INTUS
healthcare

Intus Healthcare

Information Security Management Policy

Purpose

Information that is collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, as well as possible judgements being made against Intus Healthcare Ltd.

This Information Security Policy sits alongside the 'Privacy Policy (MP002-1) and System Manual (MP010-3) to provide an outline of, and justification for, Intus Healthcare's risk-based information security controls.

Objectives

Intus Healthcare's security objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Our authorised users can securely access and share information in order to perform their roles
- Our physical, procedural and technical controls balance user experience and security
- Our contractual and legal obligations relating to information security are met
- Our teaching, research and administrative activity considers information security
- Individuals accessing our information are aware of their information security responsibilities
- Incidents affecting our information assets are resolved and learnt from to improve our controls

Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used at Intus Healthcare Ltd, in all formats. This includes information processed by other organisations in their dealings with Intus Healthcare Ltd.

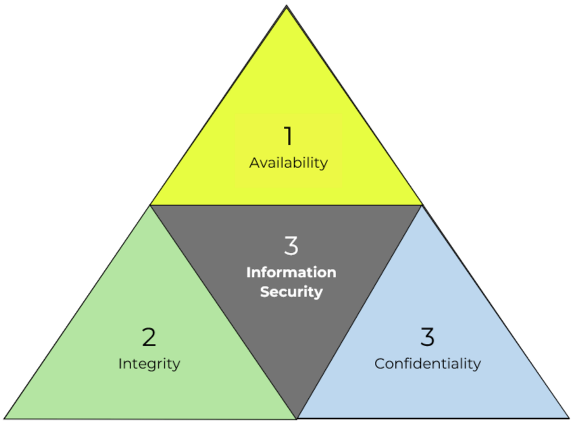
The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Intus Healthcare information and technologies. This includes external parties that provide information processing services to Intus Healthcare.

Policy Statement

It is Intus Healthcare's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained

- Availability – information will be accessible to authorised users and processes when required



Information Security Governance

1. Information Security Leadership

- **Senior Information Risk Owner (SIRO):** Overseeing all security investigations that seek to obtain factual evidence to support or disprove alleged misuse of the computing environment and/or data.
- **IT Team:** Responsible for overseeing the information security program and ensuring compliance with this policy.
- **Leadership Team:** A cross-functional team responsible for reviewing and endorsing security policies, procedures, and initiatives.

2. Risk Management

- Conduct regular risk assessments to identify, evaluate, and mitigate risks to information assets. Appendix C – Managing Risks (System Manual MP010-3)
- Implement controls to manage identified risks, ensuring they are within acceptable levels.

3. Organisation of information security

Intus Healthcare Ltd have implemented suitable governance arrangements for the management of information security. All information assets will be classified according to their legal requirements, business value, criticality and sensitivity. Classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

4. Asset Management

- Asset Inventory: Maintain an up-to-date inventory of information assets, including hardware, software, and data.
- Ownership and Responsibility: Assign ownership of assets to individuals responsible for their protection and maintenance.
  Employees are required under contract to return all property assets and any original or copy documents provided or obtained in the course of their employment.

5. Access Control

- Implement role-based access controls (RBAC) to ensure that only authorised individuals have access to information assets.
  Administrator access is not provided without permission from the General Manager or the wider Leadership Team.
- Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. The separation of duties will be implemented, where practical.
- Use multi-factor authentication (MFA) for accessing the Intus Healthcare critical systems and information.
- Regularly review and update access permissions based on role changes or employment status.

6. Password-Based Access and Technical Controls

Passwords are protected against brute-force password guessing by:

- Activating multi-factor authentication (MFA) on all systems and software where it is available.
- Creating strong passwords.
  - Use at least 12-16 characters (longer is better).
  - Mix uppercase & lowercase letters, numbers, and symbols (!@#$%^&*).
  - Avoid common words and predictable sequences (e.g., password123 or abcdef).
  - Use passphrases—a random combination of words (e.g., BlueTiger$Skyline99).
  - Don’t reuse passwords across different accounts.
  - Use a password manager (Google Chrome) to randomly generate and store strong passwords.

