CONTROLLED DOCUMENT

University Hospitals Birmingham NHS Foundation Trust

Information Security and Access Control Policy

CATEGORY	Policy
CLASSIFICATION:	IT
PURPOSE	To provide a balance between security and ease of use by providing a comprehensive and consistent approach to the security management of information across the Trust
Controlled Document Number:	168
Version Number:	4.0
Controlled Document Sponsor:	Medical Director
Controlled Document Lead:	Head of IT Governance and Compliance
Approved By:	Chief Executive
On:	01/12/2019
Review Date:	01/12/2022
Distribution: • **Essential Reading for:** • **Information for:**	 All staff All staff

Contents

1 Policy Statement

1.1 The purpose of this Information Security and Access Control Policy and its associated documents is to ensure University Hospitals Birmingham NHS Foundation Trust (the Trust) has an overall information security management framework which protects to a consistently high standard, all Trust information from all potentially damaging threats and vulnerabilities, whether internal or external, deliberate or accidental by:

1.1.1 Describing the principles of information security and explaining how they shall be implemented in the Trust:

1.1.2 Creating and maintaining a level of awareness for information security as an integral part of the day to day business:

1.1.3 Ensuring that all users of Trust IT systems are aware of, and fully comply with, their duties as described in this policy and its associated procedures: and

1.1.4 Protecting IT systems under the control of the Trust; be they internally or externally hosted.

1.2 The objectives of this Policy are to maintain:

1.2.1 **Confidentiality** - Access to data is confined to those who have legitimate authority to view it.

1.2.2 **Integrity** – Data is timely, accurate and complete and amended only by those specifically authorised to do so.

1.2.3 **Availability** - Information shall be available and delivered to an authorised person, at the time when it is needed.

1.3 All users of Trust IT systems must abide by the rules set out in this Information Security and Access Control Policy and associated documents. Failure to comply with this policy may result in the individual or the Trust being prosecuted.

1.4 The Medical Director may delegate approval of all procedural documents associated with this policy to the Director of IT services, including any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

2. Scope

2.1 This policy applies to all areas and activities of the Trust and to all individual users employed by the Trust including contractors, volunteers,

students, locum and agency staff (including bank), staff employed on honorary contracts, non-executive directors and any other individual or organisations granted access to Trust systems (all of these categories of users being referred to in this policy as 'staff').

2.2 This policy applies to all information held on electronic assets, Trust information in transit and activities carried out on mobile devices.

3. Framework

3.1 This policy sets out the high level framework for Information Security within the Trust. The framework is divided into the following sections:

3.1.1 Policy management, education and awareness (see 3.3)

3.1.2 Computer, system and network security (see 3.4)

3.1.3 Access Management (including remote access) (see 3.5)

3.1.4 Asset Management (see 3.6)

3.1.5 Business Continuity and Disaster Recover (see 3.7)

3.1.6 Removable media (see 3.8)

3.1.7 Security by Design (see 3.9)

3.1.8 Incident management (see 3.10)

3.1.9 Compliance, validation and accreditation (see 3.11)

3.2 Terms shall be given the meaning as detailed in the Glossary contained in Appendix A.

3.3 Policy management, education and awareness

3.3.1 The information security framework detailed in this policy is supported by the following Controlled Documents.

- Access Control Procedure - Secure access to network services and systems provided by IT.
- IT Acceptable Use Policy – Acceptable practices and responsibilities expected of staff with access to computers and moveable devices (e.g. laptops, phones, etc.).
- Procurement Policy and Procedure - Appropriate supplier checks and relevant contractual clauses for third party suppliers who will have access to the Trust network, information systems or data.

- Policy and procedure for the management of medical devices - Data security questions as part of the pre-acquisition questionnaire for third Party medical devices

- Digital Equipment Disposal Procedure

- Mobile Devices – Use of all mobile devices capable of storing information.

- Removable Media Procedure – Use of all removable media capable of storing information.

3.3.2 All staff must attend information security training sessions as identified in the IG Training Needs Analysis (TNA). This includes face to face training (e.g. corporate induction and annual re-fresher IG training), e-learning, as well as bespoke training session (e.g. cyber security for Information Asset Owners.

3.3.3 An on-going awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary. This may include ad hoc exercises such as phishing emails, screensavers or promotion of new controlled documents in 'In the Loop'.

