DATA CENTRE SECURITY

SUMMARY OF PRINCIPAL CHANGES

General changes
This document has been subject to the annual review process led by the Chief Information Officer and has been re-issued with amendments, effective 1 September 2014.

*(Amendments to version **03.0,** Appendix IV, UPR IM01, are shown in italics.)*

Structure

1 INTRODUCTION

1.1 This document sets out the University's arrangements for Data Centre Security, the key principles which underpin them and is supplementary to the Information Management Policy (UPR IM02[1]). It should be read in conjunction with UPR IM01[2] and its relevant appendices and the national JANET Acceptable Use Policy.

1.2 This document is informed, but not bound by, the standard code of practice: BS 20000 and the UCISA/JISC Information Security Toolkit (Edition 3).

2 PURPOSE

The University's information and the systems that store and manipulate that information are major corporate assets which must be protected. In determining its Data Centre Security arrangements, the University has adopted principles, policies and practices which maximise protection against risks so that the security of its information and systems is assured and the health and safety of staff working within University Data Centres protected.

[1] UPR IM02 'Information Security Policy'

[2] UPR IM01 'Computer Networks, Security of Information Systems and the Protection of Information Systems from Computer Viruses'

3 SCOPE

3.1 All Members of the University, as defined in UPR GV06[3], are required to comply with these arrangements which also apply to collaborative activities undertaken with Partner Organisations.

3.2 The University's wholly-owned subsidiary companies and their wholly-owned subsidiaries which operate with the Financial Regulations of the University (UPR FR06[4]) are automatically subject to the policies and procedures set out in this document.

3.3 Wholly-owned subsidiary companies which operate with separate Financial Regulations and partly-owned companies will be subject to the policies and procedures set out in this document (Appendix IV, UPR IM01) unless, for good reason, an exception is granted by the Chief Information Officer, in which case the necessary provision will be made in the Financial Regulations, Shareholder's Agreement and Memorandum of Understanding.

4 ACCESS TO DATA CENTRES

4.1 Data Centres must be kept locked at all times.

4.2 *Other than in an emergency (section 4.6, refers)* access to Data Centres, cabinets and their contents and computer network equipment is restricted to persons authorised by the Chief Information Officer (or nominee).

4.3 For regular authorised access to Data Centres, a person must complete a Data Centre Access Request Form and obtain an authorised access card from the Chief Information Officer (or nominee).

4.4 All persons granted authorised access to Data Centres must undertake the required training and comply fully with Data Centre security requirements and all relevant University policies and regulations.

4.5 Where a University post has designated specific Data Centre responsibilities, this will be made clear in the Job Description and staff appointed to such posts must receive an appropriate briefing and training as part of their induction.

4.6 Access in an emergency

4.6.1 In the event of fire or other emergency, Security Staff and/or staff of the Department of Estates, Hospitality and Contract Services and/or the emergency services and/or agreed University contractors, may enter a Data Centre without prior permission, to deal with the incident.

4.6.2 The Chief Information Officer (or nominee) must be notified of such entry as soon as reasonably possible.

4.7 Contractors and visitors

4.7.1 All contractors requiring regular and agreed access to Data Centres must follow the requirements of 4.2, 4.3 and 4.4 above and sign in and out of the Data Centre on each occasion.

[3] UPR GV06 'Membership of the University'

[4] UPR FR06 '*Corporate Governance and Financial Regulation'*

4.7.2 Contractors undertaking equipment maintenance, computer network services and information systems work must have obtained the prior approval of the Chief Information Officer (or nominee) and must also have obtained the appropriate authorisation and the necessary Contractors' badge in accordance with the procedures established by the Director of Estates, Hospitality and Contract Services and the requirements of the University's security regulations and procedures (UPR HS05[5], refers).

4.7.3 Contractors who fail to comply with these requirements may be challenged and may be asked to leave University premises if they are unable to produce a valid badge and the necessary authorisation.

4.7.4 Other contractors and visitors requiring ad hoc access to Data Centres must be escorted at all times by an authorised person nominated by the Chief Information Officer (or nominee); comply with the provisions of this University policy and regulation and *comply* with any specific instructions given by the authorised person during the course of their visit to the Data Centre

4.8 Installation of equipment

The specification of any equipment to be installed in a Data Centre and the arrangements for the installation of that equipment must have the prior written consent of the Chief Information Officer (or nominee).

4.9 Compliance

4.9.1 This section (4.9) must be read in conjunction with UPR IM08[6].

4.9.2 Data Centre management processes must enable the University to comply with its legal, statutory and contractual obligations and any national agreements that it has entered into.

4.9.3 It is the responsibility of each individual working within a Data Centre to ensure compliance with agreed good Health and Safety practices. These include, but are not limited to, ensuring all floor tiles are put back correctly after lifting, that no cardboard boxes or waste materials are left behind to cause a safety or fire hazard or to obstruct Fire Exits and that no equipment is tampered with or interfered with where the individual has not had appropriate authorisation and training or guidance in its use.

4.10 Outsourcing and third party access

4.10.1 This section (4.10) must be read in conjunction with section 6.3, *Appendix I,* UPR IM01[7] and UPR HS05[5].

4.10.2 External suppliers who are contracted to supply goods and services to the University that will bring them into contact with the University's Data Centre environment must agree to comply with the Data Centre Security arrangements set out in this document and with all other relevant University policies and regulations.

