Information Security Policy

Information Technology (IT)

The following statement has been endorsed by both the Vice Chancellor (Professor Karen Holford) and the Director of Information Technology (Gregor Waddell) 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 appropriately.

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 Technology Executive and formally approved by the Information Assurance Committee (IAC), must be implemented by all Faculties/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 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 Technology, in collaboration with the IT Executive is responsible for developing appropriate information security policies and standards.

The Information Security and IT Infrastructure Teams are responsible for the day-to-day operational information security and assurance activities including appropriate protection of personal and financial data.

Faculties/PSU's and associated entities are responsible for embedding information security policies and standards and supporting this policy.

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.

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 Faculties/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.

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

The University also supports the National Cyber Security Centres (NCSC) Cyber Essentials[1] certification scheme, which is a pre-requisite when bidding for UK Government contracts that involve handling sensitive and personal information.

6. Information Security Risk Management

The Information Security Team will liaise with stakeholders across the University to ensure that an appropriate process is used to identify, assess, rank and feed risks into the information security risk register.

The process should assess:

- The business harm likely to result from a security failure, considering 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 IT Security Board 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 and undertake information security risk assessments prior to new services and/or systems being implemented, and annually for those that have been assessed as critical to the University, using 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 Faculties/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
- Cyber Essentials scheme - Link

[1] https://www.ncsc.gov.uk/cyberessentials/overview

- 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
- Payment Card Industry Data Security Standards (PCI DSS)
- 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 surveillance cameras.

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. Operational Security

The Information Security and IT Infrastructure Teams in conjunction with colleagues within the IT Professional Services Unit and business/system owners will undertake security assurance activities as follows:

- Run an annual schedule of penetration tests on key systems using contracted certified external parties
- Run regular vulnerability scans on IT services
- Ensure that appropriate actions are undertaken in a timely manner to address any discovered vulnerabilities, patch systems in-line with best practice and external certification requirements and monitor adherence to security baselines
- Run and monitor preventative and reactive security controls
- Segregate or temporarily suspend IT systems or services that do not meet minimum standards

11. Reporting

The Information Security Team will provide relevant reports and metrics to show the performance of current information security measures (regarding preventative and reactive controls), assess progress, highlight concerns, and show the level of cyber security maturity across the University.

12. 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 Technology 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 work area and other information assets

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

13. 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.

For incidents involving personal data please report to gdpr@cranfield.ac.uk immediately.

Appropriate processes and procedures have been implemented to initiate, record, manage and where necessary escalate the emergency response to the incident. Faculties/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.

14. Compliance with Information Security Policy and Standards

The Information Security Team in conjunction with the IT Security Board 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 to comply with the law and applicable regulations and to ensure appropriate use of Cranfield University IT systems.

15. Information Security policies, procedures, and guidance (IT users)

Cranfield University has defined several 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 sections of this policy.

IT Users' policy and procedures document – CU-IT-POL-1.01

Principle policy for all IT users of University systems and services.

Information Security policy – CU-IT-POL-2.01 (this document)

Information Handling policy and procedures CU-IT-POL-3.01 (Internal only)

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.

Password policy and procedure – CU-IT-POL-4.01

Policy and guidance for the creation, protection, and use of passwords to protect University information.

Information security guidance document – CU-IT-ISGde-5.01

User awareness guidance on the most common ways that users, information, and information system can be compromised.

Acceptable Use Policy for External Partners - CU-IT-PROC-6.01

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.

16. Information Technology internal policies (internal only)

IT operational policies - CU-IT-POL–7.01 (Internal only)

17. Information Technology standard operating procedures (Internal only)

IT standard operating procedures - CU-IT-PROC–8.01 (Internal only)

18. IT information sheets (Internal only)

The IT function provides a range of helpsheets on the University's intranet site (Internal only).

19. Other relevant Policies and Procedures (Non-IT)

Card Payment Data Security policy (Internal only)

Data Protection Policy

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

Document control

Document title	Information Security Policy - Open
Document number	CU-IT-POL-2.01
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Technology
Implementation/effective date	2010
Approval by and date	Information Assurance Committee; 19/09/2024
Date of last review and version number	September 2024; V2.0
Date of next review	August 2025
Standards reference	DCPP CSM; ISO 27001
Information categorisation	Open

Document Review

Version	Amendment	By	Date
2.0	Annual review	Information Security	October 2024