

PROCEDURE

Effective Date: Approved August 1, 2005

Approved By: President's Council

Authority: RCW

Cancels: See Also: POL-5351.10 Maintaining Physical Control Over Cash
 PRO-U5351.10A Maintaining Backup Keys and Combinations Within a Department

PRO-U5351.10B MAINTAINING BACKUP KEYS AND COMBINATIONS IN A CENTRAL FACILITY

NOTE: University Policy #U5351.10 requires a backup key for each Custodian's locking cash handling storage device to be kept under dual control. Backup keys to a Custodian's storage device may be accessed by that Custodian, in the event the Custodian loses or misplaces the original key. Any other access to backup keys requires the action of two individuals. This procedure provides a detail of actions required to restrict and document access to backup keys held in a central facility.

Action by:**Action:**

Financial Manager

1. **Obtains** permission to store backup keys from central facility manager.
2. **Acquires** single locking device (locking bag or box or pre-numbered tamper-proof plastic bag) to hold the backup keys/combinations.
3. **Records** the following information on a Backup Key Authorization List:
 - Description (e.g. key #) of key(s) stored and Custodian of each key (can access backup key without another individual).
 - Other individuals authorized to access backup keys (access requires presence and signature of two individuals).
4. **Creates** an Access Log with the following information to document all access to the backup keys/combinations:
 - Date backup key is accessed
 - Description (e.g. key #) of key being accessed
 - Bag #, if tamper-proof plastic bags are used
 - Signature(s) of employee(s) accessing the key
 - Date/Signature(s) employee(s) returning the key
5. **Writes** tamper-proof bag # on log if applicable.
6. **Delivers** Backup Key Authorization List, Access Log and single locking device containing backup key to manager of central facility.
7. **Gives** permission to store backup keys to Financial Manager and **stores** backup keys in locking device in facility.
8. When employee(s) request access to backup keys:
 - **Verifies** that employee(s) are on department authorized list;
 - **Ensures** access log is completed (with signature of Custodian or two other authorized individuals);
 - **Releases** key;
 - **Notifies** Financial Manager that backup key has been accessed.

Manager of Central Facility

Financial Manager

9. **Ensures** that backup keys are replaced and access log is completed.