



Idaho State University

POLICIES AND PROCEDURES (ISUPP)

Building Access and Physical Security

ISUPP 11030

POLICY INFORMATION

Policy Section: *Facilities*

Policy Title: *Building Access and Physical Security*

Responsible Executive (RE): *Vice President for Operations*

Sponsoring Organization (SO): *Operations*

Effective Date(s): *TBD*

Last Reviewed: *New Policy*

Next Review: *December 2031*

I. INTRODUCTION

This policy establishes a comprehensive framework for managing building access and physical facility security across the University. It defines roles, responsibilities, and enforcement authority related to keys, Access Credentials, and secure space, identifies criteria for high-risk physical spaces, and ensures the integrity of Access Credential systems through formalized key records, audits, and re-keying standards.

Through implementing University building Access Credential controls and establishing mandatory, enforceable requirements the University seeks to reduce the risk of unauthorized access, loss of assets, safety breaches, and compromise of sensitive research and systems.

II. DEFINITIONS

- A. Access Credential. Any mechanism used to unlock or permit entry to a physical space. Access Credentials include Hard Copy Keys, Access Cards, Electronic Keys, fobs, mobile credentials, access codes, or any other method of gaining entrance to secured University facilities.
- B. Access Card. A physical or digital credential that grants permission to a restricted area, system, or service.
- C. Access Credential Authority. The University authority designated to govern Access Credentials, including issuance, records, audits, and re-keying decisions. Access Credential

Authorities have authority over Bengal Cards, Hard Copy Keys, Electronic Keys, fobs, mobile credentials, access codes, or any other method of accessing secured University spaces with Access Credentials.

- D. Access Control Logs. A record documenting the issuance, usage, and return of Access Credentials which monitor University facility access.
- E. Adequate Cause. One or more acts or omissions which, singly or in the aggregate, have directly and substantially affected or impaired an employee's performance of his or her assigned duties or the interests of the Idaho State Board Education or University. In addition, any conduct seriously prejudicial to the Board or University may constitute Adequate Cause for discipline up to and including dismissal or termination of an employee.
- F. Authorized Access Credential Requestor. Individual responsible for requesting Access Credentials for authorized personnel including, cards, codes or stand-alone lock access within their department, building, or functional unit.
- G. Bengal Card Services. Any station at any University location that is authorized to issue Bengal Cards.
- H. Building Access. Using Access Credentials to enter a physical facility or specific areas within the physical facility.
- I. Card Access Listing. Recorded listing of Users who have been given Access Credentials through cards.
- J. Critical Information. Information identified by applicable laws, regulations, or policies as confidential, protected, or regulated records and stored in hard copy form, such as individually identifiable health information, education records, non-public institutional data, confidential information, or sensitive scientific or sponsored project information.
- K. Electronic Key. An electronic hardware device used to wirelessly authenticate Access Credentials, usually with a key fob.
- L. Electronic Key Listing. Recorded listing of Users who have given Electronic Key access.
- M. High-Risk Physical Space. A physical space meeting specific criteria that require enhanced Access Credential controls.
- N. Key Box. A physical box managed by software used to store Hard Copy Keys.
- O. Key Holder. An individual to whom a Hard Copy Key has been issued.
- P. Key System Authority (KSA): The University position designated to govern Hard Copy Key issuance, records, audits, and re-keying decisions.
- Q. Hard Copy Key. Physical cut key that uses non-electronic mechanisms to gain facility access.
- R. Hard Copy Key Listing. A record identifying all Hard Copy Keys, Key Holders, door cores, keying levels, and any related data.

- S. Principle of Least Privilege: Granting the minimum access necessary to perform authorized duties.
- A. User. Any individual who accesses, attempts to access, interacts with, transmits, receives, stores, or otherwise utilizes University Access Credentials. This includes, but is not limited to, students, faculty, staff, affiliates, contractors, volunteers, visiting researchers, third-party service providers, automated processes, guests, and any other entity granted explicit or implicit authorization to use University systems, networks, data, or services.
- T. Stand Alone Lock. Electronic or Hard Copy Key security device that operates independently without being connected to a central network, or software.

III. POLICY STATEMENT

The University maintains a controlled approach to building access to protect people, property, research, and information. Building Access is granted using the Principle of Least Privilege, and aligned to role-based needs. Access Credentials are subject to review, audit, and revocation. Failure to comply with this policy may be considered Adequate Cause and may result in corrective action, up to and including termination of employment, loss of access, disciplinary measures, contract remedies, or referral to law enforcement.

