**Vortex IQ Information Security Policy**

**1. Purpose**

The purpose of this Information Security Policy is to establish and maintain the confidentiality, integrity, and availability of Vortex IQ’s information assets and to protect the organisation, its customers, partners, and employees from information security risks.

**2. Scope**

This policy applies to all employees, contractors, partners, and third parties who access or manage Vortex IQ’s information systems, data, and infrastructure, including all physical and digital assets.

**3. Information Security Objectives**

* Protect information from unauthorised access, disclosure, alteration, and destruction.
* Ensure the confidentiality, integrity, and availability of all data processed or stored by Vortex IQ.
* Comply with applicable legal, regulatory, and contractual security requirements.
* Promote a culture of security awareness and responsibility.

**4. Roles and Responsibilities**

* **Information Security Officer (ISO):** Oversees the implementation, monitoring, and enforcement of security policies and procedures.
* **Employees and Contractors:** Responsible for complying with this policy and reporting any security incidents or vulnerabilities promptly.
* **IT Team:** Implements technical controls, monitors systems, and manages access rights.
* **Third Parties:** Must adhere to Vortex IQ’s security requirements through contractual agreements.

**5. Access Control**

* Access to systems and data is granted on a need-to-know and least privilege basis.
* Strong authentication mechanisms, including multi-factor authentication (MFA), are required for all remote and privileged access.
* User access rights are regularly reviewed and promptly revoked upon termination or role change.

**6. Data Protection**

* All sensitive and personal data must be encrypted in transit and at rest using industry-standard encryption protocols.
* Data backups are performed regularly and stored securely to enable recovery in case of data loss or corruption.
* Data retention and deletion practices comply with applicable regulations and contractual obligations.

**7. Network and System Security**

* Firewalls, intrusion detection/prevention systems, and secure network architecture are employed to protect systems.
* Regular vulnerability assessments and penetration tests are conducted to identify and remediate security weaknesses.
* Software and systems are kept up to date with security patches and updates.

**8. Incident Management**

* All security incidents and suspected breaches must be reported immediately to the Information Security Officer.
* An incident response plan is maintained and regularly tested to ensure timely containment, investigation, and resolution of incidents.
* Lessons learned from incidents are used to improve security measures continuously.

**9. Physical Security**

* Access to physical premises housing critical infrastructure is restricted and monitored.
* Visitors are required to sign in and be escorted while on premises.

**10. Employee Awareness and Training**

* All employees and contractors receive mandatory security awareness training upon onboarding and periodically thereafter.
* Training covers data protection, phishing awareness, secure password practices, and incident reporting.

**11. Compliance and Auditing**

* Compliance with this policy is monitored through regular internal audits and reviews.
* Non-compliance may result in disciplinary actions, up to and including termination.

**12. Policy Review**

This policy is reviewed at least annually or following significant changes to technology, business processes, or regulatory requirements.