ACCESS CONTROL MANAGEMENT PLAN

Campus Planning and Facilities
Division of Business and Finance

June 7, 2017

I. BACKGROUND

The University Police Department (UPD) Technology Division is currently responsible for the management and administration of the University's Access Control System, both electronic and mechanical. The division also manages the University wide intrusion defense system, the CCTV system, the Global Facility Management System (electronic key lock boxes), the CAD/RMS system, the 800mh radio system, and all computers, hardware and software systems related to these functions. All security and access control functions are fully managed and controlled by UPD with support from Campus Planning and Facilities (CP&F) (door hardware and electrical/electronic services) and ITS (networking and systems support).

Campus Planning and Facilities has played a limited role in access control at UWG. Activities have been limited to management of service keys and rings used by CP&F service employees, management of contractor keys, and consulting with the maintenance trades on door hardware and low voltage systems. Planning and Construction Services has assisted UPD and individual departments in the installation of new access control systems and devices, and has worked closely with UPD on the development and application of building standards for access control systems.

The Senior Vice President for Business and Finance has charged UPD and CP&F with reviewing the current state of Access Control Systems and Services at UWG and creating a plan and recommendations for more effective administration of these systems and services based on best practices and an appropriate division of responsibilities and resources.

ACCESS CONTROL POLICY AND STANDARDS COMMITTEE

On March 21, 2017, UPD and CP&F jointly chartered the *Access Control Policy and Standards Committee.* The Committee was charged with assessing the university's security and access control systems, developing a new policy and standards for these systems and services, and making recommendations regarding division of responsibilities, allocation of resources, and processes for security and access control administration at UWG. This was a cross-divisional task force composed of representatives from CP&F, UPD, Facilities, Risk Management, ITS, SAEM, HRL, Auxiliary Services, the Center for Business Excellence, and Academic Affairs. Also included were stakeholders from the full spectrum of the university. A series of committee meetings here held to begin the development of the policy and operational standards for the Access Control Program (ACP). In addition, a series of stakeholder meetings were conducted to provide opportunities for collaboration on policy and operational issues surrounding access control.

PROJECT OBJECTIVES

The objectives developed during the policy and standards phase of this plan were as follows:

1. Assess the current policy, standards, organization, resources, workflow, and operational components of the university's Access Control System.

2. Research examples of policies and standards that represent best practices in Access Control Services in UWG's peer and aspirational institutions.
3. Develop a framework for Access Control Services at UWG, taking into account the university's governance structure, strategic plan, culture, and resources.
4. Develop a university policy for Access Control Services through cross-divisional collaboration. Submit the policy for approval through appropriate governance structures.
5. Develop operational standards for Access Control Services that align with UWG and BOR policies. The standards should include security considerations, approval processes, control processes, accountability measures, infrastructure management, data governance, software systems management, and daily operations.
6. Review and amend, if necessary, the Standards through a cross-divisional collaborative effort involving impacted stakeholders.

II. RISK AND OPPORTUNITY ASSESSMENT

The administration of an Access Control Program carries a number of risks to the University, its agents, and its premises. These risks include:

1. Loss or lapse of strict key, key blank, and access card control could compromise the safety and security of persons and property on campus and could expose the university and university system to significant liability for loss.
2. Transfer of responsibility without corresponding transfer of resources (people, space, equipment, supplies, and capital) could compromise the effectiveness of the security and access control programs.
3. Lack or lapses in recorded chain of accountability for all issued keys and access levels could compromise the integrity of the entire key hierarchy, up to and including the great grandmaster level. The compromising of high-level key or cards carries a direct and significant impact on the safety and security of students, employees, premises, and property.
4. Failure to collaborate cross-divisionally throughout development of policies and standards could undermine the buy-in by critical stakeholders, and could compromise the integrity of the system.

