**Procedure: Campus Access Control Management**

Authority for Procedure granted by UWG #7009 Access Control and Security Systems Administration.

A. Background

An essential security element is maintaining adequate Access Control so that University Facilities may only be accessible by Authorized Persons. Issuance of Access Credentials shall be diligent, systematic, and audited, as inadequately controlled access devices result in poor security and risk to life, health, and property. Each Unit shall adopt and implement this procedure and follow the Access Control Standards relating to electronic access and the issuance of physical keys, access cards and codes, and biometric credentials for access to University Facilities. All employees and Units within the scope of this procedure are responsible for compliance to ensure the safety of the University Community and the protection of University property and resources.

B. Purpose

This procedure regulates access to University of West Georgia (UWG) Facilities and premises. It ensures that any individual, Unit, or Affiliate within the scope of this procedure is aware of their respective responsibilities when assigned Access Credentials. This procedure will help provide a safe and secure campus environment through the management of Access Control Systems and credentials.

UWG’s commitment to maintaining a safe and secure campus is demonstrated through the following:

1. Establishing procedures and guidelines for managing Access Control for all University Facilities.
2. Achieving maximum security while maintaining reasonable usability of University Facilities by Authorized Persons.
4. Maintaining a recorded chain of accountability for all credentials issued.

C. Responsibilities

The **Chief of the University Police Department (CUPD)** is responsible for authorization and delegation of authority in accordance with these procedures.

**Department Heads (DH)** (Including VPs, AVPs, Deans, Department Chairs, and Directors) are responsible for authorizing the issue of any keys or access cards for the facilities allocated to their Unit based on the Access Level required.

**Information Technology Services (ITS)** is responsible for providing technical application support and performance monitoring for access control applications. ITS will provide hardware and configuration support for all infrastructure devices beyond the end-point devices (e.g., servers and network devices).

**Departmental Access Coordinators (DAC)** within each Unit are responsible for determining whether all persons requesting access keys or cards to their Unit spaces have an operational requirement. DACs ensure that all access keys and cards are recovered when the Key Holder leaves the University, changes Units, or is no longer authorized to enter the facility/space.

**Delegated Authorities** the CUPD may assign Delegated Authority for access control to a Unit that demonstrates a plan, procedures, personnel, training, and resources to independently manage access to specific facilities at delegated **Access Control Levels**. Delegated Authorities must administer their
programs in full compliance with University Access Control policies, operational standards, and procedures.

**Keyholders** Keys/cards to University spaces issued to individuals remain the property of the University. Upon receipt of a key/card, the individual key/cardholder agrees

1. to the proper use and care of the key/card;
2. not to loan, duplicate or use the key/card in any unauthorized manner;
3. to return it to the issuing authority upon demand and/or when no longer required for operational reasons.

**NOTE:** Master Keys shall be secured (behind a minimum of two locks) after assigned working hours. Master Keys shall NOT leave the UWG campus and shall be returned to Access Control upon demand or when no longer required for operational reasons.

**UWG Community members** must refrain from installing unauthorized locking devices on University doors. No doors may be secured except by a locking device approved and/or installed by the University to ensure access in an emergency.

**D. Prohibited Actions**

The following actions are prohibited by UWG employees, students, or Affiliates under this procedure and may result in disciplinary action or loss of access privileges:

1. Loaning keys or other Access Credentials.
2. Transfer of keys without authorization.
3. Unauthorized sharing or possession of access control data or files.
4. Unauthorized mailing of keys or access cards.
5. Unauthorized duplication of keys or other Access Credentials, including cloning of another Faculty, Staff, or Student ID Card or access card.
6. Using a key or Access Credential for non-University business without prior authorization.
7. Altering, bypassing, or defeating keys, locks, or mechanisms.
8. Propping doors open without authorization.
10. Damaging, tampering with, or vandalizing University locks and/or hardware.
11. Admitting unauthorized person(s) into the building.
12. Failure to return a key when requested by Access Control, UPD, the issuing department, or upon leaving the employment of the University.
13. Failure to report lost or missing key(s) or other Access Credential(s).

