Cyber Security Policy

Tony Gee
Consulting Engineers

This Cyber Security Policy establishes the framework for protecting the digital assets, data, and information systems of Tony Gee. This policy applies to all employees, contractors, and third-party users who access the Company's IT systems. It covers all information assets, including data, software, systems, networks, and both fixed and portable devices.

All users with access to company information assets shall comply with the following measures, with the requirements of the company Data Protection Policy, and with the company Computer Equipment and Internet Acceptable use Policy:

Access Control

- User accounts shall only be assigned based on role-based access control (RBAC) and permissions reviewed when roles change and removed for inactive or leaving employees.
- Multi-factor authentication (MFA) shall be adopted wherever possible.
- Passwords and MFA secrets or codes must meet complexity requirements, must be unique to each individual and must never be shared.

Data Protection

- The company shall appoint a Data Protection Lead to advice the organisation regarding data protection law and data privacy matters, to monitor compliance, and liaise with regulators as required.
- All personnel handling data shall comply with the requirements of the Data Protection Policy and uphold the principles of the UK GDPR.
- Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.
- Company data shall not be stored on or transmitted by unapproved devices or systems (e.g. transmitted to personal email addresses).

Network System and Device Security

- The company shall implement firewalls and endpoint security solutions and users must not attempt to circumvent such systems.
- All software and hardware shall be updated regularly ensuring that vulnerabilities are addressed promptly, effectively preventing exploitation of known security issues. Patches for critical vulnerabilities shall be applied as soon as possible upon release.
- All remote connections to company internal systems shall be only from company-owned hardware with up-to-date endpoint protection, and all such connections shall use authorised VPN systems and be validated by MFA.
- Staff working from home shall comply with the security requirements of the ‘Home Working’ procedure.
- Staff shall not leave devices unattended in any public place.

Asset Management

- The company shall maintain an inventory of IT assets, including hardware and software.
- Unused or outdated assets shall be securely decommissioned and disposed of, including by physical destruction of data storage media.

Cyber Security Policy

Tony Gee
Consulting Engineers

Incident Response and Reporting

- All security incidents must be reported to IT immediately.
- Any incident that may constitute a data breach shall be reported to the company IT Director and Data Protection Lead for assessment and possible reporting to the ICO.

Training and Awareness

- The company shall carry out periodic cybersecurity awareness training and all staff shall complete mandated training promptly.
- The company may carry out covert testing of staff cyber security awareness (e.g. phishing campaigns) and staff shall cooperate with these tests.

Business Continuity and Disaster Recovery

- The company shall complete regular data backups which will be stored securely and tested for recovery periodically.
- A documented Business Continuity Plan shall be maintained.

Automatic technical controls may be implemented to assist users in complying with these controls, but where technical measures are not implemented users are responsible for complying with this policy.

Elements of this policy may be delegated to contractors or suppliers, but where this is done a written contract or statement of work shall be agreed defining responsibility for any elements of this policy so delegated.

Signed:

Alasdair Fowler
Chief Executive Officer

Reviewed Date: January 2025