ISMS-08 ICT Security Policy

To the requirements of ISO 27001:2013

Document Ref:	ISMS-08 ICT Security Policy
Version:	1
Date of Version:	01/09/2017
Author:	Juliet Moran
Approved by:	Alistair Bates
Confidentiality Level:	Controlled: **Uncontrolled if printed**

Table of Contents

0. Applied Controls

Control Ref	Title
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

1. Introduction

Hosting Systems Limited recognises that ICT systems and information are valuable assets which are essential in supporting Hosting Systems Limited's strategic objectives. Hosting Systems Limited 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. Hosting Systems Limited is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets belonging to the Company and that of its Clients.

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 Hosting Systems Limited's reputation.

This Policy details Hosting Systems Limited'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 Hosting Systems Limited staff on the corporate intranet and is available to external parties on Hosting Systems Limited's website at http://www.hostingsystems.uk

The approach is based upon recommendations contained within ISO 27002 Information technology. Security techniques. Code of practice for information security controls.

2. Scope

This ICT Security Policy applies to:

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

    - Hosting Systems Limited employees
    - Clients
    - Contractors
    - Temporary staff
    - Partner organisations

- Volunteers
- Any other party utilising Hosting Systems Limited 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 Policy is based on the principles set out in the British Standard for Information Security - *ISO/IEC 27002.*

Hosting Systems Limited is committed to the development and maintenance of an Information Security Management System based upon the International Standard.

Hosting Systems Limited 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 Hosting Systems Limited'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.

3.1 Authorised Use

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

3.2 Acceptable Use

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

3.3 Security Awareness

Hosting Systems Limited 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.

3.4 Business Continuity

Hosting Systems Limited 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 Hosting Systems Limited is reliant.

3.5 Monitoring and Reporting

Hosting Systems Limited 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 Hosting Systems Limited's information assets and ensure compliance with Hosting Systems Limited's policies. Hosting Systems Limited 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 Hosting Systems Limited'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.

3.6 Risk Assessment

Hosting Systems Limited has developed a Risk Management Strategy and the risk to Hosting Systems Limited's ICT systems and information will be managed under this framework with reference to the guidelines detailed in ***BS ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management***. Reviews are independent, unbiased and verified by either internal audit or external parties when required.

3.7 Security Policy Review

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

3.8 Asset Management

Hosting Systems Limited will maintain an inventory consisting of all information assets which will be managed in accordance with Hosting Systems Limited's information security policies and procedures.

3.9 Sanctions

Failure of Hosting Systems Limited employees to comply with Hosting Systems Limited's Information Security Policy may lead to disciplinary action under Hosting Systems Limited's disciplinary procedure.

Failure of contractors, temporary staff, partners or third party organisations to comply with Hosting Systems Limited's Information Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

4. Compliance with Legal and Contractual Obligations

Hosting Systems Limited 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)

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

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

5. Responsibilities

5.1 Co-Ordination:

Hosting Systems Limited co-ordinates information security management across the company network via the IT Department.

5.2 Security Officer:

Hosting Systems Limited's Information Security Management Representative 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 Hosting Systems Limited to ensure good working practices and to minimise the risk to Hosting Systems Limited's reputation.

5.3 Directors:

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

5.4 Users of Resources:

It is the responsibility of any individual or organisation having access to Hosting Systems Limited's ICT systems and information to comply with Hosting Systems Limited'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 Hosting Systems Limited's Incident Reporting system.

6. Development of specific ICT Policies, Procedures and Guidelines

Hosting Systems Limited 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 Hosting Systems Limited assets, or an event which is in breach of Hosting Systems Limited's security procedures and policies.

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

Hosting Systems Limited 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.

7.1 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 Hosting Systems Limited's associated policies.

7.2 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 via the Service Support operator taking a telephone call or via website or via an e-mail. Once the incident has been entered into the system, an email is generated and sent to the Information Security Management Representative and also copied to a Director.

The Information Security Management Representative 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 in the Incident management logging system.

_____

A Bates
Managing Director

Appendix A: List of ISMS Security Policies

Title	Status
ISMS-01 Statement of Applicability (SoA)	Published
ISMS-02 Acceptable Use Policy	Published
ISMS-03 Access Control Policy	Published
ISMS-04 Asset Management Policy	Published
ISMS-05 Digital Records Preservation Policy	Published
ISMS-06 Records Management Policy	Published
ISMS-07 Encryption Policy	Published
ISMS-08 ICT Security Policy	Published
ISMS-09 Information Backup & Restore Policy	Published
ISMS-10 Information Classification & Handling Policy	Published
ISMS-11 Internet and Email Acceptable Use Policy	Published
ISMS-12 ISMS Policy	Published
ISMS-13 Operational Management	Published
ISMS-14 Password Policy	Published
ISMS-15 Record Disposal Policy	Published
ISMS-16 Scanning and Disposal Policy	Published
ISMS-17 Secure DesK Policy	Published
ISMS-18 Secure Email Policy	Published
ISMS-19 Security Incident Management Policy	Published
ISMS-20 Server Security Policy	Published
ISMS-21 Supplier Security Policy	Published
ISMS-22 Third Party Connection Policy	Published
ISMS-23 Wireless Network Policy	Published

Appendix B: List of ISMS Security Procedures

Title	Status
ISMS-24 Data Protection & Storage Media Handling Procedures	Published
ISMS-25 Desktop PC Security Procedures	Published
ISMS-26 Disposal of ICT Equipment	Published
ISMS-27 Document and Record Control Procedures	Published
ISMS-28 Business Continuity Policy Manual	Published
ISMS-29 Improvement Procedure	Published
ISMS-30 Incident Reporting and Management Procedure	Published
ISMS-31 Information Classification and Handling Procedures	Published
ISMS-32 Information Systems Development and Maintenance Procedures	Published
ISMS-33 ISMS Internal Audit Procedure	Published
ISMS-34 Laptop & Mobile Device Security Procedures	Published
ISMS-35 Malicious Software and Anti Virus Procedure	Published
ISMS-36 Mobile Phone Procedures	Published
ISMS-37 Physical and Environmental Infrastructure Procedure	Published
ISMS-38 Records Appraisal Procedure	Published
ISMS-39 Risk Assessment and Treatment	Published
ISMS-40 Security Awareness Procedure	Published
ISMS-41 Teleworking and Mobile Working Procedures	Published
ISMS-42 Management Review Procedure	Published