Security Access Control System

Operations Manual

Updated April 2008

Theresa A. Thayer, Manager
Key/Card Control Center
2003 Millikin Road - #035
Columbus OH 43210-1268

http://fod.osu.edu/keys
614-292-1415 • 614-292-6751 fax • key-card@osu.edu

THE OHIO STATE UNIVERSITY
Facilities Operations and Development

Table of Contents

Building Access

Electronic access to exterior and interior doors can be controlled by the following methods:

Scheduling – The system can schedule general door openings and closings and/or access to individuals through keypads or card readers in advance on a regular schedule or for specific, one-time special events. This feature usually involves a control device that acts as a security alarm (see below).

- Door Control Devices
- Keypads – allow access to individuals through a code or PIN number that is entered on the keypad.
- Card Readers – allow entry by swiping an authorized card.
- Door Contacts – electronic door contacts can be installed to control the building open and close schedule. This can be done without a card reader or keypad to secure the exterior doors on a building. At least one door should be a card reader or keypad to track access.

Building Alarms

Building alarms can sound locally and/or send a signal to Security and Fire Prevention Services. Some types of alarms are ...

- Security – including unscheduled or unexpected door openings, door propping, motion and heat detection, glass breaks.
- Fire – these alarms are triggered by the sensors detecting smoke and/or heat.
- Environmental – these alarms can be triggered by various causes such as temperature, moisture, etc.
- Trouble/fault/hazard – these alarms detect problems with the device and send notification to the individuals monitoring alarms.

Activity reports on card swipes, keypad entry, and alarms are available from Key/Card Control Center.

Facilities Operations and Development and/or Security and Fire Prevention Services will provide testing upon the completion of the project installation. We will require a 2-week no fault or trouble condition period before monitoring the building security. If you've contracted with Security and Fire Prevention Services for the monitoring of door conditions and alarms, you must complete an Alarm Account call list. Please contact Security and Fire Prevention Services at 292-6677 for additional information and the Alarm Account form. In addition to testing, Facilities Operations and Development requires the below listed items and forms to be completed before the system is brought online. Refer to topics enclosed for further information on each.

1. Person responsible for system (Authorization for Granting Card Access form)
2. The initial list of people who will receive card access (Card Access Request form)
3. Call list for alarms (Dispatch File form)
4. If you have installed keypads (Keypad Account Setup form)
5. Building Schedule (Electronic Door and Alarm Schedule form)
6. New override cores installed and keys issued
7. Annual order for servicing (not required, recommended – 100-W for servicing)

On new installations, the security system vendor should provide a 1-year installation and hardware warranty. The electrical contractor should also provide an installation warranty; please refer to the vendor's warranty contract for this information. The requesting department is responsible for the cost of maintaining and repairing all devices and hardware related to the Access Control and Security System.

It is highly recommended that you maintain an Annual Order with the Lock Shop for servicing your system. System problems will be serviced only after the payment source is received. The Lock Shop will determine if the alarm condition is billable. Inspection is required before determining billable status ... it could be a warranty issue, a problem caused by a contractor in your area, or a communication line problem, etc.

If you are installing a security system that encompasses all or most of the exterior part of the building, we recommend the following card swipe test for faculty/staff/students. All card access requests must be received and entered by our department before this test. Then, schedule with Key/Card Control Center testing of card swipes. We will lock down a designated door and have all staff swipe their cards to enter the building. If the card does not work, we can make corrections and check for bad cards. This helps the employees with the transition. We recommend this be done a few days within the same week before the system is fully brought online and locked down. We also recommend that you notify all employees the dates of the test by posting signs throughout the building. Also, notify your employees that their current brass keys to the exterior doors will no longer work. All keys are to be returned to the Key/Card Control Center.

New Override Cores & Keys

As part of the installation, new brass key override cores must be installed on all security system control devices, so the building can be opened in case of a system failure. This includes all doors with or without card readers. A new restricted core code must be established with the Lock Shop and installed to eliminate existing keys being used. If your system is being monitored by Security and Fire Prevention Services, every time an override key is used, an alarm will go to their monitoring station as an intrusion, and the OSU Police will be dispatched to that location. Security and Fire Prevention Services may charge for system abuse and false alarms. The OSU Police department may also charge for excessive and/or false alarms requiring a police officer dispatched. Override keys issued should be highly restricted and limited in numbers. These keys should be used only in case of an emergency if your system is malfunctioning or down.

Authorization for Granting Card Access

This form is used to appoint a person or people in your department to maintain the security system access. The appointees will be responsible for requesting and removing card access or keypad access, making building schedule change requests, and reporting system problems. Use one form for each appointee. This form must be approved and signed by your Dean, Chair, or Director. You can separate responsibilities by assigning one person to be responsible for the exterior part of the building and another person to be responsible for a computer lab, for example. Responsibility can also be split up between several departments by floor or area. Upon completion of this form (Authorization for Granting Card Access), all forms and correspondence from Key/Card Control Center will be e-mailed to the authorized parties.

