Password Policy

Section 1. PURPOSE AND SCOPE

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and exploitation of Clark University's resources. All users, including employees, students, contractors and vendors with access to Clark University systems are responsible for taking the appropriate steps as outlined in this policy to select and protect their passwords.

This document is intended to offer minimum standards for system and application administrators and developers. A department and/or system administrator may implement a more restrictive policy on local systems where deemed appropriate or necessary for the security of electronic information resources. Regulatory, compliance, or grant requirements supersede any standards defined below.

Section 2. DEFINITIONS

Sensitive Information: Any data (electronic or physical), for which the compromise of confidentiality, integrity, and availability could have a material adverse effect on Clark University's interests, the conduct of University programs or the privacy to which individuals are entitled. Examples include: Personal Information and Protected Health Information as defined below; any data protected by the, Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data; or data that the University determines is in need of protective measures.

Access or Login Credentials: Information presented by a user to an authentication authority for identification and login access to previously authorized resource(s). Access or login credentials are usually comprised of a User ID (username) and a Password, although other methods like certificates, biometric information, security questions and multifactor authentication are being used more widely.

Information Security Office (ISO): The division of the University’s Information Technology Systems responsible for overseeing information security and acting as the point of contact for violations (inadvertent or deliberate) or issues: infosec@clarku.edu

Simple Network Management Protocol (SNMP): Protocol used to manage and monitor network devices like servers, switches, routers, firewalls, etc.

Password: A sequence of characters used to authenticate a person’s identity. Passphrases, passcodes and personal identification numbers (PIN) serve the same purpose as a password.

Privileged account: A privileged account is an account with a high level of access to a system, and is typically used by a systems administrator to log into servers, switches, firewalls, routers, database servers, and the many applications they manage.

User level account: Accounts assigned to users to provide them with access to University resources such as email, private websites, hosted administrative systems, etc.

Service account: An account used by systems rather than by users. These accounts are usually under the responsibility of systems administrators and are used to run automated processes like scheduled tasks, deployments, monitoring, running services on computers and servers, etc. If these accounts also have high levels of access to resources, they are also considered Privileged Accounts.

Section 3. CREATION OF PASSWORDS

Passwords created by users of University systems, and on systems where technology makes it possible, shall conform to the following standards:

Your password must be a minimum of 15 characters long and must contain three of the four categories below:

- At least one special character (&,#,-,_, etc.) (excluding the apostrophe ‘).
- At least one uppercase English letter (A to Z)
- At least one lowercase English letter (A to Z)
- At least one digit (0-9)

Passwords SHALL NOT contain:

- Sequences of three or more characters from your Clark username or email address
- Patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Password examples defined on the support site, (e.g. Welcome!23)

These provisions shall be enforced electronically whenever possible.

Changing Passwords

Passwords must expire after no longer than 365 days. Whenever possible, change your password on campus, with a wired connection. If you have to change your password from off-campus, connect to the VPN first. For information on connecting to the VPN follow this link: **https://www.clarku.edu/offices/its/a-z-service-catalog/vpn/**

Protecting a Password

- Passwords are confidential information (see Data Classification Policy).
- Passwords must not be included in email messages or other forms of electronic communication.
- Passwords must not be written down on paper and stored an open and obvious areas.

Sharing a Password

- Clark Account Online IDs are issued to individuals for their exclusive use, and passwords may not be shared.
- Departmental account passwords must be shared only with appropriately designated departmental personnel. Such passwords should be shared securely using a password manager such as LastPass.
- Users need to beware of "phishing" or other social engineering scams where a user may have a password requested over the phone. University information technology personnel (i.e., ITS Help Desk, ISO, Departmental Technical Staff), as a best practice, will not request a user's password.

Reporting a Password Compromise

- Suspected compromises of passwords must be reported immediately to the Clark ITS Help Desk at helpdesk@clarku.edu, 508-793-7745.
- The password in question must be changed immediately.

Section 4. EXCLUSIONS AND SPECIAL CIRCUMSTANCES

Exceptions to this Policy shall only be allowed if previously approved and is documented and verified by the Chief Information Officer.

Section 5. ENFORCEMENT

Faculty, staff, and student employees who violate this University policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.

Students who violate this University policy may be subject to proceedings for non-academic misconduct based on their student status.

Faculty, staff, student employees, and students may also be subject to the discontinuance of specified information technology services based on the policy violation.

Related Policies and Regulations

Acceptable Use Policy

Data Classification Policy

History/Revision Information

Responsible Office/ Division: ITS
Effective Date: February 26, 2024
Last Amended Date:
Next Review Date: February 26, 2027