The Chief Facilities Officer, pursuant to the authority of UWG Policy 7.3, establishes the following procedures on Access Control Management.

A. BACKGROUND
An essential element of security is maintaining adequate Access Control so that University Facilities may only be accessed by those persons who are authorized. 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 department 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 Campus Facilities. All units and departments within the scope of this procedure are responsible for compliance to ensure the safety of the University community and the protection of University premises and resources.

B. PURPOSE
The purpose of this Procedure is to regulate access to University of West Georgia (UWG) facilities and premises and to ensure that any individual, college, department, operating unit, program, 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 diligent control of Access Control Systems and credentials.

The University is committed to a safe and secure campus in its operations and practices. This commitment is demonstrated through:

- Establishing procedures and guidelines in managing Access Control for all University Facilities.
- Meeting or exceeding applicable security and access rules, laws, mandates, and best practices.
- Achieving maximum security while maintaining reasonable usability of University Facilities by Authorized Persons.
- Maintaining strict control of the campus Access Control Systems, including approval, distribution, duplication, and monitoring of Access Credentials.
- Maintaining a recorded chain of accountability for all keys issued.
- Restoring physical security in a timely manner should Access Control has been compromised.
- Communicating the institution’s responsibilities and successes publicly and through all levels of leadership.
C. DEFINITIONS

1. **Access Control System** – Any mechanical or electronic device or devices 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.

2. **Access Control File** - Critical records maintained by Facilities Services - Access Control Office, including key codes, key copy numbers, key issuance records, Access Control Database, and electronic access data, as well as departmental control access data.

3. **Access Credential** – Any means or device used to lock, unlock, open, or gain access into a secured area. This includes but is not limited to metal key, combination, keypad code, keypad PIN code, WolfCard, Access Card, magnetic, proximity, biometric, RFID (radio frequency identification), or any combination of devices used to lock, unlock, open, or gain access to a secured area.

4. **Access Level** - The level of authorization required for any given access request, dependent on the lowest “access level” that will accomplish the operational purpose.

5. **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, alumni, summer scholars, summer campers, Campus Center members, and tenants (non-UWG staff) renting space in a University Facility. Affiliated Organizations are defined by BOR Business Procedures Manual, section 17.1.

6. **Authorized Person** – UWG employees, currently enrolled students, and “Affiliates” in possession of a duly issued and valid “Access Credential” permitting entry into “University Facilities”.

7. **Construction Core** - A special temporary core and related keys issued by Access Control to a contractor for the purpose of restricting access to spaces under construction to contractor personnel and UWG emergency personnel.

8. **Delegated Authority** - Assignment of limited authority by the Chief Business Officer to a department or “unit” that demonstrates that it has a plan, personnel, training, and resources to independently manage access to specific facilities at delegated access levels within the requirements of this procedure.

9. **Department Head** - Person in a department/ “unit” responsible for appointing a “Departmental Access Coordinator” and authorizing individual key requests within their specific department. This is reserved to Assistant Vice Presidents (AVP’s), Deans, Directors, or Chairs.

10. **Departmental Access Coordinator** – “Department Head” or other person delegated by the “Department Head” to coordinate and/or approve access requests based on “delegated authority”, adherence, and implementation of this procedure.

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

12. **Emergency Response Personnel** - Individuals assigned “Access Credentials” that allow “Emergency Access” to a broad number of campus facilities for the purpose of providing emergency services.
13. **Key Bank** - A single secured location for the storage of keys by a Department or “Unit” for short term issue to “Authorized Persons” to meet “Unit” operational needs.

14. **Master Keys** - Keys that allow access into a group of rooms or building.

15. **Operator Keys** - Keys that allow access into a single room or a suite of rooms keyed alike.


17. **Residence Hall Room Key** – A key which allows access into a student’s living space in a residence hall room or suite.

