

UTAH STATE UNIVERSITY

ACCESS CONTROL POLICY

21 JAN 2011

(Last Update)

TABLE OF CONTENTS

I.	ACCESS TECHNICAL GROUP MEMBERS	3
II.	INTRODUCTION	4
III.	ACCESS DEFINITIONS	4
IV.	ACCESS APPROVAL	5
V.	ACCESS CONTROL REQUEST FORM.....	6
VI.	SIGNATURE CARD	6
VII.	OBTAINING ACCESS	6
VIII.	PICK UP KEYS/ACCESS CARDS	6
IX.	ACCESS TRANSFERS	6
X.	ACCESS DISPERSALS	7
XI.	BROKEN/WORN OUT KEYS OR ACCESS CARDS	7
XII.	TEMPORARY ACCESS.....	8
XIII.	DUPLICATING ACCESS AND CHANGING LOCKS.....	8
XIV.	RETURNING KEYS/ACCESS CARDS	9
XV.	LOST/STOLEN KEYS OR ACCESS CARDS/FEES	9
XVI.	ACCESS CONTROL RECORDS/INVENTORY LISTS ..	10
XVII.	ACCESS CONTROL	11

I. ACCESS TECHNICAL GROUP MEMBERS

Steve Mecham	Director, Chief of Police steve.mecham@usu.edu
Stanley Kane	Director of Operations & Maintenance stanley.kane@usu.edu
Ben Berrett	Director, Design & Construction ben.berrett@usu.edu
Curtis Leishman	Locksmith CRL curtis.leishman@usu.edu
Kirk Lukenbill	Locksmith CRL kirk.lukenbill@usu.edu
Russ Moore	Foreman Structures Shop russ.moore@usu.edu
Wade Nield	Specialist, Support Services wade.nield@usu.edu
Linda Hudson	Supervisor Customer Service linda.hudson@usu.edu
Dave Petersen	Manager Facilities Operations dave.petersen@usu.edu
Howard Bee	Foreman Electrical Shop howard.bee@usu.edu

UTAH STATE UNIVERSITY ACCESS CONTROL POLICY

II. INTRODUCTION

The objective of the access control policy is to provide a reasonable level of security for the University and, at the same time, allow as much freedom of access as possible to the campus community.

III. ACCESS DEFINITIONS

- A. Building Master Access Control. Allows access to all rooms within a single building excluding mechanical, communication, electrical, and custodial rooms.
- B. Department Master Access. Allows access to all rooms within an individual department.
- C. Group Master Access. Allows access to limited subgroup areas within a single department.
- D. Outside Door Access. Allows access to a specific building from a specific outside door.
- E. Individual Access. Allows access to a single room.
- F. Mechanical Access. Allows access to mechanical areas, roofs, and outside entrances to buildings for service people.
- G. Custodial Access. Allows access to Custodial closets and designated outside doors.
- H. Communication Access. Allows access to Communication closets.
- I. Electrical Access. Allows access to Electrical Vaults and closets.
- J. Utility Master Access. Any key or access that includes Communication Closets, Machine Rooms, Custodial Areas, and Electrical Vaults.
- K. Prox Card Access. Allows access to any building or room having an I-Class reader.

IV. ACCESS APPROVAL

Requests for access are approved as outlined below. A Dean, Vice President, or Director may designate someone from his/her area to approve the request and sign for access.

<u>Access Type</u>	<u>Authority</u>
Building Master Access	Dean, Vice President, Non-Academic Director responsible for the building, and Chief of Police
Department Master Access	Department Head, Director, and Chief of Police
Group Master Access	Department Head or Director
Outside Door Access	Department Head or Director
Individual Access	Department Head or Director
Mechanical Access	Director of Facilities Operations and Chief of Police
Communication Access	Director of Communication
Electrical Access	Director of Facilities Operations
Custodial Access	Director of Facilities Maintenance
Utility Master Access	Director of Facilities Operations, Director of Communication, Director of Facilities Maintenance, Associate Vice President Facilities and Chief of Police

NO INDIVIDUAL MAY SIGN THEIR OWN ACCESS REQUEST.

Individuals denied access by the Access Control Office may appeal, in writing, to the Access Technical Group if the request is believed to be unjustly denied. The Access Technical Group will then determine if circumstances warrant the issuance of access to the appealing party.

V. ACCESS CONTROL REQUEST FORM

Access to buildings, rooms, and closets are issued by the Access Control Office only when a completed Access Control Request Form is signed by the authorized parties. The Access Control Request Form is valid for thirty (30) days following the date of authorization. Access Control Request Forms can be obtained from the Central Distribution Center.

VI. SIGNATURE CARD

Each Dean, Vice President, Department Head, Director, or their designee who authorizes and signs the Access Control Request Form must have a signature card on file with the Access Control Office. The card must be approved by the Dean, Vice President, or Director responsible for the area. The signature cards must be signed at the Access Control Office. A valid photo ID will be required from the person signing the signature card.

