Information Security Policy

Inmind Reference:	GDPR01
Category:	General Data Protection Regulation (GDPR) Policy
Version Number:	1.3
Reviewed on:	January 2018
Next review date:	January 2019
Lead Officer:	GDPR / Director of Contract Performance
Equality Impact Assessment completed:	Yes

Applicable Legislation/Regulations:
NHS Information Security Policy Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 Information Commissioners Office (ICO) General Condition 21 – NHS Standard Contract – Patient Confidentiality, Data Protection, Freedom of Information and Transparency NHS Digital
Codes of Practice:
NHS Information Risk Management – Digital Information Policy
Purpose:
The purpose of the policy is to ensure that Inmind has practical measures in place to support its compliance with the Data Protection Act and such extensions to the scope of that act as are covered by the recommendations of the Caldicott Report (1997) and to ensure that Inmind's information and IT assets are to be made secure and protected from harm from whatever source. It is intended to safeguard that the interests of Inmind's Service Users and employees by protecting them from access to unsuitable material access through Inmind's IT systems and to protect the company's own interests. It also sets out the steps which must be undertaken in the case that there is any actual, suspected or possible breach of security. The aim of the policy is to ensure the security and confidentiality of all information assets, information systems, applications, networks and hardware owned or controlled by Inmind. This will be achieved by: ➢ Ensuring that all employees are aware of and comply with relevant legislation and principles ➢ Ensuring that IT Department employees understand the need for security and confidentiality of data and that a culture of security is developed and enhanced. Inmind will take seriously any actual, attempted or suspected infringement of the policies in this and other documents, and may take disciplinary action against any employee acting or attempting to act in breach of them.

Version Control Table		
Date Ratified	**Version Number**	**Status**
Jan 2018	1.3	Live

Date	Key Revision
Jan 2018	Change in CQC Regulation and Regulated Activity from the original policy
Jan 2018	Updated information throughout policy to reflect new guidelines

Please check to ensure this is the most current electronic copy of this document as it is updated and published in electronic format only (hard copies may become out of date).

1.0 The Policy

1.1 This document sets out Inmind Healthcare Group's (Inmind) Information Security Policy. It contains the policy and practical information relating to Asset Management, Access Control, Network Security, New Systems, Mobile Computing and Information Security Event reporting/management.

Whilst the separate policy document "IT Acceptable Use Policy (AUP)" is targeted at all of Inmind's IT users, this document is seen as complementary to it and provides details of the underlying policy and the environment on which the AUP is based.

This document is therefore aimed primarily at the IT Department, who are responsible for providing the necessary tools and controls to enable the requirements of the AUP to be satisfied.

Members of the IT Department are also bound by the AUP and the provisions of this document are considered supplementary to and not replacing the provisions of that document. This document does not intend to restate the provisions of the AUP except insofar as it describes the manner in which the technical aspects of that policy are brought about.

1.2 The Scope

This policy and procedures apply to all information, information systems, networks & applications at all Inmind establishments, to all Inmind employees and system users and to any third party Service Providers used by Inmind.

In this document the term 'employees' is understood to mean Inmind permanent employees and any contracting or temporary employees or service providers.

1.3 Responsibilities

- Responsibility for Information Security lies with the Senior Information Risk Officer (SIRO) and the IG Steering Group.
- Responsibility for implementation and maintenance of this policy lies with the IT Manager / Information Security Manager.
- Responsibility for the security of specific IT and Information Assets lies with the designated owner of the asset.
- Responsibility for the practical implementation of the policies in this document lies with individual members of the IT Department charged with carrying out specific tasks.
- Responsibility for management of Security events varies depending on the nature and severity of the incident. For low-level incidents, such as software malfunctions, these may be managed at the IT Helpdesk level. For more serious events, the IT Manager, Caldicott Guardian or SIRO may take responsibility. The procedure for Information Security Event Reporting and Management is detailed below in the relevant section.

2.0 The Procedure

2.1 General Principles

Inmind's right of access to data and systems: Inmind retains the right to access and monitor any and all data on any of its systems and in any and all of the applications on those systems. It furthermore retains the right to make use of monitoring and auditing software to support this right.

Minimise security burden: Security measures should be as simple and transparent to users as is possible commensurate with the threat they are intended to combat. For example, the fewer IDs and passwords a user must remember, the less the risk that they will have to write them down.

Maximise use of automated central security controls: Inmind promotes the use of Microsoft Active Directory for its sites and for access to its mail servers. Where possible, automated processes should be used to ensure (for example) that user passwords are changed on a periodic, systematic basis and that passwords conform to the company's standards.

