5000 DHS Employee Information Technology Security Requirements

I. Applicability

All DHS employees and authorized users of DHS Information Systems must follow this policy as well as all DHS Information Technology (IT) Security Policies (5000 series) and IT Security Procedures (APMs 120-129) to remain in compliance with state and federal regulations.

II. Security Training

(a) All new users of DHS information systems must complete the IT Security and Privacy training available on DHS Share immediately upon hire or prior to accessing any confidential or protected information.

(b) Current users of DHS Information Systems must retake the IT Security and Privacy training available on DHS Share annually to maintain access to DHS systems. Retraining or additional, more focused training may also be given as deemed necessary by the employee's supervisor or as a sanction for an infraction as outlined in DHS Policy 4002, "Privacy and Security Sanctions."

(c) Failure to complete training in a timely fashion will result in deactivation of the employee's network account. Employees who can't complete job duties without network access may face disciplinary action, even termination. The user's access may be reactivated when IT security training is completed.

III. Information Systems Access

(a) Access to DHS Information Systems is obtained from the Authorized DHS Approving Manager (ADAM) within the employee's division. ADAMs and new users must follow the procedures detailed in APM 125 "Information System Access Procedures."

(b) Authorized employees and users are assigned a unique personal identifier and must utilize a smart card or username and password to gain access to DHS Information Systems. Divisions may impose additional ID or authentication requirements, though they must meet all applicable state and federal guidelines. Such requirements will be managed by the division's own System Administrator.

(c) Employees and users of DHS information systems have no expectation of privacy while utilizing state-furnished computer equipment or electronic devices.

IV. Password Requirements

Employees/authorized users who utilize usernames and passwords must construct strong passwords that can't be easily guessed and are composed of random characters as

instructed by APM 125, "Information Systems Access Procedures." Passwords shouldn't be left where easily found. Sharing of passwords is strictly forbidden.

V. Information Technology Security Audit and Compliance

The DHS IT Security Office will conduct security audits and reviews of identified systems and resources as required by federal and state regulations. All DHS employees must cooperate with IT security auditors. See DHS APM Chapter 121, "Audit Compliance" for procedures and expectations of an IT Security Audit.

VI. Security Standards for External Devices

(a) No external storage media, including privately owned media, may be introduced into any DHS facility without complying with all DHS IT Security standards (see IT Security Office). Commercially recorded, purchased, and stamped CDs and DVDs are allowed in the facility but may not be attached to a DHS device that has access to the DHS Information System.

(b) Any external storage media removed from any DHS facility must be encrypted utilizing DHS approved encryption procedures in DHS APM 126, "Acceptable Encryption." Storage media includes but is not limited to flash drives, CDs, DVDs, any optical storage media, portable music players, zip disks, cartridges, backup storage tapes, portable hard drives, etc.

(c) External storage media may be transported outside of a facility if the data is necessary for the employee's job tasks and is stored on an encrypted device or medium that's approved by the DHS Office of System Technology (OST).

VII. Internet Filtering

(a) Internet access is restricted to minimize risks to DHS's mission critical systems and to ensure productive use of staff time. Internet filtering will be maintained by the IT Security Office as an acceptable enterprise solution. Filtering can be implemented for a single internet site or a general class of sites.

(b) Employees who find websites that may need to be blocked or unblocked from DHS access may email their requests to the IT Security Office using this address: internetfiltering@arkansas.gov. The DHS Chief Information Security Officer (CISO) will work with the DHS Chief Information Officer to make a determination based on OST policies and procedures.

(c) DHS employees with devices that require access to blocked sites for DHS business related purposes may request access for their specific use. Some requests may require approval by the employee's division director and the CISO.

VIII. Failure to Comply

Violations of this policy is subject to disciplinary action as outlined in DHS Policy 4002, "Privacy and Security Sanctions" as well as DHS Policy 1084, "Employee Discipline: Conduct/Performance."