Conversely, a well administered Access Control Program will return many opportunities and benefits to the University:

1. Improved grandmaster key hierarchy under a patented keyway, resulting in a more secure keying system and significantly reducing the possibility of unauthorized key blank acquisition and key duplication.
2. A more clearly defined policy and procedure for approval of keys and access at appropriate organizational levels.
3. Documented chain of custody for all key and electronic access credentials.
4. Elimination or recall of all permanently issued grandmaster keys. Any remaining high level keys in existence will be secured in a key management system with full chain of custody.
5. A database of all keys issued to employees, students, and affiliates.
6. Centralization of access control infrastructure management and related systems.
7. Cross-training in critical access control roles to ensure continuity of service and security.
8. Greater efficiency in the management of maintenance and repair tasks associated with access control.
9. Standardization of access control policies and procedures across campus.

III. POLICY FRAMEWORK

MISSION AND VALUES

ACHIEVEMENT
CARING
COLLABORATION
INCLUSIVENESS
INNOVATION
INTEGRITY
SUSTAINABILITY
WISDOM
Student Success
Academic Success
Successful Partnerships
Operational Success
engage west
Best place to work, learn, and succeed.

The Access Control Plan will be implemented in full support of the University of West Georgia Strategic Plan. It is grounded in UWG's vision to be the *best comprehensive university in America – sought after as the best place to work, learn, and succeed.* In carrying out this plan, we seek to embody the UWG values of *achievement, caring, collaboration, inclusiveness, innovation, integrity, sustainability, and wisdom.*

POLICY

An essential element of security is maintaining adequate Access Control so that University Facilities may only be accessed by those persons that are authorized. Issuance of Access Credentials must 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 Policy 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 units and departments within the scope of this policy are responsible for compliance to ensure the protection of University resources.

PURPOSE

The purpose of this plan is to regulate access to University of West Georgia facilities and premises and to ensure that any individual, college, department, operating unit, program, or affiliate within the scope of this policy is aware of their respective responsibilities when assigned Access Credentials. This policy 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 standards 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 Access Credentials issued,
- Restoring physical security in a timely manner whenever Access Control has been compromised
- Communicating the institution's responsibilities and successes publicly and through all levels of leadership.

DEFINITIONS

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, SAM boxes, lock cylinders, padlocks, equipment panel locks, exit devices, vehicle ignition systems, Access Credentials, and the related computer systems, software, and infrastructure.

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.

Affiliate – Non-employee members of the UWG community that include but are not limited to: vendors, volunteers, observers, trustees, members of the citizen's board, dependents of UM employees, retirees, emeriti faculty, alumni, summer scholars, summer campers, Campus Center members, and tenants (non-UWG staff) renting space in a University Facility.

Authorized Person – UWG employees, currently enrolled students, and Affiliates in possession of a duly issued and valid Access Credential permitting entry into University Facilities for a specific approved purpose.

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

ROLES AND RESPONSIBILITIES

The Chief Business Officer (CBO) is responsible for authorization and delegation of authority for the Access Control Program (ACP). This role approves policy and operational standards and allocates institutional resources in support of the program.

The Chief of Police (CUPD) is responsible for campus security and public safety. This role includes approval of building operating schedules, 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 after-hours lock/unlock requests.

The Chief Facilities Officer (CFO) is responsible for developing and implementing policy for the ACP. This role approves operational standards and procedures for program administration and ensures that resources are appropriately aligned with program activities and requirements. The CFO is consulted on the issuance of grandmaster keys and access levels and ensures the integrity of the Access Control Program.

VPs, 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. They may appoint Key Approving Authorities for this purpose. All requests for master or sub-master keys must be approved by the individual(s) who has authority to access all the spaces and facilities accessed by the master key, normally a Vice-President, AVP or Dean, in consultation with the Chief of Police and the Chief Facilities Officer.

The Director of Facilities, through the **Locksmith Shop** is responsible for the selection, installation, maintenance, repair and replacement of door lock cylinders and lock sets. They are responsible to receive key and lock change requests from the Access Control Office and perform the requested work within a reasonable time frame. The Locksmith will prepare service key rings and contractors' key rings as necessary for issuing by **Administrative Services**. The Locksmith is responsible to maintain up to date records of all keys produced, issued, returned and destroyed, as well as the keyways and codes for all locking devices installed throughout the university, 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 and contractor rings, SAM box management, and program reporting and accountability management. The ACO is responsible to confirm that all persons requesting keys or cards to departmental spaces have a bona fide operational requirement for the key or card, and that the lowest level access is granted to achieve this operational requirement. The ACO routes access requests to the appropriate Access Approving Authority (A^3) and maintains records of all keys and access levels issued.

