Network Security Policy

Contents

1. Introduction. 2
2. Aims and Objectives. 2
3. Definitions 2
4. Policy Statement 2
5. Arrangements 3
6. Risk Assessment 4
7. Responsibilities 7
8. Competence 8
9. Monitoring 9
10. Audit and Review 9
11. Equality Impact Appraisal 9

1. Introduction.

1.1. This document defines the Network Security Policy for South East Coast Ambulance Service NHS Foundation Trust ('the Trust'). The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network. This document sets out the Trust's policy for the protection of the confidentiality, integrity and availability of the network. It establishes the security responsibilities for network security and provides reference to documentation relevant to this policy.

2. Aims and Objectives.

2.1. The aim of this policy is to ensure the security of the Trust's network. **To do this the Trust will:**

- Ensure that the network is available for users.
- Preserve integrity by protecting the network from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets.
- Preserve confidentiality by protecting assets against unauthorised disclosure.

3. Definitions

3.1. The network consists of a collection of communication equipment such as switches and routers which acts as an infrastructure to support the interconnection of information systems and devices such as servers, printers and personal computers.

4. Policy Statement

4.1. This policy applies to all networks within the Trust used for:

- The storage, sharing and transmission of non-clinical data and images.
- The storage, sharing and transmission of clinical data and images.
- Printing or scanning non-clinical or clinical data or images.
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images.

5. Arrangements

5.1. The overall Network Security Policy for the Trust is described below.

5.2. The Trust information network will be available when needed. It can be accessed only by legitimate users and will contain complete and accurate information.

5.3. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this**, the Trust will undertake to the following:**

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost-effective manner.

5.4. The Trust will comply with appropriate legislation. **The following list is not exhaustive and may be added to over time:**

- Copyright, Designs & Patents Act 1988.
- Access to Health Records Act 1990.
- Computer Misuse Act 1990.
- The Data Protection Act 2018.
- The General Data Protection Regulation 2018.
- The Human Rights Act 1998.
- Electronic Communications Act 2000.
- Regulation of Investigatory Powers Act 2000.
- Investigatory Powers Act 2016.
- Freedom of Information Act 2000.
- Health & Social Care Act 2012.

5.5. **CHECK** is the scheme under which **NCSC** approved companies can conduct authorised penetration tests of public sector and **CNI** systems and networks.

6. Risk Assessment

6.1. The Trust will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

6.2. Risk assessment will be conducted annually by the IT Senior Infrastructure Engineer to determine the Common Criteria for Information Technology Security Evaluation Criteria (Common Criteria) assurance levels required for security barriers that protect the network.

6.3. Unless dictated otherwise by relevant authorities such as NHS Digital, formal risk assessments will be conducted using the Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM) and will conform to the CHECK Scheme.

6.4. Physical and Environmental Security.

6.4.1. Network computer equipment will be housed in a controlled and secure environment.

6.4.2. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

6.4.3. Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

6.4.4. The IT Head of Infrastructure & Networks is responsible for ensuring that door lock codes (where applicable) or access control permissions are reviewed/changed following a compromise.

6.4.5. Critical or sensitive network equipment will be protected from power supply failures. It will be protected by intruder alarms, environmental controls and fire suppression systems. Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

6.5. Access Control to Secure Network Areas.

6.5.1. Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The IT Head of Infrastructure & Networks will periodically review a list of those with unsupervised access.

6.5.2. All visitors to secure network areas must be authorised by the IT Security Manager or IT Senior Infrastructure Engineer. Such visitors will be made aware of their security obligations and will record their attendance and purpose via an IT visitors' book. The IT Senior Infrastructure Engineer will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

6.6. Access Control to the Network.

6.6.1. Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to the Trust's Remote Access Policy.

6.6.2. There must be a formal, documented user registration and de-registration procedure for access to the network. A relevant line manager must approve user access. Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.

6.6.3. Security privileges (i.e. Elevated privileges, 'super-user' or network administrator rights) to the network will be highly moderated and allocated on the requirements of the user's job/role, rather than on a status basis.

6.6.4. All network users will have their own individual user identification and password. Users are responsible for ensuring their password is kept securely and confidentially (see User Responsibilities). User access rights will be immediately removed or reviewed for those users who have left the Trust, are seconded or changed jobs as notified by the HR Service Centre or appropriate line management.

6.6.5. All network users who also have security privileges will have separate accounts for their 'day to day access and their elevated privileges. These accounts must NOT have the same password or derivative of.

6.7. Third Party Access Control to the Network

6.7.1. Third party access to the network will be based on a formal contract that satisfies all necessary NHS governance requirements which includes the signing of an Information Sharing Agreement. All third-party access to the network must be authorised, logged and reviewed by the IT Security Manager.

6.8. External Network Connections

6.8.1. All connections to external networks and systems will be documented and receive approval from the senior IT management team before they commence operation. Such connections to external networks and systems will conform to the NHS-wide Network Security Policy, relevant Codes of Connection and supporting guidance.

