MILLIGAN

CAMPUS SAFETY

ACCESS CONTROL POLICY

5.8.26

Table of Contents:

1. Purpose

Milligan University is committed to maintaining a safe, secure, and welcoming campus environment. The purpose of this policy is to establish clear standards for the management of physical access to university buildings, rooms, and other secured spaces through keys, cards, mobile credentials, electronic access control systems, door hardware, and related procedures.

This policy is intended to:

- protect students, employees, guests, and university property;
- support appropriate access for academic, residential, administrative, ministry, event, and operational needs;
- ensure access is granted only to authorized persons with a legitimate university need;
- create accountability for who has access to university spaces and when;
- establish standards for door security, door schedules, and credential use; and
- reduce risk related to unauthorized entry, lost credentials, propped doors, misuse, theft, vandalism, and emergency situations.

All keys, access cards, mobile credentials, door codes, electronic permissions, door hardware, and access-control records associated with Milligan University facilities are the property of the university.

No person is entitled to building or room access simply by status, preference, convenience, or informal departmental practice. Access will be granted only through approved university processes and may be modified, suspended, or removed at any time when necessary for safety, staffing changes, housing changes, policy compliance, operational needs, or institutional risk management.

No university department, office, or employee may independently install, replace, reprogram, bypass, or substantially modify locks, card readers, cylinders, door hardware, access-control software, schedules, or access permissions outside the university's approved process.

2. Scope

This policy applies to all Milligan University-owned, leased, managed, or controlled buildings, facilities, exterior doors, interior doors, gates, locking systems, keys, access cards, mobile credentials, electronic access control systems, and related access-control records.

This policy applies to:

- faculty, staff, and administrators;
- students and student employees;
- Residence Life staff and student leaders;
- contractors, vendors, consultants, and service providers;
- temporary workers, affiliates, and guests who are granted university access; and
- any office or department that requests, approves, uses, or manages access to university space.

This policy does not replace specific residence hall guest policies, student conduct policies, emergency procedures, or facilities work-order procedures, but works alongside them.

3. Definitions

Access control system means the university's approved physical access system used to grant, restrict, monitor, or revoke access to buildings, doors, rooms, gates, or other secured areas.

Credential means any approved means of entry, including a university ID card, mobile credential, fob, key, keypad code, or other approved device.

Electronic access means access granted through the university's electronic access control system.

Physical key means any key, core, cylinder, or mechanical means of entry controlled by the university.

Access holder means a person who has been issued access credentials under this policy.

Access approver means the person authorized to approve access requests for a given building, department, or space.

Building administrator means the office, department head, director, dean, Residence Life official, or other authorized leader responsible for approving access to a given space.

Sensitive space means an area with elevated security, confidentiality, operational, or safety concerns, including but not limited to residence halls, data rooms, health-related spaces, cash-handling areas, storage areas, equipment rooms, records rooms, and research or restricted-access areas.

Door schedule means the approved operating schedule for when a door is unlocked, card-controlled, locked, alarmed, or otherwise restricted.

Temporary access means access approved for a limited period for a specific purpose.

4. Access Categories

Access may be issued in the following categories:

- **standard employee access** based on job duties and assigned workspace;
- **student residential access** based on housing assignment;
- **student worker access** based on approved role and work schedule;
- **faculty access** based on teaching, advising, studio, office, or approved program needs;
- **administrator or leadership access** based on role-based institutional responsibilities;
- **contractor/vendor access** based on approved scope of work and time period;
- **temporary/event access** for short-term operational needs;
- **after-hours access** for approved business or program needs; and
- **emergency or privileged access** for a limited number of authorized personnel.

5. Criteria for Granting Access

Access will be granted only when the request is tied to one or more of the following:

- assigned office, classroom, lab, residence hall, or work area;
- required work responsibilities;
- approved student employment or campus leadership duties;
- approved housing status;
- approved event, program, production, or ministry support responsibilities;
- contractor or vendor work authorized by the university;
- emergency response, maintenance, custodial, or on-call responsibilities; or
- another documented institutional need approved through the appropriate chain.

Access will not be granted solely for convenience when other reasonable arrangements exist.

6. Approval and Request Process

Requests must be approved by the appropriate access approver for the area involved. Depending on the space, this may include:

- a department head or director;
- a dean or vice president;
- the Residence Life office for housing-related access;
- the responsible safety/access control office for system administration and final approval; and/or
- additional approvers for sensitive spaces.

6.1 Minimum request information

Requests should include:

- the full name of the person needing access;
- university affiliation and role;
- requested building(s) and door(s) or access group(s);
- reason access is needed;
- start date and, if applicable, end date;
- access level requested;
- sponsoring department or office; and
- approver name and date.

Temporary access should be used whenever permanent access is not necessary. Temporary access should have a defined end date and should expire automatically when feasible.

7. Credentials and Individual Responsibilities

All issued credentials remain the property of Milligan University. Each access holder is responsible for protecting their credentials and using them only for authorized purposes.

7.1 Prohibited conduct

The following are prohibited:

- lending, sharing, duplicating, or transferring keys, access cards, mobile credentials, fobs, or codes;
- using another person's credential;
- allowing another person to use a credential issued in your name;
- intentionally bypassing or defeating access controls;
- misrepresenting the need for access;
- retaining access devices after separation, transfer, or expiration of authorization; and
- unauthorized copying or creation of physical keys.

