UC Davis Security Integration Plan

Campus Security Standards Committee:
• Allen Tollefson, Associate Vice Chancellor - Facilities Management
• Jill Parker, Associate Vice Chancellor - Safety Services
• Clayton Halliday, Assistant Vice Chancellor - Design and Construction Management
• Emily Galindo, Director - Student Housing
• André Knoesen, Chair - Academic Senate
• Leslie C. Moore, Director of Safety and Hospitality Services – UCDMC
• Brian Buckley, Security Director

Our Challenge:
The safety and security of each member of UC Davis should be the University’s highest priority just as it is to parents who send one of the most valuable parts of their lives, their child, into our care. Fundamentally, the basis for all security starts with a robust, fully integrated security system that serves as the backbone for all physical security measures. Essential elements in advanced security systems are access control, video security and alarms. Determining both the need and plan for an integrated security system at UC Davis is the charge of the Campus Security Standards Committee.

This committee was tasked with reviewing existing security technology at UC Davis to include access control, alarms and video monitoring and then determining if a single centralized and standardized system for security should be adopted. If such a system be recommended, the elements considered to be fundamental to the system were to be identified. Additionally, the committee was charged with determining a budget for this standardized security platform and the unit to be charged with its operation and control. The conclusions of this committee are listed below.

Context and Scope
The campus has never had an integrated security system. Currently, UC Davis has over 15 different types of access control systems in use on campus. These systems are purchased, maintained and operated by individual departments without centralized oversight or coordinated response in the event of an emergency. As an example, in just one building on campus, Kemper Hall, five separate access control systems are in use that are paid for and operated by individual departments. Furthermore, none of the 15 types of systems currently in use on campus integrate with each other and none of the systems’ functions are shared with the UC Davis Police Department.

Excluding housing areas, approximately 930 doors are currently electronically operated for access at UC Davis. All remaining doors (approximately 30,000) use hard keys for access. Most buildings at UC Davis have no electronic door access controls whatsoever and rely on hard key opening and closing of the buildings, usually by custodial staff.
More than 1,000 video security cameras of varying type and quality exist on campus, estimated because heretofore unknown systems have been routinely found to exist. All are individually purchased, maintained and operated by separate departments. Determination as to who may view these cameras is currently made by individual departments with no centralized oversight. The cameras vary widely as to quality and the potential for possible transfer to an integrated video system. None of the cameras, other than those in use at the UC Davis Police Department for the Department's own buildings, are available for viewing by the UC Davis Police Department.

Approximately 275 individual intrusion alarm systems currently exist at UC Davis. These alarm systems, although purchased by individual departments at the University, are managed and monitored by the UC Davis Police Department. Our goal is to move both access control and video monitoring to the UC Police Department where alarm oversight already exists. Virtually every UC campus other than UC Davis has an integrated security system. As an example, UC Berkeley has had an integrated security system for almost 20 years and UC Merced has had one since its inception. These systems are directly tied to their respective police departments.

**The Plan:**

The committee recommends that the campus invest in the purchase of a single, centralized, and standardized security platform that will be directly operated, maintained and controlled by the UC Davis Police Department according to agreed-upon policies. Existing security technology will be consolidated into the platform, whenever possible.

Included will be the execution of policies that govern the installation and use of all access control, video devices and intrusion alarm devices at UC Davis. Additional employee positions will be added in the UC Davis Police Department to oversee the centralized security platform, mirroring existing positions at the UC Berkeley Police Department.

**Investment Needs**

It is estimated that $8.5 million is needed to implement a fully integrated door access control system across the entire UC Davis campus. This amount would include the electronic conversion of approximately 6,000 doors. Implementation would occur over a three to five year period (a three year allocation estimate is below) allowing for the conversion of approximately 2,000 doors per year.

It is estimated that 1.6 million dollars is needed to implement a fully integrated video control system across the campus. Although this amount could be allocated over a three to five year period if necessary, an immediate conversion of all video devices to a single platform is strongly recommended.

The addition of four security positions would be made to the UC Davis Police Department with individual positions responsible for access control, access card services, video management and alarm monitoring.

**Execution:**

- **Purchase of software** head-end systems capable of managing a campus-wide One Card access control system and a video control system.
- **Funding for the transfer and conversion of the existing 928 electronically operated doors** on campus from separate stand-alone systems to an integrated centralized system managed by the UC Davis Police Department (similar to alarms that are already managed by the UC Davis Police Department).
• **Funding for the conversion of 2,000 doors per year** for 3 years from hard keys to electronic access control (doors will be prioritized for conversion based on identified security needs).

• **Funding for the acquisition and conversion of approximately 1000 security cameras** to an integrated centralized camera system managed by the UC Davis Police Department (similar to alarms that are already managed by the UC Davis Police Department).

• **Transfer of all UC Davis card access systems** (including the card system currently in use by the UC Davis Registrar’s Office) to the UC Davis Police Department.

• **Funding for four new security positions** within the UC Davis Police Department responsible for management of access control, access card services, video management and alarm monitoring.

• **Adoption of campus policies governing all access control and video monitoring** at UC Davis (similar to the already existing alarms policy).

---

**Supporting documents related to the execution of this plan are available via the links below and in the following pages**

- **Pricing Summary** – [http://facilities.ucdavis.edu/docs/pricing.pdf](http://facilities.ucdavis.edu/docs/pricing.pdf)


- **Policies (Draft)**

- **Position Descriptions**
### PRICING SUMMARY

<table>
<thead>
<tr>
<th></th>
<th>CBORD</th>
<th>Lenel</th>
<th>Software House</th>
<th>Avigilon VMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Deployment Cost</td>
<td>$8,492,834</td>
<td>$9,208,984</td>
<td>$8,844,595</td>
<td>$1,613,346</td>
</tr>
</tbody>
</table>

**Cost Breakdown**

<table>
<thead>
<tr>
<th>Description</th>
<th>CBORD</th>
<th>Lenel</th>
<th>Software House</th>
<th>Avigilon VMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head End System Cost (including SSA through 5 Years)</td>
<td>$162,578</td>
<td>$255,704</td>
<td>$198,059</td>
<td>$289,435</td>
</tr>
<tr>
<td>System Engineering Cost (Full Deployment)</td>
<td>$854,705</td>
<td>$911,576</td>
<td>$883,484</td>
<td>$44,801</td>
</tr>
<tr>
<td>Building Conversion Cost (4,012 Doors and 885 Cameras)</td>
<td>$7,475,550</td>
<td>$8,041,704</td>
<td>$7,763,052</td>
<td>$1,279,110</td>
</tr>
</tbody>
</table>

**Build Hardware Conversion Cost Breakdown Options:**

<table>
<thead>
<tr>
<th>Description</th>
<th>CBORD</th>
<th>Lenel</th>
<th>Software House</th>
<th>Avigilon VMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per Year Field Cost over 5 Years</td>
<td>$1,666,051</td>
<td>$1,790,656</td>
<td>$1,729,307</td>
<td>$264,782</td>
</tr>
<tr>
<td>Per Year Field Cost over 3 Years</td>
<td>$2,776,752</td>
<td>$2,984,427</td>
<td>$2,882,179</td>
<td>$441,304</td>
</tr>
<tr>
<td>Phase 1 (Year 1)</td>
<td>$2,814,435</td>
<td>$3,017,706</td>
<td>$2,919,137</td>
<td>$984,075</td>
</tr>
<tr>
<td>Phase 2 (Year 2)</td>
<td>$2,355,361</td>
<td>$2,562,285</td>
<td>$2,461,945</td>
<td>$79,745</td>
</tr>
<tr>
<td>Phase 3 (Year 3)</td>
<td>$1,838,190</td>
<td>$1,970,952</td>
<td>$1,906,574</td>
<td>$215,290</td>
</tr>
</tbody>
</table>