Access Approving Authorities (A^3) are responsible to determine that all persons requesting keys or cards to their departmental spaces have a bona fide operational requirement for the key or card. Key Approving Authorities are to ensure that all keys and cards are recovered when the key holder leaves the university, changes departments or is no longer is authorized to enter the spaces accessed by the keys/cards. The Access Control Office is to be advised of such changes so keycards can be deactivated and advised whenever keys and cards are re-issued. Keys/cards that are no longer required may be returned to the Access Control Office.

Special Authorities: Following an application and review process, the Chief Business Officer may delegate Special Authority for access control 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. Examples of special authorities might include HRL, Campus Center, and the Library. The department or unit will be required to fund all activities associated with the delegated authority including personnel costs, training, software licensing, computer systems, hardware installation and upgrades, and other operating costs. Special Authorities must administer their programs in full compliance with University Access Control Program 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 and sub-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 Locksmith. Keys to filing cabinets, desks, cabinets, lockers etc. will remain the responsibility of the person in charge of the area.

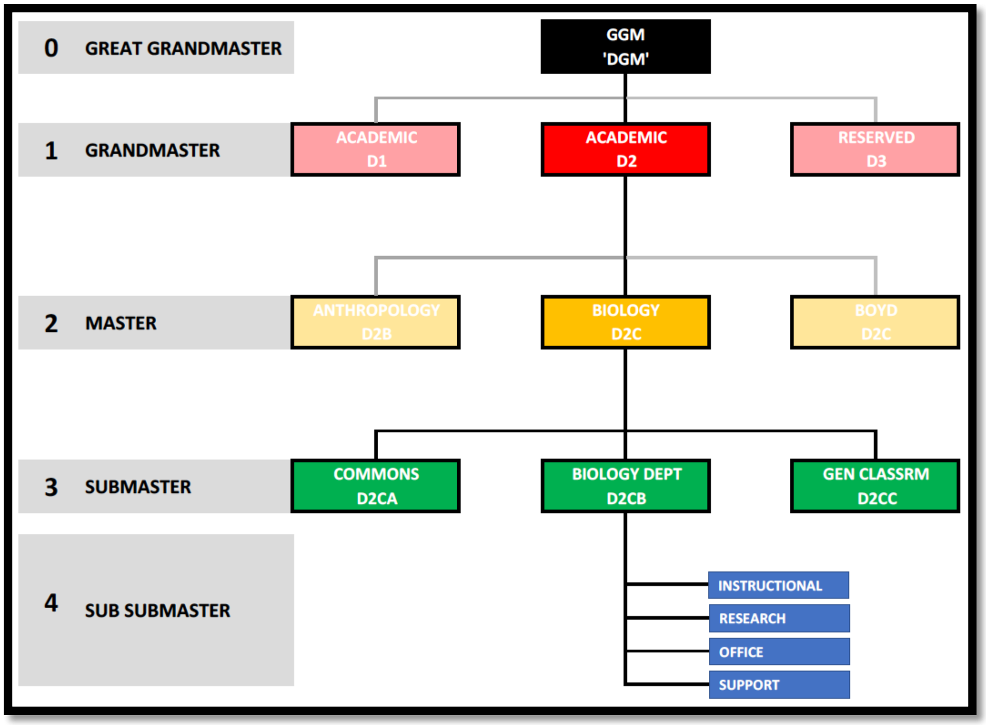
Space allocation authorities are responsible to provide up to date lists semi-annually to the Chief Facilities Officer of rooms and spaces allocated to each department/unit on campus. They are also to advise the Chief Facilities Officer of any changes to those lists as they occur.

ACCESS LEVELS

The Access Control Program is based on the granting of access to University Facilities by Authorized Persons for specific operational purposes. Access is granted by way of a *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.

