Electronic Information Security Overarching Policy

Last Revised 7 December 2021

Document Control

Title	Electronic Information Security Overarching Policy
Abstract	The aim of this document is to outline all the Information Services policies that govern how the University of Stirling manages its information security.
Version	1.5
Date Issued	7 December 2021
Status	Issued
Document owner	Information Services
Creator name	Dr David Telford
Creator organisation name	The University of Stirling
Subject category	Information security
Access constraints	Public

Document Revision History

Version	Date	Author	Summary of changes
0.1	28 Aug 2019	David Telford	Initial draft
0.2	29 Aug 2019	James Blair	Review
0.3	29 Aug 2019	David Telford	Review and updates with acknowledgements added
0.4	3 Sep 2019	Steven McIntosh	Review with minor updates
0.5	4 Sep 2019	James Blair	Minor updates
0.6	12 Sep 2019	Gerry Mason	Minor updates
1.0	29 Oct 2019	David Telford	Governance team updates
1.2	6 Dec 2019	Sonia Wilson	Minor updates
1.3	6 Dec 2019	Gerry Mason	Minor updates
1.4	02 Sep 2020	Victoria Szymanska	Review and minor updates
1.5	7 Dec 2021	Victoria Szymanska	Review and minor updates

Document Dependencies

Title	Document Name
Incident management Policy	01 The University of Stirling Incident Management Policy
Network security Policy	02 The University of Stirling Network Security Policy
Access control Policy	03 The University of Stirling Access Control Policy
Data security Policy	04 The University of Stirling Data Security Policy
Systems management Policy	05 The University of Stirling System Management Policy
Software & DevOps Policy	06 The University of Stirling Software & DevOps Policy
Third Party Access Policy	07 The University of Stirling Third Party Access Policy
System usage Policy	08 The University of Stirling System Usage Policy
BCP/DR Policy	09 The University of Stirling Business Continuity and DR Policy
Compliance Policy	10 The University of Stirling Compliance Policy

Table of Contents

1 Introduction

The University of Stirling will protect its information from data breaches, the leaking of sensitive and confidential information, the willful or unintentional failure of information integrity and the disruption of the systems and services that allow authorised users access to its information. The University staff, students and authorised users will at all-times adhere to the University Information Security policy and its interdependent supporting policies detailed in this document. The policies are designed to support all activities involving information and require all staff, students and authorised users to work collectively to protect and secure the University of Stirling's information and the information it stores on behalf of others.

The Electronic Information Security Policy has been approved by the University Strategy & Policy Group (USPG) and the University Court and is part of the University's suite of policies and procedures. This policy has been developed and is reviewed annually on behalf of USPG by the Executive Director of Information Services and the University's Information Security Board working within Information Services. All changes to this policy will be communicated to staff, students and authorised information technology users. The policies will also be reviewed in light of changes to legislation, the evolving threat landscape and relevant organisational changes. Regular risk assessments will be carried out on all systems that are the primary sources of Information and those that receive, process or transmit this information. This will identify the likely impacts and possibility of security breaches.

The University of Stirling will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its Electronic Information Security Policy.

All staff, students and authorised users must comply with this Electronic Information Security Policy. Failure of a user to comply with this policy will lead to the relevant University disciplinary procedures being invoked and, should criminality be discovered, these may be reported to the police or legal action taken.

2 Scope

The Electronic Information Security Policy applies to all staff, students and authorized users who access the University's information technology resources.

This policy applies to all use of information and information technology on the University of Stirling's premises and includes any devices owned privately and used on or off campus, and to technology and devices provided by the University of Stirling wherever it is used, and to all external access to the University of Stirling's information technology from wherever this is initiated.

3 Roles and Responsibilities

The Executive Director of Information Services is responsible for recommending updates to the Electronic Information Security Policy which will be reviewed annually and in the event of legislative, organisational or threat landscape changes. Revisions to the Electronic Information Security Policy will be approved by the USPG and the University Court. Where necessary, recommendations will be submitted to the University identifying resources, systems and services necessary to improve security measures in support of the revised policies.