3.3.4 All staff are expected to adhere to a 'clear desk' policy and use screensavers when leaving their desks unattended.

3.4 Computer, system and network security

3.4.1 All new information systems, applications and networks must have an approved security plan in place before they commence operation.

3.4.2 Management of computers shall be controlled through standard operating procedures (SOPs) which have been authorised by the Medical Director. The Medical Director may delegate this responsibility to the Operational Director of IT Services.

3.4.3 All business databases and network files must be backed up to enable recovery. Off-line, network disconnected copies must be kept in addition to network accessible copies.

3.4.4 Provision of the network is contracted via a Third Party supplier, who must abide by the nationally defined NHS Health and Social Care Network (HSCN) Connection Agreement, including the terms and conditions of the IG Assurance Statement and a "Satisfactory" annual self-assessment of the DSPT.

3.4.5 There must be an annual penetration test of the network, including a vulnerability scan and checks that default passwords have been changed. Any critical or high vulnerabilities detected which remain

unresolvable must be documented and agreed with the Senior Information Risk Owner (SIRO).

3.4.6 Every asset in the network must be configured securely individually as well as protected by a network architecture which secures the perimeter. Environments must be segregated.

3.4.7 The risk of weak links or 'single points of failure' must be identified and mitigated by establishing resilient, redundant, complementary controls and separation of duties.

3.4.8 The security of IT systems must be regularly tested as part of regular 'business as usual', with the frequency of testing determined by the criticality of the system (see also Business Continuity and Disaster Recovery– 3.7).

3.4.9 Changes to information systems, applications or networks shall be reviewed and approved in line with Trust's processes managed by the Change Advisory Group (CAG).

3.4.10 The default/third party supplier recommended configuration of Trust critical systems must be reviewed by staff with sufficient expertise.

3.4.11 Users are not permitted to install software on Trust systems without explicit permission by the Trust's IT department. Any exception request must be raised via the IT Service Desk. Users breaching this requirement may be subject to disciplinary action and any unapproved software removed.

3.4.12 Information transfers outside the Trust shall be conducted using encrypted devices.

3.5 **Access Management (including remote access)**

3.5.1 Access to information, including enhanced (privileged) access, shall be restricted to authorised users in accordance with the Principles of Least Privilege, which means they are given the minimum access needed to perform their duty, limitation of use (e.g. time limited) and segregation of duties.

3.5.2 Staff are responsible for keeping their user authentication information (user names and passwords) secret. Actual or suspected compromise of user credentials must be reported as an IT security incident which will result in a change of those details.

3.5.3 Physical and electronic (digital) access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

3.5.4 Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

3.5.5 The default position is that access to computers or systems is granted on an individual basis. Generic log-ins remain the exception but may be granted by authority of the SIRO provided there is an overriding business need and a risk assessment has been undertaken which sets out how any associated risks are mitigated.

3.5.6 Third party support access may be provided by IT Services in accordance with the Principle of Least Privilege for the shortest amount of time. Such access shall only be granted following satisfactory due diligence on the supplier, the approval of the associated information privacy impact assessment and the supplier signing up to appropriate terms in the supplier agreement, including specific confidentiality and accountability clauses.

3.5.7 An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis by Information Asset Owners and as part of an audit by IT Security to ensure compliance with this policy.

3.5.8 Remote access to Trust network and systems must be requested via the IT service desk and will be provided via software and services which require additional user authentication. Staff and third party suppliers, using remote access facilities, may do so from private locations, provided such access has been granted by the individual who is responsible for the contract, records are maintained of who specifically has used remote access facility, the purpose and date of such access, and a secure network connection is being used.

3.5.9 Staff shall ensure that computers used for remote access are using up to date malicious software (“malware”) protection. Any personally identifiable data (PID) or Trust intellectual property accessed from remote locations must not be stored locally.

3.5.10 Staff must further ensure that family and friends do not have access to Trust services and systems at the remote location and must take protective measures against eaves-dropping when using mobile devices in public places.

3.6 **Asset Management**

3.6.1 All IT assets must be physically protected from threats and environmental hazards through the effective use of suitable security measures, including but not limited to physical access controls to buildings such as burglar alarms, and secure storage facilities such as lockable cabinets.