*Average per door/camera cost below do not include headend costs figures:*

- Per Door Conversion Cost Average of Existing Reader and Hardware: $1,413
- Per Door w/ New Doors Reader and Hardware: $4,413
- Per Camera Conversion (Existing Analog Camera of Encoders): $625
- Per Camera Replacement w/ 300' of New Cable: $1,735
<table>
<thead>
<tr>
<th>Product</th>
<th>CBORD</th>
<th>Lenel</th>
<th>Software House</th>
<th>Avigilon VMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head End System Cost (Software Only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Head End Software Cost (7000 doors/900 Cameras)</td>
<td>$70,600</td>
<td>$94,000</td>
<td>$122,500</td>
<td>$253,185</td>
</tr>
<tr>
<td>Head End Hardware</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>$26,250</td>
</tr>
<tr>
<td>Client Licenses Included/Cost</td>
<td>Unlimited</td>
<td>0 included/$2,800</td>
<td>100 Included/$500</td>
<td>Unlimited</td>
</tr>
<tr>
<td>License Cost for 25 Clients</td>
<td>$0</td>
<td>$70,000</td>
<td>$0</td>
<td>N/A</td>
</tr>
<tr>
<td>Badging Station Client Included/Cost</td>
<td>Unlimited</td>
<td>0 included/$3491</td>
<td>10 Included/$2,500</td>
<td>N/A</td>
</tr>
<tr>
<td>License Cost for 10. Clients</td>
<td>$0</td>
<td>$34,910</td>
<td>$0</td>
<td>N/A</td>
</tr>
<tr>
<td>Sub Total:</td>
<td>$70,600</td>
<td>$198,910</td>
<td>$142,000</td>
<td>$289,435</td>
</tr>
<tr>
<td>Yearly Maintenance Cost (Yr. 1 included w/ purchase)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSA Annual Support Cost (2000 doors) Yr. 2</td>
<td>$22,150</td>
<td>$13,677</td>
<td>$13,500</td>
<td>$0</td>
</tr>
<tr>
<td>SSA Annual Support Cost (2000 doors) Yr. 3</td>
<td>$22,704</td>
<td>$14,019</td>
<td>$13,838</td>
<td>$0</td>
</tr>
<tr>
<td>SSA Annual Support Cost (2000 doors) Yr. 4</td>
<td>$23,271</td>
<td>$14,369</td>
<td>$14,183</td>
<td>$0</td>
</tr>
<tr>
<td>SSA Annual Support Cost (2000 doors) Yr. 5</td>
<td>$23,853</td>
<td>$14,729</td>
<td>$14,538</td>
<td>$0</td>
</tr>
<tr>
<td>Sub Total:</td>
<td>$91,978</td>
<td>$56,794</td>
<td>$56,059</td>
<td>$0</td>
</tr>
<tr>
<td>Grand Total SMS Head-End + 5 Yr. SSA</td>
<td>$162,578</td>
<td>$255,704</td>
<td>$198,059</td>
<td>$289,435</td>
</tr>
<tr>
<td>Building Hardware Conversion Cost</td>
<td>Phase 1 Total Doors</td>
<td>1502</td>
<td>Phase 1 Estimated Doors w/ Readers</td>
<td>501</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------</td>
<td>------</td>
<td>-----------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td>Phase 1 Estimated Doors Requiring Readers</td>
<td>501</td>
<td>$2,158,218</td>
<td>$2,259,853</td>
</tr>
<tr>
<td></td>
<td>Phase 1 Total Cameras</td>
<td>651</td>
<td>Phase 1 Camera Conversions (Analog)</td>
<td>131</td>
</tr>
<tr>
<td></td>
<td>Phase 1 Camera Replacements</td>
<td>520</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Sub Total:</td>
<td>$2,814,435</td>
<td>$3,017,706</td>
<td>$2,919,137</td>
<td>$984,075</td>
</tr>
<tr>
<td>Phase 2 Total Doors</td>
<td>1529</td>
<td>Phase 2 Estimated Doors w/ Readers</td>
<td>510</td>
<td>$668,014</td>
</tr>
<tr>
<td></td>
<td>Phase 2 Estimated Doors Requiring Readers</td>
<td>510</td>
<td>$1,687,347</td>
<td>$1,790,809</td>
</tr>
<tr>
<td>Phase 1 Total Cameras</td>
<td>53</td>
<td>Phase 1 Camera Conversions (Analog)</td>
<td>11</td>
<td>$0</td>
</tr>
<tr>
<td></td>
<td>Phase 1 Camera Replacements</td>
<td>42</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Sub Total:</td>
<td>$2,355,361</td>
<td>$2,562,285</td>
<td>$2,461,945</td>
<td>$79,745</td>
</tr>
<tr>
<td>Phase 3 Total Doors</td>
<td>981</td>
<td>Phase 3 Estimated Doors w/ Readers</td>
<td>327</td>
<td>$428,595</td>
</tr>
<tr>
<td></td>
<td>Phase 3 Estimated Doors Requiring Readers</td>
<td>327</td>
<td>$1,409,595</td>
<td>$1,475,976</td>
</tr>
<tr>
<td>Phase 1 Camera Conversions (Analog on Encoders)</td>
<td>28</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Phase 1 Camera Replacements</td>
<td>114</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Sub Total:</td>
<td>$1,838,190</td>
<td>$1,970,952</td>
<td>$1,906,574</td>
<td>$215,290</td>
</tr>
<tr>
<td>Housing Perimeter Doors</td>
<td>96</td>
<td>$41,942</td>
<td>$48,438</td>
<td>$45,288</td>
</tr>
<tr>
<td>Housing DC Doors</td>
<td>100</td>
<td>$425,623</td>
<td>$442,323</td>
<td>$430,108</td>
</tr>
<tr>
<td>Sub Total:</td>
<td>$467,565</td>
<td>$490,761</td>
<td>$475,396</td>
<td>$0</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----</td>
</tr>
<tr>
<td><strong>Engineering Costs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Standards</td>
<td>$6,000</td>
<td>$6,000</td>
<td>$6,000</td>
<td>$2,000</td>
</tr>
<tr>
<td>Head End Specification and Design</td>
<td>$10,000</td>
<td>$10,000</td>
<td>$10,000</td>
<td>$3,000</td>
</tr>
<tr>
<td>Existing System Conversion at 7.55% of Installed Cost</td>
<td>$134,608</td>
<td>$155,456</td>
<td>$145,346</td>
<td>$7,969</td>
</tr>
<tr>
<td>New System Design at 12.5% of Installed Cost</td>
<td>$710,098</td>
<td>$746,120</td>
<td>$728,138</td>
<td>$33,833</td>
</tr>
<tr>
<td><strong>Sub Total:</strong></td>
<td>$854,705</td>
<td>$911,576</td>
<td>$883,484</td>
<td>$44,801</td>
</tr>
<tr>
<td><strong>Grand Total of Deployment</strong></td>
<td>$8,492,834</td>
<td>$9,208,984</td>
<td>$8,844,595</td>
<td>$1,613,346</td>
</tr>
</tbody>
</table>

***NOTES
Grand total SMS figures assumes 1/3 of the average of the total number of perimeter doors have existing access control that will be converted and 1/3

Grand total figures for cameras assumes 20% of the existing cameras will be used with video encoders and the remaining 80% will be replaced with
# Table of Contents

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.O.C.</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>2</td>
</tr>
<tr>
<td>Security Management Description</td>
<td>3</td>
</tr>
<tr>
<td>Design Standards</td>
<td>5</td>
</tr>
<tr>
<td>Implementation Guidelines</td>
<td>14</td>
</tr>
</tbody>
</table>
Background

The purpose of this Security Standard Document is to document the specific goals and objectives of the Security Management System for the University of California, Davis (UCD), to define the major system software and hardware components that comprise the SMS, and to provide general the design guidelines for integration of the SMS into new and existing building projects and site improvement projects throughout UCD facilities. The principal goal of this document is to provide consistent design and implementation standards for the integration of physical electronic security devices. The design standards included in this document describe system device performance requirements for each of the applicable devices that may be included within a specific project. The subsequent implementation standards establish a protocol for device type selection – when and where to install a particular devices.

Historically, the implementation of security systems and infrastructure in new and retrofit building projects at UCD has been determined by various entities that have are not directly responsible for the safety and security of the students, staff and facility. This resulted in fragmented group of systems that are unmanageable for UCD Police. Recently, UCD has undertaken the incorporation of all Building Intrusion Alarms Systems (BIAS) into a centralized monitoring and control platform that now allows alarms throughout UCD facilities to report directly to Campus Police Dispatch. This has improved response times to alarms and increased the reliability and functionality of these systems. UCD Police have set a goal to centralize monitoring and control of the Access Control Systems and Video Surveillance Systems that are deployed throughout the Campus and facilities. Achieving this goal is more complex than the centralization of the BIAS but it is not insurmountable. The initial step in the process was to establish and implement a Security Management System that serves as the nexus for Campus wide control and management of access controlled doors and video surveillance cameras.

The Security Management System (SMS) is a unified security management platform that provides integration capabilities for four primary security sub-systems. The purpose of this implementation standard is to document the specific goal and objectives of the SMS, to define the major system software and hardware components that comprise the SMS, and to provide general design guidelines for integration of the SMS into new and existing building and site improvement projects on Campus.
The Security Management System is a unified security management tool that provides UCD Police with a physical security information and situational awareness management system. The SMS serves as a foundational tool used by UCD Police in their continuing efforts to ensure a safe and secure learning environment for students, faculty and staff.

