smartclinic

CYBER SECURITY POLICY

July 2024 – V3

Introduction

At Smart Clinic, safeguarding the confidentiality, integrity, and availability of our digital assets, client information, and operational systems is of paramount importance. This Cyber Security Policy outlines our commitment to protecting against cyber threats and ensuring the secure handling of all digital and information assets within our organisation.

This policy serves as an overarching framework that encompasses a range of sub-policies related to information security, cyber security, and digital data protection. These include, but are not limited to, access control, data encryption, incident response, and acceptable use policies. Together, they form a comprehensive approach to maintaining the security and resilience of our digital environment.

The designated *Responsible Person* for the implementation, maintenance, and monitoring of this policy is Harry Cramer, who is accountable for ensuring compliance across all levels of the organisation.

To maintain its relevance and effectiveness, this policy is reviewed on an annual basis in accordance with Smart Clinic’s Document Control Matrix. Updates may also be made on an ad-hoc basis to reflect emerging threats, regulatory changes, or organisational developments.

By adhering to this policy, all employees, contractors, and third-party service providers contribute to creating a secure, compliant, and trustworthy environment for our clients and stakeholders.

Contents

Section 1 – Information security

Information classification policy

Purpose

The purpose of this Information Classification Policy is to establish a framework for classifying and handling information based on its level of sensitivity, value, and criticality to Smart Clinic. As an occupational health provider, we process a wide range of information, including highly sensitive personal and medical data. Proper classification and handling are essential to comply with legal obligations and to protect the rights and privacy of our clients, employees, and partners.

Scope

This policy applies to all Smart Clinic employees, contractors, temporary staff, and third-party service providers who access, process, or manage information in any format (electronic, paper, or verbal).

Information Classification Levels

All information can be classified into one of the following categories:

- **Confidential**
  Information that is highly sensitive and restricted to authorised personnel. This includes personal health data, medical records, employee files, and other data protected under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
  Examples: Patient health records, staff disciplinary files, incident investigation reports.

- **Internal Use Only**
  Information intended for internal operational use that does not fall under the 'Confidential' classification but should not be disclosed publicly.
  Examples: Internal memos, internal audit reports, operational procedures.

- **Public**
  Information that is approved for public release and presents no risk to Smart Clinic if disclosed.
  Examples: Marketing materials, published policies, website content.

Data Handling Procedures

To protect information in accordance with its classification, the following handling guidelines apply:

a. Confidential Information

- Must be encrypted in transit and at rest.
- Access restricted to authorised personnel only.
- Physical copies must be stored in locked cabinets in secure areas.
- Must not be shared via unsecured channels (e.g. personal email, USB drives).
- Disposal must be carried out securely (e.g. shredding for paper documents, secure wiping of digital media).

b. Internal Use Only

- May be shared within the organisation as required for business purposes.
- Should be stored on secure, access-controlled systems.

- Disposal should follow standard secure deletion procedures.

c. Public

- Must be reviewed and approved by relevant authority before publication.
- No special handling or protection required after approval.

Roles and Responsibilities

- **All Employees:** Must understand and apply the appropriate classification and handling procedures for the information they access.
- **Managers:** Are responsible for ensuring staff are aware of this policy and receive appropriate training.
- **Information Governance Lead:** Oversees the classification framework, monitors compliance, and updates the policy as required.

Compliance with UK Legislation

Smart Clinic adheres to all relevant legislation including, but not limited to:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Computer Misuse Act 1990**

Failure to comply with this policy may result in disciplinary action and/or legal consequences.

By understanding and implementing this Information Classification Policy, Smart Clinic employees and partners help ensure the confidentiality, integrity, and availability of information, protecting both individuals and the organisation.

Automatic logout statement

To maintain the security and integrity of our digital systems and protect sensitive personal and medical data, Smart Clinic enforces an automatic logout policy for all internal and external system users.

All users will be automatically logged out after **60 minutes of inactivity**. This applies to staff, contractors, and external partners accessing Smart Clinic's systems, whether working on-site or remotely. The purpose of this policy is to reduce the risk of unauthorised access to information, particularly in cases where a device or session is left unattended.

Inactivity is defined as a lack of interaction with the system, including keyboard, mouse, or touchscreen input. After 60 minutes of inactivity, the session will be terminated, requiring the user to log in again to resume work.

This policy aligns with our broader information security measures and supports compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, ensuring appropriate technical controls are in place to safeguard personal and health-related data.

Exceptions to this policy are rare and must be approved by the Information Governance Lead in consultation with IT and security teams. Any such exceptions must be documented and subject to risk assessment.

All users are expected to take responsibility for protecting their sessions and are encouraged to manually log out if they are stepping away from their device.

Encryption

At Smart Clinic, the confidentiality, integrity, and security of client and patient data are of the highest priority. To protect sensitive information from unauthorised access, tampering, or loss, we implement robust encryption measures in line with current industry best practices and applicable UK legislation.

All client and patient data—whether stored (at rest) or transmitted (in transit)—is encrypted using appropriate cryptographic standards, such as AES-256 for data at rest and TLS 1.2 or higher for data in transit. These encryption protocols are widely recognised for their strength and reliability in safeguarding sensitive health and personal information.

This encryption policy applies across all Smart Clinic systems, including electronic health record platforms, cloud services, mobile devices, backup storage, and internal communication tools. Encryption is a mandatory control and a key component of our broader data protection and cyber security framework.

Our approach aligns with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which mandate appropriate technical measures to ensure the security of personal data. Encryption also supports our compliance with the NHS Data Security and Protection Toolkit where applicable.

Regular audits and technical reviews are carried out to ensure encryption standards remain up to date and effective. Any changes in technology or legal requirements will prompt a review of our encryption practices to ensure ongoing compliance and security.

By enforcing strong encryption standards, Smart Clinic ensures that sensitive client and patient information is protected at all stages of its lifecycle.

Data destruction

Smart Clinic is committed to ensuring that all personal, medical, and operational data is retained only for as long as necessary and is securely destroyed once it reaches the end of its defined retention period, as set out in our Data Policy and in accordance with relevant UK legislation.

When data reaches the end of its retention schedule, it is destroyed using secure and irreversible methods to prevent any risk of unauthorised access, data breaches, or misuse. The method of destruction depends on the format of the data:

- Digital Data is permanently deleted using certified data-wiping tools that comply with recognised standards, such as NIST 800-88 or equivalent. Where data is stored on physical media (e.g. hard drives, USBs), the devices are either securely wiped or physically destroyed (e.g. degaussed or shredded).

- Paper Records containing personal or sensitive information are destroyed using cross-cut shredding or are disposed of via a trusted and GDPR-compliant confidential waste disposal service, which provides certification of secure destruction.

These processes are carried out by authorised personnel only, in line with our access control and data handling procedures.

Our data destruction practices support compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which require organisations to ensure that personal data is not kept longer than necessary and is disposed of securely.

Destruction of data is documented where required, and routine audits are conducted to verify compliance with retention and disposal requirements. Through these measures, Smart Clinic ensures the secure and responsible handling of data throughout its lifecycle.

Unauthorised transfer of data

Smart Clinic is committed to protecting client, patient, and organisational data from unauthorised access, disclosure, or loss. To ensure data security we have strict controls in place to prevent the unauthorised transfer of data via email, web browsers, or other transfer mechanisms.

Unauthorised Data Transfer Controls

All data transfers must be authorised, secure, and necessary for legitimate business purposes. To prevent accidental or intentional unauthorised transmission:

- **Email systems** are configured to prevent the sending of sensitive data to unauthorised recipients. Encryption is enforced for emails containing confidential or personal information.
- **Web browsers** are monitored and restricted to prevent uploading or downloading of sensitive data to unauthorised platforms or cloud services.
- **Removable media and file-sharing platforms** are restricted or disabled by default. Any exceptions require formal approval and are subject to audit.
- Staff must not use personal email accounts or unauthorised messaging platforms to transmit company data.

Data Loss Prevention (DLP) Controls

Smart Clinic employs technical controls, including Data Loss Prevention (DLP) tools, to monitor and block the movement of sensitive data across networks, devices, and applications. These tools:

- Detect and prevent the sharing of confidential data outside authorised channels.
- Alert administrators to suspicious or non-compliant behaviour.
- Automatically apply policies based on data classification levels.

All employees are trained in data handling protocols and are required to report any suspected data loss or unauthorised transfer immediately. Regular audits and policy reviews ensure these controls remain effective and responsive to emerging threats.

By implementing these safeguards, Smart Clinic reinforces its commitment to maintaining data security and upholding the trust of our clients and patients.

Security Patching

Smart Clinic recognises the critical importance of maintaining up-to-date security across all IT assets to protect against vulnerabilities and cyber threats. To ensure the integrity and resilience of our systems, we follow a proactive approach to regular security patching for all hardware and software components.

This includes:

- Endpoint devices (e.g. laptops, desktops, mobile devices)
- Servers (on-premises and cloud-based)
- Network infrastructure (e.g. firewalls, switches, routers)
- Business applications and software platforms

Security patches and updates are applied in line with vendor recommendations and release schedules. Where feasible, patches are tested in a controlled environment before deployment to minimise disruption and ensure compatibility with existing systems.

Critical security patches are prioritised and applied as quickly as possible, typically within defined timeframes set by our internal risk management protocols. Automated patch management tools are used where appropriate to streamline deployment, track compliance, and ensure consistent coverage across the organisation.

Devices or systems that are no longer supported by vendors are reviewed regularly and either upgraded, isolated, or decommissioned in a timely manner to prevent exposure to unpatched vulnerabilities.

Regular audits and vulnerability scans are conducted to identify missed updates and ensure adherence to patching policies. Any deviations or delays are documented and addressed through risk-based decision-making and remediation plans.

Through timely and consistent patch management, Smart Clinic reduces the risk of security incidents and ensures our systems remain protected against evolving threats.

Penetration testing

At Smart Clinic, we are committed to proactively identifying and addressing security vulnerabilities within our digital infrastructure. As part of our cyber security strategy, we conduct annual penetration testing to evaluate the resilience of our systems against real-world cyber threats.

Penetration testing is performed by qualified, independent professionals who simulate attacks on our network, applications, and systems to uncover potential weaknesses. This includes external and internal testing across critical assets such as servers, web applications, endpoints, and network devices.

All identified vulnerabilities are categorised based on risk level (e.g. critical, high, medium, low) and are addressed promptly in accordance with our internal remediation timelines.

- Critical and high-risk vulnerabilities are prioritised and resolved as a matter of urgency.
- Medium and low-risk findings are tracked and resolved in line with operational priorities and business impact.

Each test results in a formal report, which is reviewed by our Information Security and IT teams. Findings are documented, and remediation actions are monitored to ensure completion. Where necessary, retesting is conducted to verify that vulnerabilities have been effectively mitigated.

Penetration testing supports our commitment to continuous improvement and helps ensure the ongoing security of client and patient data, as well as the reliability of our services.

Section 2 – Code and system development

Change management

Smart Clinic maintains a structured change management process to ensure that all modifications to our IT systems, applications, and infrastructure are carried out in a controlled, secure, and reliable manner.

All proposed changes—whether routine, emergency, or major—are subject to formal review and approval. This process includes a thorough information security assessment to evaluate potential risks to data confidentiality, integrity, and system availability.

As part of the change process, an impact assessment is conducted to determine the effect on users, services, compliance, and business operations. This includes reviewing dependencies, security implications, and potential disruptions.

To protect service continuity and minimise risk, every change plan must include a rollback procedure. This ensures that, in the event of an unsuccessful or disruptive change, systems can be quickly restored to their previous stable state without compromising data or operational integrity.

All changes are logged, reviewed by relevant stakeholders, and tested in controlled environments where feasible before deployment. Post-implementation reviews are carried out to confirm success and identify lessons learned.

Through this controlled approach, Smart Clinic ensures that system changes support business objectives while maintaining high standards of security and reliability.

Auto-run

Smart Clinic confirms that Auto-Run functionality has been disabled on all Windows-based systems across the organisation. This security measure is in place to prevent the automatic execution of files from external media such as USB drives, CDs, and DVDs, which could introduce malware or unauthorised software into our environment.

Disabling Auto-Run reduces the risk of infection from removable media and forms part of our broader endpoint security strategy. Where systems or devices do not support Auto-Run, this control is not applicable but remains monitored to ensure ongoing compliance with our security standards.

This configuration is enforced through centrally managed group policies and verified as part of routine security audits.

Source code access

Smart Clinic maintains strict controls over access to all program source code to protect the integrity, confidentiality, and security of our software and digital services.

All source code is stored in a secure code repository, which is protected by robust access controls. Access is granted on a least privilege basis, meaning only authorised personnel with a legitimate business need can access or modify the code. Role-based permissions are applied to ensure developers, reviewers, and administrators have only the access necessary for their responsibilities.

Multi-factor authentication (MFA) is enforced for all users accessing the repository, and all access is logged and audited. The system maintains a complete audit trail of all access, changes, and activities, allowing for full traceability of who accessed or modified code and when.

Regular reviews of access rights are conducted to ensure permissions remain appropriate and to revoke access when no longer required. All changes to the codebase follow a defined version control and peer review process to ensure accuracy, accountability, and security.

These measures help ensure the integrity of our software development processes and reduce the risk of unauthorised changes or insider threats.

Software development lifecycle

Smart Clinic follows a defined Software Development Life Cycle (SDLC) process that incorporates security at every stage to ensure the development of secure, reliable, and compliant software solutions.

Our SDLC includes the following key phases: planning, requirements gathering, design, development, testing, deployment, and maintenance. At each phase, security input is integrated to identify and mitigate potential risks early in the development process.

