Client:	**Internal**
Document Title:	**Information Security Policy**
Viper Innovations Document No.	**5320-145036 – rev 02**
Customer Document No.	**N/A– rev N/A**
Date:	**16 April 2024**

Rev	Date	Description	Prepared	Checked	Reviewed	Approved
1	07/11/2023	First issue.	Steve Simpson	Russell Carleton	Deanna Bleakman	Edward Davies
2	16/04/2024	Update to Information Security Objectives (section 2) following ISO 27001 audit.	Steve Simpson	Russell Carleton	Jo Palmer	Edward Davies

TABLE OF CONTENTS

SECTION **PAGE**

1 INTRODUCTION

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Security of information held within the business, and consideration of how that information is obtained, stored, accessed, managed and disposed of, is critical to preserving the confidentiality, integrity and reputation of Viper Innovations.

Information may be put at risk by poor education and training and a breach of security controls. Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against the company. Therefore, it is essential for the business to develop and communicate a policy covering all relevant areas of information security.

1.1 PURPOSE

The purpose of this Information Security Policy is to establish a policy and procedures to ensure the confidentiality, integrity, and availability of all information assets within Viper Innovations.

1.2 SCOPE

This Policy and its supporting controls, processes and procedures apply to all information used and held within Viper Innovations, in all formats. This includes information processed by Viper on behalf of clients and other organisations in their dealings with Viper.

1.3 ROLES & RESPONSIBILITIES

The IT Manager is responsible for the contents and management of this policy document.

This policy applies to all employees, contractors and third-party vendors (Users) who have access to Viper's information assets and/or provide information processing services to Viper, including but not limited to computer systems, networks, data and facilities.

1.3.1 Management Responsibilities

The Viper Senior Management Team (SMT) shall demonstrate leadership and commitment to information security by providing the necessary resources, establishing policies and promoting a culture of security awareness.

1.3.2 Employee & User Responsibilities

All Viper employees and other Users shall be responsible for protecting the confidentiality, integrity and availability of information assets held within Viper Innovations. They must comply with the organization's information security policies and report any security incidents or vulnerabilities promptly. Refer to the "IT User Code of Conduct & Acceptable Use Policy" (5320-145037).

1.4 ACRONYMS, ABBREVIATIONS & DEFINITIONS

Asset: ISO 27001 defines an asset as any valuable location within an organisation's systems where sensitive information is stored, processed or accessible (e.g. a laptop, computer, phone, corporate network, etc).

CCTV: Closed Circuit Television

IAM: Information Asset Managers – delegated responsibility for day-to-day management of information within their assigned assets.

IAO: Information Asset Owners – overall accountability and ownership of information management within their assigned assets.

Information Asset: A collection of knowledge or data that is organized, managed and valuable (e.g. a paper document, a digital document, a database, a password or encryption key, Intellectual Property, etc).

IT: Information Technology

MFA: Multi-Factor Authentication

SMT: Senior Management Team

User/Users: All Viper employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties who have access to Viper’s Information Assets and/or provide information processing services to Viper, including but not limited to computer systems, networks, data and facilities.

1.5 RELATED DOCUMENTS

This policy document needs to be read and understood in the context of other policies and procedures constituting the Viper Innovations Management System, which can be found in SharePoint and Starjar. References to appropriate policies and procedures are contained within this document and are listed below:

5320-130114	Employee Handbook - Policies & Procedures
5320-130118	Risk Assessment Procedure
5320-133135	Supplier Approval Process and Approved Vendor List Management
5320-140545	Password and Authentication Policy
5320-145037	Information Technology User Code of Conduct & Acceptable Use Policy
5320-145216	CCTV Policy
5320-145273	Business Contingency and Continuity Plan
ISO 27001	Information security, cybersecurity and privacy protection — Information security management systems — Requirements

2 INFORMATION SECURITY OBJECTIVES

Viper's overall information security objective is to ensure appropriate availability, confidentiality and integrity of information and data is maintained at all times so as to protect business operations whilst enabling employees/other Users to perform their duties.

