Campus Access Control Services

As part of the University's integrated physical security systems, the campus access control services include the following:

- facilitating requests for FredCard access for individuals to interior and exterior doors within residential and academic buildings
- facilitating automated lock and unlock schedules for interior and exterior doors
- access control compliance reporting
- remote security management for badging, alarm and event monitoring
- project management, planning, designing, and programming the campus access control systems infrastructure: communication panels, iclass card readers, sounders, REX motions sensors, contacts, and security cameras

Retention Policy

- Security Camera System recorded video is minimum 31 days.
- Campus Access Control System logs is 31 days.
- Audio Recording System is 31 days.

Definiton of Terms

- FREDCard shall mean the official identification card issued by the UNIVERSITY to students, employees and affiliates. The FREDCard is produced by the Faculty Student Association (FSA) and is a multi-technology credential utilized for various services and systems throughout the UNIVERSITY. Different colors are utilized on the FREDCard to designate affiliations (e.g. Students, Faculty and Staff = Blue, Visitors = Green, Contractors = Orange, Summer Conferences = Tan etc.)
- ProWatch Campus Access Control System shall mean the electronic access system that is part of the UNIVERSITY's integrated physical security system which allows authorized users to use a FREDCard as the means of gaining physical access to designated exterior and interior spaces. This system replaces traditional keys with an electronic FREDCard reader that is networked into the current Information Technology infrastructure to allow for remote communication. The electronic access readers use iClass contactless Corporate 1000 card technology for secure access control. The system is currently utilized for facilitating requests for FREDCard access for individuals to interior and exterior doors within residential and academic buildings, facilitating automated lock and unlock schedules for interior and exterior doors, access control compliance reporting, remote security management for badging, alarm and event monitoring. The systems consists of servers, client workstations, networked communication panels, iclass card readers, sounders, REX motions sensors, contacts, electronic door strikes and panic devices.
- Building Access Coordinator(s) shall mean those UNIVERSITY employees or affiliates who are designated as the primary point of contact by department or organization as being responsible for requesting FREDCard access control provisioning and deprovisioning, clearance codes assignment, door schedules and access control functionality for assigned doors within their building(s). All interior and exterior doors within their scope of responsibility have designated physical numbers and access control levels which are to be utilized for submitting requests. All BAC members will be approved annually by the appropriate President's Cabinet member.
- Compliance Report(s) shall mean the reports produced by the ProWatch Campus Access Control System which could include FREDCard user physical access control logs to physical space(s)and clearance code(s), logical device configuration(s) and other audit logs for the purpose of maintaining regulatory compliance, criminal investigations, internal investigations and system audits.
- Access Control Clearance Code(s) shall mean the logical group of card readers for interior or exterior doors that have timezones assigned for designated specific access levels for users. All Access Control Clearance Codes will need the proper written approval by the designated Building Access Coordinator.
- Default Access Control Clearance Code(s) shall mean a set of access control clearance codes that are approved by the Chief of the UNIVERSITY Police Department or Director of Facilities Services or Director of Residence Life and used to facilitate normal UNIVERSITY business operations (e.g. maintenance).
- Access Control Level(s):
- Level 1 Access Control shall mean the (public) physical security level assigned to exterior and interior doors generally accessed by the public. Building Access Coordinators can approve access.
- Level 2 Access Control shall mean the (restricted) physical security level assigned to residential living spaces or spaces with equipment owned by the UNIVERSITY generally accessed by the campus community. Building Access Coordinators and Departmental Directors/Chairperson/Head /Dean shall approve access.
- Level 3 Access Control shall mean the (confidential) physical security level assigned to exterior and interior doors to highly-sensitive areas such as evidence room, cash control, data center, disaster recovery sites and file rooms. President's Cabinet members or designees shall approve access.
- Door Schedule(s) shall mean the time schedule assigned to door(s) to remotely and automatically lock (Card-Only Mode) and unlock for the purpose of facilitating business operations for UNIVERSITY departments and affiliates.Building Access Coordinators manage weekly door schedules for their designated set of building doors.

- Physical Door(s) shall mean the point of entry or exit to physical space controlled by manual keys or the campus access control system. All physical doors on the campus access control system will have official numbers assigned to them to distinguish them for key and access control request purposes and access control level assignment.

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()

Related articles

- Virtru Protected Email Guide
- Technology Procurement Process
- Fredonia Mail Data Loss Prevention Policy for Credit Card Numbers (CCN) and Social Security Numbers (SSN)
- How do I mark or unmark Spam in Gmail?
- Connecting to FREDsecure with Android