

VCare

Policies & Procedures

Cyber Security Policy and Procedures v1.0

Introduction 4
Objective .....**Error! Bookmark not defined.**
Scope 4
Governance and responsibility.....4
Risk management 4
Data Protection Consent.....4
Security measures 4
Cybersecurity Awareness and Training 4
Incident response and reporting.....4
Compliance.....5
Third-Party and Vendor management.....5
Monitoring and enforcement 5
Policy Review and updates..... 5
Conclusion.....5

VCare Consultancy Services Ltd.

Cyber Security Policy and Procedure

Policy Lead	**Mrs. Tavleen Sharma (Registered Manager)**
Version No.	1.0
Date of issue	January 2025
Date to be reviewed	January 2026

Purpose and Introduction

The purpose of this Cyber Security Policy is to outline VCare's approach to securing our IT infrastructure, networks, data, and operations against cyber threats. As a UK-based company, we are committed to complying with all applicable regulations, including the UK's Data Protection Act 2018, the General Data Protection Regulation (GDPR), and other relevant cybersecurity frameworks to safeguard our information assets, protect sensitive data, and ensure continuity of operations.

Objective

The primary objective of this policy is to establish a framework to:

- Protect [Company Name]'s information and assets from cyber threats.
- Prevent unauthorized access, disclosure, alteration, or destruction of data.
- Ensure business continuity in the event of a cyber incident.
- Promote cybersecurity awareness among employees and stakeholders.

Scope

This policy applies to all employees, contractors, and third-party partners who access, manage, or process VCare Consultancy Services Limited's data, IT systems, and networks. It covers:

- Information assets (both digital and physical)
- Network infrastructure and data transmissions
- Employees' use of company devices and services
- Vendor and third-party access to company systems

Governance & Responsibility

- **CISO (Chief Information Security Officer):** The CISO is responsible for overseeing the cybersecurity program, ensuring compliance with laws and regulations, and providing guidance on cybersecurity risks.
- **IT Department:** The IT department is responsible for implementing, maintaining, and monitoring security controls on networks, systems, and devices.
- **Employees:** Every employee is responsible for understanding and following the cybersecurity policies, procedures, and best practices outlined by the company.

VCare Consultancy Services Ltd.

Risk Management

VCare will perform regular risk assessments to:

- Identify and evaluate cybersecurity threats and vulnerabilities.
- Implement risk mitigation strategies and controls based on the severity of identified risks.
- Continuously monitor the effectiveness of risk mitigation measures.

Data Protection

- **Data Classification:** Data will be classified into categories (e.g., confidential, internal, public) to determine the appropriate level of protection.
- **Encryption:** Sensitive data must be encrypted both at rest and in transit to protect it from unauthorized access.
- **Access Control:** Access to sensitive data and systems will be granted on a need-to-know basis, with role-based access control (RBAC) implemented to restrict access.
- **Data Retention and Disposal:** Data will be retained according to legal requirements and securely disposed of when no longer needed.

Security Measures

- **Network Security:** The company will implement firewalls, intrusion detection and prevention systems, and other security technologies to protect the corporate network.
- **Endpoint Security:** All devices (laptops, desktops, mobile devices) connected to the network will have antivirus software, device encryption, and security patches applied.
- **Multi-Factor Authentication (MFA):** MFA will be used for all critical systems and remote access to enhance login security.
- **Software Updates:** Regular patches and updates will be applied to all systems and applications to address vulnerabilities.
- **Backup and Recovery:** Regular data backups will be performed, and recovery procedures will be tested to ensure business continuity in case of a cyberattack or disaster.

Cybersecurity Awareness and Training

- All employees must complete mandatory cybersecurity training during onboarding and on an annual basis thereafter.
- Employees will be educated on recognizing and reporting phishing attempts, social engineering attacks, and other cybersecurity threats.
- Cybersecurity awareness will be promoted through internal communications, simulated phishing campaigns, and ongoing learning opportunities.

Incident response and reporting

- **Incident Response Plan:** The company will maintain an incident response plan to ensure a timely and effective response to cybersecurity incidents, including data breaches, system compromises, and malware infections.
- **Reporting:** Employees must immediately report suspected or actual cybersecurity incidents to the IT department or designated personnel. Incidents will be investigated, documented, and, if necessary, reported to relevant authorities, including the Information Commissioner's Office (ICO), in compliance with the GDPR.
- **Post-Incident Review:** After an incident, a review will be conducted to identify root causes, weaknesses in security controls, and areas for improvement.

VCare Consultancy Services Ltd.

Compliance

VCare Consultancy is committed to compliance with the following standards and regulations:

- UK Data Protection Act 2018.
- General Data Protection Regulation (GDPR).
- Network and Information Systems (NIS) Regulations.
- Cyber Essentials certification.
- ISO/IEC 27001:2013 (Information Security Management).

- Payment Card Industry Data Security Standard (PCI DSS), if applicable.

The company will regularly audit its systems and processes to ensure compliance with these regulations.

Third-Party and Vendor Management

- All third-party vendors with access to company systems or data will be subject to security reviews to ensure they meet [Company Name]'s security standards.
- Data-sharing agreements will include security clauses to protect the integrity and confidentiality of shared information.
- Regular assessments will be conducted to evaluate the cybersecurity practices of third-party vendors.

Monitoring and Enforcement

- The IT department will continuously monitor networks, systems, and user activities to detect and respond to security incidents.
- Violations of this policy will be taken seriously and may result in disciplinary action, up to and including termination of employment.

Policy Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in the cybersecurity landscape, regulatory requirements, or the company's operational needs.

Conclusion

Cybersecurity is a shared responsibility across the organization, and VCare Consultancy Services Limited is committed to providing a safe and secure environment for our employees, customers, and partners. By adhering to this policy, we aim to reduce the risks associated with cybersecurity threats and ensure the confidentiality, integrity, and availability of our information systems.

VCare Consultancy Services Ltd.