- During the planning and requirements phases, security requirements are captured alongside functional needs to ensure compliance with internal policies and industry best practices.
- In the design phase, threat modelling and risk assessments are performed to identify vulnerabilities and define secure architectures.
- Throughout development, secure coding practices are followed, and developers are trained in common vulnerabilities (e.g. OWASP Top 10) to reduce the risk of introducing security flaws.
- In the testing phase, code undergoes static and dynamic analysis, as well as security-specific testing such as vulnerability scanning and penetration testing, where appropriate.
- During deployment, configurations are reviewed to ensure systems are securely set up and hardened before release.
- Ongoing maintenance includes monitoring, patching, and incident response processes to address emerging threats or discovered vulnerabilities.

Security reviews and approvals are required at key decision points, and any identified risks must be resolved or formally accepted before moving to the next phase.

By embedding security throughout the SDLC, Smart Clinic ensures that our software is developed in a secure, compliant, and resilient manner, reducing risk and protecting the data and trust of our clients and patients.

Coding best practices

At Smart Clinic, we are committed to developing secure, reliable, and high-quality applications and systems that protect the confidentiality, integrity, and availability of data. To achieve this, we follow industry-recognised security best practices throughout the development lifecycle.

Our secure development practices include:

- Secure Coding Standards: All developers adhere to secure coding guidelines to prevent common vulnerabilities such as injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and insecure deserialization. We reference established frameworks such as the OWASP Top 10 and CWE/SANS Top 25.
- Code Reviews and Peer Validation: All code changes are subject to peer review to ensure quality, functionality, and security. Reviews focus on detecting security flaws, coding errors, and adherence to standards.
- Access Control and Authentication: Applications are built with strong authentication mechanisms (e.g. multi-factor authentication where applicable) and role-based access controls to ensure only authorised users can access sensitive functions or data.
- Data Protection: Sensitive data is protected using encryption in transit and at rest. Input validation, output encoding, and secure session handling are implemented to prevent data leakage or manipulation.
- Environment Separation: Development, testing, and production environments are separated to prevent cross-environment risks. Test data is anonymised or synthetically generated to avoid exposing real client or patient information.
- Security Testing: Applications undergo regular security testing, including static and dynamic analysis, dependency scanning, and where appropriate, penetration testing.
- Dependency Management: Third-party libraries and components are regularly reviewed and kept up to date to avoid known vulnerabilities.
- Developer Training: Development staff receive ongoing training on secure development techniques and emerging threats to stay current with best practices.

By embedding these security measures into our development processes, Smart Clinic ensures that all applications and systems meet the highest standards for security and resilience.

Data validation

Smart Clinic implements strict data validation controls to ensure that all inputs to and outputs from our applications are secure, accurate, and consistent with expected formats. These measures are critical in preventing common security vulnerabilities and ensuring the reliability of our systems.

All data inputs—whether from users, third-party systems, or internal sources—are validated against predefined rules to verify their type, format, length, and value range. This helps prevent injection attacks (such as SQL or command injection), buffer overflows, and other forms of malicious data entry. Input validation is enforced on both the client and server sides to ensure defence in depth.

For data outputs, we apply appropriate sanitisation and encoding techniques to prevent the unintentional exposure of sensitive data and to protect against cross-site scripting (XSS) and other output-based vulnerabilities. This ensures that only authorised and correctly formatted data is presented to users or passed to external systems.

Validation logic is consistently implemented across all applications and reviewed regularly as part of our secure software development process. Automated testing tools are used where appropriate to identify and correct any weaknesses in input/output handling.

By enforcing rigorous validation of data inputs and outputs, Smart Clinic enhances the integrity, security, and stability of our digital services, helping to protect our users, systems, and the sensitive information we manage.

Environment segregation

Smart Clinic enforces strict segregation between development, testing (staging), and production environments to ensure the integrity, confidentiality, and stability of our systems and data.

Each environment is logically and physically separated, with dedicated infrastructure, access controls, and user permissions. This separation ensures that activities carried out in development and testing do not impact the performance or security of live production systems.

Only authorised personnel are granted access to each environment based on their role and responsibilities. Developers and testers do not have direct access to production systems, and any changes to production are deployed through a controlled and audited change management process.

Segregating these environments reduces the risk of data leaks, configuration errors, and system downtime, and is a core part of our secure software development and operational practices.

Smart Clinic follows a formal and structured multi-environment testing process to ensure the quality, security, and reliability of all software developments before they are deployed to live systems.

1. **Development Environment**
   In this initial environment, developers build and test new features, enhancements, or bug fixes. Unit tests and basic integration checks are performed here to verify core functionality. Developers use version control systems and peer review practices to maintain code quality and collaboration.

2. **Staging Environment**
   Once development work is complete, code is promoted to the staging environment, which closely replicates the live production setup. Comprehensive testing takes place here, including functional testing, regression testing, load/performance testing, and security assessments. This stage ensures that the application behaves as expected under realistic conditions.

3. **Production Environment**
   Following successful validation and sign-off in staging, changes are carefully deployed to the live production environment during scheduled maintenance windows. Deployment follows a formal change management process, including risk assessment, documented rollback plans, and post-deployment monitoring.

This layered approach ensures any issues are identified early, and only thoroughly tested and approved changes reach the live environment, reducing operational risk and maintaining service continuity for Smart Clinic’s users and stakeholders.

Testing data

Smart Clinic strictly enforces the use of dummy, anonymised, or synthetic data during all phases of system and application testing. Live production data is never used in development or testing environments to protect the confidentiality and privacy of client and patient information.

Test data is carefully designed to simulate real-world scenarios and system behaviour without exposing personal or sensitive information. Where anonymised data is required, it is processed to remove or obfuscate any identifiable fields, ensuring it cannot be traced back to real individuals.

This policy applies to all forms of testing, including unit testing, system integration testing, user acceptance testing (UAT), and performance testing. Test datasets are stored securely, version-controlled where applicable, and access is limited to authorised personnel involved in testing activities.

By using only non-production data in test environments, Smart Clinic significantly reduces the risk of data breaches, supports compliance with data protection obligations, and maintains the trust of our clients and patients.

Section 3 – Networks

Firewalls and network protection

Smart Clinic employs a comprehensive firewall strategy to protect all network traffic and ensure the confidentiality, integrity, and availability of our systems and data. This includes the use of network firewalls and web application firewalls (WAFs) to monitor, control, and filter traffic entering and leaving our digital infrastructure.

Our firewalls are configured with a default “deny all” policy, meaning all traffic is blocked unless it is explicitly permitted based on approved rules and business requirements. This approach minimises exposure to unauthorised access, malware, and other external threats.

Network firewalls are deployed at key points within our architecture to segment internal systems and protect critical assets, while WAFs are implemented to inspect and defend our web-facing applications from common threats such as SQL injection, cross-site scripting (XSS), and other vulnerabilities identified by the OWASP Top 10.

Firewall rules are tightly controlled and reviewed on a regular basis to ensure they remain relevant and secure. In addition, a formal annual review of all firewall configurations and policies is conducted to assess their effectiveness, validate ongoing requirements, and implement improvements as necessary.

By maintaining strong firewall controls and conducting regular reviews, Smart Clinic ensures a robust, layered defence against cyber threats across all areas of the network and application infrastructure.

Network segmentation and segregation

Smart Clinic applies network segmentation and segregation principles to ensure that systems with different security requirements are appropriately isolated from one another. This approach helps limit the spread of threats, enforce least-privilege access, and protect sensitive systems from unnecessary exposure.

High-risk or critical systems, such as those handling patient data or financial transactions, are placed in tightly controlled segments with limited access routes. Access between network segments is governed by strict firewall rules and access control lists (ACLs), with monitoring to detect and prevent unauthorised traffic.

Systems that have been retired or decommissioned are promptly removed from all active network segments and access points. Before decommissioning, data is securely wiped or migrated as per the data retention policy, and all system credentials and configurations are invalidated. These systems are then powered down and, where applicable, physically removed from the environment to eliminate potential backdoor risks.

This layered network design improves visibility, contains incidents, and strengthens overall cyber resilience.

Isolation of publicly accessible networks

All public-facing services at Smart Clinic, such as customer portals, appointment booking systems, and APIs, are hosted in a dedicated Demilitarised Zone (DMZ) to ensure they are isolated from internal business and clinical networks.

The DMZ is a specially configured network zone that allows limited, controlled connectivity from external users while preventing direct access to the internal Smart Clinic infrastructure. Firewall policies strictly control incoming and outgoing traffic, and only essential ports and protocols are permitted. These services are continuously monitored and regularly patched to maintain security.

Reverse proxies, intrusion prevention systems, and web application firewalls (WAFs) are used within the DMZ to provide additional layers of protection against web-based attacks. Logs and access attempts are monitored and audited to detect potential anomalies or breaches. This DMZ architecture helps minimise the blast radius of any compromise and ensures that Smart Clinic's core systems remain protected even when public-facing services are exposed to the internet.

DOS and DDOS

Smart Clinic employs a combination of proactive and reactive security measures to protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which could otherwise threaten the availability of our online services.

At the network perimeter, firewalls and intrusion prevention systems are configured with rate-limiting, connection throttling, and anomaly detection rules to filter out suspicious traffic. These tools help mitigate volumetric attacks by identifying abnormal patterns and blocking excessive or malicious connection attempts before they reach critical services.

For internet-facing services, Smart Clinic leverages cloud-based DDoS protection services capable of absorbing and filtering large-scale attack traffic before it impacts internal systems. These services include features such as traffic scrubbing, geo-blocking, and real-time traffic analysis.

Incident response procedures are in place to escalate and contain potential DDoS events quickly. Logs and metrics from security devices are reviewed regularly to identify and learn from attempted attacks, helping to continuously improve our defensive posture.

Together, these protections ensure that Smart Clinic's systems remain accessible, resilient, and secure against service disruption threats.

Remote connections

Smart Clinic ensures that all remote connections to internal networks or systems are conducted using secure, encrypted communication protocols to prevent unauthorised access and protect the confidentiality of transmitted data.

All remote access must be established through a Virtual Private Network (VPN) or Secure Shell (SSH) connection, depending on the use case. These connections require strong authentication, including the use of multi-factor authentication (MFA), and are encrypted using modern cryptographic standards such as AES-256 to safeguard data in transit.

Access is limited to authorised personnel and is granted on a role-specific, least-privilege basis. Remote sessions are logged and monitored for unusual or unauthorised activity, and timeouts are enforced after a period of inactivity.

By implementing these secure remote access controls, Smart Clinic ensures that staff can safely connect to critical systems while maintaining high standards of data security and operational integrity.

Data transfers

At Smart Clinic, data transfers are generally not required, as all client and patient information is securely stored on our own servers and accessed via encrypted client portals designed to ensure secure, role-based access to information.

In the rare instances where data transfers are necessary, strict protocols are followed to ensure the security of the information in transit. Transfers are only carried out using encrypted channels, such as SFTP (Secure File Transfer Protocol), TLS-encrypted email, or other secure, pre-approved methods.

Sensitive data is encrypted using strong algorithms (e.g. AES-256) before transfer, and any recipients must authenticate their identity and confirm receipt through secure channels. All data transfers are logged and subject to access and audit controls.

These precautions ensure that any required data movement is conducted with the highest level of security, minimising risk and maintaining the confidentiality and integrity of the data involved.

Cryptographic keys

Smart Clinic implements strict controls over the generation, storage, usage, and access of cryptographic keys to ensure the confidentiality, integrity, and authenticity of sensitive data, including patient and client information.

All cryptographic keys are securely generated using industry-standard algorithms and are stored in secure key management systems or encrypted storage environments. Access to cryptographic keys is strictly limited to authorised personnel on a need-to-know and role-specific basis. Administrative privileges required to manage keys are tightly controlled and subject to multifactor authentication (MFA) and audit logging.

Access to keys is governed by role-based access controls (RBAC) and enforced through system policies to prevent unauthorised use or disclosure. Key usage is monitored, and all access and operations involving cryptographic keys are logged and auditable to provide full traceability.

Key rotation schedules are established in line with best practices, and keys are periodically rotated, retired, or revoked to reduce risk. In the event of suspected compromise, emergency key revocation and re-issuance procedures are in place.

By maintaining robust cryptographic key management practices, Smart Clinic ensures that encryption processes remain effective, secure, and aligned with industry standards for protecting sensitive digital assets.

Remote access

Smart Clinic enforces strict security measures to protect all remote access to internal systems and networks. All remote users must authenticate via secure channels, and access is only granted to individuals with a legitimate business need.

A key control in securing remote access is the use of Multi-Factor Authentication (MFA), which is mandatory for all users connecting from external networks. This ensures that access is protected by a second layer of identity verification beyond just a username and password.

Remote access is only permitted via approved secure methods, such as Virtual Private Networks (VPNs) with strong encryption protocols (e.g. AES-256), and Secure Shell (SSH) with public key authentication for administrative access. Session timeouts and automatic logout policies are enforced to reduce the risk of unattended active sessions.

All remote access sessions are monitored and logged, and any anomalous activity is automatically flagged for review. Access permissions are reviewed regularly and revoked when no longer required.

These combined controls ensure that Smart Clinic maintains secure, accountable, and resilient access to its systems when working remotely.

Network connections

Smart Clinic permits only pre-approved and risk-assessed network connections to internal systems and infrastructure to safeguard operational security and protect sensitive data.

All network connections, including third-party integrations, remote sites, and cloud-based systems, must undergo a formal risk assessment prior to approval. This assessment evaluates:

- The sensitivity of the data involved.
- The origin and destination of traffic.
- The security posture of any third-party providers.
- Compliance with Smart Clinic's internal cybersecurity and data protection policies.

Only connections that meet Smart Clinic's technical, operational, and regulatory standards are approved. All approved network connections are documented, reviewed periodically, and subject to ongoing monitoring and logging.

Unauthorised network connections are prohibited and are automatically blocked by firewall and intrusion prevention systems. This policy ensures that only secure, controlled, and justifiable connections are permitted, significantly reducing the organisation's exposure to cyber threats.

Vulnerability scanning

Smart Clinic maintains a proactive security posture through continuous automated vulnerability scanning across its digital infrastructure.

All internal and external systems, including servers, endpoints, web applications, and network devices, are regularly scanned using industry-recognised tools. These scans are configured to run on a frequent and automatic schedule, ensuring near real-time detection of known vulnerabilities, misconfigurations, and emerging threats.

Vulnerability data is automatically logged and assessed against industry-standard threat databases, such as CVE and NVD. Any vulnerabilities identified are categorised by risk level and prioritised for remediation based on their potential impact and exploitability.

In addition to automated scanning, results are regularly reviewed by Smart Clinic's security team to validate findings, implement patches, and update scanning rules. This process ensures that vulnerabilities are quickly addressed, reducing the risk of compromise and maintaining a strong security posture.

Intruder detection

Smart Clinic maintains a proactive and layered approach to network and cloud security by implementing advanced monitoring controls, including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM) technologies.

These systems continuously monitor network traffic, cloud environments, and system behaviours for suspicious activities, policy violations, and known threat patterns. The IDS components are used to detect and alert on potential intrusions, while IPS components actively block or mitigate threats in real time, based on defined rules and threat intelligence feeds.

In addition, Smart Clinic utilises a centralised SIEM platform to collect, aggregate, and analyse log data from across the organisation's infrastructure, including firewalls, servers, endpoints, and cloud services. This enables real-time threat detection, historical analysis, and automated alerting on high-risk events.

Our logging and monitoring policy mandates:

- 24/7 log collection from critical systems.
- Real-time alerting on defined security incidents.
- Regular review of event logs by trained personnel.
- Audit trails for all security-related activities, retained in accordance with our data retention policies.

When a potential threat is identified, it is promptly escalated to Smart Clinic's security team, who follow defined incident response procedures for containment, investigation, and remediation. All events are documented, and lessons learned are integrated into future preventative measures.

These controls ensure a robust and responsive security environment, supporting early detection and effective response to cyber threats, and helping to protect the confidentiality, integrity, and availability of Smart Clinic's systems and data.

Capacity and load

Smart Clinic employs real-time monitoring of system capacity and load across all critical infrastructure to ensure optimal performance, stability, and reliability of services. This includes continuous tracking of CPU usage, memory, disk I/O, network throughput, and application-specific metrics on servers, cloud environments, and network devices.

Our monitoring tools are configured with threshold-based alerts, which automatically trigger when resource utilisation exceeds defined safe limits. Alerts are escalated through a multi-stage process:

- Stage 1 – Informational Alert: Notification sent to technical team when resource usage exceeds 70% of capacity.
- Stage 2 – Warning Alert: At 85%, an urgent notification is issued and logged as a potential performance risk.
- Stage 3 – Critical Alert: At 95% or above, the issue is escalated to senior IT staff for immediate response and potential remediation action.

When excessive load is detected, our response measures may include:

- Scaling resources vertically or horizontally (e.g., adding more compute or load-balancing traffic).
- Restarting or redistributing services to reduce strain on specific nodes.
- Temporarily limiting non-essential processes or external access points to maintain core service availability.
- Investigating potential root causes such as inefficient code, traffic spikes, or service misconfigurations.

System performance and load considerations are integral to all development work. During the planning and design phases, solutions are evaluated for efficiency, scalability, and resource usage. Applications are built following best practices in performance optimisation, including code efficiency, caching, database indexing, and asynchronous processing where appropriate.

In addition, new features or services are tested in staging environments under simulated load to assess performance impact prior to deployment. This proactive, performance-aware development model helps ensure Smart Clinic's systems remain responsive, stable, and scalable as demands evolve.

Activity monitoring

Smart Clinic maintains a comprehensive and secure process for logging, monitoring, and storing all user activity across the network to support accountability, security auditing, and threat detection.

All user actions—such as logins, logouts, file access, system changes, administrative activity, and data interactions—are automatically recorded in detailed audit logs. These logs are captured in real time and are transmitted to a centralised logging and monitoring environment that is logically separated from the systems and applications being monitored. This separation ensures the integrity, confidentiality, and availability of log data, and prevents tampering or interference by users or system-level compromises.

The logging infrastructure is backed by a Security Information and Event Management (SIEM) platform, which aggregates and analyses logs to detect suspicious behaviour, policy violations, and security incidents. Alerts are triggered for anomalous activity, and all incidents are reviewed and triaged by Smart Clinic's IT and security teams in accordance with our incident response procedures.

Audit logs are retained for a defined period in line with internal policy and regulatory requirements, and are securely encrypted both at rest and in transit. Access to logs is strictly limited to authorised personnel and is itself logged and monitored.

This robust approach to user activity monitoring enhances operational transparency, supports compliance efforts, and strengthens Smart Clinic's ability to detect and respond to internal and external threats effectively.

Cloud services

At Smart Clinic, none of our core systems or infrastructure are classified as 'cloud services', as our primary data storage and applications are hosted on our own secured servers and managed environments.

However, we acknowledge that from time to time, we may use third-party cloud-based applications or services to support specific operational needs (e.g., productivity tools, communication platforms, or specialist software). When such services are used, Smart Clinic ensures that appropriate safeguards are in place to protect the confidentiality, integrity, and availability of any data processed or transmitted.

These safeguards include:

- Due diligence and risk assessment of the cloud service provider, including a review of their security certifications (e.g., ISO 27001, SOC 2).
- Ensuring the provider has robust encryption protocols in place for data at rest and in transit (e.g., TLS, AES-256).
- Reviewing and agreeing on data processing agreements (DPAs) and privacy terms to ensure compliance with relevant legal and regulatory obligations.
- Enforcing role-based access controls and multi-factor authentication (MFA) for all access to cloud services.
- Limiting the use of cloud services to only those which are approved and assessed through our internal governance processes.
- Monitoring and auditing access and activity where possible, to detect any unauthorised use or potential data exposure.

By applying these controls, Smart Clinic ensures that any use of cloud-based services aligns with our commitment to data protection, cyber security, and responsible digital governance.

Anti-malware

Smart Clinic implements a comprehensive anti-malware strategy to protect all endpoints and internal IT infrastructure against malicious software, including viruses, ransomware, spyware, and other emerging threats.

At the core of this strategy is the deployment of a robust Endpoint Detection and Response (EDR) solution across all devices, including desktops, laptops, servers, and mobile endpoints. This EDR system provides real-time threat detection, behavioural monitoring, automated response capabilities, and detailed forensic analysis to identify and contain threats before they can cause harm.

Key anti-malware controls include:

- Real-time scanning and protection against known and unknown threats.
- Automated response actions such as quarantining files, terminating malicious processes, and isolating compromised devices from the network.
- Regular signature updates and threat intelligence feeds to stay ahead of the latest malware variants.
- Centralised management and alerting, allowing the IT and security teams to monitor the health and security status of all endpoints from a unified dashboard.
- Routine scans and system checks, scheduled to ensure ongoing protection and compliance with internal security policies.

In addition to technical controls, Smart Clinic enforces security awareness training to help users recognise and avoid malware threats, such as phishing emails and suspicious downloads.

Together, these measures ensure that Smart Clinic maintains a strong, proactive defence against malware, minimising the risk of disruption to operations and safeguarding sensitive client and patient data.

Email security

Smart Clinic maintains strong email security practices to protect against spoofing, phishing, and unauthorised interception of email communications.

We implement Opportunistic TLS (Transport Layer Security) for all outbound and inbound email traffic. This ensures that, where supported by the recipient's mail server, email transmissions are encrypted in transit, reducing the risk of eavesdropping or tampering during delivery. While Opportunistic TLS does not guarantee encryption in every instance, it enhances the baseline security of email exchanges and aligns with industry best practices.

To further protect our email domain from impersonation and abuse, Smart Clinic configures and actively manages the following email authentication protocols within our DNS services:

- SPF (Sender Policy Framework): Specifies which mail servers are authorised to send emails on behalf of our domain. This helps prevent spoofed messages from reaching recipients.
- DKIM (DomainKeys Identified Mail): Applies a digital signature to each outgoing email, allowing receiving mail servers to verify that the message was not altered during transmission and that it originated from an authorised source.
- DMARC (Domain-based Message Authentication, Reporting and Conformance): Builds on SPF and DKIM by instructing receiving servers how to handle emails that fail authentication checks. It also provides detailed reporting, enabling Smart Clinic to monitor and respond to unauthorised use of our domain.

These layered email security measures significantly strengthen Smart Clinic's ability to prevent email-based threats, maintain the integrity of our communications, and protect both internal users and external recipients.

Section 4 - Hardware

Inventory of assets

Smart Clinic maintains a comprehensive and up-to-date central register of all company assets, which includes both hardware and software resources. This inventory is managed under the supervision of a designated responsible person within the IT department, who ensures the accuracy and completeness of asset records.

Each asset entry includes key details such as:

- Purchase date
- Number of historical users
- Expected lifespan
- Expected upgrade or replacement date

This asset inventory plays a vital role in lifecycle planning, budget forecasting, and incident response, ensuring that all equipment is properly tracked, maintained, and decommissioned in accordance with our operational and security standards.

Hardware encryption

To safeguard sensitive information and ensure data confidentiality, all company hardware—especially laptop computers—is encrypted using high-grade encryption standards (e.g., AES-256). This protects devices in the event of loss or theft.

Additionally, all company laptops are configured to allow remote wiping, enabling Smart Clinic's IT team to securely erase all data if a device is lost, stolen, or otherwise compromised.

As part of our provisioning process, all network devices and other systems have their default credentials changed immediately upon installation to strong, unique passwords, reducing the risk of unauthorised access.

Personal devices

Smart Clinic enforces a strict no personal device policy for work-related activities. The use of personal laptops, tablets, or smartphones for accessing or processing company data is explicitly prohibited. This control is in place to ensure data security, reduce risk of unauthorised access, and maintain clear boundaries between personal and business information.

Only company-issued and managed devices are permitted for all operational tasks, and these are subject to the full range of security controls outlined in our IT policies.

Destruction

Smart Clinic ensures that all equipment and media that are no longer required are securely and permanently destroyed in accordance with our data protection and disposal policies.

Devices are first assessed for reuse or repurposing; if no longer viable, they are decommissioned and passed to certified third-party disposal providers. These providers carry out secure physical destruction or digital sanitisation of equipment, and provide destruction certificates for record-keeping and audit purposes.

This process guarantees that sensitive information cannot be recovered or accessed once a device has been taken out of service.

Software on production systems

Smart Clinic has strict procedures governing the installation of software on both production systems and end-user devices.

Only approved software is permitted on IT production environments, and all installations must be:

- Reviewed for security and compliance risks
- Requested through formal channels
- Authorised by the IT department

End-user systems are configured to restrict administrative rights, preventing unauthorised software installation. Any exceptions must be logged, justified, and approved in advance.

This controlled approach ensures system stability, prevents security vulnerabilities, and maintains compliance with our operational standards.

Section 5 – Physical security

CCTV

Smart Clinic utilises Closed-Circuit Television (CCTV) systems as an essential component of our overall security strategy to protect our premises, assets, staff, clients, and sensitive information.

The CCTV cameras are strategically positioned to cover all critical areas of our facilities, including entrances and exits, server rooms, reception areas, and other locations where sensitive information or valuable equipment is stored or processed. This coverage helps deter, detect, and investigate unauthorised access or suspicious activities that could impact both physical security and cyber security.

All CCTV footage is securely stored for a minimum of three months, in compliance with data protection regulations and internal retention policies. Access to CCTV recordings is strictly limited to authorised personnel only and is controlled through secure authentication measures to prevent unauthorised viewing or tampering.

The CCTV system supports Smart Clinic's cyber security framework by:

- Providing a physical audit trail to correlate with security incidents involving IT assets or data breaches.
- Assisting in the detection of unauthorised physical access to areas housing critical IT infrastructure.
- Enhancing overall situational awareness and incident response capabilities.

Smart Clinic is committed to ensuring that the use of CCTV respects individuals' privacy rights while maintaining a safe and secure environment for all stakeholders. All CCTV operations comply with applicable laws and regulations governing surveillance and data protection.

Access control

Smart Clinic enforces a strict Access Control Policy to safeguard our premises, IT systems, and sensitive data from unauthorised access, ensuring the security of both physical and digital environments.

Access to all Smart Clinic facilities, including sensitive areas such as server rooms and data centres, is restricted to authorised personnel only. Physical access controls include secure entry systems such as keycards, biometric scanners, or PIN codes. Access rights are regularly reviewed and promptly updated to reflect personnel changes or evolving security requirements.

For IT systems and digital resources, access is granted based on the principle of least privilege, ensuring users have only the permissions necessary to perform their job functions. Access credentials are managed securely, and multi-factor authentication (MFA) is enforced for critical systems to reduce the risk of unauthorised access.

All access attempts—both physical and logical—are logged and monitored continuously. Any suspicious or unauthorised access attempts trigger alerts and are investigated in accordance with Smart Clinic's incident response procedures.

Access rights and permissions are reviewed on a regular basis to ensure ongoing appropriateness and compliance with company policies and regulatory requirements.

This robust access control framework helps prevent unauthorised entry or data breaches, protects client and patient information, and supports Smart Clinic's commitment to maintaining a secure and compliant environment.

Alarms

Smart Clinic utilises a comprehensive office alarm system to enhance the physical security of our premises outside of operating hours and during periods of low occupancy.

The alarm system is installed across all critical entry points and sensitive areas within the facility, providing real-time detection of unauthorised access, forced entry, or other security breaches.

Importantly, the alarm system is directly connected to the local police station, ensuring an immediate response in the event of an alarm activation. This connection enables rapid intervention, helping to protect personnel, assets, and sensitive information from potential threats.

The alarm system is regularly tested and maintained to ensure optimal functionality and reliability. Access to alarm control is restricted to authorised personnel only, with clear procedures in place for arming, disarming, and responding to alarm events.

Smart Clinic's office alarm system forms a critical part of our broader security framework, supporting both physical safety and the protection of cyber infrastructure by safeguarding the environments where IT systems and data are housed.

24-hour security

Smart Clinic benefits from 24-hour site security services to ensure the ongoing safety and protection of our premises, personnel, clients, and sensitive assets at all times.

Our facility is located within Gadbrook Park, a well-established Business Improvement District (BID) that provides additional coordinated safety and security measures across the park. This collaborative environment enhances overall site security through regular patrols, monitored access points, and shared intelligence among BID members.

The dedicated security personnel on site conduct continuous monitoring, access control enforcement, and incident response throughout the day and night. Their presence serves as a deterrent to unauthorised activity and supports rapid intervention in case of any security concerns.

This 24-hour security coverage complements Smart Clinic's internal security controls, including CCTV, alarm systems linked directly to local police, and access management policies, creating a layered defence that protects both physical infrastructure and the sensitive data we handle.

Smart Clinic regularly reviews and coordinates with Gadbrook Park BID and our security providers to ensure that security measures remain effective and aligned with evolving threats and operational needs.

Section 6 – Team and Training

Acceptable use

At Smart Clinic, all IT assets and information systems are to be used in a manner that protects the confidentiality, integrity, and availability of sensitive medical and occupational health data. Users are expected to act responsibly and in compliance with all applicable internal policies and healthcare regulations.

Employees must:

- Use systems solely for authorised business purposes.
- Protect patient and client records from unauthorised access, especially in line with ethical obligations in occupational health.
- Refrain from installing unauthorised software or hardware.
- Avoid using corporate systems for personal social media, gaming, or unapproved file sharing.

Deliberate misuse, including data exfiltration or unauthorised system probing, is considered gross misconduct and may lead to dismissal and legal action.

Use of mobile devices

Mobile device usage at Smart Clinic is strictly controlled due to the sensitivity of patient data handled in occupational health services. All company-issued mobile devices must:

- Be encrypted to industry standards.
- Include remote wipe capabilities in case of loss or theft.
- Use secure authentication methods such as biometrics or strong PINs.

Accessing clinical systems or sensitive data on personal mobile devices is strictly forbidden. Devices are monitored by mobile device management (MDM) software to ensure compliance.

There is more information about this referenced throughout this policy.

Remote working

Remote working is permitted only under secure, pre-approved conditions. Employees accessing clinical or HR records from remote locations must:

- Use Smart Clinic-issued devices configured with endpoint protection.
- Connect via an encrypted VPN with enforced multi-factor authentication.
- Never store patient records locally or print confidential material at home.

Remote work must be conducted in private, secure environments to comply with occupational health standards and protect medical confidentiality.

Password statement

Strong authentication is critical in protecting Smart Clinic's systems. All users must:

- Create passwords of at least 12 characters with complexity (uppercase, lowercase, numbers, special characters).
- Change passwords every 90 days.
- Use unique passwords for each system.
- Store credentials securely (approved password managers only).

Systems containing patient or medical data have additional controls, including lockout after repeated failed attempts and MFA.

Clear desk and clear screen statement

To prevent unauthorised access to sensitive records, all staff must:

- Lock their computer screens when unattended.
- Store patient files, notes, and forms in locked cabinets.
- Avoid leaving printed reports or prescriptions in shared areas.
- Dispose of printed documents in confidential shredding bins.

This is especially important in shared clinic rooms or multi-use medical environments.

Removable media

Due to the high risk of data leakage and malware, Smart Clinic prohibits the use of USB drives and other removable media unless:

- Explicitly approved for a defined clinical or administrative purpose.
- Scanned for malware before use.
- Logged and monitored by IT.

Alternative secure data transfer methods (e.g., encrypted email, secure client portals) must be used wherever possible.

Non-disclosure of commercially sensitive information

All employees must protect Smart Clinic's commercially sensitive information, including:

- Pricing structures.
- Client engagement strategies.
- Clinical service delivery models.

Staff are required to sign confidentiality agreements upon employment. Disclosure of sensitive data to external parties, including clients or competitors, without authorisation is strictly prohibited.

Background checks

Given the sensitive nature of occupational health data, all new hires must undergo:

- Identity verification.
- Right-to-work checks.
- Criminal record checks (e.g., DBS for clinical roles).
- Employment and reference verification.

This process is overseen by HR and completed before any system access is granted.

Breach of policy

Smart Clinic enforces a zero-tolerance policy on deliberate breaches of IT or data protection policies. Breaches will be investigated under formal HR procedures and may result in:

- Warnings (verbal/written).
- Suspension pending investigation.
- Dismissal for gross misconduct.

Incidents involving patient data or system security will also be reported to regulatory bodies (e.g., ICO) as required.

Offboarding

All departing employees, including contractors and clinical staff, undergo a structured offboarding process, which includes:

- Immediate revocation of access to clinical systems and communication platforms.
- Return of all equipment, badges, and storage devices.
- Reassignment or secure deletion of patient notes or records held by the individual.
- A formal exit checklist signed by both HR and IT.

The process ensures continuity of care and protection of confidential data.

Section 7 – Business continuity and disaster recovery plan

Introduction

This Business Continuity and Disaster Recovery Plan (BCDRP) outlines the structured response procedures and responsibilities to be followed in the event of a disruption or disaster that significantly affects the normal operations of the business. Its purpose is to ensure that Smart Clinic can continue to provide essential occupational health services, protect critical data and infrastructure, and recover operations as quickly and effectively as possible.

This plan applies to any incident—natural, technological, or human-made—that has the potential to impact the delivery of clinical services, patient care, business systems, or operational processes. Examples include, but are not limited to, fire, flood, cyberattack, widespread power failure, or significant system outages.

The BCDRP is designed to:

- Minimise the impact of a disruption on our clients, patients, and staff.
- Protect vital records, patient data, and infrastructure.
- Provide a clear and tested roadmap for restoring essential services in a timely manner.
- Maintain compliance with regulatory and industry requirements related to information security, healthcare provision, and data protection.

This operating procedure is to be invoked under the authority of the designated Business Continuity Lead when a disaster scenario is declared. It includes both short-term emergency response and longer-term recovery efforts to return to full operational capability.

Regular testing, review, and updates of this plan are conducted to ensure its effectiveness and alignment with the evolving risk landscape and Smart Clinic's strategic objectives.