Lowest level of access: All system users, especially those in the IT Department shall access systems with the lowest level (i.e. least functionality) of access commensurate with carrying out the specific task. IT system users who require elevated access to systems for specific purposes shall use that access only when they are actually carrying out some function which requires this form of access and as soon as the task is finished, must sign off and revert to normal access. In addition, any vendor-provided IDs and default passwords which are set when software is delivered or installed shall be removed or disabled before the system commences use.

Asset ownership: All information assets have designated owners who are responsible for preserving the integrity and security of those assets for which they are responsible.

2.2 Backup and Recovery

All data contained on Inmind's in-house systems will be backed up as often as necessary to ensure that the business of Inmind is not significantly disrupted by failures within a system. All backups are held in a fireproof media safe. Need to check that this is correct – it is at variance with the Data Protection Policy that states that backup media is stored in fire safes

Backup procedures shall be tested periodically on a random basis, but with no longer than 3 months between tests. This will consist of carrying out a restoration of random files to a designated directory. These tests will be carried out by Inmind's nominated IT Services subcontractor and the results made known during Service Support Meetings.

Only IT Department employees or their nominated sub-contractors may undertake restoration of data.

2.3 Acceptable Use

Inmind expects all its employees to use computers reasonably and for the purposes only of Inmind's business. All users of Inmind computer systems must note that the Computer Misuse Act 1990 makes it a criminal offence for an unauthorized person to illegally access, attempt such access or misuse a computer. Monitoring acceptable use: Inmind may implement and monitor IT systems usage through software which will:

- Monitor internet access made from any of its computers, whether these are used in- house or as part of its mobile inventory
- Capture, store, index and retain all email traffic through its servers
- Ensure that only properly licensed software, acquired by Inmind is deployed on its systems in accordance with the licence conditions.
- Prevention of software installation: Inmind will further restrict end-user modification of systems by using security settings which:
- Prevent installation of any software other than by authorised, qualified IT employees acting with proper authority
- Prevent user access to computer settings and hardware configurations and these shall only be modified by authorised, qualified IT employees acting with proper authority
- Where possible, Inmind will prevent access to unsuitable web sites.

2.4 Anti-Virus

Inmind will maintain antivirus software on all systems which are potentially subject to attack. The IT Department (or IT Services Subcontractor) will ensure that regular updates are being received.

For all in-house systems connected to the network, this will be kept up to date and refreshed as often as new data is received from the anti-virus software provider. For mobile systems, connecting to the Inmind network or direct to the internet will automatically trigger an update to the latest version.

Anti-Virus – Treatment of e-Mails: Since end users are not permitted under Inmind policy to install software on their systems, any emails containing executable files are to be isolated and quarantined automatically. This provision includes files with the extensions .exe, .bat, .scr, .vbs, .eml. Receipt of such files are treated as a security event and reported accordingly. As this is not a normal method of distributing software upgrades and fixes, even if the file appears to come from a safe source it will be treated with suspicion.

Anti-Virus Alert: From time to time, warnings are issued of potential internet exploits which may require special attention (e.g. major denial of service or bot attacks). In this case, Inmind will obtain advice from their AV Software provider as to the best methods of avoiding adverse effects and put these into action.

Anti-Virus Action: When a virus alert occurs on a computer, the computer will be turned off and isolated from the network. The IT Department's responsibility in this case is to:

- Verify the existence of the virus
- Identify the source of the virus
- Determine the spread of the virus internally and externally
- Obtain the risk assessment of the virus from the AV Software Provider
- If necessary, disable the WAN until the virus has been eliminated
- Cleanse all infected computers
- Warn any external parties who may have been affected

A Security Incident report shall then be completed.

If it is suspected that the virus was introduced maliciously then a report is to be submitted to the IT Manager detailing the circumstances and effects upon Inmind business practice.

2.5 Data Encryption

Inmind will provide a facility to encrypt files sent by e-mail or transportable media, which are of sufficient strength to resist attacks by non-specialised agencies. This is currently considered to be 256-bit encryption.

At present, given Inmind's network security controls there is no requirement for any in- house data to be encrypted. Any confidential information sent by email is only to be sent only once it has been encrypted.

Any removable data storage devices which are used to transport confidential information must have their data encrypted.

Any confidential information held on portable devices must be encrypted. If the data cannot be encrypted to a sufficient standard, it must not be taken offsite.

