NHS
Cornwall and Isles of Scilly

IT security policy

Date approved: 05 June 2026

This is a joint policy between Cornwall Partnership NHS Foundation Trust and Royal Cornwall Hospitals NHS Trust adopted by NHS Cornwall & Isles of Scilly ICB.

Purpose: To provide direction and support to all staff members on information technology security in accordance with business requirements, NHS guidance and relevant laws and regulations.

Target audience: Applicable to employees, contractors, visitors, volunteers etc. who are authorised to use the Cornwall NHS managed network

Document sponsor and role: Kelvyn Hipperson CIO
Document sponsors contact details: Number in full, not extension only.

Document definition: Policy

Freedom of information: Can be released under the Freedom of Information Act 2000

Audience:
☒ Royal Cornwall Hospitals NHS Trust
☒ Cornwall Partnership NHS Foundation Trust
☒ NHS Cornwall & Isles of Scilly Integrated Care Board

Publication location:
☒ Internet and intranet ☐ Intranet only

Key words: Security, Controls, Incident, Disposal, Breach, Governance,

---

NHS Cornwall & Isles of Scilly ICB approval process

Supporting committee: Information Governance Steering Group
Approved at (if applicable): Information Governance Steering Group
Date: March 2026

Executive lead approved: Company Secretary
Date: 5 June 2026

Document library section: Information management and IT, Information technology

Version control

Version	Date	Sponsor and/or reviewer	Changes (key points)
v2.0	March 2016	A. Mann and S. Lobb	Review
v2.1	July 2016	A. Mann, IT Security Manager	Removal of references to PCH, but inclusion of PCHHQ
v3.0	February 2019	A. Mann, IT Security Manager	Updated several sections including Government Classification Scheme, email guidance, Appendix 3 and new Data Protection Act 2018.
v3.1	March 2020	A. Mann, IT Security Manager	6.5.5 Systems Administrators – inserted. 6.10. Incident Management – substantial changes. Links to CHO email addresses and documents
	March 2022	EMG CW	Extended to July 2022
v3.2	July 2022	A. Mann, IT Security Manager	References to NHS Kernow replaced by CIOSICB. Incident Management section updated. Approved at information governance subcommittee in August 2022.
v4.0	02/01/2023	A. Mann, IT Security Manager	Converted to Joint Policy Template
V4.1	24/12/2025	A. Mann, IT Security Manager	Updated to new joint policy template. Changed CHO to C&IoS ICS. Updated glossary. Removed Government classification scheme information. Paper shredding size has been updated for sensitive information in Appendix 6.
V5	June 2026	Philippa Harding, NHS CIOS Company Secretary	Agreed at the March 2026 Information Governance Steering Group and approved by the Company Secretary in June 2026.

This document replaces: IT/005/22 IT security policy

Contents

Summary 8
1. Introduction 9
2. Scope 9
3. Definitions and glossary 10
4. Ownership and responsibilities 16
4.1. Role of the Chief Executive 16
4.2. Role of the Chief Information Officer 17
4.3. Role of the IT security management team 17
4.4. Role of Cornwall IT services 17
4.5. Role of the information asset owners 18
4.6. Role of the line managers 18
4.7. Role of the IGG/SC 19
4.8. Role of individual staff 20
5. Standards and practice 20
5.1. Risk management 20
5.1.1 Risk assessment 20
5.1.2 Risk analysis 20
5.1.3 Risk mitigation 21
5.2. Asset management 21
5.2.1 Inventory 21
5.2.2 Ownership 22
5.2.3 System level security policies 22
5.3. Physical and environmental security 22
5.3.1 Physical access control to designated critical data centres and critical comms rooms 22
5.3.2 Air conditioning 23
5.3.3 Fire and water 23
5.3.4 Power (inc. UPS) 23
5.3.5 General 23
5.4. Communications and operational management 23
5.4.1 Archives 24
5.4.2 Backups 24

5.4.3 Logging and alerting 25
5.4.4 Change control 26
5.4.5 Patching/application updates 26
5.4.6 Monitoring 27
5.4.7 Configuration settings 27
5.4.8 Anti-virus (malicious software protection) 27
5.4.9 Third party contracts (monitor and review) 29
5.4.10 Live testing 29
5.4.11 Software acceptance criteria 29
5.4.12 Network security controls 29
5.4.13 Disposal of IT equipment 30
5.5.14 Security of data in transit (physical and electronic) 35
5.4.15 Penetration testing 36
5.4.16 Mobile and home working 36
5.5. Access control 39
5.5.1 Passwords 39
5.5.2 Network 40
5.5.3 Systems 40
5.5.4 Systems administrators 40
5.5.5 Applications 41
5.5.6 Review rights and privileges 41
5.5.7 Remote/mobile working 41
5.5.8 Inactivity time outs (system and application) 42
5.6. Software development ..... **Error! Bookmark not defined.**
5.6.1 Requirements 42
5.7. Procurement 43
5.8. Project management 43
5.9. Incident management 45
5.9.1 Role of the CITS IT security managers 45
5.9.2 Role of the CITS senior manager 46
5.9.3 Role of the CITS managers 47
5.9.4 Role of the incident manager 47
5.9.5 Role of the incident team 47

5.9.6 Role of the CITS service desk 47
5.9.7 Role of the CITS staff member 48
5.9.8 Incident 48
5.9.9 Reporting 49
5.9.10 Responding to a reported IT incident 49
5.9.11 Managing and containing an IT security incident 50
5.9.12 Escalating an IT security incident to NHS England 50
5.9.13 Reporting an information governance incident 50
5.9.14 Reporting a serious incident 51
5.9.15 Reporting an IT security incident to the EPRR lead 51
5.9.16 Closing down an incident 51
5.9.17 Follow-up on an incident 52
5.9.18 Receiving a threat notification 52
5.9.19 Acknowledging a High Severity Alert (HSA) 52
5.9.20 Responding to an HSA 52
5.9.21 Responding to a medium and low severity threat notifications 52
5.9.22 Managing and containing medium and low severity threat notifications 53
5.9.23 Closing Down medium and low severity threat notifications 53
5.9.24 Follow-up on a medium or low severity threat notification 53
5.9.25 Additional resources 54
5.10. Business continuity 54
5.11. Disaster recovery 55
6. Dissemination and implementation 55
6.1. Security: job definitions and awareness training 55
7. Related legislation, national and local guidance 56
8. CFT Associated Trust policies and documents 57
9. Training requirements 57
10. Implementation 58
11. Document monitoring arrangements 58
12. Environmental sustainability 59
13. Updating and review 59
14. Equality and diversity 60
Equality impact assessment form 61

Appendix 1: HI & ICT Project Management Lifecycle 63
Appendix 2: Backup event log 65
Appendix 3: Example backup tape rotations 66
Appendix 4: IT security server room survey 68
Appendix 5: Server room risk assessment template 72
Appendix 6: National data destruction guidelines 77

Data Protection Act 2018 (UK General Data Protection Regulation legislation)

The Trusts have a duty under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed, and documented. We cannot rely on opt out; it must be opted in.

Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679, contact the Information Governance Team.

- Cornwall Partnership NHS Foundation Trust: Email cpn-tr.infogov@nhs.net
- Royal Cornwall Hospitals NHS Trust: Email rch-tr.infogov@nhs.net
- Cornwall and the Isles of Scilly Integrated Care Board: Email ciosicb.corporategovernance@nhs.net

Summary

This policy describes the technical and operation controls in place to protect the organisation's information and provides the guidance and reassurance that will enable employees and staff seconded to, or commissioned by the organisation, in discharging their duties responsibly and with confidence when using the network and information systems; ensuring that the information and data is kept accurate, relevant, safe and secure, complete and confidential at all times.

1. Introduction

1.1. This document has been produced to ensure that:

- IT systems used by the Cornwall and Isles of Scilly Integrated Care System (C&IoS ICS), made up of the Cornwall and Isles of Scilly Integrated Care Board (the C&IoS ICB), the Royal Cornwall Hospitals NHS Trust (RCHT), the Cornwall Partnership NHS Foundation Trust (CFT), Kernow Health CIC (the NHS 111 and out-of-hours provider, KHCIC) and the GP practices across Cornwall and the Isles of Scilly, collectively the Cornwall and Isles of Scilly ICS member organisations, the C&IoS ICS members are properly assessed for security
- appropriate levels of security maintain the confidentiality, integrity and availability of information and information systems
- all users of the Cornwall NHS managed network are aware of the limits of their authority and their accountability
- appropriate guidance on these issues is communicated at all levels.

1.2. The C&IoS ICS relies on information technology (IT) systems to record, manage and inform their clinical and business processes. These information systems hold important and confidential information in respect of their employees and staff seconded to, or commissioned by the organisation, their service users, other stakeholders and the business elements of managing their affairs.

1.3. This policy describes the technical and operation controls in place to protect the organisation's information and provides the guidance and reassurance that will enable employees and staff seconded to, or commissioned by the organisation, in discharging their duties responsibly and with confidence when using the Cornwall NHS managed network and information systems; ensuring that the information and data is kept accurate, relevant, safe and secure, complete and confidential at all times.

1.4. This version supersedes any previous versions of this document.

2. Scope

2.1 This policy applies to all authorised users of the Cornwall NHS managed network, systems, IT and communications equipment who may be creating information, documents or records, whether they are employed directly by the C&IoS ICS members, contractors, NHS professionals, bank staff, voluntary organisations or suppliers granted access for support purposes.

2.2 Aspects of IT security are governed by UK and EU legislation. Breaches in some of this legislation, such as the Data Protection Act and Computer Misuse Act, may

result in individuals being personally liable and may result in police prosecution as well as disciplinary action.

3. Definitions and glossary

3.1. Applications / software – Computer programs designed to store and manipulate information to support (or provide) a service.

3.2. Archive / archived – Information that is no longer current which is retained to allow future access should the need arise. This may mean that the information is moved to slower access devices or compressed but will still be accessible.

3.3. Availability – Information is delivered to the right person when it is needed.

3.4. Backup – A copy (or the activity to produce a copy) of data stored on a computer. This is usually performed on servers and the copy of the data stored on a magnetic tape. This will enable the 'restoration' of information following a data loss incident and forms part of business continuity and disaster recovery activities.

3.5. Brute force attack – A trial-and-error method used to obtain information such as a user password or personal identification number (PIN).

3.6. Business continuity – The activity performed by an organisation to ensure that services are available to patients and staff. Business continuity will include a range of technical controls to maintain the availability of systems (based on its criticality to the organisation) from identified 'threats or vulnerabilities (such as loss of power, hardware failure, heat, etc.). Business continuity extends to delivering the service without access to IT services.

3.8. Change Advisory Board (CAB) – The CITS Change Advisory Board reviews all system change requests to ensure that changes are planned and managed to minimise impacts to service delivery.

3.9. CITS – Cornwall IT Services, Royal Cornwall Hospitals Trust. CITS provide comprehensive information and communications support to C&IoS ICS members. The CITS IT Service Desk can be contacted by calling extension 1717 (01209 881717) or non-urgent requests can be sent via the CITS Portal: http://cits.cornwall.nhs.uk/

3.10. Confidentiality – Ensuring that personal, sensitive and/or business critical information is appropriately protected from unauthorised access and is only accessed by those with an approved need to access that information.

3.11. Cornwall COIN – a CITS managed Community of Interest Network (COIN). This wide area network links all the computers across all C&IoS ICS sites with the national N3/HSCN network.

3.12. Critical data centre – Server room containing computers that process and store information relating to C&IoS ICS members critical clinical and business systems.

3.13. Critical communications (comms) room – Network communication room (or cabinet) that is relied upon to provide access and availability to C&IoS ICS members critical clinical and business systems.

3.15. Critical systems – Critical systems are defined as those systems that are necessary to support essential services as identified within the DSP Toolkit.

3.16. Cyber – Involving, using or relating to computers, especially the internet.

3.17. Cyber bullying – Cyber harassment or online bullying. A form of bullying or harassment using electronic means. Cyberbullying is when someone bullies or harasses others on the Internet, particularly on social media sites.

3.18. Cyber Security – Is a term to cover defence against attacks primarily from the Internet. These attacks can take many forms from direct hacking attempts, emails containing malware or links to infected websites, etc.

3.19. Database – an organised collection of information/data.

3.20. Data deduplication – (often called "intelligent compression" or "single-instance storage") is a method of reducing storage needs by eliminating redundant data. Only one unique instance of the data is actually retained on storage media, such as disk or tape. Redundant data is replaced with a pointer to the unique data copy.

3.21. Data Security and Protection Toolkit (DSP Toolkit) – This replaced the Information Governance (IG) Toolkit and is an online system which allows organisations to assess themselves or be assessed against NHS England Information Governance and Data Protection policies and standards

3.22. Denial of service (DoS) – A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network.

3.23. Degaussing – the application of a strong magnetic field that disrupts/re-aligns/destroys the surface layer on a magnetic storage device (such as hard drives

and backup tapes) rendering the information stored on the device unrecoverable (permanently erased).

3.24. Disaster recovery – The actions needed to restore systems/services following a break in service delivery outside of the agreed tolerance level. This is usually due to a major or unforeseen incident.

3.25. Distributed denial of service (DDoS) – Identical to a DoS but the incoming traffic flooding the victim originates from many different sources.

