2.4 Physical Access Control and Security System Policy

Policy Statement
University of Georgia (UGA) employees shall take every reasonable step to develop and implement effective physical access control and security systems procedures in order to facilitate safety, and instill a culture of security throughout the University community.

Reason for policy
The objective of the University of Georgia’s Physical Access Control and Security Systems Policy is to provide structure for the utilization of the access control and security system solution utilized on campus. This system exists to support the safety of the University community. Safety is enhanced when each individual department and unit within the University emphasizes a culture of security within their area of responsibility. Clear policies and guidelines facilitate this collaborative endeavor.

Procedures
Individual departments of the University bear the responsibility for making day-to-day decisions regarding their overall building security. These decisions include establishing guidelines for qualifications required for access to buildings under their control, door lock schedules, and alarm activation and deactivation schedules. UGPD and FMD personnel are available for consultation on these matters, but the ultimate responsibility for security protocols for any individual building ultimately lies with the senior-most UGA administrator housed in that building, or overseeing the personnel housed in that building. These individual departmental protocols, must, however, conform to the guidelines set forth below.

Access Control Access Control Committee
Policy revisions, prioritization of conversion, and administrative decisions that affect the access control system configuration on the University campus will be reviewed and approved by a system Access Control Steering Committee (the “Access Control Committee”). The members of this committee will include representatives from:

- UGA Police Department (UGPD) – Chair
- Office of Emergency Preparedness (OEP)
- Environmental Safety Division (ESD)
- Enterprise Information Technology Services (EITS)
- Office of Information Security (OIS)
- Office of University Architects (OUA)
- Facilities Management Division (FMD)
- Auxiliary Services (UGACard)
- Office of the Provost
- Office of the VP for Research
- Athletic Association
System Criteria

All access control and security systems at the University, including those being installed in new construction, major renovation, or specifically added to an existing structure, shall conform to the following criteria:

Hardware:

- Mechanical locking or keyed systems shall conform to University construction standards, currently the BEST Access System. Door hardware, latches and other systems shall be compatible with these keyways.

- A computer-based card access system shall conform to the University standard currently selected for campus-wide control. The current product is “Andover”, but the University is moving to “Gentec.” Access features will include University standard building panels that will connect to the central computer, via University backbone, compatible door hardware, intrusion detection and other monitoring equipment, and sensors as defined by an appropriate security analysis.

- Additional levels of access control can be applied through use of compatible biometric devices, keypad devices, or other equipment as necessitated by the security analysis.

Software:

The software system utilized for the card access system will be the standard system University-wide. This will be operated on a server housed in the University computer operations center. Software support will be coordinated by Facilities Management Division (FMD) and regular software maintenance fees will be paid by FMD.

Building Components:

Door latching systems, operating controllers and other mechanical devices can be sourced from multiple vendor systems as long as they are compatible with the building panels, and meet with the architectural standards established by the Office of University Architects.

- Card reader devices must be compatible with the UGACard system; they can be either magnetic swipe readers, or proximity readers. (Note: if proximity readers are used, all respective users must be advised to request specific UGACards, as the standard UGACard does not currently include a “proximity chip.”)

- Biometric or key pad devices must be compatible with the building panels. Biometrics may include hand geometry readers or fingerprint readers, depending on the security assessment and implementation space available.

- Video monitoring devices can include either digital or analog cameras that record digitally. Implementation of video monitoring shall be approved by the Access Control Committee, and implementation shall include appropriate signage.

- Standards for security hardware sensors, control panels and dialers will be set by the Access Control Committee.

- There may be some areas of campus that will see the need for security systems that are not part of the card access system. Any security alarm system installed must conform to standards set by the Access Control Committee.

Construction and Maintenance

Construction:

Construction of the access control and security systems will be included in any new building design and/or in any major building renovation. It is the responsibility of the design official (e.g., OUA, FMD, Real Estate Foundation) to
ensure that the appropriate standards are met. Replacement of existing access control and security systems, whether mechanical or card access, shall be accomplished through a coordinated University system implementation managed by FMD. Prioritization of replacement will be accomplished as specified by the Access Control Committee.