Only Mobile (smart) phones supplied by Inmind and under their control are not to be used for corporate e-mails as these fall outside of the control of Inmind IT.

2.6 Business Continuity / Disaster Recovery

The IT Department will, in conjunction with other departments, develop, maintain and periodically test a Business Continuity / Disaster Recovery plan. This will identify, assess and evaluate possible incidents and their effect on Inmind and its operations. The plan will be developed by the IT Manager and will be updated whenever there is a material change in the circumstances of the business (e.g. new premises).

2.7 New Systems

All new systems shall be subject to approval by the IG Committee, who shall ensure that any new information systems, applications and networks shall be subjected to a risk assessment to determine the security controls required.

This evaluation will include, but not be limited to the requirements for:

- Physical security
- Modes of access and network security
- User access permissions and the associated approval processes
- Disaster recovery
- Administration responsibility

No new system can be put into operation until the plan produced as a result of the risk assessment has been approved by the IG Committee. In addition, and where appropriate, the IG Committee shall ensure that the impact of any new system on the company's Confidentiality and Data Protection Policies is assessed and have developed guidelines for a Privacy Impact Assessment to support this requirement.

2.8 Access Control

Access to any of Inmind's IT facilities or data is restricted to authorised users only. All access to systems and data will be controlled by means of password-controlled accounts which will be issued to authorised users only.

Maintenance of software and hardware related to access control will be carried out by members of the IT Department or authorised vendor employees under the supervision of members of the IT Department. All changes and updates will be risk assessed in advance and a record of changes will be maintained which will include the names of those responsible and dates undertaken.

These accounts will be maintained in a security environment and where available, based on Microsoft's Active Directory (AD). This will be maintained in a manner which is sufficiently granular as to allow users to be allocated just such access rights as they need to carry out their responsibilities. Access to the AD change facilities is restricted and limited to named individuals with security responsibility.

This approach allows the minimisation of the number of IDs and passwords required. In general, a user will have one ID and password for e-mail and one which is used to access data to which they have legitimate access.

New accounts: If a new ID is required for a new or temporary employee, this will be processed as part of the induction process and the request will come from head office. A new user is allocated appropriate access through AD and be provided with an ID and a password as set by the IT department.

Application/Data Access: Authorisation to use an application or access specific data is controlled and users will be granted access only to such applications and data as

they require to carry out their duties. Asset owners will be responsible for gaining and granting approval for such access on request when they are satisfied of the need to do so. When applications offer the facility to create different levels of user (e.g. 'Administrator', 'User') this will be used and system users are granted the lowest level of access commensurate with being able to carry out their duties.

Account modification: Requests for changes if a system user (including IT employees) requires changes to their access (for example, access to a new application), then a request, agreed by the function manager or head office will be received. If this is in order the change will be made by the IT department.

Retirement and Deletion of accounts: As soon as an employee leaves Inmind's service, or in case of severe disciplinary matters as soon as the IT Department is notified of the requirement, access to the account associated with the person will become restricted such that only IT Department employees can have access. The account will not normally be deleted until one calendar month after the departure of the employee to allow any transfer of data or similar activities have been completed. In extenuating circumstances, the account may be retained indefinitely if an appropriate business case is raised.

IT users may need to have more than one form of access in that they may require a normal security level ID for day to day tasks, but an elevated access for systems maintenance purposes. It is mandatory that such elevated access is used ONLY when such tasks are actually being carried out. In all other respects, the elevated account maintenance is subject to the same restrictions as a normal account. Passwords will be maintained according to the rules set out in the Acceptable Use Policy.

Forgotten passwords: If a password is forgotten, a new temporary password may be requested from the IT Department. This will be issued only once it has been determined that the requestor is the correct person associated with the ID for which the password is to be issued. The password issued will be capable of allowing a single access to the system for the purposes of setting up a new password.

Compromised password: If a user has reason to believe that their access has become compromised by exposure of a password, a new password is to be issues, and the incident recorded as a Security Event.

2.9 Network Security

Access to all of Inmind's networks is restricted to authorised users. Any access is only granted after a risk assessment and approval from the IT Manager. In general, no third party equipment shall be attached to Inmind's network. If, for maintenance or upgrade reasons, it becomes necessary to connect non-Inmind owned hardware to Inmind's network, a risk assessment should be carried out. The following courses of action are to be considered:

- Can the task be undertaken by disconnecting and Inmind hardware affected from the network?