3.26. Encryption – The means of automating the protection of IT systems, information and data by making them unreadable without an electronic 'key' code from outside influences, e.g., unauthorised access to CHO hardware and software in the event of loss or theft.

3.27. Fake login page – A replica of a real login page used to trick people into entering their login credentials, which hackers can later use to break into online accounts., that mirror legitimate pages by using company logos, fonts, formatting, and overall templates.

3.28. Government security classifications – Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification – OFFICIAL, SECRET and TOP SECRET.

3.29. HSCN – The Health and Social Care Network is a national network that connects all NHS organisations together.

3.30. IGG/SC – Information governance matters are reviewed and authorised for the organisation within the following groups/committees – information governance group (RCHT), information governance Subcommittee (CFT and C&IoS ICB).

3.31. Information asset owner (IAO) – will normally be a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. There may be several IAOs within an NHS organisation, whose departmental roles may differ. IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

- What information assets are held, and for what purposes.
- How information is created, amended or added to over time.
- Who has access to the information and why.
- The inherent risks to their asset.

3.32. IT – Information technology is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

3.33. IT security incident – Any event that have resulted in, or may have resulted in, the interruption to or loss of IT service to one or more service users, with a major incident causing significant disruption to the business.

3.34. Malicious insider – Staff members or contractors, who have access to the network infrastructure, who take advantage of their access to inflict harm on an organisation.

3.35. Memory sticks – A portable (pocket sized) storage device used for the ad-hoc transfer of information between computers via the Universal Serial Bus (USB) port.

3.36. Mobile IT device – These IT devices are designed to be able to provide electronic access to information whilst on the move or at different locations, e.g., laptops, tablets, Notebooks, PDA's, smart phones, etc.

3.37. Network – Connects IT equipment together to enable the transfer of information. Networks fall into one of these categories:

- LAN – local area network, joining computers and IT equipment in close proximity such as an office or building using wires.
- WLAN – wireless local area network, the same as a LAN but using wireless technology (electronic signals/radio transmissions).
- WAN – wide area network, joining computers or other LANs across a large geographical area.

3.38. OWASP – The open web application security project is an online community focused on improving the security of software. OWASP continually reviews IT threats experienced in the wild and produces a 'Top 10' assessment to educate developers, designers, architects, managers and organisations about the consequences of the most common and most important web application security weaknesses. The DS&P Toolkit Data Security Standard 9.2 states 'Web

applications owned by the organisation are secured against OWASP Top 10 vulnerabilities.

3.39. PC – Personal computer, a generic term used to describe most computers designed for use by one person at a time.

3.40. PID – Personal identifiable data/information is information about a person which would enable that person's identity to be established by one means or another. This might be detail that would make it easy for someone to identify a person, such as an unusual surname or isolated Postcode or bits of different information which if taken together could allow the person to be identified. Personal identifiable data includes one or more of the following.

- Name.
- Postcode.
- NHS number or other identifiable number.
- Date of Birth.
- Online identities such as usernames and IP addresses.
- Photographs and digital images.
- Clinical diagnosis, where this is unusual or rare.

3.41. Pattern wiping – A method of overwriting data in such a way as to make the retrieval of information previously stored unrecoverable. Pattern wiping software write sequential patterns of data on top of each part of the disk during several write passes e.g.

1st write	01101100
2nd write	10010011
3rd write	00101110

This method attempts to mask any previous data with two sets of data that are a mirror of each other, thus ‘blanking’ previous data stored. A random set of data is utilised to fill available space with meaningless information.

3.42. Phishing attack – A type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious code on the victim's infrastructure like ransomware.

3.43. Purging – Data purging is the removal of information such that it is deemed irrecoverable. Connecting for Health specify pattern wiping to a minimum of seven passes to ensure that the information has been ‘purged’.

3.44. Ransomware – A type of malicious code or virus that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.

3.45. Recovery – Restoration of a system to its desired state following a failure in the operation of the system.

3.46. Remote Access – The ability to access information stored on the Cornwall CoIN from a device not directly connected to it. This could be to support mobile working whilst not on an ICS member's site, home working or access by a third-party organisation for the maintenance and support of a system/application. Remote access is via a number of approved, secure channels, but the preferred option is via Microsoft's Direct access .

3.47. Respond to an NHS Cyber Alert (ReTAnCA) – A portal provided by NHS England to allow health and care organisations to submit acknowledgements and responses to high severity alerts (HSA), issued by NHS England in relation to critical and high-risk cyber security vulnerabilities that need to be remediated within fourteen days.

3.48. Sensitive PID – Is a category of personal information that is usually held in confidence and whose unauthorised disclosure, misdirection or loss of integrity could adversely impact on an individual, an organisation or on the wider community. Examples of sensitive PID are where personally identifiable information contains details of:

- Health or physical condition
- Biometric data
- Genetic data
- Sexuality/sexual life
- Ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Political opinions
- Criminal convictions

3.49. Server – A computer on a network that runs one or more applications/ services (as a host) that can be accessed by other authorised users. This could be a database, file share, mail/printing services, etc.

3.50. SIRO – Senior information risk officer owns the Trusts overall information risk policy and risk assessment process ensuring that there is a robust incident reporting process for information risks. The SIRO should report to the organisations Board and provides advice on the content of the statement of internal control/annual governance statement in respect to information risk.

3.51. Social media disclosure – The unauthorised publication of confidential, sensitive or personally identifiable information on social media, used to share or exchange information, ideas, pictures and videos with others via the Internet, including but not limited to Facebook, Instagram, Twitter and Snapchat.

3.52. UPS – Uninterruptable power supply, a power supply that typically includes a battery to maintain power in the event of power outage. These can provide power for varying periods of time but are primarily used within the Cornwall COIN to provide protection from damage to servers from fluctuating power input and from short term power loss and resumption of power. The UPS is not for the purposes of business continuity as it will not provide power for a building.

3.53. User – Any authorised person that accesses the Cornwall COIN or uses equipment provided, or adopted, by the organisation. This includes, but is not limited to, non-executive Directors, GP's, employees, consultants, contractors, researchers, trainees, students, temporary staff and supplies (who have been granted access for support purposes.

3.54. Virus – A type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected".

3.55. WEEE – The Waste Electrical and Electronic Equipment Regulations 2006 Directive.

3.56. Website defacement – An attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.

3.57. Wiping/data wiping – The data wiping process involves the formatting of a hard drive. This procedure is only used when the hard disk is to be re-used within the same security boundary to enable the re-imaging of the operating system and required applications.

4. Ownership and responsibilities

4.1. Role of the Chief Executive

Ultimate responsibility for information security rests with the Chief Executive.

4.2. Role of the Chief Information Officer

The chief information officer is responsible for ensuring that IT security is implemented and managed for the organisation.

4.3. Role of the IT security management team

The IT security management team is responsible for implementing, monitoring, documenting, reporting and communicating IT security across the C&IoS ICS in compliance with all UK legislation, local and national policy and guidance. They have the appropriate authority to deal with all matters relating to this policy and must be provided direct access to all relevant staff members following the reporting of a suspected, or actual, IT security incident.

Responsibilities of the IT security management team include:

- monitor and report the organisations current IT security status to the relevant IGG/SC
- maintain a current copy of the IT security policy and make it available to all users as required
- ensure that IT security is implemented to the level as defined in this policy
- assessment and response to threats as identified by NHS England on behalf of the organisation.
- ensure compliance with legislation, regulations and best practice guidance
- ensure that relevant users are aware of their information security responsibilities
- ensuring that IT devices are protected against malicious code
- producing regular cyber security reports regarding key performance indicators and assurances regarding cyber security.

4.4. Role of Cornwall IT services

Cornwall IT services provide comprehensive computing and IT communications support to the C&IoS ICS members. Services and functions include:

- operations and support of the application, IT, security and communication systems used across Cornwall
- project and programme management of the implementation of new or replacement information and technology systems
- IT training and education to ensure that staff have the skills required to be competent in their use of information systems
- application and web development.

CITS have specific responsibilities with regards to the implementation, practices and enforcement of this policy.

4.5. Role of the information asset owners

For the purposes of security, one local Information asset owner (IAO) will be appointed for each logical or physical set of information assets relating to software or applications. For shared systems, agreement will be reached on there being one owner. IAO's are responsible for:

- understanding what information is held
- knowing what is added and what is removed
- understanding how information is moved
- knowing who has access and why.

These responsibilities are demonstrated by the following tasks:

- ensuring that information assets receive an appropriate level of protection with regard to access to and handling of information
- ensuring that a system level security policy has been produced, detailing what the system does, the information stored and access and security controls in place to protect it.
- conducting an annual review of users who have access (and the level of access) to their information assets
- ensuring that a data protection impact assessment has been completed and is reviewed following any changes in the system that affects the information stored or access to the information
- documenting and disseminating business continuity plans to users to enable minimum services levels to continue in the event of a loss of IT services
- mapping the information flows both internally, with other systems, and externally to other organisations.

4.6. Role of the line managers

Line managers are responsible for asset management of physical devices allocated to the staff under their responsibility.

Line managers are responsible for the asset management of physical devices, including but not limited to PCs, laptops, mobile devices, Smartcards and memory sticks, required by their staff to undertake their duties, for the asset's lifetime.

Responsibilities include:

- specifying a business need prior to purchase
- ensuring budgetary provision before purchase
- purchase of equipment through approved channels
- ensuring that equipment is assigned to authorised staff

- maintaining a register of all assets and who they are assigned to
- notifying CITS when assets change location or are are-assigned to another member of staff
- undertaking an annual review to ensure that the equipment provided to staff is still required for their role
- ensuring that equipment is returned when it is no longer required
- ensuring that IT assets are disposed of in accordance with this policy.

Prior to an employee leaving or change of duties, line managers should ensure that:

- the employee is informed in writing that he/she continues to be bound by their signed confidentiality agreement
- passwords are removed or changed to deny access
- relevant departments are informed of the termination or change and, where appropriate, the name is removed from authority and access lists
- reception staff and others responsible for controlling access to appropriate premises are informed of the termination and instructed not to admit in future without a visitor's pass
- where appropriate, staff working out notice will be assigned to non-sensitive tasks or are appropriately monitored
- organisation property is returned, including all IT, mobile, access and security devices (swipe cards, keys, etc.).

Prior to an employee starting employment, it is the line managers responsibility:

- to ensure that the IAO has authorised access for each system that the new employee will be required to use
- to supply CITS with the details required to set up the user. This can be achieved by calling the CITS service desk or completing the eForm on the CITS Portal pages.

When the employee starts, it is the line managers responsibility to ensure that they aware of and understand the IT security policy and acceptable use policy.

4.7. Role of the IGG/SC

The IGG/SC is responsible for:

- reviewing and ratifying the IT security controls within the policy
- receiving notification of breaches of this policy
- receiving reports.

4.8. Role of individual staff

IT Security is the responsibility of all staff. Staff are responsible for:

- adherence to this policy.
- reporting any breaches of the policy.

5. Standards and practice

5.1. Risk management

5.1.1 Risk assessment

- IT system risk assessments are to be undertaken by the information asset owner annually, or following any significant system change, to ensure that threats that could affect information's integrity, availability and potential for unauthorised disclosure have been considered and mitigated to an appropriate level.
- CITS will be responsible for undertaking risk assessments to cover:
  - Server rooms
  - Networks (LAN, WAN, Wireless)
  - IT projects
  - IT processes (e.g., IT disposal, information transfer, etc.)
- All internet facing systems should be risk assessed, penetration tested and reported to the relevant IGG/SC.

5.1.2 Risk analysis

The DSP Toolkit has a number of requirements and guidance that relate to the protection of information, and these have been used as well as industry standard threats to inform the following process:

Assets: Identify major assets (hardware and information)

Values: Assess asset value in terms of their importance as well as financial value.

Threats: Identify potential threats (defined as 'person or thing likely to cause damage or danger')

Vulnerabilities: Weakness or impact as a result of the identified threat.

Security requirements: Agreed organisational controls to mitigate the effects of the identified vulnerabilities.

Controls / gaps: Actual controls in place and gaps identified where there is deviation from the security requirements.

Risks: Risk determination based on the risk classification matrix with the controls currently in place.

Recommendations: Recommendations of further controls, if necessary, to reduce the risk to an acceptable level.

- A number of security and management controls have been defined in the server controls framework and network controls framework. These are the standard controls that should be implemented across the ICS IT estate and have been based on previous risk assessments, DSP Toolkit requirements/ NHS England guidance, HMG requirements and IT industry standard practices.
- To identify if all the current controls are in place and to inform the risk assessment process, a server room survey form (Appendix 4) has been developed. This is to be used annually during a site visit to record the current status of server room and the results of the survey used to form the risk assessment.
- The results from the server room survey are transposed to the risk assessment template (server room risk assessment template - Appendix 5) to identify any gaps in the agreed controls as per the server controls framework and a risk assessment score is calculated based on the level of consequence and the likelihood. Additional controls are recommended, and a new risk assessment score is shown if these additional controls were implemented.
- The RCHT risk classification matrix will be used to assess the level of level of consequence and likelihood.

5.1.3 Risk mitigation

Residual risks will be reported to the IGG/SC as appropriate.

