1002 Secure Employee Workstation Policy

I. Applicability

These rules apply to all DHS employees, contractors, workforce members, and anyone with access to confidential DHS client information or DHS information systems.

II. Policy

(a) All DHS employees and contractors are required to protect confidential information, whether it's on paper or in electronic form (emails or in a DHS system, like the MMIS or CHRIS). Examples of confidential information include, but aren't limited to: identifiable information regarding foster children, or any agency client, as well as protected health information of Medicaid recipients or facility residents.

(b) Employees must restrict the visibility of DHS client information or protected data files (confidential information) while working with such items at their desks by taking the following measures:

(1) Ensure that workstations are positioned away from public viewing.

(2) Ensure that unauthorized visitors are not left unattended.

(3) Ensure that all confidential information is erased from whiteboards/chalkboards, and cover flip charts.

(4) Ensure that file cabinets or briefcases containing confidential information are kept locked when not in use.

(5) Ensure that keys, access cards, and smart cards used to access confidential information are not left unattended.

(6) Do not store passwords near computers.

(c) Lock confidential documents in a cabinet when leaving your workstation, if even for a brief period.

(d) Lock computer terminals when leaving your workstation, if even for a brief period. Secure your computer by typing "Ctrl, Alt, Delete" and select "Lock This Computer."

(e) Authorized DHS wireless device users should keep the devices locked away when not in use and utilize the passcode locks on them. (Also follow DHS Policy 1074.)

(f) Use only DHS approved computing devices assigned to you by your supervisor. The removal of computing devices with confidential information from the premises must have prior approval by management and must be encrypted using procedures found in the "Acceptable Encryption Procedures" (APM 126). The assignment of a device

to an individual constitutes prior approval by management (DHS Policy 5003, "Wireless Networking").

(g) Do not use personal wireless devices for transmitting (via email or text message) confidential information. For example: do not take a picture of a foster child with a personal cell phone. Do not email confidential information to your personal email address. Employees who fail to comply with this rule are subject to discipline based on DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

(h) Do not use personal flash drives/USB drives, CDs, or DVDs on DHS equipment. Use only approved storage devices obtained through the DHS Office of Information Technology (OIT). If such approved storage devices contain protected health information (PHI) or personal information (PI) under the Arkansas Personal Information Protection Act (PIPA), such devices may not be removed from the DHS premises without being encrypted.

(i) Immediately remove documents containing confidential information from printers, copiers, and fax machines.

(j) Use only the locked shred bins for confidential documents when they are no longer needed. Do not use the recycling bins to dispose of documents that contain confidential information, Federal Tax Information (FTI), or Social Security Administration (SSA) data. All documents containing confidential information must be destroyed in compliance with the "IT Data Destruction and End of Life Procedures" (APM 129).

(k) Ensure that computer terminals do not display any Federal Tax Information (FTI) during visits by unauthorized personnel.

(l) Data provided by the SSA is restricted to authorized employees who need such access to perform their official duties. All SSA data must be destroyed in compliance with the "IT Data Destruction and End of Life Procedures" (APM 129).

III. Identification Badges and Proximity Cards

(a) DHS employees must present a valid ID badge to obtain access to DHS facilities and must wear their badge at all times while in a DHS facility. Failure or refusal to present a badge must be reported as a security incident using the Incident Reporting System on DHS Share.

(b) All new employees must obtain a badge as soon as possible but no later than two (2) weeks of the date of hire. It is the supervisor's responsibility to ensure a new employee gets an ID badge.

(c) Employees shall not change their profile photograph on DHS Share, Skype, or Microsoft Outlook without the consent of the DHS IT Security Office. The photographs used for DHS badges also serve as the DHS internet profile photograph

taken at DHS Security. The photograph on the badge is the individual's official DHS photo and should match the profile photograph at all times.

(d) ID badges and proximity cards are the property of DHS. Employees are responsible for protecting badges against unauthorized use and must return them in good condition.

(e) Lost or stolen badges or proximity cards must be reported on the Incident Reporting System (on DHS Share) as soon as possible after the loss or theft is discovered.

IV. Visitors to DHS Facilities

(a) All visitors to DHS facilities must be accompanied by an employee at all times in areas where confidential data are present or where DHS information systems are present.

(b) Visitors must comply with ID badge requirements pertaining to the specific DHS location being visited.

(c) Visitor's badges are issued only for a specific event, meeting, or day.

(d) Division Directors or their designees may specify areas where business visitors may work unaccompanied.

V. Failure to Comply

Failure to comply with this policy can result in restriction or suspension of all network access to DHS Information Systems, deactivation of network attached devices, civil and criminal penalties, and contractual penalties. In addition, DHS employees are subject to disciplinary action outlined in DHS Policy 4002, "Privacy and Security Sanctions" and DHS Policy 1084, "Employee Discipline: Conduct/Performance."

VI. Definitions

(a) Confidential Information means information that is protected from disclosure by federal law (such as the Health Insurance Portability and Accountability Act [HIPAA], Health Information Technology for Economic and Clinical Health [HITECH], Social Security Administration [SSA]) or state law or regulation. Under DHS policy, examples of confidential information include: information that identifies a foster child, foster or adoptive parents, or Medicaid recipents, as well as Protected Health Information, Federal Tax Information, and Social Security Administration data.

(b) Computing devices include, but are not limited to, laptops, notebooks, iPads, smart phones, tablets, and computers.