# Information Security and Risk Assessment Policy (N-051)

| | |
|---|---|
| Version Number: | 3.06 |
| Author (name & job title) | Richard Brumpton<br>Head of Information Technology |
| Executive Lead (name & job title): | Peter Beckwith<br>Director of Finance/SIRO |
| Name of approving committee: | Information Governance Committee |
| Date approved: | 22 September 2020 |
| Date Ratified at Trust Board: | 28 March 2017 |
| Next Review date: | December 2023 |

Policies should be accessed via the Trust internet to ensure the current version is used.

## Contents


1. INTRODUCTION....3
2. SCOPE....3
3. POLICY STATEMENT....3
4. DEFINITIONS....3
5. DUTIES AND RESPONSIBILITIES....4
   5.1. Chief Executive....4
   5.2. Director of Finance....4
   5.3. Senior Information Risk Owner....4
   5.4. Head of Information Governance and Legal Services....4
   5.5. Head of Information Technology....5
   5.6. Information Governance Officer....5
   5.7. Privacy Officer....5
   5.8. Information Asset Owners....5
   5.9. Information Asset Administrators....6
   5.10. All Staff....6
6. PROCEDURES....6
   6.1. Physical Security....6
   6.2. Mobile Devices....7
   6.3. Viruses and Malware....7
   6.4. Use and Installation of Software....7
   6.5. Access Controls....7
   6.6. Network and Infrastructure....8
   6.7. Data and Information Backup....8
   6.8. Incident Reporting....8
7. EQUALITY IMPACT ASSESSMENT....8
8. BRIBERY ACT....8
9. IMPLEMENTATION AND MONITORING....9
10. REFERENCES/EVIDENCE/GLOSSARY....9

Appendix 1: Document Control Sheet Template....10

Appendix 2:Equality Impact Assessment (EIA) Toolkit....12

## 1. INTRODUCTION

The purpose of this policy is to protect, to a consistently high standard, all information assets, including patient records and other Trust corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

The Trust will apply core principles of risk assessment and management by identification and quantification of information security risks in terms of their perceived severity of impact and the likelihood of occurrence.

This policy should be read in conjunction with other Trust policies specified in section 12.

## 2. SCOPE

The Information Security and Risk Policy applies to all members of staff; to Trust and Social Services staff who are seconded to the Trust, contractors, temporary and agency staff, students and other staff.

The Information Security and Risk Policy applies to information, information systems, networks, physical environment supporting the Trust's business functions and to the relevant people who support those business functions. This policy applies to all electronic and manual information systems.

## 3. POLICY STATEMENT

This policy correctly applied and adhered to, will achieve a comprehensive and consistent approach to the security management of information throughout the Trust, ensure continuous business capability and minimise both the likelihood of occurrence and the impacts of any information security incidents.

The objective of this policy is to ensure the security of Trust primarily information assets, to ensure:

- Confidentiality - to preserve the confidentiality of all information.
- Integrity - the accuracy and completeness of information and processing to ensure confidence in the authenticity of the information.
- Availability - that authorised users have access to information and associated assets when required.

The aim is to ensure that Trust information systems, applications and networks are available when required, they can be accessed only by legitimate users and contain complete and accurate information. Furthermore, information systems, applications and networks must also be able to withstand or recover from threats to their availability, integrity and confidentiality.

## 4. DEFINITIONS

| | |
|---|---|
| Risk | The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood. |
| Consequence | The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event. |
| Likelihood | A qualitative description or synonym for probability or frequency |
| Risk Assessment | The overall process of risk analysis and risk evaluation. |
| Risk Management | The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects |

| | |
|---|---|
| Risk Treatment | selection and implementation of appropriate options for dealing with risk. Conceptually treatment options will involve one or a combination of the following; avoid the risk, reduce the likelihood of occurrence, reduce the consequence of the occurrence, transfer the risk, retain/accept the risk. |
| Risk Management Process | The systematic application of management policies, procedures and practices to tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. |

## 5. DUTIES AND RESPONSIBILITIES

### 5.1. Chief Executive

The Chief Executive as Accountable Officer has overall accountability and assurance, through the Statement of Internal Control that all information security risks to the Trust are effectively managed and mitigated.

### 5.2. Director of Finance

The Director of Finance will be the senior manager with Board level responsibility for information security. The Director of Finance is the Senior Information Risk Owner (SIRO).