7. Acceptable use

General

- MFA Requirement: Personal devices may be used for multi-factor authentication (MFA) for approved software platforms; ensuring devices are secure and updated.
- Distraction Management: Use of personal devices for non-work-related activities during work hours should be minimised to maintain productivity.

- Reporting Issues: Any loss, theft, or suspicious activity related to personal devices must be reported to IT immediately to protect company data.

Remote Working

Employees working remotely must comply with all company security policies to protect sensitive data and systems. This includes:

- Using only company-approved devices to access company resources.
- Ensuring secure Wi-Fi connections (no public or unsecured networks unless using a VPN).
- Keeping devices password-protected and locked when not in use.

Additional security expectations for remote work, including equipment handling and confidentiality, are outlined in the Hybrid and Remote Working Policy. Employees must review and adhere to these guidelines when working outside of Intus Healthcare premises.

When accessing company data on a personal device

- Confidential Information: Storing or accessing confidential company information on personal devices is regulated to prevent data breaches.
- Employees who have applications on their personal mobile phones that provide access to work systems including and not limited to MS Teams, outlook, support tickets and D365, must only download apps from official app stores.
- Employees are prohibited from downloading 'unsigned applications' - an app that has not been digitally signed by a verified developer. These apps lack a certificate that confirms its origin and authenticity, making it potentially unsafe to install as it could be malicious or from an untrusted source.
- Employees must have anti-malware software installed and a current, supported version of the phone's operating system.

8. Internal Network Security

At Intus Healthcare, we maintain two separate internal networks to ensure security and data protection:

- **Employee Network** – Restricted to authorised employees and company-approved devices. This network provides access to internal systems, shared resources, and business-critical applications.
- **Guest Network** – A separate, isolated network for visitors, contractors, and non-employee devices.

9. Guest Network Security Controls

Guests cannot access any company resources or employee devices while connected.

- **Device Isolation:** Guests can only see their own device on the network. They cannot detect or interact with other devices, ensuring data security and privacy.
- **Automatic Restrictions:** Even after leaving the building, guest users will only retain visibility of their own device while connected to the network.
- **Limited Access:** The Guest Network provides internet access only and does not connect to internal systems, printers, or file shares.

These controls are in place to prevent unauthorized access, mitigate cybersecurity risks, and protect company data. Employees should always connect to the Employee Network when accessing company systems.

10. Physical and Environmental Security

- Secure physical access to facilities and information assets through access controls.
- Implement environmental controls to protect information assets from damage due to fire, flood, or other environmental hazards.

11. Cryptography

Intus Healthcare Ltd will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

12. Human resources security

Intus Healthcare Ltd's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training is mandatory for all staff.

13. Operations security

Intus Healthcare Ltd will ensure the correct and secure operation of information processing systems. This will include:

- Documented operating procedures
- The use of formal change and capacity management
- Controls against malware
- Defined use of logging
- Vulnerability management

If an external service is suspected to be compromised, Intus Healthcare follows these steps to secure accounts:

- Immediate Password Reset – Change the password to a strong, unique one and review multi-factor authentication (MFA) settings.
- Access Review – Check logs for unauthorised access and assess potential data exposure.

- Notification – Inform relevant stakeholders and affected users if necessary.
- Security Reinforcement – Implement additional controls like IP restrictions and remind employees of credential best practices.
- Monitoring – Continuously monitor for suspicious activity and update security policies as needed.

14. Communications security

Intus Healthcare Ltd will maintain network security controls to ensure the protection of information within its networks. Intus Healthcare Ltd will also provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities. This is in line with the classification and handling requirements associated with that information.

15. Supplier Relationships

- Assess and manage the risks associated with third-party suppliers and partners.
- Ensure that contracts with suppliers include appropriate information security requirements.