The SMS is comprised of three major electronic security sub-systems.
- Access Control System (ACS)
- Building Intrusion Alarm Systems (BIAS)
- Video Surveillance System (VSS)

Each of these sub-systems is comprised of command/control hardware and software and field devices. The command/control hardware and software are standardized so as to provide UCD with a single, unified operational platform for the physical security systems management. Security field devices will be designed and specified on a project specific basis throughout the course of the execution of new and retrofit construction. Individual projects may include hardware and software components (i.e. data storage and licenses) that are added to increase the capacity of the UCD system/sub-system. Not all of the devices described in this document will necessarily be included in each project. It is the responsibility of the design team assigned to each project to use the security standards and protocols in this document to develop the appropriate deployment strategy and device requirements for their particular project.

**Access Control System**

The ACS is the core platform of the SMS. It is a software based system that provides the command and control functionality for the access control doors and associated alarm devices, stores access control credentials and privileges (ID Cards), provides the primary graphical user interface for monitoring and managing electronic security events and alarms, and serves as the central repository for system events that can be used for investigative and administrative purposes. In addition, the SMS provides the central integration facilities for the other electronic security sub-systems through seamless system software interoperability and management that provides a single human-to-system graphical user interface for the configuration, management and control of these systems.
**Building Intrusion Alarm System**

The BIAS is primarily hardware based. It is comprised of existing building and room alarm panels and associated field devices. These systems are identical to small commercial and residential “burglar alarm systems” in that the panel receives alarm signals from various field devices and, when the system is armed, transmits that alarm information to a central alarm monitoring system. The centralization of the BIAS is largely complete at UCD and the integration of the BIAS into the SMS will provide UCD Police with centralized, integrated alarm interface that ties graphical mapping capabilities and real-time and recorded video into the existing alarm monitoring capabilities.

**Video Surveillance System**

The VSS is a software based sub-system that operates at a deep integration level with the SMS. The software provides configuration, control, monitoring and recording management of digital video cameras and digitally encoded signals from analog cameras. By being a fully integrated component with the SMS, video monitoring is an event based practice where specific video data is displayed when associated with a particular programmed alarm event within the system. This feature serves as an effective situational management tool for UCD Police to utilize on a real-time basis. In addition, all cameras are recorded within the system and video is to be stored for a minimum of 30 days so the VSS also serves as a valuable investigative tool. The system is network based and is substantially reliant on the network backbone infrastructure for transmission of video data. VSS recording devices, which have a substantial amount of drive space allocated for storage, are distributed throughout buildings and facilities to reduce network traffic demand and to provide fault tolerance.
Design Standards

This section includes technical standards data and criteria that should be used, in whole or in part, by security design professionals on a project specific basis. The intent of the material provided is to serve a guideline for establishing performance criteria and maintaining conformance UCD Security System Standards. The systems designed on particular projects must maintain conformity and operation with the SMS software as described and installed. As such, major system components are manufacturer specific and substitution will not be permitted. However, field devices are specified on a performance basis. Where make and models are specified, the information is to serve solely to establish performance criteria. In such cases, make and model information will be followed by, “or equal” and should be specified as such in the project specific design documentation.

General Security Requirements

A  CODES AND STANDARDS
All work shall be in accordance, where applicable, with the latest edition of the following:
- California Building Code – Title 24 (CBC)
- California Electrical Code (CEC)
- California Fire Code (CFC)
- Electronics Industries Association (EIA)
- Institute of Electrical and Electronic Engineers (IEEE)
- National Electrical Manufacturers Association (NEMA)
- Occupational Safety and Health Act (OSHA)
- All other State and local codes and ordinances that may prevail

B  DESCRIPTION OF WORK
Work includes the design, procurement and installation of SMS devices and equipment and integration of the devices and equipment to UCD’s SMS, comprised of the following sub-systems:
- ACS
- BIAS
- VSS
Specific devices types, locations and interconnection requirements are described and detailed within project specific documents, in accordance with these UCD Security Standards.

Security related work may require system configuration and programming of existing UCD systems. Coordinate all such configuration and programming requirements with the UCD.

C QUALIFICATIONS OF CONTRACTOR
The Contractor should maintain all current licenses required to provide the specific work efforts of the specific project.

The Contractor should utilize installation and service technicians whom are competent; factory trained and certified personnel capable of installing and maintaining the system and providing reasonable service.

D MATERIAL SUBSTITUTIONS
Whenever materials, equipment or processes are specified or described in this Standard by using the proprietary name of an item or the name of a particular manufacturer, fabricator, supplier or distributor, the naming of the item is intended to establish the type, function and standard of quality and performance required by this Contract. It is not the intent of UCD to exclude other materials, equipment, or processes or to limit competition in bidding. Therefore, unless the proprietary name referred to in the specifications is followed by words indicating that no substitution is permitted, materials, equipment, or processes of other manufacturers, fabricators, suppliers, or distributors will be considered by UCD for substitution.

Consideration will be given to a proposed substitute only when sufficient information is submitted to UCD to determine that the proposed substitute material, equipment, or process is in fact equivalent in all respects to the materials, equipment, or processes named in the specifications.

Where the phrase “or equal,” occurs in this Standard, do not assume that the materials, or equipment, will be approved as equal until the item has been specifically so approved for this work by UCD.

The Owner, based upon conformance and integration with existing system equipment, has selected primary system components as specified. No substitutions will be accepted for these components.
E  INSTALLATION
Systems, equipment and devices should be installed by competent tradesmen, skilled in this class of installation.

Systems should be installed in a manner that is consistent with the provisions and intent of the project specific Specifications, the Drawings, and the referenced Codes and Standards, and in accordance with equipment manufacturers’ written Specifications and instructions and these Standards.

Installation workmanship should be accomplished in a neat and professional manner, meeting industry standards.

F  ACCEPTANCE TESTING AND COMMISSIONING
On-site Acceptance Testing with witness by UCD, providing all personnel and equipment necessary to perform these tests, should be included in each project referencing work included in this standard.

Acceptance Testing should include operational verification and testing of all new and existing devices installed, modified and/or associated with the scope of this Project.

Security Management System Requirements
A  SMS SERVER AND SOFTWARE
The SMS server is existing. It resides on the UCD Ethernet infrastructure on a dedicated security VLAN. All ACS panels and devices specified for UCD projects shall be fully compatible with the SMS.

The configuration and programming of all panels and devices associated with a specific project shall be included as a requirement within that project. All configuration and programming shall be coordinated with UCD Police representatives and shall match the existing naming and classification schema.

B.  ACCESS CREDENTIALS
Access credentials (cards and fobs) are a foundational part of the ACS. UCD maintains, control over and issues multi-technology cards that function with existing 125MHz proximity card readers as well as newer Smart Card readers. Individual project designed and specified under these Standards should not need to provide access credentials within the scope of work.
C. ACS PANELS
In all circumstances ACS panels shall be fully compatible with and made operational within the existing SMS.

1. ACS Panels should have the following minimum characteristics:
   - ACS panels should be Ethernet capable, utilize an imbedded operating system to provide distributed ACS functionality.
   - ACS panels should be provided with proximity card reader interface capabilities, and input/output functionality.
   - ACS panels should be specified with appropriate panel power supplies, lock power supplies and isolation lock isolation relays. All power supplies should be provided with internal minimum 7amp-hour batteries.

2. Enclosure Tamper Switches
   - If not already equipped from the factory, all ACS panel, power supply and ancillary board enclosures should be equipped with an enclosure tamper switch.
   - Tamper switches should be single-pole, single throw (SPST) units to provide supervision of enclosure doors.
   - Tamper switches shall be tested and proven capable of initiating an alarm signal when the protected door is opened 3/8” on the latch side.
   - Tamper switch should be installed inside the enclosure.

D. ACS and BIAS FIELD DEVICE HARDWARE REQUIREMENTS
1. Card Reader
   - The reader is available in a variety of form factors. The particular form factor that is most suitable to the installation environment should be specified on a per project basis.
   - The reader should be capable of reading and processing the contactless Smart Card and Wiegand Proximity technologies as utilized by UCD.
   - The reader should be read when presented in any orientation or at any angle to the surface of the reader (minimum read range: 3.5”).
   - The reader should power the card, process the encoded data, and output the data to the access system in less than 175 milliseconds.
   - The readers should have an audible "beep" tone feature to indicate to the user that the card or tag was read.
• Accidental or intentional transmission of radio frequency signals into the reader should not compromise the system.
• Damage or vandalism to the reader should not damage any other part of the access control system.
• Individual card reader finishes and colors should be coordinated with the Project Architect and UCD.