CONTEXT		LEVEL	
CAMPUS	GRANDMASTER	0	**Great Grandmaster** keys/cards represent the highest access levels, granting access to multiple buildings and/or keyways. Grandmaster keys will not be issued to anyone other than the locksmith and Campus Security.
ZONE	ZONE MASTER	1	**Grandmaster** keys/cards provide access to multiple buildings or functional areas and will generally not be issued without approval from the UPD Chief and CFO. Grandmasters will be serialized and tightly controlled.
BUILDING	MASTER	2	**Master** keys/cards provide access to an entire building or major functional unit. Master Keys are to be treated with the greatest care and are not to be issued to individuals unless approved by the appropriate Key Approving Authority and Chief Facilities Officer. These keys are not to be removed from UWG property.
DEPARTMENT	SUBMASTER	3	**Submaster** keys/cards provide access to a department within a building. And are not to be removed from UWG property.
UNIT	SUB-SUBMASTER	4	**Sub-submaster** keys/cards provide access to multiple spaces in a specific functional area within a department. Example: a Dean's suite or specific set of labs.
INDIVIDUAL	OPERATOR	5	**Operator** keys/cards provide access to an individual space.

The diagram to the right represents a typical key hierarchy for an academic building. The key structure progresses in a branching structure to create lower level submasters from the high level grandmaster. Higher level keys operate all locks in the structure below.



APPROVAL LEVELS

Each access level will have a corresponding approval level.   For credentials that have multiple access levels (such as a service key ring or WolfCard encoded with multiple levels) the required approval level will apply to the highest level for that credential. Access Approving Authorities may only approve access to spaces within their unit or functional area, and may not grant access beyond their own access level approval. The following table provides approval levels and examples:

ACCESS LEVEL	APPROVAL LEVEL	EXAMPLES
LEVEL 0 – GGM	CUPD + CFO + CBO + VP	All patented Grandmaster and Great Grandmaster keyways; PEAK masters; High-security masters; All control keys; ALL-ACCESS cards, SAM bypass keys, rings with multiple legacy grandmasters (GGM, GGMV, GGMT). (Generally Prohibited)
LEVEL 1 – GM	CUPD + CFO + VP	Legacy grandmasters (GGM, GGMV, GGMT), Zone Masters on patented keyways, resident room master keys and cards, high security keys, ALL-BUILDING-PERIMETER cards, rings with multiple Masters. (Generally Prohibited. SAM-controlled issue of legacy GM's permitted for service rings only)
LEVEL 2 – MA	DIR/CHAIR + CFO + AVP/DEAN	Building Master keys and cards (including rings); building perimeter keys and cards, Utility Masters, life safety panels and masters. (SAM / Restricted issue only)
LEVEL 3 – SM	DIR/CHAIR	Departmental submaster, classroom submaster, mechanical room submaster (Short-term issue only. Must be secured and may not leave campus)
LEVEL 4 – SS	SUP/AD + DIR/CHAIR	Office suite; lab sub-submaster; construction core (Long-term issue permitted)
LEVEL 5 - OP	SUP/AD + DIR/CHAIR	Individual room key or card (Long-term issue permitted)

SENIOR LEADERSHIP [SL]	INSTITUTIONAL LEADERSHIP [IL]	DEPARTMENT LEADERSHIP [DL]
PROV - Provost	*AVP – Assoc/Assist VP/Provost*	*DIR – Director*
CBO – Chief Business Officer	*DEAN – College Dean*	*CHAIR – Department Chair*
VP – Divisional VP	*CUPD – Chief University Police Dept*	*AD – Assoc/Asst Director*
	CFO – Chief Facilities Officer (AVP CP&F)	*SUP - Supervisor*

