MacEwan UNIVERSITY | OFFICE OF THE CHIEF INFORMATION OFFICER

Manage the IT Physical Environment Framework

Standard

Effective Date: September 24, 2015

Authority & Alignment

Authority: D1200 Code of Conduct, D3300 Internal Controls, D8030 Technology Management
Alignment: International standards – Cobit, ISO 27002, NIST SP800-53 and SP800-63

Overview

The organization must have effective physical security controls in line with business requirements. The organization must have documented physical and environmental security standards for all areas that host in-scope financial or business critical systems or devices that support these systems.[1]

Protection for computer equipment and personnel requires well-designed and well-managed physical environment. The process of managing the physical environment includes designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions that result from damage to and loss of computer equipment.[2]

This standard outlines the requirements for the IT process of managing the physical environment that satisfies the business requirement for IT of protecting computer assets and business data and minimizing the risk of business disruption by focusing on providing and maintaining a suitable physical environment to protect IT assets from access, damage or theft. This is achieved by

- Implementing physical security measures
- Managing physical environment[3]

Scope

This framework standard will apply to the main data center, the disaster recovery site, and all communication rooms at all campuses of MacEwan University (the "University").

Compliance & Exceptions

Responsibility for compliance with University policies and standards extends to all members of the University community. Non-compliance may create risk for the University and will be addressed accordingly (see clause 4.5.1 "Respect for the law and University governance" of the University's policy D1200 Code of Conduct – Employees for additional guidance).

Standard Requirements[4]

The following requirements will apply to the main data center, the disaster recovery site, and all communication rooms:

---

[1] Office of the Alberta Auditor General, 2011 GCCR

[2] DS12 COBIT® 4.1 © 2007 IT Governance Institute

[3] Ibid.

[4] Much of the wording of the requirements is borrowed from COBIT® 4.1 © 2007 IT Governance Institute.

1. The Director of IT Infrastructure and Operations is responsible for the requirements of this standard and is accountable to the CIO for the effectiveness of all controls established to fulfill the requirements.
2. Information and Technology Services (ITS) will put in place equipment that is capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vandalism, or power outages. This equipment will be inspected regularly to ensure its proper functioning.
3. ITS will define and implement procedures to grant, limit, and revoke access to the main data center and the disaster recovery site according to business needs, including emergencies. Access will be justified, authorized, logged, and monitored. This will apply to all persons entering the areas, including staff, temporary staff, clients, vendors, visitors, or any other third party.
4. ITS will ensure that specialized equipment and devices are installed to monitor and control the environment in the data center, disaster recovery site, and communication rooms.
5. ITS will ensure that IT infrastructure components, including power and communications equipment, are managed in accordance with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.

Related Content

Type	*Link*
Reports	Air Conditioner service reports (Facilities) UPS Service Reports Facilities Incident Reports Server Room door access audit reports Visitor logs
Standard	IT Server Room Access Controls Standard

Measurement[5]

- ✓ Amount of downtime arising from physical environment incidents
- ✓ Number of incidents due to physical security breaches or failures
- ✓ Frequency of physical risk assessment and reviews
- ✓ Annual review of A/C, Emergency Generator, UPS reports

Contact

Director, IT Infrastructure and Operations

[5] Ibid.