2. Door Position Switches/Alarm Contact
• Switches should be single-pole, double throw (SPDT) unit to provide single circuit operation suitable for a line supervision.
• Switches should be capable of initiating an alarm signal when the protected door is opened 1” on the latch side.
• Recessed switches and magnets should be a minimum of 3/8” diameter and a maximum of 1” diameter.
• Surface mount switches should be mounted to door headers and the associated magnet shall be surface mounted to the door.
• Surface mount contacts and magnets should have aluminum housings and be equipped with an armored cable jacket.
• Overhead door contacts should be floor mounted and the associated magnet should be surface mounted to the overhead door.
• Overhead door contacts and magnets should have aluminum housings and be equipped with an armored cable jacket.

3. Request-to-Exit (REX) Devices
• Where feasible, REX devices should be supplied integral with electronic door hardware as defined in the door hardware standards as specified in and coordinated with Division 8.
• REX switches should be single-pole, single throw (SPST) dry micro switch.
• In circumstances where it is not feasible for the REX to be integral with the door hardware, a passive infrared motion sensor should be specified.
• Passive infrared REX devices should have an adjustable detection curtain, set to reliably activate prior to an individual exiting but to minimize incidental activation from passersby.
• Individual passive infrared finishes and colors should be coordinated with the Project Architect and UCD.
• In circumstances where neither an integral REX nor passive infrared REX is suitable for installation, a push button REX should be utilized.
• REX push button should be mounted to a double gang steel face plate engraved with the words “Push to Release” and the plate shall be installed onto an existing stainless steel pedestal at the applicable door location.
• REX push button should include a DPST dry relay switch.
• REX push button should include a pneumatically controlled adjustable (2-60 seconds) time delay reset.

4. Hardwired Electric Locks
• Hardwired electric locks should be electrified mortise, cylindrical, strike, rim device, exit device and/or electromagnetic lock as defined by the door hardware standard.
• Locks should operate at 24 VDC.
• Locks should have integral REX switch wherever practical.
• Locks should be provided with appropriate wire transfer or electrified door hinge.
• Locks should be fail-secure.

5. Wireless Electric Locks
• For medium security applications wireless electric locks should be utilized.
• Trim and finish of electric locks should match UCD hardware standards per the project specific requirements and specifications.
• Wireless locks should incorporate proximity card reader, door position switch and REX device.

6. Emergency Door Release (EDR):
• EDR should be used in conjunctions with electromagnetic locks where required by local fire code.
• EDR should be mounted to a single gang stainless steel face plate engraved with the words" Emergency Release".
• EDR should include a 1-9/16” Red mushroom activation button.
• EDR should include a pneumatically controlled adjustable (2-60 seconds) time delay reset.
• EDR should include a DPST dry relay switch with one pole hardwired to locally interrupt lock power and the other pole hardwired to the ACS panel and configured as a hardwired input.

7. Motion Detectors
• Motion detectors should be used to provide internal area alarm detection on a time scheduled basis.
• Motion detector should utilize microwave and passive infrared technology to reduce false alarms.
• Motion detector should be surface or flush mount in a standard double gang junction box.

8. Glass Break Detector
• Glass break detectors should be used to provide internal area alarm detection of intrusion attempts through exterior/perimeter glass.
• Glass break detectors should provide low and high frequency detection to reduce the likelihood of false alarms.
• Glass break detectors should be zoned within rooms when complete glass protection requires multiple devices.

9. Microwave Beam Detectors
• Microwave beam detectors should be used to provide internal area alarm detections of intrusion attempts through shy lights, glass roof panels, and/or high ceiling windows that are accessible from the exterior.
• Microwave beam detectors are typically long range devices that include an active unit at one end and a passive unit at the other.
• Where microwave beam detectors are required, infrastructure and architectural coordination will be required.

10. Local Alarm Horn:
• Some perimeter exit doors may be designated as “Emergency Exit Only” and will be equipped with door positions switches/alarm contacts.
• Upon a violation of an emergency exit door, a local horn should be provided to activate a high level sounder. The horn should continue to sound until expiration of the pre-determined software dwell time.
- Horn should deliver a minimum +/-90 peak db.
- Horn must have a sound that is distinguishable from the fire alarm system.

**Video Surveillance System Requirements**

**A. VSS SERVER**

The VSS server is existing. It resides on the UCD Ethernet infrastructure on a dedicated security VLAN. All VSS devices specified in and provided for UCD projects shall be fully compatible with the VSS.

Supplemental server hardware may be required to support the cameras installed as part of the VSS on a given project. When that is the case, the hardware should be provided to exceed the minimum specified requirements for such hardware as published by the manufacturer at the time of design and specification.

The VSS requires each camera in the system to be licensed. Add-on camera licenses should be specified within each project design to accommodate the cameras specified within that particular project.

The configuration and programming of all devices associated with a specific project shall be included as a requirement within that project. All configuration and programming shall be coordinated with UCD representatives and shall match the existing naming and classification schema.

**C. VSS DATA STORAGE**

Video data consumes a considerable amount of digital storage. It also requires a considerable amount of network bandwidth, in relation to other network system, to stream video. Therefore, VSS data storage needs to be provided on a per project basis in the form of Network Video Recorders (NVR). The specified storage should be capable of storing all video data, from all project related cameras for a minimum of 30 days, at the following (per-camera) parameters:

- Maximum specified camera resolution
- Minimum four (4) image per second continuous recording
- Minimum fifteen (15) images per second event recording, for the event duration and 10 seconds pre and post event.
D CAMERAS
In all circumstances VSS cameras shall be fully compatible with and made operational within the existing VSS. Specified cameras should meet or exceed the following:

- Cameras should utilize TCP/IP Ethernet with a codex compatible with the existing VSS.
- Cameras should be powered with Ethernet PoE.
- Cameras should use a high resolution, progressive scan, 1/3-inch or greater CMOS imager that provide minimum HD720 (1280x720) pixel resolution.
- Camera resolution should be use based with a minimum HD720 resolution.
- Cameras should be provided with auto-iris, vari-focal lenses with a range applicable to capture the desired field of view.
- Interior cameras should be suitable for interior installation environments.
- Exterior cameras should be suitable for exterior installation environments and should be provided with integral heaters/blowers/seals/etc. necessary to operate in the applicable exterior environment.
- Camera should be as discreet as possible and color, finish and form factor should be closely coordinated with the project architect to balance use and function while maintaining the desired aesthetic of the facility.
This section details the standard protocol to be followed when designing and deploying the SMS sub-system and devices identified in this document. The protocol should be applied to new building, site improvements, and renovations. Deployment considerations include three levels of protection, designated low, medium and high. Such designation can be applied to a room, internal area, or building.

High Security Designation

A  DEFINITION

High security areas are those that require electronic security devices to provide system monitoring capabilities on a real-time basis. Devices installed in high security areas should be hardwired to ACS and/or BIAS panels or VSS network switch (as appropriate to the specific device) and should be configured and programmed to provide instantaneous alarm/video notification either 24/7 or on a schedule as defined by and coordinated with UCD. Examples of such areas include:

- Ground level access to the first floor building perimeter.
- Computer rooms/data centers
- MDF/MPOE
- High value laboratories
- Administrative areas where cash is transacted
- Senior Administrative Offices
- Physical and electronic records storage areas
- Other locations as defined and designated by UCD

B  ACS DEPLOYMENT

The deployment of ACS devices for high security designated areas includes hardwired access controls for the doors that lead into these areas. Hardwired access control doors should include four devices, at a minimum:

- Proximity card reader
- Door position switch/alarm contact
- Electronic lock
- Request-to-Exit device
Doors can also include other ancillary devices, as defined within the door hardware requirements, which should be integrated with the ACS when applied to high security areas. These may include:

- Automatic openers
- ADA openers
- ADA buttons
- Exit devices
- Remote door release buttons

All electronic door hardware devices should be included within the Division 8 specifications for any given project. The security specification should call for close coordination with Division 8. These devices should be electronic version of the locking hardware and devices as defined within the UCD door hardware standard. Whenever feasible, the request-to-exit device should be included as an integral feature of the electronic door hardware. Request-to-exit devices shall not preclude exiting from the interior or require the use of a key, any special knowledge or effort. All security requirements shall conform to California Building Code 1003.3.1.

C  BIAS DEPLOYMENT

BIAS devices can be hardwired or wireless and should be connected to either the ACS or BIAS panel as appropriate to the project. BIAS devices include:

- Door position switch/alarm contact
- Glass Break Detectors
- Motion Detectors
- Beam detectors
- Sonic detectors
- Hold-up Buttons
- Lockdown Buttons
- Duress/Panic Buttons
- Other devices as directed by the UCD

Door position switch/alarm contact should be used on all doors that lead into high security areas but that do not require access control functionality. Furthermore, regular use of the door should be discouraged to prevent nuisance alarms. Therefore, they should be keyed to a building master or grandmaster, in accordance with UCD keying standard.
Glass Break Detectors should be used within high security areas that may be accessible breaking a window, sidelight, or glass panel. The detector should be selected for the particular glass installed. The use of glass break detectors is preferable since they can be armed and operation 24/7 with little risk of false alarm but should be avoided in laboratory environments or other locations where there is a potential of incidental glass breaking. In these areas, motion detectors set on a time schedule of armed through the ACS or BIAS panel should be used.

