Vercity Management System

Policy

Title:

Digital Security Policy

Doc Reference:

GLB-GEN -TEC-POL-0332

Version:

2.0

Effective Date

02-01-2026

SUMMARY

This policy establishes the framework for managing digital security within Vercity Holdings. It ensures confidentiality, integrity, and availability of information assets, aligning with ISO/IEC 27001 standards. It applies to all employees, contractors, and third parties accessing organisational systems.

1. PURPOSE

The purpose of this Digital Security Policy is to ensure the confidentiality, integrity, and availability of Vercity Holdings' information assets, systems, and data. This policy outlines the security standards and requirements necessary to protect these assets against unauthorised access, misuse, disclosure, or destruction in compliance with ISO/IEC 27001.

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 based on ISO/IEC 27001.
- **MFA:** Multi-Factor Authentication.
- **BYOD:** Bring Your Own Device.
- **Data Classification:** As per the requirements in the Information, Classification & Handling Standard.

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.
- **Head of HSEQ:** Management Representative responsible for the Vercity Holding Information Security Management System.
- **ITC Manager:** Responsible for the development, implementation, maintenance, and enforcement of this policy.
- **Vercity Digital Team:** Responsible for enforcing technical controls and monitoring systems to ensure compliance with the policy.
- **Employees and Contractors:** Expected to understand and comply with the IT Security Policy and report any security incidents promptly in accordance with the Breach Investigation Standard.
- **Third-Party Vendors:** Comply with contractual security requirements and demonstrate adherence to this policy.

5. POLICY

5.1. Information Security Management System (ISMS)

Vercity Holdings maintains an ISMS based upon ISO/IEC 27001 to ensure a systematic approach to managing sensitive information and implementing appropriate security controls. The ISMS will be reviewed and updated regularly to address emerging security risks and maintain compliance with the ISO standard.

5.2. Risk Management

Vercity Holdings will identify, assess, and manage information security risks associated with its assets, technologies, and processes. Risk assessments will be conducted at least annually, or whenever there is a significant change in technology, processes or the threat landscape.

To maintain the security and integrity of our organisation, it is crucial that all staff members promptly report any observed risks or potential breaches to gdpr@vercity.co.uk in line with the Vercity Holdings Breach Investigation Standard. By doing so, we can ensure that these issues are addressed swiftly and effectively, minimising any potential damage. This proactive approach not only helps in safeguarding our systems and data, but also reinforces our commitment to maintaining a secure and compliant work environment.

5.3. Access Control

- **User Access Management:** Access to information systems and data is granted on a "least privilege" basis, based on job roles and responsibilities. User access rights are reviewed regularly.
- **Authentication and Authorisation:** All users must authenticate using secure methods, such as multi-factor authentication (MFA), to access critical systems. Access will be granted only as per defined approval workflows.
- **Remote Access:** Remote access to the organisation's network must be secured using a work device running Zscaler. Unauthorised remote access is strictly prohibited.
- **Systems and Cloud Services Administrative Access:** To maintain the highest level of security and integrity within our organisation, it is imperative that administrators use their administrator accounts exclusively when accessing critical systems and making changes to systems or programs. This practice ensures that all actions are properly logged and traceable, reducing the risk of unauthorised access and potential security breaches. By strictly adhering to this protocol, we can safeguard our systems, protect sensitive data, and maintain compliance with industry standards and regulations.

5.4. Data Classification and Protection

Data within the organisation is classified according to its sensitivity and value. Classification levels include Confidential, Restricted, and Public. Security controls are applied based on data classification, ensuring that sensitive information is encrypted, both in transit and at rest, and handled according to applicable regulations. Further details can be found in the Information Classification and Handling Standard.

5.5. Physical Security

It is important that access to infrastructure elements are restricted to only those individuals who require it; therefore, we have implemented the following measures:

- Access to data centres and critical facilities is restricted to authorised personnel only and is controlled using key cards, biometric systems, or equivalent measures.