16. Information Security Awareness and Training

Users receive education on the importance of cybersecurity, online safety, best practices for setting strong passwords, and recognising attempts to obtain or compromise data. This includes mandatory completion of training modules on the following topics:

- Phishing
- Cybersecurity and Phishing
- Essential Digital Skills – Social Media Awareness
- Essential Digital Skills – Transacting Online

Each training module has an expiry date, after which employees must retake the course to maintain compliance. In addition, we will:

- Provide specialised training for individuals with specific information security roles.

17. Information security aspects of business continuity management

Intus Healthcare Ltd will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters. This is to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience.

Business continuity plans must be maintained and tested in support of this policy. Business impact analysis will be undertaken, detailing the consequences of:

Information Security Backup

The backup, storage, and recovery of information to ensure its availability, integrity, and confidentiality. This applies to all organisational information systems, including servers, databases, applications, and user devices. It encompasses all forms of data and information, whether electronic or physical, across all locations.

Our organisation is committed to maintaining the availability and integrity of its information by implementing robust backup and recovery processes.

1. Responsibilities:

- **Leadership Team:** Overall responsibility for ensuring the implementation and compliance with this policy.
- **IT Team:** Responsible for managing the backup infrastructure, executing backup processes, and conducting regular testing of backup and recovery procedures.
- Ensuring that all information is included in the backup schedule.
- Employees: Adhere to this policy and report any issues related to backup and recovery.

2. Backup Procedures:

- Backup schedules are documented and approved by the Leadership Team.
- Backups are stored in a secure, access-controlled environment.
- A copy of the backup is stored in a cloud storage solution to ensure geographic redundancy.
- Backup media is protected against environmental threats and unauthorised access.
- Access to any of the Backup’s is on Role-based access controls (RBAC) - need to know basis only.

3. Recovery Procedures:

- Regular Testing
  - Backup and recovery processes are tested at least semi-annually.
  - Tests simulate various disaster scenarios to ensure the effectiveness and efficiency of recovery procedures.
- Documentation
  - Recovery procedures are documented, including step-by-step instructions and contact information for key personnel.
  - Documentation is reviewed annually and updated regularly to reflect any changes in the IT environment or backup procedures.
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
  - Defined and documented RTO and RPO for different types of data are included in the SLA for our IT managed service provider.
  - Ensure backup and recovery processes are designed to meet these objectives.

4. Security and Compliance:

- Access to backup media and systems are restricted to authorised personnel only.
- Encryption must be used for backup data in transit and at rest.
- Regular supplier audits are conducted to ensure compliance with this policy and relevant legal, regulatory, and contractual requirements.

5. Retention and Disposal:

- Backup data retention periods are based on contractual, business, legal, and regulatory requirements.
- Backup media is disposed of securely and in accordance and securely destroyed when no longer needed.

Employee Offboarding Security Measures

When an employee leaves Intus Healthcare, a structured offboarding process is followed to ensure the protection of company assets and information. This process is governed by Intus Healthcare's Employee Exit Policy and includes the following security measures:

1. Access Revocation:

- Immediate termination of access to all company systems, applications, and networks.
- Deactivation of employee accounts, including email, cloud storage, and internal communication platforms.

2. Return of Company Assets:

- Employees must return all company-owned devices and equipment, including laptops, mobile phones and monitors.
- Any physical documents or confidential materials must be returned or securely destroyed as per company policy.

3. Data Security and Confidentiality:

- Employees are reminded of their confidentiality obligations even after departure.
- A review is conducted to ensure that the departing employee has not retained or transferred any company data in violation of policy.

4. Email and Communication Forwarding:

- Employee email accounts may be monitored or redirected for a limited time to ensure business continuity.

5. Review of Third-Party Access and Dependencies:

- Vendors, partners, and external stakeholders who had contact with the departing employee are notified as necessary.
- Any external access granted to third parties on behalf of the employee is reviewed and revoked where applicable.