5.2. Asset management

5.2.1 Inventory

- To maintain appropriate protection for information assets it is essential that the organisation knows how many and what assets need to be protected.
- Assets are classified as either hardware or information/software.
  - Hardware – CITS will be responsible for keeping an asset register of all servers, PC's and laptops per organisation that have been procured or adopted by CITS. The primary purpose for this will be to ensure software license compliance, fault history and to inform the device replacement programme.

- Information/software – This relates to a collection of information such as systems, databases, files, associated documentation (training manuals, guidelines, etc.). An inventory of all information assets will need to be maintained by the information asset owner and fed into the organisation's corporate asset register (which is used to record organisational and departmental dependencies).

5.2.2 Ownership

Operational responsibility for an information asset will be undertaken by the information asset owner. For shared services that cross organisations there may be more than one information asset owner, but a primary information asset owner should be agreed by all parties.

5.2.3 System level security policies

System level security policies should be completed by the Information Asset Owner for each information system to ensure the security and integrity of the information. The Policy will document the current controls in place to protect the information, such as access control, security controls, backup / restoration procedures, business continuity, disaster recovery, etc.

5.3. Physical and environmental security

5.3.1 Physical access control to designated critical data centres and critical comms rooms

- physical security for server and network rooms will take the form of at least two levels to restrict access, e.g., separately locked cabinets/rooms and restricted access to building or area
- In security designated areas visitors access must be controlled and should include the following requirements:
  - the reason for access has been verified before access is granted
  - supervised access
  - escorted access when visiting critical data centres or critical comms rooms
- except in places of public access, staff members will be instructed to challenge strangers
- access to critical data centres and critical comms rooms will be confined to designated staff, whose job function requires access to that particular area/equipment
- the IT security management team may give restricted access to other staff where there is a legitimate need for such access
- authenticated representatives of third-party contractors will only be given access through specific authorisation from the IT security management team, unified

communications manager or server team manager and must be escorted in server and comms rooms at all times.

5.3.2 Air conditioning

- All critical server rooms should be protected against over-heating by the use of air conditioning.
- Air conditioning/ventilation should be implemented where there is not suitable air flow or heat monitoring arrangements should be in place.
- Air conditioning should be controlled, monitored and maintained by the Estates Department (or NHS property services as the landlord).

5.3.3 Fire and water

- Smoke detectors should be installed in all server rooms and fire alarm warnings must be auditable from within the server room.
- Suitable fire extinguishing equipment should be installed in, or within close proximity to, the server room.
- Servers should be protected against water damage and raised from floor level; pipe work should be kept to a minimum and regularly inspected to ensure they are in a good state of repair. Server rooms should not be located in areas that are at risk of flooding.

5.3.4 Power (inc. UPS)

- All equipment in critical data centres and critical comms rooms should be protected from power failures or other electrical anomalies by a UPS. This provides protection against damage due to electrical spikes.
- IT equipment supporting C&IoS systems and services identified as requiring the highest level of availability should be linked to an external generator (power would normally cover the entire building to allow access to IT in the event of a total loss of power).
- The quality of power to a server room should be controlled, monitored and maintained by the Estates Department (including site generators and UPSs).
- Power and telecommunications cabling carrying data or supporting IT services will be protected accordingly.

5.3.5 General

Eating and drinking is forbidden in all server and comms rooms.

5.4. Communications and operational management

5.4.1 Archives

- Archived and recovery data will be accorded the same security as live data and must be held in a separate location.
- Archived data must be physically secure and subject to a retention period.

5.4.2 Backups

- Data will be protected by clearly defined and controlled back up procedures which will generate data for business continuity, disaster recovery and archiving purposes.
- Backups will be appropriate according to service need, e.g.:
  - critical Systems located in the data centre
  - corporate systems
  - local tape solution for satellite offices
- Backup management software is implemented to ensure security of all managed backups and should be configured to encrypt information written to removable media or a portable device.
- Critical system and corporate wide backups will be managed by CITS:
  - Critical systems will be hosted within a resilient environment, subject to the applications' capabilities.
  - Applications hosted in the data centre are backed up using disk to disk technologies which leverages data deduplication technology and long-term backups are carried out to a physical tape library. This design allows for fast backups and recoveries due to the relative speed of disk over tape but is supported by a physical tape backup. Backup to tape is carried out as a daily full disk dump to a tape library solution, overwritten on a three-day cycle.
  - Corporate systems (not hosted in the data centre environment) are achieved via conventional tape backup, rotated daily and stored in a fireproof safe at a physically significant separate location from the associated server room.
- CITS will check the electronic backup logs for all servers on a daily basis and investigate any recorded messages. In the event of an identified tape failure the tape will need to be replaced immediately. If two or more tapes fail from the same batch within a month cycle, then the whole batch should be replaced. However, when loading tapes, any issues identified need to be reported to CITS immediately.
- Restoration of application data:
  - May only be undertaken with formal permission of the systems IAO or in line with the business continuity/disaster recovery plan.
  - Relevant software, hardware and communications facilities will be checked before using back-up data if live data has been corrupted.
  - CITS will maintain a log of work carried out to include all remote system maintenance, engineering and upgrade work, (including software) containing:
    - Date
    - Reason

    - Version
    - Authority
    - Outcome
- All tapes that have been replaced need to be physically destroyed. CITS are responsible for the collection and disposal of tapes co-ordinated and monitored through the CITS Service Desk.
- The labels on the media will ensure that data is not identifiable by unauthorised persons.
- In addition to conventional backups, key clinical systems functioning inside business-critical database systems e.g., Oracle, Cache, etc. have the ability via system journals / transactional logs to roll back to specific points in time.

5.4.3 Logging and alerting

- All IT requests for service and notifications of incidents must be reported to the CITS service desk.
- Requests for Service and Incidents must be entered on the corporate call logging system following confirmation of identity of the caller.
- Information to be recorded:
    - Username
    - Organisation
    - Department
    - Location
    - Asset Ref
    - Description of service request/incident.
    - Call subject classification
    - Call severity
    - Allocated to
- In the case of an incident, the service desk should contact the IT security management team at the earliest opportunity.

5.4.4 Change control

Any significant changes (or changes likely to impact on service provision) to the C&IoS ICS infrastructure must be submitted as a 'request for change' (RfC) for approval by the CITS Change Advisory Board (CAB) before they can be enacted.

5.4.5 Patching/application updates

- All critical operating system and security patches should be applied to all servers, subject to application warranted environments and agreed server downtime by the affected information asset owner.
- When any changes to the operating system are necessary, application systems will be tested to ensure that there is no impact on security.
- All software will be quality assured before release for live use. This process will include:
  - stand-alone and integration testing by an independent test group
  - the use of configuration management to construct and retain controlled versions of the software release
  - validation that any changes to a version of software correspond to either:
    - an authorised change to requirements
    - or an authorised correction of a failure to achieve an objective
  - maintenance of auditable records of each process undertaken in providing a new software version or release
- Where the software release is to be used at several locations, the quality assurance process will be carried out by a central group.
- All testing will be fully documented, and the results distributed to all interested parties ensuring that no personal identifiable information is released.
- The access control procedures applying to operational application systems will also apply to test applications programmes.
- Access to operational application systems will be limited to the end users, while access to test programmes will be limited to development staff.
- Development staff must not modify live files and systems testing must not take place in the live system environment.
- Copying, archiving and dumping of any data will be authorised by the information asset owner and copies will be treated with the same level of security and access restrictions as the originals.
- Live sensitive data must not be used for testing, training or demonstration purposes unless so transformed that it is not possible to identify the original content.
- All proposed changes to a system will be processed under a formal change control system which includes an assessment of the impact on security of the change.
- A record of all changes will be maintained.

5.4.6 Monitoring

- There are established procedures authorised by management for monitoring system use and a process for the management of system alerts where access was unusual or inappropriate.
- Audit trails recording all security related events should be produced and kept for an agreed time period.
- Areas to be considered are:
  - access failures
  - review of log-on patterns for indications of abnormal use or revived user-IDs
  - allocation and use of accounts with a privileged access capability
  - tracking of selected transactions
  - the use of sensitive resources.
- Audit requirements will be agreed with the appropriate management and information asset owners.
- Audit checks will be limited to read-only access to software and data and access should be monitored and logged
- Access to system audit software tools will be controlled to prevent any possible misuse or compromise.
- Audit software tools must be separated from development and live/operational systems; they should not be held in media libraries or user areas.
- Audit trails show user ID's, dates, times, terminal ID and activity/event. These can be system generated i.e., an audit of who updated a field within a database or an automatic log of internet access activity.
- All real time clocks will be set to an agreed standard.
- There will be a procedure for checking and correcting any variation in the clock and it must not be possible to reset the system clock without the details of the change and the user being logged.
- Audit logs statistics will be used to monitor systems performance and the detailed logs may be accessed routinely to detect/prevent misuse or as part of an authorised security investigation.

5.4.7 Configuration settings

IT network and server configurations will be regularly stored and documented for use as part of any restoration process.

5.4.8 Anti-virus (malicious software protection)

- Malicious software and, primarily, software viruses are like human viruses in that they can spread from one computer to others and, in the worst case, all machines networked to an infected machine can be very quickly affected. The effects can be obvious in that the machine stops working properly but also the effects can be partially

hidden where the virus causes the computer to send sensitive information out of the organisation or to disrupt other computers over the network.

- To protect the network from malicious code:
  - All IT devices, that are capable, should be protected by anti-virus software (including, servers, desktops, laptops and mobile devices).
  - IT project managers should ensure that new IT projects include the requirement that protection against malicious code is considered for all IT devices.
  - Inbound and outbound emails should be scanned for malicious code.
  - Internet activity should be scanned for viruses and access to websites may be blocked if they have been classified as a security risk.
  - The anti-virus software should be automatically and regularly updated with the latest definitions.
  - IT devices not owned by the organisation or deployed by CITS should not be connected to the network (with the exception of the staff and public Wi-Fi segregated network) without the approval of the IT security team.
  - Users must not download and install unauthorised software (including screen savers, desktop themes, games, music/video downloading agents, etc.).
  - All software should be appropriately licensed
- Managed exceptions to the standard anti-virus configuration: A defined configuration for anti-virus software clients for servers, desktops, laptops and mobile devices is agreed and reviewed regularly by the IT Security Management Team. On occasion it may be necessary to modify some or the entire configuration sets to accommodate the requirements of particular systems or scenarios. When a requirement to modify the configuration sets is identified the IT security manager will be notified of the required change and will assess the required changes in line with any potential or known threats or risks. Any changes that are agreed by the IT security management team will be submitted as a request for change in line with current CITS procedures.
- Disinfecting a virus: When a virus is detected on a server, desktop, laptop or mobile device a pop-up may appear on the users' screen notifying them that a virus has been detected. The CITS Service Desk will analyse information about the virus infection and if it is found that the anti-virus client could not automatically disinfect, or remove removed, the virus a call log will be raised for the virus to be disinfected.
- Removing anti-virus software: The need to remove the anti-virus client should be rare and should usually only need to occur when significant corruption exists or under controlled conditions when attempting to diagnose a system fault. There are configuration sets and systems in place to prevent staff members from removing or tampering with anti-virus client software. Should a legitimate need to remove the anti-virus client be identified then the documented procedure for the removal as agreed and reviewed by the IT Security Management Team should be followed by authorised CITS engineers.

5.4.9 Third party contracts (monitor and review)

- All NHS contracts should include the NHS standards terms and conditions.
- On-going maintenance arrangements will be the subject of contractual agreements and must be reviewed annually and approval by the appropriate information asset owner. The contract will be required to cover:
  - level of maintenance
  - access control
  - software/application updates to ensure inter-operability with operating system patches
  - minimum levels of performance
- Any request for remote support of IT systems should only be permitted subject to:
  - the necessary confidentiality and non-disclosure agreements being in place
  - any personal identifiable data being secured in line with NHS England standards

5.4.10 Live testing

- To protect the integrity of live and operational clinical and business information, any testing of systems should be undertaken within a test environment, which is physically or logically separate from the live system. Live PID should not be used for test purposes unless agreed by the SIRO following a formal risk assessment.
- In the case where live data is approved for final systems testing, the testing will be carried out under safe-haven conditions and strict access, audit and output management procedures will be followed and monitored and must be in accordance with the use of live or real data in information system testing procedure.

5.4.11 Software acceptance criteria

- Formal documented user acceptance criteria will be available against which the system can be acceptance tested, and acceptance test plans must include attempts to cause security failures.
- Acceptance testing and approval will be undertaken by users who have not taken part in the development or procurement.
- No system should be accepted for live operational running until the information asset owner has approved the formal documented hand over procedures, which must contain a section specific to security.

5.4.12 Network security controls

- Firewalls – The Cornwall CoIN will be protected against unauthorised access at the perimeter by approved firewalls.
- Wireless – Clinical wireless network encryption deployed at a minimum of 256-bit WPA2 with AES.

- Network encryption – Any secure socket level (SSL) or virtual private network (VPN) is deployed as a minimum of 256-bit encryption.

