Information Security Policy

Information Services (External version)

The following statement has been endorsed by both the Chief Executive and Vice Chancellor (Professor Sir Peter Gregson) and the Director of Information Services (Gio Lusignani) of Cranfield University: -

“The University recognises that information and information systems are valuable assets which must be protected. Sharing information is a key enabler in supporting the University’s strategic objective but it is imperative that this is undertaken securely and fully complies with all legal obligations. This Information Security Policy sets out the University’s approach to the secure management of Information and information systems.”

1. Purpose

The purpose of information security is to provide a clear guidance framework that safeguards the reputation of Cranfield University and protects information systems and their users. This will be achieved through the development and implementation of appropriate controls and supporting mechanisms that:

- identify good practices in information security management
- optimise the management of risks
- ensure compliance with legal and regulatory requirements
- minimise the impact of unexpected information security incidents
- provide suitable security education, training and awareness programmes
- give the necessary assurances that information is being handled properly.

2. Scope

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and legal compliance. All users have obligations to maintain appropriate levels of information security to meet the University’s legal and contractual obligations.

The policies and standards defined for Cranfield University by the Information Security Working Group (ISWG), and formally approved by the Information Assurance Committee (IAC), must be implemented by all Schools/Professional Service Units (PSU’s) and included in all service legal agreements and contracts with Group companies and other associated entities.

3. Accountabilities

The Information Assurance Committee (IAC) is responsible for establishing and maintaining effective lines of accountability, responsibility and authority for protecting information assets. It will ensure that the critical information asset register is maintained, and support the development and implementation of information security policies and standards. In addition, it will prioritise information assurance activities, define the information risk posture of the University and monitor these activities.

Director of Information Services (IS), in collaboration with the Information Security Team and the Information Security Working Group (ISWG) is responsible for developing appropriate information security policies and standards.

Members of the ISWG will assist the Information Security Team in ensuring the continuous development and review of appropriate information security practices for the University.

The Information Security Team is responsible for the day-to-day operational information security and assurance activities including appropriate protection of personal data.

Schools/PSU's and associated entities are responsible for embedding information security policies and standards, and providing appropriate representation on the ISWG.

Employees, students, contractors and other agents of Cranfield University and service providers (where applicable) are responsible for complying with the relevant requirements of the policies and standards.

All users have an obligation to use information and information systems responsibly. Rules are defined in the Regulations for the use of Computing Facilities and in Acceptable Use policies.

4. Definition of information security

The ISO/IEC 27000 Information Security Management Systems (ISMS) standards provide the following definitions of the three main aspects of information:

CONFIDENTIALITY	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
INTEGRITY	The property of accuracy and completeness
AVAILABILITY	The property of being accessible and usable upon demand by an authorized entity

5. Information Security Standards

The Information Security Standard (ISO/IEC 27001 series) is the primary reference for designing and implementing information security within Cranfield University.

Use of the standard enables Cranfield University to deploy security controls consistently across all Schools/PSU's and to define its requirements for security in all third party contracts and partnerships. The standard also provides a means of benchmarking against other organisations and a method of checking that security polices and standards are being implemented effectively.

A number of policies, standards and guidelines have been developed to complement and enhance the security management processes defined in the standard. These are described in the Policies and Standards sections of this policy.

6. Information Security Risk Management

The nominated representative(s) of each School/ PSU will follow an appropriate process to identify, assess, rank and feed risks into a pan-University major information security risk register.

The process should assess:

- the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;
- the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.
- whether risks can be mitigated to a level that should be accepted

The third bullet point would be subject to oversight by the IAC to ensure that any risks affecting the University as a whole, could be assessed and evaluated before any mitigating actions were accepted. The Information Security Team will provide general advice, guidance and support on all matters relating to information security, and may undertake periodic assessments of the general security risks to information and services to facilitate this process. The Information Security Team will utilise an 'in-house' risk assessment and management tool to formalise risk management across the University.

7. Compliance with Legal and Contractual Requirements

All Pro-Vice-Chancellors of Schools/PSU Directors are responsible for ensuring that their information systems and, where applicable, the supporting infrastructure complies with the relevant legislation and contractual requirements, including the:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 & Codes of practice
- Freedom of Information Act 2000 (inc. University's Publication Scheme)

Please note that this is not a definitive list but a representation of applicable laws in this area.

The University will also comply with all contractual requirements related to the holding and processing of information:

- JANET Acceptable Use Policy issued by Joint Information Systems Committee (Jisc) – Link
- UK Government's Security Policy Framework - Link
- MOD Standards (HMG IS1 & IS2 which are aligned to ISO 27001: 2005)
- Defence Standard 05-138 Issue 2: cyber security for defence suppliers - Link
- The terms and conditions of licences and contracts.

8. Physical Security

The University will ensure that appropriate physical security controls are used to protect information and information systems. These will include photo-id for all staff, students and contractors, site visitor access controls, card-enabled door access controls and on-site security patrols and closed circuit television (CCTV).

In addition, where there is a high density of IT infrastructure (Data Centres) further physical measures will exist such as security shutters, window bars (where appropriate), and tokenised door intruder alarm systems.