Beam detectors or sonic detectors should be used to monitor possible intrusion into high security areas by means other than through doors and windows. Skylights, fiberglass wall panels, and block walls are some examples.

Hold-up/panic buttons should be hardwired to the ACS or BIAS panel and should be included in the following locations:

- Financial transaction counters/registers
- Admissions and Records
- Financial Aid
- Library
- Counseling
- Dean’s/Chancellor’s Offices
- Other locations as designated by the UCD

Lockdown button should be hardwired to the ACS or BIAS panel. Lockdown buttons should be configured to lockdown the room, area, floor or building as designated by UCD. In addition, lockdown buttons must be configured as a high priority alarm within the SMS and should be configured to annunciate until acknowledged by a police dispatcher/operator. Lock down buttons that are not primarily designated as hold-up/panic buttons should be included in the following locations:

- Classrooms
- Office reception desks
- Select administrative offices
- Any other area as designated by the UCD

Duress buttons may be hardwired or wireless. While hardwired duress buttons should be used when feasible, wireless buttons are acceptable when hardwiring is not possible or is impractical. Duress buttons are devices that notify police dispatchers of a duress situation is a location
where money is not transacted or where lockdown is not required as a result of button activation. Duress button should be included in the following locations:

- Individual administrative offices where designated by UCD
- Individual faculty offices where designated by UCD
- Locker rooms
- Dressing rooms
- Any other locations as designated by UCD

D VSS DEPLOYMENT

VSS deployment for high security areas chiefly involves the installation of IP based, high definition cameras at strategic locations inside and outside of buildings. Cameras should be included in project designs wherever live and recorded video can effectively supplement ACS and BIAS devices. Typical locations include:

Main exterior pathways around buildings
- Exterior quads/gathering areas
- Exterior approaches to main building entrances
- Interior lobby/corridor/hallways at main entrances
- Interior office lobbies
- Book Store
- All interior counters/windows where duress and holdup buttons are installed which include, but are not limited to:
  - Financial transaction counters/registers
  - Admissions and Records
  - Financial Aid
  - Library
  - Counseling
  - Dean's/Chancellor's Offices
- Other areas as designated by UCD

Medium Security Deployment

A DEFINITION

Areas that require electronic security devices to provide system monitoring capabilities on a less than real-time basis are considered medium security. These areas should be equipped with devices that will provide alarm and event tracking data that are primarily used for
investigative purposes and that do not require immediate alarm annunciation and response. Primarily these
areas will be operational within the ACS and will be secured with wireless electronic locks that include integral proximity access control card readers, door status and request-to-exit switches. Video surveillance may be included for these areas as well, but only as directed by UCD. Examples of areas suitable for medium security deployment include:

- Smart classroom (except doors that lead to the building exterior)
- Classrooms that only have exterior doors
- Administration Office Suites and/or Doors (except doors that lead to the building exterior)
- Office with only have exterior door(s)
- IT/Data Closets
- Electrical Rooms
- Mechanical Rooms
- Other medium security rooms as directed by UCD

**Low Security Deployment**

**A DEFINITION**

Areas that require no electronic security protection but will require mechanical locks as defined in the door hardware standard. Examples of such areas include:

- Closets
- Conference/meeting rooms that do not have doors leading to the building exterior
- General storage rooms
- Offices
- All other rooms and areas not otherwise directed by UCD as medium or high security areas
I. Purpose

This section sets forth requirements and standards for the installation and use of electronic access control systems on all properties owned, leased, operated or maintained by UC Davis. The policy will impact systems that are centrally connected via wired or wireless infrastructure. Stand-alone systems are not impacted. The focus of this policy is to control perimeter entry points and high-risk rooms as warranted.

II. Policy

All new electronic access control systems that are on exterior access doors or other high-risk locations shall have the ability to be connected to the Campus Security Management System. When any currently deployed system is replaced it must be replaced with a new system that allows the Campus Security Management System to be the controlling platform. This policy includes all university owned property.

The Campus Security Management System will be controlled by the UC Davis Police Department.

III. Requirements

A. Approval for access control devices

1. The UC Davis Police Department will be the governing body to approve requests for the installation, maintenance and use of all card access control devices placed on property owned, leased, operated, or maintained by UC Davis for the purpose of security.
2. Following approval of a request for the installation of a card access-related device on property owned, leased, operated, or maintained by UC Davis, notification of the intent to install the card access control device shall be made by the Police Department to all parties having a recognized interest in card access monitoring including the Academic Senate, the Academic Federation, The Graduate Student Association, Associated Students of the University of California, union representatives and University administration.

B. Electronic Access Control systems will have the ability for full integration into the Campus Security Management System.

1. A campus standard as determined by the UC Davis Chief of Police shall be developed and employed concerning the type and quality of access control devices to be installed for security and access control monitoring purposes on all property owned, leased, operated, or maintained by UC Davis.
2. Upon adoption of this policy, all new plans for the installation or upgrade of any device whose purpose is to monitor or control any and all forms of building and room access shall be required to conform to the campus standard.
C. Monitoring, retention, release, and use of access control device records

1. Access control records shall be maintained for security purposes and shall be administered and maintained by the UC Davis Police Department.

2. All recorded entry and exit records shall be maintained by the UC Davis Police Department for the prevention, deterrence and investigation of criminal activity.
   a. Use for any other purpose will be prohibited unless otherwise sanctioned by the Chief of Police and University administration consisting of the Chancellor and/or Provost or his designee. If the entry and exit logs involve access by a member of the faculty as defined in APM Section 110-4(15), the Provost and Executive Vice Chancellor shall consult in writing with the Chair of the Academic Senate and the Academic Federation. The time period allowed for consultation shall be specified by the Provost and Executive Vice Chancellor and shall not exceed five (5) working days.
   b. Custody of entry and exit logs for security and criminal investigative purposes shall be solely under the control of the UC Davis Police Department. Entry and exit logs shall be maintained for at least thirty (30) days unless needed for evidentiary purposes.

3. Requests for any recorded entry and/or exit card access log providing evidence of the movement of any person on property owned, leased, operated, or maintained by UC Davis should be made in writing to the UC Davis Chief of Police. Release of recorded access card data shall be limited to the following:
   a. Any law enforcement entity having a valid subpoena, search or seizure warrant signed by a court of law.
   b. Any private entity having a valid subpoena signed by a court of law.
   c. Any campus entity having demonstrated a justifiable need approved by the Chief of Police and University administration consisting of the Chancellor and or Provost and/or his or her designee.
   d. As determined by the UC Davis Chief of Police.

D. Relinquishment of control of existing access control devices

Upon adoption of this policy, the oversight of all card access control devices shall be relinquished to the UC Davis Police Department. Should technical or financial issues delay the implementation of this requirement, all card access system administration shall be turned over to the UC Davis Police Department as soon as possible.

IV. Further Information
For further information contact the UC Davis Police Department (http://police.ucdavis.edu/ 530-752-1727).
I. Purpose

This section sets forth requirements and standards for the installation and use of video security devices on all property owned, leased, operated or maintained by UC Davis exclusive of the UC Davis Medical Center.

II. Policy

A. UC Davis respects the freedom, privacy and civil liberties of all individuals accessing university owned, leased, operated or maintained property. This policy is created to ensure the legal and ethical use of security related video on all property owned, leased, operated or maintained by UC Davis is in accordance with University policy and state and federal law.

1. All video recording devices that are used for prevention, deterrence, and investigation of criminal activity shall be governed by this policy.

2. All video images created for security purposes on UC Davis property are considered University property subject to this policy.

B. Video images and data taken on UC Davis property for security purposes shall be monitored and maintained exclusively by the UC Davis Police Department or the department’s written designees.

1. Access to video images and data will be limited to the Chief of Police or written designees or approved designees as defined within a Delegation of Authority document.

2. All images taken or recorded by UC Davis on its property for security purposes are the property of the University and may not be released without the written authorization of the UC Davis Chief of Police or designee.

3. This policy does not apply to video images taken for the purpose of research or any other purpose not related to University security.

III. Requirements

A. Approval for video recording devices for security purposes

1. UC Davis Police Department and its written designees are the sole entities authorized to approve requests for installation, maintenance, and continued use of all video recording devices placed on University property for the purpose of security including crime prevention, deterrence, and investigation.

2. The UC Davis Chief of Police, or designee, is responsible for reviewing each request to determine if the installation request for security cameras is consistent with University policy.