The University's senior responsible officer for information security, the Information Services Information Security Manager (ISM) will lead the communications, advise on training and compliance and necessary actions to ensure secure use of University's information and technology. Further, they shall share best practice and information on relevant codes of practice, cyber security certification and compliance and is responsible for advising appropriate persons on the compliance with this policy and its associated codes of practice.

The responsibility for safeguarding University primary information systems and ensuring that specific security processes are carried out lies with the System Sponsor and manager for that system. The System Sponsor is normally the Head of the Department managing that information system (See Appendix 1).

Any manager within Information Services acting as Duty Manager can approve emergency action to be taken when required to enforce this policy. Longer term action requires the written approval of The Executive Director of Information Services and the University Secretary or, in their absence, a member of USPG (see Appendix 2) within 2 working weekdays.

4 Business Continuity

All primary corporate and academic information systems are required to have documented Disaster Recovery (DR) and Business Continuity Plans (BCP). Recovery processes and annual formal risk assessments should be undertaken to determine the level of criticality to the organisation. These should specify what level of business continuity planning is needed as well as when and how these are tested.

It is a University of Stirling requirement that all BCP plans are tested regularly. Plans will be scrutinised by both internal and external auditors to verify the level of testing and whether the plans are appropriately developed to meet the needs of recovery from a realistic disaster or malicious attack scenarios.

The frequency of testing is defined at an appropriate level for each system and documented within the DR and BCP plan and will include tests to confirm relevant staff and teams are able to put the plan into operation.

All relevant staff will receive appropriate training to be able to carry out their role with respect to business continuity plans.

5 Security Breaches

All potential suspected or identified security breaches of this policy should be immediately reported to the Information Services 'Service desk' on extension 7250 or by emailing information.centre@stir.ac.uk. Confidentiality of the information supplied will be maintained and shared only with appropriate staff on a need to know basis, including the Information Services Duty Manager and the Information Security Manager. Following a report of a breach an investigation will be instigated to ascertain the level of security breach and necessary actions.

If a suspected or actual breach of security has occurred the Information Security Manager will lead the necessary actions to secure the breach and may temporarily suspend access to system(s), data, software or networks.

The Information Services Duty Managers have the authority to protect the University against breaches of security by whatever means is deemed necessary and reasonable. These actions, if continuing, will require the written authority of the Executive Director of Information Services, the University secretary or in their absence a USPG member within 2 working days.

6 Monitoring and Logging

The University will continually monitor network activity and data movements within the University and levels of data leaving the University systems and services.

Information Services will regularly review reports from JANET Computing Emergency Response Team (JANET CERT), HEFESTIS, the UK National Cyber Security Centre and other security sources and respond with actions to secure University digital, data and technological resources. The Monitoring and Logging Policy and all interdependent polices are linked within this document.

7 Supporting Policies

This overarching Electronic Information Security Policy's related and interdependent policy statements are designed to cover all key areas of Information Security based on the ISO 27000 series of information security standards and will reflect and respond to Cyber essentials Certification and future Scottish Government cyber security standards.

The overarching Policy and its interdependent policies are linked from this document and published on the University of Stirling's website. Staff, students and other persons authorised to use the information technology of University of Stirling are required to read these policies and adhere to them.

Assistance, advice or clarification can be sought from the Information Services Information Security Manager. Contact the Information Services 'Service desk' on extension 7250 or by emailing information.centre@stir.ac.uk for further information.

