Vercity Management System

Policy

Title:

Digital Information Security Policy

Doc Reference:

GLB-GEN -TEC-POL-0334

Version:

2.1

Effective Date

27-05-2026

SUMMARY

This policy outlines the framework for managing information security within Vercity Holdings, ensuring compliance with ISO/IEC 27001, Cyber Essentials, and UK Data Protection Laws. It defines responsibilities, processes, and controls to protect information assets and maintain confidentiality, integrity, and availability.

1. PURPOSE

To establish a systematic approach for safeguarding information assets against unauthorised access, disclosure, alteration, and destruction. The policy aims to ensure compliance with legal, regulatory, and contractual obligations while supporting continual improvement of the Information Security Management System (ISMS).

2. SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and other personnel, as well as any third-party entities with access to Vercity Holdings' information systems and data. The policy applies to all devices, networks, applications, and services owned, leased, or operated by the organisation.

3. DEFINITIONS

- **ISMS:** Information Security Management System.
- **ISO/IEC 27001:** International standard for information security management.
- **Cyber Essentials:** UK government-backed certification for basic cyber security controls.
- **Confidentiality, Integrity, Availability (CIA):** Core principles of information security.

4. ROLES AND RESPONSIBILITIES

- **Chief Digital Officer:** Responsible for endorsing and overseeing the Digital Security Policy, ensuring adequate resources are allocated for policy implementation and monitoring.
- **ITC Manager:** Responsible for the development, implementation, maintenance, and enforcement of this policy.
- **Managers:** Responsible for implementing this policy within their business areas, ensuring staff compliance, managing information security risks, protecting information assets, and reporting any actual or suspected incidents.
- **Employees and Contractors:** Must protect, handle, and share data in accordance with Data Protection Laws and other relevant regulations, report any actual or suspected breaches, and maintain confidentiality and integrity of information.
- **Vercity Digital Team:** Assigns security roles, conducts regular audits, provides training, and supports continual improvement of the Information Security Management System.

5. POLICY

Vercity Holdings has implemented an Information Security Management System, complying with the requirements of ISO/IEC 27001 and Cyber Essentials, to ensure that we assess risks within the business and strive to prevent security incidents.

The scope of this Security Management System includes information stored on computers, transmitted across networks, printed out or written on paper, stored on portable media, or spoken in conversation or over the telephone.

It is our policy to ensure that:

- we comply with UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.
- we understand the needs and expectations of all interested parties and have determined those interested parties that are relevant to the information security management system.
- assigned relevant information security roles and responsibilities.
- all customer, client or Group held data is protected, handled, and shared where necessary in accordance with the requirements of UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of the country of the data owner.
- regular audits and reports are prepared, which will be reviewed by the Executive Board.
- all breaches of Information Security, actual or suspected, are reported and investigated up to Board Level.
- confidentiality of information is assured.
- integrity of information is maintained.
- regulatory and legislative requirements, together with any contractual security obligations, are met.
- information is protected against unauthorised access.
- objectives and targets are set and monitored to achieve continual improvement in our Information Security Management System.
- information security training is provided, where required.
- standards and procedures are implemented to support this Policy.
- continual improvement is applied across our products and services to ensure the effectiveness of our Information Security Management System.

To achieve this consistently and efficiently, we operate a quality system which meets the requirements of ISO/IEC 27001.

We set and regularly review quality objectives and targets to achieve these aims.

6. POLICY REVIEW

This Policy will be reviewed annually or whenever there are significant changes in technology, legal, or regulatory requirements. Changes will be approved by senior management and communicated to all personnel.

DOCUMENT CONTROL (THIS DOCUMENT)

Author	Checker	Reviewer	Approver
Nigel Keen	Clare Le Grys	Richard Puckey	James Turnbull
27/05/2026	27/05/2026	27/05/2026	27/05/2026

Revision History

Version	Date	Description of Change	Author
1.0	13/01/2025	Initial draft	ITC Manager
1.1	20/01/2025	Draft reviewed by Risk and Compliance	HSEQ Manager
1.2	18/02/2025	Updated following Initial ISO/IEC 27001 Audits	ITC Manager
1.3	04/08/2025	Document control & Amendment history added	ITC Manager
2.0	30/10/2025	Transferred to new corporate template	ITC Manager
2.1	27/05/2026	Managers roles and responsibilities added	ITC Manager

End.