3.6.2 Maintenance and repair of Trust IT assets shall be performed and logged in a timely manner, with approved and controlled tools.

3.6.3 Software and hardware must be maintained through its lifetime with the implementation of updates and alterations ("patches"). The installation of software updates and patches shall be managed by appropriately trained staff and following routine change management processes.

3.6.4 IT assets using unsupported software must be identified and risk assessed, with the SIRO confirming whether the risks will be treated or tolerated.

3.6.5 IT assets containing person identifiable data (PID) or business confidential/sensitive information shall be disposed of in line with the following guidelines to prevent unauthorised disclosure:

- NHS Digital Disposal and Destruction of Sensitive Data
- The Information Commissioner's Office (ICO) IT asset disposal for organisations
- The Waste Electronic and Electrical Equipment Directive (WEEE)

3.6.6 The transfer or destruction of IT assets must be documented by the business unit responsible for the asset, using logs which shall be retained for a minimum of one year or longer depending on the risk and relevant retention guidelines. Refer to the 'Record Management Policy' for further information.

3.6.7 All IT assets containing business critical information shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset. IAO's may be assisted by one or more Information Asset Administrators (IAA).

3.6.8 A register of all IAOs and IAAs shall be maintained by the Information Governance department. Assets shall be classified in terms of business value and criticality. The flow of data between an IAO's assets and any internal or external systems or parties shall be included in the asset register.

3.6.9 IAOs are responsible for ensuring appropriate access to their systems, based on the Principle of Least Privilege (including Third

Party suppliers), carrying out (privacy) security risk assessments (as required) and maintaining System Level Security Policies (SLSPs) for systems under their control. Specific responsibilities may be assigned and obligations communicated directly to those who use the system.

3.6.10 Agreements with suppliers shall include requirements to address information security risks and service delivery management considerations.

3.7 Business Continuity and Disaster Recovery

3.7.1 Each business unit (ward/department/division) is responsible for ensuring that business critical systems, applications and network, for which they are responsible have an approved business impact assessment and business continuity/disaster recovery plan in place which is deployed in the event of an emergency.

3.7.2 Any business continuity plan must rely on alternative systems, processes and records which meet the demands of the critical system they are meant to replace.

3.7.3 The Business Continuity and Emergency Planning team must ensure that each plan is tested in appropriate intervals. Following each business continuity exercise, an issue and action log shall be produced.

3.7.4 Business Continuity must be considered as part of information security by design (see 3.8) and should cover internally and externally supplied systems.

3.7.5 Business continuity arrangements must take into account the objectives of this policy to maintain the required level of information security during adverse conditions.

3.7.6 All emergency contacts must be kept up to date, in hard copy in a secure location.

3.8 Removable media

3.8.1 Removable media of all types that contain software or data from external sources, or which have been used on external digital equipment, require the approval of the Trust before they may be used on Trust systems.

3.8.2 Read-only access to removable media is permitted, provided such media is fully virus checked before being used on Trust equipment.

3.8.3 Further details are available in the Removable Media Procedure. Users breaching this requirement may be subject to disciplinary action.

3.9 Security by design

3.9.1 Information security must be addressed in all stages of projects involving IT systems, regardless of whether they involve the procurement of a new system or a re-configuration of an existing system. Where personal identifiable information might be at risk, a privacy impact assessment (PIA) must be undertaken, which shall include any security risks, as specified in the PIA Procedure.

3.9.2 The core principle of a (privacy) security risk assessment and management requires the identification and quantification of the risks in terms of their perceived value of asset/information at risk, the severity of impact and the likelihood of occurrence.

3.9.3 Once identified, all (privacy) security risks shall be managed in line with the Trust's Risk Management Policy, using available controls, including but not limited to policy/procedures, training; 2 factor user authentication, encryption of data at rest and in transit, audits, network monitoring, software tools such as anti-virus protection, hardware constraints and data anonymisation/pseudonymisation.

3.9.4 For third party supplier systems the Trust's IT service model contract must be used. For further advice, staff should consult with the Procurement Department.

3.9.5 System logs must record user activity (e.g. view and amend) and those logs must be protected from unauthorised access and synchronised with other system's logs.

3.9.6 IT system design must consider capacity management capabilities where the use of resources can be monitored, tuned and projections of future capacity requirements can be made.