FISCAL ACCOUNTABILITY

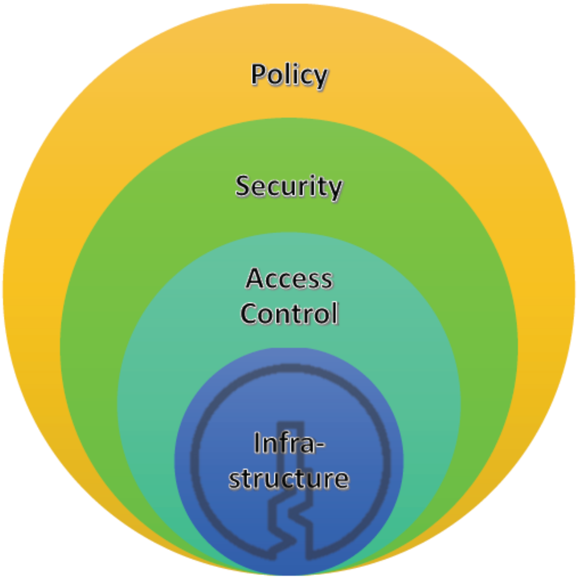
Access Level Approval includes fiscal accountability for all keys issued. The impact associated with the loss of a Level 2 key or higher is significant. The risk of criminal acts, including crimes against persons, and the cost of re-keying an entire building or buildings are high.   In the event a key is lost, the approver will be responsible for all costs associated with replacing the effected cores and keys. The following table demonstrates the range of costs associated with the loss of various access level keys:

▪ LEVEL 5 Operator:	$25 - $50 (1 Core)
▪ LEVEL 4 Sub-Submaster:	$100 - $500 (4 – 16 cores)
▪ LEVEL 3 Dept Submaster:	$500 - $2,000 (16 – 64 cores)
▪ LEVEL 2 Building Master:	$2,000 - $15,000 (64-256 cores)
▪ LEVEL 1 Legacy GM / Zone:	$30,000 - $60,000 (2,000 + cores)
▪ LEVEL 0 Grandmaster:	$200,000 + (>5,000 cores)

IV. OPERATIONAL PLAN

OPERATIONAL TIERS

The Access Control Plan is built on a layered model. Each layer, or tier, is built on the foundation of the underlying tier, and is dependent on that tier for authority, policy, principles, and standards. The basic operational structure is as follows:



Policy Tier: Authority for Access Control Policy resides at the highest level of university leadership and is subject to review and approval by the Policy Committee and the Vice Presidents. Policy development and oversight will be administered by the standing *Access Control Policy and Standards Committee.* This is a cross-divisional advisory working group that will develop and administer access control policy in alignment with UWG's mission, vision, and strategic plan.

Security Tier: Under BOR policy, responsibility and accountability for security and public safety is retained by University Police. UPD will retain direct responsibility for campus security including high level integrity of access control systems. UPD will also retain intrusion detection, video surveillance, emergency response dispatch, and perimeter security for buildings and premises. Authority for administration and daily operations for the Access Control Program is delegated to Campus Planning and Facilities, contingent upon compliance with Policy and Security requirements.