Violations of this procedure may result in additional costs to the Unit and/or Affiliate. Employees may be subject to disciplinary action by the Office of Human Resources per the Employee Handbook.

Students violating this procedure are subject to revocation of access and/or additional action by the Office of Community Standards in accordance with the Code of Conduct.

**E. Access Levels**

Access (i.e., a key, access card, biometric data, or access code) is granted based on the lowest Access Level that will accomplish the operational purpose. Each Access Level is associated with rules of issuance and approval levels. See [Access Control and Authorization Requirements](#).

**F. Financial Accountability**
Units may be financially responsible for costs associated with the installation, upgrades, repair, and maintenance of Access Control Systems in spaces controlled by the Unit. In the event of lost or stolen keys, Affiliates and Units may be financially responsible for costs associated with re-keying.

G. Access Control Standards

**Key and Lock System:** University keying systems shall be approved and administered by the University Police Department (UPD). Installation of unauthorized keying systems on UWG spaces (including but not limited to interior/exterior containers, cold storage, and lockable office systems with demountable partitions) is prohibited.

**Electronic Access System:** card Access Control Systems must be approved and administered by Access Control.

**Secure Asset Management (SAM) Boxes:** Access Control shall review and approve/deny any deviation from the use of this asset box system.

1. To Request Access Credentials

Access Credentials must be approved by the appropriate authority(ies) prior to issue. Individuals will be issued key/access cards at the minimum required access level to provide operational support.

Requests for Access Credentials (key/access cards) shall be submitted to the Access Control Office using the [Key Request form.](#)

Key Holders must sign a Key Agreement Form before issuing keys. *This form is generated by the Access Control key tracking system and shared electronically.*

2. Return and Revocation of Access Credentials

All keys/access cards are the property of the University and must be returned upon transfer or separation of employment. The manager/Unit shall not retain keys for use with a replacement employee. Obsolete or unneeded keys must be returned to the Lock Shop for disposal.

**Changes In Employee Status** Upon separation (i.e., retirement, resignation, transfer, or termination) of employment, the employee’s manager is responsible for ensuring the employee’s key/access card is returned to Access Control.

Units should retain keys to desks, file cabinets, etc., for reissue. Before an employee’s departure, the Departmental Access Coordinator should contact Access Control to confirm a list of keys issued to the employee. For employees having any electronic access on or before the last day of employment, the manager shall notify the Access Control Manager or designee via email ([access@westga.edu](mailto:access@westga.edu)) to terminate the individual's electronic access.

**Suspension and/or Revocation** Card Access and Keys may be suspended or revoked by CUPD or Vice Presidents of the respective Units for repeated and/or serious violations of Access Control policy and procedures. In such cases, the official suspending or revoking access shall prepare a justification and submit a written notice to the employee and the Department Head.

Suspension or Revocation is an administrative action to secure University Facilities and is not a disciplinary action. Such action is subject to due process and appeals to the next level of authority.

3 Lost, Stolen, or Missing Access Credentials

Loss of a key/access card can result in a financial loss to the University and expose the University Community to unnecessary risk.
Report lost, stolen, or missing key/access cards to each of the following within two hours of the loss being discovered or immediately upon the start of the next working shift if discovered while off duty:

i. University Police Department Dispatch Center at 678-839-6000,
ii. Access Control at 678-839-3101, 678-839-3805, or access@westga.edu, and
iii. notify the Department Head.

Failure to report lost or stolen keys may subject
- the employee to disciplinary action in accordance with the UWG Employee Handbook,
- Students to disciplinary action by the Office of Community Standards in accordance with the Code of Conduct.

Approvers of the original lost, stolen, or missing key(s) shall be notified of the loss within 48 hours.

H. Installation and Maintenance

UPD is the authorized agent for installation, maintenance, and control of all locks and keys/access cards, including periodic replacement and upgrading to maintain security for University Facilities. This responsibility includes maintaining keys/access cards, records, and cores and designing lock systems.

