University of Ulster Policy Cover Sheet

Document Title	Electronic Information Assurance and Information Security Management System Policy 2.1
Custodian	Chief Finance and Information Officer
Approving Committee	ISD Committee, Library, Information and Student Administrative Services Committee (LISASC), then Senior Executive Team (SET)
Policy approved date	ISD Committee – 2014 – 11 – 17 LISASC – 2015 – 02 – 17 SET – 2015 – 03 – 16
Policy effective from date	2015 – 03 – 16
Policy review date	2017 – 03 – 16

Changes to previous version
Reference UK Government's National Cyber Security Strategy (HM Government 2011) in Introduction and Background

FOREWORD

Information Assurance is a key component within our governance of information and serves to provide the confidence that information systems of the University will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. There is little information that exists that will not at one time or another be stored or transmitted electronically. Information on paper as soon as it is fixed or input into a computer enters the electronic world. From here the information can be changed, deleted or broadcast to the world. Electronic information must be readily available when needed and trusted to be accurate. Sometimes there are confidentiality concerns and these need to be addressed if we are to protect our professional reputation. Ensuring the confidentiality, availability and integrity of all electronically held information is the goal. "Information Assurance" is the term we use to describe this goal.

This policy document defines the operation and scope of the Information Security Management System (ISMS) employed in the governance and management of its information. The ISMS exists to assure availability, integrity and security of information assets, and in so doing, provides assurance to continuity of University business during challenging events. Whilst clearly, there is a technical element to this activity, fundamentally our success in achieving information assurance will come from individual and collective approaches to our stewardship responsibilities and through the careful management of our information risks.

INTRODUCTION AND BACKGROUND

Information is essential to the governance, management, administration and operation of the University, and the security and effective control of information is fundamental to its success.

The UK Government’s National Cyber Security Strategy (HM Government 2011) identifies Universities as a strategic and valuable asset, reflecting their contributions to many aspects of economic and personal life. The strategy highlights the need for Universities to maintain confidence in the security of their information assets.

Information Security, which is more generally referred to as Information Assurance, is founded on three major concepts - those of Confidentiality, Integrity and Availability. The goal of this policy, and the standards and procedures that support it, is to remove or reduce the risk of threats and vulnerabilities which may compromise the use of the University’s information assets.

An ISMS exists which is comprised of processes and structures necessary for managing information security.

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

AIMS, PURPOSE AND SCOPE OF THE POLICY

This policy aims to establish the University's commitment to, and responsibilities for Information Assurance;

The purpose of the policy is to assure the University's overriding business objectives through a strong and proportionate framework of measures which are designed to:

- Ensure Confidentiality, by protecting assets against unauthorised disclosure
- Preserve Integrity, by protecting assets from unauthorised or accidental modification
- Maintain Availability, by ensuring that assets are accessible as and when required by those authorised to do so

This policy, supported by the operational and technical standards, procedures, guidelines and codes of practice defined within the IT Policy Implementation Framework, is applicable to all of the University's electronic information assets, and those employees, students, associates, or third parties who create, process, manage, or use them.

This policy will be reviewed every 2 years and updated as necessary to ensure that it remains appropriate in the light of relevant changes to the law, other University policies, or contractual obligations.

DEFINITIONS AND CLARIFICATION

Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information Assurance will ensure that the University of Ulster's information assets will be available when needed, will be accessed only by authorised users, and will contain complete and accurate information. Information systems will be able to withstand, or recover quickly from, threats to their confidentiality, integrity and availability. The University will implement robust assurance measures, commensurate with the sensitivity, criticality and value of the University's information assets, in order to protect and defend its business operations, service quality, legal position, and reputation.

The University **Information Security Management System** (ISMS) is a system that manages Information Technology (IT) related risks to achieve an acceptable level of risk. The ISMS includes policies, standards, codes of practice and guidelines along with systems and procedures for implementation, operation, monitoring, review, maintenance and improvement of the ISMS. Other important documents within the ISMS which shall be regularly maintained and reviewed include the Information Security Risk Register, Information Inventory and Statement of Applicability.

Data needed to conduct business and the technical equipment to manage (input, store, display and print) the data are called **Information Assets**. They can represent a large portion of intangible and tangible assets within an organisation. Within the University, they are usually one of three types:

- Pure information or data objects, such as files, documents, etc.
- Software systems that may be used to process, display, or manage information, such as databases, web-sites, collaboration tools, records management systems, etc.
- Physical assets and facilities such as servers, PCs/laptops/phones, storage, networks, or data centres.