5.4.13 Disposal of IT equipment

- Disposal is the final chapter in the asset management lifecycle and the importance of following strict, secure processes is often overlooked as the physical asset has reached the end of its useful life and has limited financial value. However, it is likely to remain a significant information asset that, if not securely disposed, could result in an unauthorised disclosure breaching the Confidentiality: NHS Code of Practice, distress for patients, a loss of public confidence in the NHS challenging recommendations from the Information Commissioner's Office for a breach in the Data Protection Act.
- Information Technology allows for the storage of vast amounts of information which has traditionally been within dedicated server rooms. Due to technological advancements and the shift to a more mobile workforce, it is possible to store large amounts of business-critical information on portable and office related equipment (including laptops, memory sticks, cameras, multifunction printers, fax machines and photocopiers). It is important, therefore, to consider what happens to this equipment when it comes to the end of its life and leaves the organisation, to protect against an unauthorised disclosure incident.
- It is important to note that information can be retrieved from any form of electronic storage (e.g., disks, memory sticks/cards, cameras, phones, backup tapes, etc.) after it has been deleted (and even after formatting the device). Therefore, it is important that any device that has been used to store personal identifiable or sensitive organisational information is correctly sanitised before it is disposed of or passed on (this may include a user's personal device if it has been used for authorised work purposes).
- The ICS members own their IT equipment. Staff members should contact the CITS Service Desk to dispose of any IT equipment as part of the agreed replacement programme, or if it is deemed uneconomical to repair. It is only the organisation who owns the IT equipment which has the authority to decide whether their equipment is to be disposed and the responsibility of CITS to ensure that this is done securely.
- Disposal of equipment may arise as follows:
  - the IAO, in agreement with CITS, considers the equipment unsuitable for the required function
  - the equipment is beyond economic repair
  - agreement by the information asset owner, normally at the end of its useful life, for disposal under the capital replacement programme
  - agreement by the organisation for transfer to another body or organisation
  - the equipment is surplus to requirement and cannot be reused elsewhere within the organisation.
- In addition to data protection requirements, disposal of electronic equipment must comply with the WEEE directive. If the IT equipment can be re-used, it will be redeployed elsewhere within the organisation. Appropriate information security

controls will be applied, based on risk and NHS England standards, as the device moves between security boundaries.

- CITS are responsible for the disposal of items purchased by the organisation recorded on the CITS IT asset register. The type of equipment that CITS are responsible for disposing includes:
  - PC's
  - Monitors
  - Laptops, tablets and notebooks
  - Printers
  - Electronic storage devices (e.g., memory sticks.)
  - Mobile phones
  - Keyboards and mice
  - Docking stations
  - Backup tapes
  - Servers
  - UPS
  - Switches and hubs
- CITS do not manage the disposal of the following types of devices:
  - Photocopiers
  - Fax machines
  - Monitor stands
  - Televisions
  - DVD players
  - Video recorders
  - Medical equipment

Some of this equipment may retain information in memory (e.g., photocopier and fax machine) and specialist destruction will need to be sought.

- All PC's (including laptops, notebooks, etc.) authorised for disposal will have the hard disk removed and securely stored by CITS for a period of 1 month to ensure against data loss. If, during this period, a user identifies that some files have not been transferred they must call CITS immediately to request a file restore.
- The equipment may be dismantled by CITS and used for spare part purposes or redeployed in another department. Hard disks must be purged of data if moved to a new security boundary or wiped of data before re-use within the same security boundary.
- In the event that any equipment is beyond economical repair or has no other useful life all data will be destroyed as per this policy based on media type.
- Physical disposal will be undertaken by a contracted third party. A Disposal Log will be kept by CITS for each IT asset showing current disposal status (i.e., pending disposal, data destruction method/date and physical disposal method/date). the IT asset register will be updated to show current asset status.

- CITS will retain any documentation and certification relating to the disposal of IT equipment by any third-party contractor and will make this available to the organisation on request.

5.4.13.1 CITS disposal process

- Requests for the disposal of IT assets will normally come via a service desk request, part of an IT replacement program or as part of a technology refresh.
- CITS engineers will complete a disposal form which will require signing as confirmation of the equipment taken for disposal.
- All IT equipment transported between sites as part of this process should only be undertaken by CITS staff and will be required to be secured in transit. PC's and items of low risk can be transported in a car or van and should be positioned out of site (e.g., in the boot).
- Devices containing large amounts of patient or sensitive information will require individual risk assessments to be undertaken to ensure the security of information whilst in transit (e.g., servers).
- All devices to be disposed by CITS must be stored securely.
- CITS will remove all hard disks from equipment for disposal and must:
  - Have a sticker affixed displaying the asset reference number (CITSPC no.)
  - Be entered on the disposal log (CITSPC number, serial number, organisation, engineer and date).
  - Be retained for a period of 1 month (in the event that it is found that information needs to be transferred prior to destruction).
  - Be degaussed, if magnetic media, by the approved device (CESG Higher rated), marked as data destroyed and the disposal log updated.
  - Stored for collection and physical disposal in line with the IT disposal contract.
- The service desk call should be updated with information showing the current status of the request and the IT asset register must be updated accordingly at each stage of the process.
- It is the user's responsibility for requesting file restoration for any hard disk removed prior to disposal within the 1-month retention period. It is not possible to guarantee any file recovery after this period has elapsed.
- Local disk data purging facilities exist within CITS, but where the destruction of information is undertaken by a contracted third party, the following criteria must be met:
  - hard Disk serial numbers recorded for third party disposal
  - hard Disks collected and a list of serial numbers signed for
  - hard disks securely transported between premises (e.g., in a locked container)
  - hard disk serial numbers sent to company to verify expected delivery for destruction
  - electronica confirmation of destruction by serial number and certificate of destruction
  - annual audit of security controls in place

- faulty magnetic disks to be returned to supplier as part of a maintenance contract will follow the data destruction procedure (including degaussing and entry on the Disposal Log) before being returned.
- faulty solid-state devices should not be returned and should be physically destroyed (or securely wiped).

5.4.13.2 Data destruction by media type

- Data storage devices that allow for data to be saved multiple times does not remove information when a file is deleted. It is very easy to retrieve deleted information before it is over written. This is possible because, by saving information the storage device is physically changed and it will therefore remain until it is physically changed again, e.g., by saving new information. It is possible to recover information (or partial information) for an extended period after deletion. It is also possible to retrieve some information even after the information has been overwritten as there is a magnetic 'footprint' or residual image left on the device (especially for hard drives) and it may take several overwrites before the information is irretrievable.
- There are many different types of storage devices/media and the methods of ensuring that the possibility that information is not disclosed will vary. This list is not to be regarded as exhaustive and other media may well be identified as potentially capable of retaining person identifiable data in line with NHS and HMG Destruction Standards, see Appendix 6.

Hard drives (magnetic)

Hard disk drives are extremely popular and are widely used as the primary storage medium for the majority of servers and PCs. Physically, they can be extremely small while simultaneously providing large amounts of storage space.

The storage medium usually consists of a glass platter with a magnetic substrate. Data remains even after removal of power from the drive.

Disposal type: data wiping, destruction

Data wiping involves the writing of overlapping binary information which completely masks previously stored information, a minimum of seven passes are required to meet NHS England requirements/guidelines for data purging. This process allows the disks to be re-used or disposed of by a third party in line with the WEEE directive.

Data can be destroyed on the hard disk by degaussing the hard drive. This involves the passing of electricity through the hard drive which disrupts the magnetic field to such a level that it destroys all information on the device and also renders the device unable to store any future information. Degaussing will need to be carried out to the appropriate CESG standard based upon the IL rating of the data store on the device (national destruction guidelines are listed in Appendix 6).

Solid state devices (SSHD, memory sticks, etc.)

Solid state devices usually consist of integrated circuits and information is stored on silicon chips. SSD makes it possible to store large amounts of information on very small devices (e.g., memory sticks). All portable devices (including laptops) must be encrypted as per a Department of Health mandate.

Disposal type: physical destruction only

Pattern wiping of these devices has recently been identified as potentially ineffective at purging information and therefore physical destruction may be the only method to render the information as irrecoverable. Destruction methods include incineration, shredding or securely wiped (see Appendix 6 for national guidelines).

Optical disks (CD, DVDs, etc.)

Write once optical: CD-ROM and DVD-R.

CD-ROMs and DVD-Rs consist of a plastic platter with an optical substrate applied; a focused laser beam writes the data by 'burning' the substrate.

Write many optical: CD-RW and DVD-RW.

Although similar to write once media, write many media uses a light sensitive dye to record the data instead. Laser light changes the state of this dye; this allows the re-writing of the media (although data may not be written sequentially).

Disposal type: destruction

Whilst it is acceptable to dispose of redundant or damaged CD-ROM and DVD through the confidential waste service within the organisation it is advisable that any optical disk containing particularly sensitive information is cut in half before contacting CITS to arrange for disposal.

Backup tapes

Modern magnetic tape is most commonly packaged in cartridges containing two reels with a single span of magnetic tape onto which backup data is written sequentially. Modern cartridge formats include DAT/DDS, DLT and LTO with capacities in the tens to hundreds of gigabytes.

Disposal type: destruction

It is essential that due to the high volumes of data held on a backup tape that CITS are contacted to arrange for backup tapes to be collected and destroyed. Tapes will be degaussed or incinerated and entered on the Disposal Log.

5.5.14 Security of data in transit (physical and electronic)

- Formal agreements, such as information sharing agreements, will be established for the exchange of critical or sensitive data between the wider health community and other establishments (including partners, Government agencies and other service providers) which include:
  - management responsibilities for controlling and notifying transmission despatch and receipt
  - minimum technical standards for packaging and transmission
  - courier identification standards
  - responsibilities and liabilities in the event of loss of data
  - data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations
  - technical standards for recording and reading data and software
  - any special measures required to protect very sensitive items.
- All external information flows must be protected in transit to using well-configured encryption.
- Large or 'bulk' information transfers must be authorised by the Information Asset Owner and Head of Information Governance prior to contacting CITS to enable and manage the secure transfer.
- Only authorised and reliable transport couriers will be used at all times and packaging will be sufficient to protect the contents from physical damage during transit and to comply with manufacturers' specifications.
- A list of authorised couriers should be maintained, and transportation should be carried out in a secure manner. Authorised couriers will be selected from the public sector Secure Courier List (as of March 2013):
  - CitySprint
  - DX group
  - E-Courier UK Ltd.
  - Government Car and despatch agency
  - TNT UK
  - Royal Mail group
- Controls will be implemented to reduce security risks with electronic communications taking the following into consideration:
  - vulnerability to unauthorised interception or modification
  - vulnerability to error, i.e., incorrect addressing
  - legal considerations such as the need for proof of origin, despatch, deliver and acceptance
  - publication of directory entries
  - remote access to electronic communication systems.
- If patient information needs to be sent via email, it must be protected in transit using one of the following options (in priority order):
- NHSmail to NHSmail (i.e., @nhs.net to @nhs.net)

- NHSmail to any another email account using AES 256-bit encryption (include '[secure]' in subject line).
- Faulty Hard Disk covered under a maintenance contract that are required to be returned for replacement or repair must either be transported securely and protected by an appropriate contract to ensure protection against unauthorised disclosure or the data purged/destroyed before the return of the disk.

5.4.15 Penetration testing

- Penetration testing of all web/internet facing servers should be conducted before live deployment, following any significant changes to perimeter security and should be tested annually against OWASP to ten vulnerabilities.
- Penetration testing plans should be agreed by the SIRO.
- Penetration testing should be undertaken as part of a rolling program to ensure that all identified risk areas have been tested every three years.
- Results of penetration testing and remediation plans should be reported to the IGG/SC.

5.4.16 Mobile and home working

- Mobile computing is a term used to describe the use of a number of mobile IT devices and storage media to process and store information electronically. Typically, this will include items such as:
  Mobile devices
  - laptop, notebook and tablet PCs
  - smartphones and iPhones

  Storage media
  - smartphones and iPhones
  - solid state memory devices (e.g., USB memory sticks)
  - optical discs (DVD and CD-ROM)
  - removable or external hard disc drives
- Mobile IT devices purchased through CITS do not include manufacturer support or insurance against damage or theft. If this is a requirement, these should be purchased directly by the budget holder.
- All mobile devices used for processing/storing NHS information must be encrypted. This was mandated in 2008 by David Nicholson, NHS Chief Executive, and is a required NHS England standard as part of the DSP Toolkit.
- Device encryption is only as secure as the password key that protects it. Encrypted device passphrase/passwords must therefore be suitably long and complex, so that it is difficult to crack, and must never be a dictionary word or name. Never send or store the decryption passphrase or key with encrypted mobile device.
- Mobile/remote working can greatly improve patient care services and also contributes to the improvement of working lives and organisational efficiency. These benefits,

however, present significant risks. Information is no longer retained within the security systems provided within the organisation – it is moving around the country and potentially even abroad.