3. Following approval of a request for installation of a video recording device for security purposes by the UC Davis Police Department, notification of the intention to install cameras shall be made by the Police Department to all parties having a recognized interest in the request including the Academic Senate, Academic Federation, The Graduate Student
Association, Associated Students University of California, union representatives and University administration.

B. Standardization of security related video recording device equipment

1. A campus standard as determined by the UC Davis Chief of Police and the UC Davis Assistant Vice Chancellor of Facilities Management shall be developed concerning the type and quality of recording equipment to be installed for security purposes.

2. Upon adoption of this policy, all new requests for security camera installation should conform to the campus standard. New camera systems must be able to connect with the Campus Security Management System platform.

3. Video recording equipment that exists for security purposes that does not meet this standard will be reviewed for approval on a case by case basis by the UC Davis Chief of Police to determine if the inability to meet the campus standard shall detrimentally affect the health, safety or welfare of the UC Davis community.

4. Existing security-related video equipment that does not conform to the campus standard and does not pose a risk to campus safety, health, or welfare shall be permitted to be maintained until the equipment reaches the end of its service level life or effective life, when it will be replaced with conforming equipment. Equipment determined to be critical to matters of life and safety that cannot be made functional in accordance with the campus standard shall be replaced.

C. Location of and signage for security related video recording devices

1. Signage advising that an area is being recorded by video devices will be placed in all areas where video security recording will be in effect unless such signage is determined in a specific instance to be detrimental to a criminal investigation. Signage and notification are not required if a video-recorded event requires enhanced security.

2. The UC Davis Police Department shall determine where security cameras can be placed on University property in accordance with applicable laws relating to privacy and consistent with University rules and policies.

3. Primary locations for the installation of security cameras include but are not limited to the following:
   a. University owned, leased, operated or maintained property and buildings
   b. At access points for public rooms and laboratories containing high value equipment or information
   c. Buildings required to be monitored by law or regulation
   d. Public access areas
   e. Parking facilities
   f. Other areas targeted as part of a criminal investigation

4. Video recording equipment is not permitted in the following areas without a court order:
   a. Restrooms
   b. Locker rooms
   c. Residential bedrooms
d. Sensitive research

D. Monitoring, retention, release, and use of recorded images

1. All video recordings created for security purposes shall be monitored, maintained and used by the UC Davis Police Department or its written designee according to University policy and applicable federal and state laws.

2. Video monitoring will be conducted in a professional, ethical and legal manner, by operators trained in the proper use of the technology. Training will be periodic and consistent with industry standards, and includes technical, legal and ethical parameters for proper use.

3. All recorded images retained by UC Davis that are maintained for the primary purpose of investigation, prevention and deterrence of criminal activity by the UC Davis Police Department shall remain in the custody of the UC Davis Police Department or its designee.
   a. Use for any other purpose will be prohibited unless otherwise sanctioned by the Chief of Police and University administration, consisting of the Chancellor and/or Provost or his or her designee. If the recorded images involve a member of the faculty as defined in APM Section 110-4(15), the Provost and Executive Vice Chancellor shall consult in writing with the Chair of the Academic Senate and the Academic Federation. The time period allowed for consultation shall be specified by the Provost and Executive Vice Chancellor, and shall not exceed 5 working days.
   b. Custody of retained images for security and criminal investigative purposes will be under the control of the UC Davis Police Department or its written designee. Images are to be retained for at least thirty (30) days unless needed for evidentiary purposes.

4. Requests for access to recorded security-related media maintained as evidence by the UC Davis Police Department should be made in writing to the UC Davis Chief of Police. Release of images will be limited to the following:
   a. Any law enforcement entity having a valid subpoena, search or seizure warrant signed by a court of law.
   b. Any private entity having a valid subpoena signed by a court of law.
   c. Any campus entity having demonstrated a justifiable security need approved by the Chief of Police and University administration consisting of the Chancellor and/or Provost or his or her designee.
   d. As determined by the video policy review committee or the UC Davis Police Department.

5. Information obtained in the course of legitimate law enforcement review may be used to support disciplinary proceedings against faculty, staff, and/or students.

E. Relinquishment of existing video recording equipment

The monitoring of all video recording equipment in use on property owned, leased, operated or maintained by UC Davis for the purpose of security shall be relinquished to the UC Davis Police Department unless otherwise permitted by the UC Davis Chief of Police. Requests to continue the use of video recording equipment shall be made in writing to the UC Davis Chief of Police and shall specify the type of equipment being used and the intended purpose for recording. Written approval will be granted on a case by case basis for a renewable period not to exceed two (2) years.
F. Designees authorized by the UC Davis Chief of Police to conduct video recording

The UC Davis Chief of Police may authorize and designate specific entities on campus to conduct video recording in matters not considered to involve significant criminal activity. This authorization shall be in writing and shall specifically set forth the type of activity being monitored and the intended purpose for which the video will be used. Applicants requesting to be designees shall submit a request in writing to the UC Davis Chief of Police specifying the type of activity to be recorded, the location of cameras and the intended use of video recordings. Written approval will be granted on a case by case basis for a renewable period not to exceed two (2) years.

Annual Video Policy Review

A committee shall be established for the purpose of annually reviewing this policy and reviewing the placement of cameras that have occurred during the preceding year. Included on this committee shall be members of the Academic Senate, the Academic Federation, Staff Assembly, The Graduate Student Association, Associated Students University of California, union representatives, Facilities Management, Division of Student Affairs, Student Housing, UC Davis Stores, Campus Recreation and Unions, University Administration and the UC Davis Police Department.

IV. Further Information

For further information contact the UC Davis Police Department (http://police.ucdavis.edu; 530-752-1727).
Card Access Services Analyst

1. Job Summary

Involves the management, long-range planning, organization, coordination, oversight and/or performance of multiple operational activities and services for one or more buildings, including space planning, general maintenance, call center triage and tracking of repair services, move planning and coordination, development of procedures, policies and communications related to infrastructure and safety. (For Facilities Project Management, see Facilities Development/EH&S Job Field.)

2. Scope

Generic Scope (Uniform across all jobs at this level - do not modify): Professional who applies acquired job skills, policies, and procedures to complete substantive assignments/projects/tasks of moderate scope and complexity; exercises judgment within defined guidelines and practices to determine appropriate action.

Custom Scope: Applies campus policies and procedures to resolve a variety of facilities management issues. Works on facilities management problems of moderate scope where analysis of situations or data requires a review of a variety of factors.

3. Key Responsibilities

<table>
<thead>
<tr>
<th>% of time</th>
<th>Essential Function (Yes/No)</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>Yes</td>
<td>Manage and supervise Card Access Services Unit staff. Ensure staff have adequate resources to create new access cards, student identification cards, and employee identification cards. Audit access card users as needed. Schedule staff to meet unit and University operational needs. Provide direction to unit to ensure staff meets unit and University operational needs. Mentor, train, and evaluate unit staff.</td>
</tr>
<tr>
<td>15</td>
<td>Yes</td>
<td>Manage campus-wide card access systems located in the card access services office. Ensure card access services office equipment operates properly with host systems. Update systems, software, and database information on a daily basis. Interact with applicable IT groups, Facilities, Auxiliary Services, outside campus departments, and/or outside vendors for system maintenance, hardware firmware updates, and software updates. Make recommendations and provide solutions to applicable parties to enhance or improve card access services office system operation. Research emerging trends in card access security. Ensure card access security systems adhere to campus policies and procedures.</td>
</tr>
</tbody>
</table>
4. Knowledge and Skills

- Knowledge of UC Davis network infrastructure and design as applied to card access security.
- Project management skills to develop card access services office projects.
- Experience using word processing, spreadsheet, presentation, and office applications.
- Experience writing professional correspondence and reports.
- Experience using professional interpersonal communication skills to interact with all members of the campus community, using tact and diplomacy.
- Experience mentoring and directing students and/or career staff in a supervisory capacity.
- Demonstrated experience using organizational, analytical, and problem solving skills.
- Demonstrated experience with card access systems, equipment, software, transmission methods, and troubleshooting.

5. Education and Training

Education/Training:

- Bachelor’s degree in related area and/or equivalent experience/training

Licenses or certifications, if any:

- California Driver’s license

Special Conditions of Employment:

- Must pass criminal background check
- Must participate in California DMV Driver Pull Notice program

6. Problem Solving

Common problems solved by the employee:

- Troubleshoot card access office equipment and system functionality.
- Utilize database to maintain and track inventory of card access system users.
- Manage unit staff scheduling to maintain card access office staffing levels.
- Manage and collaborate with multiple vendors to install and repair card access office systems.
Unusual or complex problems solved by the employee:

- Ensure unit staff receive adequate training and resources to maintain unit operations.
- Review, document, and provide corrective action for employee disciplinary issues.
- Manage periods of high demand for access cards; such as, freshman student orientation.