For the Key/Card Control Center to ensure security levels, the appointee's return e-mail address will be verified on every request received. This means web servers cannot be used because we are unable to identify the person sending the request.

All Key/Card Control Center forms can be found on our website:
http://fod.osu.edu/keys
Please note that all security and card access forms are in two versions. These forms are similar but require specific information based on which security system you have installed ...

- The current MDI System
- The new Lenel Security System.

Facilities Operations and Development

Lenel Appointed Authorized Contact

035 Central Service Building • 2003 Millikin Road • Columbus OH 43210
614-292-1415 • 614-292-6751 fax • key-card@osu.edu

Use this form to appoint a person(people) in your department to maintain the security system. The appointees can be responsible for requesting and removing card access, making building schedule change requests, and reporting system problems. You can separate responsibilities by assigning the exterior doors to the Building Coordinator and the computer lab to the Lab Manager. Responsibility can also be divided among several departments. This form must be approved/signed by your Dean, Chair, or Director. Because we must have an original signature, we will not be able to accept this form electronically.

We recommend that each department have at least two authorized individuals—a primary and a back-up. For security purposes, it is also recommended that the list of authorized individuals be kept to a minimum. When filling out the form, please list each building with corresponding room numbers, exits, closets, and corridors separately. If more space is needed, please feel free to use the back of the form. Upon completion of this form, the Key/Card Control Center will email all correspondence to the authorized parties.

This person will be responsible for (check all that apply) ...	Please check only one ...
☐ Granting & removing card access ☐ Maintaining building schedule ☐ AAM Administrator	☐ New person ☐ Replacing (person's name) ☐ Update (reason)

Org or Dept #	Dept Name
Responsible for these buildings ... SAMPLE	
Door/Room Description(s)	

Name (print or type)	Signature
Mailing Address	
E-mail	Phone

I hereby authorized the above individual to grant card access to the building and rooms specified above.

Date | Authorized Signature of Dean, Chair, Department Admin Required | Name (print or type)

To provide continuity, the Key/Card Control Center has designed a Card Access Request form. This form was designed as a text (TXT) file to be flexible in transmitting through various versions of e-mail. All the necessary forms will be e-mailed to you. Please contact the Key/Card Control Center for this form. Submit all requests to key-card@osu.edu. We will reply via e-mail upon completion of your request.

To grant card access, you must provide specific information—the building name, room numbers, a shift or access level, faculty/staff/student name, social security number, and BuckID number or hospital ID number. You may list 1 to 100+ names on one form if the room number(s) and the shift or access level is the same.

After installation and testing, we will e-mail the authorized parties the door/room descriptions. To maintain consistency, please use these same door/room descriptions on the Card Access Request form. This form is used for all requests, your initial setup, and maintaining your access requests. These descriptions are usually established with you during installation and testing.

Immediately report lost or stolen BuckIDs and Hospital IDs first to the department, then to the University Police (292-7677), and then to the Key/Card Control Center (292-1415).

BuckIDs
Turn BuckIDs in to the Key/Card Control Center or Lost & Found. They will be checked for card access on the campus Access Control and Alarm Monitoring System. If the BuckID has access to academic buildings, we will deactivate card access and forward the card to BuckID services in Lincoln Tower. For additional information about BuckIDs, please refer to their website at http://buckid.osu.edu/account/lost.asp.

Hospital IDs
Turn Hospital IDs in to the Key/Card Control Center or Lost & Found. They will be checked for card access on the campus Access Control and Alarm Monitoring System. If the Hospital ID has access to academic buildings, we will deactivate that card access and forward the card to Hospital Security (293-8500).

