Heriot-Watt University
Information security framework

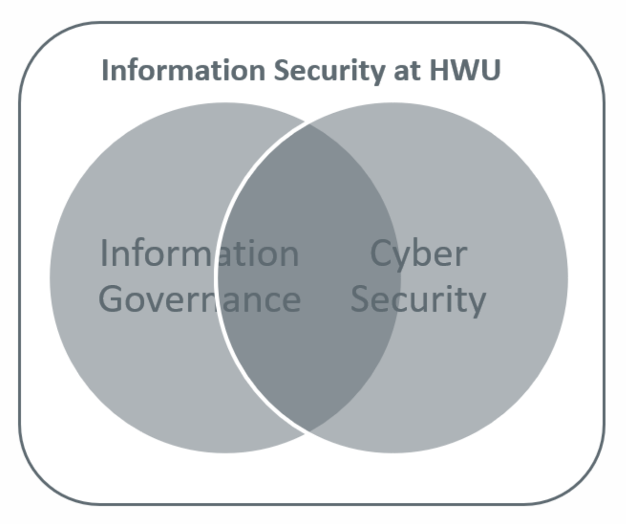
Introduction

This document sets out the framework of documents that govern information security within the University. The framework contains:

- This document
- Information security policy
- Standards and controls
- Standard operating procedures
- Additional supporting policies that require to be separate to the information security policy for specific reasons, such as the data protection policy

Information security overview

The University defines information security as covering both cyber security and information governance and as you would expect there is a large overlap between these two areas.

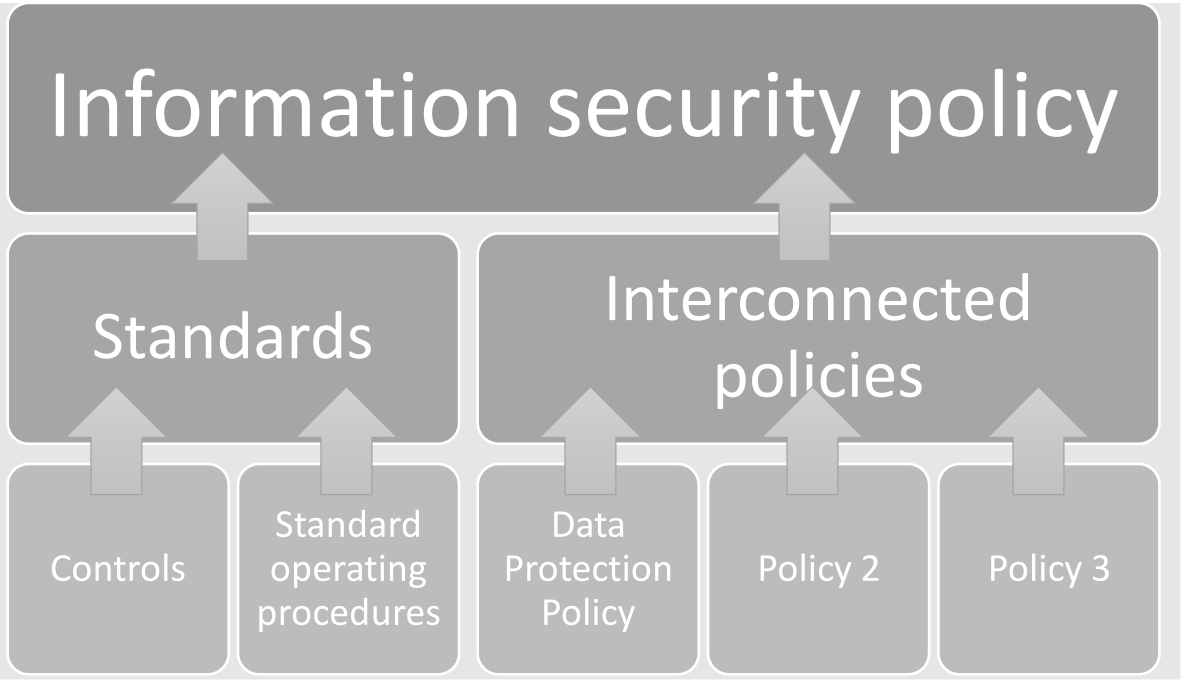


The University operates 4 joint committees or working groups covering this remit:

- Global Information Governance and Data Protection Committee
- Cybersecurity Risk Management group
- Cybersecurity working group
- Joint information Security Working Group

It is fundamental that we understand that information security is not just information technology, systems or firewalls. Information security is considered in our framework through three lenses; people, process and technology.