VII. OBTAINING ACCESS

The department who requests access for an employee must submit a completed Access Control Request Form to the Access Control Office. The department retains the pink copy. The Access Control Office retains the white copy for its records. The yellow copy will be returned to the department who authorized the keys and Access Cards when the key or Access Card is ready to be picked up.

Access Cards and keys cannot be obtained through the mail. They must be issued at the Access Control Office to the individual who requested access. Proper identification will be required to pick up keys/Access Cards.

Generally students may not have master keys or master access issued to them.

VIII. PICK UP KEYS/ACCESS CARDS

After the Facilities lock shop prepares a key or access card, it is the responsibility of the college or department to ensure that the individual employee or student picks up the key or access card. For keys or access cards not claimed within thirty days, colleges or departments will be billed for each key or card that has not been picked up.

IX. ACCESS TRANSFERS

All keys or Access Cards must be checked out and in to the Access Control Office by the person to whom they are issued. The transfer of keys directly from one person to

another must be completed at the Access Control Office. Access Cards may not be transferred from one individual to another.

X. ACCESS DISPERSALS

Each college/department determines access that may be issued to its personnel. Full-time employees, students and part-time employees may not have more than one key/card to the same area.

Employees may not check out keys or Access Cards to disperse to students or part-time employees. Individuals must obtain their own access through the Access Control Office.

Students and part-time employees who are issued keys will be assessed a \$25.00 deposit. A deposit of \$5.00 will be required on Access Cards. The deposit will be refunded when the key(s) or Access Card is returned.

If a college/department desires to control the keys or Access Cards to its own area, a request must be made in writing to the Access Technical Group. The request must state the reason the college/department needs to control its own keys or Access Cards. Such requests are discouraged but may be approved by the Access Technical Group under extenuating circumstances.

If approval is granted, the college/department must check out all keys or Access Cards at the Access Control Office so that a current access list detailing the keys or Access Cards checked out to the college/department may be maintained. The college/department will be responsible for the return of all keys or Access Cards and for the collection of lost or stolen replacement fees. The college or department will be responsible for the cost of re-keying or replacing cards due to lost items and must maintain the established record system. A current list of those who have been issued access must be maintained by the college/department. Access reports must be submitted bi-annually or approval may be revoked.

An individual losing a key or an Access Card must inform the Access Control Office within 24 hours of lost or stolen keys or Access Cards.

XI. BROKEN/WORN OUT KEYS OR ACCESS CARDS

Keys or Access Cards that are broken or worn out must be returned to the Access Control Office for replacement by the person to whom they are issued. The broken or worn out keys or Access Cards must be turned in before new ones will be issued. There will be no charge for broken or worn out keys or Access Cards.

XII. TEMPORARY ACCESS

College/department and other personnel requiring temporary access must present an approved Access Control Request Form to the Access Control Office stating the length of time access is required. The Access Control Request Form must be properly completed and approved by the appropriate authority. Temporary keys or Access Cards will not be granted to those who have forgotten or misplaced their keys/Access Cards. They must rely on the University Police to obtain access to the locations that need to be entered.

Under certain circumstances, University access may be granted to outside vendors for service or bidding a project. An Access Request Form must be signed by a Dean, Vice President, or Associate Vice President Facilities, authorizing the issuance of the access. This request must also be approved by the Chief of University Police. Keys will be issued on a temporary basis from the Access Control Office. A \$500 fine will be charged to the department that authorized the request if key/Access Cards are not returned.

Occasionally, a private contractor will be on campus for an extended period of time and will need access to various areas to complete their work. In these situations, Facilities Planning, Design and Construction must complete an Access Request Form requesting the necessary access; approved by the Director of Operations for Facilities. The keys or Access Cards will be issued at the Access Control Office. The contractor will be required to sign a Contractor Key Acknowledgment for the keys or Access Cards to verify they will pay a fine of \$2000 per key that is lost, stolen, or late. All fines will be deducted from contracts pending with Utah State University.

XIII. DUPLICATING ACCESS AND CHANGING LOCKS

State of Utah law prohibits the removal/installation of locking mechanisms or the duplication of any Utah State University key or Access Card by anyone other than the University Access Control Office. USU is using ASSA high security cylinders and keys to increase security and provide excellent access control. ASSA High Security Lock Company holds utility and design patents and will initiate a lawsuit against anyone (individual or company) who duplicates its keys except for its registered agent. The USU Lock Shop is the only registered agent to make keys or Access Cards used by the University. The USU Lock Shop is the only agent to purchase and issue proxcards.

Door locks may only be removed or changed by the University locksmiths. Departments will be responsible for any cost incurred to resolve unauthorized changes.

