Policy title:	Information Security Policy
Policy owner:	Chief Information Officer
Department:	I&T Directorate
Date approved:	July 2021
Date of review:	July 2023
Approval route:	Executive Board
Circulation:	All staff and students
Publication:	External

Information Security Policy

1 Introduction

1.1 This policy underpins all SOAS relevant policies, procedures, standards and guidance for the security of electronically stored data. This policy is related to the School's policies on data protection and records management and is prepared and implemented in reference to the SOAS Data Governance Strategy.

1.2 SOAS recognises the need for its students, staff and visitors to have access to the data they require in order to carry out their work and study. Information security helps protect against breaches of confidentiality, failures of data integrity or interruptions to the availability of data and ensures appropriate legal, regulatory and contractual compliance.

2 Scope

2.1 This policy applies to:

- Any IT systems attached to SOAS networks;
- Any IT systems supplied by SOAS;
- Any communications sent to or from SOAS irrespective of platform;
- Any data which is owned, controlled or processed by SOAS, including data held on systems external to the university network;
- All approved users of SOAS's data including all staff and students,

contractors, suppliers, partners and external researchers who may be authorised access to SOAS data;
- All locations from which SOAS data is accessed including home and offsite use; and
- All equipment used to access SOAS data at any time.

3 Policy statements

SOAS Information Security Policy follows the principles, guidelines and responsibilities as set out in the industry standard Information Security Management System (ISMS) ISO 27001 ISO/IEC 27001:2013.

These include:

- Data will be protected in line with relevant legislation, notably those relating to Data Protection, Human Rights, Freedom of Information as well as relevant SOAS policies.
- Each information asset group will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Data will be made available solely to those who have a legitimate need for access.
- All data will be classified according to an appropriate level of security.
- The integrity of data will be maintained.
- It is the responsibility of all individuals who have been granted access to data to handle it appropriately in accordance with its classification.
- Data will be protected against unauthorised access.
- Compliance with the Information Security Policy will be enforced.

SOAS follows a risk-based approach to Information Security. To determine the appropriate level of security control applied to IT systems, a risk assessment will identify the likelihood and impact of security incident and define security requirements. The Information Security Architect and the Data Protection Officer can provide advice for an Information Security Risk Assessment.

This policy follows ISO 27001 Information Security Principles and the fourteen sections below address one of the defined control categories.

3.1 Information security policies

3.1.1 Further policies, procedures, standards and guidelines exist to support the Information Security Policy and have been referenced within the text. Further information is available for staff on the MySOAS IT Services pages.

3.1.2 The current I&T related SOAS' Policies are:

- Appropriate Use of IT Policy
- Email Policy
- IT Procurement Policy Desktop and Laptop Purchase, Deployment and Disposal Policy

3.1.3 SOAS's IT equipment connects to the internet via Jisc's JANET network and must comply with their security policies and legal requirements. SOAS's policies will be updated to reflect significant changes in JANET policies and all applicable law.

3.2 Organisation of information security

3.2.1 SOAS will define and implement roles for the management of information security. This includes identification and allocation of security responsibilities to initiate and control the implementation of information security across SOAS.

3.2.2 The hierarchy of responsibility is:

- Board of Trustees is accountable for the SOAS Risk Register;
- The Data Governance Steering Group (DGSG) has representatives from all relevant sections of SOAS and its purpose is to influence, oversee, promote and improve data standards and compliance with the Data Protection Laws (Data Protection Act 2018 and UK GDPR, as defined by section 3(10) of the DPA 2018);
- The Information Security Architect supported by the I&T senior management team, Governance and Legal Services and the Information Compliance Manager, manages information security, providing advice and guidance on the implementation of this policy;
- Data owners and stewards are responsible for compliance with this policy;
- IT system owners are responsible for ensuring that appropriate security arrangements are in place for IT administrative access and security controls on managed systems are compliant;
- Information users assume local accountability for data management and compliance with this policy. They are responsible for reporting any actual or suspected breach in information security or any working practice that increases the risk of a potential information security breach.

3.3 Human resources security

3.3.1 All approved users of SOAS IT services must demonstrate an understanding of the Data Protection Laws. Staff must successfully complete the mandatory "Information security awareness" and Data Protection training.

3.3.2 This policy and expectations for acceptable use should be communicated to all users of SOAS IT services. Breaches of policy are handled by staff line management with assistance from the Information Security Architect.

3.3.3 Security responsibilities should be included in job role descriptions, person specifications and personal development plans. Individuals accessing SOAS data must seek advice from I&T if in any doubt of responsibilities.

