2.4 Physical Access Control and Video Security Systems Policy

Policy Statement

University of Georgia (UGA) employees shall take every reasonable step to develop and implement effective physical access control and video security systems procedures 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 Video Security Systems Policy is to provide structure for the utilization of the access control and video security system 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 and Video Security Committee

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

- UGA Police Department (UGPD) – Co-Chair
- Facilities Management Division (FMD) – Co-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)
- Auxiliary Services
- Office of the Provost
- Office of the Vice President for Research
- Athletic Association
- University Housing
Access Control 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, whether owned, leased, or occupied by the University of Georgia 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 “Genetec.” The University is currently migrating from the old campus standard product, “Andover Continuum.” 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 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 if 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 must be EV2 Smart Card readers as specified by the UGA OneCard project.

Biometric or keypad devices must be compatible with the building panels. Biometrics may include hand geometry readers, fingerprint readers, eye/face scanners, or other devices depending on the security assessment and implementation space available.

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.

Video Security System Criteria

All video security systems at the University, including those being installed in new construction, major renovation, or specifically added to an existing structure, whether owned, leased, or occupied by the University of Georgia shall conform to the following criteria:

Hardware/Systems:

An IP based video security shall conform to the University standard, “Genetec.”
Video monitoring devices shall include digital IP based cameras and video security devices compatible with the current version of the University standard system, “Genetec.” The Access Control Committee shall approve implementation of video monitoring, and implementation shall include appropriate signage.

Software:

The software system utilized for the video security system will be the standard system University-wide. Video shall be stored in servers housed in the University computer operations center or locally in the facility in which the cameras reside. Facilities Management Division (FMD) will coordinate software support and regular software maintenance fees will be paid by FMD.

Standards:

All video security footage must be stored for a minimum of 30 days. Video security footage should not be stored for longer than 90 days unless required by policy or applicable law. Video retention must comply with USG (University System of Georgia) ‘Security Surveillance Records’ records retention standards (0472-13-029A, B, and C).

All installed video security systems must comply with the UGA EITS High Bandwidth Consumption Systems Policy.

No video security footage shall be released to parties internal or external to the University except as authorized by official UGA duties, for duly issued subpoenas, open records requests, or as required by law. Security video is to be used to protect the safety and property of the University and should not be used for academic, instructional, or other purposes unless approved by the Access Control Committee. All release of video security footage must respect the Intellectual Property of the University and its employees. The Access Control Committee must approve any other release of footage.

The Access Control Committee will set standards for video security devices, video servers, and video storage devices for video security hardware. Any installed video security hardware must meet with the architectural standards maintained by the Office of University Architects.

No fake/dummy cameras or false signage that may portray an undue expectation of security are allowed.

No intentionally concealed or covert cameras are allowed.

No video security device shall use audio recording technology unless approved by the Access Control Committee.

All video security footage is the property of the University.

Tampering with live or recorded video security footage may result in appropriate disciplinary action, up to and including termination of employment.

Exclusions:

The video security section of this policy only applies to the Athens campus and surrounding areas. While remote campuses and sites are not responsible for complying with the centralized storage and video security system selection, they are still responsible for complying with all applicable policies and laws.

The following uses of video are excluded from Video Security System Criteria as listed in this policy:

1. Instructional, academic, or artistic purposes.
2. Capturing public events and performances.
3. Recording promotional or news events.
4. Convenience such as weather or construction viewing.
5. Video conferencing.
6. University research purposes.
8. Transportation and personnel (on-body).
10. Temporary camera installations as part of an on-going investigation. The Chief of Police must approve any use of this exception.

Any requests for further exceptions regarding video security must be made in writing directly to the Access Control Committee. The Access Control Committee will provide a timely response confirming the acceptance or rejection of any exception request.

For all exceptions or exclusions any higher applicable governance, policies, and laws shall apply.

Construction and Maintenance

Construction:

Construction of the access control and video 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 video security systems to the University standard system 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.

Departments may request the installation of a new access control and/or video security system to be funded by the requesting department through the Access Control Committee. Any other requests for the installation of new or the replacement of legacy access control systems should be made as part of a Major Repair and Renovation (MRR) request.

Maintenance:

Maintenance of all resident instruction access control systems that comply with the University standard will be accomplished by FMD. Maintenance of departmentally owned video security systems is ultimately the responsibility of the owning department. FMD can help coordinate maintenance of departmentally owned video security systems as personnel and resources in FMD are available. 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 video security systems. 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 access control or video security systems arise.

Re-occurring Costs:

FMD maintains the servers, storage, and re-occurring card reader licensing costs for the access control systems at no reimbursable cost to the University.

