Standard for Physical Security of Division of IT Facilities

Physical security of Division of IT (DoIT) facilities must be maintained to reduce potential loss, theft, damage, service interruption, breach of sensitive data, and unauthorized access. Physical access to division facilities, including leased spaces, is provided to authorized individuals via mechanical and electronic methods. Access to these facilities is a privilege and is determined based on the needs and requirements of the university. The safety and security of DoIT personnel, physical space, assets, and sensitive information is a shared responsibility of all Division of Information Technology employees.

1. Purpose: This standard establishes expectations for access to and use of DoIT facilities by employees and authorized visitors. It describes the responsibilities, conditions, and practices for mitigating risks and maximizing the protection of personnel, physical assets, and private information within the control and/or ownership of the university.

2. Scope: This standard applies to all Division of IT employees and individuals with authority to access DoIT facilities. It applies generally to all DoIT facilities but does not preclude the existence of more specific security and access procedures for areas having unique security requirements e.g. Data Centers, Telecom Rooms).

3. Standard: This standard sets forth the following expectations and responsibilities.

i. DoIT employees must not share their access credentials or physical keys with anyone.
ii. DoIT employees should not prop doors or hold them open for others to enter, especially individuals they do not know. Employees should keep secured doors locked during times designated by the supervisor or facilities manager. Likewise, windows should not be left open when an area is unoccupied.
iii. Employees and their visitors may only access a space for the intended use of the space and activities within the facility must be consistent with the business reason for accessing the facility.
iv. Employees must always accompany visitors while on premises and are responsible for violations of this standard by the visitors they authorize to be there. If there is a need for a visitor to be on the premises outside of business hours, a responsible employee will be selected by a supervisor to escort the visitor and be responsible for ensuring they vacate the facility when the business need is concluded.
v. All critical, valuable, or sensitive information handling activities must take place in areas which are physically secured and protected against unauthorized access, interference, and damage.
vi. In work areas or during meetings in which sensitive data is being used or discussed, individuals who are not DoIT employees or authorized contractors or consultants must be supervised by an authorized DoIT employee and must be made aware of the importance of maintaining confidentiality and integrity of the data.
vii. Within DoIT facilities, university-owned equipment should be located in areas that protect it from physical and environmental threats to minimize the risks of loss, damage, theft or compromise of assets and interruption to the organization’s activities.
viii. All building maintenance or secured card access requests should be made using the IT Buildings and Grounds Maintenance (Facilities) portal on the 4Help website.

ix. Violations of this standard by university employees may result in loss of some or all access privileges and in disciplinary action when appropriate.
x. DoIT employees who observe behavior of others in the facility that indicates potential violation of this standard must report it immediately to their supervisor.

4. Definitions

Access Credential: A means of gaining physical access including physical keys, Hokie Passport Cards, fobs, and other access mechanisms provided by the DoIT or the university.

Authorized User or Visitor: An individual in possession of a physical access credential or who is authorized to use or visit the facility, as evidenced by Visitor badge and/or being escorted at all times by a DoIT employee. Visitors are authorized by proxy when on the premises together with one or more authorized persons.

5. References

Division of IT Facilities Manual

University Policy 5000, University Facilities Usage and Events: https://policies.vt.edu/5000.pdf

6. Maintenance of Standard

The CIO's Chief of Staff is responsible for this IT Standard. Questions may be directed to kmccrery@vt.edu.

7. Revisions