6. Post-Exit Monitoring:

- Logs and system access records are reviewed to detect any unauthorised access attempts.
- Any suspicious activity related to the former employee is investigated and reported to IT Team.

By implementing these measures, Intus Healthcare ensures that employee departures do not pose a security risk to company information and assets. The Employee Onboarding & Exit Policy is regularly reviewed and updated to align with best practices and compliance requirements.

Information Security Incident Management & Response

Intus Healthcare provides a structured and systematic approach to managing information security incidents. This approach aims to minimise the impact of incidents, ensure swift and effective response, and prevent future occurrences.

Objectives

- Timely Response: Ensure prompt detection, reporting, and response to information security incidents.
- Minimise Impact: Reduce the impact of incidents on the organisation’s operations, reputation, and assets.
- Root Cause Analysis: Identify and address the root causes of incidents to prevent recurrence.
- Continuous Improvement: Enhance the organisation’s information security posture through lessons learned and continuous improvement.

1. Information security aspects of business continuity management

Detection and Reporting:

- Detection: Implement monitoring and detection tools to identify potential incidents.
- Intus Healthcare’s IT estate is continually monitored by our IT Team.

Reporting:

- Establish procedures for reporting incidents. Employees must report any suspected incidents to the Leadership Team immediately.
- All staff report IT issues to our IT support company.

Classification and Prioritisation:

- Classification: Assess and classify incidents based on their severity and potential impact.
- Prioritise incidents to ensure that the most critical incidents are addressed first.

Incident Analysis:

- Initial Analysis: Conduct an initial analysis to understand the nature and scope of the incident.
- Detailed Analysis: Perform a detailed analysis to identify the root cause and affected systems or data.

Containment:

- Immediate Actions: Take immediate steps to contain the incident and prevent further damage.
- Short-term and Long-term Containment: Implement both short-term and long-term containment strategies as necessary.
- Eradication: Identify Malicious Activity: Identify and remove any malicious activity or artifacts from affected systems.
- Vulnerability Mitigation: Address vulnerabilities that were exploited to prevent recurrence.

Recovery:

- System Restoration: Restore affected systems and services to normal operation.
- Validation: Validate that systems are secure and functioning correctly before returning to production.

Post-Incident Activities:

- Documentation: Document all actions taken during the incident response process.
- Lessons Learned: Conduct a post-incident review to identify lessons learned and areas for improvement.
- Security controls and recommendations should be made to the Leadership Team
- Reporting: Report the incident to relevant stakeholders and, if necessary, to regulatory authorities, such as
    - Information Commissioner's Office (ICO) (Cyber Attacks)
    - CQC
    - FCA
    - MHRA
    - National Cyber Security Centre (NSCS)
    - Action Fraud
    - Police
    - Intus Healthcare’s insurance company

Note - this list may not be exhaustive, and dependant on the actual incident additional stakeholders or regulatory authorities may need to be notified.

2. Communication

- Internal Communication: Ensure clear and timely communication among Leadership and IT Teams and affected parties.
- External Communication: Manage communication with external stakeholders, including customers, partners, and regulators, as necessary.

3. Training and Awareness

- Incident Response Training: Provide regular training to relevant personnel on incident response procedures.
- Awareness Programs: Conduct awareness programs to educate employees on how to recognise and report information security incidents.

Compliance and Continual Improvement

- Regularly review and ensure compliance with relevant legal, regulatory, and contractual obligations.
- Conduct internal and external audits to verify adherence to this policy
- To take appropriate action in the event of any breach, this may include taking disciplinary action against the individual(s) concerned up to and including dismissal from the company and possible criminal and/or civil litigation.
- Regularly review and update the information security policy and procedures to address emerging threats and changes in the organisational environment.

Reporting

If you suspect a security breach, you are required to report it to the leadership team immediately. Please retain any documents to support your suspicions.

Review of this document: annually by Operations Manager.

Next review date: February 2026.

This policy will be reviewed annually and updated as necessary to ensure its relevance and effectiveness in safeguarding our organisation's information assets.