XIV. RETURNING KEYS/ACCESS CARDS

Before exiting the University or transferring to another department, all students, faculty, and staff must return their University keys and Access Card to the Access Control Office.

Each college/department is responsible for advising all exiting or transferring employees of their obligation to return University keys or Access Cards to the Access Control Office prior to leaving campus. Students and employees who have a deposit on file with the Access Control Office will be given a voucher at the time keys or Access Cards are returned that can be redeemed at the Cashier's Office for the amount of deposit. Vouchers not redeemed within 90 days will forfeit the deposit.

Faculty and staff failing to return keys or Access Cards before transferring to another department or leaving the University may have a hold placed on their next paycheck.

Students failing to return keys or Access Cards before transferring departments, leaving the University, or by the due date listed on the Access Control Request Form will have a hold placed on their transcripts, final paycheck, or registration packets. Deposits are forfeited.

If a hold is placed on a final paycheck, transcripts, or registration packet at the University, it can only be removed by returning keys or Access Cards to the Access Control Office or by paying the appropriate fee listed in Section XIV (Lost or Stolen Access Control) for each uncollected key or Access Card. The intent is to demonstrate that uncollected keys or Access Cards seriously compromise the security of the campus.

If an employee or student leaves the University without returning their key(s) and/or Access Card or paying the appropriate lost key/card fee, their department will be liable for the costs incurred to re-key.

XV. LOST/STOLEN KEYS OR ACCESS CARDS/FEEES

All lost or stolen keys or Access Cards must be reported to the concerned college/department, the Access Control Office and to the University Police. The University Police will complete a Lost or Stolen Access Control Report. Replacement of keys or Access Cards will not be made until the Lost or Stolen Access Control Report is completed.

To replace lost or stolen keys or Access Cards, individuals must complete an Access Control Request Form. In the "List of Requested Access Control" portion of the form, individuals must indicate that the keys or access cards are replacements. The Access Control Request Form must then be approved as outlined in Section IV (Access Approval) and signed by University Police.

A key or Access Card replacement fee will be assessed for all replaced keys or Access Card at the following rates:

<u>Access Type</u>	<u>Replacement Fee</u>
Building Master Access	\$200
Utility Master	\$200
Department Master Access	\$100
Sub Master Access	\$50
Outside Door Access	\$50
Individual Access	\$25
Communication Access	\$50
Electrical Access	\$50
Mechanical Access	\$200
Custodial Access	\$25
Access Card	\$5

The individual to whom the replaced key or Access Card is issued is responsible for payment of the replacement fee.

If an individual's keys or Access Cards have been stolen, that person may appeal the lost or stolen key or Access Card by presenting to the Access Technical Group a police report. If it is determined that negligence on the part of the individual did not contribute to the key or Access Card being stolen, the fee will be waived.

If a Dean, Vice President, Director or Department Head believes that extenuating circumstances justify not charging a replacement fee for a lost key or Access Card, an appeal can be presented in writing to the Access Technical Group to determine whether or not a replacement fee is required.

If keys have been lost or stolen it is critical that those doors affected by the loss of the keys be rekeyed. To rekey a room, the department needs to send a completed work order to Facilities.

XVI. ACCESS CONTROL RECORDS/INVENTORY LISTS

The Access Control Office maintains a complete computerized Access record on each key or Access Card issued. An Access Control Inventory List will be sent to each college/department on an annual basis for reconciliation purposes. This list identifies all the college/department employees who have access rights issued to them. College/department personnel are responsible to verify that the report is accurate. Colleges/departments should maintain a complete and current list that indicates the following: name of key or Access Card holder, key number, date issued, and date to be returned to the Access Control Office. The college/department's access list will

help when reconciling the Access Control Inventory List sent from the Access Control Office. Discrepancies should be reported to the Access Control Office within thirty (30) days. An amended list will be printed and sent back to the department to ensure that changes have been accurately entered on the access record system. Since each person or college/department is financially responsible for all keys or Access Cards issued, accurate information is essential.

If a college/department requires an Access Control Inventory List more often than annually, it is available upon request from the Access Control Office.

XVII. ACCESS CONTROL

Utah State University is in the process of installing a Central Electronic Access Control System in several new buildings on campus. The new system is expected to expand into a campus wide system with buildings coming on line as funds become available. INET is providing the software and all controllers and door hardware will need to be compatible with their system. Stand alone systems such as Omni Lock and Locknetics will no longer be allowed on campus buildings maintained by Facilities. Existing systems will still be maintained at a cost to the Department until updated. Departments will be responsible for costs incurred on Department doors to install and maintain Access Control hardware. However, after installation, Facilities will administer the new system at no cost to the Department.

The Central Access Control System will be controlled and maintained by Facilities with no cost to the individual departments.