1. Key and Core Changes

Locks may be rekeyed to reestablish security. Following a risk assessment, the CUPD or their designee may require rekeying of spaces impacted by lost, stolen, or missing keys. Requests for rekeying may be initiated by the applicable Division VP, AVP/Dean, or Department Head. Approved requests should be sent via email to Access Control at access@westga.edu. In the event a Key Holder loses a key or fails to return a key to Access Control, the Key Holder's Unit may be charged, in part or entirely, for the cost of rekeying to reestablish security in the affected area(s).

Units requesting core and/or key changes to meet programmatic or re-organizational needs will be charged all costs associated with the requested scope of work.

2. Access Control and Locks

Installation of non-authorized key/Access Control Systems on University Facilities is subject to corrective action, removal, and/or replacement.

Facilities Development and Sustainability (FD&S) will fund the service and maintenance of all perimeter mechanical locking and door hardware in Educational and General spaces.

UPD will fund the service and maintenance of SAM boxes.

Housing and Residence Life (HRL) will fund the service and maintenance of all perimeter mechanical locking and door hardware in UWG HRL facilities.

Auxiliary Units may be charged for labor, materials, and maintenance of mechanical locking and door hardware, including electronic Access Control Systems, in buildings and areas under the control of the Auxiliary Enterprises.

Units will fund the installation, service, and maintenance of electronic Access Control Systems within the Unit’s controlled spaces.

I. Building Perimeter Door Security
1. **Operating Hours**: Building Operating Hours are scheduled by Access Control or the respective Delegated Authority in consultation with UPD. Building Operating Hours may be changed upon written notification to the Access Control Office or the respective Delegated Authority by the Vice President, AVP, or Dean(s) with the jurisdiction of the building or their delegated person. Routine changes in building operating hours related to special events are approved through the [ReserveWest system](#).

2. **Building Closure**: Building closure or lockdown due to inclement weather, University closure, or other emergencies may be approved by the President, Chief of Police, or their designee. The Vice President or Director of Housing may authorize the closure of residential buildings.

3. **Perimeter Access Control**: UPD is the authorized agent for installing, maintaining, and controlling all building perimeter mechanical locking and door hardware, Access Control Systems, and devices at UWG. HRL has Delegated Authority to control access for residential building perimeter door Access Control Systems.

4. **University Employees**: Faculty and staff requiring building access during periods when the building is secured should email access@westga.edu and their supervisor. The employee's supervisor and Department Head or Departmental Access Coordinator may approve/deny the access request. Access Control will reprogram the electronic lock generally within three business days of receipt of the request.

5. **Non-University Employees**: Other individuals (i.e., volunteers, international students, visiting faculty, contractors, vendors, etc.) may request building access during periods when the building is secured. The responsible UWG Employee, such as the University Project Manager/Maintenance Supervisor, are required to complete the [Contractor/Vendor Request Form](#). Forms may be emailed to Access Control at access@westga.edu.

6. **Students**: Students may be granted building access to exterior and/or interior doors during secured building periods, as applicable. The responsible Department Access Coordinator (DAC) must complete the Student Access Request Worksheet (DAC may request access to the Student Access Request Worksheet by emailing access@westga.edu). Student access will be automatically terminated at the end of each semester if no end date is given.

7. **Unlock Requests**: UPD is the authorized agent for after-hours unlock requests, subject to the availability of officers and verified identification and authorization of the requestor. To request after-hours unlocks, call (678) 839-6000.

---

**J. Unauthorized Access**

1. All Access Credentials remain the property of UWG.

2. No person shall gain access to University Facilities using an Access Credential not authorized for their use. Any person using a lost or stolen Access Credential to gain access to University Facilities may be subject to disciplinary action or criminal prosecution.

3. Access Credentials are authorized only for state business. No employee shall use an Access Credential to gain access to University Facilities for personal use or access. Such use may subject the employee to disciplinary action and/or criminal prosecution.

4. Access Control shall periodically monitor and audit electronic access and report unauthorized access to CUPD for investigation and/or corrective actions or recommendations.

---

**K. Access Control Systems Administration**

1. Access Control serves as the central authority for administering Access Control Systems.
2. Changes to permissions within Access Control software, including Delegated Authorities, shall be approved on a case-by-case basis by Access Control using the End-User Agreement form.