- It is recognised that the provision of a mobile IT device allows the device to be used both within the Cornwall CoIN and away from the normal office environment in locations such as:
  - the staff members home (will usually require prior authorisation from the line manager and will be subject to the organisation's home working policy)
  - in another organisation's office
  - a suitably equipped hotel room whilst away on organisation business
  - within range of a wireless Internet connection (such as a 'hotspot')
  - offline access in public areas (such as a train)
  - overseas (additional authorisation may be required and legal advice may need to be sought)
- Connection to a third-party network (any network other than the Cornwall CoIN, e.g., another corporate network or to a wireless internet connection whilst working within different offices or in a hotel) may require the use of additional hardware and/or software. If there is any doubt as to the suitability of a particular environment advice should be sought from the CITS Service Desk. In particular, mobile computing users should ensure that:
  - the password used to access any third-party network is not saved electronically
  - any password used is entered manually on each login attempt
  - the login name and password for a third-party network is different to that which is used to access the Cornwall CoIN
  - the environment in which the mobile IT device is to be used is suitable, appropriate and has the necessary technical capability to allow the safe use of the device.
- Advice should also be sought regarding the remote working environment and, in particular, the following:
  - Health and safety issues – health and safety issues are beyond the scope of this document and mobile computing users are responsible for ensuring that the working environment and equipment is used in a way that will not cause harm to the individual or the device. Advice can be sought from a health and safety representative or the line manager.
  - Physical security issues – mobile computing users should ensure that their monitor/screen cannot be overlooked by unauthorised persons or that information is not stored in a way that can be accessed by unauthorised persons (such as at home on a family PC).
- It is essential that sensitive, highly confidential and PID should only be stored on a mobile IT device with the permission of the relevant information asset owner and after notifying the Head of Information Governance. The information should be safely removed from the device at the earliest opportunity.

- Removable media should only be used as a temporary storage medium, particularly for sensitive or personal identifiable data (PID) and any data stored on removable media should be deleted at the earliest opportunity.
- Remote access users will only gain access to the Cornwall CoIN via an authorised encrypted channel such as a CITS provided laptop (Microsoft Direct Access) or using multi-factor authentication.
- Full access to applications stored on a mobile IT device is permitted whilst the mobile IT device user is away from the normal office environment, but it should be borne in mind that this policy strictly forbids the downloading, installation or use of unauthorised software onto such devices whether used in a remote environment or not.
- The use of freeware or shareware that does not benefit from independent security evaluation or that is not approved by the IT security management team is not permitted.
- Access to applications and systems that contain sensitive or PID is only permissible on authorised mobile IT devices and should only be accessed by authorised mobile computing users.
- Before any organisation owned data can be copied and transported on any mobile IT device, permission should be granted by the line manager responsible for the work area, or the Information Asset Owner, before the transfer of PID. Permission should also be granted by the Caldicott Guardian or Head of Information Governance. Sensitive information or PID must not be stored on any unauthorised mobile IT device.
- Data intended for storage on a mobile IT device must be considered for its potential impacts if lost, stolen or otherwise compromised. If large amounts of PID is to be stored on a mobile IT device, then a formal risk assessment should be conducted and authorisation from the Head of Information Governance sought
- Mobile computing users should be trained in the use of encryption tools or application facilities provided, and for the handling of encrypted mobile IT devices.
- Mobile computing users are not permitted to download offensive material to any authorised mobile IT device.
- Any data copied to non-CITS managed computers from removable media should be permanently deleted at the earliest opportunity (normal deletion will move the data to the Recycle Bin). Staff downloading data to non-CITS managed computers are responsible for its security and may be liable for any loss or theft of said data.
- File storage must only be carried out in accordance with the laws that protect copyright, designs and patents and in line with the Records Management: NHS Code of Practice.
- Mobile computing users should ensure that information stored on a mobile IT device is ‘backed up’ to ensure that the data can be recovered for business continuity. Staff members must also take account of the limitations, including those contained within the manufacturer’s specification or guarantee, of certain mobile IT devices for the short or long-term storage of data archives or backups. All files and information saved to the critical data centre CITS will automatically be backed up overnight.

- The mobile computing user must accept responsibility for the proper use and security of any mobile IT device in their care and must:
  - never leave a mobile IT device unattended in a public place
  - never leave a mobile IT device unattended in a non-secure area
  - avoid leaving the mobile IT device within sight of ground floor windows or within easy access of external doors
  - store authentication tokens separately from the mobile IT device
  - return to the office environment and securely store any mobile IT device if the device is not intended to be used for any period of time
  - report the loss or theft of any mobile IT device or the loss or theft of any authentication token to the CITS Service Desk, including details of any sensitive data or PID stored on the mobile IT device. The loss of a mobile IT device will not only mean the loss of availability of the device and its data but may also lead to the disclosure of patient or other sensitive information. This loss of confidentiality, and potential integrity, may be considered more serious than the loss of the physical asset.
- CITS has limited or no control over the IT security environment of any network/ Internet connections made whilst away from the normal office environment. Therefore, before an authorised mobile IT device is connected to a third-party network, suitable security precautions should be implemented:
  - encryption applied to all mobile devices and provided an encryption facility for files required to be transferred/ transported
  - installation/enabling of a firewall
  - anti-virus installed and up to date
  - software updates and patches installed to the most recent, applicable level
  - suitable web content filter configured to restrict the categories of websites that are accessible in line with the office-based environment.
- Whilst every endeavour will be made by CITS to assist a mobile computing user whilst working away from their normal office environment, it must be stressed that support for an authorised mobile IT device may be limited to basic troubleshooting procedures via telephone support. Any work requiring a site visit may only be carried out at the user's normal base the organisation's premises. The CITS Service Desk should be contacted for support or to report an incident on (01209 88) 1717.

5.5. Access control

5.5.1 Passwords

- Password settings include:
  - Minimum length – the minimum numbers of characters that can be used for a password

- Level of complexity – No complexity would consist of alphabetic letters. High complexity would include uppercase and lower-case letters, numbers and special characters (such as '#','!', '*', etc.)
- Ageing – the period of time before the password 'expires' and the user is forced to change it.
- Failed attempts/Lock out – the number of incorrect password entries at the login stage before the account is 'locked'.

- User login password settings are defined by each organisation
- Administrator passwords must be 'long' and complex.
- Passwords should not be dictionary words or be easily guessable.
- Passwords should never be written down (if they are they should be written in such a way that they are not obviously a password).

5.5.2 Network

Only CITS managed devices (including PC's, laptops, mobile phones etc.) or third-party devices explicitly approved by the IT Security Management Team are to be connected to the Cornwall CoIN. Requests for connection of unauthorised devices can be made via the CITS Service Desk, and these will be reviewed by the IT security management team and the Head of Information Governance on a case-by-case basis. This is to ensure that minimum levels of security are applied to all devices on the network and risk of unauthorised access and data 'leakage' is minimised.

5.5.3 Systems

System administrator – certain IT functions will require the highest privilege setting to be enabled. This level of access is required to undertake many users support functions (such as user account changes/password resets, remote control of a PC, etc.) as well as network and server configuration. System Administrator rights will be strictly controlled by the CITS Technical Services and Service Desk team managers and only given to roles that require them. An annual review of system administrator accounts will be undertaken by the IT security management team.

5.5.4 Systems administrators

- Systems administrators have increased levels of access and elevated rights. System administrators therefore have a great deal of power and with that power comes great responsibility, as they are not subject to most of the role limiting protection that is applied to normal user profiles. A System Administrator needs to work to the highest standards with respect to the confidentiality, integrity and availability of the systems they support.
  - Confidentiality – ensuring that only the information needed to undertake a task is viewed and that it is not disclosed further.

    - Availability – ensuring that a system up time' is kept as high as possible and all maintenance is agreed with the information asset owner.
    - Integrity – ensuring that records are not inappropriately altered.
- System administrators will be expected to sign an agreement informing them of their privileged level of access and their responsibilities.
- System administrators must not perform high risk activities, such as reading emails or browsing the Internet, whilst logged in as a system administrator.

5.5.5 Applications

Access to applications is controlled by the relevant information asset owner. Access and privilege levels are to be reviewed annually.

5.5.6 Review rights and privileges

- Access to systems, including privilege level, must be reviewed by the information asset owner following any significant change and at least annually.
- Corporate system administrator access is to be reviewed annually by the IT security management team.

5.5.7 Remote/mobile working

- Remote access – multi-factor authentication is required for remote access to the Cornwall CoIN, when not using a CITS provided laptop with Microsoft Direct Access. Line management authorisation will be required for staff requesting remote access based on business need.
- Remote third-party access – should be compliant with the third-party supplier remote access procedure as well as NHS England requirements and recommendations.
    - Access should be via HSCN via CITS Citrix Portal. All other remote access channels must be risk assessed and authorised by the relevant SIRO. All connections must be encrypted to NHS England standards, include strong authentication and risk assessed.
    - Third-party access should not be enabled by default. Authorisation must be provided by the IAO, based on a specific business need, for CITS to enable remote connection.
    - If the third-party wishes to instigate a remote connection, they must provide details of the reason for access and a description of the works to be undertaken to the IAO for authorisation.
    - Remote access will only be made via agreed channels to ensure that access can be managed and audited.
    - The Remote support connection should be terminated when the fault is fixed, or the supplier ends the session

    - Activity relating to the remote support session should be recorded and held in an audit log
- Legacy connections should be reviewed as part of a systems contract renewal process to ensure compliance. Connections which fall outside of the third-party supplier remote access procedure will need to be separately risk assessed and agreed by the SIRO.

5.5.8 Inactivity time outs (system and application)

- The default setting is fifteen minutes inactivity before the device should automatically lock (requiring the password to be re-entered before use). There are some devices that require this to be extended (such as in Theatres), but this should be authorised by the Head of Information Governance.
- Applications can also be set to lock/close down after a period of inactivity and this period should be defined by the system's information asset owner.

5.6. New systems

5.6.1 All new systems must have a Data Protection Impact Assessment (DPIA) completed by the IAO before the system goes live. The DPIA must be submitted to the organisations IG Lead who will ensure that authorisation process by the SIRO is followed.

5.6.2 Artificial Intelligence (AI) and systems with embedded AI have addition Data Protection Act and organisational requirements:

- Information Governance and IT Security should be engaged early to ensure information security, data protection, and patient confidentiality are maintained.
- AI tools may only be used where they have been formally approved and risk assessed and where their use complies with relevant legislation, NHS guidance, and organisational policies.
- AI tools that are embedded in Medical devices must be classed as Category One devices.
- Staff must not input confidential, personal, or patient identifiable information into AI systems unless explicitly authorised and appropriate safeguards are in place.
- Accountability for decisions remains with the organisation and its staff, and AI outputs must be subject to appropriate human oversight and validation.

5.7. Software development

5.7.1 Requirements

- Before contracting the operation, development or maintenance of any systems:
    - the agreement of IAOs of the applications will be obtained

- any systems containing PID will require a data protection Impact Assessment to be undertaken and submitted to the Head of Information Governance
- risk assessment to be undertaken with regard to security and confidentiality
- the third party will conform to all necessary organisation IT security requirements
- procedures will be devised, and responsibilities allocated for the reporting and handling of security incidents
- all contracts will specify the level of security to be provided by the supplier in accordance with the system security policy
- All contracts will specify contractor's responsibilities for confidentiality of personal data as per the DSP Toolkit and information assurance requirements as well as operational requirements to protect the integrity and availability of the system and information

5.8. Procurement

5.8.1 All IT equipment and software should be purchased through official purchasing channels (normally this will be via CITS). Procurement procedures will ensure:

- Compliance with relevant security and data protection legislation
- Hardware or software changes affecting network management or other operational sites are agreed by all parties affected
- Any new IT facilities provide an adequate level of security and will not adversely affect existing security
- Mandatory and desirable security requirements are included in procurement specifications
- The IT security management team is consulted to ensure that the selected hardware or software meets agreed security requirements.
- Compatibility with existing IT infrastructure can be considered/ tested.
- IT project management and technical resource considerations can be investigated.

5.8.2 Procurement should be managed by the organisation's Procurement Team to ensure that contracts include legal requirements, NHS Standard terms and conditions and service specific requirements.

5.9. Project management

5.8.1 CITS provides IT project management for the C&IoS ICS.

- IT Projects are managed in line with PRINCE2 methodology.
- Security issues will form part of any project's definition.

5.8.2 The project initiation document should contain explicit products and tasks such as the preparation of a system security policy, secure operating procedures and business continuity plans.

5.8.3 Project approval should be withheld until the necessary security requirements have been built into the project plan.

5.8.4 A written statement of system security policy should be incorporated into, or annexed to, the specification for all new or replacement computer systems. The policy should contain the following sections:

Introduction

- Name of system and reference number (if any)
- Location of system
- Estimated dates for installation and operation of system
- Brief purpose of system and its components
- Name of information asset owner

Scope of the system

- The role of the system (i.e., what functions it is expected to perform)
- What the system will process (e.g., personnel data or payroll data)
- The number of users and positions
- System configuration

Risk assessment: a synopsis of the risk assessment to be done during user specification of the system consists of:

- Assessment impact of:
  - system unavailability
  - anti-virus protection
  - destruction of data
  - unauthorised disclosure (access control, protection in transit, etc.)
  - unauthorised modification
- Asset valuation
- Threats and vulnerabilities and associated risk categorisations with plans for reducing risks including business continuity and disaster recovery plans
- Main conclusions and prioritised recommendations

Security standards: Any applicable security standards with which the system must comply.

Security domains: Which must be included for networked systems and may be considered for other systems.

Administration of security:

- Date of expiry of the system security policy
- References to supporting documentation and contracts
- What changes can be made to the system without invalidating the system security policy
- Review time scales and mechanisms.

5.9.5 Formal documented hand over procedures will have specific security requirements as approved by the IT security management team containing (at least):

- The status of adherence to all security standards relevant to the development environment
- Documented reasons for the relaxation of any standards
- Security system test data and results
- References to risk assessment reports
- System test security sign-off (by the IT security management team).

