



## Electronic Communication and Internet Use

<b>Policy Type:</b>	Information Management	<b>Policy Number:</b>	813
<b>Original Issue:</b>	07/01/2012	<b>Effective Date:</b>	08/30/2023
<b>Document Owner's Approval:</b>	 <hr/> Howard Thibodaux, Information Technology Director		
<b>Executive Director's Approval:</b>	 <hr/> Kristin Bonner, MHA, BSN, RN, Executive Director		

**Policy Statement:**

South Central Louisiana Human Services Authority (SCLHSA) employees, interns, and contractors authorized to use SCLHSA computers and other electronic communication systems shall adhere to standards as regulated by SCLHSA, CARF, and the State of Louisiana Office of Telecommunication Services (OTS).

**Rationale:**

To establish guidelines and restrictions regarding use of email and Internet access provided by and maintained by SCLHSA.

**Procedure:**

A. Definition:

**Electronic Mail (email)** - A system for sending and receiving messages electronically over a computer network for internal and external communications.

B. **Electronic Mail (email):**

SCLHSA employees are allowed the use of the email system for carrying out the responsibilities of the agency and for efficient sharing of information necessary to conduct Authority business. The following provisions shall regulate use of the SCLHSA email system:

1. The MS Exchange email accounts are provided by OTS. All messages composed, sent, or received on the email system are and remain the property of OTS and SCLHSA. SCLHSA reserves the right to review, audit, access, and/or disclose any message sent over the email system when necessary to prevent system misuse or to comply with judicial orders.
2. The primary purpose of email is to assist employees in fulfilling their duties and responsibilities. Any other use is prohibited. Employees are expected to use the email system responsibly, thoughtfully, and in a professional manner at all times. Need for access is determined by the appropriate Site Manager, Division Director, IT Director or the Executive Director.
3. Supervisors are responsible for determining whether email use by employees under their supervision is interfering with the employee's productivity. Upon request and approval of the Executive Director, reports on the amount of an employee's email use will be provided to that employee's supervisor(s) and/or the IT Director for review.

4. Attachments to email should not exceed three (3) megabytes. Three megabytes of data is roughly equivalent to 2700 pages of text. Larger files should be transferred by other methods.
5. Email users must respect the rights of all other users of the system and not knowingly use this resource in any way that is disruptive or damaging to the system, or offensive to any other user.
6. Email should not be broadcast (i.e., sent to all users in the State E-Mail System's address books) without express permission of the Executive Director. Users should refrain from using "Reply All" when responding to one or more persons.
7. The email system is not to be used to solicit for personal gain, for commercial ventures or for religious or political causes.
8. Email users may only use the email system for subscribing to mail lists that are related to official business or professional enhancement in support of the SCLHSA mission.
9. The email system is not to be used to create any offensive or disruptive messages. Examples of misuse of email facilities include, but are not limited to, distribution of chain letters, photographs, music files, use of obscene language, harassment, and violations of existing SCLHSA, state, or federal policies or regulations.
10. Any employee who violates this policy or uses the e-mail system for improper purposes shall be subject to disciplinary action up to and including termination.
11. Because e-mail is not stored indefinitely by SCLHSA, employees are responsible for maintaining records of critical business documents either by archiving the messages or printing the messages and then securely storing the paper files.

#### C. **Secure Email (Encryption):**

The below information is provided to help all staff understand and utilize the Secure Email Feature that OTS has implemented. IT has added this feature for all of our email accounts as a way to send highly confidential and private information via our la.gov email accounts. Using the secure email feature is easy, but it must be used properly to be effective.

##### **How to send a [secure] email:**

1. To send a secure email you have to bracket the word **secure** in the subject line, anywhere.
2. Nothing can touch the outer parts of the brackets.
3. If any letter or character should touch any part of the brackets, the email is no longer secure.
4. You must utilize the Brackets [ ] and not the parenthesis { }.

##### **See the examples below:**

- a. [secure] This is good – Anywhere in the subject line is good.
- b. [secure]this will not work – The word "this" is too close to the bracket.
- c. This {secure} is not good – Brackets not Parenthesis!
- d. This [secure] is good – Anywhere in the subject line is good.
- e. This is good [secure] – Anywhere in the subject line is good.

#### D. **Internet Access and Use:**

1. Access to the Internet will only be provided to employees for the sole purpose of fulfilling responsibilities and job duties as defined by SCLHSA. The following guidelines shall be used to regulate and provide Internet access.
  - a. Access to the Internet will be made available to all employees who have a need to obtain information over the Internet in the performance of their responsibilities and job duties.
  - b. Use of the Internet for any purpose other than legitimate SCLHSA business or SCLHSA research is prohibited and may result in disciplinary action up to and including termination

- c. All Internet data that is composed, transmitted and/or received by SCLHSA computer systems is considered to belong to SCLHSA and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
  - d. The equipment, services and technology used to access the Internet are the property of SCLHSA and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.
  - e. SCLHSA IT Department has the capability and the authority to evaluate the performance and use of its IT resources and will routinely monitor their use. SCLHSA IT will maintain a log of all access to the Internet. Reports of activity will be made available upon request by management. The IT Director or a designee may conduct random audits of users' accounts.
  - f. All sites and downloads may be monitored and/or blocked by SCLHSA if they are deemed to be harmful and/or not productive to business.
2. Use of the Internet for any purpose other than legitimate SCLHSA business or SCLHSA research is prohibited. Unacceptable use of the Internet by employees includes, but is not limited to:
    - a. Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal or offensive material.
    - b. Using computers to perpetrate any form of fraud, and/or software, film or music piracy
    - c. Stealing, using, or disclosing someone else's password without authorization.
    - d. Downloading, copying or pirating software and electronic files without authorization or that are copyrighted.
    - e. Sharing confidential material, trade secrets, or proprietary information outside of the organization.
    - f. Bypassing Internet security restrictions to access unauthorized websites.
    - g. Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.
    - h. Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.
    - i. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
    - j. Passing off personal views as representing those of the organization.
  3. Supervisors are ultimately responsible for determining when an employee's Internet use is interfering with that employee's ability to perform duties. SCLHSA employees do not have a right to, or expectation of, privacy while using any government equipment at any time.
  4. Supervisors and Division Directors are responsible for the enforcement of this policy.
  5. Individuals, who abuse these resources, knowingly interfere with the operation of IT systems, or otherwise fail to comply with the provisions of this policy are subject to disciplinary action, including loss of privileges and up to termination.

**Compliance Requirement:**

There are no compliance requirements for this policy.

**Attachments:**

There are no attachments for this policy.

**Linkages:**

There are no linkages for this policy.