POLICIES AND PROCEDURES

Information Technology Services

Access Control

ISUPP 12040

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Access Control*
Responsible Executive (RE): *Chief Information Officer*
Sponsoring Organization (SO): *Information Technology Services*
Dates: Effective Date: *March 28, 2016*
Revised: *May 4, 2018*
Review Date: *May 2021*

I. INTRODUCTION

It is the objective of Idaho State University (ISU) to prevent unauthorized access to its IT System by establishing access controls based on business and security requirements.

II. DEFINITIONS

A. **Chief Information Officer:** The ISU executive in charge of Information Technology Services.

B. **Critical Information:** Information identified by applicable laws, regulations or policies as personal information, individually identifiable health information, education records, personally identifiable information, non-public personal or institutional data, confidential personal information, or sensitive scientific or sponsored project information.

C. **Data Management Zone (DMZ):** A segment of ISU's Information Network that intercepts electronic traffic and brokers requests, providing an extra layer of protection for sensitive ISU resources which are not allowed to be directly accessible from the Internet.

D. **Essential Computing Resources:** Shared computing resources which cannot undergo loss of access for more than twenty-four (24) hours without causing unacceptable consequences due to a break in business continuity.

E. **Information:** A data set that is considered valuable to an organization. Information is classified in the *Information Technology Services Asset Management Policy ISUPP 2430*.

F. **Information Network:** A telecommunications network that allows Information Systems to electronically exchange data.

G. **Information Owner:** The ISU faculty, staff, or department responsible for accuracy, integrity, and timeliness of a defined subset of ISU's Information, and authorized to grant or deny access to that Information.

H. **Information Security Manager:** The ISU employee that is responsible for leading information security activities at ISU.

I. **Information System:** A computing device that stores, processes, or transmits Information.

J. **Information System Administrator:** The ISU employee that is responsible for the protection and proper use of a specific Information System as assigned by an Information Owner.

K. **Institutional Information:** Information used for the purpose of conducting University business the disclosure, alteration, or destruction of which could result in a moderate level of risk to the University. Information that is not explicitly classified as Critical Information or Public Information should be treated as Institutional Information.

L. **IT System:** ISU's data processing hardware, software, data transmission equipment and infrastructure, data storage devices, and the electronic information stored, processed, or transmitted via these components (including electronic mail).

M. **Public Information:** Information made freely available to the public or if disclosed, is not expected to cause any harm to ISU or any individual associated with or accessing the information.

N. **Storage Media:** Devices designed and dedicated to storing data electronically (e.g., hard disk drives, tape drives and magnetic tape, flash drives, recordable CD/DVD, etc.).

O. **Virtual Private Network (VPN):** Software that extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

III. POLICY STATEMENT

ISU will implement and enforce information access control measures defining under what conditions faculty, staff, contractors, and/or volunteers or technology processes have access to ISU information resources.

IV. AUTHORITY AND RESPONSIBILITIES

All members of the ISU community, including faculty, staff, volunteers, contractors, and visitors are responsible for proper access control to ISU's Information and the IT System.

The Information Technology Services department is charged with seeing that all procedures are followed and for taking corrective action when access to Information and/or the IT System is or may be compromised.

V. PROCEDURES TO IMPLEMENT

A. Business Requirement

1. All accesses to, uses of, and processing of Information must be consistent with ISU policies and standards.
2. Information must be used only for the business purposes expressly authorized by management.
3. Access will be granted only to those individuals who have a legitimate need and only for the minimum access necessary.
4. Access permissions will be granted based on pre-defined roles, whenever possible.

B. User Access Management

1. ISU maintains the authority to protect the confidentiality, integrity, and availability of the information within ISU's IT System at any time, and without prior notice, by:
    a. Restricting or revoking access,
    b. Inspecting, copying, removing, or otherwise altering any data, program, or other system resource that may undermine these objectives,
    c. Taking any other steps deemed necessary to manage and protect its IT System.

    ISU is not responsible for loss or damage to data or software that results from its efforts to meet these security objectives.
2. Access Accounts

a. Access permissions will ensure consistent treatment of all faculty, staff, students, and third parties.

b. Data custodians and/or System Administrators will annually review access permissions to ensure that they are the minimum required for each individual to complete his/her job duties.

c. Access will be granted via a unique, non-generic, password-protected user identifier that is registered in a central identity repository managed by ISU's Information Technology Services department.

d. Third parties will only be granted temporary access for a pre-determined length of time, which defaults to thirty (30) days if not specified otherwise in writing at the time when access is granted.

e. Accounts which have not been used for a contiguous period of thirty (30) days may be disabled.

f. Special system privileges, such as the ability to examine the files of other users, must be approved by the Office of General Counsel, Human Resources, or Public Safety in consultation with the Chief Information Officer.

g. The Chief Information Officer must review and approve all agreements with third parties that involve access to CRITICAL or Institutional Information before the agreement is finalized.

3. User Responsibilities

   a. Individuals given an account granting access to any portion of ISU's IT System are required to:

      i. Securely create, use, store, and manage their account passwords. Passwords, if written down, must be secured in a non-public area where they are not open to viewing by other individuals in the area.

      ii. Secure information systems when not in use, through screen locking or logging off (see attachment: Access Control Standards – Session Time-out Standard).

      iii. Secure Storage Media.

