UNIVERSITY OF WOLVERHAMPTON INFORMATION SECURITY FRAMEWORK

1. INTRODUCTION

1.1. University of Wolverhampton's computer and information systems underpin all University of Wolverhampton's activities, and are essential to ensure the university provides a high quality student experience, pursues academic excellence, scholarship and enhances the employability of our students through supporting collaborative, innovative and enterprising delivery of all programmes.

1.2. The University of Wolverhampton seeks to be internationally orientated, strengthening links with the global community and strengthening partnerships, both within the UK and externally, in order to provide a process for an effective two-way knowledge, opportunity and innovation exchange between partners.

1.3. The University of Wolverhampton recognises the need for its members, employees and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this requirement.

1.4. Security of information must therefore be an integral part of the University of Wolverhampton's management structure in order to maintain continuity of its business, legal compliance and adhere to the University's own regulations and policies.

1.5. The University will operate in a manner where security of information is balanced with appropriate information accessibility; providing the optimum level of risk management to support the University's strategic goal of being a University of Opportunity which maintains strong global and international partnership links.

2. PURPOSE

2.1. This information security policy defines the framework within which information security will be managed across the University of Wolverhampton and demonstrates management commitment to meeting the strategic direction and support requirements for information security throughout the University of Wolverhampton. This policy is the primary policy under which all other technical and security related polices reside. (Appendix 1).

3. SCOPE

3.1. This policy is applicable to and will be communicated to all staff, students and other relevant parties including governors, employees, visitors and contractors.

3.2. It covers, but is not limited to, any systems or data attached to the University of Wolverhampton's computer or telephone networks, any systems supplied by the University of Wolverhampton, any communications sent to or from the University of Wolverhampton and any data which is owned either by the University or held on systems external to the University of Wolverhampton's network.

4. ORGANISATION OF INFORMATION SECURITY

4.1. The university will appoint an InfoSec lead officer for the organisation who is ultimately responsible for the maintenance of this policy and for compliance within the University of Wolverhampton. This policy has been approved by University of Wolverhampton Corporate Management Team and forms part of its policies and procedures.

4.2. The Corporate Management Team are responsible for reviewing this policy on an annual basis. They will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing to achieve the objectives of this policy.

4.3. The Information Security Manager is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy.

4.4. The Information Systems Committee comprising representatives from all relevant sections of the University is responsible for identifying and assessing security requirements and risks.

4.5. It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are:

1. Made fully aware of the policy
2. Given appropriate support and resources to comply.
3. Receive adequate training to ensure regulatory and legislative compliance is achieved.

4.6. Each Faculty and business department will appoint a responsible named individual known as the Information Risk Owner for their business area. This role will be responsible for selling information security to devolved departments, ensuring compliance with information security policy and be the initial data manager responsible for data breach containment and breach reporting to the Data Protection Officer for assessment.

4.7. The Information Risk Officer will be responsible for assisting with information risk assessments as required by the ISMS Forum and for compiling an Information Asset Register for their area of responsibility.

4.8. It is the responsibility of each member of staff to adhere to this policy.

5. POLICY STATEMENT

5.1. The University of Wolverhampton is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the University of Wolverhampton. It is the University of Wolverhampton's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

5.2. To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

5.3. Specialist advice on information security shall be made available throughout the University of Wolverhampton and advice can be sought via the University's Information Security Coordinator and/or the Data Protection Officer.

5.4. It is the University of Wolverhampton's policy to report all information or IT security incidents, or other suspected breaches of this policy. The Faculty or business unit will follow the University's advice for the escalation and reporting of security incidents and data breaches that involve personal data which will subsequently be reported to the University's Data Protection Officer for assessment and reporting, where applicable. Records of the number of security breaches and their type should be kept and reported on a regular basis to the Information Systems Committee and Information Security Coordinator.

5.5. Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour, may result in disciplinary action.

Version	v.2.0	Author	Stephen Hill
Approved Date	19/05/15	Approved by	Information Security Project Board (CMT)
Review Date	September 2017		

APPENDIX 1 – SUPPORTING POLICIES

1.1.	Information Governance Policy	Published
1.2.	Data Classification Guidance	Published
1.3.	T&Cs IT Account	Published
1.4.	Encryption Policy	Published
1.5.	Information Security Staff Training	Awaiting Launch (June 2016)
1.6.	Working Practices for Protecting Electronic Information	Requires Development
1.7.	Information Security Workbook for procurement of Software or Services involving UoW information	Requires Development
1.8.	Guidance on Use and Selection of Cloud Service Providers	Requires Development
1.9.	Regulation of Investigatory Powers Act Statement	Requires Development
1.10.	FOI Publication Scheme	Requires Development
1.11.	Guidance on Email Management	Requires Development
1.12.	Research Data Policy	Requires Development
1.13.	Risk Management Policy	Requires Development
1.14.	Open Access Policy	Requires Development
1.15.	Data Protection Policy	Published
1.16.	Policy for Taking Images and Recording	Published
1.17.	ICT Acceptable Use Policy	Published
1.18.	Policy on Safeguarding Children, VP and Vulnerable Adults	Published
1.19.	Data Retention Policy	Published
1.20.	Intellectual Property Policy	Published
1.21.	Cookies Policy	Published
1.22.	Electronic Information Security Policy	Published
1.23.	WEE Collection Procedure	Published
1.24.	FOI Guidance	Published
1.25.	Statement on Copyright	Published
1.26.	CCTV Manual	Published
1.27.	Codes of practice for post-graduate research	Published
1.28.	ITS Technical Procedures	Published