18. **SAM Box** - A Security Asset Management device used for the secure storage and automated secure issuance of “Service Rings” to an “Authorized Person” to provide routine operational access, “Service Access”, and “Emergency Access” to “University Facilities”. Access to the “SAM Box” and “Service Rings” shall be through an authorized “Access Credential” administered by the “Access Control Office”.

19. **Service Access** - Access for the purposes of providing maintenance, repair, or building care services.

20. **Service Personnel** - Individuals assigned “Access Credentials” that allow “Service Access” to a broad number of campus facilities for the purpose of providing routine maintenance, repair, and building care services.

21. **Service Ring** - One or more keys issued to an “Authorized Person” for the duration of their shift or on demand to allow “Service Access” to spaces that are not occupied and/or controlled by them. For example, a combination of master, submaster, and “operator keys” to allow a custodian access to all spaces in a building for cleaning.

22. **Unit** - Any college, department, program, research center, business service center, auxiliary service center, office, or other operating unit.

23. **University Facilities** – Any building, room, property, equipment, container, or premises owned, operated, or leased by UWG.

**D. RESPONSIBILITIES**

The **Chief Business Officer (CBO)** is responsible for authorization and delegation of authority for the **Access Control Program (ACP)**.

The **Chief of the University Police Department (CUPD)** is responsible for campus security and public safety. This role includes security of building perimeters, approval of great grand master (level 0) and grand master (level 1) keys and access levels, investigation of access control breaches and lost credentials, intrusion detection and reporting, video surveillance, and lock/unlock requests.

The **Chief Facilities Officer (CFO)** is responsible for developing and implementing policy for the **ACP**. This role approves procedures and guidelines for program administration and ensures that resources are appropriately aligned with program activities and requirements.

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

The Director of Facilities, through the Locksmith Shop is responsible for the selection, installation, maintenance, repair and replacement of door lock cylinders, lock sets cores, keyways, keys, and service rings, with the exception of desks, cabinets etc.

The Director of Facilities, through the Access Control Office (ACO) is also responsible for administration of access management and approval procedures including key requests, electronic access requests, administration of service rings, SAM box management, program reporting, maintaining the Access Control File, and accountability management.

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 that all persons requesting keys or cards to their departmental/unit spaces have a bona fide operational requirement for the key or card. DAC's ensure that all keys and cards are recovered when the key holder leaves the university, changes departments or is no longer authorized to enter the spaces accessed by the keys/cards.

Delegated Authorities: Following an application and review process, the CBO may assign Delegated Authority for access control to a department or unit that demonstrates that it has a plan, procedures, personnel, training, and resources to independently manage access to specific facilities at delegated Access Levels. Delegated Authorities must administer their programs in full compliance with University ACP 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/card holder agrees:
   a) to the proper use and care of the key/card;
   b) to store master keys securely on campus outside of working hours;
   c) not to loan, duplicate or use the key/card in any unauthorized manner;
   d) to return it to the issuing authority upon demand and/or when no longer required for bona fide operational reasons.

All UWG community members are responsible to refrain from installing unauthorized locking devices on university doors. To ensure access in the event of an emergency, no campus area may be secured except by a locking device approved by the University.

E. PROHIBITED ACTIONS
The following actions by UWG employees, students, or Affiliates are prohibited under this procedure and may result in disciplinary action or loss of access privileges. Violations of this procedure may result in additional costs to the department, Unit, or Affiliate and may subject the employee to disciplinary action in accordance with the UWG 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.

- Loaning keys or other **Access Credential**.
- Transfer of keys without authorization.
- Unauthorized sharing or possession of access control data or files.
- Unauthorized mailing of keys or access cards.
- Unauthorized duplication of keys or other **Access Credential**, including cloning or copying of another person’s Faculty, Staff, or Student ID Card or access card.
- Using a key or **Access Credential** for non-university business without prior authorization.
- Altering, bypassing, or defeating keys, locks or mechanisms.
- Propping doors open without authorization.
- Installing unauthorized **Access Control Devices** in **University Facilities**.
- Damaging, tampering or vandalizing any University lock or hardware.
- Admitting **unauthorized person(s)** into the building.
- Failure to return a key when requested by the Access Control Office, UPD, the issuing department, or upon leaving the employment of the University.
- Failure to report lost or missing key(s) or other **Access Credential(s)**.

