Royal Holloway University of London

Information Security Policy

Document Id	Information Security Policy
Sponsor	Laura Gibbs
Author	Nigel Rata
Date	15th May 2014

RHUL, Egham Hill, Egham, Surrey, TW20 0EX.

Version Control Log

Version	Date	Change
1.0	10/01/09	Initial draft for review
1.1	12/08/10	Updated
1.2	12/05/10	Updated
1.3	6/10/10	Updated
1.4	02/03/11	Updated based on comments from ITUAG (19/10/10)
1.5	21/02/12	Remove 'confidential' status to 'For internal use'
1.6	13/02/13	Annual review and update
1.7	15/05/2014	Annual review and update

Document Approval

Name	Approval Date
Laura Gibbs	27.5.14
ITUAG	11.12.14

1. Introduction

The University recognises that information and information systems are valuable assets which play a major role in supporting the University's strategic objectives. Information security is important to the protection of the University's reputation and the success of academic and administrative activities. It is also an integral part of the information sharing which is essential to academic and corporate endeavour. The management of personal data has important implications for individuals and is subject to legal obligations. The consequences of information security failures can be costly and time-consuming.

The Information Security Policy sets out appropriate measures through which the University will facilitate the secure and reliable flow of information, both within the University and in external communications. It comprises this document, which sets out the principles and framework, and a set of specific policies, codes of conduct and guidelines addressing individual aspects of security (listed in Appendix A). The approach is based on recommendations contained in British Standard 7799 - A Code of Practice for Information Security Management.

2. Objectives

The objective of the Information Security Policy is to ensure that all information and information systems upon which the University depends are adequately protected to the appropriate level.

3. Scope

The Information Security Policy applies to information in all its forms. It may be on paper, stored electronically or held on film, microfiche or other media. It includes text, pictures, audio and video. It covers information transmitted by post, by electronic means and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

The policy applies to all staff and students of the University and to other users associated with the University. With regard to electronic systems, it applies to use of University owned facilities and privately/externally owned systems when connected to the University network directly or indirectly. ('Owned' is deemed to include leased, rented or on-loan).

The policy applies to all University owned/licensed data and software, be they loaded on University or privately/externally owned systems, and to all data and software provided to the University by sponsors or external agencies.

4. Policy Statement

The University is committed to protecting the security of information through the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure
- integrity: safeguarding the accuracy and completeness of information and processing methods
- availability: ensuring that information and associated services are available to authorised users when required

The University will develop, implement and maintain policies and procedures to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security, in particular the following policy requirements:

4.1 Authorised Use

University information systems are provided to support the University's activities including learning, teaching, research, administration and approved business activities. Only staff, students and other persons authorised by appropriate University authority are entitled to use the University's information systems.

4.2 Acceptable Use

All users have an obligation to use information and information systems responsibly. Rules are defined in the Regulations for use of University Computing Facilities and in Acceptable Use policies. Users accept these terms of acceptable use when they either connect a device to the RHUL data network (via wire or wireless connection) and/or log onto the RHUL computer systems.

4.3 Monitoring and Privacy

The University respects the privacy of its users and there is no routine monitoring of e-mail content or individual Web access. However, the University reserves the right to make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers Act.

4.4 Protection of Software

All users must comply with the Copyright, Designs and Patents Act 1988 under which it is an offence to copy software or licensed products without the permission of the owner of the copyright.

4.5 Retention and Disposal of Information

All staff have a responsibility to consider security when using and disposing of information in the course of their work. The University will determine retention periods for certain kinds of information and departments should establish procedures appropriate to the information held and processed by them, and ensure that all staff are aware of those procedures.

4.6 Virus Control

The University is developing an Antivirus Policy and it will be an offence within the University Regulations to knowingly introduce a virus or take deliberate action to circumvent precautions taken to prevent the introduction of a virus. Currently all domain based, centrally managed computers should run the centrally managed virus protection software.

4.7 Business Continuity

The IT Department will contribute to, and regularly update, the University business continuity management process to counteract interruptions to normal University activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

5. Legal and Contractual Requirements

The University will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing if information. This includes the following Acts and the guidance contained in the Information Commissioner's Codes of Practice:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act (1988)
- Data Protection Act 1998
- Freedom of Information Act (2000)
- Human Rights Act (1998)

- Regulation of Investigatory Powers Act (2000)

The University will also comply with all contractual requirements related to the holding and processing of information:

- JANET Acceptable Use Policy issued by UKERNA
- Code of Conduct on the Use of Software and Datasets issued by JISC
- The terms and conditions of licences and contracts
- The terms and conditions of authentication systems, eg. Athens

6. Responsibilities

The IT department is responsible for the Information Security Policy.

The IT department will designate the role of Information Security Officer within the department who will be responsible for development of the policy, will co-ordinate implementation and dissemination, and will monitor operation. Each specific policy will have a Nominated Officer responsible for updating of that element of policy (see Appendix A). The Nominated Officer, assisted by the Information Security Officer, will promote awareness of and compliance with the policy, provide advice and guidance on good practice relating to the policy, and bring forward revisions to the policy as necessary.

Everyone granted access to University information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policies, codes of conduct and guidelines.

Each individual is responsible for protecting the University's information assets, systems and infrastructure, and will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

All staff, students and other users should report immediately any observed or suspected security incidents where a breach of the University's security policies has occurred, any security weaknesses in, or threats to, systems or services. Reports should be made to the Head of Department, the owner of the information, or, where the IT infrastructure is involved, IT Services Desk or the Director of IT Services.

Those responsible for information or information systems, for example database and IT systems administrators, must ensure that appropriate security arrangements are established and maintained.

7. Policy Awareness and Disciplinary Procedures

The Information Security Policy will be made available to all staff and students and maintained by the Information Security Officer. Staff, students, authorised third parties and contractors given access to the University information systems will be advised of the existence of the relevant policies, codes of conduct and guidelines. Users will be asked to confirm that they understand the policy before being given access to some systems.

Failure to comply with the Information Security Policy may lead to suspension or withdrawal of an individual's access to information systems and the possibility of further action by the University in line with the current College Acceptable Use Policy (AUP).

The relevant section from the AUP is printed below:

> **AUP Section 9 - SANCTIONS**
>
> The main sanction taken against those who breach the computer regulations is withdrawal of the use of computer facilities. In serious cases the full range of disciplinary action will be taken and may include police action. Any complaint against a student will result in an instant response with immediate suspension of the account while the complaint is investigated. With many offences (including defamation, computer misuse and obscene publication) it is likely that a zero-tolerance approach will be pursued with a permanent withdrawal of computing facilities.
>
> If you have any queries regarding these regulations, please contact the Deputy Registrar and CIO, Laura Gibbs.

Failure of a contractor to comply could lead to the cancellation of a contract and, in certain circumstances, legal action may be taken.

8. Information Security Education and Training

The University recognises the need for all staff, students and other users of University systems to be aware of information security threats and concerns, and to be equipped to support University security policy in the course of their normal work. Appropriate training or information on security matters will be provided for users and departments will supplement this to meet their particular requirements. The Information Security Office will undertake a proactive campaign of awareness and monitor/report upon the type and frequency of incidents.

9. Maintenance

The Information Security Policy will be monitored by ISAG (Information Services Advisory Group) and reviewed as necessary. Revisions will be subject to appropriate consultation.

The Information Security Officer will report on a summary and exception basis and will notify stakeholders of issues and bring forward recommendations.

Departments may be required to carry out periodic risk assessments and establish and maintain effective contingency plans. They are also required to carry out regular assessment of the security arrangements for their information systems.

Those responsible for information or information systems must carry out periodic risk assessments of their information and the security controls in place. They must take into account changes in business requirements, changes in technology and any changes in the relevant legislation and revise their security arrangements accordingly.

10. Related Policies

Use of University computing facilities is covered by the University Regulations.

Aspects of Information Security are also addressed by the Financial Regulations (for example asset management and inventory records, which form one aspect of BS 7799), and by the University Security Policy which deal with physical security of assets including Computers.

Appendix B is an outline of the 20 critical controls for cyber security at Royal Holloway.

Acknowledgments

This policy includes material adapted from policies developed by Imperial College and Oxford Brookes University and Warwick University.

The policy is structured on the recommendations of the KPMG Information Security Policy Review (January 2002) based on the principles of BS7799.

Appendix A - Information Security Policies

The following documents are currently published or planned. A full summary of these and other polices can be found in the ITUAG policy schedule.

Regulations and Policies

1. University Regulations - Regulations governing the use of University computing facilities – In place:

http://www.rhul.ac.uk/it/tos/regulations.aspx

2. Information Security Policy – Draft – This document.

3. Regulation of Investigatory Powers Act/Freedom of Information Statement and Procedures – Planned

4. Anti-Virus Policy – Draft – will be tabled at 03/11 ITUAG.

5. Rules for Connection to the Campus Data Network – Draft

6. Policy on connection of web and electronic mail servers to the campus data network – Planned

7. Internet usage policy – In place

8. Third party access policy – Planned

9. Data Backup Policy – Approved

10. Firewall Security Policy – Planned

11. IP Allocation and Management Policy – In Place – not yet published on the web.

12. Data Protection - In place – http://www.rhul.ac.uk/foi/dataprotectionpolicy.html

13. Computer Account Password Policy

Additional sections to complete - develop guidelines and codes of practice.

Appendix B – 20 Critical Controls

This paper is not published along with this policy as it contains a summary of our position against a number of critical security principles. The critical controls document is confidential.