Maintenance:

Maintenance of all resident instruction access control and security systems that comply with the University standard will be accomplished by FMD. FMD will not assume responsibility for maintenance of existing systems unless requested by and funded by current owners. For non-resident instruction facilities, the corresponding units will be fiscally responsible for maintenance of the access control and security system. These organizations can be supported by FMD through a maintenance agreement or may choose to use other means as appropriate.

It will be the responsibility of each department or unit to contact FMD, or the appropriate vendor, when issues with the security system or support equipment (telephone, telephone line, wiring, etc.) arise.

Exceptions:

There are some departments or units on campus that may have out-of-the-ordinary applications for card access and security related to their mission and their facility. In cases where a department or unit feels that there should be an exception, it is the department or unit head’s responsibility to notify the Access Control Committee of their needs and/or concerns. The Access Control Committee has the final approval for any and all exceptions. Any organization requesting a stand-alone system should formally submit to this committee in writing a “cause for exception” letter. All exceptions request must be reviewed for justification and merit.

Monitoring

Monitoring of the computer based access control and security systems will be the responsibility of the UGA Police Department. One of the major benefits of the compatible central system is the capability to view centrally the status of the access control system in buildings and to respond appropriately. The UGA PD will facilitate the monitoring of all compatible, computer access control and security systems (burglar/intrusion) through whatever option or options are most cost effective for the University.

Management of the Card Access System

Overall:

The UGA Police Department has overall responsibility for the management of monitoring and emergency control of the card access system. The UGPD will have “Master Key” privileges and control of emergency lockdown procedures. The UGPD management involvement will be limited to allow access in cases of emergencies (i.e. fire, flooding, medical, etc.), and to lock down facilities in an instance when the campus has been closed due to natural or man-made disasters. The UGPD will not assume any responsibilities from the departments or units within a building for opening or closing the facility, or for granting or denying access to card holders, and the UGPD cannot act as the fail-safe for after-hours access for event(s), delivery(s) or personnel who have forgotten the necessary items needed for access to the building.

Buildings:

Like current keyed procedures, building schedules and lockup arrangements will remain the responsibility of the senior administrator in each building. An appropriate staff member will need to be tasked and trained to coordinate building door schedules, and to approve individuals to access the building after normal business hours and access other administrative areas through the web interface.

Each person, who would normally receive a key to the building, will need to be added to the access list for the appropriate building or area. Access is accomplished by updating an individual’s building access authority on the central server. All university employees and students (UGACard holders) will be listed in the central server.
Instructions and implementation procedures will be conveyed to new employees during the orientation process. Visitors who require routine after-hours access to buildings (i.e. would normally be issued a building key) can be issued a visitor badge (non-UGA Card ID). These badges are available from the university ID card unit, are serialized, and must be controlled as any key would normally be. There will be a cost for these visitor cards just as there is a cost for a UGACard ID, and this cost will be the responsibility of the requesting department.

Certain buildings housing high profile units may require internal control of access without connection to the university network. It is the expectation that, where practical, the hardware and software vendors used throughout the University would be the default vendors for these units. Monitoring of access and mechanical systems failures for these units will be provided as required by the unit. Connection to the police system for intrusion alert can be accomplished via modem or communications to campus security directly from the unit staff. These exceptions to university-wide access and monitoring standards will be determined on a case by case basis.

**Coordination with Police and Facilities Management Resources**

Each alarmed facility must provide **at least** five (5) after hour/weekend contacts and is required to contact the University of Georgia Police Department when the need arises to change contact information. Alarm contacts must be responsive to calls and requests for input. Updated contact information should be given to the UGPD Assistant Communications Coordinator for Technology in a timely fashion, for example when faculty/staff retire or leave the department. Contact personnel shall not include anyone employed by the Physical Plant Division (as opposed to the actual department or unit of the University housed in the alarmed facility). Contact personnel shall provide **at least** one (1) after hour number in which they can be reached after business hours and on weekends. Contact personnel shall include the Department Head and other staff/faculty who have knowledge of the system and access to the WebClient interface for Andover / Genetec controlled buildings.

**System Maintenance and Work Orders**

The University of Georgia Police Department will **not** be responsible for alarmed facility service repairs or equipment problems/malfunctions. The Police Department will only be responsible for monitoring the facility’s alarm activations. The University of Georgia Facilities Management Division should be notified immediately by individual departments for alarm malfunctions. When maintenance is needed for a system, a work order should be completed through the work orders website. For Andover / Genetec related issues, employees can also contact someone in FMD IT through andover@fmd.uga.edu or 706-542-7551 if there is an issue that cannot be handled with a work order.

