Heriot-Watt University
Information Security Framework
Key roles and responsibilities

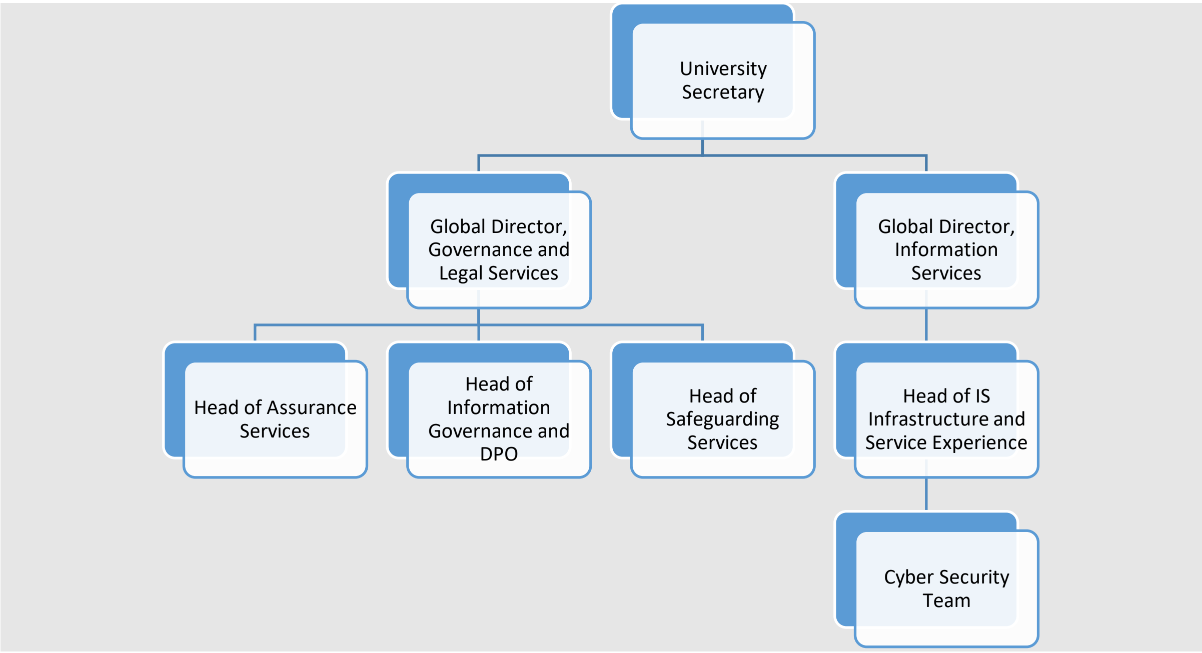
Introduction

This document should be read alongside the Information Security Policy and Framework. It sets out details of key roles, responsibilities, and accountabilities for Information Security management.

Organisational diagrams showing

1. **Key roles and reporting lines**
2. **Governance structure**

1. Key information security roles and reporting lines


University Secretary
Global Director, Governance and Legal Services
Global Director, Information Services
Head of Assurance Services
Head of Information Governance and DPO
Head of Safeguarding Services
Head of IS Infrastructure and Service Experience
Cyber Security Team

University Secretary	Has Senior Management accountability for Information security and information governance

Global Director, Information Services (IS)	Owner of strategic cyber security risks Has overarching responsibility for the Information Security Framework Escalates urgent cyber issues to University Executive

Head of IS Infrastructure and Service Experience	Responsible for monitoring and recommending actions to mitigate cyber security risks. Works collaboratively with Head of Information Governance on joint aspects of Information Security Framework, monitoring and reporting on information security risks and investigating information security incidents

Cyber Security and Compliance Manager, IS	Responsible for leading team to implement and monitor cyber security controls

Global Director, Governance and Legal Services (GaLS)	Owner of strategic information governance risks Has senior management responsibility for information governance management Escalates urgent information governance issues to University Executive Chairs Global Information Governance and Data Protection Committee

Head of Information Governance and Data Protection Officer Head of (IG&DPO), GaLS	Responsible for recommending organisational measures to comply with data protection laws and other information governance regulations Works collaboratively with Head of IS Infrastructure and Service Experience on joint aspects of Information Security Framework, monitoring and reporting on information security risks and investigating information security incidents, Escalates urgent data protection issues to the University Secretary