### F. ACCESS LEVELS

The Access Control Procedure (ACP) is based on the granting of access to **University Facilities** by **Authorized Persons** for specific operational purposes. Access is granted by way of an **Access Credential** in the form of a key, access card, biometric data, or access code. Under this ACP, the level of authorization required for any given access request will be dependent on the lowest **access level** that will accomplish the operational purpose. Each **Access Level** is associated with rules of issuance and approval levels as follows:

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Context</th>
<th>Type of Access</th>
<th>Authorized Users</th>
<th>Approval/Rules of Issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Great-Grandmaster (Campus)</td>
<td>All patented Grandmaster and Great Grandmaster keyways; PEAK masters; High-security masters; All control keys; ALL-ACCESS cards, <strong>Override keys; SAM</strong> bypass keys, rings with multiple legacy grandmasters (GGM, GGMV, GGMT).</td>
<td>Possession of keys off campus or by unauthorized personnel is prohibited. Controlled use only by Locksmith and University Police.</td>
<td>Generally Prohibited. <strong>Emergency Access</strong> only. APPROVAL: CUPD + CFO + CBO + Divisional VP</td>
</tr>
<tr>
<td>1</td>
<td>Grandmaster (Legacy or Zone)</td>
<td>Legacy grandmasters (GGM, GGMV, GGMT), Zone Masters on patented</td>
<td>Possession of keys off campus or by unauthorized</td>
<td><strong>SAM-controlled issue of Level 1 keys is permitted for Service</strong></td>
</tr>
</tbody>
</table>

UWG Procedure 7.3.1 – Access Control Management
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Master (Building)</td>
<td>Building Master keys and cards (including rings); building perimeter keys and cards, Utility Masters; life safety panels and masters; key bank access keys. Rings or Key Banks containing multiple Access Levels within a building.</td>
<td>Possession of keys off campus is prohibited. Not eligible for permanent issue. Pre-authorized access via a SAM-controlled issue only.</td>
<td>SAM-controlled issue of Level 2 keys is permitted for daily operations, Service Rings and Emergency Access. APPROVAL: SUPERVISOR + DH</td>
</tr>
<tr>
<td>3</td>
<td>Submaster (Department)</td>
<td>Departmental submaster, classroom submaster, mechanical room submaster.</td>
<td>Possession of keys off campus is prohibited unless pre-approved at time of issuance. Pre-authorized access via a SAM-controlled issue or authorized Key Bank.</td>
<td>SAM-controlled or Key Bank issue of Level 3 keys is permitted for daily operations, Service Rings and Emergency Access. APPROVAL: SUPERVISOR + DH</td>
</tr>
<tr>
<td>4</td>
<td>Sub-Submaster (Area)</td>
<td>Office suite; Residence Hall room group; lab sub-submaster; classroom sub-submaster; construction core; group of rooms keyed alike (more than 10 but less than 20 cores).</td>
<td>Long term issue permitted. Pre-authorized access via a SAM-controlled issue or authorized Key Bank.</td>
<td>SAM Controlled, Key Bank, or permanent issue. APPROVAL: SUPERVISOR + DH</td>
</tr>
<tr>
<td>5</td>
<td>Operator (Room)</td>
<td>Individual room key or card, or group of rooms keyed alike (10 cores maximum); Padlocks keyed alike</td>
<td>Long term issue permitted. Pre-authorized access via a SAM-controlled issue or authorized Key Bank.</td>
<td>SAM Controlled, Key Bank, or permanent issue. APPROVAL: SUPERVISOR + DH</td>
</tr>
</tbody>
</table>

UWG Procedure 7.3.1 — Access Control Management
G. **FINANCIAL ACCOUNTABILITY**
The CFO shall establish Guidelines governing financial accountability in connection with this Procedure, subject to approval by the CBO. **Units** may be financially responsible for costs associated with the installation, upgrades, repair, and maintenance of electronic **Access Control Systems** in spaces controlled by the **Unit. Affiliates** and **Units** may be financially responsible for costs associated with re-keying in the event of lost or stolen keys.