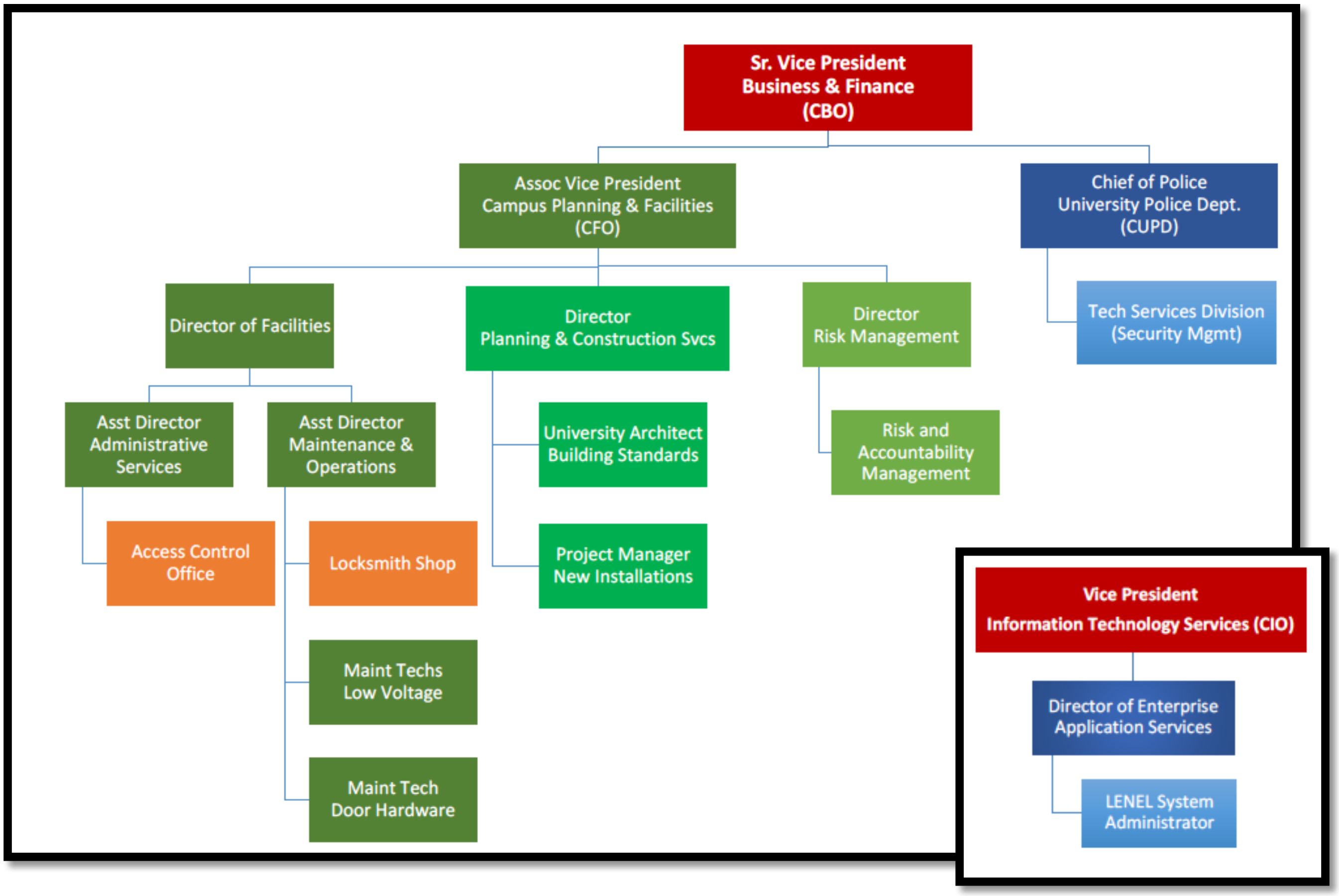
Access Control Tier: Access Control Management, including planning and daily operations, will be primarily administered by Campus Planning and Facilities. Under the supervision of the Assistant Director of Administrative Services (ADAS) in Facilities and Grounds, the Access Control Manager will ensure that all keys and access cards are issued in accordance with policy and are duly authorized. This position will also ensure that key issue and electronic access records are maintained, and that a chain of custody is established for all keys. The Access Control Manager will oversee the key and access request processes and will authorize cutting of keys or granting of access levels based on policy requirements.

Infrastructure Tier: The Assistant Director of Maintenance and Operations (ADMO) in Facilities and Grounds will have primary responsibility for management of access control infrastructure including the Lock Shop (key and core management), Carpentry Shop (door hardware), and Electric Shop (electronic access control devices). The ADMO will administer service contracts (i.e. Stanley, Best, and Lenel) as needed to maintain and operate the components and systems associated with Access Control. The Lock Shop will perform all activities related to core management, cutting and duplication of keys, and management of key rings as authorized by the Access Control Manager via a duly issued work order. The Carpentry Shop will provide support, supplemented by vendors as needed, for door and door hardware components of the access control infrastructure. The Electrical Shop will provide support, supplemented by vendors as needed, for electronic access devices, power supply, SAM boxes, and related systems. The Director of Planning and Construction Services will oversee new access control installations and will develop building standards for renovation and new construction. The Director of Enterprise Application Services in ITS will be responsible for system administration for applications and systems related to access control, including Lenel, IP network, CMMS, CAFM, key request applications, and key tracking database. The Chief Facilities Officer will facilitate coordination across departments and divisions to ensure seamless delivery of services.

