

# Christopher Newport University

## **Policy: Building Access Policy**

### **Policy Number: 7005**

Executive Oversight: Executive Vice President  
Contact Office: Information Technology Services and University Police  
Frequency of Review: Annually  
Date of Last Review: December 2016

#### **A. PURPOSE**

The following policy is intended to document building access. The effective control and security of University buildings are necessary for the safety and protection of University personnel, property, equipment, and private information.

#### **B. POLICY STATEMENT**

This policy directs how the University controls access to its administrative, academic and public use buildings. This policy does not address building access to Residential Housing.

#### **C. PROCEDURES**

It shall be the responsibility of the Emergency Policy Group to establish building hours and after-hour access protocols for faculty, staff, students and others based on the recommendations of the Building Access Policy Committee, co-chaired by the Chief of Police and Chief Information Officer.

##### **1. Building Operations**

###### **a. Building Opening & Closing**

Buildings whose exterior doors use programmable electronic controls shall have a routine schedule, such that the doors will automatically unlock and lock on a daily basis. Buildings that do not have programmable electronic controls in place shall be opened and closed by facilities management staff or University Police for opening and closing.

###### **b. Building Hours**

Building hours are posted on the official “Building Hours” website. For safety purposes, persons using a building when it is closed are encouraged to call the University Police when entering and leaving the buildings. University Police can be contacted at 757-594-7777.

**c. University Closed**

There are times during the year in which the University closes and it is expected that buildings will be closed to the public. All academic and administrative buildings with electronic access control will close on these dates. Additionally, any electronic student access to spaces in these buildings will also be disabled on these dates, absent a specific demonstrated need.

**d. Emergency Closures**

When personal safety and or/building security becomes a concern, the University may close or change the hours of operation in any or all facilities. Classes, reservations and events scheduled in those facilities may be relocated, postponed or canceled entirely. The University will attempt to advise appropriate personnel of these closings.

**2. Access Control Standards**

Access to buildings is available via electronic card access or a hard key. All electronic access shall be assigned to a user via their CNU ID card, known as a “Captains Card.” Hard keys must be issued by Plant Operations. Hard keys shall never be used for access that is controlled electronically, except in case of an emergency. This requirement includes all Housekeeping, Maintenance and University Police staff.

Installation of alternative access control methods or unapproved modifications to existing access control methods is expressly prohibited and a violation of University policy.

**3. Access Granting Authorities**

To ensure the correct and proper assignment and verification of access, the Emergency Policy Group shall designate Access Granting Authorities (AGAs). The AGAs will serve as liaisons to help coordinate building security. AGAs may be designated by building or department and are responsible for the verification of existing access, review of access requests, and notifications of access removal for all access controlled spaces under their jurisdiction.

**4. Access Requests**

Access is available to a user based upon their role and its attendant privileges at the University. Additional access may be requested through the appropriate AGA and activated by IT Services and/or Plant Operations only upon approval.

Persons authorized to be in the buildings after-hours may be accompanied by others (e.g., roommates or family members). Non-authorized persons must be attended by an authorized person and the authorized person is responsible for the person who accompanies them.

## **5. Access Removal**

All assigned access is time-limited. Building access for faculty and staff will be removed upon termination or transfer. AGAs shall review all granted access at the conclusion of each academic term and shall remove access from anyone who is no longer engaged in activities requiring access.

## **6. Community Responsibilities and Sanctions for Violations**

The safety and security of the University's physical space and assets is a shared responsibility of all members of the University community. Access to the University's facilities is considered a privilege, and is determined and assigned based on the specific needs and requirements of the University and the user. All members of the campus community are responsible for the following:

- Keeping all hard keys and Captains Cards in a safe place.
- Not lending access devices to others.
- Not propping doors open or leaving them unlocked during hours when the facility is normally closed to the public.
- Not creating, duplicating, possessing, or using access devices (hard keys and Captain's Cards) to a facility without proper approval.
- Not damaging, tampering, vandalizing, altering or modifying access devices, hardware; locks or other access mechanisms.
- Reporting unusual access control locks or other access activity that is out of the ordinary to University Police.
- Reporting theft of a Captain's Card immediately to University Police.
- Reporting the loss of a Captain's Card within 24 hours to the Captain's Card Office.
- Returning access devices (hard keys and Captain's Cards) upon leaving the University.

Those found in violation of this policy shall be subject to sanctions that include: loss of access privileges; payment of replacement or rekeying costs, and, disciplinary action, up to and including termination.

## **D. APPROVAL AND REVISIONS**

**Approved By:** Emergency Policy Group, July 1, 2014

**Revision 1:** Emergency Policy Group, October 29, 2015

**Revision 2:** Policy Committee, January 18, 2017

**E. NEXT REVIEW DATE:** January 2018