Preamble: Authentication of users and applications, accessing or processing data is a fundamental requirement of information security to ensure confidentiality and integrity of data. This policy establishes authentication requirements for the use of University of Idaho technology resources.

Contents:

A. Definitions
B. Policy
C. Scope
D. Exceptions to the Policy
E. Contact Information
F. References

A. Definitions – Types of Authentication. Below are the most common types of authentication used at the university.

A-1. Password: a combination of letters, numbers, symbols, and special characters that can be used to authenticate a person to an account accessing a technology resource. Long forms of passwords are sometimes called a passphrase.

A-2. Biometric: unique physical or behavioral characteristics of a person that can be analyzed to uniquely identify and authenticate a person to an account for accessing a technology resource.

A-3. Token: a hardware or software device that can be cryptographically verified as unique.

A-4. Geolocation: for purposes of this policy, geolocation refers to the process of identifying the locations of a user based upon the known locations of their Internet Protocol (IP) addresses, or from data collected from their authenticated devices with built-in location detection.

A-5. API Token: for purposes of this policy, an application program interface (API) token is a unique, long, token or key that may provide authentication for an application to access another service or application.

A-6. Personal Identification Number (PIN): a short number or password used locally on a device as a convenient authentication alternative to typing a full password.


B. Policy. Consistent with the university’s requirements for identity and access management, users must protect the integrity of their authentication methods, for all UI technology resources requiring their authentication. All authentication types must be secured as appropriate for the level of risk.

B-1. Responsibility of Users:

a. Users are responsible for keeping passwords and all other types of authentication secure and confidential, including not sharing or storing passwords in an insecure manner. Passwords should not be written down and/or left in an easily accessible location.

b. Passwords are confidential university information and should never be stored electronically without strong encryption.

c. All passwords must be changed at first issuance or use.

d. Passwords must not be shared for any individual accounts, including with IT support professionals, and only shared for other account types as defined in UI Identity and Access Management (APM 30.10) to the minimum extent required. If anyone asks a user for their password, they are obligated to report this to ITS Security as a security incident.

e. For any shared passwords, whenever any person with knowledge of the password changes to a role where they no longer require knowledge of the password (i.e., leaves the university or changes positions), the password must be changed.

f. Passwords for UI systems must be unique. Users should never use their UI password for any third-party systems, even if used for UI business purposes. Users should never use the same password for privileged and non-privileged accounts.

g. Users must not store passwords with applications or use the “remember password” functions built into web browsers. Using a third-party password manager is highly encouraged to create strong
passwords and store them securely. (Contact ITS for a list of currently recommended password managers.)
h. Always log out of applications or lock computers when leaving a computer to prevent unauthorized use.
i. Users must not attempt to circumvent UI established authentication processes.
j. Users must follow ITS standards for authentication and password specifications. (See ITS Standards http://www.uidaho.edu/its/standards/

B-2. Remediation and Compliance. Noncompliance with this policy shall be considered a violation of UI Acceptable Use (APM 30.12) and will be addressed and remediated accordingly.

C. Scope. This policy applies to all account holders regardless of affiliation with access to university data or information systems.

D. Exceptions to the Policy. Exceptions to this policy may be submitted in writing to the UI Information Security Officer who will assess the risk and make a recommendation to the UI Chief Information Officer. Exceptions must be reviewed for reauthorization on no less than an annual basis.

E. Contact Information. The ITS Information Security Office (its-security@uidaho.edu) can assist with questions regarding this policy and related standards.

F. References.

APM 30.10 – Identity and Access Management Policy
APM 30.11 – Data Classifications and Standards
APM 30.12 – Acceptable Use of Technology Resources
NIST SP800-53r4
NIST SP800-171
HIPAA Security Rule 164.312(d)