SUBJECT: KEY AND OTHER ACCESS DEVICE CONTROLS - Procedures

1. General Conditions

All University space will be secured by locks and access systems under the University Master Lock System or other approved systems as administered by the Facilities Department. Every department will have its own master designation. This master designation will be determined by the building that houses the majority of the department or group's space.

General Space Keying Guidelines

Offices-Every office will be keyed to the master designated for that department, regardless of office location.

Communication and Server Rooms - Will all be keyed alike under the ITS department master.

Computer Labs (student and teaching) - Will be keyed differently under the ITS department master.

Computer Labs (departmental e.g. Computer Science) - Will be keyed under that department's master.

Research Labs - Will be keyed under that department's master.

Teaching Labs (restricted for the exclusive use of one department, e.g. Medical) - Will be keyed under that department's master.

Video Conference and AV Rooms - Will be keyed alike under the ITS department master.

Classrooms (restricted for the exclusive use of one department, e.g. Medical) - Will be keyed under that department's master.

Building stairwells, Common Area doors that are used by more than one department, and exterior doors (with the exception of Agora) - Will be keyed alike under that building's designated master.

Areas with separate master under the Q grandmaster

1) Mechanical and Electrical Rooms - Will be keyed alike under the Facilities Department master only.

2) Janitor Closets - Will be keyed alike under the Janitorial department master.

3) Agora Stairwells, Common Area Doors used by more than one department, and Exterior Doors Entrance Doors - Will be keyed alike.

4) Classrooms, Lecture Theatres, Teaching Labs, Meeting Rooms and Conference Spaces that are used by more than one department will be keyed individually under the appropriate master.

5) Elevator Rooms - Will be keyed alike under the Facilities Department master only.

A separate restricted key system will be used in areas that cannot fall under the University master system. (See Locks Removed from the Master System)

Requests for keys for other office items such as desks, cupboards, file cabinets etc. will be made through the Facilities department, but are not tracked in the Access Device Records. These keys do not require Access Device Request Forms, but can be made through Livetime.

2. Emergency Access

In emergency situations (generally, an "emergency" is a situation in which a person locks his or her home or vehicle keys in an office, and has no other way to retrieve them), UNBC Security may assist entry once proper identification has been produced. Other access requests may be approved by the officer in charge, according the Security Standing Operating Procedures.

3. Issuance of Access Devices to Outside Vendors

Access devices will not be issued to outside vendors. Those vendors needing access to university space will be able to sign out appropriate devices from UNBC Security, providing that permission has been given in writing (via a Work Permit), in advance for the area(s) in question.

4. Requests for Access Devices, Lock Changes, or Lock Maintenance

To make a request for an access device, use an *Access Device Request Form* available on line at ________.

Upon receipt of completed request form, the order will be filled and the requestor will be notified that the access device can be picked up in the Facilities Department. If the device is not picked up within 30 days, it will be returned to the lock shop and the request becomes null and void.

Appropriate identification (UNBC ID Card) must be presented at the time of pick up.

By signing the receipt of issuance the key holder is regulated by this policy for the use and care of a University access device.

5. Lost / Loaned Access Devices

Key holders are responsible for reporting lost access devices immediately to the Facilities Department and the Department of Risk Management.

In the event that it is necessary to re-establish security by re-keying an area, the cost will be charged to the Department concerned. The decision whether or not to re-key an area due to a loss of security will be made by the Director of Risk Management.

The loaning of Access Devices is Strictly Prohibited.

6. New Access Devices for transferring Employees

In cases of employee transfer or termination, management is responsible for the recovery of issued access devices from that employee; their return to UNBC Facilities Department; ensuring the deactivation of electronic access control devices; and ensuring that lock combinations (numerical) are changed.

Employees transferring from one department to another shall return and account for all access devices issued for the former department prior to receiving access device for the new department. In cases where an employee is moving from one space to another within a department all access devices that are no longer needed on a continuing basis must be returned to the Facilities department accompanied by a Key Return Form at www. ___________.

7. Hiring, Promotion, Transfer, or Termination

Human Resources is responsible for notifying the Facilities Department whenever there is an employee hire, transfer, or termination.

8. Unreturned Access Devices

The Authorizing Authority is responsible for ensuring access device are returned from an employee leaving the University. When an employee terminates employment from the University and fails to return Access devices, the authorizing department must attempt to recover them by whatever means available. Should attempts fail, the access device(s) will be declared lost and the responsible department will be assessed a lost key and/or re-key charge. Upon termination, all access devices must be returned to the Facilities Department, along with an Exiting Employee Summary (obtained from Human Resources) that will be signed by a Facilities Assistant (or other Facilities representative) before final check/pay will be issued.

9. Departmental Sign Out Access Devices

Departments can request sign out access devices for use within their designated space. The sign out records for these access devices are to be administered by the authorizing authority for that department or their designate, and are to be available for examination by the Facilities or Risk Management Departments if deemed necessary. The responsibility for these access devices falls on the authorizing authority who signed for them in the same manner as if they were issued to that person. Such uses for these access devices would be for visiting faculty who only need access to the space for a short term, or to be signed out by department members who only needs access to a space on a limited or rotating basis.

10. Non Functional Access Devices

Any device which fails to open doors for which it is cut or programmed must be returned to the Facilities department immediately.

If the fault is due to regular wear and tear, the Access Device will be replaced at no cost.

11. Locks Removed from the Master System

To remove a space from the Primary Master System, the appropriate Dean or Director will forward a letter to the Director of Facilities documenting the need for removal from the Primary Master System. The decision to allow an area to be removed from the University Primary Master System will be made by the Director of Facilities Management and/or the Chief Financial Officer.

Mandated by law or High Risk Areas

Removal of University space from the primary master system may be approved where removal is mandated by law or high risk areas. This includes spaces as follows: pharmacies or drug storage, volatile storage, radiology storage, physical plant, vaults where money or valuables are stored, locksmith room, areas that may create a safety risk, areas that and area where contagious disease experiments are conducted.

These locks may be operated only by the operating key and the control key. Master Keys will not open them.

The spaces, although removed from the Primary Master System, will be accessible by Security and the Facilities Department in the event of an emergency. Some examples of these types of areas are the bookstore/cornerstore, the warehouse, and the mechanical bypass key for electronic access control.

Duplicates of all keys not on the master system will be kept in a lockbox at security and in the locksmith room along with appropriate sign out and safety procedures.

12. Access Device Identification and Marking

Keys should be marked by Lock Label and ID number only.

Caution: In no instance may access devices be identified by stamping, marking, labeling or tagging them with cut codes, room numbers, or other personal identification. For more information, contact the Locksmith.

13. Periodic Inspections

It is recommended that departments conduct yearly access control audits in their areas. The Facilities Management Department, in conjunction with the Risk Management Department, may conduct an access control audit on your unit at any time to determine if any loss of security has occurred.

14. Access Approval

Deans, Directors, and authorized delegates may approve key requests for employees within their jurisdictions. The responsibility for the use of issued access devices is the responsibility of the key holder AND the unit head authorizing the issue of the device.

Approving authorities can obtain an Access Device Approving Authority form (ADAA form) from the Facilities Department, and on it designate who can approve access device requests for different areas that fall under their jurisdiction. It is the department heads responsibility to notify the Facilities department of any changes in approving authority, by way of the aforementioned form.

All requests must have "one up" approval.