3.9.7 Use of application services over the public network should include authentication processes when PID is involved. Consideration of non-availability of services should be included in the system design. Application service transactions should be protected against alteration, incomplete messages, disclosure, duplication or replay.

3.9.8 Operating platforms must be hardened against threats.

3.9.9 Use of cryptographic controls must be regulated.

3.9.10 Trust IT systems must take account of intellectual property rights.

3.10 Secure system development and maintenance

3.10.1 System development activity must take into account information security considerations. Application software in the Trust's possession must be preserved in a source code management system with restricted, auditable access. IT System configuration data must be copied, with the copy being held separately from the operational system. Systems must be probed for vulnerability before the go-live date or significant change, and at least annually afterwards. Test data should be carefully selected, protected and controlled. There must be a separate environment for development, testing and production for all business critical applications, with appropriate segregation of duties. These environments must be kept separate by system-enforced security measures appropriate to protect the sensitivity of the information. IT system changes must be subject to formal change control procedures. Cryptographic keys must be considered managed information assets and subject to change controls.

3.10.2 Superfluous system components must be removed from the operational system, where possible.

3.11 Incident Management

3.11.1 All suspected or actual information security incidents, near misses (security events) and weaknesses must be reported via the Trust's online incident reporting system (Datix) and managed in accordance with the Policy for the reporting and management of incidents, including serious incidents requiring investigation' and the Trust's 'Information Governance and IT Security Management (Personal Data Breach) Procedure.

3.11.2 Incident evidence must be handled with care and attention to its potential further use and protected from unauthorised access and alteration.

3.11.3 Root cause analysis is conducted routinely as part the Trust's lessons learned activities following an information security incident.

3.11.4 Any NHS Digital CareCert bulletins or threat notification will be triaged by a member of the IT department who shall log those with a potential impact on the Trust on the Trust's online incident reporting system (Datix).

3.12 Compliance, Validation and Accreditation

3.12.1 Security risks by exceptions shall be monitored by those who have been given express authority to deviate from the standard approach

(e.g. where generic log-ins have been authorised on an exceptional basis, there must be one individual who is responsible for monitoring compliance with this policy and any associated documents).

3.12.2 All contracts of employment will contain a confidentiality clause. In addition, staff with privileged access rights (system administrators) must sign a local confidentiality statement which holds them to account to the highest standard.

3.12.3 IT security shall conduct regular compliance audits in line with an annual audit plan.

3.12.4 IT service contracts managers, or individuals with corresponding responsibility, shall ensure that security risks are being monitored as agreed in the IT service contract.

3.12.5 The Trust's IT department shall maintain ISO 27001 accreditation.

3.12.6 The Trust as a whole is committed to achieving 'cyber essential plus' accreditation by 2020.

4. Duties

4.1 Director of IT Services

The Director of IT has delegated responsibility for information security on behalf of the Medical Director. The day to day activities required to effectively implement and maintain this policy will be performed through the Lead Security and Test Manager.

4.2 Senior Information Risk Owner (SIRO)

The Director of Corporate Affairs is the Trust's SIRO. The SIRO is accountable for fostering a culture for protecting and using data, providing a focal point for managing information risks and incidents and is concerned with the management of all information assets and their regulatory and legal requirements. The SIRO is responsible for determining the approval processes for enhanced privileges/exceptional access rights and any other security risks for which there is not yet a standardised approach.

4.3 Caldicott Guardian

The Caldicott Guardian has a strategic role in ensuring that personal information relating to patients is used legally, ethically and appropriately and that patient confidentiality is maintained at all times.

4.4 Members of the Information Governance Group (IGG)

The Information Governance Group (IGG) comprises the Trust's SIRO, Data Protection Officer, Information Governance Lead, Information Security Manager, divisional representatives, as well as representatives from Informatics, Medical Records and Therapies. Through this group, the Board is advised of common approaches to Information Governance/Security and assured of Trust practices. The Information Security Advisory Group, Information Governance Assurance Group and several Task and Finish Groups report into IGG.

4.5 Members of Information Security Assurance Group (ISAG)

Members of the Information Security Assurance Group are responsible for ensuring common approaches are agreed to information security incidents and risks, and to monitor compliance with this policy, including the management of user access controls, privileged access rights, security risk assessments requiring approval by the SIRO and any other information security issues.