Keys and other Access Credentials remain the property of the University and must be returned when requested for any reason. Users may be held responsible for rekeying spaces if Access Credentials are misplaced or otherwise not returned.

IV. AUTHORITY AND RESPONSIBILITIES

- A. Access Credential Authority. Responsible for Access Credential issuance, revocation, audit, and decisions to rekey. The Access Credential Authority must also maintain complete and accurate records.
- B. Authorized Access Credential Requestors. University employee who holds the authority to request Access Credentials for authorized Users to gain access to University facilities.
- C. Campus Access Credential Administrator. Responsible for coordinating the request of Access Credentials between satellite campuses. The Campus Access Credential Administrator determines the appropriate locking mechanism and access credentialing appropriate for an area, including process for distributing and revoking Access Credentials.
- D. Bengal Card Services. Responsible for issuing Bengal Cards and maintaining accurate and complete records of Bengal Card issuance.
- E. Department Heads and Supervisors. Request Access Credentials based on verified business need. Ensure return of Access Credentials based on role change or separation. Ensure timely notification to Credential Access Authority of personnel changes affecting

access control. Participate in audits and remediate processes based on audit findings.

- F. Employees. Safeguard and return Access Credentials. All employees have the responsibility proactively monitor and protect University areas identified as High Risk spaces.
- G. Facilities Services (Facilities), or designee. Acts as ACA with the responsibility to issue, track, recover and revoke Access Credentials. Responsible for maintaining and auditing credential listings. Facility Services must maintain, initiate, conduct and enforce Access Credential audits, and require corrective actions, including rekeying, when deficiencies are identified. Holds the authority to deny or suspend access when records are incomplete, inaccurate, or noncompliant.
- H. Housing. Maintain Access Credential Authority for University Housing with the responsibility to issue, track, recover and revoke Access Credentials. Responsible for maintaining and auditing credential listings. Facility Services must maintain, initiate, conduct and enforce Access Credential audits, and require corrective actions, including rekeying, when deficiencies are identified. Holds the authority to deny or suspend access when records are incomplete, inaccurate, or noncompliant.
- I. Information Technology Services (ITS). System administrator over Electronic Key access, and access removal. Oversees the installation of card readers and other electronic or digital systems. Acts as ACA for card access and mobile credentials including, but not limited to, issuing, tracking and revoking card access and/or mobile credentials. Responsible for maintaining and auditing credential listings.
- J. Access Credential Holders. Safeguard credentials and prevent sharing or duplication. Report loss, theft, or suspected compromise immediately. Comply with audits and return requirements.
- K. Public Safety. Supports access enforcement, emergency access and revocation protocols, including adding users on intrusion alarms, incident response, and investigations involving access compromise. Public Safety is also responsible for after-hours access requests.
- L. Risk Management. Advises on risk classification, high-risk space designation, and establishing and maintaining necessary controls.

V. ACCESS CREDENTIAL MANAGEMENT

- A. Scope.
 - 1. This policy applies to all University-owned, leased, or controlled facilities.
 - 2. This policy applies to all individuals granted access to University buildings or spaces, including employees, Users, students, contractors, affiliates, volunteers, and visitors.
 - 3. This policy applies to all Access Credentials of any kind.
- B. Access Credential Authorization.

1. Authorized Access Credentials.

- a. Authorized Access Credentials are provided only through Facilities or the specific Access Credential Authority for the facility.
 - b. Access Credentials received by any other means are not authorized. Possessing unauthorized Access Credentials is prohibited by the University.
 - c. Unauthorized Access Credentials must be returned to Facilities or Public Safety.
2. Access must be authorized by a Department Head or Authorized Access Credential Requestor and approved by the Access Credential Authority.
3. Individuals must be provided the Least Privilege and facility access necessary to complete assigned roles within the University.
4. Access to facilities is role-based and, where feasible, time-bound.

B. Prohibited Practices.

1. Engaging in prohibited practices will be considered Adequate Cause that may result in disciplinary action up to and including termination of employment. Prohibited practices include, but are not limited to:
- a. Failure to secure High-Risk Spaces;
 - b. Unauthorized duplication of Access Credentials;
 - c. Sharing Access Credentials;
 - d. Circumventing locks or access controls; and/or,
 - e. Installation of software systems, key access hardware, or Access Credential hardware systems without prior written approval from the Access Credential Authority.

