University of CINCINNATI	*Policy Title:* **Password**	*Policy Number:* **9.1.23**
Category: Information Technology	**Effective Date:** 09/25/2019	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Faculty/Staff/Students/ Affiliates	**Prior Effective Date:** 09/26/2018	**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

IT@UC and University of Cincinnati Data Custodians (computer systems administrators) are responsible for ensuring that university information is protected from inappropriate 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 IT@UC's Service Desk.
- Access to software applications used to host, display, process and/or transmit Restricted data such as applications for human resources, accounting, student information system, restricted research data, etc., must utilize the multi-factor authentication solution provided by Office of Information Security.
- Passwords must meet the following criteria:
  - Minimum of eight characters
  - Must contain at least one each of the following: uppercase (A-Z), lowercase (a-z), alphanumeric (0-9) characters
  - Passwords may not contain any form of your name or username.
  - Password reuse is not allowed for at least the past 6 passwords.
  - 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 (ideally 5 or less)
- 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. For example, the Payment Card Industry – Data Security Standard (PCI-DSS) requires password expiration of no longer than 90 days.
- Identifiers such as Username must be unique and must not be reused.
- Disable authentication after an appropriate period of inactivity as required by regulatory compliance.

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

Document History

Issued: 09/24/2014
Reviewed: 01/21/2016
Revised: 11/21/2016
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019