H. **PROCEDURES**

1. **Access Control Standards**
   a. **KEY AND LOCK SYSTEM**: All campus keying systems shall utilize the Best™ Small Format Interchangeable Core (SFIC) patented keyway system approved and administered by Campus Planning & Facilities (CP&F). The installation of any unauthorized keying systems on any campus space, including but not limited to interior and exterior containers, cold storage, and lockable office systems with demountable partitions, shall be prohibited.
   b. **ELECTRONIC ACCESS SYSTEM**: All campus card **access control system** components must be compatible with Lene OnGuard **Access Control System** and administered by the Access Control Office.
   c. **SAM BOXES**: devices shall be manufactured by Key Systems Inc. and operate via the GFMS software. Any deviation from this box shall be approved by the **Access Control Manager**.

2. **Requesting, approving, and issuing of Access Credentials**
   a. Requests for **Access Credentials** (key and access cards) shall be submitted to the **Access Control Office** using the designated online Access Request and/or Key Request form. Routine requests should be filled within three (3) business days. Urgent requests will be filled as quickly as resources allow.
   b. All **Access Credentials** must be approved by the appropriate authority(ies) indicated in **Section F: Access Levels** above prior to issue.
   c. Individuals shall be issued the least number of key/access cards at the lowest level in the locking system hierarchy that is necessary to provide the required access. Access to Level 1 and Level 2 keys, if approved, will be provided via a **SAM box** as available.
   d. All keyholders must sign a key authorization form (generated by Facilities key tracking system) prior to being issued keys.

3. **Return and Revocation of Access Credentials**
   a. **PROPERTY OF THE UNIVERSITY**: All keys/access cards are the property of the University and must be returned upon transfer or termination of employment. Keys shall not be retained by the manager/department for use with a replacement employee. Obsolete or unneeded keys must be returned to the Lock Shop for disposal.
   b. **CHANGES IN EMPLOYEE STATUS**: Upon the retirement, resignation, transfer, or termination of employment, the employee’s manager is responsible for ensuring that the employee’s keys are returned to the **Access Control Office**. Keys to desks, file cabinets, etc. should be retained by the department for reissue. In advance of any departure, the Manager should contact the **Access Control Office** to confirm a list of keys issued to the employee. If the employee has any electronic access, on or before the last day of employment the manager shall notify the **Access Control Manager** or his/her designee via email to uwg_access_control@westga.edu
have the individual's electronic access authorization terminated.

   c. REVOCATION OF ACCESS: Card Access and/or Keys may be suspended or revoked by the Chief Facilities Officer, Chief of Police, or Vice President 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 employee’s department head. Suspension or Revocation is an administrative action to secure campus facilities, and is not a disciplinary action. Such action is subject to due process and appeal to the next level of authority.

4. Lost, Stolen, or Missing Credentials
   a. Loss of keys/access cards can result in great financial loss to the University and expose University community members to unnecessary risk.
   b. If an individual loses a key/access card or it is stolen, the individual must immediately report this to the University Police Department Dispatch Center at 678-839-6000 and also notify their Department Head and the Access Control Office at 678-839-3101 or 678-839-3805 within 2 hours of the loss being discovered, or immediately upon the start of the next working shift if discovered while off duty. Failure to report lost or missing keys may subject the employee to disciplinary action in accordance with the UWG Employee Handbook.
   c. At the discretion of the CFO, The Department or Unit originally requesting/approving the lost or missing key may be responsible for the cost of changing all key cores impacted by the lost key. This cost will be substantial for higher level keys (Level 0, 1, and 2).
   d. Approvers of the original lost, stolen, or missing key(s) shall be notified of loss within 48 hours.