### 5.3. Senior Information Risk Owner

- Act as an advocate for information security risk and provide written advice to the Accountable Officer on the content of their annual Statement of Internal Control in regard to information security risk.
- Receive training as on an annual basis to ensure they remain effective in their role as Senior Information Risk Owner.
- Review and agree actions in respect of identified information security risks.
- Ensure the Trust's approach to information security risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.
- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS Information Governance requirements.
- Ensure that there are effective mechanisms in place for reporting and managing Serious Incidents (SIs) relating to the information of the Trust. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.
- Ensure new or proposed changes to Trust processes or information assets that have been identified have information security, confidentiality and data protection, and information quality requirements defined at an early stage of the project.

### 5.4. Head of Information Governance and Legal Services

- Ensure the development and maintenance of appropriate policies and procedures that demonstrate commitment to and ownership of information security responsibilities.
- Ensure that annual assessments and improvement plans are prepared for approval by the Information Governance Committee in a timely manner.
- Ensure that all staff have ready access to Trust policies, procedures and Guidance documents and know where to go for advice when needed.
- Ensure any security issues are reported to the Senior Information Risk Owner (SIRO).
- Ensure Information Asset Owners are identified in each Trust Department and ensure that they are briefed in their responsibilities.
- Monitor and maintain the Trust Information Asset Register.

### 5.5. Head of Information Technology

- Protect all hardware, software and information assets under their control. This will be achieved through the implementation of a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its assets.
- Take preventative steps to stop staff from downloading and installing software utilities and applications from the internet without the consent of the IT Service Desk.
- Carry out security risk assessment(s) in relation to all the business process covered by this policy. These risk assessments will cover all information systems, applications and networks that are used to support those business processes. The risk assessment will identify the appropriate security controls required to protect the information systems.
- Ensure that all users of the system are made aware of the contents and implications of relevant system security policies and security operating procedures.
- Ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. All staff to be made aware that irresponsible or improper action will result in disciplinary action(s).
- Ensure that all newly developed information systems, applications and networks are approved by the Information Programme Board before they commence operation.
- Ensure that measures are in place to detect and protect information systems, applications and networks from viruses and other malicious software.
- Ensure that all connections to external networks and systems have documented and approved system security policies and that all connections to external networks and systems are approved before they commence operation.
- Ensure that operational applications, systems and networks are monitored for potential security breaches. Security incidents, whether actual or suspected, must be reported and investigated in accordance with the requirements of the Trust's incident reporting procedures. The IT Service Desk will remind staff of this fact when notified of any occurrences which may be considered a reportable incident. A summary of IT security incidents will be recorded by means of an Information Security Incident Log which will be provided to the Information Governance Committee on a quarterly basis.
- Ensure that there is an effective configuration management system for all information systems, applications and networks.
- Ensure that contingency plans and disaster recovery plans are produced for all critical applications, systems and networks.
- Adhere to the information security policies of other health organisations and local authorities that may share information processing facilities such as wide area networks.

### 5.6. Information Governance Officer

Provide security awareness training for staff as stated in the Information Governance Training Policy to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities.

### 5.7. Privacy Officer

Provide an audit of clinical systems as requested to support evidence gathering in relation to investigations of security incidents, data breaches, or complaints.

### 5.8. Information Asset Owners

- Act as nominated owner of one or more information assets of the Trust.
- Identify Information Asset Administrators to assist them with their duties, where this is appropriate and necessary.

- To complete a System Level Security Policy and Risk assessment to document, understand and monitor what information assets are held, for what purpose, how information is created, amended or added to, who has access to the information and why.
- To ensure that systems meets the Trusts information security standard.
- Identify information necessary in order to respond to incidents or recover from a disaster affecting the information asset.
- Take ownership via input to the Trusts Information Asset Register of their local asset control, risk assessment and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks.
- Provide support to the Trust's Senior Information Risk Owner to maintain their awareness of the risks to all information assets that are owned by the Trust and for the Trust's overall risk reporting requirements and procedures.
- Ensure that relevant staff are aware of and comply with expected Information Governance working practices for the effective use of owned information assets.
- Provide a focal point for the resolution and/or discussion of risk issues affecting their information assets.
- Ensure that the Trust's requirements for the information incident identification, reporting, management and response apply to the information assets they own.
- Ensure new or proposed changes to Trust processes or information assets are identified and flagged with the Senior Information Risk Owner so that information security, confidentiality and data protection, and information quality requirements are defined at an early stage of the project.
- Undertake training in information risk management every two years.