An **Information System** is any combination of IT and people's activities that support operations, management, and decision making.

An **Information Inventory** is a listing of an organisation's Information Assets along with classification and other pertinent attributes.

An **Information Security Risk Register** is a list of potential IT-related risks to information, along with the likelihood, severity and ranking (priority) indicating the attention and resources the potential risk should attract, along with controls for reducing or eliminating the risk.

A **Statement of Applicability** documents information security control objectives and controls for a given domain and scope.

PROCEDURE

Ultimate responsibility for the execution of this policy rests with the Vice-Chancellor of the University. An IT Policy Implementation Framework of documents exists for the oversight of this policy's implementation and performance.

The responsibility and accountability for Information Assurance of specific information assets shall lie with the relevant senior officer of the department which is identified as the information asset owner.

This policy is implemented and supported by operational and technical standards, procedures, guidelines and codes of practice defined within the IT Policy Implementation Framework.

IMPLEMENTATION

The University ISMS is designed to be implemented in line with the provisions of the following International Standards:

- ISO/IEC 27001:2005 - Information Security Management – Requirements
- ISO/IEC 27002:2005 - Code of Practice for Information Security Management
- ISO/IEC 27005:2011 - Information Security Risk Management.

An institutional information inventory is maintained in order to:

- Determine the existence, ownership, and accountability of information assets;
- Support the management and resourcing of information assurance activities;

The institutional information risk register is regularly reviewed and maintained for those risks identified as applicable across the entire University.

Information assets of the University will be classified according to the Protective Marking Standard. The classification of an information asset will be used to determine the necessary assurance activities, and the relevant risk ownership. This will be used as input to the University's Stewardship Statements.

The IT Policy Implementation Framework will comprise specific operational and technical standards, procedures, guidelines and codes of practice, which will determine how assurance of the information assets will be achieved. The IT Implementation Framework shall be considered as part of this policy and shall have equal standing. It will address, not exclusively:

- User accounts and access
- Wired and wireless networks
- Protective marking of classified documents
- Records retention and disposal
- Secure storage and archival

- Acceptable use of IT
- IT monitoring
- PC and portable device security
- Data centre access
- Systems administration
- Disaster recovery
- Disposal of IT devices

A Statement of Applicability (SoA) is maintained as a requirement of standard ISO/IEC 27001:2005. The SoA identifies standard risk categories, whether they are applicable to the scope and domain being considered along with the control that is being applied to the risk.

Specialist advice and where appropriate, training courses or materials relating to information security, shall be made available throughout the University.

The implementation of this policy shall be reviewed independently of those charged with its implementation.

COMPLIANCE

Compliance with this Policy and its relevant Standards and Procedures, will be supported by:

- Evidentiary reviews, including quality assurance and testing activities;
- Monitoring and reporting of network and system activity;
- Implementation of appropriate information security technologies;

Any breaches of policy, or deliberate non-compliance with standards and procedures, will be investigated, reported and could lead to disciplinary action. The appropriate disciplinary action will be determined according to circumstance, in conjunction with the HR Department in the case of staff, and in conjunction with the relevant Dean of Faculty in the case of students.

In the event that an employee or student is aware of a potential breach of this policy, they are encouraged to report their concerns to their manager or Dean.

Where external organisations or individuals are using, or providing services for, the University’s information assets, they are required to comply with this policy, and the security standards and procedures that underpin it.

OTHER RELEVANT POLICIES, PROCEDURES AND SCHEMES

Policy/procedure/scheme	Scope
Data Protection Policy	Entire University
University IT Strategy	Entire University
User Account and Access Policy	Entire University
Document Management Policy	Entire university
Acceptable Use Code of Practice	Entire University
User Account Management Code of Practice	Entire University
Authentication Standard	Entire University
Password Standard	Entire University
Personal Computer Security Standard	Entire University
Networks Standard	Entire University
Wireless Networks Standard	Entire University
Protective Marking Standard	Entire University
Records Retention and Disposal Schedule	Entire University
Secure Storage and Archival Code of Practice	Entire University
Disposal of IT Devices Standard	Entire University
IT Monitoring Policy	Entire University
IT Monitoring Code of Practice	Entire University
Desktop PC Physical Security Standard	Entire University
Portable Devices Security Standard	Entire University
Information Security Risk Register	Information Services
Information Inventory	Entire University
Statement of Applicability	Entire University
Data Centre Access Policy	Information Services
System Administrators Code of Practice	Entire University
ISD Disaster Recovery and Data Backup Policy	Information Services