Video security system servers, storage, and camera capital and maintenance costs are funded by the department that owns the video security system. FMD maintains the re-occurring camera licensing costs for the video security systems at no reimbursable cost to the University.
Exceptions:

There are some departments or units on campus that may have out-of-the-ordinary applications for card access and video 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 in writing of their needs and/or concerns. The Access Control Committee has the final approval for all exceptions. All exceptions requests must be reviewed for justification and merit.

Monitoring:

Monitoring of the UGA Standard computer-based access control and video security systems will be the responsibility of the UGPD. One of the major benefits of the compatible central system is the capability to view centrally the status of the access control and video security systems in buildings and to respond appropriately. The UGPD will facilitate the monitoring of all compatible, computer access control and video security systems through whatever options are most cost effective for the University.

Generally, the UGA Police Department does not monitor video security system feeds in real time during normal operations. However, cameras may be monitored when circumstances suggest it is prudent and as staffing allows. The video security systems are used by UGPD to assist in the response of events as they occur or for after the fact investigative purposes.

Monitoring of video security systems will be conducted in an ethical, professional, and legal manner consistent with all existing University policies and applicable laws, including the Non-Discrimination and Anti-Harassment Policy and Title IX Sexual Discrimination, Harassment and Assault. Monitoring of video security must be used in such a manner to protect the Intellectual Property of the University and its employees. Violation of this policy and other relevant policy or law may result in appropriate disciplinary action, up to and including termination of employment.

Departments may also locally view and monitor their access control and video security systems. Use of these systems shall meet all requirements of this policy and any other applicable policy or law.

The existence of a video security device does not guarantee that the device is functioning or being monitored in real time.

Management of the Card Access System:

Overall:

The UGPD 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. Changing facility lock schedules due to an expected weather event is the sole responsibility of the department or unit in charge of that facility. 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 events, deliveries or personnel who have forgotten the necessary items needed for access to a building.

Buildings:

Like current keyed procedures, building schedules and lockup arrangements will remain the responsibility of the senior administrator in each building. Appropriate staff members will need to be tasked and trained to coordinate building door schedules, and to approve individuals to access the building after normal business hours or access other normally locked 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 ID badge. These badges are available from the UGACard Office, 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 by the Access Control Committee.

Building administrators are responsible for maintaining up-to-date access lists for their building. Building Administrators will update access no more than five business days after terminations and no more than 30 days after other personnel status changes in accordance with all applicable University, USG, and other policies. The building administrator must perform an annual audit of the people who have access to their building at least.

**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 UGPD 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 for non-Facilities Management Division buildings shall not include anyone employed by the Facilities Management 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-hours 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 web client interface for Andover / Genetec controlled buildings.

**System Maintenance and Work Orders:**

The UGPD will not be responsible for alarmed facility service repairs or equipment problems/malfunctions. The UGPD 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 resident instruction access control facilities, [https://workrequest.fmd.uga.edu](https://workrequest.fmd.uga.edu), or to the owning department for non-resident instruction access control or any video security systems. For Andover/Genetec software related issues, employees can also contact someone in FMD IT during standard UGA business hours through [accesscontrol@uga.edu](mailto:accesscontrol@uga.edu) or 706-542-7551 if there is an issue that cannot be handled with a work order.

**Alarm Protocol:**

1. When an alarm is received by the UGPD, an officer is sent to respond.

2. 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 may be called. When an alarm contact is called, they will be asked to decide: 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.
3. 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.

4. If a door is malfunctioning and has alarmed multiple times, the alarm contact will be called, the contact can request it be disregarded until the next morning, and the contact shall follow-up with the Assistant Communications Coordinator for Technology and FMD Work Orders.

5. In all instances in which hardware appears to malfunction or alarms are received without obvious cause, affected department shall 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 UGPD: 706-542-5813.

Questions for the UGPD after business hours and on weekends can be directed to 706-542-2200.

Andover/Genetec software issues can be reported during business hours via email at accesscontrol@uga.edu or by contacting FMD IT at 706-542-7551.

The FMD Work Orders office can be reached during business hours at https://workrequest.fmd.uga.edu or 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 installations, 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: P. Daniel Silk, Chief of Police
Phone Number: 706-542-1032

FAQs

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

**Answer:** Contact FMD IT via email at accesscontrol@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 Work Orders here, [https://workrequest.fmd.uga.edu/](https://workrequest.fmd.uga.edu/), and FMD IT via email at accesscontrol@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 accesscontrol@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 and FMD IT via email at accesscontrol@uga.edu or by phone at 706-542-7551.

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

**Answer:** No. UGPD and FMD personnel cannot grant access to buildings.

Policy Dates

Effective Date:  
Date Last Updated: 03/24/22  
Date of Last Review:  
Date of Approval:  
Previous Version of Policy: