SECURITY OF MANAGEMENT AND ADMINISTRATIVE INFORMATION

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 minor amendments, effective 1 September 2014.

---

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

Structure

---

1 INTRODUCTION

1.1 This policy and its supporting regulations and procedures were originally approved by the Senior Executive Group with effect from 1 September 2001 and have b*een amended with effect from 1 September 2014 on the authority of the Secretary and Registrar* It provides a basis for ensuring that authorised workers have timely and appropriate access to and use of computerised administrative information, whilst safeguarding the confidentiality, security and integrity of that information and of the University's management and administrative information.

1.2 The University's information systems are accessed via and/or used in conjunction with the University's computer networks. This document should, therefore, be read in conjunction with Appendix I, UPR IM01[1].

2 ADDITIONAL DEFINITIONS

For the purposes of this document (Appendix II, UPR IM01) the following definitions apply. These definitions are additional to those given in section 2, UPR IM01[2].

---

[1] Appendix I UPR IM01 '*Computer Network Management Policy*'

2.1 **'Authorised Member':**

a person employed by, or retained as a consultant and/or on a temporary or casual basis, by the University, the wholly-owned subsidiary companies of the University or their wholly-owned subsidiaries or staff of member institutions of the Hertfordshire Higher Education Consortium (HHEC) who, as part of the remit of their duties for the University, subsidiary company or Consortium, require access to the University's management and administrative information and whose access to these systems has been authorised in accordance with the regulations set out in this document;

2.2 **'confidential information':**

any information that requires special safeguards because of its private nature, in particular, personal information relating to staff and students or information that is commercially sensitive;

2.3 **'management and administrative information':**

a central or local information system and its content used by the University for corporate management and/or for administrative purposes.

3 SCOPE

3.1 This policy applies to all management and administrative information owned, managed or supported centrally within the University and/or by Strategic Business Units and/or by the wholly-owned subsidiary companies of the University or their wholly-owned subsidiaries. 'Conduct of the University's business' would include, but is not limited to, all administrative functions undertaken by Authorised Members on behalf of the University or its subsidiary companies by means of the University's information systems, the creation of teaching materials, the production of research papers and any other activities conducted via the University's staff network.

3.2 The policy applies to any person accessing or using any administrative information system owned, managed, supported or operated by or on behalf of the University of Hertfordshire, including any such information system that is not operated on University premises and equipment loaned to Members of the University for business use at home *under the provisions of UPR FR06*[3].

3.3 This policy should be read in conjunction with the University's Data Management Policy (UPR IM16[4]) and its appendices.

4 POLICY

4.1 Development and support of information security processes

4.1.1 It is the policy of the University to implement processes to protect the security and confidentiality of its management and administrative information. These processes will:

i identify who may be permitted to access the University's management and administrative information;

ii stipulate the extent to which these individuals may be permitted to manipulate the University's management and administrative information;

iii make clear the obligation placed on authorised workers to maintain security and confidentiality;

---

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

3 UPR FR06 'Corporate Governance and Financial Regulation'

4 *UPR IM16 'Data Management Policy'*

iv specify the arrangements for the release of information;

v establish mechanisms to secure management and administrative information against loss, damage, corruption or unauthorised access or use.

4.1.2 The University will address security issues during the purchase and implementation of all new management and administrative information systems. All management and administrative information systems purchased or implemented by the University will, therefore, be capable of compliance with these regulations.

4.1.3 Where appropriate, Heads of Strategic Business Units will develop and maintain local management and administrative information security policies which are consistent with this policy for those areas for which they are responsible.

4.1.4 The Human Resources Development Unit will ensure that the induction programme for all new staff includes specific information and advice concerning this policy and local management and administrative information security policies.

4.1.5 Heads of Strategic Business Units will establish appropriate procedures within those areas for which they are responsible, to ensure that members of staff receive a copy of this document and any local management and administrative information security policy that may apply and any amendments that may be made to these subsequently.

4.2 **Authorisation to access management and administrative information**

4.2.1 Access to the University's management and administrative information will be granted solely for the purpose of enabling the conduct of the University's business. Therefore, the level of access granted to an individual will be consistent with his or her responsibilities as an Officer of the University.

4.2.2 Each manager is responsible for determining the management and administrative information to which individuals for whom they are responsible should be allowed access.

4.2.3 The University's management and administrative information may be accessed only by Authorised Members (section 2.1, refers). This access will be in accordance with the limits of the authority granted to them.

4.2.4 The Chief Information Officer, in conjunction with the relevant Data Stewards, will establish appropriate mechanisms to monitor access to centrally managed management and administrative information. Heads of Strategic Business Units will establish consistent and appropriate mechanisms in line with this policy to monitor access to locally managed management and administrative information.

4.2.5 All passwords for the University's information systems are confidential. These include, but are not limited to, passwords to network systems, central computer systems, computer workstations and University on-line services.

4.3 **Security of management and administrative information**

4.3.1 Management and administrative information exceptionally located in unsecured areas (in particular desktop services equipment) must be secured against theft and use by unauthorised persons.

4.3.2 An 'unsecured area' is defined as an area that is not, nor cannot be, locked and/or an area that can be accessed by unsupervised students or other persons who do not have the appropriate clearance.

4.3.3 Authorised Members logging on to an information system must log off or lock the workstation when leaving the system unattended.

4.4 Security of computer-related media

4.4.1 Printed reports containing confidential or sensitive information must be stored in a secure area that cannot be accessed by individuals who do not have the appropriate authorisation.

4.4.2 These reports may be made available only to individuals who have the appropriate authorisation or clearance.

4.4.3 Confidential reports will be shredded before being discarded or disposed of via confidential waste sacks where these are available.

4.4.4 The use of portable media, such as disks and USB drives, for confidential information should be avoided. Where such media are used temporarily for holding confidential information, they must be protected physically and only made available to those with the appropriate authorisation. Information stored temporarily on portable media must be transferred promptly to University corporate systems and storage.

4.4.5 Managers will establish appropriate arrangements for the secure transmission of management and administrative information seeking advice, as appropriate, from the Chief Information Officer and/or appropriate Data Steward.

4.4.6 Managers will establish appropriate mechanisms for monitoring compliance with these requirements.

4.5 Protection of computerised files

4.5.1 Heads of Strategic Business Units will ensure that, within those areas for which they are responsible, schedules are established for making back-up copies on a regular basis of data files stored on computer workstations, network file servers and other computer systems and for recording that the necessary copies have been made.

4.5.2 All management and administrative information must be stored on the corporate systems and file storage infrastructure.

4.5.3 Back-up copies will be stored in a safe location (not exposed to heat or magnetic fields). Back-up copies for network file servers and central computer systems will not be stored in the same building as the related systems or file storage devices.

4.5.4 Managers will establish appropriate mechanisms for monitoring compliance with this requirement.

4.6 Off-campus and wireless network access to management and administrative information

Off-campus access and on-campus wireless network access via the VPN service to management and administrative information held in University systems and services on the staff network, is restricted to Members of the University in Membership category B (UPR GV06[5], refers) and to designated approved suppliers for whom off-campus access has been identified as essential by the appropriate Head of Strategic Business Unit and notified in writing to the Chief Information Officer (or nominee).

4.7 Security of networked management and administrative information

4.7.1 All networked management and administrative information must be on the staff network on a closed logical network that is distinct from that used by students. The network will be separated from external links with a secure firewall.

4.7.2 The Chief Information Officer will establish appropriate mechanisms for monitoring the firewall.

---

5 *UPR GV06 'Member of the University'*

4.8 **Security of central management and administrative information and computer networks**

On behalf of the University, the Chief Information Officer and the appropriate Head of Strategic Business Unit will:

i develop, implement and maintain appropriate disaster prevention measures and a documented disaster recovery procedure for central management and administrative information and computer networks;

ii develop, implement and maintain a documented change control procedure for central corporate applications and associated programs.

5 IMPLEMENTATION

5.1 System Security Administration

5.1.1 The Data Steward (or nominee) designated for the management and administrative information concerned, is responsible for the authorisation of access privileges and user roles for use of the management and information system through an authorisation process agreed with the Chief Information Officer.

5.1.2 All authorised access privileges and user role(s) for Members of the University will be notified to the Chief Information Officer who will arrange for their secure implementation using an individual University username and password for each authorised person.

5.1.3 The Chief Information Officer will maintain a list of all authorised Data Stewards and their nominees and their respective areas of responsibility (Appendix I, UPR IM16[1], refers).

5.2 Passwords

5.2.1 Each Authorised Member who is granted access privileges and user roles for use of a management or administrative information system will have a unique, personal password associated with his or her University username. Each user is responsible for keeping this password confidential and secure and for changing this password in any circumstances where they may have reason to believe the security has been compromised or it may have become known to another person.

5.2.2 Other than in exceptional circumstances, passwords must not be shared between users, including users who are employed on a 'job sharing' basis. Exceptions to this regulation are permissible only with the prior written approval of the responsible Data Steward who must notify the Chief Information Officer of the exception and the reasons for granting permission.

5.2.3 Managers will establish appropriate mechanisms for monitoring compliance with this requirement.

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