30.10 – Identity and Access Management Policy
October 5, 2018 (rewrite)

Preamble: This establishes access management policies and standards that allow only authorized individuals to manage and access university data and systems. It also requires use of university accounts for university business.

Contents:

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

A. Definitions.

A-1. Account: For purposes of this policy, an account is an electronic identifier used by systems and applications to authenticate and authorize users or processes to access university technology resources and to facilitate auditing of activities associated with an individual user.

A-2. Account Types:

a. Individual – Primary account assigned to a single individual for access to technology resources, including interactive logon to computers, email, VPN, Banner, or other U of I resources.

b. Shared – Account used or shared where multiple users know the password or otherwise use the account for interactive logon.

c. Functional – Account used by applications and processes and not interactively by end users.

d. Privileged – Individual account utilized for elevated access to systems or data, which may include authority to make changes to access permissions, roles, security configuration, or non-public data of other users.

e. Resource – Account utilized for tracking or use of a resource (typically for rooms or equipment in Office 365), and not logged on to interactively.

f. Sponsored – Individual account assigned to a single individual where the user does not have a formal affiliation with the University, either as an employee or student.

g. Temp or Emergency – Account utilized for temporary access to a system or resource outside of automated account management. This account type may include generic guest accounts.

h. Third party accounts – Individual or shared accounts created in non-university systems (e.g., Twitter, Instagram, etc.) for performing duties on behalf of the University.

A-3. Authentication: Authentication is the process by which a system or application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized. Authentication factors may include something you know (e.g., password), something you have (e.g., hardware token, certificate, or Duo software authenticator), or something you are (usually a biometric, like a fingerprint).

A-4. Authorization: A process by which access to a resource is authorized based upon the authenticated identity or account.

A-5. Federated Identity: An account which can be used across disparate technology systems or organizations, typically through a Single Sign On (SSO) service.
A-6. **Single Sign On**: Use of a single account to access multiple applications or systems.

A-7. **Account manager**: An individual or system that manages accounts, assigns accounts to individuals, and grants privileges to accounts.

**B. Policy.** Access to university systems and data must be provided in a way that such access can be audited and uniquely tied to the persons and their role with the university.

**B-1. Responsibilities of Account Managers:**

a. **Authority**: Managing accounts is the responsibility of Information Technology Services (ITS). All accounts must be managed in accordance with current ITS standards, including requirements for identity vetting, passwords, multifactor authentication, federation, auditing, and lifecycle (creation and termination). ITS may publish standards to supplement and enforce this policy.

b. **Automation**: Automated account management (software and/or scripts) shall be used to ensure accounts are managed as appropriate when each account user’s role with the university changes according to official university records in Banner. Use of all accounts shall be monitored by automated tools to detect atypical use and take appropriate action, up to and including disabling of the account.

c. **Access**: Access granted to each account must be reviewed at least annually by appropriate data stewards (see APM 30.11) or account managers to ensure all access is authorized.

d. **Temp Accounts**: Temporary or emergency accounts shall be disabled or removed automatically to prevent misuse. Such accounts shall not be created when another method of providing access to university technology resources reasonably exists.

e. **Shared Accounts**: Shared accounts shall not be created or assigned when an individual account access method is available.

f. **Sponsored Accounts**: All such accounts must be sponsored by a full-time, benefits-eligible university employee and periodically renewed. Only individuals with legitimate and documented work or academic reasons may hold an account. Sponsored accounts shall not be assigned when another method of account assignment is available.

**g. Inactive Accounts**: Built-in or automated systems shall disable any account which has been determined to be inactive. Account inactivity timeframes will be determined according to risk and published as ITS Standards, but in no case should they exceed 180 days. Exceptions can be made for accounts which are not used interactively or where active use is not expected or cannot be accurately determined.

**h. Lifecycle**: All accounts shall be maintained only as long as there is a documented affiliation of the account holder with the university. Accounts shall not be created until there are sufficient records in Banner to uniquely identify the account holder. Changes to university roles of the account holder require review of access granted to their accounts. This includes changing of assigned access, or up to and including account renaming or creation of a new account for the new role.

i. **Auditing**: Information systems used at the UI must audit account creation, modification, enabling, disabling, and removal actions and notify the account managers or security operations team and/or log centrally.

