Sheffield Hallam University

Physical and Environmental Security Policy

Issuing Authority: Leon Etherington,
Acting Chief Information Officer,
Information Systems and Technology

Signed: 

Date Effective: March 2016

Review date: February 2018

Version: 2016.2

Physical and Environmental Security Policy

Objective

To prevent unauthorised access or damage to IT services. To prevent the loss of, damage to, or compromise to information assets, and interruption to the business activities of the University.

Policy Requirements

1. All computer equipment that provides access to University information should be kept secure by physical means or by using good practice (this is especially important for users of mobile devices: refer to the ***Working off-campus policy and guidance***).
2. File servers and equipment that store or process key information or high availability data shall be located in physically secured areas.
3. Entry to secured areas shall be restricted to authorised users:
   - Employees of the University shall have their SHUcards encoded with the access rights approved by their line manager and the Director of IS&T.
   - Employees shall not lend their SHUcard to anyone, or allow anyone to follow them through card-controlled doors (tail gating)
   - Access rights shall be revoked immediately for staff who leave the employment of the University
   - Other visitors shall be granted access for specific and authorised purposes only, and shall be supervised
   - A log shall be maintained of all access to restricted areas, via the signing out of access keys and the entry card system logs.
4. ***Cabling between buildings***
   Cables between buildings should be underground wherever possible. Ducts and entry points into buildings should be secure, and inspected annually for signs of damage or interference. A log of these inspections shall be retained by Head of Networks and Infrastructure.
5. ***Internal cabling***
   Wherever possible, cabling within buildings should be installed in ceiling voids and secure ducts.
6. ***Wireless access points***
   Wherever possible, wireless access points should be installed at a high level to make them less exposed and more secure from theft or tampering.
7. ***Communications racks and wiring cabinets***
   All communications equipment shall be kept secure, either in locked rooms or in racks and cabinets with locks. Keys to communications rooms, racks and cabinets shall be held securely by technical specialists and the University Security Service so that they are not available to individuals who are unauthorised to access network devices.
8. ***Environmental controls***
   Data centres shall be protected by appropriate air conditioning and very early smoke detection (VESDA) systems. Temperatures in data centres shall be monitored by Operations staff, and undue variances reported immediately to the University's Estates Department.
   Equipment shall be protected from power failures or electrical anomalies. Data centres shall be protected by suitable local stand-by power supplies (generator or uninterruptible power supply).
   Wiring cabinets, and the rooms in which they are located, should be inspected annually to assess security risks and hazards arising from environmental conditions. A log of these inspections shall be retained by Head of Networks and Infrastructure.

9. ***Equipment Maintenance***

   Equipment shall be maintained in accordance with manufacturers' recommendations, to ensure its availability and integrity. All faults (or suspected faults) shall be logged in the current Incident Management System and all changes shall be logged in the current Change Management System. All regular maintenance checks such as PAT testing shall also be recorded.

10. **Inventory**

    An inventory shall be maintained of file servers and communications equipment and recorded in the current Asset Management System, which shall be regularly checked to ensure that the University's information assets are accounted for.

11. ***Disposal of Equipment***

    All items of equipment containing storage media shall have any software or sensitive data irretrievably removed before disposal, or shall be processed by a company that is accredited by ICER (Industry Council for Electronic Equipment Recycling) to recycle IT equipment and that will provide certification of destruction of data. This shall be in accordance with the Disposal of IT Equipment Policy