3.3.4 Employee signed contracts enforce compliance with SOAS' policies.

3.3.5 Upon termination of a staff appointment, People Services will revise the staff record system accordingly, triggering IT systems account termination processes in line with account access policies. Not all system access is automatically controlled, for example in local systems and records. Therefore, line managers must ensure that appropriate staff exit procedures are in place to remove access to all systems upon staff exit or change of role.

3.3.6 Academic staff who retire but continue their academic association with SOAS may retain their account on the network with approval from HOD and HR.

3.3.7 The Information Security Architect may authorise legally compliant monitoring of IT systems to investigate security incidents and compliance with SOAS' policies.

3.4 Asset management

3.4.1 All assets (data, software, processing equipment and IT services) will be identified and owners documented to be responsible for the maintenance and protection of those assets in accordance with SOAS's policies. All data created, received or retained must be protected in line with SOAS information classifications.

3.4.2 Line managers must ensure that all IT assets owned by SOAS must be returned to I&T Directorate by any party upon termination.

3.4.3 All SOAS information assets shall be retained in line with the SOAS Retention Schedule. Data must be stored on facilities provided by SOAS as advised. Protected and Restricted data must not be stored on any device without adequate protection.

3.4.4 Mass storage devices such as CDROM, DVD, memory cards or USB drives should be treated in the same way as Protected/Restricted data and must be locked away at the end of the working day. For further guidance for staff refer to the IT services page on file storage.

3.4.5 Physical records containing Protected/Restricted data shall be disposed of securely by using provided confidential waste shredding services or shredders.

3.4.6 Owners of research data should seek guidance on anonymization, initially

from the IT Service Desk.

3.5 Access control

3.5.1 A procedure for user account creation and deletion must be maintained for access to all IT systems. Access will be granted according to an individual's role and the relevant access policy.

3.5.2 Mandatory authentication must be used. Two factor authentication must be used for accessing Protected/Restricted data, where this service is provided by SOAS. Separation of duties must be maintained, where practical.

3.5.3 User with administrative rights must use their normal user accounts for standard IT system access and only use elevated privileges when required. Administrative account passwords must be set to a longer length and more frequent resets than a standard account to reduce risk.

3.5.4 Users must not share their login details to access IT services. Passwords must be in accordance with the Password Policy.

3.5.5 All IT equipment and systems connected to the SOAS network or connecting remotely must meet the minimum specification defined in the Patching Policy, utilising an operating system still receiving security updates with antivirus software installed.

3.6 Encryption

3.6.1 SOAS I&T will provide guidance and tools to ensure proper and effective use of encryption to protect the confidentiality and integrity of data and IT systems.

3.6.2 The individual or unit managing encryption must ensure that the encryption keys are safeguarded against accidental or unauthorised disclosure. It is also critical that encryption keys are securely backed up, as losing an encryption key will mean the encrypted data is lost forever.

3.6.3 Data encryption is required for Protected/Restricted data transmitted over data networks.

3.6.4 Mobile computing devices must be encrypted. If unsure take advice from the IT Service Desk before applying an encryption key.

3.7.0 Physical and environmental security

3.7.1 Data centres, computer rooms, and communications facilities used for hosting equipment for information processing, must be physically protected from unauthorised access to prevent theft or damage. Facilities must also be adequately protected against environmental damage such as by fire or flood.

3.7.2 Computer equipment must be password protected if left unattended. A screen lock must be activated when there is no activity for a short period of time. Passwords must not be written down anywhere near IT equipment.

3.7.3 Portable computing devices must be locked away at the end of the working day.

3.7.4 All SOAS owned equipment must be disposed of in a controlled manner. Any staff wishing to dispose of IT equipment must contact the IT Service Desk to arrange collection.

3.8 Operational security

3.8.1 Operational changes to equipment, infrastructure, or software affecting SOAS's production IT services and suppliers must follow IT&IS change management procedures.

3.8.2 I&T provide backup services for managed storage. Information owners must ensure that appropriate backup and system recovery measures are in place for locally managed and third-party services they use. Appropriate security measures must be taken to protect against damage or loss of backup media. Backup recovery procedures must be tested on a regular basis.

3.8.3 It is not permitted to connect personally owned equipment to any network socket; personally owned devices shall use the eduroam or guest wireless network.

3.8.4 Any device connected to the SOAS network (excluding eduraom and other guest wifi) must comply with the Patching Policy. Devices which are not compliant will be liable to physical or logical disconnection from the network without notice. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing.

3.8.5 Individuals installing software themselves are responsible for that installation. Those responsible for software must monitor relevant sources of information for security update alerts.

