1001 SECURE EMPLOYEE COMMUNICATIONS

I. Applicability

This policy, which applies to all DHS employees and workforce members, serves to regulate the correct use of communication to securely deliver confidential information handled by DHS employees for the purpose of conducting agency 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 IT Security Office. The report can be made on DHS Share by clicking on the "DHS Real Time Incident Reporting" logo. The DHS Privacy Office or IT Security Office can be contacted for more guidance.

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, such as Protected Health Information of Medicaid patients or the personal information of DHS employees, clients, or foster children.

(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 (for example, a sign-out sheet) 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 all 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) Employees may face disciplinary action for inappropriate or excessive use of DHS email or DHS internet. Excessive use means usage that interferes with job duties, responsiveness to job functions, or completing assigned tasks. If a supervisor suspects an employee of excessive or inappropriate use of email or internet because it is interfering with job duties or disrupting the work environment, then the supervisor may request an IT audit of the employee's internet use at work (go to DHS Share and click on "DHS Internal Affairs Reporting"). The audit may result in disciplinary action against the employee, including termination.

(f) Only use DHS issued 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. Employees who fail to comply with this rule will face disciplinary action based on DHS Policy 4002, "Privacy and Security Sanctions." Repeated violations will result in termination.

(g) 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 SSA, Federal Office of Child Support Enforcement, or Bureau of Fiscal Service, through email, fax, or a multi-function device is prohibited.

IV. Email

(a) Emails containing confidential information (personal identifying information or protected health 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 or body of the e-mail. Failure to do this must be reported as a privacy/security incident.

(b) Confidential information (like a client or foster child's name) 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 must be conducted on DHS email (for contractors, DHS business must be conducted on their secure work email addresses).

(d) Emails containing confidential information (for example, identifiable details of a Medicaid patient, or a foster child, or any agency client) 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) Employees should copy and paste the following "Confidentiality Notice" statement to appear in their automatic "Signature" so that it appears on all emails they create:

"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 distribution 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."

Employees should ask their supervisors for assistance in how to create the email signature or contact the Organizational Development and Training Unit within the DHS Office of Finance and Administration and enroll in a Microsoft training course.

(g) Employees are responsible, and therefore held accountable, for each and every email they send including emails that employees forward or reply.

(h) 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, in turn, 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.)

(i) The DHS email system and all associated email records, DHS email addresses, and DHS email accounts and mailboxes are the property of the state of Arkansas and are subject to public release. Before releasing information in such cases, parties should seek guidance from the Office of Chief Counsel (OCC) or the DHS Privacy Office.

(j) Email Records are subject to the provisions of Arkansas records and retention statutes and subject to retention requirements specified in regulations governing conduct of programs administered by DHS.

V. Faxes

(a) All fax messages from DHS employees that contain confidential information must be sent only to a specific person for whom such information has been determined to be authorized. It should be established, by prior telephone contact, 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. Other

(a) DHS Divisions that are Covered Entities may utilize the following secure options for agency approved data shares once any appropriate agreement is in place:

(1) Within a password protected folder on DHS SharePoint;

(2) On an encrypted, passkey protected, portable hard drive approved for use by the DHS Chief Information Security Officer (CISO); or,
(3) By a secure internet method approved by the DHS CISO.

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.

(b) DHS employees utilizing VoIP devices must adhere to DHS APM 127, "Voice-over Internet Protocol Procedures."

VII. Failure to Comply

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

VIII. Assistance

DHS employees or supervisors may submit any questions regarding this policy to the OCC Policy Section via email at DHS.OCC.Policy@dhs.arkansas.gov or by contacting the OCC DHS Policy Manager.

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 agency'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 on-going 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.