University of CINCINNATI	*Policy Title:* **Password**	*Policy Number:* **9.1.23**
Category: Information Technology	**Effective Date:** 06/24/2021	**Policy Owner:** VP & CIO, Digital Technology Solutions
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** 09/25/2019	**Responsible Office(s):** Office of Information Security

Background

Strong authentication is an important aspect of computer security and is the front line of protection for user access to computerized information systems containing Restricted data, identity information, financial information, or other electronic information. This policy is to ensure that all university employees, contractors, vendors with access to university systems and students take responsibility for using appropriate means to establish positive identification when accessing university information systems.

Policy

The University of Cincinnati and all individuals accessing or using information technology resources are responsible for ensuring that university identities and credentials are protected from inappropriate use or disclosure.

- Passwords must be protected from disclosure and must not be shared. Users who suspect that their passwords have been disclosed or compromised must immediately reset all passwords in question via Password Self Service (PSS) and notify the Service Desk.
- Access to applications used to host, display, process and/or transmit Restricted, or regulated data, must utilize the multi-factor authentication solution provided by the Office of Information Security.
- Passwords at minimum must meet the following criteria:
  - Eight characters.
  - Must contain at least three of the following categories: uppercase (A-Z), lowercase (a-z), alphanumeric (0-9) characters, special character.
  - Passwords may not contain any part of your name or username.
  - Last 6 passwords may not be reused.

    - Default passwords must be changed immediately.
    - All passwords must be encrypted and/or hashed during transit and when stored.
    - Password lockout must occur after authentication failure of multiple attempts.
    - Expiration period of no longer than 180 days.
        - Some regulations or contractual obligations may require more stringent requirements than listed above. If applicable, those requirements must be applied to ensure compliance. Identifiers such as Username must be unique and must not be reused.
- Use of personal credentials for automated systems and processes is not permitted. Service accounts must be utilized for automated processes used in support of approved university technologies.
    - Service accounts must be requested and approved via standard university process.

Definitions

Data Custodian: computer system administrators responsible for the operation and management of systems and services which store or provide access to institutional data.

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu