

Freeway Medical Information Security Policy and Process Overview Document 2026-27

COMMITMENT TO DATA PROTECTION & CONFIDENTIALITY

Freeway Medical - Chromis UK Limited is dedicated to protecting the confidentiality, integrity, and availability of all data it handles. This policy outlines our information security processes, particularly focusing on the handling of third-party customer data, which includes account manager information, payment information for credits, and business communication data..



Freeway Medical Information Security Policy and Process

Overview Document 2026-27

Purpose and Scope

This policy sets out the information security controls used by Freeway Medical / Freeway Med-Tech, trading names of Chromis UK Ltd. It applies to employees, contractors and relevant third parties and covers business information and personal data throughout storage, processing, transmission and disposal.

Information Security Objectives

Confidentiality: information is accessible only to authorised persons. Integrity: information remains accurate, complete and protected from unauthorised change. Availability: information and systems remain available to authorised users when required.

Data and Asset Management

Information and systems should be identified, handled according to sensitivity and business need, and retained only for as long as required. Personal data is subject to the principles of data minimisation, storage limitation and appropriate security.

Access Control

Access is granted on a least-privilege and business-need basis. User accounts must be individual, reviewed when roles change and removed promptly when no longer required. Strong authentication, including multi-factor authentication where required by company controls or risk, must be used.

Secure Configuration and Updates

Company devices, software, network equipment and cloud services must be securely configured. Supported software must be maintained and security updates or vulnerability fixes applied in accordance with company procedures and risk.

Encryption and Secure Handling

Appropriate encryption and secure protocols are used to protect sensitive information at rest and in transit according to risk. Portable devices and removable media must be appropriately controlled. Sensitive information must not be transferred through unapproved channels.

People and Awareness

Employees must complete relevant security and data-protection awareness activities and remain alert to phishing, social engineering and other threats. Suspected compromise, loss or unauthorised disclosure must be reported immediately.

Cyber Security Controls

Chromis UK Ltd maintains proportionate technical and organisational controls, including firewalls, secure configuration, security update management, user access control and malware protection. Controls are reviewed as technology and risk change.

Backups and Resilience

Business-critical information is backed up using appropriate solutions. Backup arrangements are protected from unauthorised access and should be capable of supporting recovery following accidental loss, system failure or cyber incident. Recovery arrangements are tested or reviewed periodically.

Third Parties and Cloud Services

Suppliers and service providers that process or host company or personal data must be subject to proportionate security and data-protection due diligence. Contracts and access arrangements should reflect the sensitivity of the information and applicable legal obligations.

Incident Response and Personal Data Breaches

Security incidents must be reported immediately to ITsupport@freewaymedical.co.uk. Incidents will be contained, investigated, documented and assessed for legal or contractual notification requirements. Where a personal data breach is notifiable under UK data-protection law, notification to the ICO will be made without undue delay and, where feasible, within 72 hours of awareness.

Monitoring and Review

Security controls, access and relevant system events are monitored or reviewed proportionately to risk. Periodic audits and management review are used to identify improvements. This policy will be reviewed at least annually and following significant security, legal, organisational or technology changes.

Roles and Responsibilities

Management is accountable for ensuring proportionate information-security arrangements. IT is responsible for technical security administration and incident coordination. All users are responsible for following this policy, protecting credentials and promptly reporting security concerns.

Legal and Framework Alignment

The company applies the security principle and accountability requirements of UK data-protection law and maintains its information-security arrangements with reference to current UK cyber-security good practice and its applicable Cyber Essentials controls.

10. Contact Information

Contact Information

For questions, security concerns or to report an incident, contact the IT department at ITsupport@freewaymedical.co.uk.

Policy Approval and Acknowledgment

This Information Security Policy is approved by the management of Chromis UK Ltd. Employees and relevant associates are required to understand and comply with the controls and responsibilities applicable to their role.

Review Status

Policy reviewed: 28 September 2026

Next review: September 2027, or earlier following a significant incident or material change in legal, organisational, technical or cyber-security requirements.

Signed on behalf of Freeway Medical / Freeway Med-Tech - trading names of Chromis UK Ltd.



Director / authorised signatory

RENEWED 2026-27