1001 SECURE EMPLOYEE COMMUNICATIONS

I. Applicability

This policy, which applies to all Department of Human Services (DHS) employees and workforce members, regulates the correct use of communication to securely deliver confidential information handled by DHS employees for the purpose of conducting Department business. This policy ensures that DHS staff uses electronic communications (email, faxes, etc.) in a manner that conforms to all applicable state and federal rules and regulations.

II. Report Incidents

Failing to comply with this policy, even if unintentional, must be reported as a privacy or security incident to the DHS Privacy Office or Office of Information Technology (OIT). The report can be made on DHS Share by clicking on the "DHS Real Time Incident Reporting" logo.

III. Policy

(A) Each employee is responsible for ensuring the privacy and security of confidential information as defined by state or federal law, regulation, or policy (See 4002 "Confidential Information" definition). Employees are accountable for every email they send or to which they reply.

(B) Employees who are authorized to remove files from the office in the course of their job duties shall be held accountable for the protection of those files (refer to DHS Policy 4002, "Privacy and Security Sanctions"). Divisions shall develop their own systems to keep track of files that leave the office, who removes them, as well as the date and time of removal and return of the files.

(C) All employees who need access to any DHS information systems (even just to use email) must complete DHS Privacy and Security training promptly upon hire, prior to accessing any confidential information, and annually.

(D) DHS reserves the right to monitor all aspects of email, internet, and DHS network usage with or without notice. Employees have no reasonable expectation of privacy in the use of email, internet, or any DHS network.

(E) Only use DHS purchased and OIT approved equipment or Chief Information Security Officer (CISO) authorized equipment, including wireless devices, for transmitting confidential information. Do not use personal computers, personal wireless devices, or personal accounts for emailing, text messaging, storing, or transmitting confidential information unless the access is through the DHS Portal or Outlook Web Access (OWA). Employees who fail to comply with this rule will face disciplinary

action based on DHS Policy 4002, "Privacy and Security Sanctions." Note: A list of DHS-approved devices can be found on the DHS Share site.

(F) The transfer of Federal Tax Information (FTI), such as federal tax returns or return information received directly from the IRS or a secondary source, such as Social Security Administration, Federal Office of Child Support Enforcement, or Bureau of Fiscal Service is restricted only to systems utilizing IRS-approved encryption methods.

IV. Email

(A) Emails containing confidential information that will be sent to an email address other than @dhs.arkansas.gov must be encrypted before being sent. Employees encrypt confidential emails by typing the word **"SENSITIVE"** in the subject line or body of the e-mail. Failure to do this must be reported as a privacy/security incident. To assist in this, employees will copy and paste the following "Confidentiality Notice" statement to appear in their automatic "Signature" so that it appears on all emails they create:

This email may contain sensitive or confidential information.

Confidentiality Notice: The information contained in this email message and any attachment(s) is the property of the State of Arkansas and may be protected by state and federal laws governing disclosure of private information. It is intended solely for the use of the entity to which this email is addressed. If you are not the intended recipient, you are hereby notified that reading, copying, or distributing this transmission is STRICTLY PROHIBITED. The sender has not waived any applicable privilege by sending the accompanying transmission. If you have received this transmission in error, please notify the sender by return and delete the message and attachment(s) from your system.

(B) Confidential information must never be placed in the subject line of an email.

(C) Employees or workforce members must never email confidential information to their personal email addresses. All DHS or work-related business that includes confidential information must be conducted on secure DHS, business, or vendor email addresses.

(D) Emails containing confidential information shall only be sent to persons who need to know the information. Group, global, or broadcast email addresses shall not be used to share confidential information unless all recipients need to know the information.

(E) Emails containing confidential information shall contain only the minimum necessary information to accomplish the purpose of the communication.

(F) Theft, unauthorized disclosure or destruction, tampering with other employee's email accounts, or any evidence indicating the misuse of the DHS email system may result in discontinuing access to all DHS networks and information systems which will

result in sanctions against the employee, or termination. (See the Appendix attached to this policy for examples of inappropriate uses of email and the internet.)

(G) The DHS email system and all associated email records are the property of the State of Arkansas and are subject to public release unless Federal or State law exempts their release. If email records are requested through a subpoena or Freedom of Information Act (FOIA) request, release is governed by DHS Policy 1053, "FOIAs, Subpoenas, Requests for Disclosure, Legal Opinions." Email records are subject to all state and federal laws and will be retained accordingly.

V. Faxes

(A) All fax messages from DHS employees that contain confidential information must be sent only to a specific, authorized person. It should be established that a specific person is present to receive the transmitted fax.

(B) Fax messages from DHS employees must use a cover sheet with the word **"CONFIDENTIAL"** appearing in bold letters near the top of the form and include this statement:

"Prohibition of Disclosure: This information has been disclosed to you from records that are confidential. You are prohibited from using the information for other than the stated purpose; from disclosing it to any other party without the specific written consent of the person to whom it pertains; and are required to destroy the information after the stated need has been fulfilled, or as otherwise permitted by law. A general authorization for the release of medical or other information is not sufficient for this purpose."

