Security Management Policy

CASTOR VALI

Policy Statement

As a security and risk management provider, Castor Vali is committed to safeguarding its assets, information, employees, and operations against security threats and risks. This Security Management Policy outlines our approach to establishing, implementing, maintaining, and continuously improving our security posture to protect against unauthorised access, disclosure, alteration, destruction, or disruption.

Purpose

The purpose of this policy is to ensure a secure and resilient environment by managing risks associated with our physical and information assets. It aims to protect the integrity, confidentiality, and availability of information and to ensure the safety of all personnel and assets.

Scope

This policy applies to all employees, contractors, and third-party service providers of Castor Vali, encompassing all physical and digital assets, including data, information systems, networks, buildings, and equipment.

Objectives

Castor Vali's integrated management system provides the framework to ensure the delivery of these security management objectives:

- Setting and reviewing security objectives and targets designed to ensure continual improvement in its security performance.
- To identify and evaluate security risks and implement appropriate controls to mitigate them.
- To comply with all applicable legal, regulatory, and contractual security requirements.
- To foster a culture of security awareness and responsibility among all staff.
- To ensure that security measures are reviewed and updated in response to changes in the threat landscape or business operations.
- A risk management approach to business planning.

Roles and Responsibilities

- **Senior Management** is responsible for endorsing the Security Management Policy and providing the necessary resources for its implementation.
- The **Chief Operating Officer** is responsible for overseeing the development, implementation, and maintenance of the security management system.
- **Country Managers and Department Heads** are responsible for reviewing and implementing the policy within their respective areas and for ensuring their staff comply with security procedures.
- **All Employees** are responsible for adhering to security policies and procedures and for reporting any security incidents or vulnerabilities.

Risk Management

A risk management process has been established within the management system to identify, assess, and prioritise security risks. Appropriate controls will be implemented to mitigate identified risks to an acceptable level.

Access Control

Access to physical and information assets will be controlled and restricted based on the principle of least privilege. Access rights will be granted in accordance with job requirements and revoked promptly upon termination of employment or change in job role.

Physical Security

Physical security measures will be implemented to protect premises, assets, and personnel from unauthorised access, damage, or interference. This includes secure entry points, surveillance systems, and emergency response procedures. These measures will be reviewed and assessed periodically.

Information Security

Information security measures have been adopted to protect the confidentiality, integrity, and availability of data. This includes encryption, firewalls, anti-virus software, and secure data storage and transmission practices. Refer to our Information Security Policy for more details.

Incident Management

A procedure has been established for the reporting, investigation, and resolution of security incidents. Lessons learned from incidents will be used to strengthen security measures. Refer to the management system for more details.

Training and Awareness

Regular security training and awareness programs will be conducted to ensure that all employees are informed about security policies, threats, and their responsibilities in maintaining a secure environment.

Compliance and Audit

Regular audits and reviews will be conducted to ensure compliance with this policy, regulatory requirements, and industry best practices. Non-compliance issues will be addressed promptly.

Policy Review and Update

This policy will be reviewed annually or more frequently if significant changes occur in the threat landscape or business operations. Amendments will be made as necessary to ensure its continued effectiveness.

Policy approved by: **Steve Grant**
CEO
Castor Vali Group