7.2 Lost, stolen, or compromised credentials

Lost, stolen, or compromised keys, ID cards, mobile devices used for credentialing, fobs, or door codes must be reported immediately to the Campus Safety office.

The university may immediately deactivate a credential, change permissions, replace cylinders, change codes, or take other action necessary to reduce risk. The university may assess replacement charges or department costs associated with lost credentials, replacement keys, re-coring, reprogramming, or other corrective action as appropriate.

8. Door Use, Door Security, and Building Entry Standards

Doors that are intended to be locked, card-controlled, alarmed, or otherwise secured must remain in their designed operating condition.
Except for approved operational purposes that are actively supervised, propping open secured doors is prohibited. Doors should never be left unsecured in a way that defeats their intended access-control function.
Individuals may not allow unauthorized persons to enter secured areas by following behind them, being waved through, or otherwise bypassing required authentication.
Emergency exit doors, panic hardware, exit alarms, closers, latches, fire-rated doors, and related life-safety devices may not be blocked, disabled, tied back, altered, or used improperly.
Departments and individuals may not independently alter door hardware, install aftermarket locks, tape over latches, disable strikes, wedge doors, remove closers, obstruct latching, or make modifications that affect fire-rating, egress, ADA function, or security.
Broken locks, failing closers, doors that do not latch, doors that do not align, reader malfunctions, forced-entry concerns, and similar issues must be reported promptly to the Campus Safety Office.

9. Building Hours and Door Schedules

Door schedules for university buildings and spaces must be established and maintained through the Campus Safety office in consultation with the president's office.

Buildings may operate in one or more of the following modes:

- **public/open hours** during which designated doors are unlocked for normal use;
- **controlled hours** during which designated doors require approved credentials;
- **closed hours** during which access is restricted to approved personnel only; and
- **emergency or special operations modes** as needed.

Access during university breaks, reduced-service periods, holidays, closures, and summer operations may be reduced or modified based on institutional need.

10. Employee, Student, and Affiliate Access

Employees may be granted access only to spaces necessary for their current role. When an employee or student changes roles, offices, departments, or work assignments, access should be reviewed and adjusted promptly.

Physical keys will be issued only when necessary and only to named individuals. Keys should not be issued to a department for general pass-around use unless a controlled check-out method has been specifically approved.

Upon resignation, termination, graduation, withdrawal, removal from housing, suspension, expiration of contract, or other separation from the university, access must be removed or adjusted as appropriate and credentials returned. For involuntary separations, suspensions, or urgent risk concerns, the university may remove access immediately.

Residential students will receive access appropriate to their assigned building and approved residential spaces. Residence Life professional staff, on-call staff, and designated student leaders may be granted broader residential access based on their role and duty responsibilities. Tailgating, door propping, use of emergency-only doors for routine access, and other attempts to bypass residential access controls are prohibited and may result in student conduct action or loss of access privileges.

Contractors, vendors, consultants, and temporary workers may receive access only when sponsored by a university department and approved through the Campus Safety Office. Their access must be limited to the specific area needed; the approved dates and times needed; the specific project or service being performed; and the least access necessary to complete the work. At the end of a project, service period, or contract, all issued credentials must be returned and/or deactivated promptly.

The university may require escorted access rather than independent credentials where appropriate.

11. Special Events, Programs, and Temporary Operations

Access for camps, conferences, performances, summer groups, volunteers, visiting speakers, external renters, or other temporary users must be coordinated through the Campus Safety office and the sponsoring university department.

Temporary access for these groups shall:

- be documented in advance;
- be limited to the necessary buildings, doors, and times;
- include a defined sponsoring office;
- include clear responsibility for supervision and conduct; and
- end automatically or be removed immediately after the event or program.

13. Sensitive and High-Risk Spaces

Some areas require heightened approval, tighter controls, and more frequent review. These may include:

- residence life master-access spaces;
- IT and network rooms;
- records and compliance storage;
- cash-handling locations;
- health- or counseling-related spaces;
- hazardous materials storage;
- key shops, control rooms, and security system rooms;
- mechanical or infrastructure spaces; and

- any other location designated as high risk.

Access to these spaces will be strictly limited, documented, and periodically reviewed.

14. Emergency Access, Lockdown, and Immediate Changes

The Campus Safety office, or designated university leadership acting through that office, may grant, revoke, or modify access immediately in response to:

- threats to safety or security;
- emergencies or disaster response;
- active investigations;
- personnel actions;
- student welfare concerns;
- lost or stolen credentials;
- compromised doors or hardware;
- break-ins or suspicious activity;
- planned campus closures; or
- other urgent operational or risk concerns.

The university may temporarily secure buildings, override door schedules, or limit access during incidents, weather events, major campus gatherings, or emergency response operations.

The university may re-core locks, replace cylinders, change codes, or reprogram doors whenever needed for safety, separation, key loss, construction, hardware failure, policy enforcement, or other operational reasons.

15. Privacy and Appropriate Use of Access Data

Access-control records are sensitive university records. They will be used only for legitimate university purposes, including operations, investigations, emergency response, compliance, and safety management.

Access data shall not be used for personal curiosity or informal monitoring. Access to system records should be limited to personnel with a legitimate need to know.

16. Exceptions

Exceptions to this policy must be approved in writing by the President or designee after consultation with the Campus Safety Office, Information Technology, and legal counsel as appropriate.