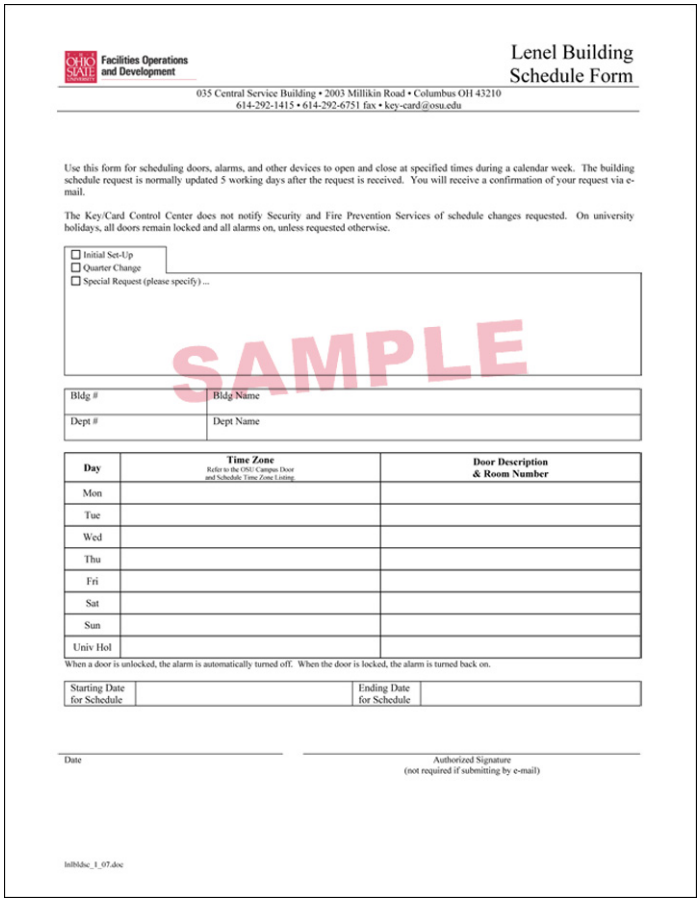
Building schedule programs are designed to automatically lock and unlock doors. Before the system is brought online, a building schedule is required for all door-control devices. A schedule is required for Monday through Sunday, 24 hours a day. The form name is "Electronic Door and Alarm Schedule" form. You may need to use more than one form if your doors are on a separate schedule. Example ...

- The exterior doors/readers are on a schedule to unlock in the morning and lock down in the evening, but your computer lab rooms are to remain locked always. This requires two forms—one for the exterior doors and one for the lab. On University holidays, all doors remain locked and alarmed, unless requested otherwise.

To set up a new schedule, the form must be received by Key/Card Control Center one week before the effective date. Security and Fire Prevention Services is not notified of building schedule changes. You will receive confirmation from us upon completion of your schedule change.

We recommend installing a keypad to override your building schedule for special events and break changes.

If a building schedule did not run and it is outside of our office hours (see last page), you can contact Security and Fire Prevention Services to unlock a door, based on their requirements.



Facilities Operations and Development

Lenel Building Schedule Form

035 Central Service Building • 2003 Millikin Road • Columbus OH 43210
614-292-1415 • 614-292-6751 fax • key-card@osu.edu

Use this form for scheduling doors, alarms, and other devices to open and close at specified times during a calendar week. The building schedule request is normally updated 5 working days after the request is received. You will receive a confirmation of your request via e-mail.

The Key/Card Control Center does not notify Security and Fire Prevention Services of schedule changes requested. On university holidays, all doors remain locked and all alarms on, unless requested otherwise.

☐ Initial Set-Up
☐ Quarter Change
☐ Special Request (please specify) ...

SAMPLE

Bldg #	Bldg Name
Dept #	Dept Name

Day	Time Zone (Refer to the OSU Campus Door and Schedule Time Zone Listing)	Door Description & Room Number
Mon		
Tue		
Wed		
Thu		
Fri		
Sat		
Sun		
Univ Hol		

When a door is unlocked, the alarm is automatically turned off. When the door is locked, the alarm is turned back on.

Starting Date for Schedule		Ending Date for Schedule	

Date

Authorized Signature
(not required if submitting by e-mail)

