organization Responsibilities, Emergency Response & Operations, Training and Awareness and Testing.
- (b) Plans must contain Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
- (c) Technological solutions for data availability, data protection, and application recovery must be considered by data gathered by the BIA and CA.

#### VI. Vital Records

- (a) OST shall maintain a single, comprehensive electronic inventory of all servers, network equipment, relevant configuration, and model information, and the applications they support. This inventory should be aligned with the service catalog and the technical service catalog.
- (b) All physical backup data must be labeled and logged, and are available for use during an emergency within stated recovery time objectives. A documented decision making process will be used to determine what subset of backup data will be additionally encrypted, and stored off-site in a secured location outside of the geographical area of the system they are backups of.
- (c) DR plans must be stored in a single, comprehensive database.
- (d) DR plan owners need to be able to access a copy of emergency and recovery plan(s) independent of IT services and/or network.

- (e) Upon completion or update, DR plans must be sent to the CIO and CISO for review.
- (f) Plan information must be reviewed and updated as warranted by business and/or information systems environment changes, at least annually.

#### VII. Plan Attributes

- (a) Plans must address an outage that could potentially last for a period of up to six weeks.
- (b) Plans must identify risk exposure and either accept the risk or propose mitigation solution(s).
- (c) Backup strategies must comply with predefined businesses continuity requirements, including defined recovery time and point objectives. Backup strategies must be reviewed at least annually or whenever any significant change occurs.
- (d) Recovery strategies must meet recovery objectives defined in the “DR Tier Chart.”
- (e) Approved recovery strategies must be tested to ensure they meet required recovery time and recovery point objectives.
- (f) Recovery strategies must be implemented within a previously agreed upon period of time, generally not more than one hundred and eighty (180) days after management approval.
- (g) The CIO or designee is required to provide DR training and awareness activities at least annually.

#### VIII. Maintenance

- (a) Plans must contain current and accurate information.
- (b) Planning must be integrated into all phases of the IT system life cycle.
- (c) IT DR tests that demonstrate recoverability commensurate with documented IT DR plans must be conducted regularly; as well as when warranted by changes in the business and/or information systems environment.
- (d) Backup media supporting critical business processes must be tested semi-annually. Reviews are required within sixty (60) days after a test to correct exposed deficiencies.
- (e) Plan revisions must be completed within sixty (60) days after a DR test is completed.
- (f) The following maintenance activities must be conducted annually:

- (1) Update the documented DR plan;
  - (2) Review the DR objectives and strategy;
  - (3) Update the internal and external contacts lists;
  - (4) Conduct a simulation/desktop exercise;
  - (5) Conduct a telecommunication exercise;
  - (6) Conduct an application recovery test;
  - (7) Verify the alternate site technology;
  - (8) Verify the hardware platform requirements; and,
  - (9) Submit the DR Status and Recoverability Report.
- (g) IT managers in DHS divisions and offices are responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.

#### IX. Failure to Comply

Failure to comply with these procedures as well as any DHS IT Security Policy or Procedure may result in termination or disciplinary action as outlined in DHS Policies 4002 “Privacy and Security Sanctions” and 1084, “Employee Discipline.”

#### X. References

- (a) DHS, Office of Systems and Technology, Information Technology Unit
- (b) CMS Minimum Acceptable Risk Standards (CMS MARS-E)  
<http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>
- (c) IRS Publication 1075 (IRS) <http://www.irs.gov/pub/irs-pdf/p1075.pdf>

# DHS ADMINISTRATIVE PROCEDURES MANUAL

## Chapter 129

### Title: Data Destruction and Information Processing Equipment End of Life Procedures

#### I. Applicability

These procedures specify the steps for the safe retirement and/or disposal of Data Storage Media and Information Processing Equipment from agency use as required by Ark. Code Ann. §25-34-102, and ensures compliance with all applicable federal (HIPAA) regulations regarding the security of confidential information. This chapter applies to all DHS employees, volunteers, and contractors or entities that handle DHS information or interact with Information Processing Equipment or Data Storage Media.

#### II. Document Destruction

Use only the locked shred bins to destroy confidential documents when they are no longer needed. Do not use the recycling bins to dispose of documents that contain Protected Health Information (PHI), Personal Identifying Information (PII), Federal Tax Information (FTI), or Social Security Administration (SSA) data. All DHS Divisions and Offices will work with the DHS IT Security Office and the DHS Privacy Office during the planning, purchasing, and development phases of shredding contracts to ensure the destruction of confidential documents is handled appropriately.