The interdependent policies are:

Title	Document Name
Incident Management Policy	01 The University of Stirling Incident Management Policy
Network Security Policy	02 The University of Stirling Network Security Policy
Access Control Policy	03 The University of Stirling Access Control Policy
Data security Policy	04 The University of Stirling Data Security Policy
Systems Management Policy	05 The University of Stirling System Management Policy
Software & DevOps Policy	06 The University of Stirling Software and DevOps Policy
Third Party Access Policy	07 The University of Stirling Third Party Access Policy
System Usage Policy	08 The University of Stirling Acceptable Use Policy
BCP/DR Policy	09 The University of Stirling Business Continuity and Disaster Recovery Policy
Compliance Policy	10 The University of Stirling Compliance Policy
Policy and Monitoring and Logging Policy	11 The University of Stirling Policy and Monitoring and Logging Policy

8 Legislation

Information security at the University of Stirling is subject to legislation including the following:

1. Computer Misuse Act (1990);
2. Freedom of Information (Scotland) Act (2002);
3. General data protection regulation;
4. Data Protection Act (2018);
5. Copyright, Designs and Patents Act (1988);
6. Criminal Justice and Public Order Act (1994) ;
7. Human Rights Act (1998);
8. Regulation of Investigatory Powers Act (2000);
9. Lawful Business Practice Regulations (2000);
10. Regulation of Investigatory Powers (Scotland) Act (2000);
11. Communications Act (2003);
12. Terrorism Act (2006);
13. Police And Justice Act (2006);
14. Acceptable Use Policy of the Joint Academic Network (JANET), a copy of which can be viewed at URL: http://www.ja.net/company/policies/aup.html.

Note: Users must also comply with any regulations and instructions displayed alongside Information Technology facilities.

9 User Compliance and Disciplinary Action

The staff terms and conditions of employment state that employees must follow the University regulations which include this policy.

Line Managers must provide specific guidance on legal compliance to any member of staff whose duties require it.

The Student Regulations state that students must follow University regulations which include this policy.

All third-party users who are given access to the University's information technology must agree to abide by the University's Electronic Information Security Policy.

This policy is available electronically in the Information Services section of the Intranet.

It is also available in hard copy from the IS Service Desk. Updates will be published in the same locations.

Failure of a user to comply with any part of the Electronic Information Security Policy will lead to the relevant disciplinary procedures being invoked and actions may be reported to the police or legal action may be taken.

10 Disclaimers

The University of Stirling accepts no responsibility for the malfunctioning of any equipment or software, failure in security or integrity of any stored program or data or for any loss alleged to have been caused whether by defect in the resources or by act or neglect of the University of Stirling, its employees or agents.

11 Responsibilities

Role	Responsibilities
USPG and the University Court	Authorise policy
Information Services Directorate	Define policy
Information Security Board	Create procedures, standards and controls
Information Security Manager	Has direct responsibility for maintaining this policy and providing advice on implementation.
Information Centre (Security Incident Response Team)	Handle incoming incidents
IS staff	Be familiar with and adhere to the policies at all times.

Appendix 1

Main University System Owners:

Role	Responsibilities
Head of Student Systems & Data	Tribal
Head of Systems & Treasury	Agresso
Estates Systems Manager	Archibus
Learning and Teaching Support Manager	Canvas
Head of HR services	SAP
Research Systems Manager	Worktribe, ethics?system
Head Digital & Content	University website
Head of Business Applications	Library System, Data warehouse
Head of Policy & Planning	Management Information systems

Appendix 2

University Strategy & Policy Group (USPG) Membership:

Principal & Vice-Chancellor

University Secretary & Chief Operating Officer

Senior Deputy Principal

Deputy Principal (Research)

Deputy Principal (Education and Students)

Deputy Principal (Internationalisation)

Deputy Secretary

Executive Director of Finance

Executive Director of Communications, Marketing and Recruitment

Executive Director of HR and Organisation Development

Appendix 3

Acknowledgements:

This policy suite has been developed with the assistance of ucisa's Information security management toolkit, HEFESTIS (HE/FE Shared Technology & Information Services), HEIDS (Higher Education Information Directors Scotland) and from colleagues from across the Higher Education & Further Education sector.