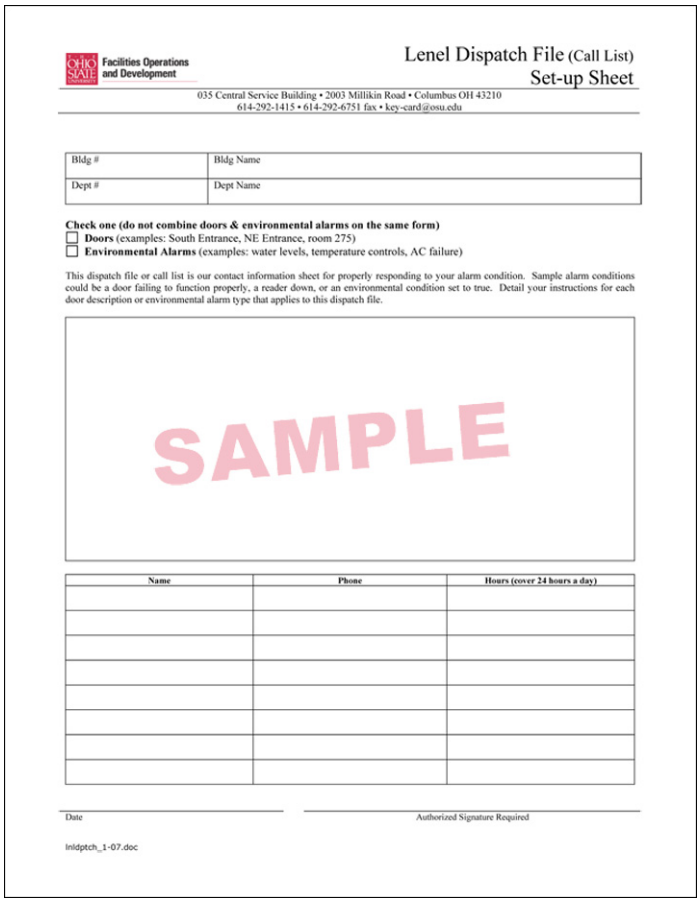
lnlbldsc_1_07.doc

- During office hours (see last page), contact the Key/Card Control Center at 292-1415.
- After office hours, on weekends, and on holidays, contact Service2Facilities at 292-6158.

Again, it is highly recommended that you maintain an Annual Order with the Lock Shop for servicing your system. System problems will be serviced only after the payment source is received. The Lock Shop will determine if the alarm condition is billable. Inspection is required before determining billable status. It could be a warranty issue, a problem caused by a contractor, or a communication line problem, etc.

Dispatch File (Call List)

If a door is not functioning properly (system faults), a reader is down, or an environmental condition is in alarm, the dispatch file or call list is our contact information sheet for properly responding to the alarm condition. These alarms will come in as Hazard Alarms. (The dispatch file call list is not used for door props or intrusions—those are security issues.) Check either door or environmental alarm, and use a separate form for doors and environmental alarms. List each door description or environmental alarm type that applies to each dispatch file. Then detail out your call list or response instructions.



Facilities Operations and Development

Lenel Dispatch File (Call List)
Set-up Sheet

035 Central Service Building • 2003 Millikin Road • Columbus OH 43210
614-292-1415 • 614-292-6751 fax • key-card@osu.edu

Bldg #	Bldg Name
Dept #	Dept Name

Check one (do not combine doors & environmental alarms on the same form)
☐ **Doors** (examples: South Entrance, NE Entrance, room 275)
☐ **Environmental Alarms** (examples: water levels, temperature controls, AC failure)

This dispatch file or call list is our contact information sheet for properly responding to your alarm condition. Sample alarm conditions could be a door failing to function properly, a reader down, or an environmental condition set to true. Detail your instructions for each door description or environmental alarm type that applies to this dispatch file.

SAMPLE

Name	Phone	Hours (cover 24 hours a day)

Date

Authorized Signature Required

lnldptch_1-07.doc

Power Supply & Malfunctions

If the building's power supply is shut off, the control panel is malfunctioning, or the card readers are not operating, the system default is to lock all doors. Card readers will not operate, and the building's open and close schedule will not process. Egress fire doors located in corridors and stairways must be tied into the fire alarm system so the doors can fail unlocked in case of a fire alarm or power failure. All systems have a 2-hour window with a back-up battery supply for alarm reporting only. As an example, intrusion alarms, fire alarms, etc., will still report to Security and Fire Prevention Services. All doors should have a brass key override core installed. Again, when an override key is used, contact Security and Fire Prevention Services immediately to let them know that your security system is down. Also contact Service2Facilities to report the building condition and create a work order. When the power resumes, make sure all your doors are closed before running your daily opening/closing schedule to avoid trouble conditions (doors may not lock or unlock if doors are propped open). In this event, you could receive door prop alarms.

Communication Line Problems

If the security system is reporting communication line problems, it cannot communicate with the network and may not process your building's open and close schedule. Card readers and/or security panels have a local memory and can hold a specific number of cardholder records in that local memory. Cardholder records stored in memory can still be granted access if your communication lines are down. A communication line failure alarm should have already been reported to Security and Fire Prevention Services. Contact Security and Fire Prevention Services to verify. Also, contact Service2Facilities to report the condition.

The MDI card readers hold the last 1,000 entries and will grant access only to those recorded in memory.

The Lenel card readers hold all users that currently have access to those specific doors in memory

Card Reader Problems

All doors should have a brass key override core installed. In the event that a card reader is down and the door is propped or an override key is used, contact Security and Fire Prevention Services immediately to let them know your system is down. When an override key is used or a door is propped, an alarm will report to Security Service, and the Police will be dispatched. Contact the Key/Card Control Center during office hours or Service2Facilities after hours to report a problem. It is highly recommended that an annual order be created at the time of installation for servicing. Most of the card reader problems are billable to the department, unless it is under warranty. All after-hour service calls require a 100-W.

Contact Information

Key/Card Control Center
035 McCracken Power Plant
2003 Millikin Rd.
614-292-1415
e-mail: key-card@osu.edu
http://fod.osu.edu/keys

Mon – Fri 7:30a to 4:30p