The City University of New York

IT Security Procedures - Data Center Security & Environment Supports, #2009-02

Issued by: Brian Cohen, Associate Vice Chancellor and Chief Information Officer
Effective date: 12/01/2009, Last revision date: 11/20/2009
Questions, comments, revisions: Computing & Information Services Information Security, security.cuny.edu

---

Scope: Data center facilities managed by the University or Colleges.

Related Policies and Procedures (under Info Security Policies at security.cuny.edu):
Policy on Acceptable Use of Computer Resources
IT Security Procedures

1. At a minimum the following protections must be provided:

   a. Data centers will have controlled access either through card swipe capabilities or key locks. Access cards and keys will be given only to those with a strict need to access, re-evaluated annually by the College CIO or, for Central Office departments, the University CIO. Access cards and keys will be retrieved and access revoked immediately when responsibilities no longer require access or upon termination of employment.

      For data centers with card swipe systems, all authorized persons entering a data center at the same time will each be required to swipe his or her badge for entry.

      For data centers with key access, combination lock or similar systems, all authorized persons will sign-in on an entry/exit log book located near the data center entrance.

      Regardless of the access entry system type, visitors must be accompanied by an authorized person at all times and sign-in and sign-out on an entry/exit log book.

      Swipe badge logs and an entry/exit log book will be reviewed and regularly monitored by data center supervision. A record of this review will be maintained.

   b. The location of computer rooms will not be publicized unless faculty, students or staff have a business need to frequent the computer room for College-provided IT services (e.g., Help/Service Desk, printing, equipment disposal).

   c. Data center exit signage will be prominently displayed with a working fire extinguisher near each exit door, and fire safety training will be provided for data center operations staff.

d. All business-critical equipment will be protected from hardware damage due to power interruptions or fluctuations.

e. Copies of critical business data backups will be regularly rotated to a secure and accessible offsite location. An inventory of offsite-stored critical business data backups continually kept updated.

f. Temperature and humidity will be manually monitored and anomalies investigated and corrected by the appropriate staff.

g. Protective equipment and instructions for emergency water situations (e.g., floods, pipe bursts) will be immediately available to all data center staff.

h. Generally accepted data center0 cable labeling practices will be followed for wiring and cables.

2. An annual risk assessment to evaluate the adequacy of data center protection levels must be completed and documented. Investments in additional physical data center infrastructure will be a business decision made by the appropriate authorities based upon economic factors and the results of the risk assessment. Additional protection mechanisms may include:

a. Backup generators

b. Automatic fire suppression

c. Video surveillance

d. Emergency lighting

e. Camera surveillance and environmental monitoring in real time

f. Piggy back entry control

g. Water detection systems

h. Location of water pipes

i. Window elimination, re-enforcement, blinds/curtains