The framework
The policy framework of related and interconnected statements and documents can be visualised as below:



The University utilises the framework for the following purposes:

- Protect the University’s own information assets and technology services and assets being processed or held by the University on behalf of other parties by identifying, managing and mitigating information security threats and risks
- Define security requirements that are effective, sustainable and measurable and achieve the appropriate balance of usability and security
- Identify, contain, remediate and investigate information security incidents and apply lessons learned to maintain and assist in improving the University’s information security risk posture
- Develop an informed information security approach that takes account of the operational requirements for all areas of the University, including teaching, research, students and professional services
- Assist in the compliance of contractual, legal or regulatory obligations
- Provide assurance to the governing body and internal and external stakeholders that the University has a robust control environment in place to protect information assets through an effective information security management system.

The framework takes a holistic approach to information security risk management that we achieve by:

- Identifying and assessing information security threats
- Developing and implementing a combination of people, process and technology controls to mitigate these threats in line with the University’s defined level of acceptable risk and agreed objectives.

The information security policy framework assists with the following areas:

- Informing our business continuity planning and business impact assessments
- Protect our intellectual property rights, financial interests and completive edge

- Safeguard the interests and privacy of our students, staff and stakeholders and retain their trust
- Comply with the law and defend ourselves against legal action
- Maintain our reputation.

Framework components

The policy

The policy describes the high-level requirements for information security within the University. It also sets out the roles and responsibilities for everyone involved in ensuring good information security within the University.

Standards and controls

The Information Security standards are the minimum requirements needed to fulfil the information security policy. Each standard is comprised of a number of controls to check how well the standard is being met. The standards supplement the policy and provides detail om what is required within specific areas.

Standard operating procedures

The framework also includes the standard operating procedures designed to assist in the delivery of the standards and controls and ultimately to meet the requirements of the policy. These procedures are guidelines and provided to assist rather than being a set of rules. These can be either process or technical procedures.

The Standards and Procedures are the minimum requirements for information security (or the ‘baseline’). Where additional information security controls are required for research, legal, regulatory or governance purposes the Information Services and Information Governance teams will work with relevant stakeholders to enhance the controls accordingly.

Version	Date	Action/Changes
1.2	24/05/2023	Endorsed by University Executive.

Appendix 1 – Index of interconnected policies and supporting documents

			Areas of policy that are supported			
Document name	**Description**	**Associated Policies and Standards**	**1.1**	**1.2**	**1.3**	**2.1**
Data protection policy	The policy and its supporting procedures and guidance support University compliance with its obligations as a Data Controller and where applicable, a Data Processor under data protection law.					
Information Security Classification	Identify, classify and protect information assets in accordance with the associated documentation and Standards (listed below). Implement security controls that are proportionate to the defined classification. Senior Managers will appoint Information Asset Owners and Local Information Asset Managers to govern business critical information assets in accordance with the key responsibilities defined in the Information Governance and Records Management Policy.	• Information Classification Standard • Data Protection Policy • Information Governance and Records Management Policy				
Information Security Controls	Protect all processes, technology, Services and facilities through information security controls as detailed in the associated Standards.	• Access Management Standard • Operational Security Standard • Asset Management Standard • Secure Configuration Standard				

		• Security Testing Standard • Physical Security Standard • Human Resource Security Standard • IT and Communications Facilities Acceptable Use Policy
Information Security Incident Management	Identify report, contain, investigate and remediate Information security incidents are in accordance with the Incident Management Standard and reporting Procedure.	• Information Security Reporting Procedures • Information Security Incident Management Standard.
Contractor Risk Management	Before contracting with and using a third-party provider for any services which involves contact with University information, carry out an information governance and security risk assessment, including where necessary a data protection impact assessment (DPIA) is to ensure they comply with the University's Information Security Policy. Data Protection Policy and appropriate Standards.	• Data Protection Policy, • Information Governance and Data Protection Risk Assessment and DPIA Procedures • Third Party Standard • Cloud Security Standard.
Risk Assessment	Where appropriate, carry out a proportionate risk assessment on all processes, including data processing activities, technology, services and facilities in accordance with the associated Standard to manage risk within appetite.	• Risk Management Standard • Information Governance and Data Protection Risk Assessment and DPIA Procedures

Business continuity	Establish and maintain back-up and disaster recovery plans, processes and technology, in accordance with the Business Continuity Standard to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.	• Business Continuity Standard.
Remote working	Where off-site working takes place, including home working, implement appropriate security controls in accordance with the associated Standards.	• Mobile Device and Remote Working Standard • BYOD Standard • Travelling Overseas Standard.