5. Key and Core Changes
   a. CP&F is responsible for maintenance and service of all locks including periodic replacement and upgrading in order to maintain proper security.
   b. Locks may be rekeyed to reestablish security. Following a risk assessment, the CFO may require rekeying of spaces impacted by lost, stolen, or missing keys.
   c. Requests for rekeying may be initiated by the applicable Division VP, AVP/Dean, or Department Head. Approved requests should be sent via email to the Access Control Manager or his/her designee at uwg_access_control@westga.edu. The cost of rekeying will be borne by the Department that approved the lost or missing key(s). If a key holder loses a key or fails to return a key to the Access Control Manager, the key holder’s Unit may, at the discretion of the appropriate University executive/Division-head, be charged, in part or entirely, for the cost of rekeying to reestablish security in the affected area(s).
   d. Departments 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.

6. Installation and Maintenance of Access Control and Locks
   a. CP&F is the authorized agent for installation, maintenance, and control of all locks and keys/access cards for the University Facilities. This responsibility includes design of lock systems, maintenance of core, keys/access cards and records.
   b. Installation of non-authorized key/access control systems on University facilities is prohibited and is subject to corrective action, removal, and/or replacement at the expense of the unit.
7. Building Perimeter and Exterior Door Security
   a. OPERATING HOURS: Building Operating Hours will be scheduled by the Access Control Office 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 jurisdiction of the building or their delegated person. Routine changes in building operating hours related to special events will be approved through the ReserveWest system.
   b. BUILDING CLOSURE: Building closure or lockdown due to inclement weather, campus closure, or other emergency may be approved by the President, Chief Business Officer, Chief of Police, or Manager of Emergency Operations. Closure of residential buildings may be approved by the Vice President or Director of Housing.
   c. PERIMETER ACCESS CONTROL: CP&F is the authorized agent for installation, maintenance, and control of all building perimeter and exterior doors access control systems and devices on campus. Housing and Residence Life has delegated authority to control access for residential building perimeter and exterior door access control systems.
   d. UNIVERSITY EMPLOYEES: Faculty and staff requiring building access during periods when the building is secured will complete the appropriate Access Request form. The employee’s supervisor and Department Head or Departmental Access Coordinator must approve the form. Once approved, the Access Control Office will reprogram the electronic lock generally within three business days of receipt of the request.
   e. NON-UNIVERSITY EMPLOYEES: Other individuals, such as construction contractor personnel and vendors, may request building access during periods when the building is secured. The responsible University Project Manager/Maintenance Supervisor should complete the Contractor Access Request Form. The form must contain the names of the Contractor or Site Coordinator and the responsible individual being granted access; start date/time and the termination date/time for this access. The responsible CP&F Director must approve the form. The University Project Manager/Maintenance Supervisor will deliver the completed form to the Work Information Center located in the Facilities Complex or email the completed form to the Access Control Manager or his/her designee at uwg_access_control@westga.edu.
   f. STUDENTS: Students may be granted building access (exterior and/or interior doors as applicable and necessary) during periods when the building is secured. The responsible Department Access Coordinator will complete the Electronic Access Authorization and...
Acceptance Form. The form must contain the names and student ID# of each student being granted access (an attached listing of students may be provided), the extent of the access (days and times), and the termination date for this access. Student access will be automatically terminated at the end of each semester if no end date is given.

g. UNLOCK REQUESTS: University Police Department is the authorized agent for after-hours unlock requests subject to availability of officers and verified identification and authorization of the requestor. Facilities personnel are not authorized to unlock buildings after hours for unknown or unverified requesters.

