
ACCESS CONTROL

Purpose:

To establish University policy regarding access control to the campus.

Scope:

Applies to all points of access to the university campus.

Responsible Party:

Finance and Administration, 426-1200

POLICY

I. Policy Statement

The university will control access to its facilities in an effort to accomplish the following goals: (1) promote and maintain the safety and security of university students, staff, and visitors; (2) protect university property; (3) secure university records; and (4) protect the integrity of university research projects.

II. General Guidelines

- A. Ownership of Keys and Access Codes: All keys and access cards issued under this policy are the property of Boise State University.
- B. Responsibility for Access Control: The Vice President for Finance and Administration has overall responsibility for the granting of access to university facilities, issuance of all keys and access cards, and the delegation of related duties.
- C. Administration of Access Control Systems: The Facilities Operations and Maintenance Department (FO&M) is responsible for overall administration of key and card access systems for all university facilities, except those operated by Student Housing. Student Housing will be responsible for administering the key control for buildings they operate.
- D. Installation and Modification of Doors and Locking Devices: All installations or modifications of doors or locking devices in university facilities must be approved by the FO&M Department or Student

Housing, whichever has jurisdiction. Any individuals or departments found to have violated this policy will be responsible for all expenses incurred to rectify the condition.

III. Key Guidelines

A. Facilities Operations and Maintenance Responsibilities: The FO&M Department will be responsible for the following:

1. Installation and maintenance of all interior and exterior door locks;
2. Cutting and issuance of door keys;
3. Maintenance of accurate records and controls to provide accountability for all keys issued; and
4. Establishment of procedures to govern the issuance and control of keys.

B. Department Responsibilities: Each university department is responsible for designating a key coordinator who will be in charge of key control for that area. This individual will be responsible for the following:

1. Requesting keys from FO&M for department members;
2. Collecting keys from individuals upon their departure from the university, transfer to another department, or when a key is no longer needed;
3. Notifying FO&M when keys are transferred between members of the department so the university records can be updated;
4. Immediately reporting any lost keys;
5. Securing and accounting for any inventory of keys issued to the department for temporary use by students or other authorized individuals; and
6. Responding to periodic key audits by FO&M.

C. Individual Responsibilities:

1. University keys are provided for the exclusive use of the individual they are issued to and may only be used in their official capacity at the university.

2. All keys must be returned to the departmental key coordinator or the FO&M Department when changing departments or upon termination or departure from the university
- D. Duplication: Reproduction of university keys by anyone other than the Facilities Operations and Maintenance Department or Student Housing is prohibited.
- E. Master Keys: Grand master keys will be issued only when a compelling need is established, approved in writing by a Vice President or the President, and authorized by the Executive Director of Facilities Administration. Building or department master keys will be issued with written approval of the appropriate Dean, Director, or Department Head. The Director of FO&M will approve any master keys issued to university service personnel.
1. Keys to communication rooms will only be issued upon approval from the Executive Director of the Office of Information Technology.
 2. The Director of FO&M or their designee must authorize keys to electrical and mechanical rooms.
 3. Rooms will not be keyed off the university master key system unless recommended by the Director of Campus Security to address a serious life safety or security concern.

IV. Electronic Locking Systems

- A. Administration of Campus Wide Card Access System: The campus wide access control system will be administered and maintained by the Facilities Operations and Maintenance Department. The responsibilities of administration include:
1. Computer system maintenance including hardware and software updates;
 2. Coordination of new installations or upgrades;
 3. Delegating authority to grant access privileges;
 4. Maintenance of accurate controls and records to provide overall accountability for an individual authorized for access;
 5. Programming authorized access into the system; and

6. Deactivating cards upon notification of loss, theft, termination, or change in status.

B. Granting Access Privileges:

1. The FO&M Department will have primary responsibility for granting access to campus buildings other than those operated by Student Housing. This access will only be granted upon receipt of written authorization from the appropriate director or department chair.
2. Individual departments and facilities may also designate someone in their organization to grant access privileges to areas within their control and responsibility. In most cases, this individual will also be the key coordinator for the department. The Director of University Security will grant this authority at the written request of the appropriate Dean, Director, or Vice President.
3. The Director of University Security may terminate any or all access privileges he or she deems necessary to address a serious security concern.

C. Issuance of Cards: The issuance of cards to be used with the access control system will be responsibility of the Campus ID Office. These responsibilities include:

1. Issuing campus ID cards with proximity reader capability to eligible individuals and inputting this information on the card access database; and
2. Developing procedures related to the issuance of these cards.

D. Control of Information in Card Access Database: Information in the card access database is considered confidential and will be restricted to authorized individuals. Only the Director of University Security and the system administrator will have the rights to generate usage reports from this database.