Vandagraph Sensor Technologies
15 Station Road, Cross Hills, Keighley,
West Yorkshire BD20 7DT, UK
Tel +44 (0) 1535 634900 Fax +44 (0) 1535 635582
e-mail: info@vandagraphst.com www.vandagrapst.com

Vandagraph Sensor Technologies Ltd

Cyber Security Policy

Effective Date: 18 May 2026
Review Date: 18 May 2027
Approved By: Derek Lamb – Managing Director

---

1. Purpose

The purpose of this Cyber Security Policy is to define the measures and principles used by Vandagraph Sensor Technologies Ltd (VST) to protect company systems, business data, customer information, supplier information, and operational infrastructure from cyber security threats.

The company recognises that cyber security is an ongoing process involving technology, procedures, staff awareness, controlled access, monitoring, and continual improvement.

This policy supports:

- Business continuity
- Data protection obligations
- ISO 9001 and ISO 13485 management systems
- Supplier and NHS security expectations
- Protection against unauthorised access, malware, phishing, ransomware, and data loss

---

2. Scope

This policy applies to:

- All staff, directors, contractors, and authorised users
- Company servers, systems, and infrastructure
- Remote access systems
- Email systems and cloud services
- Internal business systems including Intrastats
- Company-owned and authorised remote devices used for company business

This policy covers both live and development environments.

---

15 Station Road, Cross Hills, Keighley,
West Yorkshire BD20 7DT, UK
Tel +44 (0) 1535 634900 Fax +44 (0) 1535 635582
e-mail: info@vandagraphst.com www.vandagrapst.com

3. Responsibilities

Managing Director

The Managing Director is responsible for:

- Overall cyber security oversight
- Approval of security policies
- Reviewing major cyber incidents
- Ensuring appropriate technical controls are maintained

System Administration

Authorised administrators are responsible for:

- Maintaining server security
- Applying updates and patches
- Managing backups and disaster recovery
- Managing access permissions
- Monitoring infrastructure and services

Staff Responsibilities

All staff are responsible for:

- Protecting passwords and login credentials
- Following company cyber security procedures
- Reporting suspicious emails or activity
- Maintaining reasonable security on devices used for company access
- Avoiding unauthorised software or unsafe practices

---

4. Access Control

The company operates a controlled-access model for all major systems.

Security controls include:

- Individual user accounts
- Centrally managed access permissions
- Role-based permissions where applicable
- Ability to revoke access immediately when required
- Restricted administrative access to servers and infrastructure

Access is granted only where required for legitimate business purposes.

15 Station Road, Cross Hills, Keighley,
West Yorkshire BD20 7DT, UK
Tel +44 (0) 1535 634900 Fax +44 (0) 1535 635582
e-mail: info@vandagraphst.com www.vandagrapst.com

Shared accounts are minimised where possible and restricted to approved operational requirements.

---

5. Passwords & Authentication

The company requires:

- Strong passwords for all critical systems
- Multi-factor authentication (MFA/2FA) on critical external services including financial and account systems
- Password confidentiality
- Immediate reporting of suspected credential compromise

Passwords must not be:

- Shared between users
- Reused across critical systems where avoidable
- Stored insecurely

---

6. Remote Access & Infrastructure Security

The company operates a self-hosted Linux-based infrastructure using supported Ubuntu LTS operating systems.

Security measures include:

- HTTPS encryption for externally accessible systems
- Reverse proxy architecture using NGINX
- Limited externally exposed services
- Restricted SSH administrative entry points
- Controlled administrator access
- Segregation between public-facing and internal systems where practical

Remote staff primarily access systems through secure browser-based interfaces rather than direct server access.

Direct exposure of unnecessary remote administration services is avoided.

---

7. Device & Endpoint Security

Staff using devices for company access are expected to:

- Keep systems updated

- Maintain antivirus/security protections where applicable
- Use supported operating systems where possible
- Avoid installing untrusted software
- Lock devices when unattended

The company primarily uses browser-based access systems, reducing local storage of company information on remote devices.