8. Unauthorized Access
   a. No person shall gain access to University Facilities using an Access Credential which has not been 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.
   b. All Access Credentials remain the property of the University of West Georgia. No person shall duplicate, clone, or reproduce any Access Credential without authorization, and possession or use of an unauthorized credential may result in disciplinary action and/or criminal prosecution.
   c. Authorized users of Access Credentials shall not loan or transfer any Access Credential to any person who is not authorized. Financial accountability incurred by the unauthorized loaning or transfer of Access Credentials will be the responsibility of the original key/card holder’s approving Unit. Issue of Access Credentials through an authorized Key Bank, SAM Box, or Delegated Authority agreement will not be considered “unauthorized loan or transfer” under this procedure.
   d. 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.
   e. The Access Control Office shall periodically monitor and audit electronic access and shall report unauthorized access to the CFO and UPD for investigation and/or corrective actions or recommendations.

9. Access Control Systems Administration
   a. The Access Control Office (ACO) serves as the central authority for administering the access control systems by overseeing access control hardware installations, programming of hardware, initial hardware acceptance testing, troubleshooting hardware issues, troubleshooting software related issues when applicable, support and training for Delegated Authorities, managing system infrastructure, record retention and managing system user accounts and permissions. All users accounts require Single Sign On and be linked to an Active Directory account. Generic user accounts are prohibited.
   b. ITS manages IT-related system infrastructure to include network switches, servers, OS patching, application patching and upgrades, maintenance and backup of databases, and IP addresses. ITS Client Services is responsible for installing access control system software on client workstations upon approval of the Access Control Office. ITS shall not create nor assign user accounts or permissions. Authorized ITS personnel shall be granted elevated system permissions to assist in troubleshooting software and server-related issues outside the scope of the Access Control Office.
c. Changes to permissions within Access Control software for any person, including Delegated Authorities, shall be approved on a case-by-case basis by the Access Control Manager, CFO, and requesting Unit Head using the End-User Agreement form. Such permission may be revoked at any time following due process.

d. Delegated authorities shall be provided with limited access to access control systems to manage access levels, scheduling of locks, run reports, and trace activity of cardholders within authorized segments. Delegated authorities shall not modify or manipulate hardware and software related programming. Tasks outside the scope of delegated authorities shall be coordinated with the Access Control Office.

10. Key Bank Approval and Management

a. Units may request approval for operation of a Key Bank for short-term issue keys to individuals approved by the Department Head or Department Access Coordinator to meet the Unit's operational needs.

b. Key Banks must be approved in advance by the Department Head, Access Control Office, and Chief Facilities Officer and must be administered in compliance with the Access Control Procedures and Key Bank guidelines.

c. Key Banks will be Designated as Level 2 access under the procedure, with required approvals from Department Head, CFO, and AVP/Dean.

d. Key Bank shall be assigned to an individual UWG employee who will be responsible for maintaining key inventory, issue records, periodic reconciliation, and periodic reporting to the Access Control Office.

e. Requesting Department will be required to develop a procedure for the Key Bank and submit it to the Chief Facilities Officer for review and approval. The procedure should include the tracking instrument (paper or digital) for check-in and check-out of keys with appropriate controls and retention of records.

f. The key bank should be secured in a manner that maintains record of individuals having access. (e.g. in a SAM box or locked cabinet with electronic access control). Key Bank may be secured in a locked cabinet or file utilizing an approved lock, in which case a digital or paper key issue log shall be recorded and retained.

g. The requesting Department of Unit will pay all costs associated with establishing and maintaining the Key Bank, including replacement of keys and cores that result from lost or missing keys.

