Owner:	**Chief Information Officer**
Version number:	1
Date of approval:	June 2019
Approved by:	**Information Security Steering Group**
Effective date:	June 2019
Date of last review:	**New**
Due for review:	December 2019

Physical Security Policy

1. SCOPE AND PURPOSE

1.1 This policy is a sub-policy of the Information Security policy and applies to all staff employed by the University including individuals working on a voluntary, honorary, placement or casual basis or through an agency and authorised users that have access to information and information technology provided by or through Bournemouth University (BU).

1.2 This policy sets out BU's intent and commitment and its expectations of those listed above to preserve the confidentiality, integrity and availability of the information it holds on behalf of its students, staff and other stakeholders.

1.3 This policy also aims to ensure BU's regulatory compliance, operational resilience, reputation and ability to sustain revenue.

1.4 This policy covers the topics related to Physical Security which includes:

a) physical protection
b) power supplies
c) hazard protection

2. KEY RESPONSIBILITIES

2.1 The BU Board has delegated day-to-day responsibility for compliance with the policy to the Chief Information Officer.

2.2 Executive Deans of Faculties and Directors/Heads of Professional Services will be responsible for information security within their area of business and directly accountable to the Chief Information Officer (CIO) and BU Board for findings in non-compliance to this policy

2.3 Business and System owners, including academic staff, are responsible for implementing the administrative and technical controls which support and enforce this policy.

2.4 All those outlined in 1.1 are responsible for complying by adopting the process and procedures which support this policy.

3. LINKS TO OTHER BU DOCUMENTS

3.1 In addition to this document and the supporting set of “strategic policy” documents which form the Information Security policy set, there are several BU policies which compliment this policy, as follows:

- Information Security Policy
- Data Protection Policy
- Disciplinary Policy
- Acceptable Use Policy
- Access Management Policy
- Mobile Computing Policy
- CCTV Policy and Procedures

Policy

4. PHYSICAL PROTECTION

4.1 There will be documented standards/procedures for the physical protection of the BU infrastructure including its buildings, facilities, power supplies, water and drainage, emergency services, data centres, networks, telecommunication equipment, offices and other important assets.

4.2 Standards/procedures will cover:

a) protecting critical facilities against unauthorised access
b) locating critical facilities away from public access or approach
c) managing the authorisation for access to facilities
d) restricting visitor access in controlled areas

4.3 Buildings that house critical facilities should be protected against unauthorised access by:

a) providing physical protection on vulnerable access points, eg locks, security guards, etc
b) utilising closed-circuit television (CCTV)
c) utilising intruder detection systems and testing them regularly

4.4 Critical facilities should be protected by locating them away from public access and keeping details confidential when creating signage, drafting building plans, telephone directories and maintenance schedules.

4.5 Physical access to critical facilities will be protected by:

a) defining and strengthening the physical security environment
b) keeping buildings under surveillance
c) locating computer screens so that information cannot be overlooked
d) isolating holding areas for receipt of deliveries

4.6 Access to critical facilities, including those that support or enable the organisation's infrastructure, should be restricted to authorised individuals by:

a) installing locks activated by keypads, swipe cards or equivalent
b) locking doors and windows when the environment is vacated
c) fitting intruder alarms
d) ensuring all individuals wear visible means of identification
e) requiring staff to challenge strangers
f) using security guards

4.7 Authorisation to gain physical access to critical facilities will be:

a) issued in accordance with documented procedures
b) reviewed regularly, to ensure that only appropriate individuals are allowed access
c) revoked promptly when no longer needed

4.8 Visitors to critical facilities will be:

a) permitted access only for defined and authorised purposes
b) monitored by recording arrival and departure times
c) obliged to wear visitor identity badges at all times when on the organisation's premises
d) supervised at all times
e) issued with instructions explaining the security requirements detailing emergency procedures and, where appropriate, restricting the use of audio and video recording equipment
f) required to return all physical access mechanisms, such as keys or access cards, once they are no longer needed

4.9 Individuals will be required to obtain written approval before leaving the organisation's premises with critical IT equipment (servers, network devices, specialist equipment).

5. POWER SUPPLIES

5.1 Power supplies to facilities should be protected against power outages to prevent services from being disrupted.

5.2 Supplies to facilities should be protected by:

a) uninterruptible power supply (UPS) devices
b) installing surge protection equipment
c) providing backup electricity generators, with adequate fuel, in the event of extended power failure
d) installing emergency lighting in case of main power failure
e) where deemed appropriate, locating emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency

5.3 UPS devices should have the battery capacity to allow critical systems, network equipment, voice facilities and supporting systems to shut down in an orderly manner.

5.4 Emergency equipment should be serviced in accordance with manufacturer recommendations and tested regularly.

6. HAZARD PROTECTION

6.1 Facilities such as data centres, networking and telecommunications equipment and other important assets should be protected against fire, flood, environmental and other hazards.

6.2 They should be located in a safe environment and in areas that are:

a) constructed using fire resistant materials for walls, doors, windows and furniture free from intrinsic fire hazards
b) fitted with fire detection systems
c) protected with fire suppression systems

6.3 Fire alarms should be monitored continuously, tested regularly and serviced in accordance with manufacturer specifications.

6.4 The impact of hazards should be minimised by:

a) locating hand-held fire extinguishers so that minor incidents can be tackled quickly
b) training staff in the use of fire extinguishers and other emergency/safety equipment, and in evacuation procedures
c) conducting fire drills so that staff know how to safely exit the organisation's premises
d) monitoring and controlling the temperature and humidity of data centres and computer rooms in accordance with manufacturers' recommendations

General

7. REFERENCES AND FURTHER INFORMATION

7.1 The Information Security policy and this sub policy are written in accordance with the Information Security Forum (ISF) Standards of Good Practice (SOGP).