3.8.6 SOAS inspects systems connected to our network for vulnerabilities. If critical and high vulnerabilities are detected that cannot be mitigated, the system will be disconnected from the network.

3.8.7 SOAS shall maintain a policy covering logging and monitoring on the network.

3.9.0 Communications security

3.9.1 SOAS maintains network security controls to ensure the protection of data within its network and the internet.

3.9.2 Segregation shall exist between 'internal' and eduroam/guest network traffic. Appropriate controls will be enforced between security zones to reduce the risks of compromise, denial of service attacks, malware infection and unauthorised access to data.

3.9.3 Guidance should be sought from the IT Service Desk for information on secure data transfer.

3.10 System acquisition, development and maintenance

3.10.1 Information security requirements must be defined during the development of business requirements for new IT systems and reviewed following significant changes to existing IT systems. IT can provide advice on the security requirements for new IT services and significant changes to existing IT services.

3.10.2 Smaller pieces of work resulting in any change in the IT estate must follow the SOAS IT work request process where Information security is defined

3.10.3 If relevant, projects will be advised to complete a Data Protection Impact Assessment by the Information Compliance Manager.

3.11 Supplier relationships

3.11.1 Suppliers must follow SOAS security policies, change control process and support arrangements. Contact IT Service Desk for further guidance.

3.11.2 Supplier activity may be monitored according to the data classification, IT service and perceived risks to SOAS.

3.12 Information security incident management

3.12.1 All information security incidents or other suspected breaches of this policy must be reported immediately to the IT Service Desk. For the escalation and reporting of data breaches that involve personal data, follow the procedures in the IS Significant Incident Plan (CP-IN02).

3.12.2 Information Security incidents will be investigated in accordance with the IS Significant Incident Plan (CP-IN02) to determine whether any underlying security concern need to be recorded, corrected and built into future controls to ensure safeguarding of individuals rights and freedoms. If appropriate, concerns will be added to the IT risk register.

3.13 Information security aspects of business continuity management

3.13.1 SOAS will protect critical IT services from the impact of major incidents to ensure recovery in line with documented priorities. This includes appropriate backup and resilience. Business continuity plans must be maintained and tested. Business impact analysis should be undertaken of the consequences of major security incidents.

SOAS will follow the IS Significant Incident Plan (CP-IN02) in response to any major cyber security incidents.

3.14 Compliance

3.14.1 Compliance with the controls in this policy will be monitored by the Information Security Architect and reported to the Information Security Steering Group.

3.14.2 The design, operation and use of IT systems must comply with all contracts and regulations, relevant UK, EU and international law. Chiefly this includes the Data Protection Laws, the payment card industry standard (PCI-DSS), the Government's Prevent guidance, and SOAS research contractual commitments.

3.14.3 SOAS is subject to independent audit and aims to comply with the spirit of ISO 27001 and the UK Government's Cyber Essentials scheme. Business critical systems and other systems identified as high risk will be subject to regular penetration testing.

4 Sanctions

4.1 Failure to comply with this policy, or its subsidiary policies, procedures or regulations, may result in withdrawal of access to SOAS IT services and may result in disciplinary action or termination of contract.

5 Monitoring

5.1 This policy and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. SOAS will also undertake appropriate benchmarking and auditing exercises as may be applicable periodically.

6 Exceptions

6.1 If an individual or third party cannot comply with this policy, they must contact the IT Service Desk for advice on security controls to enable compliance otherwise they must cease using SOAS data and IT services.

7 Definitions

- DGSG: Data Governance Steering Group

- ISMS: Information Security Management System
- ISO: International Standards Organisation
- ISO 27001: Industry standard for an Information Security Management System
- UK GDPR: UK General Data Protection Regulation
- JANET: Is a high-speed network for the UK research and education community provided by Jisc
- Jisc: A UK not-for-profit company whose role is to support post-16 and higher education, and research.

8 Related documents

- Acceptable Use of IT Policy
- Email Policy
- Data Breach Reporting Procedure
- IS Significant Incident Plan
- IT Procurement Policy
- Data Protection Policy
- Records Management Policy
- Retention Schedule
- SOAS Template for Data Protection Impact Assessment (DPIA)

9 Related requirements

- Data Protection Act 2018 and UK GDPR
- JANET Policies
- PCI DSS
- ISO/IEC 27001:2013
- SOAS auditor reports
- Information Commissioner's Office – UK GDPR guidance
- National Cyber Security Centre - Cyber Essentials guidance
- International Standards Organisation - ISO27001 guidance
- University and Colleges Information Systems Association - Information Security Management Toolkit