Access requests should be submitted to Line Managers together with a detailed reason for approval and onward submission to the asset owner.

- Physical assets, including servers, computers, and mobile devices, must be secured and protected against theft, loss, or damage.

5.6. Network Security

To protect the integrity and security of our network Vercity Holdings has implemented the following:

- **Perimeter Security:** Firewalls and intrusion detection/prevention systems (IDPS) will be deployed to protect the organisation's network perimeter.
- **Network Segmentation:** Critical systems and sensitive data will be isolated on secure network segments.
- **Monitoring:** Network traffic is monitored continuously for suspicious activity. Logs will be maintained for a minimum period as defined by regulatory requirements.

5.7. Endpoint Security

All endpoints, including workstations, laptops, and mobile devices, will be equipped with:

- **Antivirus and Antimalware Software:** Regularly updated and configured to scan for malicious software.
- **Patch Management:** Security patches and updates must be applied promptly.
- **Device Management:** Mobile device management (MDM) and endpoint detection and response (EDR) solutions will be implemented to secure mobile and remote devices.

Users are not to interfere or alter any of the configuration settings applied to their corporate issued device.

5.8. Application Security

All applications used within the organisation must:

- Undergo security testing (e.g., vulnerability assessments, penetration testing) before deployment.
- Follow secure coding practices to prevent common vulnerabilities, such as SQL injection and cross-site scripting (XSS).
- Be regularly updated to mitigate identified vulnerabilities.
- Users are not to install any unapproved 3rd party software without prior approval from the ITC Manager.
- Users are not to use any unapproved Cloud Storage products without prior approvals from the ITC Manager.

5.9. Management of Cloud Services

Vercity Holdings recognises the critical role of cloud services in supporting its operations and enhancing flexibility and scalability. To ensure the secure use of cloud services, Vercity Holdings will evaluate and select cloud providers based on their adherence to industry-standard security certifications (such as ISO27017 and ISO/IEC 27018 for cloud security and privacy).

All data stored, processed, or transmitted through cloud services must be classified according to Vercity Holdings' data classification policy, with appropriate controls for

encryption, access, and data segregation. Only approved cloud services may be used, and access to these services will be managed by IT with appropriate authentication and authorisation controls, including multi-factor authentication where applicable. The organisation will periodically assess and monitor the security of cloud services to address emerging risks, ensure regulatory compliance, and verify adherence to contractual obligations.

All employees must follow guidelines for secure usage of cloud resources, including avoiding the use of personal cloud accounts for work-related data and reporting any unauthorised use or access of cloud systems.

5.9.1. Exiting Cloud Services

The Cloud Service Exit Process ensures a secure, efficient, and ISO/IEC 27001: 22 compliant transition from cloud services, covering contract termination, data retrieval, deletion, and migration. It involves defined roles such as a Cloud Exit Manager and Data Protection Officer, with steps including risk assessment, communication, secure data handling, and service migration. Post-exit activities focus on auditing, documenting processes, and continuous improvement while ensuring compliance with relevant regulations and maintaining business continuity.

Further details can be found in the Vercity Holdings Cloud Services Exit process document.

5.10. Corporate Asset Management

Vercity Holdings is committed to protecting its corporate assets, which include physical assets (such as computers, mobile devices, and facilities), information assets (such as data, intellectual property, and proprietary software), and digital resources (such as network infrastructure and cloud services). All laptops are encrypted without exception prior to being issued. All corporate assets will be tracked in accordance with the Vercity Asset Configuration Management Standard.

All employees and contractors have a duty of care to handle and use provided assets responsibly, ensuring their protection, confidentiality, and integrity. Asset Configuration Management Standard will be implemented to maintain an accurate inventory of all corporate assets, including the assignment of ownership, regular audits, and prompt updates for any changes in asset status.