4.6 Members of Information Governance Assurance Group

Members of the Information Governance Assurance Group are responsible for ensuring that the Trust is compliant with relevant aspects of the Data Security and Protection Toolkit, data protection legislation and this policy, by monitoring compliance with mandatory training standards, reviewing information governance incidents and risk registers, data sharing initiatives and any other information governance issues as they arise.

4.7 Head of IT Governance and Compliance

The Head of IT Governance and Compliance is responsible for the implementation and enforcement of the Information Security and Access Control Policy by:

4.7.1 Ensuring that local practices and standard operating procedures are aligned to this Information Security and Access Control Policy:

4.7.2 Monitoring and reporting on the status of IT security within the Trust:

4.7.3 Providing advice and guidance to staff so they are aware of their responsibilities and accountability within information security:

4.7.4 Ensuring breaches of this policy are managed in a timely fashion:

4.7.5 Working closely with those responsible for information governance, patient confidentiality and information security:

4.7.6 Providing direct input to the information security components of the Data Security and Protection Toolkit; and

4.7.7 Ensuring wider learning is shared with other relevant staff.

4.8 Information Governance Lead

The Information Governance Lead is responsible for promoting a culture of good information governance within the Trust, developing and maintaining policies, procedures and protocols in compliance with relevant legislation and good practice, and monitoring proper implementation of, and compliance with, the same.

4.9 Head of ICT Infrastructure Services (IT)

The Head of ICT Infrastructure Services is responsible for:

4.9.1 Maintaining a baseline configuration of, and tested recovery processes for, infrastructure systems (email, network, authentication services, data storage and backup processes, desktop computers and remote access);

4.9.2 Malware vulnerability detection scanning systems: and

4.9.3 Infrastructure capacity planning.

4.10 Trust Security Management Specialist

The Trust Security Management Specialist is responsible for:

4.10.1 maintaining a physically secure environment and premises which contain sensitive and critical information processing facilities; and

4.10.2 staying abreast of the current security landscape.

4.11 **Information Asset Owners**

All IAOs must ensure that:

4.11.1 An inventory of their physical and electronic (digital) assets is retained:

4.11.2 (privacy) security risk assessments are carried out as required:

4.11.3 System Level Security Policies (SLSPs) are maintained for systems under their control: and

4.11.4 Access to the systems under their control is being monitored, with special attention being paid to 'movers' and leavers' (including Third Party suppliers).

4.12 **Managers with responsibility for staff**

Anyone who has a responsibility for staff must ensure that:

4.12.1 Their members of staff are aware of their security responsibilities (see Appendix B);

4.12.2 Their members of staff have appropriate training for the systems they are using; and

4.12.3 Appropriate levels of access are granted to specific individuals (e.g. Registration Authority (RA) role for staff who issue smartcards).

4.13 **Staff**

All staff must:

4.13.1 Comply with this policy and associated policies, procedures and best practice (see Appendix B);

4.13.2 Report information security incidents in accordance with the 'Policy for the reporting and management of incidents, including serious incidents requiring investigation' and 'Information Governance and IT Security Management (Personal Data Breach) Procedure';

4.13.3 Comply with the confidentiality obligations detailed in their contract of employment; and

4.13.4 Where they engage the services of a third party supplier, obtain authorisation for use of their laptop, or alternative mobile device, on Trust premises by making an IT request.

5. Implementation and Monitoring

5.1 Implementation

5.1.1 This policy will be available on the Trust's Intranet Site. The policy will also be disseminated through the management structure within the Trust.

5.1.2 Information Security training is included in the mandatory annual Information Governance Training Tool (IGTT), along with additional recommended modules.

5.2 Monitoring

Appendix A provides full details on how the policy will be monitored by the Trust.