4.10.3 Any contracts with facilities management or outsourcing companies must have incorporated within them agreed service levels consistent with the regulations set out in this document so that Data Centre security issues are addressed.

[5] UPR HS05 'Security and Public Access'
[6] UPR IM08 'Data Protection'
[7] *Appendix I, UPR IM01 'Computer Network Management Policy'*

4.11 **Operations**

4.11.1 To ensure on-going compliance with Data Centre security requirements, changes to operating procedures will require the prior written approval of Chief Information Officer (or nominee).

4.11.2 Data Centres must provide an appropriate level of physical security and access control. Members of the University with authorisation to enter such areas are to be provided with information on potential security risks and the measures in place to control them.

4.11.3 Duties and areas of responsibility must be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material/ reputational damage to the University.

4.11.4 Acceptance criteria for new information systems, upgrades and new versions shall include reference to the sustainability of those systems within the University's Data Centres.

4.11.5 The Chief Information Officer (or nominee) will:

i determine and disseminate procedures for the reporting of incidents, security breaches and potential security weaknesses in the University's Data Centres;

ii implement monitoring arrangements to inform Data Centre management;

iii determine and disseminate procedures for the reporting of Data Centre equipment malfunctions and faults;

iv require that all faults and malfunctions are logged and monitored and that corrective action is taken in a timely manner.

4.12 **Access Management**

4.12.1 This section (4.12) should be read in conjunction with UPR IM01[1], UPR IM19[8] and UPR SA12[9].

4.12.2 Procedures for managing the registration and de-registration of *the* authorisation of persons requiring access to Data Centres locations shall be established to ensure that all users access privileges match their authorisations. The Chief Information Officer will identify the authorised officers to manage and implement these procedures.

4.12.3 All users shall have a unique identifier (user ID) for their personal and sole use for access to all of the University's information services and systems. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason (section 5.2, Appendix II, UPR IM01[10], refers).

4.12.4 Access control standards must be established for all Data Centres which minimise security risks yet allows the University's business processes to be carried out without undue hindrance.

4.12.5 Access to all Data Centres must be authorised by the Chief Information Officer (or nominee) and a record must be maintained of such authorisations and the level of access privileges granted.

[8] UPR IM19 'Internet, Online communications and Social Media'
[9] UPR SA12 'Learning Resources'
[10] Appendix II, UPR IM01 'Security of Management and Administrative Information'

4.12.6 Procedures shall be established for all Data Centres to ensure that the access privileges of authorised persons are adjusted appropriately, and in a timely manner, whenever there is a change in business need or role. Authorisations and access privileges will be reviewed at regular intervals.

4.13 Use of Data Centres

4.13.1 This section (4.13) should be read in conjunction with UPR IM01[2], UPR IM19[7] and UPR SA12[8].

4.13.2 Data Centres must be safeguarded appropriately, especially when left unattended.

4.13.3 Controls will be established to ensure the safety and security of the Data Centre environment.

4.13.4 To limit their exposure to personal Health and Safety risks, Members of the University working within Data Centre environments will comply with the following Code of Practice:

a no food or drink may be brought into University Data Centres;
b packaging and/or waste materials must never be left inside;
c furniture must not be brought into any Data Centre without the express permission of the Data Centres Manager;
d aisles and exit routes must not be obstructed;
e cabinet keys must not be left in the racks (a key safe is provided for storage);
f power extension cables must never be used;
g the correct equipment for the job, for example, tile lifters or stepladders must always be used;
h the door to the Data Centre must never be propped open;
i no one must be allowed to ‘tail-gate’ behind another person entering a Data Centre legitimately.

4.13.5 The risk to human life associated with the fire suppression system must be fully understood and training undertaken in the emergency evacuation of the Data Centre.

4.13.6 All authorised persons with access to Data Centres are required to participate in annual refresher training in the safe and secure use of Data Centres. Access to Data Centres may be revoked where authorised users fail to undertake the required refresher training.

4.13.7 All authorised persons with access to Data Centres must comply with health and safety requirements for lone working, working in confined spaces, electrical safety and hazardous chemicals.

4.14 Systems Planning

The implementation of new systems or related projects must be agreed by the Chief Information officer (or nominee) prior to installation into the Data Centre.

4.15 Management guidelines

4.15.1 Changes to equipment supporting critical business systems must be planned in advance to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

4.15.2 Equipment supporting critical business systems shall be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

4.16 **Systems Management**

4.16.1 This section (4.16) should be read in conjunction with UPR IM01[2].

4.16.2 Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be available.

5 MONITORING AND REPORTING

5.1 The Chief Information officer has overall responsibility for the approval and implementation of Data Centre Security policy and security arrangements.

5.2 The Data Centres Manager must be informed of all breaches of Data Centre security through regular reporting channels and in emergencies. The Data Centres Manager must report major breaches immediately to the Chief Information Officer.

5.3 This policy will be reviewed every three (**3**) years or, exceptionally, more frequently if risk analysis or audit suggests there are new security threats that require it to be revised.

Mrs S C Grant
Secretary and Registrar
Signed: **1 September 2014**