VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

Viamed Ltd

Cyber Security Policy

Effective Date: 29 June 2026
Review Date: 29 June 2027
Approved By: Derek Lamb – Managing Director

---

1. Purpose

The purpose of this Cyber Security Policy is to establish the principles and controls used by Viamed Ltd to protect company information, customer information, supplier information, business systems and operational infrastructure from cyber security threats.

Cyber security forms an integral part of Viamed Ltd's Quality Management System, Business Continuity arrangements and Data Protection responsibilities.

Viamed recognises that cyber security is an ongoing process involving appropriate technology, secure working practices, staff awareness, risk management and continual improvement.

This policy supports:

- Protection against unauthorised access, malware, phishing, ransomware and data loss.
- Compliance with UK GDPR and Data Protection legislation.
- Business continuity and operational resilience.
- ISO 13485 and ISO 9001 Quality Management Systems.
- NHS, customer and supplier information security expectations.
- Continual improvement of cyber resilience across the organisation.

---

2. Scope

This policy applies to all employees, directors, contractors, temporary staff and authorised users who access or manage Viamed Ltd information, systems or services.

VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

The policy applies to all company-owned or authorised systems used in connection with company business, including:

- Business information and company records.
- Customer, supplier and employee information.
- Company servers, infrastructure and network services.
- Internal business systems, including Intrastats.
- Email systems, cloud services and approved third-party platforms.
- Desktop computers, laptops, mobile devices and authorised remote access devices.
- Remote and home working arrangements where company information or systems are accessed.
- Artificial Intelligence (AI) systems used for company business, where authorised by the company.

This policy applies equally to live, development and test environments where company information or systems are processed or maintained.

---

3. Responsibilities

Managing Director

The Managing Director has overall responsibility for cyber security governance and ensuring that appropriate policies, procedures and resources are in place to protect the company's information and business systems.

Responsibilities include:

- Overall cyber security oversight.
- Approval of cyber security policies and associated procedures.
- Ensuring appropriate technical and organisational controls are maintained.
- Reviewing significant cyber security incidents and corrective actions.
- Supporting continual improvement of cyber resilience.

System Administration

VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

Authorised system administrators are responsible for:

- Maintaining the security of company infrastructure.
- Applying appropriate software updates and security patches.
- Managing backups and disaster recovery arrangements.
- Managing user accounts and access permissions.
- Monitoring systems and services for security and operational performance.

Staff Responsibilities

All staff share responsibility for maintaining cyber security.

Employees are expected to:

- Protect passwords and authentication credentials.
- Follow company cyber security policies and procedures.
- Report suspicious emails, cyber incidents or security concerns immediately.
- Exercise reasonable care when using company systems and devices.
- Protect company, customer and supplier information.
- Avoid unauthorised software, unsafe practices or actions that may compromise security.
- Participate in cyber security awareness and training where required.

---

4. Access Control

Viamed Ltd operates a controlled access model to ensure that company systems and information are only accessible by authorised users for legitimate business purposes.

Security controls include:

- Individual user accounts.
- Centrally managed access permissions.
- Role-based access controls where appropriate.
- Restricted administrative privileges.
- Immediate removal or amendment of access when no longer required.

VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

- Regular review of user access permissions.

Access is granted on the principle of least privilege, ensuring users receive only the level of access necessary to perform their authorised duties.

Shared accounts are avoided wherever practical and are only permitted where operationally necessary and subject to appropriate controls.

---

5. Passwords & Authentication

Viamed Ltd requires appropriate authentication controls to protect company information and systems.

These include:

- Strong, unique passwords for all critical systems.
- Multi-factor authentication (MFA) on appropriate externally accessible services, including financial and business-critical systems.
- Protection of authentication credentials.
- Immediate reporting of suspected credential compromise.
- Prompt removal or amendment of user access where responsibilities change.

Passwords and authentication credentials must not be:

- Shared between users.
- Reused across critical systems where reasonably avoidable.
- Stored insecurely or disclosed to unauthorised persons.

---

6. Remote Access & Infrastructure Security

Viamed Ltd maintains secure information technology infrastructure designed to protect company systems, information and business operations from unauthorised access, disruption and cyber security threats.

Appropriate technical and organisational controls are implemented to support the confidentiality, integrity and availability of company information.

VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

Security measures include, where appropriate:

- Securely managed operating systems and network infrastructure.
- Firewalls and network security controls.
- Encryption of data during transmission where appropriate.
- Secure remote access for authorised users.
- Controlled administrative access to critical systems.
- Regular software updates and security patch management.
- Malware protection and endpoint security.
- System logging and monitoring to assist with the identification of potential security incidents.
- Network segmentation and access controls where appropriate to reduce cyber security risk.

Company infrastructure is regularly reviewed and maintained to support business continuity, operational resilience and the protection of company, customer and supplier information.

---

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.

Backup and restoration capability is periodically tested to verify the integrity and recoverability of company data and systems.

---

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.

---

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
- AI systems shall not be used to make autonomous business decisions without appropriate human review and authorisation.

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.

---

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

VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

- 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
- Review of user access permissions.
- Review of backup testing.
- Review of cyber security awareness.
- Review of emerging cyber threats.
-

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

This policy shall be reviewed at least annually, and following any significant cyber security incident, infrastructure change, legislative change or organisational 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.

VIAMED Ltd.
15 Station Road, Cross Hills, Keighley, West Yorkshire, BD20 7DT, UK.
Website: www.viamed.co.uk. Email: info@viamed.co.uk.
Tel: +44 (0)1535 634542. Fax: +44 (0)1535 635582.

15. Continual Improvement

Viamed Ltd recognises that cyber security threats continue to evolve and that maintaining effective cyber security requires continual review and improvement.

The company is committed to:

- Maintaining practical, proportionate and risk-based security controls.
- Continually improving cyber resilience and business continuity.
- Monitoring emerging cyber threats and industry best practice.
- Reviewing infrastructure, procedures and access controls regularly.
- Supporting staff awareness through training and communication.
- Protecting company, customer and supplier information.
- Supporting the requirements of ISO 13485, UK GDPR and applicable legal obligations.