3. Delegated Authorities shall be provided with limited access to Access Control Systems. Delegated Authorities shall not modify or manipulate hardware and/or software-related programming. Tasks outside the scope of Delegated Authorities shall be coordinated with Access Control.

L. Key Bank Approval and Management

Previously established Key Banks are designated Level 2 access, with required approvals from Department Head, CUPD, and VP/AVP/Dean.

Key Banks are assigned to individual UWG employees responsible for maintaining key inventory, issuance records, periodic reconciliation, and periodic reporting to Access Control.

All Units with existing Key Banks are required to maintain guidelines for the Key Bank. Any changes to Unit guidelines must be submitted to the Access Control Manager and CUPD for review and approval. Guidelines should include the tracking instrument (paper or digital) for check-in and check-out of keys with appropriate controls and records retention.

The Key Bank should be secured to maintain records of individuals having access. (e.g., locked cabinet with electronic access control). Key Bank may be secured in a locked cabinet or file utilizing an approved lock (a digital or paper key issue log shall be recorded and retained).

The Unit must pay all costs associated with maintaining the Key Bank, including replacing keys and cores resulting from lost or missing keys.

M. Emergency Access and Service Ring Management

Emergency Access and Service Rings may be approved for University employees who require broad access to UWG buildings. Access Control shall maintain an inventory of all keys and periodically audit and verify the integrity of each ring. Emergency Access and Service Rings shall be issued and administered through a SAM box following approval at the appropriate Access Level.

**Emergency Access:** Emergency Access rings may be approved for University officials and Emergency Response Personnel who need immediate access to University Facilities in response to incidents threatening human health and safety or UWG premises/property. Emergency Access rings shall remain on campus and secured within a SAM box.

**Service Rings:** Service Rings may be issued to University employees with duties that require access to a broad range of University Facilities. Service Rings shall be requested by the employee’s supervisor and approved at the appropriate Access Level. Service Rings shall be issued daily through a SAM box, shall not be taken off campus, and must be returned at the end of each shift. Loss of a Service Ring, improper use of the Ring, or repeated failure to return keys at the end of each shift subjects the employee to loss of access privileges and disciplinary action.

Override Keys shall only be issued to authorized UPD and Access Control personnel to provide Emergency Services.

N. SAM Box Management and Administration

Access Control is the central authority for administering Secure Asset Management (SAM) boxes, including:
overseeing installation, 
programming of hardware, 
initial hardware acceptance testing, 
troubleshooting hardware, 
software issues when applicable, 
managing system infrastructure, 
record retention, and 
managing system user accounts and permissions.

Access Control shall assign designated key slots for Delegated Authorities to manage access via a system segment. Delegated Authorities shall not have access to key slots designated to UPD, ITS, FD&S, Vendors, and Contractors.

Delegated Authorities shall be provided limited access to the SAM box management web portal. Responsibilities include management of the access to keys, running reports, Lenel OnGuard user integration, user groups, and user PINs within authorized SAM boxes. Delegated Authorities shall not modify configuration system settings, manipulate SAM box configuration, or modify system assets.

O. Access Control Delegated Authority

Delegated Authority is the assignment of limited authority by the CUPD to a Unit that demonstrates that it has a plan, personnel, training, and resources to manage access to University Facilities at delegated Access Levels independently.

The enforcement of Delegated Authority is the responsibility of Access Control and is implemented through the appropriate Unit administrator (including VPs, AVPs, Deans, Department Chairs, and Directors). The administrator's responsibility is to maintain systematic and effective control of all keys/access cards for rooms and/or buildings primarily under the control and jurisdiction of that Unit.

Delegated Authorities are responsible for issuing and tracking keys/access cards, maintaining accurate records, and/or using the access control software to grant and deny access and set time zones for the area in their jurisdiction. Keys/access cards are issued in the strict trust that proper measures will be taken to ensure their safekeeping.

P. Contractor and Vendor Access

Contractors and vendors shall not be issued Master Keys unless approved by the CUPD or their designee. Keys are not issued to subcontractors except for extenuating circumstances or prior arrangements.