Definitions and terminology

- **Business Continuity** – The ability to maintain essential functions during and after a disruption.
- **Disaster Recovery** – Specific IT and technical measures to restore data and systems following a disruption.
- **RTO** (Recovery Time Objective) – The maximum acceptable time before a disrupted service must be restored.
- **RPO** (Recovery Point Objective) – The maximum acceptable amount of data loss measured in time.
- **Critical Systems** – Systems essential to patient care and operational delivery.

Roles and responsibilities

ROLE	RESPONSIBILITY
BUSINESS CONTINUITY LEAD	Coordinates response and recovery actions, activates the BCDRP
IT LEAD	Responsible for technical recovery of systems, data, and infrastructure.

CLINICAL OPERATIONS LEAD	Ensures continuity of patient care and clinical activities.
COMMUNICATIONS LEAD	Manages internal and external communication.
HR	Supports staff deployment and monitors welfare. Investigates any mis-conduct.
CLIENT SUPPORT	Supports communications lead with any external communications.
EXTERNAL VENDORS	Assist in infrastructure recovery, cloud support, and secure data restoration.

Risk assessment and business impact analysis

Smart Clinic has conducted a comprehensive Risk Assessment and Business Impact Analysis (BIA) to identify and prioritise potential threats. These include:

- Cyberattack or ransomware incident
- Loss of clinical premises (fire, flood, etc.)
- Network or server failure
- Utility or service interruption (e.g., internet, power)
- Staff unavailability (e.g., pandemic, strike)

Critical Systems Identified:

- Electronic Medical Records (EMR)
- Appointment and scheduling systems
- Secure client portals
- Communications systems (email, VoIP)
- Remote access and telehealth platforms

SYSTEM / SERVICE	RTO	RPO
CLIENT PORTAL	4 hours	1 hour
INTERNAL SYSTEM AND MEDICAL RECORDS (EMR)	4 hours	1 hour
TELEPHONE COMMUNICATIONS	1 hour	Nil
EMAIL COMMUNICATIONS	4 hours	Nil
CLINICAL OPERATIONS	4 hours	Same day

Incident response procedure

All information security events are classified according to impact and likelihood. Staff are trained to report any suspected data breach, cyberattack, or system anomaly immediately through a designated reporting system or directly to the Information Security Officer.

Activation Criteria:

- System unavailability exceeding 1 hour
- Physical damage to clinic premises

- Loss of critical services or data

Immediate Actions:

- Activate BCDRP via the Business Continuity Lead
- Assemble the Incident Response Team
- Notify affected stakeholders and authorities as appropriate
- Communicate using pre-approved messaging templates
- Log all actions taken in the incident log

Internal Reporting:

- Staff report to IT or InfoSec via secure email or telephone
- Incident logged and categorised

External Reporting:

- Clients are notified of any breach that impacts their data within 48 hours
- ICO is notified where required under UK GDPR

All incidents undergo root cause analysis and review to prevent recurrence.

Alternative communication systems

If standard communication systems (email, VoIP) are unavailable:

- Secure mobile phones (pre-issued to leadership)
- Encrypted messaging apps approved for interim use
- Emergency group chat via cloud-hosted platform

All messages sent through alternative platforms are documented and archived.

IT disaster recovery and backup

Smart Clinic systems incorporate:

- Daily backups of all critical systems
- Encrypted offsite storage
- Backup tests performed monthly
- Data integrity checks run post-restoration
- Backup RPOs adhered to per critical system

Backups include EMR systems, internal documentation, client files, and email records. Default backup encryption standard is AES-256.

Disaster recovery is rehearsed as follows:

- Full-scale BCDRP rehearsal conducted annually
- Tabletop incident simulations held twice yearly
- Backup restorations tested monthly
- Lessons learned from exercises are documented and incorporated into future plans

Business continuity strategies

To ensure continuity of services:

- **Alternative Working Locations:** Staff are equipped for remote work. Secure remote access and virtual desktop infrastructure (VDI) are used.
- **Manual Workarounds:** Paper-based assessment tools and clinical documentation procedures are maintained for emergency use.
- **Client Communication:** Clients are notified of service adjustments with alternative support provided.
- **Service Prioritisation:** Clinical care, particularly safety-critical services (e.g., safety-critical medicals), takes precedence.

IT disaster recovery plan

- **Backups**: Daily encrypted backups of all key data to secure off-site storage. Weekly full backups tested monthly.
- **Restoration**: Servers, virtual machines, and applications restored in order of criticality.
- **Hosted Services**: Hosted applications and cloud platforms have 99.9% SLA guarantees and geo-redundant hosting.
- **Infrastructure**: Recovery of networking and server infrastructure coordinated with third-party IT partners.
- **Security Posture**: Post-recovery review includes password resets, MFA re-verification, and review of security logs.

Even during disruption:

- Patient confidentiality is maintained according to Smart Clinic's Data Protection Policy.
- Data breaches are reported within 72 hours, as per UK GDPR guidelines.
- Staff are reminded of their responsibilities under confidentiality agreements and clinical codes of conduct.

For more details, please see our Data Policy. All aspects of this policy shall still apply.

Additionally in the event of a disaster:

In the event of a disaster:

- Firewalls, endpoint protection, and access controls are prioritised for restoration
- Manual controls are used until systems are operational

- Temporary access is tightly controlled and monitored

Cyber insurance

Smart Clinic maintains active cyber insurance coverage to protect against loss related to data breaches, business interruption, and ransomware. Insurance includes:

- Incident response support
- Legal advisory
- Client notification support
- Business continuity financial coverage

Details for this are published on our website, and can be accessed upon request.

Closing thoughts

Smart Clinic is committed to the highest standards of cyber security and information governance, recognising our responsibilities as a trusted provider of occupational health services. This policy consolidates a comprehensive set of controls, procedures, and best practices designed to protect sensitive patient and client information, support business continuity, and comply with regulatory and legal obligations.

The cyber security framework at Smart Clinic is supported by clearly defined roles and responsibilities, robust technical safeguards (such as encryption, access controls, monitoring, and anti-malware protection), and a culture of security awareness across all levels of the organisation. All systems, including those used for electronic medical records (EMRs), client communication, and remote access, are maintained with a strong security posture. Controls such as role-based access, multi-factor authentication, endpoint detection and response (EDR), vulnerability management, and secure software development lifecycle (SDLC) practices ensure continued system integrity.

This overarching policy is complemented by a range of sub-policies covering acceptable use, mobile devices, password management, access control, data classification, secure software development, and disaster recovery. In addition, the organisation maintains regular training, background checks, offboarding procedures, and disciplinary processes to reduce human-factor risks.

Incidents are categorised, reported, and analysed using a structured root cause methodology. The organisation maintains cyber insurance, regularly rehearses its incident and disaster recovery responses, and ensures that all backups are encrypted, tested, and aligned with the Recovery Time and Recovery Point Objectives (RTOs and RPOs) set out in our Business Continuity and Disaster Recovery Plan.

By embedding these measures into daily operations, Smart Clinic protects both its clients and itself from evolving cyber threats—ensuring service continuity, data integrity, and ongoing compliance in the healthcare sector.