Network Security Policy

[This is a complicated policy which will not be relevant for many Care Providers, and for those for whom it is necessary you may find that your ICT Supplier/Support will be able to monitor, audit or otherwise check much of the procedures which are outlined below. There is extensive guidance on network security here: https://www.digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/network-security

1. Introduction

1.1. This Network Security Policy is the overarching policy for data security and protection for ***Insert Organisation Name Here*** (hereafter referred to as "us", "we", or "our").

1.2. 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

2. Purpose

2.1. The purpose of this policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the Data Protection Act (1998), the forthcoming General Data Protection Regulations (2016) and Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

2.2. This policy covers how we protect the confidentiality, integrity and availability of the network, establishes responsibilities for network security and provides reference to documentation relevant to this policy.

3. Scope

3.1. This policy includes in its scope all data which is stored, recorded or transferred and of which we can reasonably be stated to be either the data controller or data processor, this includes special categories of data.

3.2. This policy applies to all staff, including temporary staff and contractors

3.3. This policy applies to our networks which are used for:

3.3.1. The storage, sharing and transmission of non-clinical data and images;

3.3.2. The storage, sharing and transmission of clinical data and images;

3.3.3. Printing or scanning non-clinical or clinical data or images;

3.3.4. The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images.

4. The Policy

4.1. ***Insert organisation name here***'s information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information.

4.2. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this we undertake to:

4.2.1. Protect all hardware, software and information assets under its control;

4.2.2. Provide effective protection that is commensurate with the risks to its network assets;

4.2.3. Implement the Network Security Policy in a consistent timely manner;

4.2.4. To comply with all relevant legislation.

5. Risk Assessments

5.1. We 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.

5.2. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

6. Physical & Environmental Security

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

6.2. **[Insert job title here]** is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if she/he suspects the

code has been compromised, or when required to do so by the Data Protection Lead.

6.3. Critical or sensitive network equipment will be protected from power supply failures.

6.4. Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.

6.5. Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

6.6. **[Insert job title here]** is responsible for authorising all visitors to secure network areas and for making visitors aware of network security requirements.

6.7. All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

6.8. **[Insert job title here]** will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

7. Access Control to Secure Network Areas

7.1. Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it.

7.2. **[Insert job title here]** will maintain and periodically review a list of those with unsupervised access.

8. Access Control to the Network

8.1. 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 Remote Access Policy.

8.2. Third party access to the network will be based on a formal contract.

8.3. All third-party access to the network must be logged.

9. External Network Connections

9.1. Ensure that all connections to external networks and systems have documented and approved System Security Policies.

9.2. **[Insert job title here]** must approve all connections to external networks and systems before they commence operation.

10. Maintenance Contracts

10.1. **[Insert job title here]** will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

10.2. All contract details will constitute part of the Information Asset register **[insert IAR location here]**.

11. Data and Software Exchange

11.1. Formal agreements for the exchange of data and software between organisations must be established and approved by **[insert job title here]**

12. Fault Logging

12.1. **[Insert job title here]** is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures can be located **[insert location here]**.

13. Security Operating Procedures

13.1. Changes to operating procedures must be authorised by **[insert job title here]**.

14. Network Operating Procedures

14.1. Changes to operating procedures must be authorised by **[insert job title here]**.

15. Data Backup and Restoration

15.1. Data backup procedures are outlined in the Emergency and Business Continuity Plan document.

16. User Responsibilities, Awareness & Training

16.1. We will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

16.2. These procedures will be outlined in the staff handbook.

17. Accreditation of Network Systems

17.1. **[Insert job title here]** is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation. They will require checks on, or an audit of, actual implementations based on approved security policies.

18. Malicious Software

18.1. Ensure that measures are in place to detect and protect the network from viruses and other malicious software.

19. Secure Disposal or Re-use of Equipment

19.1. Ensure that where equipment is being disposed of all data on the equipment (*e.g.* on hard disks or tapes) is securely overwritten.

20. System Change Control

20.1. **[Insert job title here]** is responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

21. Reporting Security Incidents & Weaknesses

21.1. All potential security breaches must be investigated and reported to the Data Protection Lead and an Information Security Incident Report Form must be completed.

22. Business Continuity & Disaster Recovery Plans

22.1. Ensure that business continuity plans are produced for the network.

22.2. The plans must be reviewed and tested on a regular basis.

23. Approval

23.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	
Signature	

Approval Date	
Review Date	