Duke University - Facilities Access Governing Principles

Introduction

This document sets forth the Duke University facilities access governing principles, and defines responsibilities to maintain and apply these governing principles in accordance with the Buildings and Facilities Access Policy. The facilities access governing principles create a comprehensive expectation for managing physical access.

Duke is a community-based campus that generally allows open access to many campus buildings and facilities. The facilities access governing principles are established to balance security and functionality by respecting academic freedom, correlating with the campus physical security plan and acknowledging facility risk level.

The facilities owned, leased or operated by Duke University and its affiliated entities are deemed private property. These facilities are used for the conduct of instruction, research, patient care, housing, events, programs and administrative activities.

Definitions

1. **Access Management:** The process of granting, updating and terminating access to an individual or a group of individuals; and the process of setting, updating and enforcing access control governing principles
2. **Access Privilege:** Time-delimited or indefinite authorized building and/or door access granted to an individual or entity based upon role, responsibility or status
3. **Access Control Point:** A building exterior or interior ingress or egress point or an exterior gated ingress or egress point with access controlled using a device such as a manual lock, electronic access technology or visual identification process
4. **Facility Classification:**
    a. Occupancy - residential, in-patient care, child care, vivarium, controlled substances
    b. *Activity Conducted* – research, instruction, patient care, administration, event, public assembly, parking structures, data centers, utility plants and community benefit
    c. *Location* – campus sector, proximity to traffic artery, off-campus
    d. *Ownership* – Owned, leased, operated
    e. *Other* – mixed-use occupancy, mixed-use activity, mixed-use public venues, athletic venues and restricted facilities
5. **Local Facility Authority:** The designated responsible person for management of facilities use, assignment of space and setting hours of operation
6. **Duke Facilities:** all buildings and physical spaces owned or leased by Duke University for the purpose of ongoing or non-temporary Duke activities or programs
7. **Egress:** Building or sector exit points
8. **Ingress:** Building or sector entrance points

9. **People Classification:** The group to which a person belongs based upon functional role, authorized activities, enrollment, job description or other generally-accepted criteria. These include:
    a. Faculty – academic instructors or researchers appointed to full-time, part-time or adjunct positions, visiting faculty
    b. Students – individuals enrolled and/or participating in undergraduate or graduate courses, summer programs or post-graduate research programs and authorized
    c. Staff – all full-time, part-time or temporary Duke employees who are not members of the faculty
    d. Service Groups – Duke employees who require expanded building access to provide specialized services for the campus (for example: police, housekeeping, facilities maintenance, network/communications technicians)
    e. Affiliates and Sponsored Guests – visiting students, visiting scholars, third-party service providers and extended-term visitors who are authorized to enter and/or occupy secured campus facilities
    f. Visitors – short-term guests and event attendees who do not require non-public access to Duke facilities
10. **Sector:** A portion of a single facility or building with defined interior ingress/egress points (i.e., an entire floor of a building or research laboratories adjacent to administration or instruction space)

Facilities Access Governing principles

All Duke Facilities will be governed and managed based upon defined implementation governing principles. In the event of multiple activities within a single facility, the most restrictive expectation will govern the affected sector or facility.

1. **Physical Security Plan:** Facilities Access Governing principles comply with and support the provisions of the Physical Security Plan(s) in place for Duke University and its affiliated entities. Duke public safety can access control resources will work with local facility authorities to help them ensure their facilities comply with this standard, the Physical Security Plan and applicable best practices for security and facility control.
2. **Exterior Ingress / Egress Settings:** The default setting is "locked" for all exterior ingress and egress access points. During standard hours of public access or conduct of academic or business operations, the local facility authority may set the default as "unlocked". All facilities must have proper emergency exit provisions as governed by local and state building and fire codes.
3. **Interior Ingress / Egress Settings:** The default setting for interior doors will be "unlocked", excluding exceptions noted in items 4 and 5 (below). At the local facility authority's discretion, interior doors and access points may be locked before and after standard business hours. All facilities must have proper emergency exit provisions as governed by local and state building and fire codes.
4. **Other Interior Door Default Settings:** The default setting for all other interior doors not addressed in (2) or (3) above will be "unlocked", excluding research laboratory facilities,

individual offices, controlled inventory rooms and information technology data rooms. At the local facility authority's discretion, interior doors and access points may be locked before and after standard business hours. At the local facility authority's request, the Executive Vice President or the authorized designee may authorize full-time "locked" status for designated interior doors that do not otherwise represent a high risk or are not classified as regulated access points

5. **High Risk and Regulated Access Settings:** The default setting is "locked" for all interior doors and access points leading to high risk areas or those required by regulation to be locked at all times. High risk areas are determined by the local facility authority and/or an institutional compliance officer based upon occupant protection, sensitivity of work performed in the area, activities conducted in the area, regulatory requirements or the value of the assets located in the area. Examples include (but are not limited to): residential rooms, research laboratories, animal housing facilities, electrical and mechanical rooms, roofs, utility plants and infrastructure, and data centers. In some cases, additional security or access control mechanisms (such as video, enhanced identity techniques, etc.) may be warranted for doors and access points in these areas.
6. **Access Privileges:** Individual access privileges are based on defined criteria, which includes the people classification, residential status, work location and duties, nature of affiliation and functional roles. Local facility authorities may request exceptions to the policy or governing principles, which must be approved by the Executive Vice President or the authorized designee.
7. **Access Management:** The following functions will be responsible for ongoing access management:
    a. *Access Control Point Inventory* – Facilities Management Department (FMD), in conjunction with the DukeCard Office, must maintain a comprehensive inventory of the location and installed device for all exterior access points and for all non-standard (based upon FMD policy) hardware installed on interior doors. This must include a comprehensive inventory of the location and installed device for all authorized system-controlled or network-enabled access control points.
    b. *Access Hardware* – Facilities Management Department (FMD) will install and maintain all door and lock hardware and access control hardware that are not network-enabled for electronic authentication. The Office of Information Technology (OIT) and/or the FMD will install and maintain all network-enabled electronic lock and access control devices. FMD and OIT establish and maintain policies and procedure to coordinate service requests, installation protocol and ongoing maintenance responsibilities.
    c. *System Authentication Access Control Points* – The Facility Classification and Facilities Management risk level will govern access points that are required to maintain online or offline system authentication access control.
    d. *Standard Building Hours* – The Local facility authority establishes, publishes and updates the standard hours of operation for the building or sectors of the building.
    e. *Network-enabled Access Authentication* – The DukeCard Office administers and maintains the hardware, software and databases used to enable network-enabled or "system" authentication access control based upon individual access privileges,

standard hours of operation, or calendar of events. The DukeCard Office may additionally provide local facility authorities and others authorized by the EVP with limited distributed administration rights to access administration or door control.

8. **Facilities Access Committee:** The EVP appoints membership to a Facilities Access Committee that is responsible for outlining access privilege roles based on group membership (i.e., student, faculty, staff, sponsored guest, service provider, etc.). The EVP designates responsibility to the committee to address exceptions and requests on a building or specific case basis.
9. **Financial Responsibility:** Duke will allocate the cost of installing and maintaining all hardware and systems used to comply with the Facilities Access Governing principles. Local facility authorities will be responsible for additional one-time and annual costs incurred for specific approved requests that exceed the Facilities Access Governing principles.