ORGANIZATIONAL STRUCTURE

The Access Control Program will apply a distributed model based on specific roles and responsibilities:

Organization	Role	Responsibilities
CP&F (Business & Finance)	Program oversight	Policy, planning, coordination, service delivery
Facilities – Administrative Services (CP&F)	Access Control Management	Access request processing, program administration, approving access, authorizing credentials, SAM boxes
Facilities – Maintenance & Operations (CP&F)	Infrastructure Management	Key and core management, maintenance and servicing of door hardware and electrical components
Planning & Construction Services (CP&F)	New Installations	Planning and design for new systems, project management, building standards.
Risk Management (CP&F)	Risk and Accountability	Program assessment, risk assessment, internal review
Enterprise Application Services (ITS)	Systems Administration	Software applications, IP network, software and hardware integration
University Police Department (Business & Finance)	Security	Grandmaster access approval, building/perimeter security, breach/key loss investigation, surveillance


Sr. Vice President Business & Finance (CBO)
Assoc Vice President Campus Planning & Facilities (CFO)
Chief of Police University Police Dept. (CUPD)
Director of Facilities
Director Planning & Construction Svcs
Director Risk Management
Tech Services Division (Security Mgmt)
Asst Director Administrative Services
Asst Director Maintenance & Operations
University Architect Building Standards
Risk and Accountability Management
Access Control Office
Locksmith Shop
Project Manager New Installations
Maint Techs Low Voltage
Maint Tech Door Hardware
Vice President Information Technology Services (CIO)
Director of Enterprise Application Services
LENEL System Administrator

PROCEDURES

Campus Planning and Facilities will develop procedures governing the Access Control Program. Elements of these procedures will include:

- An online key/access request form for directors/chairs to request and approve keys and access for employees within their unit. The form will be routed for approval at the appropriate level(s).
- An online key/access request form for vendor access.
- A procedure with accompanying forms governing the management of departmental key banks, requiring key inventory, logging, chain of custody, and auditing.
- A procedure governing the security and operation of SAM boxes, including approval of service rings for authorized personnel.
- A procedure for *Special Authority* that will specify the rules and standards for those organizational units that demonstrate capability and resources to manage specified access levels in a specific facility.
- A revised master key hierarchy based on the Best CoreMax ® patented keyway system, with full retirement of the existing legacy grandmaster system in three (3) years.
- A procedure for key and core changes and key duplication, including a service level agreement for chargeback services.
- A database containing chain of custody data for all approved key issues, and maintenance of history files for electronic access (access levels granted and access attempted).
- Procedures and standards governing installation of new key and access control systems in construction and renovation projects, including a service level agreement for systems to be funded by departments.
- Creation of an assessment tool for the Access Control Program.

