Ohio Administrative Code

Rule 3341-6-62 Password Standards.

Effective: March 13, 2025

(A) Policy statement and purpose

Strong authentication and access control processes are the primary safeguards which protect university information systems, data, and other resources from unauthorized access and use. Strong authentication processes rely on constructing secure passwords and ensuring proper management of passwords. The purpose of this policy is to ensure the integrity, availability, and confidentiality of university resources, protect against unauthorized access, minimize potential security risks, and ensure compliance with laws and regulations.

This policy serves to ensure compliance with industry best practices and to meet the requirements of the following security frameworks: CIS benchmarks; ISO/IEC 27001, 27002; NIST SP 800-53, SP 800-171; PCI DSS; the HIPAA security rule; and the GLBA FTC safeguards rule.

(B) Policy scope

This policy applies to all password-protected university information systems, data, and other resources.

(C) Policy

Accounts shall be protected by strong passwords. Account users and system administrators shall protect the security of those passwords by managing passwords in a responsible fashion. System developers shall develop systems that store or transmit password data responsibly and that use secure authentication and authorization methods to control access to accounts.

(1) Required characteristics for passwords

All passwords shall have the following characteristics:

(a) Be at least twelve characters in length.

(b) Contain at least one character from each of the following types of characters:

(i) English upper case (A-Z);

(ii) English lower case (a-z);

(iii) Numerals (0-9); and

(iv) Special characters (! @,#,$,%,^,&,*)

(c) Must not contain easily accessible or guessable personal information about the user or user's family, such as names, birthdays, pets' names, addresses, etc.

(d) Must not be a publicly available password, a previously compromised password, or a simple permutation of either. For example, if the password "GoFALCONs!2023" is known to be compromised, "GoFALCONs!2024" or similar should not be used.

(e) Must not be a password that is actively being used for other non-university accounts and services.

(2) Password management requirements

The following requirements apply to all password users.

(a) Each password shall be treated as confidential information and not be shared with anyone including, but not limited to, family members, administrative assistants, or ITS personnel.

(b) Users shall not write and store passwords digitally in clear text anywhere such as in their office computer or other electronic device. If a password needs to be written down, it needs to be secured when not in use. Alternatively, a password vault or password manager can be used to store passwords confidentially (i.e., Apple passwords, Google password manager, etc.)

(c) Passwords shall not be stored in a file on any computer system, including smart devices, without being stored within an encrypted file.

(d) Passwords shall not be transmitted electronically (e.g., inserted into email messages or other forms of electronic communication) unless encrypted.

(e) Temporary or "first use" passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system and must only be valid for a limited time before expiring.

(f) One-time passwords must only be valid for a limited time before expiring.

(g) Default passwords in systems must be changed.

(h) Passwords for production systems must not be used in test and development environments.

(i) If a password is suspected of being compromised, the incident must be reported in accordance with the cybersecurity incident reporting policy.

(j) Separate user accounts for the administration of system shall have unique passwords that are separate from other accounts held by that user.

(k) Password history must be enabled where available and configured to prohibit re-use of the last ten previously used passwords.

(l) Where practical, account lockout, or other rate-limiting mechanisms, must be enabled to lock or disable the account after five unsuccessful or failed login attempts. Temporary lockouts are permitted, provided the lockout period is longer than thirty minutes.

(m) Administrator-level passwords shall be changed every ninety days.

(n) If multifactor authentication is enabled, user-level passwords shall be changed every three-hundred-sixty-five days.

(o) If multifactor authentication is not enabled, user-level passwords must be changed every one-hundred-eighty days.

(p) Passwords for accounts and systems with a specific regulatory requirement to be changed at a defined frequency must be changed according to that frequency (e.g., payment card industry card holder data, certain research data, etc.).

(q) System-level (system-to-system or non-interactive services account) passwords shall be changed after a significant event (i.e., administrator departure, suspicion, or actual compromise event).

(r) A password shall be changed after it has been compromised or disclosed.

(3) Requirements for application developers

The following additional requirements apply to application developers.

(a) Secure transmission shall be required. Application developers shall, whenever possible, develop applications that require secure protocols for authentication.

(b) Application developers shall not create applications which store passwords. If storage of password values cannot be avoided, application developers shall ensure that passwords are stored only as securely hashed values. Securely hashed values must be created by including random data (a cryptographic salt) inputted along with password data into a strong one-way hashing algorithm.

(c) Whenever possible, applications shall use the BGSU SSO service for authentication.