HERIOT WATT UNIVERSITY

Information Security Incident Management Policy

November 2017

POLICY

Approving authority:	University Executive
Consultation via:	Professional Services Leadership Board, Information Governance and Security Group
Approval date:	7 November 2017
Effective date:	7 November 2017
Review period:	Three years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Heritage and Information Governance

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.

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
- loss, disclosure, or corruption of information or devices
- near misses and information security concerns

3. OBJECTIVES

3.1 This policy aims to support the prompt and consistent management of information security incidents in order to minimise any harm to individuals or the University and reduce the risk of future breaches of security.

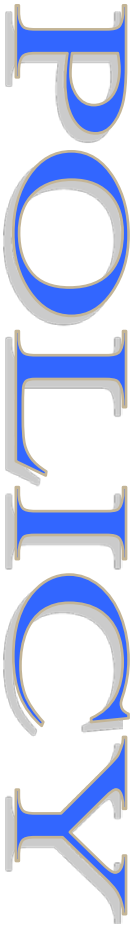
To this end all users and managers of University information and IT systems need to

- understand their roles in reporting and managing suspected incidents
- report all actual or suspected information security incidents immediately on discovery to their manager and **ITHelp@hw.ac.uk** **+44 (0) 131 451 4045**

3.2 The policy and its supporting procedures provide a 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

3.3 The University will deploy lawful and proportionate measures to protect information systems by



- monitoring traffic on its IT networks and systems to detect and alert staff to cyber security attacks and system outages

- maintaining adequate logs and evidence to enable investigation of incidents and preserve the chain of custody where this information is required for legal or evidential purposes

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, or IT systems in which this information is held. What may appear to be a physical security or IT issue may also be an information security incident and vice-versa.

Examples of information security incidents can include but are not limited to:

- Accidental or deliberate disclosure of HIGH or MEDIUM RISK information to unauthorised individuals e.g. an email containing unencrypted high risk personal information sent to unintended recipients
- Unauthorised sharing of HIGH or MEDIUM RISK information with an external cloud storage service or contractor
- Loss or theft of paper or electronic records, or equipment such as tablets, laptops and smartphones or other devices on which data is stored
- Inappropriate access controls allowing unauthorised use of information
- Suspected breach of the University IT and Communications Facilities Acceptable Use Policy
- Attempts to gain unauthorised access to computer systems, e.g. hacking
- Records altered or deleted without authorisation by the data “owner”
- Introduction of malware into a computer or network, e.g. a phishing or ransomware attack
- Denial-of-service or other cyber-attack on IT systems or networks
- A power outage that affects access to IT systems and information services
- “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
- Audible discussion of confidential topics in public
- 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 IT systems managed by, or on behalf of, the University Group
- Any other IT systems on which University information is held or processed

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 affiliates, 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 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 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.

5.2 **University senior managers, Heads of Schools and Professional Services** are responsible for liaising with the relevant colleagues listed below within Information Services, Heritage and Information Governance and Safety and Security Services to investigate and manage suspected breaches of information security relating to their areas of accountability.

5.3 **The Secretary of the University** has senior management accountability for information security. In the event of any suspected incident involving breaches of University IT and Communications Facilities Acceptable Use Policy, or allegations of illegal activity, the Secretary or her nominee, as set out in the Procedures, is responsible for authorising the monitoring of a user's IT account. This may include use of computers, email and the internet, where

POLICY

this is necessary to investigate such incidents. The Secretary or her nominee is also responsible for reporting such incidents, where necessary, to the relevant legal authorities.

5.4 **The Director of Information Services i**s responsible for reporting, investigating and taking appropriate action in response to IT systems and network security incidents and suspected breaches of the University IT and Communications Facilities Acceptable Use Policy, for escalating major incidents to the Security and Resilience Manager, maintaining procedures for responding to IT security breach scenarios and records of all incidents for evidential, audit, analysis and reporting purposes.

In all cases where a suspected incident or breach involves personal data or other HIGH RISK or MEDIUM RISK confidential information, the Director will or his nominee will inform the Head of Heritage and Information Governance immediately and liaise with the relevant members of the HIG team to investigate and resolve the issue.

5.5 **The Head of Heritage and Information Governance**, who is also the Data Protection Officer, is responsible for investigating and recommending appropriate action in response to any suspected breaches of personal data security, and will have oversight of action to be taken in response to loss or compromise of HIGH RISK or MEDIUM RISK confidential information, or systems and devices containing such information.

The Head of HIG is responsible for liaising with the Information Commissioner's Office and reporting breaches in line with regulatory requirements to report any data breach that is likely to result in a risk to the rights and freedoms of data subjects within 72 hours of discovery.

5.6 **The Director of Marketing and Communications** is responsible for coordinating internal communications and public relations and media communications in response to an incident, for maintaining pre-approved communication templates and for obtaining authorisation for the content of media communications.

5.7 **The Director of Governance and Legal Services** 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.

5.8 **The Security and Resilience Manager** is 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 that need to be managed in accordance with the University's major incident management procedures.

6. MONITORING AND EVALUATION

The University Information Governance and Security Group is responsible for reviewing reports of incidents and recommending actions where necessary to strengthen information security controls.

POLICY

The Head of HIG will monitor and review all information security incidents and make a regular report to the Information Governance and Security Group, recommending further action and any issues and risks to be escalated by the Director of Governance and Legal Services to the Secretary of the University and the Risk and Project Management Strategy Group.

7. IMPLEMENTATION

This policy will be implemented through the consistent use of

- The University Information Security Incident Management Procedures
- Information Services procedures for managing IT incident scenarios
- IT Help Desk incident triaging, management and recording system

HIG and IS will together regularly monitor and review the effectiveness of these procedures and tools and update them as needed taking account of the continually evolving threat landscape.

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.
This policy should also be read in conjunction with the Information Security Incident Management Procedures which set out how to report and manage an actual or suspected breach of information 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 its supporting procedures are based on relevant standards and guidance including:

- European Union General Data Protection Regulation
- BS ISO 27001 Information Security Management
- The Information Commissioner's Office:
  Guidance on data security breach management V2.2012121

POLICY

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.

Encryption

The process of using a cipher, algorithm or other key to convert plain text into cypher text so that it cannot be read without using another key to convert it back into plain text

HIGH RISK Confidential information

This 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 https://www.hw.ac.uk/services/docs/Infosecbasics_201605.pdf

MEDIUM RISK Confidential information

This can be summarised as:

- Any personal information that the individuals have not agreed to share e.g. lists of staff who have not completed training
- Any other information to which access must be limited on a business need to see basis e.g. a draft report

A more detailed definition can be found in https://www.hw.ac.uk/services/docs/Infosecbasics_201605.pdf

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.

POLICY

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 3274/3218/4140/3219
Email: hig@hw.ac.uk

Information Services
IT Helpdesk
Telephone: +44 (0)131 451 4045
Email: ithelp@hw.ac.uk

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V14.1 21/06/2017	7 November 2017	University Executive	Update of previous policy, approved by UE in September 2013. Minor revisions to reflect organisational developments, update links to relevant guidance and reflect feedback from the Information Governance and Security Group

POLICY