5.8.6 The CITS IT project management process is defined in Health Informatics, and IT Project Management Lifecycle, Appendix 1.

5.8.7 Each new project which involves either changes to data processing activities or the replacement of IT software with different functionality shall abide the data protection design and default principles outlined in the Data Protection Act 2018. This will include the production of data protection impact assessments, where appropriate.

5.10. Incident management

5.9.1 Role of the CITS IT security managers

The CITS IT security managers are responsible for:

- Ensuring that the incident is recorded on Datix or Ulysses (Safeguard) as appropriate in line with the Trust incident management policy
- Informing the CIO, the SIRO, the Head of Information Governance and the IT service lead within the affected customer organisation of an IT incident, providing as much detail as is available in relation to:
  - the incident itself
  - when it happened
  - the affected systems
  - the users affected
  - the sites affected
  - the cause of the incident

- Liaising with the CIO, the SIRO, the head of information governance and the IT service lead of any affected customer organisation to assess if the incident requires reporting to the Information Commissioners Office (ICO) or NHS Digital CareCERT (the Care Computer Emergency Response Team, commissioned by the Department of Health from NHS Digital to offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats).
- Acting as the main contact point for threat alert communications from NHS CareCERT
- Responding to high severity threat alerts from NHS Digital CareCERT and ensuring that they are acknowledged and updated on the CareCERT portal for each of the customer organisations.
- Ensuring that the CIO, the SIRO, the heads of information governance and the IT service leads are made aware of the threat alert, kept informed of any remedial action undertaken and informed of when the alert has been acknowledged, updated and closed.
- Assist in making an informed decision about the level of IT security incident being dealt with and communicating this to all relevant parties
- Ensuring that wider communication to affected staff members is relevant and effective
- Ensuring that any IT security incident that could have wider implications to the health and social care sector or where additional help and guidance is required to help resolve a cyber-security incident is escalated to NHS CareCERT as soon as possible
- Reporting incidents in which information held by the Trust could have been, or has been, compromised that may be INFORMATION GOVERNANCE (IG) incidents to the head of information governance.

5.9.2 Role of the CITS senior manager

The CITS senior manager is responsible for:

- Receiving notifications from CITS managers of actual or potential IT incidents
- Deciding if an IT security incident should be declared based on the reported information
- Declaring an IT incident and appointing an incident manager who will be responsible for managing the incident
- Keeping the CITS senior management team informed of progress and any significant issues or risks, formally closing an incident based on the information reported and ensuring that the relevant members of staff are informed of return to business-as-usual status
- Ensuring that any incident that is identified as a potential Serious Incident (SI) is escalated appropriately and in a timely fashion
- Reporting to the emergency preparedness, resilience and response (EPRR) Lead, any incident that may become a critical incident, major incident or a business continuity issue.

5.9.3 Role of the CITS managers

CITS managers are responsible for:

- Ensuring that IT incidents are notified to the relevant CITS senior manager
- Making themselves and staff members available to form part of the Incident Team when an IT incident has been declared.

5.9.4 Role of the incident manager

The incident manager is responsible for:

- Appointing an incident team involving the IT service lead and the information governance lead and any relevant staff members within the affected customer organisation to help manage and resolve the incident
- Managing the IT incident from when it is declared until the return to business as usual
- Managing and coordinating the incident team to ensure that the incident is resolved efficiently and effectively
- Informing the CITS senior manager of progress and any confirmed issues or risks
- Ensuring that CITS managers, CITS staff members, IT service leads, Head of information governance, the incident team and any relevant staff members within the CITS customer organisations and staff members within the customer organisations are regularly and effectively updated and informed of progress in relation to the IT incident.

5.9.5 Role of the incident team

The incident team will be selected by the incident manager or nominated from within the customer organisation, depending on the type of incident and its severity.

The incident team is responsible for:

- Helping the incident manager to resolve the incident and to keep all relevant parties informed of progress
- Ensuring that the Incident Manager is briefed regularly on progress in resolving the incident and
- Identifying any potential or actual issues and risks in relation to the incident quickly and bringing them to the attention of the incident manager in a timely and appropriate manner.

5.9.6 Role of the CITS service desk

The CITS service desk are responsible for:

- Offering first line support to ensure that the risks relating to the reported IT security incident are minimised.
- Ensuring that multiple reports from staff members from any customer organisation of the same issue are investigated and escalated as appropriate if an incident is suspected
- Providing a reliable, single point of contact specifically in relation to an IT incident
- Providing appropriate advice and guidance to callers

5.9.7 Role of the CITS staff member

All CITS staff members are responsible for:

- Reporting an IT incident to their immediate manager
- Making themselves available to be part of the Incident Team in the event of an IT incident being declared
- Ensuring that any messages given to staff members of customer organisations in relation to the incident are consistent and relevant
- Providing information relevant to the incident to the incident manager directly or via an incident team member promptly.

5.9.8 Incident

An IT security incident is defined as any event that has resulted or could result in:

- the electronic disclosure of confidential information to any unauthorised person as defined by the Data Protection Act 2018
- the integrity of the system or data being put at risk, such as identifying inaccurate information that is not pertinent, finding ways around entering mandatory information, copying information to an insecure location
- the availability of the system or information being put at risk
- the use of any electronic equipment or information to defraud the organisation
- any adverse impact, e.g.
    - on reputation
    - threat to personal safety or privacy
    - legal obligation or penalty
    - financial loss
    - disruption of services/activities.

Some examples of these types of incidents include:

- the loss of, or access to, a major clinical IT system
- the failure of the network serving an acute hospital site or a community hospital site

- the loss of access to or use of NHSmail at an acute hospital site, a community hospital site or across the entire C&IoS ICS
- the loss or theft of a PC that is unencrypted and has data stored on it
- a cyber incident:
  - a malware infection that may result in data loss or the loss of user's credentials
  - a virus outbreak (including ransomware infections)
  - distributed denial of service (DDoS)
  - brute force attack
  - phishing attack
  - social media disclosure
  - website defacement
  - malicious insider
  - fake login page
  - cyber bullying
  - unauthorised access to, or the loss of access to a staff member's ICT account or NHSmail account
  - unauthorised creation of a website for and on behalf of the organisation.

5.9.9 Reporting

- Any staff member may report an IT incident or information indicating a suspected or actual IT incident to the CITS Service Desk. In the event of an incident involving major IT system outage or a significant failure of the IT infrastructure this may result in multiple reports relating to the same incident.
- The CITS Service Desk Analyst will record the information that needs to be reported into a service request. The information to be reported will include:
  - the date of discovery of the incident
  - the location of the incident, if relevant
  - details of who discovered the incident
  - details of the incident
  - details of whether the IT incident puts the organisation or patient care at risk (if known)
  - any action taken by the person discovering the incident or the person reporting the IT incident
- The CITS Service Desk Analyst will relay details of the reported or suspected IT incident to the relevant CITS senior manager for the IT incident and brief them using the reported information.

5.9.10 Responding to a reported IT incident

- A standardised response will be followed to ensure that IT incidents that are similar are dealt with uniformly and to provide assurances that the IT incident can be contained and recovered from as quickly as possible.

- The CITS senior manager will decide, based on the reported information, whether to declare an IT incident.
- If an IT incident is declared the CITS senior manager will appoint an incident manager to resolve and manage the IT incident.
- In the event of an IT incident being declared the incident manager will appoint an incident team and will have unrestricted access to the team throughout the duration of the incident.
- The incident manager may seek the advice of the CITS senior manager or other CITS managers in the appointment of the incident team.

5.9.11 Managing and containing an IT security incident

- The incident team will provide regular updates to the incident manager in relation to the ongoing IT incident in terms of current status.
- The incident manager will ensure that the CITS senior manager is updated regularly on the IT security incident and will ensure that status updates are provided to the CIO, the SIRO, the IT Service Lead, the Head of Information Governance, the CITS Service Desk and all affected staff members on a regular basis.
- The incident manager will co-ordinate any communication in relation to the IT incident to ensure that it is consistent, concise and effective and made using the most appropriate channel in a timely fashion.
- The incident manager will ensure that any feedback or questions received during an incident are dealt with promptly and reasonably, ensuring that any unresolved issues are recorded and responded to effectively and as soon as the information can be provided.

5.9.12 Escalating an IT security incident to NHS England

- The CITS IT security manager will decide, based on the information reported, if the IT security incident needs to be escalated as a cyber security incident to NHS England when the IT security incident that could have wider implications to the health and social care sector or where additional help and guidance is required to help resolve, manage or contain the incident.
- The CITS IT security manager will ensure that NHS England is provided with the most relevant and up-to-date information relating to the IT security incident.
- The CITS IT security manager will co-ordinate any communication in relation to the IT security incident between the incident team and NHS England to ensure that it is consistent and effective and made using the most appropriate channel in a timely fashion.

5.9.13 Reporting an information governance incident

- The CITS IT security manager will report to the Head of Information Governance any incident in which information held by the organisation could have been, or has been, compromised as an information governance (IG) incident in line with the relevant incident management policy.
- The CITS IT Security manager will ensure that the Head of Information Governance is provided with the most relevant and up-to-date information to allow them to decide if the incident must be reported to the ICO.
- The CITS IT security manager will co-ordinate any communication in relation to the IT security incident and any IG incident between the Incident team and the Head of Information Governance to ensure that it is consistent and effective and made using the most appropriate channel in a timely fashion.

5.9.14 Reporting a serious incident

- The CITS senior manager will make an informed decision as to whether the IT security incident needs to be reported as a Serious Incident (an SI) in line with the relevant incident management policy to the CIO and the SIRO for appropriate escalation by the senior member of staff on duty or the on-call manager or on-call director.
- The CITS senior manager will ensure that the CIO and the SIRO are provided with the most relevant and up-to-date information relating to the IT security incident.
- The CITS senior manager will co-ordinate any communication in relation to the IT security incident between the Incident team and the CIO and the SIRO to ensure that it is consistent and effective and made using the most appropriate channel in a timely fashion.

5.9.15 Reporting an IT security incident to the EPRR lead

- The CITS senior manager will decide, based on the information reported, if an IT security incident is likely to become a critical incident, major incident or a business continuity issue and needs reporting to the EPRR lead in accordance with the EPRR strategy.
- The CITS senior manager will ensure that the EPRR lead is provided with the most up-to-date and relevant information relating to the IT security incident.
- The CITS senior manager will co-ordinate any communication between the Incident team and the EPRR lead in relation to the incident to ensure that it is effective, consistent and made using the most appropriate channel in a timely fashion.

5.9.16 Closing down an incident

- The incident manager will decide, based on the information reported, when to formally close an IT incident.
- When the decision to close an IT incident is made the incident manager will dissolve the incident team.

- The incident manager will ensure that a final status update is provided to the CITS service desk before releasing the incident team members to their normal duties.

5.9.17 Follow-up on an incident

- A root cause analysis (RCA) should be conducted by the incident manager and a report should be produced identifying and outlining the cause, any prevention and learning applied as a result, feedback on learning from all members of staff involved along with feedback on the management of the incident and any recommendations identified for implementation as required.
- Following the closure of an IT incident an all staff communication for dissemination to all affected staff members should be drafted providing general information relating to the incident and providing good practice guidelines to minimise or prevent similar incidents from occurring.

5.9.18 Receiving a threat notification

The CITS IT security management team and staff members registered on the NHS England ReTAnCA portal will receive threat notifications from NHS England both via email and via SMS text.

5.9.19 Acknowledging a High Severity Alert (HSA)

The CITS IT security management team will acknowledge HSA notifications received from NHS England on the NHS England ReTAnCA portal as appropriate.

5.9.20 Responding to an HSA

Any HSA received from NHS England will be reported as an incident by the CITS IT security management team and will be responded to, managed, contained, closed down and followed up accordingly.

5.9.21 Responding to a medium and low severity threat notifications

- For all other cyber security threat notifications, the Cornwall CSOC will analyse the details of the threat notification and will record the relevant information in a service request and an incident on the incident management system. The information to be recorded will include:
  - the date of discovery of the threat
  - the location of the threat, if relevant
  - details of the threat
  - details of whether the threat puts the organisation or patient care at risk (if known)
  - any action taken by the IT security management team.

- The Cornwall CSOC will respond to NHS England in relation to the specific threat notification. Responses may include:
  - request for detailed analysis of the identified threat activity
  - request for additional information in relation to the threat
  - confirmation that the threat is not applicable to the customer organisation identified
  - details of the local threat resolution.

5.9.22 Managing and containing medium and low severity threat notifications

- The Cornwall CSOC will receive responses from NHS England providing detailed analysis; additional information or confirmation of that the threat is not applicable to the organisation identified.
- The CITS IT security management team will ensure that the service request is resolved in line with the CITS service level agreement and that the incident is managed accordingly.
- The CITS IT security management team may seek the advice of other CITS managers, CITS staff members, the IT service lead or the head of information governance or other staff members in the relevant organisation in managing and containing the threat.
- The CITS IT security management team will ensure that all affected staff members are updated regularly on the threat and will ensure that status updates are provided to the CIO, the SIRO, the IT service lead, the Head of Information Governance and the CITS Service Desk as appropriate on a regular basis.
- The IT security management team will co-ordinate any communication in relation to the threat to ensure that it is consistent, concise and effective and made using the most appropriate channel in a timely fashion.

5.9.23 Closing Down medium and low severity threat notifications

- The CITS IT security management team will decide, based on the information reported, when to formally close down any service request in relation to a threat.
- When the decision to close down a service request relating to a threat is made the IT security management team will formally update it with the identified resolution.
- The CITS IT security management team will ensure that a final status update is provided to NHS England before closing down the service request.

5.9.24 Follow-up on a medium or low severity threat notification

- An RCA may be conducted by the IT security management team where necessary, and any recommendations will be identified for implementation as required.
- Following the closure of a medium or low severity threat notification, a communication for dissemination to CIO, the SIRO, the IT service lead, the Head of Information Governance and the CITS Service desk or other staff members in the relevant organisation should be drafted providing general information relating to the threat.

- Following the closure of a medium or low severity threat notification, the need for a global communication to all staff members in all customer organisations providing good practice guidelines to minimise or prevent similar incidents from occurring should be carefully considered.

5.9.25 Additional resources

Expert advice and resources to manage an IT incident can be sought from NHS England if required and other specialised organisations depending on the skills required.

5.11. Business continuity

All service areas must produce business continuity plans in preparation for an event which results in the loss of IT. Business continuity plans for IT are based on providing a resilient infrastructure for critical systems ensuring the maximum availability affordable, but 100% availability cannot be guaranteed.

5.10.1 Resilience

Server rooms are protected from the impacts of:

- Environmental: heat, fire, electrical (including generators or uninterruptable power supplies (UPS)).
- Hardware failure:
    - Critical systems are run in a resilient dual site data centre solution. Both data centres are fully resilient in design and able to support the current requirements independently.
    - Important systems are protected against IT failure by localised fail over facilities including clustered/load balancing environments.
    - All critical hardware is supported by third-party maintenance contracts

5.10.2 Networks

- A primary and secondary network circuit is in place for all major C&IoS ICS sites. This is to offer a level of resilience should there be a circuit failure, allowing network traffic to be re-routed across the backup circuit.
- The Cornwall CoIN is subject to separate business Continuity plans, which detail recovery procedures in the event of failure of systems.
- Firewalls should be installed on all external connectors.
- Penetration testing should be conducted on outward facing firewalls
- All primary nodes are protected against power failure by UPS batteries and the majority of the links have redundancy via alternate switches or cards. Wide area Network connections also have primary and secondary lines to buildings
- A small stock of network switches is maintained, which is utilised in the event of hardware failure to bring a minimum level of service back as quickly as possible.

- All critical Network hardware (switches, firewalls and wireless access points) to be covered by third-party/manufacturers support contracts.

5.10.3 Data loss/recovery

- Disk to disk virtual backup solution in place to cover storage area network (enabling very fast data recovery)

5.12. Disaster recovery

5.11.1 Systems are protected against interruption and data loss based on their level of criticality. The most critical systems are hosted in a mirrored data centre environment which would enable those systems to continue to be available in the event of a total loss of one of the data centres.

5.11.2 An IT disaster is any event that would lead to a significant loss of IT services, such as:

- A site loss of the IT network
- An event which renders both critical data centres inoperable
- The loss of a primary data centre
- The loss of one or both CITS primary offices
- Resourcing levels falling below minimum operational levels
- The loss of a critical clinical IT system
- An extended loss of utility services

5.11.3 The CITS disaster recovery plan details how data and IT systems/ functionality are recovered in a structured and managed manner, including the priority order in which systems should be restored.

5.11.4 Tape backups are held in a physically separate location in the event that the data centres are rendered inoperable/destroyed.

5.11.5 Disaster recovery plans should be tested annually.

6. Dissemination and implementation

6.1. Security: job definitions and awareness training

6.1.1 Definitions of job responsibilities, working practices and induction training will ensure that:

- all users are, according to their responsibilities, briefed on:

    - the IT security policy
    - the data security and protection toolkit requirements
    - relevant legislation, national policy and guidance
    - conduct and disciplinary procedures which may be invoked in the event of a breach of security
    - individual accountability
- subject to a suitable risk assessment the following information security controls should be implemented:
    - segregation of function and separation of duties
    - dual control and staff rotation
    - individual defined authorities or levels of authority
    - security privileges and access rights to specific job functions
    - job responsibilities that do not lead to conflict of interest
    - bank and temporary staff members and contractors receive equivalent induction training and sign an agreement to abide by the same codes of conduct and discipline as permanent staff members
- where temporary staff members are employed through an agency or private firm the condition described above forms part of the contract of engagement.

6.1.2 Particular reference to information security will be made when requesting recruitment references for technical or end users of information systems.

6.1.3 The appropriate confidentiality (non-disclosure) undertaking should form part of the contract of employment for all staff members.

6.1.4 Contractors are required to sign a confidentiality agreement prior to connection to the Cornwall CoIN information systems (where not already covered by an existing contract containing the confidentiality undertaking).

6.1.5 Confidentiality agreements will be reviewed when there are changes to terms of employment or contract, particular after resignations or contracts are due to end.

7. Related legislation, national and local guidance

Related Documents:

- Use of Live or Real Data in Information System Testing Procedure
- Policy to Manage Information and Records
- Records Management Policy
- Policy for Recordings and Photography
- Equality and Diversity policies
- Fraud and Corruption Policy/Counter Fraud and Corruption Policy
- Disciplinary Policy

Links to key external standards:

- Data Protection Act 2018
- Human Rights Act 1998
- The Freedom of Information Act 2000
- Health and Social Care Act
- Access to Health Records Act 1990
- Computer misuse Act 1990
- NHS England: Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992)
- Police and Justice Act 2006
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2001)
- Communications Act 2003
- Public Interest Disclosure Act 1998
- The Police and Criminal Evidence (PACE) Act 1984
- Environmental Protection Act 1990, Landfill Regulations 2002 and WEEE Directive 2003
- The Common Law Duty of Confidentiality
- Information Security Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Data Security and Protection Toolkit

8. CFT Associated Trust policies and documents

Sponsor to add details of Trust policies and documents including reference numbers and year of publication before adding the full TAP title.

- TAP Ref / Year - Title

9. Training requirements

Cornwall Partnership NHS Foundation Trust trains and educates staff in line with the requirements set out in its training needs analysis and applied to individual training records on the Trust's learning management system. Training which is categorised as mandatory must be completed in line with the training needs analysis. Staff failing to complete this training will be accountable and could be subject to disciplinary action.

Staff not up to date with mandatory training requirements will not be eligible to access funding through the central development fund.

Compliance with mandatory training is monitored through the education and training team with monthly reports to managers, bi-monthly to the education delivery group and monthly to the board's people and culture committee.

10. Implementation

Line Managers are required to confirm that the IT Security Policy and Acceptable Use Policy will be read and checked that it is understood as part of the request for an IT account process for new employees.

The Policy will be available on the corporate document library.

This will be deleted for the final version, and it is the sponsor's responsibility to contact the Rio Team.
Is there an implication to forms on RIO? No

11. Document monitoring arrangements

Information category	Detail of process and methodology for monitoring compliance
Element to be monitored	This policy will be monitored to ensure that the Trusts are compliant with the NHS data security and protection toolkit.
Lead	IT Security Management Team
Tool	Audits will be undertaken by the IT Security to check that the security controls in place comply with the levels set within this Policy. Software tools will be used where appropriate to monitor activity and compliance with this policy which will be periodically reviewed and will be made available in the course of an IT security investigation.
Frequency	Annual audits of the sever room and network controls. Monitoring of other aspects of the policy (including incident reporting) will be in line with organisations information governance committees (Subcommittees) meetings.
Reporting arrangements	Information governance committee (Subcommittee) Data security and protection toolkit.

Information category	Detail of process and methodology for monitoring compliance
Acting on recommendations and lead(s)	Recommendations will be made by the clinical informatics development plan board, Information governance committee (subcommittee), IT Security Management Team and National best practice. Implementation action plans will be agreed by the Trust IGC/IGSC, clinical informatics development plan board and updates reports will be provided as appropriate.
Change in practice and lessons to be shared	Any lessons learnt during the reviews and audits will inform and update the IT Security Policy which will be presented to the appropriate IGG/SC for consultation and ratification.

Will the monitoring arrangements result in a clinical audit: No

12. Environmental sustainability

Drafting note (deleted for final policy):
When planning and delivering service, process or policy changes all colleagues are asked to consider how the changes could support the Trust's carbon reduction work and reflect these considerations in accompanying documents.
Sponsor to add information if required.

When planning and delivering service, process or policy changes all colleagues are asked to consider how the changes could support the Trust's carbon reduction work and reflect these considerations in accompanying documents.

The Trust is committed and obligated to reduce its environmental impacts. Healthier outcomes can be achieved for people, the planet and pounds by conducting our activities in a more environmentally sustainable manner.

Email cft.sustainability@nhs.net for more information and guidance.

13. Updating and review

13.1 This Policy will be reviewed no later than every three years.

13.2 Revisions can be made ahead of the review date when the procedural document requires updating. Where the revisions are significant and the overall policy is changed, the IT security management team will re-submit the Policy to the organisations IGC/IGSC for consultation, ratification and dissemination.

13.3 Where the revisions are minor, e.g., amended job titles or changes in the organisational structure, approval can be sought from the executive director responsible for signatory approval, and can be re-published accordingly without having gone through the full consultation and ratification process.

13.4 Any revision activity is to be recorded in the version control table as part of the document control process.

14. Equality and diversity

This document complies with the Cornwall Partnership NHS Foundation Trust and Royal Cornwall Hospitals NHS Trust equality and diversity statements. The statements can be found in the Royal Cornwall Hospitals NHS Trust equality diversity and inclusion policy and Cornwall Partnership NHS Foundation Trust equality, diversity and inclusion statement.

Equality impact assessment form

Title of policy or document for assessment: IT Security Policy

Is this a new or existing document? Existing

Date of assessment: 24 December 2025

Person responsible for the assessment: Andrew Mann

What is the main purpose of the document?
This Policy describes the technical and operation controls in place to protect the organisation's information.

Who is affected by the document?
☒ Staff ☒ Patients ☒ Visitors ☐ Carers ☐ Other ☐ All

The document aims to improve access, experience and outcomes for all groups protected by the Equality Act 2010.

Are there concerns that the procedural document could have a differential impact on the following areas?
If a negative impact has been identified, please complete a full equality impact assessment by contacting the Equality, Diversity, and Inclusion Team. For Royal Cornwall Hospitals NHS Trust, email rcht.inclusion@nhs.net. For Cornwall Partnership NHS Foundation Trust, email cft.inclusion@nhs.net

Concern area	Response	If yes, what existing evidence (either presumed or otherwise) do you have for this?
Age	☐ Yes ☒ No	
Disability	☐ Yes ☒ No	
Sex	☐ Yes ☒ No	
Gender reassignment	☐ Yes ☒ No	
Pregnancy and maternity	☐ Yes ☒ No	
Race	☐ Yes ☒ No	
Religion and belief	☐ Yes ☒ No	
Sexual orientation	☐ Yes ☒ No	
Marriage and civil partnership	☐ Yes ☒ No	

Concern area	Response	If yes, what existing evidence (either presumed or otherwise) do you have for this?
Groups at risk of stigma or social exclusion such as offenders or homeless people	☐ Yes ☒ No	
Human rights	☐ Yes ☒ No	

Are there any associated objectives of the document? If yes, what existing evidence (either presumed or otherwise) do you have for this?
Click or tap here to enter details of associated objectives.

Signature of person completing the equality impact assessment:
Name: Andrew Mann
Date: 24 December 2025

Appendix 1: HI & ICT Project Management Lifecycle

Initiation

All new projects are required to complete a Project Brief which is submitted to the Programme Managers for Applications and Infrastructure.

The three Trusts then have formal review groups:

- RCHT: eHealth Programme Board.
- Cornwall Partnership Foundation Trust: Senior Management Team / IM&T Board
- CIOSICB: Senior review group.

The three groups will evaluate and decide whether the project is to be approved.

Programme Management

- Project Manager assigned and Project entered into the Projects List.
- PRINCE2 methodology is followed.
- Project Initiation Document created. All project document templates are stored in 'P:\Projects\New Projects\Templates\'. All individual project documentation is stored in 'P:\Projects\New Projects*'
- Large projects have Project Boards created following PRINCE2 principles. Smaller projects have structures incorporated into grouped Project Boards to ensure governance but also efficiency.

Project Team

- Project Team created – comprises of representatives from the service, network team, server team, security, support and data base administrators as required.
- Project Team to ensure that a Data Protection Impact Assessment (DPIA) has been completed, Security and Governance issues have been considered (including access control, anti-virus, data protection/disclosure), hardware and connection requirements have been identified.
- Third Party Contracts to include new Governance clauses (Legal Team). To include Protection/Non-Disclosure, Incident Reporting, Access Control and Security.
- Project status is reviewed monthly at the eHealth Board, IM&T Programme Board and CFT Senior Management team as appropriate.
- Projects are reported at Programme level in monthly traffic light reports.
- IT Projects to be assessed to ensure protection against malicious code (Anti-Virus) and follow IT security standards.
- The use of live identifiable data for testing purposes must be authorised by the IG Lead.