VI. Remote Work

(A) Definitions:

(1) Remote Work: any work as approved by the Department that is done outside of an official Department office.

(2) Virtual Private Network (VPN): used by those accessing the DHS network while doing Remote Work while using a DHS owned laptop accessing the network through DHS standard VPN solution.

(3) Remote Desktop Access (RDA or RDT): accessing the DHS system through the DHS Portal. This allows the user to access their desktop at the office through their own personal computer without the transfer of protected information to their own device.

(4) Outlook Web Access (OWA): a website or phone application that allows you to access your DHS email account through a personal device.

(B) DHS, when necessary, can approve either temporary or permanent permission to work from home or other secure remote locations. That work is subject to the following rules:

(1) For Remote Desktop Access, you will only utilize a router over which you have control. It will be using WPA2-AES security, with a router password that meets DHS password requirements. (This does not apply to VPN usage).

(2) Any personal device used to access the DHS Portal or Outlook Web Access will have a strong password that meets DHS password requirements.

(3) You must not allow your computer to save any passwords related to your accessing the DHS Portal.

(4) You must not allow anyone access to your computer while it is logged into the DHS Portal. You must also sign out of the Portal when you are done working.

(5) You must be aware of others who approach while you are working on DHS materials and cover your screen and any work documents until they leave the immediate area.

(6) All confidential information must be stored securely and must be treated in compliance with DHS privacy and confidentiality obligations. Note: Poor security practices at home might lead to inappropriate access by unauthorized individuals.

(7) Reporting obligations under this policy and Policy 1003, "Privacy and Security Incident Reporting" are the same for remote work employees.

(8) No files containing Protected Health Information (PHI) or Personal Information Protection Act (PIPA) identifiers or confidential or sensitive DHS information should be saved to your personal, non-DHS devices from any remote platform.

(9) Personal printers and scanners and thumb/flash drives should NOT be used while connected to a DHS computer or network to print any document containing PHI or PIPA elements or other confidential or sensitive DHS information.

VII. Other

(A) DHS Divisions that are Covered Entities (as defined in DHS Policy 4001, "Notice of Privacy Practices") may use the following secure options for Department-approved data shares once any appropriate agreement is in place:

(1) Within authentication protected sites, files, or folders;

(2) On an encrypted, passkey protected, portable hard drive approved for use by the DHS CISO; or,

(3) By a secure internet method approved by the DHS CISO.

(B) Only employees authorized by their Division and the individuals or groups listed on the agreement may have access to the password or to the passkey and the data being shared. Divisions should contact the DHS Privacy Officer for guidance on data sharing.

VIII. Failure to Comply

Violations of this policy may result in disciplinary action or termination as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline."

DHS Policy 1001 Appendix: Inappropriate Uses of Email and Internet

I. The following list is not all-inclusive, but contains examples of activities that violate the Department's intended use of the email system and the internet. All violations must be reported as a privacy or security incident to the DHS Privacy Office or IT Security Office. The report can be made on DHS Share by clicking on the "DHS Real Time Incident Reporting" logo. Failing to report a suspected privacy or security incident is also a violation of policy and subject to disciplinary action.

(A) Without proper authorization, seeking information from another user's PC, copying or modifying another user's files or data, or using passwords belonging to another user.

(B) Emailing DHS computer, system, or program passwords outside the DHS network.

(C) Failing to lock or log off or leave unattended any controlled-access computer or other form of electronic data system to which you are assigned.

(D) Sending or receiving confidential or sensitive information in violation of DHS policy or a state or federal regulation.

(E) Posting any kind of confidential information (for example, information about clients or patients) on social media.

(F) Using DHS internet, systems, or equipment to access, create, view, transmit, or receive offensive or harassing statements or language maliciously disparaging others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs. An exception would apply when such language or statements are included as objective citations in conducting official DHS business.

(G) Using email or the internet to intimidate or harass coworkers or disrupt the workplace.

(H) Operating or promoting a business, soliciting money for personal gain, or soliciting or selling products or services while on duty.

(I) Using DHS systems or equipment while promoting any political campaign.

(J) Engaging in any activity in violation of local, state or federal laws or regulations.

(K) Intentionally disrupting network or system use by others, either by introducing worms, viruses, virus hoaxes or by other means.

(L) Misrepresenting one's position or authority through email or internet use.

(M) Transmitting or, with foreknowledge, receiving offensive or sexually oriented material unless it is part of an open case or an ongoing investigation.

(N) Emailing chain letters or participating in any way the creation or transmission of unsolicited commercial email (or "spam") that is unrelated to legitimate DHS purposes.

(O) Engaging in personal activities such as dating websites or instant messaging utilities and chat rooms that are not work related.

(P) Making unauthorized electronic or paper copies of confidential DHS files or other confidential DHS data, or information not subject to disclosure under FOIA.

(Q) Purposefully or knowingly causing congestion, disruption, disablement, alteration, or impairment of DHS networks or systems.

(R) Knowingly defeating or attempting to defeat security restrictions on DHS systems and applications.

(S) Maintaining or organizing non-work related web logs such as blogs, web journals, or chat rooms.

(T) Playing games on DHS' internet or systems.