9. Network Security

The University will operate an IT network that maintains appropriate logical access and security controls, monitors for abnormal behaviour and allows adequate segregation of users, systems and data.

10. Information Security Education and Awareness

All Line Managers, Business Systems Managers and System Owners are responsible for authorising the access of users to information systems. They, in conjunction with the Information Services PSU must ensure that all University stakeholders receive adequate training on how to:

- operate the technology and information systems provided (including induction)
- understand the security risks to their information and systems
- use the security features provided within their information systems
- select, manage and safeguard passwords
- prevent the spread of malicious software and data, e.g. computer viruses, phishing and spam (unsolicited) e-mails
- identify and safeguard important records from loss, destruction and falsification
- identify and report information security incidents
- ensure the physical security of their desktop and other information assets

Cranfield University will ensure that appropriate training and awareness resources are made available to support Schools/ PSU's in carrying out this responsibility.

11. Incident Response and Business Continuity

The Information Security Team will act as the central point for receiving and responding to reports of actual or suspected information security incidents.

Appropriate processes and procedures have been implemented to initiate, record, manage and where necessary escalate the emergency response to the incident. Schools/PSU's will maintain an appropriate business continuity planning process, broad enough to respond to all types of potential failure to assets, including loss of infrastructure, information systems or critical data.

12. Compliance with Information Security Policy and Standards

The Information Security Team in conjunction with the ISWG will establish an appropriate programme of reviews and audits to ensure that the use of information and information systems are being managed in accordance with Cranfield University's information security policies, and any other relevant legal and contractual requirements.

Cranfield University respects the privacy and academic freedom of staff and students. However, Cranfield University may carry out lawful monitoring of IT systems. Staff, students and any other authorised users should be aware that Cranfield University may access network user activity logs, email, telephone and any other electronic communications, whether stored or in transit. This is in order to comply with the law and applicable regulations and to ensure appropriate use of Cranfield University IT systems.

13. Information Security Policies

Cranfield University has defined a number of policies and standards to provide detailed direction and guidance on important information security related issues.

Links to all relevant policies, standards and guidelines are provided in the following three sections of this policy.

Access to eInformation Policy (CU-IT-POL-1.01)

Policy outlining the set circumstances in which it is permissible for the University to access IT accounts, communications and/or data stored on IT equipment including any peripheral devices or hardware of staff members, students or other authorised users.

Connecting to the IT Network Policy (CU-IT-POL-2.01)

Policy outlining minimum controls for any system/equipment connecting to the University's IT network.

Data Backup Policy (CU-IT-POL-3.01)

Policy outlining how information and information systems will be backed up to safeguard information.

Data Loss Prevention Policy (CU-IT-POL-17.01)

Policy to address the risk of intentional and unintentional leakage of University 'sensitive' information.

Email Policy (CU-IT-POL-4.01)

Policy outlining how email shall be used by users of the University's IT systems.

Forensic Readiness Policy (CU-IT-POL-18.01)

Policy outlining how the University will undertake forensic investigations, using digital evidence, into the (mis)use of its information and information systems.

Information Handling Policy (CU-IT-POL-5.01)

Policy to define how information must be protected for the continuity of University business and ensure that the University meets its legal and contractual obligations.

Information Security Incident Response Policy (CU-IT-POL-6.01)

Policy is to minimise any damage caused by an information security incident by providing direction on incident evaluation, management and resolution.

Information Security Policy (CU-IT-POL-7.01)

This policy; the overriding security policy for the University.

Information Security Reporting Policy (CU-IT-POL-8.01)

Policy to determine how information security is reported within the University, outlining requirements to produce regular, formal reporting against defined controls.

Information Security Risk Policy (CU-IT-POL-9.01)

Policy describing the requirements and direction on the methods used by the University to assess and manage information security risk assessments.

Information Security Training and Awareness Policy (CU-IT-POL-10.01)

Policy describing how Cranfield University will implement and maintain an effective information security training and awareness programme across its IT user base.

IT Procurement, Recycling and Disposal Policy (CU-IT-POL-11.01)

Policy summarising the procurement, asset management and recycling/disposal of IT equipment.

IT Users Policy (CU-IT-POL-12.01)

Policy outlining the responsibilities of all IT users when accessing, processing and managing information on Cranfield University's IT systems.

Mobile Device Policy (CU-IT-POL-13.01)

Policy describing how the University and users of mobile devices can take appropriate security measures to protect Cranfield information.

Network Password Policy for IT Systems (CU-IT-POL-14.01)

Policy setting out standards for the creation, protection and use of passwords to protect University information.

Penetration Testing Policy (CU-IT-POL-15.01)

Policy outlining how information security penetration tests will be undertaken by specialist external suppliers, on behalf of Cranfield University.

Vulnerability Assessment & Remediation Policy (CU-IT-POL-16.01)

Policy outlining how Information Services (IT) will identify, assess and remediate IT vulnerabilities.

