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 unintential 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 Contaction 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 sytems 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. Application and System Registration

(a) For information systems containing Personally Identifiable Information (PII) as defined by the Arkansas Personal Information Protection Act or Protected Health Information (PHI) as defined by HIPAA, the management owner will provide to the security office, within 90 days of initial implementation, any change in the information

listed below, or upon decommissioning of the information system, and also annually during the month of September:

- Name and contact information of the management owner;
- Business purpose;
- Description of the PII and PHI information contained within the information system;
- Description of the protections in place for the information system; and
- System names and network addresses.

VI. 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.

VII. 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."

VIII. 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.

IX. 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 may contain Personally Identifiable Information. FTI data may not be masked to change the character of information to circumvent requirements.

X. References

(a) Arkansas Data and System Security Classification
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) IRS Publication 1075 Tax Information Security Guidelines
https://www.irs.gov/pub/irs-pdf/p1075.pdf

(h) Social Security Administration Safeguards (SSA)
http://www.ssa.gov/dataexchange/security.html