6.9. Maintenance Contracts

6.9.1. The IT Services Manager will ensure that maintenance contracts for network equipment are maintained and annually reviewed where necessary. All contract details will constitute part of the Trust's Information Asset register.

6.10. Data Exchange

6.10.1. Agreements must exist between local organisations and the Trust in respect of data sharing. Such arrangements are formalised within Local Information Sharing Protocols.

6.11. Fault Logging

6.11.1. The IT Senior Infrastructure Engineer is responsible for ensuring that all network faults or risks are logged and reviewed and resolved or mitigated.

6.12. Security Operating Procedures (SyOps)

6.12.1. The Trust will produce Security Operating Procedures (SyOps) and security contingency plans that reflect the Network Security Policy. Changes to operating procedures must be authorised by the IT management team.

6.13. Network Operating Procedures

6.13.1. Documented operating procedures will be prepared for the operation of the network, to ensure its correct, secure operation. Changes to operating procedures must be authorised by the IT Senior Infrastructure Engineer.

6.14. Network Device Backup and Restoration

6.14.1. The IT Senior Infrastructure Engineer is responsible for ensuring that automated backup copies of network configuration data are taken routinely, prior and post each change.

6.15. Accreditation of Network Systems

6.15.1. The Head of Infrastructure & Networks will approve new network systems before they commence operation. The Head of Infrastructure & Networks is responsible for ensuring that the network does not pose an unacceptable security risk to the Trust.

6.16. System Change Control

6.16.1. The Change Advisory Board will review configuration changes to the network. The IT Senior Infrastructure Engineer is responsible for updating all relevant policies, design documentation and procedures. Testing facilities will be used for all new network systems. Test, training and live facilities will be separated where necessary.

6.17. Security Monitoring

6.17.1. The network will be monitored for potential security breaches. This will be undertaken by infrastructure team.

6.18. Reporting Security Incidents and Weaknesses.

6.18.1. All potential security breaches must be recorded, investigated and reported by the Senior Infrastructure Engineer and IT Security Specialist. Security incidents and weaknesses must be reported using the Incident Reporting form IWR-1 in accordance with the requirements of the Trust's incident reporting policy and procedure.

6.19. System Configuration Management.

6.19.1. A reliable and consistent backup and archiving management system for the network will operate on all network platforms.

6.20. Business Continuity and Disaster Recovery Plans.

6.20.1. In the event of major failure, the business continuity plans, and disaster recovery plans will be implemented. Access will be contained within the Business Continuity Management Plan produced for the Trust. The plans must be reviewed by the senior IT management team and tested in accordance with the arrangements contained within the plan.

6.21. **Unattended Equipment and Clear Screen.**

6.21.1. Users must ensure that they protect the network from unauthorised access. They must log off the network when their work is finished. The Trust operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked, or a screensaver password activated whenever a workstation is left unattended. Users failing to comply may be subject to disciplinary action.

7. Responsibilities

7.1. Director of Finance and Corporate Services.

7.1.1. The Chief Executive has delegated the overall responsibility for the development and implementation of the Trust's Information, Network and System Security policies. The Associate Director of Information Technology has responsibility for implementing this policy within the context of IT systems development and use in the Trust is delegated further to the Head of Infrastructure and Networks.

7.2. Head of Infrastructure and Networks.

7.2.1. The Head of Infrastructure and Networks is responsible for:

- Producing and implementing effective security countermeasures.

- Production of all relevant security documentation; SyOps and contingency plans reflecting the requirements of the Network Security Policy.

- Ensuring all such documentation is forwarded to the relevant authority for inclusion in the Trust's
- Information Asset register.

- Providing advice on how to determine and implement an appropriate level of security.

- Local Managers.

7.2.2. All local Managers will have responsibilities for the network in their own area of work and will:

- Safeguard the security of the network, by ensuring that information, hardware and software used by staff and, where appropriate, by third parties, is consistent with legal and management requirements and obligations contained in the associated documentation.

- Ensure that personnel are made aware of their own security responsibilities contained in the associated documentation.

- Ensure that staff undergoes suitable security training.

7.3. All Users.

7.3.1. All Users will comply with this Policy.

7.3.2. All staff or agents acting for the Trust have a duty to comply with this policy and:

- Safeguard hardware, software and information in their care.

- Prevent the introduction of malicious software on the Trust's IT systems.

- Report any suspected or actual breaches in security in accordance with the Trust's Incident

- Reporting Policy and Procedure.

8. Competence

8.1 All staff will receive training on information security at induction and annually via statutory and mandatory training programmes. Managers and those with specific responsibility for information security will receive training appropriate to their level of responsibility. All users of the network will be provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions by users may result in disciplinary action(s).

9. Monitoring

9.1. The IT Security Manager will monitor compliance with this policy as part of the annual system of information security audits. Where the Trust deems appropriate, internal audit will be asked to conduct information security audits.

10. Audit and Review

10.1. This policy will be reviewed every three years or sooner should new systems, legislation, national guidance, or local governance arrangements change.

11. Equality Impact Appraisal

11.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

11.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.