**POLICIES AND PROCEDURES MANUAL**

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

**Introduction:**

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Lawson State Community College’s (LSCC) resources. All users, including contractors and vendors with access of LSCC systems, are responsible for taking appropriate steps as outlined below, to select and secure their passwords.

1. **Policy**
	1. Lawson State Community College is committed to maintaining systematic controls over access to the College’s data and resources. Therefore, all users, including contractors and vendors with access to LSCC systems, are required to create and use strong passwords.
	2. All user-level and system-level passwords most conform to the *Password Construction Guidelines*.
	3. Users must not use the same password for LSCC accounts as for other non-LSCC access (for example, personal email, banking, etc…)
	4. At user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every three months.
	5. Password cracking or guessing may be performed on a periodic or random basis by the Staff of the Management Information Systems Department. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines in Section 2.2 of this document.
	6. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential LSCC information.
	7. Passwords must not be inserted into email messages or other forms of electronic communication.
	8. Passwords must not be revealed over the phone, unless you have initiated contact with a known MIS Staff member.
	9. Do not reveal a password on questionnaires or security forms.
	10. Do not hint at the format of a password (for example, “my family name”).
	11. Do not share LSCC passwords with anyone, including administrative assistants, secretaries, managers, co-workers on vacation, and family members. Documents and files that may need to be shared with these individuals should be saved on the appropriate network drive.
	12. Any user suspecting that his/her password may have been compromised must report the incident to the Director of Information Management Systems and change all passwords immediately.
	13. Any exception to the policy must be approved by the Vice President over your Department only upon the recommendation of the Director of Information Management Systems.
2. **Procedures**
	1. The Management Information Systems Department uses Group Policy to enforce compliance to strong password standards and password expiration.
	2. Passwords will be changed no more than every 90 days.
	3. Password resets will be done strictly through the Microsoft Azure Password Reset Portal through a Multi-Factor Authentication Process
	4. A strong password for LSCC follows these rules:
* A minimum of eight (8) characters
* Cannot contain the User’s account name
* Contains at least one character from 3 of the following 4 categories
	+ Uppercase letters (A-Z)
	+ Lowercase letters (a-z)
	+ Numbers (0-9)
	+ Special characters (E.g., ! @ # $ % ^ & \*)
* Cannot be the same as any previously used passwords