5008.0 **MOBILE COMPUTING AND TELEWORKING POLICY**

5008.1 **Purpose:** To provide a secure framework for the use of Mobile Computing and Teleworking devices with Department of Human Services (DHS) Information Systems or DHS-related data.

5008.2 **Applicability: All** individuals granted access to DHS Information Systems, as defined below, are covered by this policy. These individuals include all employees, volunteers, contractors, temporary workers, those employed by others to perform DHS work, and others authorized to access DHS information, network, and/or systems. This policy applies to the handling of all data on mobile computing devices (see definition of Mobile Computing devices). This policy is applicable to any electronic device that is in existence at the time of its promulgation or that may come into existence any time in the future.

5008.3 **Failure to Comply:** Failure to comply with this policy and associated standards can result in restriction or suspension of all network access to DHS information. DHS employees are subject to disciplinary action, as provided in DHS Policy 1084 and 1085, for violations of this policy.

5008.4 **Policy:**

5008.4.1 Mobile Computing:

A. DHS Information Technology (IT) Security Team will publish configuration and usage standards for each major type of Mobile Computing Device.

B. Device types without published standards are not allowed and new device types shall be submitted to the IT Security Officer for evaluation and risk analysis.

C. Persons utilizing Mobile Computing Devices must comply with DHS Policy 1022 concerning required approval for the acquisition of such devices.

D. Use must be approved for each device by completing the DHS Mobile Device Agreement.

E. A mobile computing device shall be used only by the person, or persons, explicitly authorized by completion of the Mobile Computing Device Agreement.

F. Compliance with standards pertaining to security of Mobile Computing Devices is mandatory.

G. Users of mobile devices on the DHS network agree to complete all required training on mobile devices. Failure to complete training as required will result in deactivation of the device.

H. All Mobile Computing Devices must be asset tagged or tracked by the division responsible for the device.

I. Users must immediately notify the DHS IT Security Officer if the device is suspected to be lost or stolen by utilizing the IT Security Incident Reporting Form located at http://www.arkansas.gov/DHS/security

J. DHS Managers of employees with mobile computing devices will notify OST immediately upon termination of employees.

5008.4.2 Teleworking:

A. Each user's associated division executive must give authorization to telework, whether the equipment is DHS-owned or otherwise, by following DHS Policy 5003.

B. Persons using remote access to telework must be authorized as defined in DHS Policy 5003.

C. The device used for Teleworking must be afforded all reasonable protection while located in the teleworking environment. It shall not be left unattended where it can be seen and is susceptible to theft.

D. When teleworking with DHS-owned devices, no one other than the authorized user shall operate the device.

5008.5 **Definitions:**

5008.5.1 Mobile Computing Device: Any device, whether or not owned by DHS, located outside of a DHS facility which may contain information for which DHS is responsible.

5008.5.2 DHS Information Systems: DHS Network services (Network, access, E-mail, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

5008.5.3 Person: For the purposes of this policy, a person is defined as a uniquely identifiable and distinguishable human being, whose identity has been validated and whose association with DHS has been certified by the division requesting access credentials. A person may or may not be a DHS employee.

5008.5.4 DHS Facility: A location on the approved site list maintained by the Chief Information Officer of DHS. This location must be under direct DHS control and supervision and under compliance with the state and department physical and logical security standards.

5008.5.5 Teleworking: Working on DHS information or the DHS network from a location that is not a DHS Facility. This includes the use of mobile computing devices or the use of remote access.

5008.6 **Auditing and Reporting of Security Incidents:**

5008.6.1 Any device, regardless of ownership, used to process information belonging to DHS or to access DHS Information Systems, is liable to audit and remote monitoring.

5008.6.2 Any suspected security incident involving the theft, loss, or unauthorized disclosure or use of DHS information or a Mobile Computing Device must be reported within one business day to the DHS IT Security Officer.

5008.7 **Exceptions to Policy:**

Exceptions to this policy and related standards must be requested in writing to the DHS IT Security Officer. Exceptions are granted in writing on a per instance basis and approved by the CIO. Individual exceptions do not extend beyond the party to which they are issued.

5008.8 **References:**

5008.8.1 Act 1526 of 2005, State of Arkansas

5008.8.2 Act 339 of 2007, State of Arkansas

5008.8.3 Arkansas Data and System Security Classification
< http://www.techarch.state.ar.us/domains/security/standards/SS-70-001_dataclass_standard.pdf>

5008.8.4 Arkansas Encryption Standard
< http://www.techarch.state.ar.us/drafts/DRAFT_encryp_standardSS-70-006.pdf>

5008.8.5 Health Insurance Portability and Privacy Act of 1996, United States of America

5008.9 **Originating Section/Department Contact:**

5008.9.1 Office of Systems and Technology
1st Floor Donaghey Plaza North
PO Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032

5008A.0 EXTERNAL STORAGE MEDIA STANDARD

5008A.1 **Purpose:** This standard provides for the protection of Department of Human Services (DHS) data placed on external storage media. This standard also provides protection for DHS Information Systems with which external storage media may interact.

5008A.2 **Standards:**

5008A.2.1 Any external storage media outside of or removed from any DHS facility must be encrypted utilizing a DHS approved encryption method. This includes but is not limited to CDs, DVDs, any optical storage media, flash drives, portable music players, zip disks, jaz cartridges, backup storage tapes, and portable hard drives.

5008A.2.2 No external storage media, including privately owned media, may be introduced into any DHS facility without complying with this standard. Commercially recorded, purchased, and stamped CDs and DVDs are allowed in the facility but may not be attached to a DHS Information System.