### 5.9. Information Asset Administrators

- Where these have been indentified by the Information Asset Owners assist them in the day to day management of information assets, identifying and reporting any information risks as and when they arise.
- Ensure that policies and procedures are followed.
- Consult their Information Asset Owner on incident management.

### 5.10. All Staff

All staff (Trust staff, Social Services staff who are seconded to the Trust, contractors, temporary and agency staff, students and other staff) have a responsibility to protect information, systems and networks by following the procedures in this policy and the relevant Trust policies and guidance specified in section 11.

## 6. PROCEDURES

The Trust will provide specific guidance and instruction to staff in the relevant policies and procedural documents. For example security of personal information is explained in the Safe Haven Procedure and the Confidentiality: Code of Conduct.

Users breaching this requirement may be subject to disciplinary action.

Some key areas of information security and risk management are listed below:

### 6.1. Physical Security

The physical environment must be recognised as providing a layer of protection to data and information. This is achieved by the following means:

- Controlling access to sites, buildings and offices.
- Ensuring desks and work areas are clear at the end of each day.
- Use of locked cabinets within offices to restrict access to information.

- Checking that visitors to sites are authorised to be there.
- Ensuring that when information is carried off site, it his held securely in a locked case.
- Always wearing your ID badge when on Trust business.

For more in depth information in this area refer to the Trust's policy for Physical Security of Premises and Other Assets.

### 6.2. Mobile Devices

- Portable devices and removable media must be encrypted.
- Unencrypted electronic media must not be used to transport personal data. The use of unencrypted media must be approved by the SIRO, the use would be based on the risk assessment of the use of the media.

### 6.3. Viruses and Malware

The Trust will use software countermeasures and management procedures to protect itself against the effects of malicious software. All staff will be expected to co-operate fully with this requirement. See section 3.7 Electronic Communications and Emailing Acceptable Use Procedures.

### 6.4. Use and Installation of Software

- No computing equipment is to be procured or connected to any Trust network without the agreement of the IT Services.
- All computer software used by the Trust is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).
- Security issues must be considered and documented during the requirements phase and the procurement phase of all system procurements and developments. Minimum security standards will be incorporated in all new systems.
- New operational software should be quality assured. System test and live data should be separated and adequately protected.
- It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach of the licence agreement.
- Employees must not load software onto their computer before first seeking advice/agreement from the IT Services.

### 6.5. Access Controls

Access to all Trust PCs will be via a user name and password. The Trust password policy is in line with National Cyber Security Centre (NCSC) guidelines and will be enforced by Group Policy.

Passwords will be valid for 365 days and must meet the following criteria:

- Length: 10 characters (minimum)
- Complexity: A mix of character types is NOT required
- Reuse: Not matching previous 4 passwords
- Account Lockout: 5 minutes, after 10 failed attempts

Staff are advised to choose strong passwords. A good way to create a strong easy to remember password is to choose three random words that are memorable to you, but do not choose obvious easily guessed words eg names of children/family or pets etc. Do not use common passwords e.g. Password123, Summer2018. Passwords will be validated against a database of known/weak passwords.

Systems will automatically lock out after 10 minutes if there has been no activity on the PC.

Further access controls to patient and staff data bases will need appropriate security controls. These maybe either;

- Active Directory usernames and passwords
- System specific usernames and password
- Or via the use of smart cards.

Smartcard Access will be authorised and managed in line with the NHS Digital registration authority requirements see Registration Authority Policy.

System using specific usernames and passwords must ensure that they follow the minimum security requirements that match the policies applied to Active Directory.

All staff have access to remote working (VPN). Remote access is granted in line with the internal IT Good Practice Guide and Standard Operating Procedures

### 6.6. Network and Infrastructure

All network management controls and procedures will conform to the NHS wide national guidance from NHS Digital.

### 6.7. Data and Information Backup

Sensitive information should not be permanently stored on individual computers, either in folders on the device or in email accounts. Follow the Safe Haven Procedure.

Data located upon network servers will be backed up in accordance with the internal IT Good Practice Guide and Standard Operating Procedure.

The purpose of the system backups is to enable recovery of service due to a total loss of the servers. It is not a backup to archive data for audit or legal purposes – data required for audit/legal purposes should be retained in line with advice given in the appropriate Trust policies.

### 6.8. Incident Reporting

Arrangements for reporting information security incidents are detailed in the Trust's Risk Management Strategy. The investigation of incidents will follow the Guide to the Notification of Data Security and Protection Incidents

All incidents should initially be reported to the Senior Information Risk Owner and the Trust's Information Governance Team who will then assess the incident level. All reportable incidents must be reported to the Information Commissioners Office within 72 hours of notification via the IG Incident Tool on the Data Security and Protection Toolkit.

