



v1.0

www.echogenicity.co.uk

Network Security Policy

1. Introduction

- 1.1. This Network Security Policy is the overarching policy for data security and protection for Echogenicity Limited (hereafter referred to as “us”, “we”, or “our”).

2. Purpose

- 2.1. This document sets out our policy for the protection of 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 applies to all staff, including temporary staff and contractors.
- 3.2. This policy applies to our networks which are used for:
- 3.3. The storage, sharing and transmission of non-clinical data and images;
- 3.4. The storage, sharing and transmission of clinical data and images;
- 3.5. Printing or scanning non-clinical or clinical data or images;
- 3.6. The provision of internet systems for receiving, sending and storing non-clinical or clinical data or images.

4. Policy

- 4.1. Echogenicity Limited’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:

- 4.3. Protect all hardware, software and information assets under its control;
- 4.4. Provide effective protection that is commensurate with the risks to its network assets;
- 4.5. Implement the Network Security Policy in a consistent and timely manner;
- 4.6. 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. Verity Williams Curnow 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.
- 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. Verity Williams Curnow is responsible for authorising all visitors to secure network areas and for making visitors aware of network security requirements.

Scanning Cornwall’s Hearts

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. Verity Williams Curnow 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. Verity Williams Curnow 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 written contract.

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

9. External network connections

9.1. We will ensure that all connections to external networks and systems have documented.

9.2. Verity Williams Curnow must approve all connections to external networks and systems before they commence operation.

10. Maintenance contracts

10.1. Verity Williams Curnow 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 (IAR).

11. Data & software exchange

11.1. Formal agreements for the exchange of data and software between organisations must be established and approved by Verity Williams Curnow.

11.2. All exchanges of data between organisations will be recorded on the Record of Processing Activities (ROPA).

12. Fault logging

12.1. Verity Williams Curnow 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 are located in Echogenicity Head office.

13. Security operating procedures

13.1. Insert your security operating procedures here.

13.2. Changes to operating procedures must be authorised by Verity Williams Curnow.

14. Network operating procedures

14.1. Insert your network operating procedures here.

14.2. Changes to operating procedures must be authorised by Verity Williams Curnow.

15. Data backup & restoration

15.1. Ultraling/TM3/Cornwall IT are responsible for Data backup procedures

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 training to discharge their security responsibilities.

Scanning Cornwall's Hearts

16.2. These procedures will be outlined during staff induction and annual mandatory training.

17. Accreditation of network systems

17.1. Verity Williams Curnow 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. We will 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. We will ensure that where equipment is being disposed of all data on the equipment (e.g. on hard disks or tapes) is disposed of in-line with our Record Keeping Policy.

20. System change control

20.1. Verity Williams Curnow 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 Security and Protection Lead and an Information Security Incident Report Form must be completed.

21.2. We will follow the procedures set out in the Data Security Policy.

22. Business continuity & disaster recovery plans

22.1. We will ensure that business continuity plans are produced for the network.

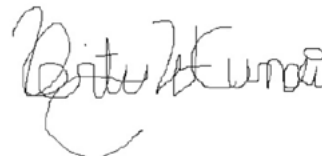
22.2. The plans must be reviewed and tested on a regular basis.

23. Approval

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

Name: Verity Williams Curnow

Signature:



Approval Date: 05.02.2024

Review Date: 05.02.2024

Scanning Cornwall's Hearts