4. Information Network Access Control

   a. All physical connectivity to ISU's Information Network must be approved by Information Technology Services.

   b. ISU's Information Networks will be divided into security zones. Zones will be protected by firewalls and other similar intrusion prevention technologies centrally controlled by Information Technology Services.

c. ISU's Information Systems will be protected by local, host-based firewalls, whenever possible. For defense-in-depth purposes, local firewalls will duplicate protections implemented in segment firewalls applicable to their individual system, whenever possible.

d. Firewalls and perimeter routers will only allow traffic through that is explicitly permitted. All other inbound traffic will be denied by default. Outbound communications should also be denied by default when feasible.

e. Information security staff will approve all requests for non-host based rule changes implemented in firewalls and other similar intrusion prevention technologies managed by Information Technology Services. Networking and Communications staff will implement approved rule changes.

f. All publically accessible Information Systems will reside in a highly controlled subnet (DMZ) with limited access to ISU's restricted Information Networks.

g. No Information Systems containing Critical Information will reside in the DMZ. Information Systems containing Critical Information will further be segmented from the rest of the protected network for additional access protection.

h. Access from a network not managed by ISU's Information Technology Services to any ISU system not in ISU's DMZ must be via a VPN solution approved by Information Technology Services and in adherence with the VPN Standard (see attachment: Access Control Standards - VPN Standard).

i. All Information Network ports in vacant offices and other areas that are not customarily in use must be administratively disabled.

j. Extensions of the Information Network, such as additional routers, bridges, wireless access points or dialup modems, will not be implemented without prior approval by Information Technology Services.

k. Connections to remote third party information systems or networks will not be established without prior approval by Information Technology Services.

l. Wireless Information Networks used for ISU transmissions of Critical Information must always be configured to employ encryption approved by the Information Security Manager (see attachment: Access Control Standards - Wireless Standards).

5. Operating System and Application Control

   a. All Information Systems will require at a minimum, a unique username and password to access the operating system; shared user accounts, blank passwords, or disabling authentication is prohibited.

b. All Information Systems will require a username and password to gain access, whenever feasible (see attachment: Access Control Standards - Password Standards).

c. All operating systems and applications will automatically enforce the User Password Standard (see attachment: Access Control Standards), whenever feasible.

d. Multi-factor authentication will be utilized, whenever feasible.

e. Whenever a system or application must store a password, the Information System Administrator will ensure that the password is never stored nor transmitted in clear text.

f. All operating systems and applications will not transmit passwords over the Information Network in clear text.

g. All Essential Computing Resources will reasonably limit the number of failed login attempts through temporary lockout or time, delaying further login attempts.

h. All Essential Computing Resources will record failed login attempts for later analysis and review.

i. All Essential Computing Resources containing Critical Information will authenticate users against a central authentication system (e.g., LDAP, Active Directory), whenever feasible.

j. All operating systems and applications containing Critical Information will automatically time-out idle user sessions as defined in the Session Time-out Standard (see attachment: Access Control Standards).

6. Application and information access control

   a. Information System Administrator's will work with ITS Information Security to ensure that data processed by ISU's IT System is properly classified before being used in test or production.

   b. All applications containing Critical Information will run on dedicated operating systems or on shared operating systems that only contain applications secured as if they contained Critical Information.

7. Mobile computing and teleworking

   a. All mobile devices (smartphones, tablets, etc.) will be locally authenticated before accessing remote resources.

   b. All access control policies will be adhered to for any faculty or staff accessing ISU Information Networks and applications remotely, regardless of ownership of the computing device.

c. When accessing Critical Information remotely, access must be made using a VPN service approved by Information Technology Services and using a dedicated ISU-owned device. This ISU owned device must be configured and managed in compliance with ISU's information security policies and not be used for personal activities beyond those outlined in ISU's *Information Technology Services Acceptable Use* ISUPP 2400.

VI. ATTACHMENTS

Access Control Standards

Attachment – Access Control Standards

A. Security Zones Standard

As regulations and requirements change, the zone into which a particular subset of data may be placed will change. However, for now there are three security zones:

Critical/Covered: A security zone for data classified as Critical Information that is considered by ISU to be extremely critical in nature, such as Information subject to specific protections under federal or state laws or regulations where a breach of data requires notification of the affected individual(s) and monetary damages may be assessed. See Information Technology Services Asset Management ISUPP 2430, V-B.

Institutional: all information not belonging in the Critical or Public security zones, including Critical Information that is not considered to be critical enough to warrant enhanced security protections provided by the Critical security zone. See Information Technology Services Asset Management ISUPP 2430, V-B.

Public/DMZ: Publicly accessible, external facing resources.

B. Password Standard:

1. Passwords will:
    a. Be eight (8) characters or longer,
    b. Be case-sensitive,
    c. Contain at least one (1) numeric character (0-9),
    d. Contain at least two (2) alphabetical characters (A-Z, a-z),
    e. Contain only the following special characters: ! _ - { } [ ] / . ?
    f. Not contain blank spaces,
    g. Be changed every 180 days or less.
2. New accounts or reset accounts will be issued unique temporary passwords that must be reset upon first login
3. If passwords are written down, they will be stored in an appropriately secure manner with restricted access.

C. Voice Mail Passwords

1. Voice mail passwords are not required to comply with ISU password construction standards, but users must select a voicemail password that is different from their phone extension, their office number, their employee number, or any other number that could be easily guessed.

D. VPN Standard:

1. VPNs will utilize SSL or IPSec protocols.
2. Access will be granted only after successful authentication against LDAP or Active Directory services managed by Information Technology Services.

E. Wireless Standards:

1. Currently, general wireless into which students and the general public are granted access will only be given direct access to the DMZ security zone. Over time, wireless access zones will be created to match the security zones.
2. Wireless Information Networks must be protected by WPA2 at a minimum.

F. Time-out Standards:

1. Logins to personal use systems such as desktops, laptops, workstations, mobile devices, etc. will time out after fifteen (15) minutes (or less) of inactivity.
2. Connections to remote applications and network application gateways will time out after forty-five (45) minutes (or less) of inactivity.
3. Upon time out, the user interface will lock or will automatically log off the user. If locked, the user must re-authenticate to resume work.