Problems/situations that are referred to this employee's supervisor:

- Purchasing authorizations.
- Vendor identification and selection.
- Significant employee disciplinary issues.
- Unique situations not covered by policy.

Please follow your department's or division's procedures for management review and then submit to your Department HR Manager.

**Document Retention**

Review the job description with the employee before submitting it and annually thereafter at the time of the employee's performance evaluation. Sign and date below and place a copy in the personnel file.

(Signature below is only required for hard-copy retention within the department. Electronic submission does not require signatures.)

<table>
<thead>
<tr>
<th>Supervisor Name:</th>
<th>Supervisor Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Signature:</td>
<td>Supervisor Signature:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Job Summary

Involves the management, long-range planning, organization, coordination, oversight and/or performance of multiple operational activities and services for one or more buildings, including space planning, general maintenance, call center triage and tracking of repair services, move planning and coordination, development of procedures, policies and communications related to infrastructure and safety. (For Facilities Project Management, see Facilities Development/EH&S Job Field.)

2. Scope

Generic Scope (Uniform across all jobs at this level - do not modify): Professional who applies acquired job skills, policies, and procedures to complete substantive assignments/projects/tasks of moderate scope and complexity; exercises judgment within defined guidelines and practices to determine appropriate action.

Custom Scope: Applies campus policies and procedures to resolve a variety of facilities management issues. Works on facilities management problems of moderate scope where analysis of situations or data requires a review of a variety of factors.

3. Key Responsibilities

<table>
<thead>
<tr>
<th>% of time</th>
<th>Essential Function (Yes/No)</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Yes</td>
<td>Manage campus-wide electronic alarm systems that monitor intrusion and fire alarm devices. Ensure that electronic alarm systems operate properly with host systems. Update systems, software, and database information on a daily basis. Interact with applicable IT groups, Facilities, Auxiliary Services, outside campus departments, and/or outside vendors for system maintenance, hardware firmware updates, and software updates. Make recommendations and provide solutions to applicable parties to enhance or improve electronic alarm system operation. Coordinate preventative maintenance program with appropriate departments. Research emerging trends in electronic alarm systems. Ensure electronic alarm systems adhere to campus policies and procedures.</td>
</tr>
<tr>
<td>25</td>
<td>Yes</td>
<td>Manage electronic alarm system repairs and new system installation projects in other than new construction on campus. Troubleshoot electronic system operation by generating electronic alarm system reports, contacting system owners, and/or contacting emergency responders on site. Make recommendations for electronic alarm system equipment installation based on site survey and/or building plan review. Ensure new system installation conforms to campus policies and procedures. Utilize false alarm</td>
</tr>
<tr>
<td>Task</td>
<td>Rating</td>
<td>Response</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Coordinate monthly electronic intrusion alarm monitoring and excess false alarm billing. Generate monthly excess false alarm report and reconcile excess false alarm billing invoices. Notify billing contacts of excess false alarm charges. Submit monthly billing reports to business office for processing. Independently resolve billing disputes.</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Support and assist Design and Construction Management project managers on varying projects requiring electronic intrusion alarm systems. Support and assist throughout the planning, design, and close out phases; including, but not limited to: maintaining project documentation and logs, reviewing contract documents and change orders, reviewing project progress and assisting with inspection, drafting and reviewing project schedules, budgets, construction documents, and estimates. Provide building plan review analysis as related to electronic intrusion alarm system design and deployment.</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Develop and provide electronic alarm system training to police personnel, Facilities, Auxiliary Services, and/or outside departments. Oversees and ensures all training and close-out documentation meets project contract requirements and are properly turned over to the appropriate entity; including warranties, site plan drawings, and applicable reference manuals.</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Assist the Card Access Analyst as needed; including, but not limited to: system maintenance, approval, and updates.</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Assist the Security Analyst complete security assessments of various UC Davis facilities.</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Assist the Video Security Analyst as needed; including, but not limited to: system approval, maintenance, updates, and archiving.</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Assist the Security Director with the annual video security review. Assist in sharing information and coordinating meetings with the video security policy committee.</td>
<td>100%</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 4. Knowledge and Skills

- Knowledge of building construction, design, construction contract administration, and California Building Codes.
- Knowledge of UC Davis network infrastructure and design as applied to electronic alarm system deployment.
- Project management skills to develop project scope and drawings.
- Experience using word processing, spreadsheet, presentation, and office applications.
- Experience writing professional correspondence and reports.
- Experience using professional interpersonal communication skills to interact with executive leadership.
- Demonstrated experience using organizational, analytical, and problem solving skills.
- Demonstrated experience with electronic alarm systems, equipment, software, transmission methods, and troubleshooting.

### 5. Education and Training

**Education/Training:**
- Bachelor’s degree in related area and/or equivalent experience/training

**Licenses or certifications, if any:**
- California Driver’s license
Special Conditions of Employment:

- Must pass criminal background check
- Must participate in California DMV Driver Pull Notice program

6. Problem Solving

Common problems solved by the employee:

- Troubleshoot electronic alarm system equipment and system functionality.
- Utilize database to maintain and track inventory of electronic alarm systems throughout the campus and health system.
- Manage and collaborate with multiple vendors to install and repair electronic alarm systems.
- Review construction blueprints and specifications to ensure compatibility of planned electronic intrusion alarm systems with campus design guide.

Unusual or complex problems solved by the employee:

- Load site maps and/or blueprints into electronic alarm system software for tracking and system use.
- Install electronic alarm system software updates which require review of entire system to verify integrity of upgrade.

Problems/situations that are referred to this employee's supervisor:

- Purchasing authorizations.
- Vendor identification and selection.
- Unique situations not covered by policy.

Please follow your department's or division's procedures for management review and then submit to your Department HR Manager.

Document Retention

Review the job description with the employee before submitting it and annually thereafter at the time of the employee's performance evaluation. Sign and date below and place a copy in the personnel file.

(Signature below is only required for hard-copy retention within the department. Electronic submission does not require signatures.)

<table>
<thead>
<tr>
<th>Supervisor Name:</th>
<th>Supervisor Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Name:</td>
<td>Supervisor Name:</td>
</tr>
<tr>
<td>Signature:</td>
<td>Supervisor Signature:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Job Summary

Involves the management, long-range planning, organization, coordination, oversight and/or performance of multiple operational activities and services for one or more buildings, including space planning, general maintenance, call center triage and tracking of repair services, move planning and coordination, development of procedures, policies and communications related to infrastructure and safety. (For Facilities Project Management, see Facilities Development/EH&S Job Field.)

2. Scope

Generic Scope (Uniform across all jobs at this level - do not modify): Professional who applies acquired job skills, policies, and procedures to complete substantive assignments/projects/tasks of moderate scope and complexity; exercises judgment within defined guidelines and practices to determine appropriate action.

Custom Scope: Applies campus policies and procedures to resolve a variety of facilities management issues. Works on facilities management problems of moderate scope where analysis of situations or data requires a review of a variety of factors.

3. Key Responsibilities

<table>
<thead>
<tr>
<th>% of time</th>
<th>Essential Function (Yes/No)</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Yes</td>
<td>Manage campus-wide card access systems. Ensure that card access equipment operates properly with host systems. Update systems, software, and database information on a daily basis. Interact with applicable IT groups, Facilities, Auxiliary Services, outside campus departments, and/or outside vendors for system maintenance, hardware firmware updates, and software updates. Make recommendations and provide solutions to applicable parties to enhance or improve card access system operation. Coordinate preventative maintenance program with appropriate departments. Research emerging trends in card access security. Ensure card access security systems adhere to campus policies and procedures.</td>
</tr>
<tr>
<td>25</td>
<td>Yes</td>
<td>Manage card access system repairs and new system installation projects in other than new construction on campus. Review and submit invoices for payment of vendor invoices to Director. Maintain relationships with vendors to ensure warranty work is completed on new systems within the warranty period. Make recommendations for card access system equipment installation based on site survey and/or building plan review. Ensure new system installation conforms to campus policies and procedures.</td>
</tr>
<tr>
<td>15</td>
<td>Yes</td>
<td>Respond to requests to archive confidential card access logs, maintaining sensitivity and exercising discretion. Respond to subpoenas requesting card access logs. Provide card access logs to appropriate UC Davis Police personnel; including, but not limited to: detectives, police officers, and police administration, as needed. Approve requests for card access logs to be released to non-law enforcement affiliates.</td>
</tr>
<tr>
<td>10</td>
<td>Yes</td>
<td>Support and assist Design and Construction Management project managers on varying projects requiring card access systems. Support and assist throughout the planning, design, and close out phases; including, but not limited to: maintaining project documentation and logs, reviewing contract documents and change orders, reviewing project progress and assisting with inspection, drafting and reviewing project schedules, budgets, construction documents, and estimates. Provide building plan review analysis as related to card access system design and deployment.</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>Develop and provide card access system training to police personnel, Facilities, Auxiliary Services, and/or outside departments. Oversees and ensures all training and close-out documentation meets project contract requirements and are properly turned over to the appropriate entity; including warranties, site plan drawings, and applicable reference manuals.</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>Assist the Security Alarm Analyst as needed; including, but not limited to: system maintenance, approval, updates, and billing.</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>Assist the Security Analyst complete security assessments of various UC Davis facilities.</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>Assist the Video Security Analyst as needed; including, but not limited to: system approval, maintenance, updates, and archiving.</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>Assist the Security Director with the annual video security review. Assist in sharing information and coordinating meetings with the video security policy committee.</td>
</tr>
</tbody>
</table>

