1. Introduction

1.1. This document gives additional details about implementing the "Physical Security" policy stated in Operations Policy for IT Service Providers (ISP-S6).

2. Building security

2.1. Normal / medium level physical security

- This applies to offices and other locations which house information, information systems or IT equipment and where no sensitive or highly confidential information is stored (in an unencrypted form). It also applies to data and voice network infrastructure housed outside secure computer rooms.

- In general there should at least be one substantial physical security measure in place at all times to protect unattended information assets.

- Staff must keep the doors and windows of unattended offices locked.

- Outside normal building opening hours building entrances, office doors and windows must be kept locked when unattended.

- Data and voice network infrastructure housed outside secure computer rooms must be physically secured, e.g. in locked security cabinets.

- Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

2.2. High level physical security

- This applies typically to computer server rooms housing important information systems or communications systems equipment. However, it may also apply to other situations where high value or highly sensitive information in an unencrypted form is being held or handled.

- Physical security to an appropriate higher standard is required. Special requirements to achieve this may involve use of:
  - Intruder detection (burglar alarms)
  - Environmental monitoring and alerting systems
  - Strong rooms
  - Door and window locks
  - Systems to control and log access to sensitive areas
  - Out-of-hours security support
  - Specialised fire extinguishing systems (which may be automatic)
• Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

2.3. Departmental managers are responsible for defining to Estates their building security requirements and Estates is responsible for determining the specifics of how to implement those requirements.

2.4. University Staff are obliged to implement or comply with building security arrangements affecting the areas they work in or visit.

2.5. A proper system to manage building access controls must be in place to cover all University buildings. This system is ultimately the responsibility of Estates.

2.6. Where Estates directly manages access controls it must hold accurate data about who is in possession of keys, access cards and access codes.

2.7. Where responsibility for managing access controls is delegated to departments, then Estates must maintain accurate data about what access controls are delegated and to whom.

2.8. Where responsibility for managing physical access controls, such as door keys or access cards, is devolved to departments then it is the responsibility of the Head of Department to ensure that a proper system to manage them is in place.

---

**Failure to comply with University Policy may lead to disciplinary action.**

---

**Document history:**

23 March 2007 (C. Nelson) Began first draft.


06 July 2010 (C. Nelson) Steering group advised change to “data and voice communications equipment”; replaced it with “data and voice network infrastructure”.

---

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.