C. Access Credential Issuance and Return.

1. General.

- a. All Access Credentials including Hard Copy Keys are the sole property of the University and must be relinquished upon request or upon leaving the University position for which the Access Credential was authorized.
- b. Failure to return Access Credentials may result in criminal or civil liability as well as disciplinary action.
- c. Users must provide written acknowledgement of Access Credential receipt at Facilities' front desk or other location designated by Facilities for Access Credential return.
- d. Individual Users are permitted one copy of Hard Copy Keys or physical Access Credentials.

- e. Departments are permitted to sign for and control multiple Access Credentials, provided that the department:
 - i. Houses the Access Credential at the department; and,
 - ii. Maintains a secure approved space for Access Credential storage.
 - f. Key rings are only issued to departments with Key Boxes or Keeper Boxes.
 - g. Departments are responsible for ensuring all keys are checked in and returned to the appropriate authority.
 - h. Individual Users and departments could be charged for rekeying any spaces associated with an Access Credential if the Access Credential is not returned to the proper Access Credential Authority.
 - i. Separation and Role Change. Credentials must be returned or deactivated immediately upon separation, or upon change to duties that no longer require Access Credentials.
 - j. Users must physically return Access Credentials to:
 - i. Facilities;
 - ii. The individual department if the key is assigned to the department for storage purposes; or,
 - iii. Their supervisor and the supervisor provides written acknowledgement of receipt.
- B. Contractor Access Credentials.
- 1. Contractor Access Credentials.
 - a. Unless otherwise authorized, Access Credentials must be returned as part of the final walkthrough.
 - b. If Access Credentials are not returned at the time of final walkthrough, the contractor may be responsible for the cost of rekeying.
 - c. Facility Services may grant extensions for extended access in writing.
- C. Re-Keying Criteria.
- 1. A door, core, or Access Credential system must be re-keyed when one or more of the following occur:
 - a. Loss or theft of a Hard Copy Key where recovery cannot be verified;
 - b. Separation, termination, or extended inactivity of an Access Credential User without confirmed Access Credential return;
 - c. Unauthorized duplication or reasonable suspicion of compromise;

- d. Identification of inaccurate, incomplete, or unreliable Access Credential records for the affected space;
 - e. Change in space designation to High-Risk Physical Space;
 - f. Renovation, reassignment, or change in use affecting access pathways; and/or,
 - g. Direction from Public Safety, Risk Management, Information Technology Services, or executive leadership.
2. Re-keying decisions are risk-based, documented, and executed under authority of the Access Credential Authority in consultation with Facilities and Public Safety.

II. HIGH RISK SPACES

A. High Risk Physical Space Criteria and Tracking.

1. High Risk Criteria. A space is designated High Risk if it meets one or more of the following risk criteria:
 - a. Hazardous or Regulated Materials. The space houses hazardous materials, controlled substances, or regulated animals or equipment. This includes, but is not limited to:
 - i. Research laboratories;
 - ii. Healthcare Clinics;
 - iii. Chemical storage rooms; and,
 - iv. Animal facilities.
 - b. Sensitive Research and Compliance. The area contains sensitive, restricted, or export-controlled research. This includes, but is not limited to:
 - i. Secure research labs;
 - ii. Data collection rooms;
 - iii. Records rooms; and,
 - iv. Prototype spaces.
 - c. Critical Infrastructure and IT Systems. The area supports critical infrastructure or physical access to Information Technology Systems or networks where unauthorized entry could result in system compromise. This includes, but is not limited to:
 - i. Data centers;
 - ii. Server rooms;
 - iii. Building control systems;

- iv. IT Data Centers; and,
 - v. Telecom rooms.
- d. Financial and High-Value Assets. The space stores cash, financial instruments, or high-value assets. This includes, but is not limited to:
 - i. Cash handling areas;
 - ii. Equipment vaults;
 - iii. Maintenance storage areas;
 - iv. Museum storage areas;
 - v. Library archives; and,
 - vi. Art storage.
- e. Life, Safety, and Emergency Operations. The space is essential to life, safety, emergency response, or continuity of operations. This includes, but is not limited to:
 - i. Emergency operations centers;
 - ii. Firearms or ammunition storage centers;
 - iii. Public Safety Equipment; and,
 - iv. Fire control rooms.
- f. Institutional Records and Critical Information. The area contains confidential, protected, or regulated records. This includes:
 - i. Hard copy records requiring confidentiality;
 - ii. Registrar archives in which records are physically stored;
 - iii. HR physical records storage; and,
 - iv. Medical or counseling records.
- g. University owned or controlled residencies.
- h. Any location designated and authorized for official Access Credential storage.
- 2. If a space meets multiple risk domains the highest risk classification governs.
- 3. Risk classifications are determined jointly by:
 - a. Facilities Services;
 - b. Access Credential Authority;
 - c. Public Safety;
 - d. Information Technology Services; and,