IT specific incidents must be reported to the IT Service desk as soon as happen (It services desk is available 24/7)

These arrangements will be regularly reviewed by the Information Governance Group.

## 7. EQUALITY IMPACT ASSESSMENT

An Equality and Impact Assessment has been carried out and no relevance has been identified against the general and specific duties of the current equalities legislation.

## 8. BRIBERY ACT

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act

are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

## 9. IMPLEMENTATION AND MONITORING

This policy will be disseminated by the method described in the Implementation section of the Policy and Procedural Documents Development and Management Policy. The implementation of this policy requires no additional financial resource.

- A quarterly summary report of all incidents relating to information security will be presented to the Information Governance Committee. The information in the
- report will be sourced from any serious untoward or adverse incidents reported through the Trust's Risk Management process and the IT Servicedesk.
- The monetary penalties from the ICO cross referenced to the controls in place to prevent a similar incident in the Trust.
- CareCERT alerts from NHS Digital that are monitored by IT Services.
- Unresolved incidents will be logged and monitored via the Trust's Risk Register.

## 10. REFERENCES/EVIDENCE/GLOSSARY

Associated Trust Policies and Procedures, namely

- IT Good Practice Guide and Standard Operating Procedures
- Records Policy
- IG and IT Forensic Investigation Procedure
- IG Incident Reporting Process
- Registration Authority Policy
- Safe Haven Procedure
- Confidentiality: Code of Conduct
- Records Management and Lifecycle Policy
- Electronic Communication and Internet Acceptable Use Procedure
- Information Governance Training Procedure
- Caldicott and Data Protection Policy
- Data Quality Policy

Associated legislation and guidance, namely:

- Department of Health information Security Management: NHS Code of Practice. April 2007
- NHS Digital Information Governance Toolkit
- Checklist Guidance for Reporting, Managing and Investigation Information
- Governance and Cyber Security Incidents Requiring Investigation
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974 (Computers)
- Copyright Designs and Patents Act 1988
- General Data Protection Regulation (EU) 2016/679
- Data Protection Act 2018

There is also an obligation for the Trust and the Humber IT Services to conform to the Common Law on confidentiality and Caldicott principles.

## Appendix 1: Document Control Sheet Template

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

| | | | |
|---|---|---|---|
| Document Type | Policy | | |
| Document Purpose | The purpose of this policy is to protect, to a consistently high standard, all information assets, including patient records and other Trust corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. | | |
| Consultation/ Peer Review: | Date: | Group / Individual | |
| *list in right hand columns consultation groups and dates - >* | 02/02/2017 | Information Governance Committee | |
| | January 2017 | Information Governance Team | |
| | January 2017 | Information Technology Team | |
| | | | |
| | | | |
| Approving Committee: | | Date of Approval: | 02 February 2017 |
| Ratified at: | Information Governance Committee | Date of Ratification: | 28 March 2017 |
| | | | |
| Training Needs Analysis:<br><br>*(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)* | None | Financial Resource Impact | None |
| Equality Impact Assessment undertaken? | Yes [ x ] | No [ ] | N/A [ ]<br>Rationale: |
| Publication and Dissemination | Intranet [ x ] | Internet [ ] | Staff Email [ ] |
| Master version held by: | Author [ x ] | HealthAssure [ ] | |
| | | | |
| Implementation: | *Describe implementation plans below - to be delivered by the Author:* | | |
| | This policy will be disseminated by the method described in the Implementation section of the Policy and Procedural Documents Development and Management Policy. | | |
| Monitoring and Compliance: | A quarterly summary report of all incidents relating to information security will be presented to the Information Governance Committee. The information in the report will be sourced from any serious untoward or adverse incidents reported through the Trust's Risk Management process and the IT Servicedesk. The monetary penalties from the ICO cross referenced to the controls in place to prevent a similar incident in the Trust and the CareCERT alerts from NHS Digital that are monitored by IT Services<br><br>Unresolved incidents will be logged and monitored via the Trust's Risk Register. | | |

