# **Vortex IQ**

# **Corporate Security Policy**

**Effective Date:** 1 July 2023
**Approved by:** Senior Management Team

### **1. Purpose**

The purpose of this policy is to establish a framework for protecting Vortex IQ’s information assets, systems, and infrastructure from security threats, ensuring confidentiality, integrity, and availability. This policy supports our commitment to safeguarding client data, intellectual property, and company reputation.

### **2. Scope**

This policy applies to all employees, contractors, consultants, and temporary staff (collectively “staff”) who access or manage Vortex IQ’s systems, data, and physical premises.

### **3. Senior Management Commitment**

Senior management fully supports this policy and is committed to providing necessary resources and leadership to maintain a strong security posture.

### **4. Security Responsibilities**

* All staff must read, understand, and comply with this policy.
* Staff will acknowledge this policy during onboarding and annually thereafter.
* Security incidents or breaches must be reported immediately to the designated Security Officer.
* Access to systems and data is granted on a least-privilege basis and regularly reviewed.

### **5. Data Protection**

* Sensitive and personal data must be handled in compliance with applicable laws and company procedures.
* Data must be stored securely using encryption where appropriate.
* Data access is limited to authorised personnel only.

### **6. Access Control**

* Unique user credentials must be used; sharing of accounts is prohibited.
* Multi-factor authentication (MFA) is mandatory for access to critical systems.
* Passwords must meet complexity requirements and be changed regularly.

### **7. Physical Security**

* Access to company premises and data centres is controlled and monitored.
* Visitors must be authorised and accompanied at all times.

### **8. Acceptable Use**

* Company systems and devices must be used responsibly and primarily for business purposes.
* Staff must not install unapproved software or connect unauthorised devices.

### **9. Incident Management**

* All security incidents must be reported promptly following the Incident Response procedure.
* The company will investigate incidents and take corrective actions to prevent recurrence.

### **10. Training and Awareness**

* Security awareness training will be provided to all staff during onboarding and refreshed annually.
* Staff are responsible for maintaining their security knowledge and adhering to best practices.

### **11. Policy Compliance**

* Non-compliance with this policy may result in disciplinary action, up to and including termination.
* Regular audits and reviews will ensure compliance with this policy.

### **12. Policy Review**

This policy will be reviewed annually or as needed due to changes in regulatory, technical, or organisational conditions.