- No testing is to be undertaken in the ‘live’ environment

Go live

- Go-Live must be approved and the schedule agreed by the weekly Change Control Board. Subsequent changes to Live systems are governed by Change Control.
- Support Hand over document completed pre go live to ensure that all elements have been completed and support teams ready to provide system support
- The Project Board formally closes the Project following implementation and subsequent review of Project Closure document.

Appendix 2: Backup event log

Date	Tape ID	Signed	Name	Notes

Add more rows as required and make sure to delete any empty rows.

Appendix 3: Example backup tape rotations

12 Week Retention Schedule:

2012	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F
JAN	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	23	24	25	26	27	30	31			
FEB			1	2	3	6	7	8	9	10	13	14	15	16	17	20	21	22	23	24	27	28	29		
MAR				1	2	5	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30
APR	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	23	24	25	26	27	30				
MAY		1	2	3	4	7	8	9	10	11	14	15	16	17	18	21	22	23	24	25	28	29	30	31	
JUN					1	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29
JUL	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	23	24	25	26	27	30	31			
AUG			1	2	3	6	7	8	9	10	13	14	15	16	17	20	21	22	23	24	27	28	29	30	31
SEP	3	4	5	6	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28					
OCT	1	2	3	4	5	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	31		
NOV				1	2	5	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30
DEC	3	4	5	6	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28	31				

Key:

- DAILY (MON-THU tape)
- FRIDAY 1
- FRIDAY 2
- FRIDAY 3
- FRIDAY 4 (Only for months with 5 Fridays)
- MONTH 1
- MONTH 2
- MONTH 3

Total Tapes Used: 11

Annual Tape Usage:

Mon	53
Tues	52
Wed	52
Thurs	52

Fri 1	12
Fri 2	12
Fri 3	12
Fri	4

Month 1	4
Month 2	4
Month 3	4

12 Month Retention Schedule:

2012	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F
JAN	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	23	24	25	26	27	30	31			
FEB			1	2	3	6	7	8	9	10	13	14	15	16	17	20	21	22	23	24	27	28	29		
MAR				1	2	5	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30
APR	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	23	24	25	26	27	30				
MAY		1	2	3	4	7	8	9	10	11	14	15	16	17	18	21	22	23	24	25	28	29	30	31	
JUN					1	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29
JUL	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	23	24	25	26	27	30	31			
AUG			1	2	3	6	7	8	9	10	13	14	15	16	17	20	21	22	23	24	27	28	29	30	31
SEP	3	4	5	6	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28					
OCT	1	2	3	4	5	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	31		
NOV				1	2	5	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30
DEC	3	4	5	6	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28	31				

Key:

- DAILY (MON-THU tape)
- WEEK 1
- WEEK 2
- WEEK 3
- WEEK 4 (Only for months with 5 Fridays)
- MONTH END TAPE (Labelled JAN, FEB, MAR, etc.)

Total Tapes Used: 20

Annual Tape Usage:

Mon	53
Tues	52
Wed	52
Thurs	52

Fri 1	12
Fri 2	12
Fri 3	12
Fri 4	4

Appendix 4: IT security server room survey

Equipment (maintenance contract details:

Location	Contact

Deputy	Inspection date

Risk – Backup procedures	Yes	No	Comments
1. Staff aware of Backup Procedure?	☐	☐	
2. Is a backup/restore/failure log kept?	☐	☐	
3. Is there a cleaning tape available and are staff briefed on its proper use, storage and life cycle?	☐	☐	
4. Are backup tapes stored in a secure area with restricted access (inc. location)? Are tapes clearly marked?	☐	☐	
5. Are backup tapes adequately protected against disaster (fire, flood, theft)? Fireproof safe/location etc.	☐	☐	
6. Do backup tapes leave the site?	☐	☐	
7. How old are the backup tapes?	☐	☐	
8. Procedures in the event of tape failure?	☐	☐	
9. How are the backup tapes disposed of?	☐	☐	
10. Has the restoration of data process been tested? (date)	☐	☐	
11. What data is held on the servers?	☐	☐	

Risk – Access	Yes	No	Comments
12. Is the system located in a secure area with restricted access? Is the room in a publicly accessible area?	☐	☐	
13. Is the server room kept locked, and the key held securely by a designated key holder?	☐	☐	
14. Is access to the server room restricted to designated staff?	☐	☐	
15. When designated staff leave can access to the server room be easily denied?	☐	☐	
16. Are visitors supervised and required to wear a visible authorisation badge, or their date and time of entry and departure recorded?	☐	☐	
17. Are staff instructed to challenge strangers?	☐	☐	

Risk – Room	Yes	No	Comments
18. Is the server room used for anything else?	☐	☐	
19. Is the server room on the ground floor?	☐	☐	
20. Are the servers and comms. equipment stored in approved, lockable cabinets?	☐	☐	
21. Windows secure?	☐	☐	
22. Is the room covered by an intruder alarm?	☐	☐	
23. Risk of liquid damage (flooding, leaks etc.)	☐	☐	
24. Are there fire and/or smoke sensors?	☐	☐	
25. Location of fire alarm and is alarm bell audible in room?	☐	☐	
26. Location and type of fire extinguishers? (Last checked?)	☐	☐	
27. Is the temperature of the server room monitored and controlled? Who is notified?	☐	☐	

Risk – Room	Yes	No	Comments
28. Is there any air conditioning? If so - check intake and extract vents for vulnerabilities to blockage.	☐	☐	
29. Is there any air conditioning? If so - check intake and extract vents for vulnerabilities to blockage.	☐	☐	
30. Is the quality of power supply monitored and controlled?	☐	☐	
31. Is eating and drinking allowed in the server room?	☐	☐	
32. Is the server room tidy and clear of surplus equipment and waste?	☐	☐	
33. Is the server room clean and free from dust?	☐	☐	
34. Are any patch leads properly routed in a tidy fashion?	☐	☐	
35. Are any power leads properly routed in a tidy fashion without the need for extension leads?	☐	☐	
36. Are any servers and comms. Equipment easily accessible without risk from slip, trip or fall hazards or risk of injury or other health and safety issues?	☐	☐	

Risk – Building / Estates	Yes	No	Comments
37. Are the Air Con vents checked for blockages?	☐	☐	
38. Are the Cables checked against rodent/animal damage?	☐	☐	
39. Is the Building protected against lightning strikes?	☐	☐	

Risk – Business Continuity / Disaster Recovery	Yes	No	Comments
40. Is there an adequate business continuity plan documenting how day to day business activity would continue in the event of a disaster affecting the server room?	☐	☐	

Risk – Business Continuity / Disaster Recovery	Yes	No	Comments
41. Is any BCP routinely and regularly tested and updated under change control procedures?	☐	☐	
42. Is there an adequate disaster recovery plan documenting how the servers and any data would be recovered in the event of a disaster affecting the server room?	☐	☐	
43. Is any DR plan routinely and regularly tested and updated under change control procedures?	☐	☐	

Appendix 5: Server room risk assessment template

Server room:

Servers	Date

Data	Review date

Threat	Vulnerability	Control Measures - checklist	Weakness identified	Consequence	Likelihood	Score	Add. Controls	Consequence	Likelihood	Score	Action/ Update
Fire				4	1	4					
	Fire in server room - loss of servers and data	Room is free of combustible materials									
		Clear from chemicals/accelerants									
		Fire/smoke sensors present									
		Location of the correct type of fire extinguishers (CO2 or Foam) are known and in close proximity.									
		Backup procedures implemented, as per policy									
	Stop/slow down the spread of fire within a building	Fire Alarms regularly tested									
		Server room fitted with a fire-resistant door, which is to be remained shut when not in use									
	Informing staff working within the server room if fire	The fire alarm bell is audible to staff whilst in the room									

	has been detected										
	Loss of entire building	Back up tapes stored in a fireproof safe or in a secure offsite location									
Flood				4	1	4					
	Servers exposed to water - loss of servers and data	Server room located above ground level									
		Backup procedures implemented as per policy									
Electrical Storms				3	1	3					
	Loss of servers and data due to lightning strike	The building is protected by adequate lightening conductors									
		Backup procedures implemented as per policy									
Other (e.g., earthquake)				4	1	4					
	Any disaster leading to the loss of servers/data	Backup procedures implemented as per policy									
Unauthorised Access				3	1	3					
	Physical breach - General	Server room locked at all times									
		No windows/secured windows									
		security/intruder alarm installed									
		Server and communications equipment stored in a lockable cabinet									
	Physical Breach - Public	Server room not located in a publicly accessible area									

		Members of the public to sign in and out from premises									
		Public to wear 'visitors' passes									
		Members of the public to be escorted at all times on the premises									
		Staff instructed to challenge strangers									
	Physical Breach - Staff	Server room access to be restricted to designated members of staff (keypad code or key lock)									
		Key to room to be held securely by designated key holder									
		Access to room removed when previously authorised staff leave organisation									
		Server room not used for any other purpose									

Unauthorised Disclosure				4	1	4					
	Backup tapes	Tapes stored in a restricted, secure area									
		Tapes clearly marked									
		Tape failures are recorded on the backup log and CITS notified for disposal									
		Disposal of tapes in accordance with the Disposal Policy									
	Disks	Disposal of disks in accordance with the Disposal Policy									

	Hacking	Server Admin Passwords changed regularly and with sufficient complexity. Only given to System Admins.									
		Servers to be protected by Firewall									
		Firewall penetration test									
Data Loss				4	1	4					
	Malicious Code	Anti-Virus installed									
	Accidental	Backup/Restoration procedures implemented as per policy									
	Back Ups	Tape unit regularly cleaned with cleaning tape and recorded									
		Tape Failures logged									
		Restoring of data has been checked.									
Damage				3	1	3					
	Slips, Trips and Falls	Server Room Tidy and free from boxes and surplus equipment									
		Access to Servers (including rear of cabinet) unimpeded									
	Physical	Cables tidy and un-stressed									
Environmental				4	1	4					
	Fluctuations in Power - damage to Server	Surge Protection									
	Loss of Power - data corruption	Uninterruptible Power Supply (with auto shut down)									

		UPS under maintenance contract/regularly tested									
	Static - damage to servers	Any personnel working on the server with be earthed with an earthing strip or use an anti-static mat									
	Over heating	Air Conditioning installed									
		Air Conditioning maintenance contract (to include regular preventative maintenance procedures)									
		Auto shutdown/alert sent to engineer when a temperature is reached									
	Leaks	Pipe work is kept to minimum and in good state of repair									
	Dust	Room is cleaned and kept dust free									

Appendix 6: National data destruction guidelines

NHS digital: destruction and disposal of sensitive data – Good Practice Guidelines v3.2 (2017)

Media Type	Data Storage Mechanism	Suggested Removal Methods
Hard Disk Drives (HDD)	Non-volatile magnetic	Multi Pass Pattern wiping, degaussing, disintegration or incineration
Solid State Disk Drives (SSD)	Non-volatile solid-state memory	Multi Pass Pattern wiping, disintegration
CD-R / DVD-R	Write once optical	Abrasion, disintegration, incineration
CD-RW / DVD-RW	Write many optical	Abrasion, disintegration, incineration
BD-R	Write once optical	Abrasion, disintegration, incineration
BD-RE	Write many optical	Abrasion, disintegration, incineration
Ultra-Density Optical (UDO)	Write once or write many optical	Abrasion, disintegration, incineration
Magnetic Tape	Non-volatile magnetic	Degaussing, disintegration, incineration
Flash Disk Drives and USB	Non-volatile solid-state memory	Multi Pass Pattern wiping, disintegration
Paper based	Printed	Micro Cross Cut Shredding, incineration
X-Ray Film	Photographic film	Shredding, metal recovery

Centre for the Protection of National Infrastructure (CPNI)
Secure Destruction of Sensitive Items: CPNI Standard – April 2014
This standard supersedes the following withdrawn standards:

- SEAP 8100 – Destruction equipment Security Equipment Assessment Panel, June 1998
- SEAP 8200 – Central destruction facilities Security Equipment Assessment Panel, June 1998
- Requirements for secure destruction – Interim standard CPNI, September 2012

Sensitive item	Process*	Required outcome
Digital memory	Cutting using a guillotine	2mm (any direction) particle
	Disintegration Hammer-milling Shredding	6mm (any direction) particle
Floppy disk	Bathing in chemical or acid	Remove recording surface
	Cutting using a guillotine	3mm (any direction) particle
	Disintegration Shredding	6mm (any direction) particle
Hard disk	Bathing in chemical or acid	Remove recording surface
	Cutting using a guillotine	3mm (any direction) particle
	Disintegration Hammer-milling Shredding	6mm (any direction) particle
Magnetic tape	Bathing in chemical or acid	Remove recording surface
	Disintegration Shredding	6mm (any direction) particle
	Smelting	Liquid slag or metal
Microform	Disintegration Shredding	2mm (any direction) particle
Optical disc	Cutting using a guillotine Disintegration Shredding	2mm (any direction) particle
	Grinding or scrubbing	Remove recording surface
Paper	Disintegration	6mm (any direction) particle
	Pulping	Remove all characters
	Shredding (cross cut)	15mm x 4mm for ‘sensitive’ paper records
SIM or smart card	Disintegration Shredding	2mm (any direction) particle
Visual display unit	Disintegration Hammer-milling Shredding	6mm (any direction) particle