5008A.2.3 Media may be transported outside of a facility if the data contained on the media is level A data, as defined by State of Arkansas, Office of Information Technology, Data and System Security Standard. This determination must be made by the asset owner of that data and recorded in a central log for each division. The classification must be clearly marked on the storage media.

5008A.2.4 Storage media that is no longer in use must be securely transported to a DHS CIO-designated location for secure destruction.

5008A.3 **Definitions:**

5008A.3.1 External Storage Media: Devices designed with the purpose of storing data in digital form which can be readily removed from a computing device to which it is attached. (Examples include: CD, DVD, CD-R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW, DVD-RAM, BluRay, floppy diskettes, flash drives, CF media, SD media, MMC media, XD media, magnetic tape, Iomega Zip media, Iomega Jaz media, external media players that allow for file storage, and external hard drives)

5008A.3.2 DHS Information Systems: DHS Network services (Network, access, E-mail, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also, any computer file, on any device in use by DHS or its agents that is shared across the DHS network or requires DHS support or contains DHS-related information, the privacy of which must be safeguarded.

5008A.3.3 DHS Facility: A location on the approved site list maintained by the Chief Information Officer of DHS. This location must be under direct DHS control and supervision and under compliance with all state and department security standards.

5008A.4 **Originating Section/Department Contact:**

Office of Systems and Technology
1st Floor Donaghey Plaza North
PO Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032

5008B.0 BLACKBERRY SECURITY STANDARD

5008B.1 **Purpose:** To provide a standard security configuration for BlackBerry devices in the Department of Human Services (DHS) enterprise.

5008B.2 **Standards:**

5008B.2.1 BlackBerry devices will require by technical control a minimum of a 4 character password. An 8 character password is recommended. This standard allows an exception to policy 5002, due to the difficulty some users may experience when attempting to enter complex passwords on the small device keyboard. Users who do not wish to enter a password before using the telephone portion of their device should consider carrying a separate telephone.

5008B.2.2 BlackBerry devices will require by technical control a 10-minute maximum time until lockout to force locking of unattended devices.

5008B.2.3 BlackBerry devices will require by technical control a 60-day expiration on device passwords.

5008B.2.4 BlackBerry devices will allow no more than 10 password attempts in any given sequence before initiating a wipe of all data stored on the device.

5008B.2.5 A firewall will be enabled on each BlackBerry device where technically available.

5008B.2.6 BlackBerry devices shall not be left unattended in public or visibly accessible in an unattended vehicle.

5008B.2.7 No health information or any information that DHS considers confidential shall be transmitted using SMS messaging, PIN messaging, third-party network instant messaging, or the service provider browser.

5008B.2.8 BlackBerry devices will require the use of the AES encryption standard to transmit information wirelessly to and from the DHS network.

5008B.2.9 DHS Managers of employees with BlackBerry devices will notify OST immediately upon termination of employees. The Office of Systems and Technology will initiate a remote wipe of the BlackBerry device followed by deactivation of the device account from the BlackBerry Enterprise Server.

5008B.2.10 All BlackBerry devices must be connected to the CIO-approved Blackberry Enterprise Server. Desktop-only connections are prohibited.

5008B.3 **Definitions:**

5008B.3.1 BlackBerry: Any device produced for information storage and transmission by the Research In Motion Corporation.

5008B.3.2 DHS Information Systems: DHS Network services (Network, access, E-mail, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it

was intended. Also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

5008B.3.3 SMS: Short message service is a technology that allows sending of short messages, also known as text messages, between mobile phones, to other handheld devices, and even to landline telephones.

5008B.3.4 PIN Messaging: A unique form of messaging implemented for sending short text messages among BlackBerry devices by use of the device PIN number.

5008B.4 **Originating Section/Department Contact:**

Office of Systems and Technology
1st Floor Donaghey Plaza North
PO Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032

5008C.0 **LAPTOP, NOTEBOOK, AND TABLET SECURITY STANDARD**

5008C.1 **Purpose:** To provide standards for use of laptop, notebook, and tablet computers in the DHS enterprise.

5008C.2 **Standards:**

5008C.2.1 The device must be connected to the DHS Network at least once monthly for a minimum of 24-hours to allow for updating of system software.

5008C.2.2 The device must be joined to a DHS enterprise domain.

5008C.2.3 The device must be fully encrypted using DHS enterprise approved encryption software.

5008C.2.4 The device must be kept in a secure location at all times to ensure access by authorized users only.

5008C.3 **Definitions:**

DHS Information Systems: DHS Network services (Network, access, E-mail, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

5008C.4 **Originating Section/Department Contact:**

Office of Systems and Technology
1st Floor Donaghey Plaza North
PO Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032

5008D.0 **HANDHELD COMPUTER AND SMARTPHONE SECURITY STANDARD**

5008D.1 **Purpose:** To provide standards for use of handheld computers and SmartPhones in the DHS enterprise.

5008D.2 **Standards:**

5008D.2.1 The device must be fully encrypted using enterprise approved encryption software.

5008D.2.2 The device must be kept in a secure location at all times to ensure access by authorized users only.

5008D.2.3 The device must be configured to automatically lock after 5 minutes of inactivity.

5008D.2.4 The device must be configured to require four or greater digit PIN number to unlock the device.

5008D.2.5 Handheld Computers and SmartPhones which are allowed by this standard are identified by make and model on a list maintained by the Office of Systems and Technology and provided with this standard.

5008D.3 **Definitions:**

DHS Information Systems: DHS Network services (Network, access, E-mail, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also, includes any computer file, on any device in use by DHS or its agents that is shared across the DHS network or requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

5008D.4 **Originating Section/Department Contact:**

Office of Systems and Technology
1st Floor Donaghey Plaza North
PO Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032