---

8. Backup & Disaster Recovery

The company maintains regular backup procedures to support business continuity and disaster recovery.

Current measures include:

- Local automated backups performed every four hours across the local network
- Daily offsite backup replication
- Daily restoration of backups to a remote cloned environment for validation purposes

This approach helps ensure:

- Backup integrity
- Disaster recovery readiness
- Operational resilience
- Recovery capability in the event of hardware failure, ransomware, or system compromise

Backup systems and restore capability are reviewed periodically.

---

9. Email & Phishing Protection

Company email accounts are protected using appropriate authentication and access controls.

Staff are expected to:

- Exercise caution with unexpected attachments or links
- Verify suspicious requests
- Report phishing attempts or unusual behaviour
- Avoid sharing sensitive information unless verified

Shared operational mailboxes are restricted to authorised personnel.

---

15 Station Road, Cross Hills, Keighley,
West Yorkshire BD20 7DT, UK
Tel +44 (0) 1535 634900 Fax +44 (0) 1535 635582
e-mail: info@vandagraphst.com www.vandagrapst.com

10. AI Usage & Data Protection

The company recognises that Artificial Intelligence (AI) technologies can provide operational benefits but also introduce risks.

The following principles apply:

- AI systems are used as assistance tools only
- AI-generated outputs must be verified by human users before reliance or implementation
- Confidential, customer-sensitive, regulated, or personal data must not be entered into unauthorised public AI systems
- Staff must consider GDPR, confidentiality, and commercial sensitivity before using AI systems

The company recognises that AI systems are probabilistic tools and may produce inaccurate or misleading outputs.

Final responsibility for decisions remains with authorised staff members.

---

11. Incident Response

Any suspected cyber security incident must be reported immediately to management or authorised system administrators.

Examples include:

- Suspected phishing emails
- Malware or ransomware activity
- Unauthorised access attempts
- Lost credentials
- Unusual system behaviour
- Data exposure concerns

Where necessary, systems may be:

- Isolated from networks
- Temporarily disabled
- Subject to password resets
- Investigated using backup and monitoring systems

Major incidents may be formally reviewed as part of the company corrective action and continual improvement processes.

---

15 Station Road, Cross Hills, Keighley,
West Yorkshire BD20 7DT, UK
Tel +44 (0) 1535 634900 Fax +44 (0) 1535 635582
e-mail: info@vandagraphst.com www.vandagrapst.com

12. Supplier & Cloud Services

The company uses a mixture of self-hosted infrastructure and externally managed service providers.

Reasonable efforts are made to:

- Use reputable providers
- Enable security protections such as MFA where available
- Limit unnecessary third-party access
- Review security implications of new services before implementation

---

13. Monitoring & Review

Cyber security is reviewed as part of ongoing management and operational review activities.

This includes consideration of:

- Infrastructure changes
- Backup performance
- Security incidents
- Access permissions
- Emerging risks
- Software updates and vulnerabilities

The policy shall be reviewed at least annually or following any major incident or infrastructure change.

---

14. Policy Compliance

Failure to comply with this policy may result in:

- Removal of system access
- Internal disciplinary action where appropriate
- Investigation of security breaches or misuse

All users are expected to cooperate with reasonable cyber security controls implemented by the company.

---

15. Continual Improvement

Vandagraph Sensor Technologies Ltd recognise that cyber security threats continue to evolve.

15 Station Road, Cross Hills, Keighley,
West Yorkshire BD20 7DT, UK
Tel +44 (0) 1535 634900 Fax +44 (0) 1535 635582
e-mail: info@vandagraphst.com www.vandagrapst.com

The company is committed to:

- Maintaining practical and proportionate security controls
- Improving cyber resilience over time
- Reviewing infrastructure and procedures regularly
- Supporting staff awareness and responsible system usage
- Protecting company operations, customer trust, and supplier relationships