

ICT Security Policy

Document Ref:	ISMS08
Version:	2.4
Date of version:	31/01/2026
Author:	Bilal Hussain
Approved by:	Andy Kynoch
Confidentiality level:	Confidential

Amendment History

Date	Version	Author	Details of Amendment
15/01/2019	v1.0	Bilal Hussain	Initial Release
10/01/2020	v1.1	Bilal Hussain	Update for 27701
10/05/2021	v2.0	Bilal Hussain	Review
10/05/2022	v2.1	Bilal Hussain	Review
26/05/2023	v2.1b	Bilal Hussain	Review
30/05/2024	v2.2	Bilal Hussain	Review & Update
30/05/2025	v2.2b	Bilal Hussain	Review
30/08/2025	v2.3	Bilal Hussain	Review & Update
31/01/2026	v2.4	Bilal Hussain	Review & Update

Table of Contents

0. References **2**

1. Introduction **2**

2. Scope **2**

3. Policy Statement **3**

Authorised Use 3
Acceptable use 3
Security awareness 3
Business Continuity 4
Monitoring and reporting 4
Risk Assessment 4
Security Policy Review 4
Asset Management 4
Sanctions 5

4. Compliance with legal and contractual obligations **5**

5. Responsibilities **5**

6. Development of specific ICT policies, procedures and guidelines **6**

7. Breaches of Policy **6**

8. Document Management **7**

Appendix A **8**

Appendix B **9**

0. References

ISO 27001:2022 Annex A Controls**:**

A.5.1	Policies for Information Security & Privacy
A.5.1	Review of the policies for Information Security & Privacy
A.5.2	Information Security & Privacy roles and responsibilities
A.5.31	Identification of applicable legislation and contractual requirements

1. Introduction

ICTS UK Group of Companies (ICTS) recognises that Information and Communications Technology (ICT) systems and information are valuable assets which are essential in supporting ICTS's strategic objectives. ICTS recognises its obligations to protect information from internal and external threats and recognises that effective Information Security & Privacy management is critical to ensure the successful enablement of ICT and delivery of business functions and services. ICTS is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets.

Information Security & Privacy management is an ongoing cycle of activity aimed at continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorised access, disclosure, modification or destruction and is vital for the protection of information and ICTS's reputation. This policy details ICTS's approach to ICT Security Management and contains no sensitive or restricted information; it may be freely publicised to relevant parties. A current version of this document is available to ICTS staff on the corporate intranet and to external parties on ICTS's website at www.ICTS.co.uk.

The approach is based upon recommendations contained within ISO27001:2022 a code of practice for Information Security & Privacy management.

2. Scope

This ICT Security Policy applies to:

- ICT systems belonging to, or under the control of, ICTS.
- Information stored, or in use, on ICTS ICT systems.
- Information in transit across ICTS's voice or data networks.
- Control of information leaving ICTS.
- Information access resources.
- Cloud based services utilised by ICTS.
- All parties who have access to, or use of ICT systems and information belonging to, or under the control of, ICTS including:
  - ICTS employees
  - Contractors
  - Temporary staff
  - Partner organisations
  - Any other party utilising ICTS ICT resources

Application of this policy applies throughout the information lifecycle from acquisition / creation, through to utilisation, storage and disposal.

3. Policy Statement

The Information Security & Privacy Policy is based on the principles set out in the British Standard for Information Security & Privacy - ISO/IEC 27001:2022
ICTS is committed to the development and maintenance of an Information Security & Privacy Management System based upon the International Standard ICTS has developed this ICT Security Policy to:

- Provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements.
- State the responsibilities of staff, partners, contractors and any other individual or organisation having access to ICTS's ICT systems.
- State management intent to support the goals and principles of security in line with business strategy and objectives.
- Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained.
- Optimise the management of risks, by preventing and minimising the impact of ICT security incidents.
- Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required.
- Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats.
- Ensure ICT Information Security & Privacy requirements are regularly communicated to all relevant parties.

Authorised Use

Access to ICT systems and Information for which ICTS is responsible is permitted in support of ICTS's areas of business or in connection with a service utilised by ICTS. Authorised users are defined as: ICTS employees, authorised contractors, temporary staff or partner organisations when using information services provided by ICTS

Acceptable use

All users of ICT systems and information for which ICTS is responsible must agree to, and abide by, the terms of ICTS's Acceptable Use Policy, associated security policies and applicable Codes of Connection or Conduct.

Security awareness

ICTS is committed to promoting safe working practices. All employees will receive security awareness training commensurate with the classification of information and systems to which they have access.

Staff working in specialised roles will receive appropriate training relevant to their role. Relevant Information Security & Privacy policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of Information Security & Privacy policies and procedures.

Business Continuity

ICTS has developed, and maintains, a Business Continuity Strategy based on specific risk assessment to maintain critical business functions in the event of any significant disruption to services or facilities on which ICTS is reliant.

Monitoring and reporting

ICTS reserves the right to monitor the use of ICT systems and information, including email and internet usage, to protect the confidentiality, integrity and availability of ICTS's information assets and ensure compliance with ICTS's policies. ICTS may, at its discretion, or where required by law, report security incidents to the relevant authorities for further investigation. As part of the standard audit review process, Internal Audit will routinely assess compliance with ICTS's ICT Security Policy and applicable ISO27001 controls and report matters to senior management where appropriate. Security incidents reported through the Security Incident Management Policy and Procedures, will inform on the effectiveness of ISO27001 controls and assist in identifying training and awareness requirements and improvements through the Improvement procedure.