#### III. Media Destruction

- (a) The DHS Office of Systems Technology (OST) provides a secure method for the physical destruction of media. Shredders capable of destroying media in accordance with state and federal rules and regulations may be used by divisions.
- (b) Physical destruction is the preferred method of media disposal as outlined below in the Destruction Matrix. However, media overwrites may be utilized by using secure deletion software that's authorized and provided by the DHS Chief Information Officer (CIO) or designee.
- (c) Media disposal, physical destruction, wipes and sanitizing, must follow the Destruction Matrix below:

Media	Clear/Wipe	Sanitize
Tape	a	a or d
Floppies	a, b	d
Non-Removable Rigid Disk (hard drive)	b	a, c, or e
Removable Rigid Disk (Zip, Jaz, other)	a, b	a, c or d
<b><i>Optical Disk (CD-R, CD-RW, DVD+R, DVD-R, DVD+RW, DVD-RW, etc.)</i></b>		
Read Many, Write Many (CD-RW)	b	d
Read Only (CD-ROM)	d	d

Write Once, Read Many (CD-R)	d	d
a. Degauss (do not degauss hard drives)		
b. Overwrite all addressable locations with a single character. (single pass overwrite)		
c. Overwrite all addressable locations with a character, its complement, then a random character and verify. (multiple pass / DoD secure overwrite)		
d. Destroy - Disintegrate, incinerate, pulverize, shred, or melt		
e. Destruction required only if restricted information is contained.		

#### IV. End of Life Procedures

- (a) A division designee shall make the initial determination that a computer or computer peripheral meets the conditions of being obsolete. Obsolete means the equipment is no longer under warranty or is no longer fit for use because it uses components that are no longer adequate to achieve the equipment's intended purpose or because the cost of the repair or replacement would be greater than the equipment's residual market value.
- (b) The division designee will email the following information for each item of obsolete equipment to the DHS CIO or designee:
  - (1) Brand;
  - (2) Model;
  - (3) Serial number;
  - (4) Inventory tag number (if any);
  - (5) Purchase date and price (if available); and,
  - (6) Service warranty expiration date (if available).
- (c) The CIO or designee will make arrangements to determine if the obsolete equipment is suitable for other purposes within DHS. This determination will be based on an estimate of the equipment's remaining useful life and knowledge of existing needs elsewhere within DHS where the equipment can be used with minimal support cost. If the equipment is redeployed within DHS, the originating division will arrange for the delivery of the equipment to the new site. If the equipment cannot be redeployed, the originating division will arrange for the equipment to be delivered to the DHS Warehouse.
- (d) All transportation of equipment to new locations will be performed in a secure manner using a CIO-approved transport provider. The sender is responsible for creating a manifest and tracking the shipment by item and description. The manifest should be maintained until the equipment arrives at the intended destination. The CIO or designee must be notified in writing of all equipment to be transported.
- (e) In accordance with the procedures listed here, the DHS CIO or designee will deliver media to the DHS IT Security Office for destruction of all data from equipment not being redeployed. The CIO or designee will document compliance by affixing a release tag or documentation to the equipment. The DHS Warehouse must ensure that equipment delivered to Marketing and Redistribution (M&R) has the appropriate OST release

documentation and media such as hard drives has been removed before the transfer of possession can be completed.

- (f) The CIO or designee must make the appropriate modifications to the AASIS inventory record for each device to be transported.
- (g) When equipment arrives at the storage facility, OST will remove all portions of the equipment that had the potential to store sensitive and/or protected DHS information. All hard drives will be wiped and sanitized according to the media destruction procedures in this APM.

#### V. Computer and electronic equipment recycling grants

- (a) Electronic equipment recycling grants must be awarded on the basis of written grant-request proposals submitted to and approved by the Arkansas Department of Environmental Quality (See AR Code Ann. § 25-34-110).
- (b) Grant requests shall be considered based upon the following criteria:
  - (1) The development of sustained processes for recovery, recycling, and remanufacturing of scrap computers and electronics;
  - (2) Minimization and elimination of substantial volumes of this material as waste;
  - (3) Creation of Arkansas jobs;
  - (4) Return of investment analysis; and,
  - (5) Available funds.
- (c) DHS Office of System and Technology may keep a back stock of computer hardware and electronics for the purpose of parts harvesting for the repair, maintenance, and upgrade of computers in use. Back stock shall not exceed 10% of the number of state employee computers in the agency.

#### VI. Other

- (a) The DHS CISO can be contacted for assistance with secure removal of DHS information from information processing equipment, printed materials, and data storage media.
- (b) DHS divisions will ensure compliance with procedures published by the DHS CISO for the secure removal of DHS information from Information Processing Equipment and Data Storage Media.

#### VII. Failure to Comply

- (a) Any violations of these procedures must be reported as a security incident on DHS Share. The DHS IT Security Office or Privacy Office must be alerted to all possible violations of privacy or security in the handling of confidential information.
- (b) Failure to comply with this, or any IT security procedure or policy will result in disciplinary action as outlined in DHS Policies 4002, “DHS Privacy and Security Sanctions” and 1084, “Employee Discipline: Conduct Performance.”

#### VIII. References

- (a) Arkansas Data and System Security Classification  
[http://www.techarch.state.ar.us/domains/security/standards/SS-70-001\\_dataclass\\_standard.pdf](http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf)>
- (b) Act 1526 of 2005, State of Arkansas
- (c) Health Insurance Portability and Privacy Act of 1996, United States of America
- (d) ISACA COBIT Standards <http://www.isaca.org/cobit>