Sensitive assets must be stored and secured according to their classification, and any transfer or disposal of assets must follow secure processes to prevent data leakage or unauthorised access. Employees are prohibited from using corporate assets for personal gain or activities outside the scope of their work. Violations of asset management guidelines will be subject to disciplinary action.

Through diligent asset management and duty of care Vercity Holdings aims to safeguard its resources, minimise risks, and ensure compliance with regulatory standards.

5.11. Bring Your Own Device (BYOD) Policy

Unless advised otherwise by an Executive Board member or the Vercity Digital Team, you should not use your personal Windows machines for work use. If you are having a problem with your work issued equipment, please contact Espria so this can be resolved.

It is acceptable to use personal mobile phones for work use, provided that the following security measures are implemented:

- The Microsoft In-Tune Portal app must be downloaded from the App / Google Play Store and installed. This creates a secure work partition on your phone, which is separate from rest of your phone. This ensures security without invading your privacy.
- Using In-Tune you must have Sophos installed.

You must also note that:

- Despite it being a personal device, relevant security software and security policies (including but not limited to this document) will be applied to the device prior to and / or upon connection to ensure security procedures and standards are maintained.
- The Company accepts no responsibility for the loss of personal data or information of personal devices connected to the System.
- The Company reserves the right to monitor any network traffic or applications used on this device for work purposes.

5.12. Data Storage

All corporate data should be saved in the appropriate SharePoint site. OneDrive is for personal work files, such as IPRs, training, work in progress etc. Sharing documents with colleagues should be done via SharePoint not OneDrive.

External storage devices such as USB sticks and external hard drives are blocked by default.

5.13. Data Backup and Recovery

Employees should not delete, destroy, or modify existing systems, programs, information, or data which could have the effect of harming Vercity or its business or exposing it to risk.

Users who create files on any computers other than the file server are responsible for ensuring that a current back up copy is available outside the primary location and for testing that copy. Regular data backups will be conducted to ensure data integrity and availability. Backups are stored securely and are tested periodically to ensure they can be restored in the event of a system failure, data loss, or cyber-attack.

5.14. Password Complexity Requirements

To protect access to Vercity Holdings' systems and sensitive information, all employees, contractors, and authorised users must adhere to the organisation's password complexity requirements. Password requirements are contained in the Password Standard.

Multi-factor authentication (MFA) is also mandated for access to sensitive systems or information. To further enhance security, storing passwords in plain text or sharing passwords with others is strictly prohibited. Password management software approved by Vercity Holdings may be used to store complex passwords securely. These requirements are designed to mitigate unauthorised access risks and enhance overall information security.

5.15. Security Awareness and Training

Vercity Holdings will provide regular security awareness training to all employees to ensure they understand the organisation's security policies, standards, procedures, guidelines and best practices. Training will include phishing awareness, password management, and incident reporting.

5.16. Privacy and Monitoring

No e-mail, voicemail or instant message sent or received through the internal system is private. We reserves the right to review, audit, intercept, access and disclose on a random basis all messages created, received, or sent over the e-mail or voicemail. Items so obtained by the business for monitoring may be disclosed without your permission. You should be aware that e-mails or voicemails, however confidential or damaging, may have to be disclosed in court or other proceedings. An e-mail, which has been deleted, can still be retrieved.

E-mail messages may be used as evidence in disciplinary proceedings, or for any other legitimate purpose as required.

Access to the e-mail system using someone else's password without prior authorisation from a Director may result in disciplinary action including, in appropriate circumstances, removal of access privileges or dismissal.

If you reasonably suspect a violation of this Policy, you should notify the Vercity Digital Team or your line manager immediately.

5.17. Employee Do's and Don'ts

These guidelines are intended to support all employees in protecting Vercity Holdings' information assets and ensuring compliance with the Digital Security Policy.