- Can the task be undertaken on a sub network isolated by firewalls and other security from the rest of the network?
- Can the work be carried out at times when adverse outcomes (i.e. system or network failure) will have least effect?
- Can all Inmind data (or at least confidential data) be isolated from the non-Inmind device?

Before any connection is permitted, it is essential that:

- The third party company has formally agreed in writing to accept Inmind's terms of security and confidentiality.
- The IT Manager has given explicit agreement and permission to the connection.

2.10 Physical Security

Access to any IT assets which do not require physical access by end-users will be restricted to just those employees (normally IT Department employees only) who need such access. All assets, such as servers, routers and similar items will be kept in secure facilities.

Access to such facilities must be strictly controlled and only named individuals will be permitted access. The types of location which require access restrictions of this nature include:

- Server rooms
- Communications rooms
- Communication Cabinets
- Rooms containing patch panels
- Rooms containing switches, routers, firewall hardware machines
- Any other rooms containing IT hardware which does not require end-user access.

The IT Manager is responsible for ensuring that there are suitable environmental controls in place for server and network equipment assets (UPS, air conditioning, fire suppression etc.) Where possible, hardware assets will be physically secured in their environment. For example, servers and communications device may be physically placed in a rack and secured with locking devices.

2.11 Firewalls

All Inmind networks will have firewall protection separating them from other networks of differing levels of trust. Firewalls will be used at all interfaces between networks.

Inmind may monitor internet activity with the use of firewall software/hardware and internet web monitoring software, which provides reports of Internet usage. This will operate in a bi-directional manner, thus protecting data held on Inmind servers from unauthorised remote access (hackers).

A copy of all firewall rule-sets will be maintained by the IT Department or their nominated subcontractors.

All firewall rule changes will be subject to a risk assessment (where appropriate) and change-control procedures.

Access to firewalls is restricted to a limited number of individuals. Any request to gain access to a firewall must be approved by the IT Manager.

Internet access is provided only for business-related purposes. Internet access is not provided for private use.

2.12 Remote Access

Remote access is achieved through PC Anywhere and Remote Desking and is intended for senior management and IT Administrators only. No remote access facilities are provided for normal users.

All users provided with remote access capability are authorised by the IT Manager.

2.13 Wireless Networks

Wireless networks are intrinsically less secure than hard-wired networks and have the potential for being attacked either for illegitimate use or for accessing information assets. All wireless networks that allow access to Inmind's corporate network will use WPA authentication and TKIP encryption.

2.14 Mobile Computing

Mobile computing whether from laptop computers, smart phones or other devices capable of storing and / or processing information presents risks and areas of concern in addition to those which apply to in-house systems. All provisions which apply to in-house systems apply equally to laptops and other mobile devices. For example, accounts set up on laptop systems are not to give access to system settings, such as BIOS settings, or allow installation of software by non-IT employees. Random periodic checks of software and data on laptops may be undertaken and recorded in an audit log.

It is understood that mobile users may need to access the Internet and email for personal reasons while travelling. Any Infringement of existing corporate IT policies to include non- appropriate Internet and email usage may be subject to disciplinary procedure.

Mobile devices (i.e. Laptops and Blackberries) are not to hold original versions of data and as a result there are no facilities provided to back up these devices. Any data is to be stored on the appropriate company servers with only off-line copies held locally only on a mobile device, synchronised whenever possible with a parent server.

2.15 Asset Management

New assets:

Requests for new assets will initially be passed to the IT Manager for evaluation and approval. All IT assets purchased will be recorded. On receipt, the asset details (e.g. Item number / Licence number) will be recorded in an asset register.

A register of each hardware asset will be maintained. NOTE: Normally, a PC, or router or similar device will count as 'a hardware asset' rather than, for example a keyboard, or a graphics card unless there is something special or unusual about it. Details of software loaded onto each computer will be maintained. Each asset, whether hardware or software, will be allocated an 'owner', who will be personally identified and who will be responsible for the day-to-day security and maintenance of the asset.

Information Systems Assets:

The nominated owner of each Information System Asset is responsible for:

- Documenting the access control processes and the associated access approval process for the asset.
- Conducting a periodic risk assessment on the asset to a programme dictated by the Information Security Manager in accordance with the Risk Management Policy.

Audit of assets:

A regular audit of information assets will be conducted.

Maintenance of assets:

Only the IT Department or their nominated subcontractors are permitted to carry out maintenance of information assets. Faults will be reported by users to the IT Helpdesk via Email or by Telephone. These may consist of (but not be limited to) network access faults, internet access problems, hardware failure, operating system failure.