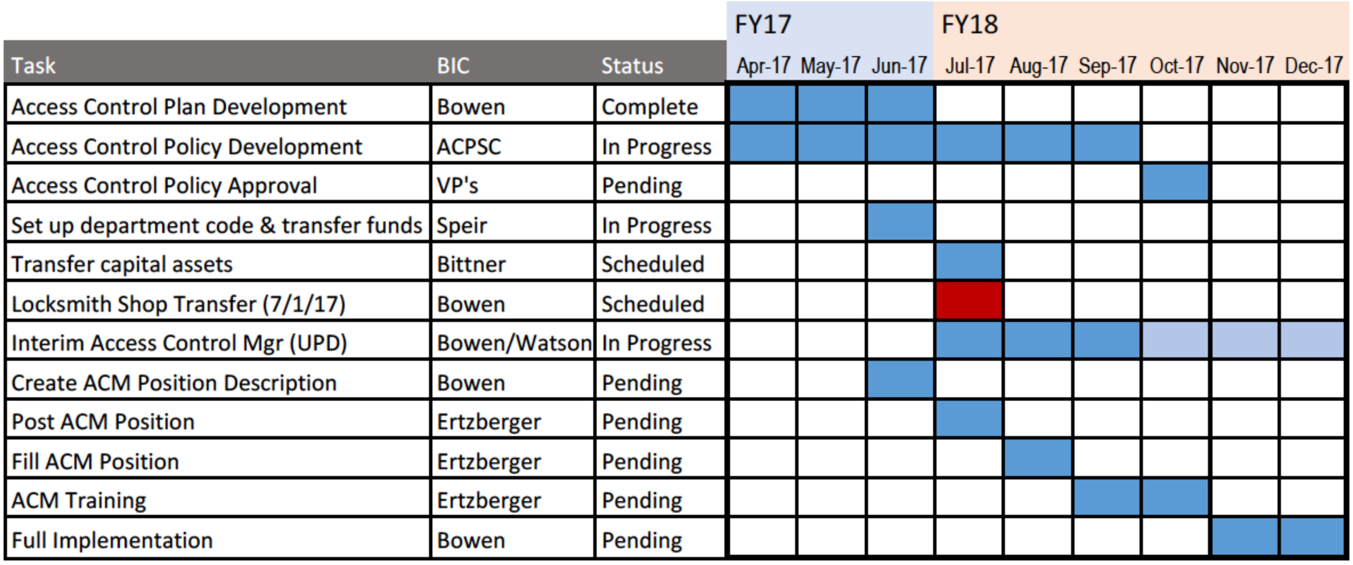
FUNDING AND FISCAL ACCOUNTABILITY

Program Funding: The Access Control Program will operate through a new department code in the Facilities and Grounds budget. The following funding sources are proposed:

Fund	Description	Est. Budget	Fund Source
Personnel Costs	Full-time and SA’s	$134,000	UPD, AUX, CP&F Funds
Supplies	Stanley Agreements	$28,300	UPD Budget
	Vendor Agreements	TDB	UPD Budget
	Operating Supplies	$40,000	Quasi-revenue offset
	Lenel Training (3 personnel)	$10,000	FY18 One-time Allocation
Travel	Travel for training	$3,000	Current CP&F Funds
Equipment	Tools and equipment	$3,000	Current CP&F Funds
	Vehicles (2)	$-	Current UPD Assets
	Capital equipment & PC's	$-	$12,000 Funded from YE FY17
Quasi-Revenue	Departmental Charges	$(40,000)	UPD Budget (based on FY17)
Total		**$178,300**	

Department / Unit Accountability: Key Approving Authorities requesting a change or upgrade to the standard locking system such as re-keying, replacing lock sets and cylinders or installation of a different security system such as electronic, biometric or card access, are responsible to cover the cost of the change and the ongoing cost of maintaining the upgraded locking system from their departmental operating budget, unless the Chief Business Officer determines that the upgrade is required for the university to maintain appropriate security. The department is also responsible for the cost of replacing lost, stolen, broken or worn keys and the cost of re-keying in the event of lost or stolen keys.

IMPLEMENTATION TIMELINE



			FY17			FY18					
Task	BIC	Status	Apr-17	May-17	Jun-17	Jul-17	Aug-17	Sep-17	Oct-17	Nov-17	Dec-17
Access Control Plan Development	Bowen	Complete	🟦	🟦	🟦						
Access Control Policy Development	ACPSC	In Progress	🟦	🟦	🟦	🟦	🟦	🟦			
Access Control Policy Approval	VP's	Pending							🟦		
Set up department code & transfer funds	Speir	In Progress			🟦						
Transfer capital assets	Bittner	Scheduled				🟦					
Locksmith Shop Transfer (7/1/17)	Bowen	Scheduled				🟥					
Interim Access Control Mgr (UPD)	Bowen/Watson	In Progress				🟦	🟦	🟦	▨	▨	▨
Create ACM Position Description	Bowen	Pending			🟦						
Post ACM Position	Ertzberger	Pending				🟦					
Fill ACM Position	Ertzberger	Pending					🟦				
ACM Training	Ertzberger	Pending						🟦	🟦		
Full Implementation	Bowen	Pending								🟦	🟦