The following objectives have been identified to support this:

1. **Information risks** are to be identified, managed and treated according to an agreed risk tolerance – The Viper Innovations Information Security Risks matrices are located in Our Management System SharePoint site and are based on the Risk Assessment Procedure (5320-130118). Risks are reviewed by the IT Manager at least annually and the time between reviews will depend on the nature of the risk and the degree of change likely in the associated work activity.

2. **Manage and control access** to business systems to ensure sufficient permissions for Users to perform their roles whilst also ensuring security of information. Individual employee details are located in the Role-Permissions matrix in SharePoint which is managed by the IT Manager and HR team. Any changes to role permissions will be identified and requested through our IT service provider with the associated approval process.

3. **Reporting and legal obligations** relating to information security are met. The requirements are identified in the Legal and Other Requirements matrix. Reporting requirements are covered by the Information Security Incident and Reporting Process with cases logged in the Incident Investigation eLog in SharePoint.

4. **Awareness of company policies:** Individuals accessing our information are aware of their information security responsibilities. Information Security policies are published by the business and are accessible to User. Users are required to demonstrate their agreement to comply with the requirements by signing up to the policies in PeopleHR.

3 POLICY STATEMENT

It is Viper's policy to ensure that information is protected from a loss of:

- **Confidentiality –** information will be accessible only to authorised Users.
- **Integrity** – the accuracy and completeness of information will be maintained.
- **Availability** – information will be accessible to authorised Users and processes when required.

Viper will implement an information security management system compliant to the ISO 27001 international standard for information security. Viper will also reference other standards as required, mindful of the approaches adopted by its stakeholders.

Viper will adopt a risk-based approach to the application of controls.

3.1 INFORMATION SECURITY POLICIES

A set of lower level controls, processes and procedures for information security will be defined, in support of this high level Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the Viper SMT, published and communicated to Viper employees and other relevant parties. Refer to section 1.5 for a list of related documents.

3.2 ORGANISATION OF INFORMATION SECURITY

Viper will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within the company.

Viper Innovations will appoint:

- An **Information Security Team** to influence, oversee and promote the effective management of company information. The team will be coordinated by the IT Manager with support from the Chief Technology Manager and the QHSE Coordinator.
- An **Information Security Specialist** to manage the day-to-day information security function. The IT Manager will undertake this role.
- **Information Asset Owners (IAO)** to assume overall accountability and ownership of information management within their assigned assets.
- **Information Asset Managers (IAM)** with delegated responsibility for day-to-day management of information within their assigned assets.

3.3 HUMAN RESOURCES SECURITY

Viper’s security policies and expectations for acceptable use will be communicated to all Users to ensure that they understand their responsibilities. Mandatory information security education and training will be provided to all employees and poor and inappropriate behaviour will be addressed.

Where practical and appropriate, security responsibilities will be included in role descriptions, person specifications and personal development plans.

All Users shall be expected to adhere to the Viper “IT User Code of Conduct & Acceptable Use Policy” (5320-145037).

3.4 ASSET MANAGEMENT & OWNERSHIP

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance, access controls and protection of their assets to ensure the confidentiality, integrity and availability of the data.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity and classification will indicate appropriate handling requirements. They will also have a defined retention and disposal schedule.

3.5 ACCESS CONTROL

Access to all information will be controlled and will be driven by business requirements. Access will be granted, or arrangements made for Users according to their role and the classification of information, only to a level that will allow them to carry out their duties (i.e. based on the principle of least privilege).

Formal User registration and de-registration procedures will be maintained for access to all Viper information systems and services. This will include strong, mandatory authentication methods such as passwords and Multi-Factor Authentication (MFA) where possible.

Specific controls will be implemented for Users with elevated privileges to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

Customer accounts that are linked to Viper services (e.g. CableGuardian, PlatformVi, etc) will be managed to ensure information security is maintained in accordance with this policy. This includes removing accounts where Viper cannot verify the identity of the customer account holder or where the customer has not used the portal for a period of time but has retained a valid login.