11. Emergency Access and Service Ring Management

a. Emergency Access and Service Rings may be approved for University employees whose responsibilities require broad access to campus buildings to carry out their assigned responsibilities. The Access Control Manager shall maintain an inventory of all keys on each ring and shall periodically audit and verify the integrity of each ring. Emergency Access and Service Rings shall be issued and administered through a SAM box or authorized Key Bank following approval at the appropriate Access Level.

b. EMERGENCY ACCESS: Emergency Access rings may be approved for University officials who demonstrate a bona fide need for immediate access to campus facilities in response to incidents that threaten human health and safety or campus premises/property. Emergency Access rings shall remain on campus and secured within a SAM box or authorized secure Key Bank.
c. 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 on a daily basis through a *SAM box* or authorized *Key Bank*, 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 a shift subjects the employee to loss of access privileges and disciplinary action.

d. *Override Keys* shall only be issued to authorized UPD, security, and access control personnel on a single-use basis to service the systems or provide Emergency Services.

### 12. SAM Box Management and Administration

a. The Access Control Office serves as the central authority for administering Security Asset Management (SAM) boxes throughout the campus, overseeing installation, programming of hardware, initial hardware acceptance testing, troubleshooting hardware issues, troubleshooting software issues when applicable, managing system infrastructure, record retention, and managing system user accounts and permissions.

b. The Access Control Office shall assign designated key slots for Delegated Authorities to manage access via a system segment. Delegated Authorities shall not have access to key slots that are designated to UPD, ITS, CP&F, Contractors, Vendors, or Risk Management.

c. Delegated authorities shall be provided limited access to the *SAM box* management web portal to manage access to keys, run reports, manage users via the Lenel OnGuard integration, manage user groups, and set user PINs within authorized *SAM boxes* or systems. Delegated authorities shall not modify configuration system settings, manipulate *SAM box* configuration, or modify system assets.

### 13. Access Control Delegated Authority

a. *Delegated Authority* is the assignment of limited authority by the Chief Business Officer to a *Unit* that demonstrates that it has a plan, personnel, training, and resources to independently manage access to specific facilities at delegated *access levels* within the requirements of this procedure.

b. This *delegated authority* procedure and its enforcement are the responsibility of CP&F, and are implemented through the appropriate *unit* administrator (Vice President, Dean, Chairperson or Director). It is the responsibility of this *unit* administrator to maintain systematic and effective control of all keys/access cards for rooms and/or buildings primarily under the control and jurisdiction of that college, department or administrative area.

c. Delegated Authorities are responsible for issuing and tracking keys/access cards and maintaining accurate records. Keys/access cards are issued in the strict trust that proper measures will be taken to ensure their safekeeping. Loss of keys/access cards can result in great financial loss to the University and expose University community members to unnecessary risk.

### 14. Contractor and Vendor Access

a. Contractors and vendors shall not be issued *Master Keys* of any type, unless approved by the Chief Facilities Officer or his designee. Keys are not issued to subcontractors except for extenuating circumstances or by prior arrangement.
b. SHORT-TERM ISSUANCE: Short-term Key Issuance refers to daily issue of a key from an authorized key bank to persons so authorized by an Approving Authority. Short-Term Keys are issued and returned during the same 24-hour period.

c. LONG-TERM ISSUANCE: Long-Term Issuance refers to issue of a key or keys to persons so authorized by an Approving Authority for a period longer than 24 hours. Maximum time of issue is 90 days, at which time the Approving Authority may re-issue the key(s) in accordance with this procedure. Long-term issues must be physically audited prior to re-issue.

I. AUTHORITY TO DEVELOP GUIDELINES

1. The AVP for CP&F / CFO is authorized to develop procedures and guidelines related to the administration of Access Control per this Procedure and evaluate adherence to this Procedure by any university Unit.
2. The CFO or his/her designee may at any time grant or rescind exceptions to this procedure based on a risk assessment or abuse of exceptions granted.
3. In the event a guideline conflicts with the UWG Policy or its associated procedures, the latter will control.

Issued by the Chief Facilities Officer, the 25 day of July, 2019

Signature, Chief Facilities Officer

Reviewed by VP Business and Finance: 

Previous version: N/A