Information Security Incident Management Policy

September 2013

Approving authority:	University Executive
Consultation via:	Secretary's Board REALISM Project Board
Approval date:	September 2013
Effective date:	September 2013
Review period:	Three years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Heritage and Information Governance

POLICY

HERIOT-WATT UNIVERSITY
INFORMATION SECURITY INCIDENT MANAGEMENT POLICY
CONTENTS

POLICY

1. INTRODUCTION

This policy is a constituent part of the Heriot-Watt University Information Security Policy Framework which sets out a framework of governance and accountability for information security management across the University.

Heriot-Watt University relies on the effective management and flow of information to enable staff and students to communicate and work effectively on its business worldwide.

Safe use of the University's information and IT systems is essential to keep it working effectively. All users of University information have a responsibility to

- Minimise the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it
- Protect the security and integrity of IT systems on which vital or confidential information is held and processed
- Report suspected information security incidents promptly so that appropriate action can be taken to minimise harm.

The University takes information security very seriously. It is necessary to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the organisation.

2. PURPOSE

This policy provides a framework for reporting and managing

- security incidents affecting the University's information and IT systems
- losses of information
- near misses and information security concerns

Everyone has an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

3. OBJECTIVES

This policy aims to support the prompt and consistent management of information security incidents in order to minimise any harm to individuals or the organisation.

To this end all users and managers of University information and IT systems need to

- understand their roles in reporting and managing suspected incidents
- report actual or suspected information security incidents promptly, following the procedures [URL link here]

POLICY

3.1 The policy and its supporting procedures provide clear and consistent methodology to help to ensure that actual and suspected incidents and near misses are

- reported promptly and escalated to the right people who can take timely and appropriate action
- recorded accurately and consistently to assist investigation and highlight any actions necessary to strengthen information security controls

4. SCOPE

4.1 What is an information security incident?

An *information security incident* is any event that has the potential to affect the confidentiality, integrity or availability of University information in any format. Examples of information security incidents can include but are not limited to:

- The disclosure of confidential information to unauthorised individuals
- Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- Inappropriate access controls allowing unauthorised use of information
- Suspected breach of the University IT and communications use policy
- Attempts to gain unauthorised access to computer systems, e, g hacking
- Records altered or deleted without authorisation by the data "owner"
- Virus or other security attack on IT equipment systems or networks
- "Blagging" offence where information is obtained by deception
- Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Covert or unauthorised recording of meetings and presentations

4.2 This policy applies to

- All information created or received by the University in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely
- All staff and students, affiliates or contractors working for or on behalf of the University and any other person permitted to have access to University information
- All University IT systems managed by IS, Schools and Institutes
- Any other IT systems on which University information is held or processed

POLICY

4.3 Who is affected by the Policy

The Policy applies to all users of University information. Users include all employees and students of the University, all contractors, suppliers, University partners and external researchers and visitors who may have access to University information.

4.4 Where the Policy Applies

The Policy applies to all locations from which University information is accessed including home use. As the University operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions the remit of the Policy shall include such overseas campuses and international activities and shall pay due regard to non UK legislation that might be applicable.

5. LINES OF RESPONSIBILITY

5.1 **All users** who are given access to University information, IT and communications facilities are responsible for reporting any actual or potential breach of information security promptly in line with the incident management procedures.

5.2 **University senior managers, the Heads of Schools, Institutes and Professional Services** and their designated managers and staff, are responsible for identifying specific categories in their areas of **HIGH RISK** and **MEDIUM RISK** confidential information, as defined in the University Policy for secure use of confidential information on portable media, authorising and monitoring access to this information and agreeing appropriate measures with the Information Security Officer to prevent unauthorised access. Heads of Schools, Institutes and Services are responsible for liaising with the relevant **lead officers** to investigate and manage suspected breaches of information security.

5.3 **The Secretary of the University** has senior management accountability for information security. In the event of an suspected incident involving IT facilities, the Secretary or her nominee is responsible for authorising the monitoring of a user's IT account, including use of computers, email and the internet in cases where this is necessary to investigate allegations of illegal activity or breaches of information security and for reporting such breaches, where relevant, to the relevant legal authorities.