- e. Risk Management.
- 4. Risk classification must be recorded in the High Risk Space Registry.
- 5. Required controls may be supplemented with compensating controls based on documented risk assessment.
- B. High Risk Space Registry.
 - 1. Facility Space Management, Public Safety, and Risk Management are jointly responsible for identifying and communicating High Risk space designation.
 - 2. The University shall maintain a centralized registry of High Risk Physical Spaces.
 - 3. The registry must be reviewed at least annually, as well as whenever:
 - a. A new building or space is brought into use; and,
 - b. Space use, occupants, or associated risks materially change.
- C. Proactive Risk Review.
 - 1. Access Credentials for High Risk areas must be audited at least twice per year.
 - 2. Public Safety, working with Facilities Space Management, must initiate reassessment of physical security controls when risk indicators arise, including but not limited to:
 - a. Changes in staffing;
 - b. Research activity;
 - c. Equipment value; and/or,
 - d. Incident history.

III. RECORD MANAGEMENT

- A. Records.
 - 1. Access Credential Listings.
 - a. The Access Credential Authority must maintain a complete, current, and accurate listing of:
 - i. Hard Copy Keys;
 - ii. Electronic Keys;
 - iii. Access Cards; and,
 - iv. Any other Access Credential.
 - b. Listings must include the following information, as applicable:
 - i. Cardholder/User name;

- ii. Authorizing official;
 - iii. Employment or affiliation status;
 - iv. Key ID;
 - v. Assignment date;
 - vi. Expiration dates;
 - vii. Keying level;
 - viii. Room number;
 - ix. Hook number and serial number;
 - x. Space designation;
 - xi. Issue date;
 - xii. Key holder;
 - xiii. Authorizing official;
 - xiv. Employment or affiliation status; and,
 - xv. Current status.
- c. Access Credentials may not be issued or retained without a corresponding valid record.
2. Record Integrity. Hard Copy Key Listings are the system of record and must be updated promptly upon issuance, return, loss, or re-keying.
3. Access Control Log Reports.
- a. Access Control Log Reports can only be viewed or accessed for official purposes.
 - b. The following departments may request access log reports:
 - i. The Office of General Counsel;
 - ii. Public Safety;
 - iii. Human Resources;
 - iv. Student Affairs; and,
 - v. The Office of Equal Opportunity and Title IX.
4. Access Credential Audits.
- a. Institution-Wide Audit. Conducted at least annually to validate completeness and accuracy of all Hard Copy Key records.
 - b. High Risk Space Audit. Conducted at least twice per year.
 - c. Triggered Audits. Required upon loss, theft, incident, audit discrepancy, or request

from Public Safety, Risk Management, or executive leadership.

d. Departments must respond to audit requests and remediate findings within timelines set by the Access Credential Authority.

e. Failure to participate in audit or remediation constitutes non-compliance.

B. Compliance and Enforcement.

1. The Access Credential Authority may immediately suspend or revoke access when records are inaccurate, audits are not completed, or risk to safety or assets is identified.

2. Departments and Users who fail to comply may be subject to access revocation, disciplinary action under applicable University policies, contract or other civil remedies, or referral to law enforcement, where applicable.

3. Persistent non-compliance may result in centralized control of access decisions for affected units.

C. Exceptions. Exceptions must be documented, time-limited, risk-assessed, and approved by Facilities in consultation with the Access Credential Authority, Public Safety, and Risk Management.

IV. RELATED LAWS AND POLICIES

A. ISUPP 1030 *University Records, Archives, and Publications*

B. ISUPP 1070 *Environmental Health and Safety*

C. ISUPP 2360 *Physical Inventory and Control of University Property*

D. ISUPP 7110 *Laboratory Safety*

E. ISUPP 9050 *University Trespass*

F. ISUPP 11010 *Use of University Space for Expressive Activity*

G. ISUPP 13020 *HIPAA Compliance*