ICT Security Policy

Document Ref:	ISMS08
Version:	1.1
Date of version:	10/09/2020
Author:	B. Hussain
Approved by:	C. Cox
Confidentiality level:	Confidential

Amendment History

Date	Version	Author	Details of Amendment
10/11/2017	1.0	B. Hussain	Initial Release
10/09/2020	1.1	B. Hussain	Review and update

Table of Contents

1. References

ISO 27001:2013 Annex A Controls

A.5.1.1	Policies for information security
A.5.1.2	Review of the policies for information security
A.6.1.1	Information security roles and responsibilities
A.18.1.1	Identification of applicable legislation and contractual requirements

2. Introduction

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

Information security 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 (UK) LTD's reputation.
This policy details ICTS (UK) LTD's approach to Information and Communications Technology (ICT) Security Management contains no sensitive or restricted information and may be freely publicised to relevant parties. A current version of this document is available to ICTS (UK) LTD staff on the corporate intranet and is available to external parties on ICTS (UK) LTD's website at www.icts.co.uk.

The approach is based upon recommendations contained within ISO27002 a code of practice for information security management.

3. Scope

This ICT Security Policy applies to:

- ICT systems belonging to, or under the control of, ICTS (UK) LTD;
- Information stored, or in use, on ICTS (UK) LTD ICT systems;
- Information in transit across ICTS (UK) LTD's voice or data networks;
- Control of information leaving ICTS (UK) LTD;
- Information access resources;
- All parties who have access to, or use of ICT systems and information belonging to, or under the control of, ICTS (UK) LTD including:

    - ICTS (UK) LTD employees
    - Contractors
    - Temporary staff
    - Partner organisations
    - Any other party utilising ICTS (UK) LTD ICT resources

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

4. Policy Statement

The Information Security Policy is based on the principles set out in the British Standard for Information Security - *ISO/IEC 27002*
ICTS (UK) LTD is committed to the development and maintenance of an Information Security Management System based upon the International Standard ICTS (UK) LTD 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 (UK) LTD'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 requirements are regularly communicated to all relevant parties.

Authorised Use

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

Acceptable use

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

Security awareness

ICTS (UK) LTD 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 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 policies and procedures.

Business Continuity

ICTS (UK) LTD 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 (UK) LTD is reliant.

Monitoring and reporting

ICTS (UK) LTD 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 (UK) LTD's information assets and ensure compliance with ICTS (UK) LTD's policies. ICTS (UK) LTD may, at its discretion, or where required by law, report security incidents to the relevant UK authorities for further investigation. As part of the standard audit review process, Internal Audit will routinely assess compliance with ICTS (UK) LTD'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 (UK) LTD has developed a Risk Management Strategy and the risk to ICTS (UK) LTD'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 (UK) LTD will conduct an annual review of the policy or following any significant security incidents, changes to UK or EU legislation or changes to ICTS (UK) LTD's business requirement or structure.

Asset Management

ICTS (UK) LTD will maintain an inventory consisting of all information assets which will be managed in accordance with ICTS (UK) LTD's information security policies and procedures.

Sanctions

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

5. Compliance with legal and contractual obligations

ICTS (UK) LTD will abide by all UK 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)

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

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

6. Responsibilities

Co-ordination: ICTS (UK) LTD co-ordinates information security management across the company network via the IT Department.

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

Directors: are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with ICTS (UK) LTD'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 (UK) LTD's ICT systems and information to comply with ICTS (UK) LTD'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 (UK) LTD's Incident Reporting system.

7. Development of specific ICT policies, procedures and guidelines

ICTS (UK) LTD 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.

8. 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 (UK) LTD assets, or an event which is in breach of ICTS (UK) LTD's security procedures and policies.

All ICTS (UK) LTD 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 (UK) LTD's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of ICTS (UK) LTD
ICTS (UK) LTD 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 be 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 (UK) LTD's associated policies.

Incident Management

During reporting of a breach, details of the incident will be entered into the call logging system - either 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 Manager and also copied to the Director. The Information Security 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.

9. Associated Records

Record name	Storage location	Owner	Protection Control	Retention Period

10.Document Management

This document is valid as of 10/11/17.

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

- Conformance to the requirements of ISO 27001:2013
- Legislative requirements defined by law, where appropriate

Appendix A

List of ISMS Security – Policies

Title	Status	Review Date
Acceptable Use Policy	Published	10/11/2021
Access Control Policy	Published	10/11/2021
Asset Management Policy	Published	10/11/2021
Encryption Policy	Published	10/11/2021
ICT Security Policy	Published	10/11/2021
Improvement Policy	Published	10/11/2021
Information Backup and Restore Policy	Published	10/11/2021
Internet and Email Acceptable Use Policy	Published	10/11/2021
ISMS Policy	Published	10/11/2021
Operational Management	Published	10/11/2021
Password Policy	Published	10/11/2021
Record Disposal Policy	Published	10/11/2021
Scanning and Disposal Policy	Published	10/11/2021
Secure Desk Policy	Published	10/11/2021
Secure Email Policy	Published	10/11/2021
Security Incident Management Policy	Published	10/11/2021
Server Security Policy	Published	10/11/2021
Supplier Security Policy	Published	10/11/2021
Third Party Connection Policy	Published	10/11/2021
Wireless Network Policy	Published	10/11/2021

Appendix B

List of ISMS Security - Procedures

Title	Status	Review Date
Data Protection & Storage Media Handling Procedures	Published	10/11/2021
Desktop PC Security Procedures	Published	10/11/2021
Disposal of ICT Equipment	Published	10/11/2021
Document and Record Control Procedures	Published	10/11/2021
Improvement Procedure	Published	10/11/2021
Incident Reporting and Management Procedure	Published	10/11/2021
Information Systems Development and Maintenance Procedures	Published	10/11/2021
Laptop & Mobile Device Security Procedures	Published	10/11/2021
Malicious Software and Anti Virus Procedure	Published	10/11/2021
Mobile Phone Procedures	Published	10/11/2021
Physical and Environmental Infrastructure Procedure	Published	10/11/2021
Records Appraisal Procedure	Published	10/11/2021
Risk Assessment and Treatment	Published	10/11/2021
Security Awareness Procedure	Published	10/11/2021
Teleworking and Mobile Working Procedures	Published	10/11/2021