**POLICIES AND PROCEDURES MANUAL**

|  |  |
| --- | --- |
| **TITLE** | **Mobile Device Security Policy – Lawson State**  **Lawson State owned mobile devices** |
| **LEGAL AUTHORITY** | **President and Cabinet** |
| **DATE APPROVED** | **PENDING APPROVAL** |

**Introduction:**

Mobile devices (E.g Smart Phones, Laptops, Tablets) are a critical component to maintaining standard business operations. Their portability and functionality have made mobile devices a necessary tool; however, their usage increases the security exposure of those employees who utilize them for business. The purpose of this policy is to establish protocols and procedures for the usage of Lawson State provided mobile devices.

**Scope:**

Any mobile device, owned by Lawson State, that will be used to access any Lawson State resources. These resources include but are not limited to Lawson State Employee Email, Blackboard ULTRA Learning Management System, “My Lawson”, Ellucian Banner ERP Software, Microsoft Teams/Sharepoint, and VPN software. Also included is any document created by or received by a Lawson State employee that is used to perform their job function at the College.

Policy 1.0 – General Information

* 1. Mobile computing devices must be protected with a password that meets the minimum standard policy as defined by Lawson State’s Password Policy and Procedures. Mobile devices that are protected by a PIN must be a minimum of six digits.
  2. All data stored on mobile devices must be encrypted.
  3. Mobile devices shall not be connected to “Unsecured” wireless networks.
  4. Location services must be enabled on all mobile computing devices.

Policy 2.0 – User Responsibilities

2.1 Lost or Stolen devices should be reported immediately to the Lawson State Community College Police Department who will immediately notify the MIS Department

2.2 No unauthorized software shall be installed on Lawson State owned mobile devices

2.3 Staff will not load illegal or pirated content onto Lawson State owned mobile devices

2.4 Staff will not remove or revoke software installed by the Lawson State MIS Department

2.5 Mobile devices owned by Lawson State, shall be returned to campus and connected to our secure wireless network at least once every 30 days.

Policy 4.0 – Audit Controls and Permissions

4.1 At the request of the MIS Department, employees shall submit their Lawson State owned mobile devices for inspection

4.2 Lawson State MIS Department reserves the right to lock any device from access to our internal or external networks to protect the security and integrity of our technology resources.

4.3 Lawson State MIS Department will notify direct supervisors, deans, and Vice Presidents and Presidents of any violation of these policies.

4.4 Lawson State MIS Department will document all data in regards to policy violation and submit reports to Human Resources for documentation in employee personnel files.

Policy 5.0 – Enforcement

5.1 Staff members found in violation of this policy may be subject to disciplinary action, up to and including termination.