**j. Relationship/Affiliation**: All individual accounts shall be assigned appropriate “eduPersonAffiliation” (see Internet2 eduPerson Object Class schema) according to their relationship(s) with the university.
**k. Federation:** Federated identity services for university accounts shall only be provided by ITS or ITS-approved systems or vendors. Federation shall be used by all university applications and websites, to meet Standards for Data Classifications, or for any service used by a large number of faculty, staff, or students.

**l. Preferred Email:** Accounts and records shall be maintained to enforce use of @uidaho.edu email addresses for communication to employees or other approved individuals conducting university business. This includes publishing in the campus directory. Students, alumni, and retirees should use alternate domains or email addresses for personal or student matters to ensure their records are separate from university business that may be subject to public records request. Active students, enrolled in the current term, must have their preferred email address set to their @vandals.uidaho.edu email address if they are not also a benefits-eligible employee. Individuals with multiple roles should be assigned a preferred email address based upon their primary role. Where possible, use of student and employee addresses for communication should favor role-based official UI addresses, rather than using the preferred address.

**m. Auto-forwarding Email:** University systems shall be configured to prevent automatic forwarding of email directly, or via rule or filter, for accounts created for conduct of university business. Where not possible to prevent this configuration, automation shall be used when possible to correct the automatic forwarding and notify the user of the change. Accounts not directly, or reasonably expected, to be involved in university business, including but not limited to students, alumni, and retirees will be allowed to auto-forward email.

**n. Account Reuse:** Once an individual account has been assigned and used by a person, it shall not be assigned or re-used by any other person. This includes both the specific account, and re-use of the email address at any future date.

**o. Privileged Accounts:** Separate individual accounts shall be created and must be used for any privileged access. Use of privileged accounts shall be logged. Privileged accounts shall not be used for non-privileged functions (email, web-browsing, etc.).

**p. Passwords:** All systems and accounts shall be configured to require or meet current ITS password standards.

**q. Least Privilege:** When provisioning accounts, principles of least privilege shall apply. To the extent possible, accounts should be granted sufficient privileges to perform approved functions and no more.

**B-2. Responsibilities of the Individual:**

**a. Authentication:** All users of accounts must protect any authentication mechanisms, including passwords or other authentication factors (MFA tokens, certificates, internet cookies, etc.) to ensure only appropriate access to university data and resources. Passwords shall not be shared.

**b. Policy:** All users of accounts must follow university policies and standards, including but not limited to, the Acceptable Use of Technology Resources (APM 30.12) and the Standards for Data Classifications.

**c. Privileges:** All accounts shall be used only for the purpose they were authorized.

**d. Misuse:** Any disclosure of an account password or suspected compromise or misuse of accounts or data must be reported immediately to the Information Security Office at security@uidaho.edu.

**e. Accounts:** All university business shall be conducted using an account associated with @uidaho.edu addresses, or approved exceptions. Non-university accounts such as personal Gmail, Yahoo, etc. accounts shall NOT be used for conducting university business. To protect personal information, Student, Alumni, and Retiree accounts shall not be used for conducting university business.
f. **Communication:** Official university communications may be delivered to preferred or required addresses for those with @uidaho.edu or @vandals.uidaho.edu addresses. Account holders must periodically check these accounts for required communication and, if forwarding is allowed, are responsible for checking the destination address. The university is not responsible for messages forwarded to third party mailboxes. Some university business processes may require receiving messages from valid U of I email addresses, and may not accept messages from third party accounts (Gmail, Yahoo, etc.).

g. **Third Party Accounts:** Accounts created in non-university systems but used for university business must be handled consistent with the policies for accounts, including association with @uidaho.edu email addresses, and the current standards published by ITS.

**B-3. Remediation and Compliance.** Noncompliance with this policy shall be considered a violation of 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 U of I 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 30.12 – Acceptable Use of Technology Resources
   APM 30.11 – University Data Classifications and Standards
   APM 30.15 – UI Password/Passphrase Policy
   NIST SP800-53r4
   NIST SP800-171
   HIPAA Security Rule 45 CFR 164.312(d)
   eduPerson Object Class Specification