3.6 PASSWORD MANAGEMENT

Passwords and passphrases shall meet the organization's password complexity requirements and are not to be shared, written down or stored in an insecure manner. Refer to the Viper “Password and Authentication Policy” (5320-140545).

3.7 CRYPTOGRAPHY & ENCRYPTION

Viper will provide guidance and tools to ensure proper and effective use of cryptography and encryption to protect the confidentiality, authenticity and integrity of information and systems.

3.8 PHYSICAL & ENVIRONMENTAL SECURITY

Information processing facilities are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

3.8.1 Physical Access Controls

Physical access controls, such as locks, access cards and surveillance systems, shall be implemented to protect facilities and equipment that house information assets.

3.8.2 Equipment & Hard Copy Disposal

Disposal of information assets, including storage media and devices, shall be carried out securely to prevent unauthorized access to sensitive information. Hard paper copies of documents that contain sensitive information are to be disposed of using the confidential waste bins located in the offices and be periodically taken away for cross shredding disposal.

3.9 OPERATIONS SECURITY

Viper will ensure the correct and secure operations of information processing systems.

This will include:

- Documented operating procedures.
- The use of formal change and capacity management.
- Controls against malware.
- Defined use of logging.
- Vulnerability management.

3.10 COMMUNICATIONS SECURITY

Viper will maintain network security controls to ensure the protection of information within its networks and provide the tools and guidance to ensure the secure transfer of information, both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

3.11 SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to mitigate any risks identified will be implemented where appropriate.

Systems development will be subject to change control and separation of test, development and operational environments.

3.12 SUPPLIER MANAGEMENT

Viper's information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

All new suppliers are subject to a review process before being added to the Viper Innovations Approved Vendors List (AVL). The review process is detailed in the "Supplier Approval Process and Approved Vendor List Management" procedure (5320-133135).

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

3.13 INFORMATION SECURITY INCIDENT MANAGEMENT

Guidance will be available on what constitutes an Information Security incident and how this should be reported (refer to the "IT User Code of Conduct & Acceptable Use Policy" (5320-145037).

Actual or suspected breaches of information security must be reported promptly to the IT Manager and/or the Viper SMT and will be investigated. Appropriate corrective actions will be taken and any learning built in to improve controls.

Viper shall establish and maintain an incident response plan that outlines the procedures for detecting, assessing, containing and recovering from security incidents. Refer to the "Business Contingency and Continuity Plan" (5320-145273) for details.

3.14 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Viper will have arrangements in place to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience.

Business continuity plans will be developed, maintained and tested in support of this policy.

Business impact analyses will be undertaken of the consequences of disasters, security failures, loss of service and lack of service availability.

Refer to the “Business Contingency and Continuity Plan” (5320-145273) for details.

4 AWARENESS & TRAINING

Employees shall receive appropriate information security training based on their job roles and responsibilities.

All Viper employees (and other Users, as appropriate) shall be made aware of this policy document and shall be expected to complete training and/or periodic reviews of its content, as and when requested. Following the training, employees shall be expected to electronically sign a personal declaration of compliance with the policy (e.g. in the online PeopleHR system).

5 COMPLIANCE

All Viper employees (and other Users, as appropriate) are expected to comply with Viper's information security policies, as well as all applicable laws, regulations, and contractual obligations. Failure to comply with this policy could result in action in line with the Viper Innovations Disciplinary Procedure, as detailed in the "Employee Handbook - Policies & Procedures" (5320-130114).

Employees (and other Users) shall be expected to promptly report any suspected violations of this policy to the Viper SMT.

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual obligations related to information security and privacy.

Viper Innovations will use a combination of internal and external audit to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures. Compliance with the controls in this policy will be monitored by the internal audit team and reported to the Viper SMT. This will include IT health checks, gap analyses against documented standards, internal checks on employee compliance and returns from Information Asset Owners (IAO).

6 REVIEW

The Viper SMT will undertake a review of this policy at least annually, or when significant changes occur, to ensure its continued relevance and effectiveness.