14. Information Security Procedures & Guidelines

Access to Electronic Information Standard Operating Procedure (CU-IT-PROC-1.01)

Standard operating procedure to ensure that any third party access (i.e. that from a party that is not the individual owner) to electronic information processed, transmitted or stored – under a user's account – is only permitted through the outlined procedure.

Cloud Security Guidelines (CU-IT-PROC-2.01)

Guidelines highlighting that University-supplied and managed 'cloud' services should be used to protect information.

Copyright Infringement Standard Operating Procedure (CU-IT-PROC-3.01)

Standard operating procedure to ensure the consistent management of any reported infringement of copyright is in compliance with legal and Janet service obligations.

Email Usage Guidelines (CU-IT-PROC-4.01)

Guidelines to ensure the effective and secure use of email.

Identity Theft Guidelines (CU-IT-PROC-5.01)

Guidelines highlighting what identity theft is, why it occurs and what steps users can take to prevent becoming a victim.

Disposal of Confidential Waste process (CU-SHE-PROC-3.10)

Procedure outlining and clarifying the process for the removal and disposal of confidential waste from campus buildings in a secure and auditable manner.

Information Handling Procedures (CU-IT-PROC-6.01)

Standard operating procedures to provide instructions on how to appropriately handle and protect University information to ensure its confidentiality, integrity and availability.

Information Security Incident Response Standard Operating Procedure (CU-IT-PROC-7.01)

Standard operating procedure to provide assurance in the consistent management of major information security (InfoSec) incidents by the Information Services Professional Service Unit (IS PSU) and other affected parties.

Information Security Roles and Responsibilities (CU-IT-PROC-8.01)

Document identifying the roles and responsibilities required for maintaining an appropriate information security-related governance framework at the University.

Information Security Working Group (ISWG); Terms of Reference (CU-IT-PROC-16.01)

Document that sets out the 'Terms of Reference' for the Information Security Working Group

Network Password Guidelines (CU-IT-PROC-9.01)

Guidelines providing useful information on how to construct and use passwords to keep information safe.

Penetration Testing Standard Operating Procedure (CU-IT-PROC-10.01)

Standard operating procedure for running and managing penetration tests.

Phishing Guidelines (CU-IT-PROC-11.01)

Guidelines highlighting what phishing is, why it occurs and what steps users can take to help prevent them becoming a victim.

Proofpoint Email Security (IT08)

Details of the email security solution provided by Proofpoint.

Ransomware Guidelines (CU-IT-PROC-12.01)

Guidelines highlighting what ransomware/scareware is, why it occurs and what steps users can take to prevent them becoming a victim.

Safe Surfing Guidelines (CU-IT-PROC-13.01)

Guidelines highlighting practical steps that users should take to assist themselves in using the Internet safely and securely.

Secure Disposal Standard Operating Procedure (CU-IT-PROC-14.01)

Standard operating procedure used at the end of the IT life-cycle to ensure that IT assets are securely disposed or recycled in-line with policy and regulations.

Social Networking Guidelines (CU-IT-PROC-15.01)

Guidelines highlighting practical steps that users should take to protect themselves when using social networking websites.

S07 Terms and conditions; External partners (CU-IT-PROC-16.01)

Terms and conditions that apply to any external partner or contractor registered to use IT systems, provided by Cranfield University, that outline the acceptable use of these systems.

15. Secure Environment Policies & Procedures

The Cranfield Secure Environment (CSE) must be used when processing data of a highly sensitive nature to support and meet the requirements of specific contracted work packages and projects. The following policies are applicable to this environment only:

Access Control Policy (CU-ITCSE-POL-10.01)

Policy describing the requirements for accessing information assets and information processing facilities of the Cranfield Secure Environment (CSE).

Access Control Procedures (CU-ITCSE-PROC- 2.01)

Procedure describing the requirements for accessing information assets and information processing facilities of the CSE.

Asset Management Policy (CU-ITCSE-POL-11.01)

Policy outlining how assets pertaining to the CSE will be managed.

Removable Media Policy (CU-ITCSE-POL-12.01)

Policy outlining that the use of removable media is not allowed within the CSE.

Security and Protective Monitoring (CU-ITCSE-POL-13.01)

Policy describing the requirements for maintaining a consistent approach to security logging and monitoring of systems and networks used within the CSE.

Supplier Assurance Policy (CU-ITCSE-POL-14.01)

Policy providing direction on the processes Cranfield University use to interact and conduct business with third party suppliers that support the CSE.

Supplier Due Diligence (CU-ITCSE-PROC-3.01)

Procedure to be used in conjunction with the Security Assurance Questionnaire to understand and rate risk profiles of potential supplier use of the CSE.

Document control

Document title	Information Security Policy (External version)
Document number	CU-IT-POL-7.01[Ext]
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Implementation/effective date	2010
Approval by and date	Information Assurance Committee; 28/09/2020
Date of last review and version number	September 2020; V1.6
Date of next review	August 2021
Standards reference	DCPP CSM; ISO 27001
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.5	Minor changes to reflect changed working practices and inclusion of new University-wide and specific Secure Environment policies	Information Security	September 2019
1.6	Document numbering introduced and policy amended to clarify CSE usage	Information Security	September 2020