| ***Document Change History:*** | | | |
|---|---|---|---|
| *Version Number / Name of procedural document this supersedes* | *Type of Change i.e. Review / Legislation* | *Date* | *Details of Change and approving group or Executive Lead (if done outside of the formal revision process)* |
| Version | | Date | Change details |
| 3.00 | Review | 14/02/14 | Reviewed. Addition of IG Privacy Officer responsibilities, section 4. Minor amendements |
| 3.01 | Review | 12/03/14 | Minor amendments. Addition of All Staff responsibilities, section 4 |
| 3.02 | Review | 19/11/16 | Remote Access included at 5.5. |

| | | | |
|---|---|---|---|
| | | | Consequences of breach added at section 5<br>Change of Policy Lead from IG Officer to IT Service Manager<br>System Level Security Policy requirement added at Information Asset Owners duties. |
| 3.03 | Review | 18/09/2018 | Update references to Data Protection Act 2018 and General Data Protection Regulation. |
| 3.04 | Review | 04/03/2019 | Change of Policy Lead to Head of Information Technology<br>Added access control requirements for non Smartcard systems |
| 3.05 | Review | 08/07/2020 | Section 6.5 access controls updated following approval of AD password policy change. |
| 3.06 | Review | 16/09/2020 | Section 6.5 access control updated in line with NCSC guidelines following approval at IG Group.<br>VPN access updated to reflect all staff have access to remote working. |

## Appendix 2:Equality Impact Assessment (EIA) Toolkit

### For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: Information Security and Risk Policy
2. EIA Reviewer (name, job title, base and contact details) Tracey O'Mullane, Information Governance Officer, Mary Seacole Building, 01482 477855
3. Is it a **Policy**, Strategy, Procedure, Process, Tender, Service or Other? **Policy**

| **Main Aims of the Document, Process or Service** |
|---|
| This policy sets out the Trust's approach to the security management of information. The policy ensures continuous business capability and minimise both the likelihood of occurrence and the impacts of any information security incidents to ensure that Trust information systems, applications and networks are available when required. |
| Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma |

| Equality Target Group | Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed? | How have you arrived at the equality impact score? |
|---|---|---|
| 1. Age<br>2. Disability<br>3. Sex<br>4. Marriage/Civil Partnership<br>5. Pregnancy/Maternity<br>6. Race<br>7. Religion/Belief<br>8. Sexual Orientation<br>9. Gender re-assignment | Equality Impact Score<br>Low = Little or No evidence or concern (Green)<br>Medium = some evidence or concern(Amber)<br>High = significant evidence or concern (Red) | a) who have you consulted with<br>b) what have they said<br>c) what information or data have you used<br>d) where are the gaps in your analysis<br>e) how will your document/process or service promote equality and diversity good practice |

| Equality Target Group | Definitions | Equality Impact Score | Evidence to support Equality Impact Score |
|---|---|---|---|
| **Age** | Including specific ages and age groups:<br>Older people / Young people / Children<br>Early years | **Low** | A web search has not identified any issues in relation to inequality to groups with protected characteristics in relation to information security.<br>No issues relating to information security have been identified through the Information Governance Log, PALS and Complaints reports supplied to the Information Governance Group or the IG Incident reporting Log<br><br>The Policy ensures the security of the Trust's primarily information assets and aims:<br>• to preserve the confidentiality of information.<br>• the accuracy and completeness of information<br>•that authorised users have access to information<br>and associated assets when required.<br><br>This is irrespective of any protected characteristics |
| **Disability** | Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities:<br>Sensory / Physical / Learning / Mental Health<br>(and including cancer, HIV, multiple sclerosis) | **Low** | |
| **Sex** | Men/Male<br>Women/Female | **Low** | |
| **Marriage/Civil Partnership** | | **Low** | |
| **Pregnancy/ Maternity** | | **Low** | |
| **Race** | Colour / Nationality / Ethnic/national origins | **Low** | |

| | | | |
|---|---|---|---|
| **Religion or Belief** | All Religions<br><br>Including lack of religion or belief and where belief includes any religious or philosophical belief | **Low** | As above |
| **Sexual Orientation** | Lesbian / Gay Men / Bisexual | **Low** | As above |
| **Gender re-assignment** | Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex | **Low** | As above |

**Summary**

| | |
|---|---|
| Please describe the main points/actions arising from your assessment that supports your decision above<br><br>There is no evidence of potentially negative effect on groups with protected characteristics.<br><br>Applying the measures set out in the Information Security and Risk Policy (and its associated policies and guidance) does not impact on anyone with protected characteristics. | |
| EIA Reviewer: Tracey O'Mullane | |
| Date completed: 11 March 2019 | Signature: T O'Mullane |