**POLICIES AND PROCEDURES MANUAL**

|  |  |
| --- | --- |
| **TITLE** | **Email Access Policy** |
| **LEGAL AUTHORITY** | **President and Cabinet** |
| **DATE APPROVED** | **June 22, 2015**  **Revised: June 28, 2023** |

**Introduction:**

Lawson State Community College (LSCC) email services support the administrative activities of the college and serve as a means of official communication by and between users and LSCC. The purpose of this policy is to ensure that this critical service remains available and reliable, and is used for purposes appropriate to the LSCC Mission.

1. **Policy**
   1. Electronic Mail (“email”) services shall be made available to every individual working at LSCC for the purpose of conducting and communicating official College business. Incidental personal use of email is allowed with the understanding that the primary use is job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.
   2. Email services are provided only while a user is employed by LSCC. Once a user is separated from LSCC, the user’s electronic services are terminated and former employees may no longer access the contents of their mailboxes, nor should they export their mailbox to a personal account before departure.
      1. Retired employees who continue to assist the college in an official capacity may continue to have access to the LSCC Email after recommendation from the Vice President’s Office and final approval by the College President.
   3. Email users are advised that electronic data (and communications using LSCC network for transmission or storage) may be reviewed and/or accessed by authorized LSCC officials for purposes related to College business. LSCC has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.
      1. Email users do not have any expectation of privacy with regard to the contents of such equipment, files, or email on LSCC’s electronic systems.
   4. Intentional and unauthorized access to other persons email is strictly prohibited.
   5. Sending “spam”, chain letters, or any other type of unauthorized widespread distribution of unsolicited email is prohibited.
   6. Use of email for non-Departmental-related commercial activities or personal gain is prohibited.
   7. Use of email for partisan political or lobbying activities is prohibited.
   8. Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications is prohibited.
   9. Use of email to transmit materials in a manner which violates copyright laws is prohibited. Please refer to <http://www.copyright.gov/circs/circ21.pdf> for information regarding educational exceptions to copyright law.
   10. LSCC attempts to provide secure, private, and reliable email services by following sound information technology practices. However, LSCC cannot guarantee the security, privacy, or reliability of its email service. All users, therefore, should exercise extreme caution in using LSCC email to communicate confidential or sensitive matters.
   11. All users of Lawson State’s email system will have their accounts protected behind a Multi-Factor Authentication System. The employee will provide an SMS number for texting of a verification code, the usage of an approved Authenticator Application on a mobile device, or in the cases of shared mailboxes an OAUTH token will be provided by the Lawson State MIS Department.
   12. Upon separation from LSCC, an employee’s mailbox will be made available to an authorized user who is assuming the separated employee’s responsibilities for a time period not to exceed 30 days. This access must be recommendation from the Vice President with final approval from the College President.
2. **Procedures**
   1. Employees should create an email account for personal use through a public service, such as the employee’s internet service provider, Gmail, Yahoo, or Hotmail. Personal emails should not be sent to LSCC accounts unless absolutely necessary (E.g., school system emergency alerts would be acceptable personal items to be sent to a LSCC email account).
   2. Email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web-links within an email message unless the user is certain that the link is legitimate. Following a link in an email message may execute code that can also install malicious programs on the workstation.
   3. Forms sent via email from an unknown sender should never be filled out by following the link. Theft of one’s identity can result.
   4. Users on an extended absence should create an Out-Of-Office message, which should include the contact information for another staff member who can respond while the user is away from the office.
   5. An email account that has been compromised, whether through password-cracking, social engineering or any other means, must be promptly remedied with the appropriate means. The appropriate means will include a password reset, review of account settings, computer scans and malware disinfection to prevent possible leakage of private information, spamming, potentially infecting others and degradation of network services. If the account is being used to harm others, the Director of Information Management Systems may disable the account until further investigation has been completed.