6. References

The Trust's Information Security arrangements take into account statutory requirements and good practice, including:

Access to Health Records Act 1990

Caldicott Principles (from the Caldicott Committee Report 1997 and the Caldicott Review 2013

Care Quality Commission: Well-Led standard

Computer Misuse Act 1990

Copyright, Designs and Patents Act 1988

Data Protection Act 2018

Department of Health: Confidentiality Code of Practice 2003

Department of Health: Information Security Code of Practice

Department of Health: Records Management Code of Practice

Department of Health NHS Information Governance Guidance on Legal and Professional Obligations 2007

General Data Protection Regulation (GDPR) 2018

HSCN Connection Agreement

Information Security Management: NHS Code of Practice – DH 2007

Interception of Communications Code of Practice 2016

ISO/IEC 27001:2013 Information Security Management Standard

Network and Information System Directive (NIS) 2016

National Cyber Security Centre guidance and standards

NHS Digital Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation

NHS Digital Forensic Readiness Good Practice Guide

NHS Data Security and Protection Toolkit

Police and Criminal Evidence Act 1984

Regulation of Investigatory Powers Act 2000

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Waste Electronic and Electrical Equipment Directive (WEEE)

7. Associated Policy and Procedural Documentation

Access Control Procedure

Business Continuity Plan

Data Protection and Confidentiality Policy

Informatics Data Quality Policy

Disciplinary Procedure

Emergency Preparedness Policy

Flexible Working Policy

Freedom of Information Act and Environmental Regulations Policy

Information Asset Procedure

Information Governance Policy

IT Acceptable Use Policy

Digital Equipment Disposal Procedure

Procurement Policy

Records Management (Corporate and Clinical) Policy

Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy & Procedure

Risk Management Policy

Appendix A - GLOSSARY

Business Continuity is an organisation's ability to ensure operations and core business functions are not severely impacted upon by a natural disaster or other unplanned incident.

Cryptographic key means special data used in the process of encryption.

Encryption means the process of encoding a message or information in such a way that only authorised users can access it.

HSCN network - HSCN is a private network, designed as a reliable business resource to carry information, which is only available to certain organisations. This is different from a 'secure' network. It means that if patient data or personal data is being transmitted across HSCN, then encryption must be used.

HSCN agreement - The Connection Agreement sets out a collaborative way of working, which means:

- HSCN customers acknowledge responsibility for securing information - practically, this means that patient data should always be encrypted when being sent across any network, including the HSCN
- ownership and responsibility for the use of the HSCN connection sits at a senior level within the organisation

Principle of Least Privilege means users are given the minimum access needed to perform their duty,

Appendix B Monitoring Matrix

MONITORING STANDARD	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
Policy management, education and awareness				
Completion of mandatory Information Security and Protection training in line with TNA .	Information Governance Lead	Information Governance Assurance Group (IGAG)	TNA in place which specifies security training for all staff commensurate with their role. Training compliance – 95% as a minimum	Quarterly
Computer, system and network security				
Third Party supplier abides by the nationally defined NHS HSCN Connection Agreement and maintains a “Satisfactory” annual self-assessment of the DSPT.	Operational Director of IT	Information Security Assurance Group (ISAG)	Contract review	Annually
Network penetration test, including vulnerability scan and checks that default passwords have been changed. Any critical or high vulnerabilities detected which remain unresolvable must be documented and agreed with	Head of IT Governance and Compliance	ISAG (with report to SIRO as and when required)	Network penetration test to be conducted by third party supplier. Scope to be agreed with IT Security Manager.	Annually

the SIRO.				
Risk of weak links or 'single points of failure' must be identified.	Head of IT Governance and Compliance	ISAG (with report to SIRO as and when required)_	Trust anti-malware management system report on active/non-active end-points and service systems. Intrusion protection system report. Intrusion detection system report. Review of actions taken as a result.	Quarterly
Users are not permitted to install software on Trust systems without explicit permission by the Trust's IT department	Head of IT Governance and Compliance	ISAG (with report to SIRO as and when required)_	Computer management suite report	Quarterly
Access Management (including remote access)				
System access	Head of IT Governance and Compliance	ISAG	• Spot checks of reconciliation of access control list with currently authorised staff • Reconciliation of existing TP supplier access accounts with list of active suppliers.	Quarterly on a rolling basis