Risk Assessment

ICTS has developed a Risk Management Strategy and the risk to ICTS's ICT systems and information will be managed under this framework *management.* Reviews are independent, unbiased and verified by either internal audit or external parties when required.

Security Policy Review

ICTS will conduct an annual review of the policy or following any significant security incidents, changes to UK or EU legislation or changes to ICTS's business requirement or structure.

Asset Management

ICTS will maintain an inventory consisting of all information assets which will be managed in accordance with ICTS's Information Security & Privacy policies and procedures.

Sanctions

Failure of ICTS employees to comply with ICTS's Information Security & Privacy Policy may lead to disciplinary action under ICTS's disciplinary procedure.
Failure of contractors, temporary staff, partners or third-party organisations to comply with ICTS's Information Security & Privacy Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

4. Compliance with legal and contractual obligations

ICTS will abide by all UK & EU legislation relating to information storage and processing including:

- The Data Protection Act (1998)
- The Freedom of Information Act (2000)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)
- UK GDPR & EU GDPR

ICTS will also comply with any contractual requirements, standards and principles required to maintain the business functions of ICTS including:

- Protection of intellectual property rights.
- Protection of ICTS's records.
- Compliance checking and audit procedures.
- Prevention of facilities misuse.
- Relevant codes of connection to third party networks and services.

5. Responsibilities

Co-ordination: ICTS co-ordinates Information Security & Privacy management across the company network via the IT Department.

Security Officer: ICTS's Information Security & Privacy Manager is responsible for ensuring policies and procedures are in place to cover all aspects of ICT systems and Information Security & Privacy. All policies will be communicated across ICTS to ensure good working practices and to minimise the risk to ICTS's reputation.

Directors: are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with ICTS's ICT Security Policy. Day to day responsibility for the management of ICT systems and information may be delegated to staff designated as information or system owners within departments.

Users of resources: It is the responsibility of any individual or organisation having access to ICTS's ICT systems and information to comply with ICTS's ICT Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the ICT systems and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the Security/Business Continuity Manager via ICTS's Incident Reporting system.

6. Development of specific ICT policies, procedures and guidelines

ICTS is committed to the ongoing development and review of ICT policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. This work will be co-ordinated by the IT Manager. A list of current supporting documents is included in Appendices A-B. New policies and procedures are distributed to all stakeholders at the time of issue. Appendices A-B of this policy are updated during the annual ICT Security review.

7. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to ICTS assets, or an event which is in breach of ICTS's security procedures and policies.

All ICTS employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through ICTS's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of ICTS

ICTS will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

Incident Reporting

Users will continually be encouraged to report any breaches to the IT Department. Breaches can involve not only Information Technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern, or which may contravene ICTS's associated policies.

Incident Management

During reporting of a breach, details of the incident will be entered into the call logging system - by the person directly reporting the incident. Once the call has been entered into the system, an email is generated and sent to the Information Security & Privacy Manager and also copied to the Director. The Information Security & Privacy Manager will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representative to deal with. Representatives looking into security breaches will be responsible for updating, amending and modifying the status and clearance code of incidents.

8. Document Management

This document is valid as of 31/01/2026.

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

- Conformance to the requirements of ISO 27001:2022
- Conformance to the requirements of ISO 27701: 2019
- Legislative requirements defined by law, where appropriate

Managing Director
Andy Kynoch



Appendix A

List of ISMS Security – Policies

Title	Status	Review Date
ISMS02 Acceptable Use Policy	Published	31/01/2027
ISMS03 Data Retention Policy	Published	31/01/2027
ISMS04 Asset Management Policy	Published	31/01/2027
ISMS05 Incident Management Policy	Published	31/01/2027
ICT Security Policy UK & Ireland	Published	31/01/2027
ISMS06 Corporate Records Management	Published	31/01/2027
ISMS07 Encryption & Cryptographic Control Policy	Published	31/01/2027
ISMS09 Improvement Policy	Published	31/01/2027
ISMS Backup Policy	Published	31/01/2027
ISMS12 ISMS Policy	Published	31/01/2027
ISMS14 Password Policy	Published	31/01/2027
ISMS15 Home Printing Policy	Published	31/01/2027
ISMS16 Disposal & Destruction Policy	Published	31/01/2027
ISMS17 Clear Desk Policy	Published	31/01/2027
ISMS18 IT Change Policy	Published	31/01/2027
ISMS20 Server & Network Security Policy	Published	31/01/2027
ISMS22 Third Party Connection Policy	Published	31/01/2027
ISMS23 Secure Development Policy	Published	31/01/2027
ISMS26 Disposal & Destruction Policy	Published	31/01/2027

Appendix B

List of ISMS Security - Procedures

Title	Status	Review Date
ISMS13 Operational Management Procedure	Published	31/01/2027
ISMS25 PC Security Procedures	Published	31/01/2027
ISMS31 Laptop & Mobile Device Security Procedures	Published	31/01/2027
ISMS32 Malicious Software & Anti-Virus Procedure	Published	31/01/2027
ISMS34 Physical & Environmental Infrastructure Procedure	Published	31/01/2027
ISMS36 Risk Assessment & Treatment	Published	31/01/2027
ISMS37 Security Awareness Procedure	Published	31/01/2027
ISMS41 Internal Audit Procedure	Published	31/01/2027