E-Mail Systems

Purpose: The purpose of the following policy is to ensure that:

a. CDS personnel is informed about the applicability of policies and laws with regard to e-mail and that e-mail services are used in compliance with these policies and laws;
b. Users of e-mail are informed about confidentiality, privacy, and security applicable to e-mail; and
c. Disruptions to CDS e-mail and other services and activities are minimized.

Policy: As a productivity enhancement tool, CDS encourages the business use of e-mail. Concerted efforts will be made to protect the security and confidentiality of information contained in these messages as well as the security of CDS's IT resources.

Procedure and/or Process:

Data Systems Manager Responsibilities:

- Establish CDS e-mail services
- Create, update, and maintain policies to ensure compliance with relevant laws and regulations

Information Technology Specialist Responsibilities:

- Create, update, terminate, and maintain user accounts
- Set up each user's mailbox with adequate security to ensure confidentiality
- Provide training to individual e-mail users in the use of the CDS e-mail system
- Provide on-going technical support to e-mail users
- Troubleshoot e-mail system problems
- Access individual's e-mail messages upon request of the employee or the Security Officer

E-Mail System Standards:

- CDS e-mail system employs unique e-mail addresses and associated passwords to isolate the communications of different users. A user must not employ the e-mail addressof any other user.
- It may be necessary for Data Systems personnel to review the content of an individual worker's communications during the course of problem resolution. Data Systems personnel may not, however, review the content of an individual worker's communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Advance approval by the CDS Security Officer is required for all such monitoring.
- CDS e-mail system is intended for CDS business activities. E-mail may be used for personal use as long as it is used reasonably. However, this does not entitle staff to any expectation of privacy.

Ownership

- E-mail messages are CDS property.
- CDS does not guarantee that electronic communications will be private. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and read by others. Since messages can be retrieved in backups, electronic communications may actually be retrievable when a traditional paper letter would have been discarded or destroyed.
- Employees must be aware that upon employment termination, their access to the CDS e-mail system will be discontinued and their e-mail accounts may be accessed by other CDS staff in order to continue to conduct agency business after their departure. All personal e-mail correspondence must be deleted prior to leaving CDS. Program Coordinators must request access to the account for a specific period of time. The Information

Systems Specialist will reset the e-mail account password and supply a new password. After the requested time period has elapsed the account will be disabled and eventually deleted.

Confidentiality:

- At no time shall confidential data be transmitted unencrypted via wireless devices or across unsecured public lines.
- Any e-mail containing confidential data sent via wired or wireless means must utilize at least 128-bit encryption and meet CDS software standards. Highly sensitive information should be placed into an MS Word document, password protected, then included as an attachment to the e-mail. The password used to lock the document should be given to the e-mail recipient over the telephone or in a separatee-mail. (Refer to P-1008 – Electronic Transmission of Protected Health Information.)
- Confidentiality Notice on E-mail. The following text must be automatically included on all e-mail messages sent from computers:

  IMPORTANT MESSAGE FOLLOWS: This message and its attachments are intended only for the individual to whom it is addressed. They are confidential and may contain legally privileged information. If you are neither the intended recipient nor the agent responsible for delivering the message to the intended recipient you are hereby notified that any dissemination of this communication is strictly prohibited and may be unlawful. If you feel you have received this communication in error please notify us immediately by return e-mail to the sender (and/or by telephone at 352.244.0628 ext.3753) and delete it from your system. We thank you in advance for your cooperation.

  CDS Family & Behavioral Health Services, Inc.
- Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, users should exercise caution when forwarding e-mail messages. Messages received from outside parties should not be forwarded to others unless the sender clearly intended this and unless forwarding is necessary to accomplish a business objective.

Security:

- Regardless of the circumstances, individual passwords must never be shared or revealed to anyone outside the Data Systems Department. Revealing a password to another party exposes the authorized user to responsibility for actions of another person. If users need to share computer resident data, they should utilize message forwarding.
- Unless tools like digital signatures and digital certificates are employed, it is relatively easy to spoof the identity of another user on the Internet. Before CDS staff release any internal agency information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed
- Unless permission from the CDS Security Officer has first been obtained, users must not use their personal e-mail accounts with an Internet Service Provider (ISP) or any other third party for any CDS business. To do so would circumvent logging and backup controls that CDS has established.
- Attachments will automatically be scanned by Microsoft Office 365 before e-mail delivery and scanned by Microsoft Security Essentials upon download. Unexpected attachments received from third parties should be viewed with suspicion. Even if the third party is known and trusted, a virus can still infect the attachment without their knowledge.
- Users must promptly report all information security alerts, warnings, and any other reported vulnerability to the Security Officer. Many of these notices are hoaxes and cause users to be unnecessarily distracted from their work. The Security Officer is the only organizational person authorized to determine appropriate action in response to such notices. Users are prohibited from utilizing CDS systems to forward these notices to other internal or external users.

E-mail Back-up and Retention:

- When an e-mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a CDS management decision, the message should be retained for future reference.
- Users should set up a regular maintenance schedule to clean out e-mail files and folders. Delete what is no longer needed, review what is left to be sure it is work related and could be needed again in the future.

Prohibitions:

- News feeds, e-mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet should be restricted to material which is clearly related to both CDS business and the duties of the receiving users and does not affect others such as downloading large files.
- Users are prohibited from using CDS computer systems for the transmission of unsolicited bulk e-mail advertisements or commercial messages that are likely to trigger complaints from the recipients. Colloquially known as spam, these prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches.
- When unwanted and unsolicited e-mail is received, CDS staff must refrain from responding directly to the sender, as this would indicate that the account is monitored regularly and would invite further junk e-mail. Instead, staff should delete the e-mail if it originated from outside of the agency. Spam may be forwarded to the Information Technology Specialist, , who can then take steps to prevent further transmissions.
- Users must not use profanity, obscenities, or derogatory remarks in e-mail messages. Such remarks, even when made in jest, may create legal problems such as trade libel or defamation of character. It is possible that such remarks would later be taken out of context and used against CDS. As a matter of standard business practice, all CDS electronic communications must be consistent with conventional standards of ethical and polite conduct.
- Misrepresenting, obscuring, suppressing, or replacing another user's identity on an e-mail system is forbidden. The user name, e-mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings. Users must not send anonymous e-mail communications.
- No media advertisement, Internet home page, electronic bulletin board posting, e-mail message, or any other public representation about CDS may be issued unless CDS management has granted approval. CDS, as a matter of policy, does not send unsolicited e-mail (also known as spam). Users are also prohibited from "mail bombing" other users in retaliation for any perceived wrong or for any other reason ("mail bombing" is described as sending a large number of messages intended to overload a server or user's electronic mailbox).
- Transmission of e-mails with sexual, ethnic, racial, and/or religious harassment content is strictly prohibited.
- Users who receive offensive unsolicited material from outside sources must not forward or redistribute that material unless it is being forwarded to their supervisor or CDS Data Systems staff in order to assist with the investigation and resolution of a complaint.
- Users should not respond directly to the originator of offensive e-mail messages. If the originator does not promptly stop sending offensive messages, users must report the communications to their supervisor, and the COO if the message is from a CDS employee. CDS retains the right to remove from its information systems any material it views as offensive or potentially illegal.