Do's

- **Use Strong Passwords**: Create strong, unique passwords for each system or application. Use a combination of uppercase letters, lowercase letters, numbers, and special characters.
- **Use a secure Password Manager** (ie 1Password, Microsoft Authenticator, Secret Server)
- **Enable Multi-Factor Authentication (MFA):** MFA is to be used for added security, especially on sensitive systems and applications.
- **Lock Your Devices:** Lock your computer, laptop, or mobile device when unattended to prevent unauthorised access.
- **Report Suspicious Activity:** Immediately report any suspicious emails, links, attachments, or activities to IT.
- **Use Authorised Software and Devices:** Only use software and devices approved by Vercity Holdings to access, store, or process organisational data.
- **Follow Data Classification Rules:** Handle information according to its classification level (Confidential, Restricted, or Public) and ensure that sensitive information is encrypted or handled securely.
- **Dispose of Sensitive Information Properly:** Shred or securely delete sensitive data before disposal, in accordance with data disposal policies.
- **Keep Software Updated:** Regularly install updates and patches on your devices to protect against vulnerabilities.
- **Participate in Security Training:** Attend all required security training sessions and complete any assigned security awareness modules.
- **Do follow the ITC Acceptable Use Standard:** This provides greater guidance on the acceptable use of company IT assets.
- **Do follow the Company Email Messaging Standard:** This provides guidance on the use of email and the expected email behaviours.

Don'ts

- **Don't Share Passwords:** Never share your passwords with others, even within the organisation. If someone needs access, follow the proper access request processes.
- **Don't Use Personal Devices for Work:** Avoid using personal devices for work purposes unless specifically authorised and configured by the Vercity Digital Team with appropriate security measures.
- **Don't Click on Suspicious Links or Attachments: Be** cautious of unexpected emails or messages with attachments or links, especially if they come from unknown or unexpected sources.
- **Don't Install Unauthorised Software:** Do not download or install software or applications that are not approved by the Vercity Digital Team. Unapproved software can pose security risks.
- **Don't Connect to Public Wi-Fi without Zscaler:** Avoid accessing sensitive information over public Wi-Fi networks. All work laptops and phones use Zscaler to ensure a secure connection from an untrusted network.
- **Don't Leave Sensitive Documents Unattended:** Avoid leaving printed sensitive information in open or unsecured areas. Store documents securely and lock them away when not in use.
- **Don't Alter and Security or Configuration Settings:** Do not interfere with any security or configuration settings on organisational devices or systems. Any modification must be approved and carried out by authorised personnel.
- **Don't Bypass Security Controls:** Do not attempt to disable or bypass security controls, such as antivirus software, firewalls, or access restrictions, for any reason.
- **Don't Forward Confidential Emails or Data:** Avoid forwarding internal emails, confidential documents, or sensitive data to personal or unauthorised accounts.
- **Don't Ignore Security Alerts:** If you receive a security alert, take it seriously. Promptly follow any instructions provided by IT or the Security team.
- **Don't Use Outdated or Unsupported Systems: Avoid** using outdated or unsupported systems, devices, or software that may not have security patches.

5.18. Incident Management

- **Incident Detection and Response:** The organisation has a documented incident response plan to detect, respond to, and recover from information security incidents.
- **Suspicious Activity:** Any suspicous or unusual activity is to be report immediately to gdpr@vercitygroup.com.
- **Incident Reporting:** All employees and contractors must report security incidents immediately to gdpr@vercitygroup.com.
- **Post-Incident Review:** All significant incidents will be analysed to identify root causes, and corrective actions will be taken to prevent recurrence.

5.19. Compliance and Audit

- Regular audits will be conducted to assess compliance with this Digital Security Policy and ISO/IEC 27001 requirements.
- Non-compliance will be reported to senior management, and corrective actions will be initiated promptly.

5.20. Exceptions

Any exceptions to this policy must be approved in writing by CDO or ITC Manager. Requests for exceptions must include a business case and associated risk assessment and also a mitigation plan.

5.21. Disciplinary Action

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

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
29/12/2025	02/01/2026	02/01/2026	02/01/2026

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

End.