5.4 **The Director of Governance and Legal Services** has senior management responsibility for the information security management and for providing proactive leadership to instil a culture of information security within the University through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

5.4 **The Director of Information Services** (or equivalent officer in Schools/ Institutes) is the lead officer responsible for reporting, investigating and taking appropriate action to address breaches of IT systems and network security, and for escalating incidents to the Information Security Officer and Head of

POLICY

Risk and Audit Management.

5.5 **The Security and Operations Manager** is the lead officer responsible for reporting, investigating and taking appropriate action to address breaches of physical security and suspected attempts to gain unauthorised access to secure areas, and for escalating incidents to the Information Security Officer and Head of Risk and Audit Management.

5.6 **The Head of Heritage and Information Governance**, as **Information Security Officer** is the lead officer responsible for investigating and taking appropriate action in all cases involving loss, theft or unauthorised disclosure of University information and for liaising with the other lead officers and Heads of Schools, Institutes or Services in the management of other information security incidents. The Information Security Officer will record and review all information security incidents and make a quarterly report to the Information Security Group, recommending further action and any issues and risks to be escalated to the Secretary of the University and the Risk Management Strategy Group.

6. MONITORING AND EVALUATION

6.1 **The University Information Security Group** is responsible for reviewing the information security related policies and procedures that comprise the ISMS, monitoring compliance with the ISMS, reviewing incidents and recommending actions where necessary to strengthen information security controls. The Director of Governance and Legal Services chairs the group and it is clerked by the Head of Heritage and Information Governance. Its membership will include representatives of all of the senior stakeholders with responsibilities for information security as set out in the Terms of Reference for the Group. Where appropriate, the group will arrange training for lead officers responsible for investigating information security incidents.

The Chair and Clerk of the Information Security Group will make an annual report to the Risk Management Strategy Group on compliance with the ISMS, recommending any actions needed to address risks and issues, for inclusion in the Audit and Risk Committee's annual report on risk management control to Court. The Chair is responsible for escalating major risks arising from a breach of information security, or other major issues that affect strategic and operational risks, promptly to the Risk Management Strategy Group and the Secretary of the University. The Chair will report as necessary to the Secretary's Board and the Information Strategy Group as part of a wider communications strategy to promote a culture of responsible information security management across the University.

The Director of Governance and Legal Services is also responsible for meeting any reporting requirements of external regulatory bodies.

6.2 **The University's Internal Auditors** will provide additional monitoring with both routine and ad hoc audits, as instructed by the University Audit and Risk Committee.

POLICY

7. IMPLEMENTATION

This policy is implemented through the development, implementation, monitoring and review of the component parts of the information security management systems as set out in the Information Security Policy Framework.

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1. University Policies and procedures

This policy forms part of the University Information Security Policy Framework and its underpinning policies, procedures and guidance which are published on the University website at: http://www.hw.ac.uk/archive/ism-policies.htm

This policy should also be read in conjunction with the Information Security Incident Management Procedures [url] which set out how to report and manage an actual or suspected breach of information or IT security.

8.2 Legal Requirements and external standards

Use of information, IT and communications is subject to U.K. and Scottish law and other relevant law in all jurisdictions in which the University operates.

All current UK Legislation is published at http://www.legislation.gov.uk/

This policy and procedure are based on good practice guidance including:

- BS ISO 27001 Information Security Management
- The Information Commissioner's Office: Guidance on data security breach management V2 0 12/12/2012

9. DEFINITIONS

Information

The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

Confidential information

The definition of confidential information can be summarised as:

- Any personal information that would cause damage or distress to individuals if disclosed without their consent.
- Any other Information that would prejudice

the University's or another party's interests if it were disclosed without authorisation.

A more detailed definition can be found in the Policy for secure use of confidential information on portable media

Information Security Management System

"That part of the overall management system based on a business risk approach to establish, implement operate, monitor review maintain and improve information security. The management system includes organisational structure, polices, planning activities, responsibilities, practices, procedures, processes and resources."
BS ISO/IEC 27001: 2005: Information Security

10. FURTHER HELP AND ADVICE

For further information and advice about this policy and any aspect of information security contact:
Heritage and Information Governance
Telephone: 0131 451 3274/3219
Email: foi@hw.ac.uk

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V12.1 22/08/2013	Provisionally approved September 2012	Secretary's Board	Minor revisions for clarity and to update links to relevant guidance

POLICY