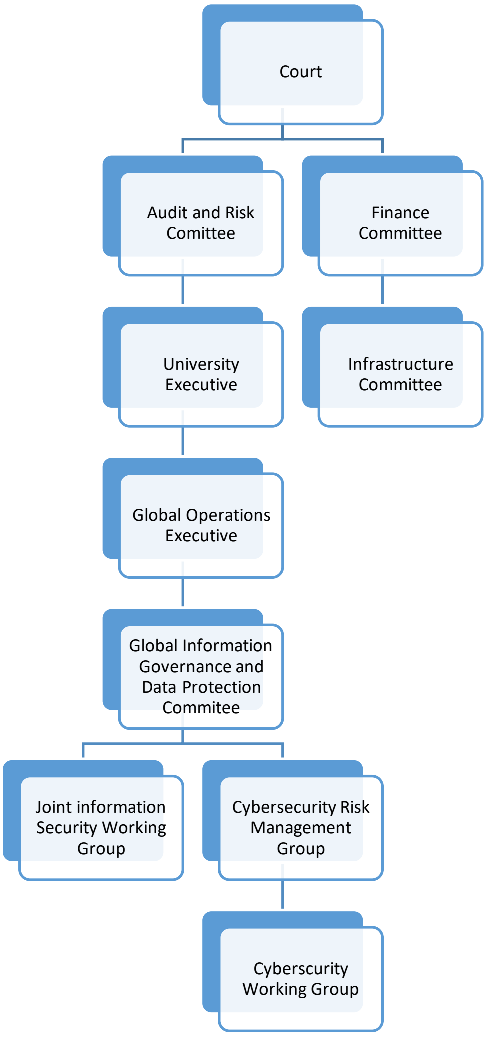
Head of Assurance Services, GaLS	Responsible for ensuring that Information Security controls are integrated within the risk, business continuity management and audit programmes and for liaising with insurers to ensure that the Framework meets insurance requirements.

Head of Safeguarding Services, GaLS	Responsible for ensuring that controls to manage the physical security of the University takes account of relevant information security risks and are integrated into the Information Security Framework

Executive Deans, Chief Operating Officers and Deputy Provosts, Heads of Global Research Institutes, Directors of Professional Services and Senior Executives from other Units**	Responsible for responsible for implementing relevant aspects of the Framework within their business areas, and for adherence by their managers and staff. This includes ▪ Assigning generic and specific responsibilities for information security management to Information Asset Owners and Local Information Asset Managers within their business areas ▪ Managing access rights for information assets and systems to ensure that employees, contractors, agents and other users have access only to such confidential information as is necessary for them to fulfil their duties. ▪ Ensuring that all colleagues in their business areas undertake relevant training provided by the University and are aware of their accountability for information security ** As set out in the Global Operations Executive Terms of Reference

Information Asset Owners and Local Information Asset Managers	Responsible for maintaining the security of the systems and information assets for which they have assigned duties of stewardship, in line with their roles and responsibilities under the Framework and the Information Governance and Records Management Policy.

2. Governance Structure


Court
Audit and Risk Comittee
Finance Committee
University Executive
Infrastructure Committee
Global Operations Executive
Global Information Governance and Data Protection Commitee
Joint information Security Working Group
Cybersecurity Risk Management Group
Cyberscurity Working Group

Court	The governing body of the University

Audit and Risk Committee	Has delegated authority from Court for oversight of cyber, information security and information governance risks, in the context of risk and compliance oversight. Recommends fundamental policies to Court. Receives annual and ad hoc reports from Global Director, IS on cyber security and from Global Director, GaLS and Head of IG and DPO on Information Governance and the work of the GIGDPC

Finance Committee	Has delegated authority from Court for oversight of the development and management of the infrastructure and IT assets of the University, delegating tasks to the Infrastructure Committee as appropriate.

Infrastructure Committee	Has delegated authority from the Finance Committee to receive and monitor global IT infrastructure strategy and a major programme of IT investments Advises the Finance Committee on matters pertaining to the global IT estate.

University Executive	Approves Information Security Policy and actions to mitigate major risks Has oversight of implementation of Framework components.

Global Operations Executive	Reviews and endorses policies that fall within the competency of the University Executive and Court, including the Information Security Policy.

Global Information Governance and Data Protection Committee (GIGDPC)	Has oversight of compliance with data protection and information governance laws and measures to mitigate information security risks. Recommends policies to the University Executive Reviews Annual Reports Monitors cyber security and information governance strategic risks and mitigations.

Cybersecurity Risk Management Group	Monitors the cyber security threat environment and recommends actions to strengthen controls in line with good practice

Cybersecurity Working Group	Develops and implements cyber security controls to support the mitigation of cyber security risks identified by the Steering Group

Joint information Security Working Group	Assists the GIGDPC in reviewing policies and procedures that comprise the Framework, recommending updates where appropriate to strengthen information security controls Monitors reports of University information security incidents and data breaches, recommending and prioritising actions to apply lessons learned to reduce risks of repetition Collaborates on user guidance, training, and awareness for the University community to raise awareness of information security risks and promote safe and secure use of information for work and study, taking account of sector good practice

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