**Short-Term Issuance:** refers to the daily issue of a key from an authorized SAM box to persons authorized by the Department Head(s). Short-term keys are issued and returned during the same 24-hour period.

**Long-Term Issuance:** refers to issuing a key to persons authorized by the Department Head(s) for longer than 24 hours. The maximum time of issue is 90 days, at which time the key(s) may reissue. Long-term issuance must be physically audited before reissue.

Recordkeeping

Access Control Files will be maintained for the retention period, as stated in the USG Records Retention Schedules.

Authority to Develop Guidelines
The CUPD or designee may grant or rescind exceptions at any time to this procedure based on a risk assessment or abuse of exceptions granted. In the event of a conflict between a University Policy or Procedure and a divisional/unit-level guideline, the University’s Policy or Procedure will control.

Definitions

**Access Control System** - Any mechanical or electronic device used to secure University Facilities. Access Control Systems include but are not limited to card readers, biometric readers, combination locks, keypads, access control panels, SAM boxes, lock cylinders, padlocks, equipment panel locks, exit devices, vehicle ignition systems, Access Credentials, and the related computer systems, software, and infrastructure.

**Access Control File** - Critical records maintained by UPD Access Control, including key codes, copy numbers, issuance records, Access Control Database, electronic access data, and Unit control access data.

**Access Credential** - Any means or device used to lock, unlock, open, or gain access into a secured area, including but not limited to metal keys, keypad codes, Access Cards and biometrics, RFID (radio frequency identification), NFC (near-field communication), or any combination of devices used to lock, unlock, open, or gain access to a secured area.

**Access Level** - A category within a given security classification limiting entry or system connectivity to only authorized persons. See Section E above.

**Affiliate** - Non-employee members of the UWG community that include but are not limited to: vendors, volunteers, observers, trustees, Foundation Boards and employees, dependents of UWG employees, retirees, emeriti faculty, alums, summer scholars, summer campers, Campus Center members, and tenants (non-UWG staff) renting space in a University Facility. Affiliated Organizations per [BOR Business Procedures Manual, section 17.1](#).

**Authorized Person** - UWG employees, currently enrolled students, and Affiliates possessing a duly issued and valid Access Credential permitting entry into University Facilities.

**Delegated Authority** - Assignment of limited authority to a unit that demonstrates that it has a plan, personnel, training, and resources to manage access to specific University Facilities at Delegated Access Levels independently.

**Department Head** - A person in a unit responsible for appointing a Departmental Access Coordinator and authorizing individual key requests within their specific Unit. This is reserved for VPs, AVPs, Deans, Department Chairs, and Directors.

**Departmental Access Coordinator** - Department Head or their designee appointed to coordinate and/or approve access requests based on Delegated Authority, adherence, and implementation of this procedure.

**Emergency Access** - Access for security, law enforcement, human safety, or urgent facility response or repair purposes.

**Emergency Response Personnel** - Individuals, assigned Access Credentials that allow Emergency Access to a broad number of University Facilities to provide emergency services.

**Key Bank** - A single secured location for the storage of keys by a Unit for short-term issuance to Authorized Persons to meet Unit operational needs.

**Master Keys** - Keys that allow access to a group of rooms or buildings.
Override Keys - Keys that allow override of Access Control Systems, security systems, SAM Boxes, or other security elements.

SAM Box - A Secure Asset Management device used for the storage and automated issuance of Service Rings to an Authorized Person. Access to the SAM Box and Service Rings shall be through an authorized Access Credential administered by Access Control.

Service Ring - Keys issued to an Authorized Person for the duration of their shift or on demand to allow Service Access to provide maintenance, repair, or building care services to spaces that are not occupied and/or controlled by them.

Unit - Any college, department, research center, business service center, auxiliary service center, or office.

University of West Georgia (UWG) Facilities - Any building, room, property, equipment, container, or premises owned, operated, or leased by the University of West Georgia (UWG).

Forms

- Key Request Form
- Contractor/Vendor Request Form
- Credential Return Form