Asset Management				
IT assets using unsupported software must be identified and risk assessed, with the SIRO confirming whether the risks will be treated or tolerated.	Head of IT Governance and Compliance	ISAG (with report to SIRO as and when required)_	Spot checks of systems listed in the IA register	Annually
Confidential and secure disposal of IT assets containing person identifiable data (PID) or business confidential/sensitive information	Head of IT Governance and Compliance	ISAG (with report to SIRO as and when required)_	Audit of appointed TP disposal company	Annually
Business Continuity and Disaster Recovery				
All business critical systems, applications and network have an approved business impact assessment and business continuity/disaster recovery plan in place which is deployed in the event of an emergency and tested in appropriate intervals. Following each business continuity exercise, an issue	Head of Business Continuity and Emergency Planning	Emergency Planning meetings with SIRO	Plan for desk top exercises	

and action log shall be produced.				
Removable media				
Mobile Devices are appropriately deployed and protected	Head of IT Governance and Compliance	ISAG	• Audit of signed Terms and Conditions form when receiving Trust Mobile Devices • Report on devices stolen/lost devices • Low usage report	Annual
Security by design				
Monitoring of IT security recommendations emanating from completed PIAs	Head of IT Governance and Compliance/ IG Lead	ISAG	IG Lead to table approved PIAs at next ISAG meeting / Head of IT Governance and Compliance to provide assurance	Quarterly
Secure system development and maintenance				
Analysis of change control success and failure trends	IT Quality and Change Manager	Deputy medical director (Change Advisory Group chair)	Report summary data on recent IT system changes.	Quarterly
Review of system design material in respect of architectural risk analysis and	IT Security Managers	ISAG	Report on recent project and design analysis.	Quarterly

threat modelling elements				
Audit of IT system development practices, including source code and configuration data management	IT Quality and Change Manager	ISAG	Report on ISO27001 audit findings.	Annually
Incident management				
Reviews of Priority 1 and 2 incidents	Head of IT Governance and Compliance	IT RCA group	Identifying trends and themes. Escalation of appropriate incidents to Exec RCA/full RCA	Weekly
Compliance, Validation and Accreditation				
Enhanced Privilege access process	Information Governance Lead	ISAG	Audit of approved application forms for staff with enhanced privilege access rights, including signatures of local confidentiality agreements.	Six monthly
IT service contracts managers, or individuals with corresponding responsibility, shall ensure that security risks are being monitored as agreed in the IT service contract.	Information Governance Lead	ISAG	Audit of IT service contracts	Quarterly

Appendix C

Users Key Responsibilities

1. Users Key Responsibilities

1.1 The purpose of this appendix is to summarise the key user responsibility requirements as laid out in the following key documents:

- IT Acceptable Use Policy
- Access Control Procedures
- Data Protection and Confidentiality Policy
- Information Governance Policy
- Information Security and Access Control Policy
- Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy and Procedure

1.2 These documents support the Trust's overall Information Security and Access Control Policy which sets out guidelines within the framework of the Department of Health (DH) Information Security Management: NHS Code of Practice (April 2007). It is your manager's responsibility to ensure that you are aware of those policies which are relevant to your role within the Trust.

1.3 By following this policy, users can minimise risks in relation to information security. Non-compliance may result in disciplinary action being taken in accordance with the Trust's disciplinary policy, and may lead, in very serious cases to dismissal, for gross misconduct; as detailed in the Trust's Disciplinary Policy, a copy of which is available via the policies and procedures link from the UHB home page.

2. Safeguarding Data – IT Essentials

- Be vigilant at all time and report (suspicious) events , or (actual) incidents

- Be wary of email and if in doubt about the validity or risk of opening attachments or clicking on links; contact the IT Service Desk for advice

- Use your own password, ensure that it is kept secret at all times and never use somebody else's.

- Do not leave computers open for unauthorised access, ensure either logged out or locked (Ctrl+Alt+Delete) when unattended.

- Do not use the internet inappropriately; just because a site isn't blocked doesn't mean that it is approved.

- Save all data to appropriately restricted UHB network drives, not to your hard drive (i.e. C:\), as network data is secure and backed up.

- Only share Person Identifiable Data (PID), confidential or sensitive information with those who are authorised to see it.

- Do not hold PID on portable media (including mobile devices) unless it is encrypted. Please contact the IT department for further guidance.

- Ensure that portable media (including mobile devices) are backed up regularly to a network drive and that they are logged onto the network regularly to receive antivirus and other major updates.

- All mobile devices, capable of storing information, should be encrypted.

- Do not load unofficial software onto Trust computers or portable media devices (including laptops).

- Apply good "cyber-hygiene" at work and at home. https://www.getsafeonline.org/