4. **Knowledge and Skills**

- Knowledge of building construction, design, construction contract administration, and California Building Codes.
- Knowledge of UC Davis network infrastructure and design as applied to card access security.
- Project management skills to develop project scope and drawings.
- Experience using word processing, spreadsheet, presentation, and office applications.
- Experience writing professional correspondence and reports.
- Experience using professional interpersonal communication skills to interact with executive leadership.
- Demonstrated experience using organizational, analytical, and problem solving skills.
- Demonstrated experience with card access systems, equipment, software, transmission methods, and troubleshooting.

5. **Education and Training**

**Education/Training:**
- Bachelor’s degree in related area and/or equivalent experience/training

**Licenses or certifications, if any:**
- California Driver’s license

**Special Conditions of Employment:**
- Must pass criminal background check
- Must participate in California DMV Driver Pull Notice program
6. Problem Solving

Common problems solved by the employee:

- Troubleshoot card access equipment and system functionality.
- Utilize database to maintain and track inventory of card access systems throughout the campus and health system.
- Manage and collaborate with multiple vendors to install and repair card access systems.
- Review construction blueprints and specifications to ensure compatibility of planned card access with campus design guide.

Unusual or complex problems solved by the employee:

- Load site maps and/or blueprints into card access software for tracking and system use.
- Install card access system software updates which require review of entire system to verify integrity of upgrade.

Problems/situations that are referred to this employee’s supervisor:

- Purchasing authorizations.
- Vendor identification and selection.
- Unique situations not covered by policy.

Please follow your department's or division's procedures for management review and then submit to your Department HR Manager.

Document Retention

Review the job description with the employee before submitting it and annually thereafter at the time of the employee's performance evaluation. Sign and date below and place a copy in the personnel file.

(Signature below is only required for hard-copy retention within the department. Electronic submission does not require signatures.)

<table>
<thead>
<tr>
<th>Supervisor Name:</th>
<th>Supervisor Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Signature:</td>
<td>Supervisor Signature:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Job Summary

Involves the management, long-range planning, organization, coordination, oversight and/or performance of multiple operational activities and services for one or more buildings, including space planning, general maintenance, call center triage and tracking of repair services, move planning and coordination, development of procedures, policies and communications related to infrastructure and safety. (For Facilities Project Management, see Facilities Development/EH&S Job Field.)

2. Scope

Generic Scope (Uniform across all jobs at this level - do not modify): Professional who applies acquired job skills, policies, and procedures to complete substantive assignments/projects/tasks of moderate scope and complexity; exercises judgment within defined guidelines and practices to determine appropriate action.

Custom Scope: Applies campus policies and procedures to resolve a variety of facilities management issues. Works on facilities management problems of moderate scope where analysis of situations or data requires a review of a variety of factors.

3. Key Responsibilities

<table>
<thead>
<tr>
<th>% of time</th>
<th>Essential Function (Yes/No)</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Yes</td>
<td>Manage campus-wide video systems. Ensure that video cameras operate properly with host systems. Update systems, software, and database information on a daily basis. Interact with applicable IT groups, Facilities, Auxiliary Services, outside campus departments, and/or outside vendors for system maintenance, hardware firmware updates, and software updates. Make recommendations and provide solutions to applicable parties to enhance or improve video system operation. Coordinate preventative maintenance program with appropriate departments. Research emerging trends in video security. Ensure video security systems adhere to campus policies and procedures.</td>
</tr>
<tr>
<td>20</td>
<td>Yes</td>
<td>Oversee and supervise Video Security Unit staff. Ensure staff have adequate resources for active and passive video monitoring. Schedule staff to meet unit and University operational needs. Provide direction to unit to ensure staff meets unit and University operational needs. Mentor, train, and evaluate unit staff.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
|15| Yes| Manage video system repairs and new system installation projects in other than new construction on campus. Review and submit invoices for payment of vendor invoices to Director. Maintain relationships with vendors to ensure warranty work is completed on new systems within the warranty period. Make recommendations for video system equipment and camera placement based on site survey and/or building plan review. Ensure new system installation conforms to campus policies and procedures.
|10| Yes| Respond to requests to archive confidential security video recordings, maintaining sensitivity and exercising discretion. Respond to subpoenas requesting security video recordings. Provide security video recordings to appropriate UC Davis Police personnel; including, but not limited to: detectives, police officers, and police administration, as needed. Approve requests for recordings to be released to non-law enforcement affiliates.
|5| Yes| Support and assist Design and Construction Management project managers on varying projects requiring video security. Support and assist throughout the planning, design, and close out phases; including, but not limited to: maintaining project documentation and logs, reviewing contract documents and change orders, reviewing project progress and assisting with inspection, drafting and reviewing project schedules, budgets, construction documents, and estimates. Provide building plan review analysis as related to video security system design and deployment.
|5| Yes| Develop and provide video software system training to police personnel, Facilities, Auxiliary Services, and/or outside departments. Oversees and ensures all training and close-out documentation meets project contract requirements and are properly turned over to the appropriate entity; including warranties, site plan drawings, and applicable reference manuals.
|5| Yes| Assist the Security Alarm Analyst as needed; including, but not limited to: system maintenance, approval, updates, and billing.
|5| Yes| Assist the Security Analyst complete security assessments of various UC Davis facilities.
|5| Yes| Assist the Security Director with the annual video security review. Assist in sharing information and coordinating meetings with the video security policy committee.
|5| Yes| Other duties as assigned|
|100%|   |   |

4. **Knowledge and Skills**
   - Knowledge of building construction, design, construction contract administration, and California Building Codes.
   - Knowledge of UC Davis network infrastructure and design as applied to video security.
   - Project management skills to develop project scope and drawings.
   - Experience using word processing, spreadsheet, presentation, and office applications.
   - Experience writing professional correspondence and reports.
   - Experience using professional interpersonal communication skills to interact with executive leadership.
   - Experience mentoring and directing students and/or career staff in a supervisory capacity.
   - Demonstrated experience using organizational, analytical, and problem solving skills.
   - Demonstrated experience with video surveillance systems, equipment, software, transmission methods, and troubleshooting.

5. **Education and Training**

   **Education/Training:**
   - Bachelor’s degree in related area and/or equivalent experience/training

   **Licenses or certifications, if any:**
   - California Driver’s license
Special Conditions of Employment:

- Must pass criminal background check
- Must participate in California DMV Driver Pull Notice program

6. Problem Solving

**Common problems solved by the employee:**
- Troubleshoot video connectivity, camera functionality, system functionality.
- Utilize database to maintain and track inventory of video systems throughout the campus and health system.
- Manage unit staff scheduling to maintain video monitoring staffing levels.
- Manage and collaborate with multiple vendors to install and repair video systems.
- Review construction blueprints and specifications to ensure compatibility of planned video security with campus design guide.

**Unusual or complex problems solved by the employee:**
- Configure video analytics to maximize intrusion detection.
- Load site maps and/or blueprints into video security software for tracking and system use.
- Install video management updates which require review of entire system to verify integrity of upgrade.
- Ensure unit staff receive adequate training and resources to maintain unit operations.
- Review, document, and provide corrective action for employee disciplinary issues.

**Problems/situations that are referred to this employee's supervisor:**
- Purchasing authorizations.
- Vendor identification and selection.
- Significant employee disciplinary issues.
- Unique situations not covered by policy.

Please follow your department's or division's procedures for management review and then submit to your Department HR Manager.

**Document Retention**

Review the job description with the employee before submitting it and annually thereafter at the time of the employee's performance evaluation. Sign and date below and place a copy in the personnel file.

(Signature below is only required for hard-copy retention within the department. Electronic submission does not require signatures.)

<table>
<thead>
<tr>
<th>Supervisor Name:</th>
<th>Supervisor Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Signature:</td>
<td>Supervisor Signature:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>