PURPOSE
To facilitate access to space and equipment by authorized users (faculty/staff, students, and affiliates) and to safeguard members of the Liberty University community and its physical assets, a policy on Access Control has been established. This policy and supporting guidelines set out specific responsibilities, conditions, and practices which are designed to address critical access needs in a manner which minimizes risks and maximizes the protection of the university's physical assets and private information.

DEFINITIONS

**Hardware** – Currently there are three different methods of Access Control at Liberty: RS2 technologies, DSX technologies, and traditional metal keys. The following is a more detailed description of these methods.

**Key** – Traditional metal keys, Flames Pass, and/or any electrical means of access.

**RS2** – This is electronic access technology that allows use of the current Flames Pass as the means of access. RS2 replaces traditional keys with an electronic door strike that is hardwired and networked into the current information technology infrastructure to allow for remote communication. The electronic access readers can be swiped horizontally or vertically.

**Metal Keys** – Traditional metal keys are the most widely used system on campus. There has been a gradual replacement of traditional keys with electronic locks over the past several years. Approximately half of our doors now use electronic access; the rest still use metal keys.

**Access** – The ability to enter university property or space by means of a traditional metal key, Flames Pass, or any electronic means of entry.

**Great Grand Master Key** – This is any combination of electronic card access and traditional metal keys that open all doors on Liberty University’s campus. Great Grand Master Keys are only distributed to the following personnel and must be approved by Access Control:

- Presidents of the university
- Provost of the university
- Senior vice presidents
- Associate vice presidents
- Chief of police and staff
- University maintenance staff
- Facilities management department

**Maintenance Master Keys** – Any combination of electronic card access and traditional metal keys that opens multiple doors on university property. Maintenance Master Keys are only distributed to the
following personnel and must be approved by the vice president of Field Operations:
• Department supervisors
• Department lead men

**Building Master Keys** - Any combination of electronic card access and traditional metal keys that opens multiple doors on Liberty’s campus. Building Master Keys are only distributed to the following personnel and must be approved by Access Control.
• Deans of schools
• Chief administrators (for control over specific areas)
• Department staff (for his/her building only, this includes office and common areas)

**Office Master Keys** - Any combination of electronic card access and traditional metal keys that opens multiple doors within a specific office suite or department space on campus. Office Master Keys are only distributed to the following personnel and must be approved by the assigned department liaison:
• Individuals specified by deans of schools or vice presidents

**Residence Keys** – These can be any combination of electronic card access and traditional metal keys that unlock doors within a student’s residence hall on campus. Students are only issued access for the building in which they live and the Flames Pass will register invalid when used in another residential university building. Residence hall Master Keys are distributed to the Office of Student Housing and must be approved by the assigned department liaison.

**BUILDING STANDARDS**

Liberty’s component standard on all new construction/alterations and remodeling is as follows.

Access Control is divided into two categories: external perimeter building Access Control and interior access and security. To the maximum extent possible and where technically feasible, authentication authorization and Access Control practices for the university must address the standards below:

**Exterior doors: RS2 technologies** – Each building achieves perimeter access through any door that opens to the outside through an online system of card readers. External perimeter access control is maintained via building time schedules.

**Interior doors: RS2 technologies** – Interior Access Control is determined by the needs of the individual schools, departments, and staff on a building basis. Exterior access into the school or department is included on the access level that has been created between Access Control and the departments. In certain circumstances, such as areas that need a higher level of security, an opportunity exists for the installation of wired locks to achieve the extra level of security that is necessary.

Access Control is to be included in the review of new construction, alterations, remodeling to insure that the component standards outlined in this policy are followed.

**Access Control policy statement** – The safety and security of the university’s physical space and assets are a shared responsibility of all of the Liberty University community. To meet this obligation, Liberty has established an Access Control policy to address the design, administration, and management of Access Control systems and measures to ensure their integrity. Access Control privileges are determined and assigned by university administrators and the Access Control Office based on the needs and requirements of the university and the key/card holder. All faculty/ staff, students, and vendors are required to sign out their keys from Access Control.
**Delivery of services** – Under normal circumstances, routine access requests are completed within the following time frames:

- RS2 (badge request): One to two business days

- Metal keys: Two business days once approved (The person who makes the request receives an email when that request is approved by Access Control)

Turnaround times may change depending on the time of year, work order volume, and staffing levels in Access Control.

In the event of a special circumstance and or an emergency, delivery of service times can be altered to accommodate the customer’s needs.

**New Employees/New Students** – Full-time employees, part-time employees (including student employees), outside contractors:

If the employee is new to campus, the following procedure must be followed:

- New full-time employees: Employee’s department or Human Resources (HR) liaison will process all necessary information through the HR system for new employee to obtain a Flames Pass from Card Services.

Once a Flames Pass has been received, the employee’s department liaison must submit a badge request to activate that employee’s department access.

For access to doors with metal keys, department contact will submit a key request as well.

**Resident Students** – The Office of the Registrar is responsible for entering the new student’s information into the university’s database. Once this information is complete, Card Services will print the student’s Flames Pass. Upon downloading the new information, the student’s card is automatically updated with tunnel and dorm access. The housing assignment that is automated on the student’s Flames Pass comes from the Office of Student Housing. Students will only be granted access to their living space (where badge access is active). Their Flames Pass will register invalid if a student attempts to enter a different residence hall.

**Commuter Students** – The Office of the Registrar is responsible for entering the new student’s information into the university’s database. Once this information is complete, Card Services will print the student’s Flames Pass. Upon downloading the new information, the student’s card is automatically updated with the tunnel access. Commuter students do not have any badge access into residence halls.

---

**SEPARATION OR TRANSFER**

**Separation** – It is the responsibility of the immediate supervisor or human resources representative to collect all access devices (metal keys, Flames Pass) issued to an individual at the time of separation. The department liaison will then:

Consult with the Access Control Office to ensure that all devices are accounted for prior to separation.

The liaison is responsible for initiating an email to Access Control to terminate all access in the system.
The liaison must surrender all collected access devices to Access Control within 24 hours of collection, to enable proper and timely verification.

**Transfer** - If an employee is transferring to a new department within the university, the following procedure must be applied:

Employee’s current department liaison must submit a request to deactivate employee’s department access (key and electronic)

Employee’s new department liaison (department contact) will submit a request to activate the transferred employee’s access (key and electronic). Access Control needs the old access returned before issuing the new access.

**Student Employee** - It is the responsibility of the immediate supervisor/department liaison to initiate an email for Access Control to terminate access to all exterior and office doors.

**Students** - Separation (voluntarily/involuntarily removed from the university). It is the responsibility of the dean of students, Student Affairs, Registrar’s Office, and/or Card Services to initiate an email to Access Control to terminate residence hall access.