No action will be taken on faults until officially reported to the Helpdesk, unless the fault is of a severe nature (e.g. server failure). The IT Department will endeavour to clear major problems with 24 hours. For lesser reported faults, the IT Department will endeavour to repair problems within 5 working days. If the delay to resumption of service is likely to be longer, the IT Department will inform the relevant people involved.

Disposal of Assets:

When IT hardware has reached the end of its useful life or is beyond economical repair then arrangements are to be made, by the IT Department, with a reputable

source for collection and disposal of such equipment. The authority of the Information Security Manager is to be obtained before disposal.

A certificate of destruction is to be obtained from the disposal company. This certificate is to be retained on file by the IT Department.

The Asset Register is to be amended to identify the disposal of the equipment.

In the event of a computer being disposed of all software is to be removed. Where the licence permits the software may be re-used or stored for future use. OEM software will be disposed of with the computer as these licences are non-transferable.

Prior to disposal all data is to be removed and the hard disk low level formatted.

2.16 **New Information Systems**

The IT Manager will ensure that all new information systems, applications and networks will be subjected to a risk assessment to determine the security controls required.

This evaluation will include, but not be limited to the requirements for:

- Physical security
- Modes of access and network security
- User access permissions and the associated approval processes
- Disaster recovery
- Administration responsibility

No new system can be put into operation until the plan produced as a result of the risk assessment has been approved by the IT Manager.

In addition, and where appropriate, the Information Security Manager will ensure that the impact of any new system on the company's Confidentiality and Data Protection Policies is assessed and has developed guidelines for Privacy Impact Assessments to support this requirement.

2.17 **Information Security Event Reporting and Management**

Security Events: All information security events will be recorded using the Incident Report (See AUP Policy). This sets out the details of an incident. All incidents that constitute and actual or potential loss of information, which could potentially lead to a breach of confidentiality, are to be reported directly to the SIRO and Director of Governance and Compliance. It is important to note all breaches must be reported to the SIRO / IG Lead / Caldicott Guardian and the Management of Serious Untoward Incidents process will be enacted, where applicable.

See Appendix 1 – Risk Assessment Matrix for further detail.

The following table sets out who will be informed depending on the type of incident:

Event Description	IT Helpdesk	IT / Info Security Manager	Caldicott Guardian	SIRO
Software malfunction	✓			
Damage to information due to flood, fire or other environmental reason	✓	✓	✓	✓
Loss or theft ofcomputer or mobile computing device (including laptop)	✓	✓	✓	✓
Loss or theft ofportable media (CD, DVD, USB memory stick)		✓	✓	✓
Unauthorised disclosure of confidential personal information		✓	✓	✓
Virus	✓	✓		✓
Corruption ofelectronic information	✓	✓	✓	✓
Unauthorised changes to personal information		✓	✓	✓
Faxed information received outside Safe Haven		✓	✓	✓
Confidential information left on photocopier		✓	✓	
Unauthorised access to locked drawer /cabinet		✓	✓	
Suspicion of computer misuse		✓	✓	✓
Loss of service availability	✓			
Window left open in unattended office on ground floor		✓		✓
Loss of password (compromised)	✓	✓	✓	✓
Loss of password (not compromised)	✓			

This is not considered to be a definitive or exhaustive list.

When an incident is reported, the IT Department carries out an immediate risk assessment to determine:

- Is there a continuing risk?
- How severe is the risk? (it is better to overestimate severity rather than the reverse)
- Are there any health and safety issues raised by this incident?
- What kind of breach of security (confidentiality / integrity / availability) has occurred?

The result of this analysis will be recorded.

Where appropriate, the IT Manager and Caldicott Guardian will undertake prompt investigation and risk assessment for each reported event and implement appropriate controls to address the risk.

Appendix 1

Equality Impact Assessment for this policy

Protected Characteristic (domain)	Area of conflict	Resolution
Age	Nil	N/A
Disability	Nil	N/A
Gender Reassignment	Nil	N/A
Pregnancy & Maternity	Nil	N/A
Race	Nil	N/A
Religion or Belief	Nil	N/A
Sex	Nil	N/A
Sexual Orientation	Nil	N/A
Marriage and Civil Partnership	Nil	N/A

All relevant persons are required to comply with this policy and must demonstrate sensitivity and competence in relation to diversity in race, faith, age, gender, disability and sexual orientation. If you feel you are disadvantaged by this policy, please contact the Registered Manager and the service will actively respond to the enquiry.