1. Access Control Systems Committee

Building/Department Partitioned OperatorsThis user is allowed access to certain areas witl
a building orcomplex, such as a custodial worker assigned to a particular area of campus.

Divisiona (le)-14 (x)]TJ -0.001 Tc 804 Tc(s)-1.3 (u)2 Td ( )Tj 0.00ayf(,)w 3 -TJ 0500ayf(,

e. Verify annually, in consultation with the applicable Vice President, Dean or Chair that those individuals with access control devices remain employed by the University and that their access piTw -39.054 -1.217 Td[(0)6.3 (e)- t58w 64 (ain)12.8 (e)7a(s)-1.41 Tw -0.391 Td[(p)2.2 7a(s)-1.

Facilities Management Department – Security System Technician(s) will assist in providing new

by the Access Control System Administrators. No external contractor service or installations shall occur without an approved funding source.

Emergency Access Control System Administrators serve as designated individuals with authority to make decisions that override the access system, such as the Chief of USA Police and the Director of Information Technology Services. [Refer to the Lockdown Standard Operating Procedures.]

Contractors, Guests, Vendors, Volunteers (Temporary Access Control Devices)

Issuance and recovery of temporary access control devices shall be in accordance with this policy and procedure. Access control device expirations shall correspond to the University's needs for individual's access privileges, as determined by the department issuing the access control device but may not exceed 12 months without Administrator approval. Example: Aramark.

Responsibilities of All Users

Security Measures for System Wide Access

Although all access control devices require care, those assigned system wide access must take extra security measures to secure the device when not in use. System wide access control devices must not leave the University campus unless job functions require otherwise. In no circumstance shall system wide access devices be left unattended or in unlocked vehicles.

Expiration

Expiration dates may not be displayed on an access control device, however temporary devices have a pre-established date from the time of issuance. Temporary access control devices, including those for contractors, visitors and others will be set for a time period which corresponds with the need of the user, with a maximum of twelve months. Expiration dates can be extended by DACs by formal request to the Campus Access Control Systems Administrators.

Replacement requests

a. In the event of loss, theft or a defective access control device, the assigned device holder shall notify their DAC. A replacement device may be issued in accordance with the department's procedure and this policy. Individuals with access control devices enabled with other functions will also need to notify each service provider to deactivate the functions.

b. The device holder shall take the replacement access control device to his/her DAC for authorization activation in accordance with the DAC's department procedure. The DAC will activate approved access authorizations for the replacement devices and deactivate the lost/stolen/defective device assignments; annotate his/her records with the change; and notify the DAC of the replacement transaction to ensure associated records remain current.

Changes in Access Requirements due to Change in Status

Departments shall implement procedures to ensure the DAC's are notified when the access requirements for an individual (employee, student, visitor, vendor, contractor, etc.) who has been issued an access control device has changed, such as due to promotions, transfer, separation, or contract expiration.

If the change is due to an individual's transfer to another department:

a. The DAC shall deactivate the department's authorization for access; the new department's DAC may activate the same access control device with the new department's access permissions, as appropriate.

b. If the change is based upon separation from employment, ending a visit to the University for a contractor whose contract/work is expiring, or the conclusion of the necessity for other temporary use, the DACs shall deactivate the department/facility access permissions and primary department DAC shall totally deactivate the access control device. The primary department DAC shall take measures to recover the device from an individual who is separating from/leaving the University and destroy access control devices that have an individual's name and image. A record of the destruction shall be retained.

c. DACs shall deactivate generic, short term access control devices issued to individuals w access permissions are no longer necessary for University purposes or their affiliation ha changed. Changes shall be documented.

Changes to Access Requirements due to Facility Additions or Renovations

Facility additions or renovations that involve access control systems shall be communicated to the Campus Access Control Systems Administrators and applicable DACs. The DAC will notify the affecte DACs, who shall notify their affected access control device holder. The relevant DAC shall update/activate access permissions in keeping with department authorizations and University poli

Personal Emergency Access to Buildings and Rooms

In case of a personal emergency inability of an individual to access his/her access control device, the individual must first contact his/her supervisor, department manager, or department access contro to gain access. If unsuccessful, the individual may contact the University Police Dispatch who will attempt to contact the Security Systems Technician or Locksmith for access. The individual's iden university affiliation, and access authorization shall be verified prior to granting access.

Restricted Access Areas

Departments with restricted/high risk areas that require additional access controls, such as specia labs, shall develop written procedures for controlling access to their restricted areas, in consultation with the applicable DAC, Campus Access Control System Administrators and other university officia necessary. The procedures shall include:

a. Eligibility requirements for access
b. How to request access
c. Who has authority to approve access
d. Who issues the access control device
e. Who maintains and secures the access control records and unassigned devices
f. How will access control devices be recovered when required
g. Other considerations, as appropriate

Unauthorized locks or access control components will be replaced at the expense of the departm and/or college