**Alarm Protocol:**

- When an alarm is received by the University of Georgia Police Department, an officer is sent to respond.
  - If the responding police officer arrives on scene and cannot identify a clear cause for an alarm that alleviates any need for concern, the alarm contact will be called. When an alarm contact is called they will be asked to make a decision: the contact can either 1) respond to the alarm and meet officers on scene to make sure that everything is as it should be; or 2) choose to follow up the next business day with the Assistant Communications Coordinator for Technology.
  - If faculty/student/staff are found in the building, are reasonably understood to be the cause of the alarm, and no other suspicious circumstances are noted, then a contact will not be called, but will receive a follow-up e-mail the next day by the Assistant Communications Coordinator for Technology.
  - If a door is malfunctioning and has alarmed multiple times, the contact can request it be disregarded until the next morning and follow-up with the Assistant Communications Coordinator for Technology.
  - In all instances in which hardware appears to malfunction or alarms are received without obvious cause, affected department are strongly advised to contact the Facilities Management Division as well as the UGPD Assistant Communications Coordinator for Technology to collaboratively work to diagnose and fix the issue.
False Alarm Policy:

- Reducing the number of unnecessary alarms is an important responsibility for all parties involved. Because unnecessary alarms waste important University resources, all reasonable efforts must be pursued to keep them to an absolute minimum.

- If a department using an access control system is not responsive to UGPD and FMD efforts to address unnecessary alarms, the Police Chief reserves the right to pursue alternative efforts to gain cooperation, potentially including a $50 fine in instances in which repetitive false alarms are received and facility personnel are not receptive to collaborative efforts to identify and fix the causes of those alarms.

Additional contacts

Questions regarding the access control and security system policy should be directed to the Assistant Communications Coordinator for Technology at the University of Georgia Police Department: (706) 542-5813. Questions for the Police Department after business hours and on weekends can be directed to (706) 542-2200. Andover / Genetec issues can be reported via email: report Andover Control problems, or by contacting the FMD IT at 706-542-7551. The FMD Work Orders office can be reached during business hours at (706) 542-7456, and on weekends through the UGPD Communications Center at (706) 542-2200.

Responsibilities

The senior-most UGA administrator housed in a building or overseeing the personnel housed in a specific building is responsible for the day-to-day security protocols of that building, to include liaising with UGPD and FMD to identify, diagnose, and correct the sources of unnecessary alarms.

The Access Control Committee is responsible for policy revisions, prioritization of conversion, and administrative decisions that affect the access control system configuration on the University campus.

FMD is responsible for the maintenance of access control hardware and software.

UGPD is responsible for the law enforcement response to alarm activations.

The Chief of Police has the responsibility of providing for the safety of students, faculty, staff and visitors at the University of Georgia.

Responsible University Senior Administrator: Vice President for Finance & Administration

Responsible University Administrator: Executive Assistant to the Vice President for Finance & Administration

Policy Owner: Chief of Police

Policy Contact: Jimmy Williamson, Chief of Police

Phone Number: 706-542-1032

FAQs

**Question:** I cannot access the Andover computer in my office or remotely via WebClient. Whom do I contact?

**Answer:** Contact FMD IT via email at andover@fmd.uga.edu, or by phone at 706-542-7551.

**Question:** My access control system appears to be malfunctioning, whom do I call?

**Answer:** Contact FMD IT via email at andover@fmd.uga.edu, or by phone at 706-542-7551.

**Question:** I cannot remember my password to the Andover system. Whom do I call?

**Answer:** Contact FMD IT via email at andover@fmd.uga.edu, or by phone at 706-542-7551.

**Question:** The contact list for my facility has changed. Whom do I need to notify?

**Answer:** Notify the UGPD Assistant Communications Coordinator for Technology at 706-542-5813, or by email at kmastriano@police.uga.edu.

**Question:** Can the UGPD give me access to my building after hours or if I lose my access card?

**Answer:** No. UGPD personnel cannot grant access to buildings.
Policy Dates
Effective Date:

Date Last Updated: 06/10/2016

Date of Last Review:

Date of Approval:

Previous Version of Policy: