

*Data facilities* are controlled facilities with a primary purpose of housing servers, networking equipment and other computing *devices*. Access to university, college, department or other *data facilities* must be controlled and restricted to appropriate personnel.

### 1. Administrative Standards

Access control procedures must be in place to reasonably ensure that only authorized personnel have access to a *data facility*. Access privileges must be reviewed at least annually.

Visitor, contractor or other appropriate but non-routine access to a *data facility* must be granted and escorted or logged by designated personnel. Either a visitor or service badge must be assigned or the person must be escorted while in a *data facility*.

### 2. Environmental Standards

Adequate conditioned power, uninterruptible power supplies, fire suppression devices, climate control and other environment maintenance equipment must be used if an assessment of the criticality and sensitivity of systems housed within the *data facility* deems it appropriate.

**Note:** The need for and depth of these types of services within the *data facility* is information developed within a business continuity and disaster recovery plan.

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

### Related Standards, Procedures and Information

Information Security Terms Guideline (IS-G100)  
Information Security Policy (IS-100)  
Access Control Standard (IS-S500/700)  
Management Responsibilities for Information Security Standard (IS-S400)  
Business Continuity and Disaster Recovery Planning Standard (IS-S900)  
Policy on Access to University Building Restricted Areas

### Revision History

Initial Draft	11/20/07
Effective Date	7/1/08