|  |  |
| --- | --- |
| **Policy/Procedure Title:** | **Network Security Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | Information Governance | | |
| **Number** | **IG-10 Network Security Policy** | | |
| **Author** |  | **Ratified by** |  |
| **Date Written** |  | **Ratification date** |  |
| **Date Distributed** |  | **Review date** |  |
| **Responsible Committee** |  |  |  |
| **Version Number:** | **Date:** | **Supersedes Version No:** | |
| 1 |  |  | |

These procedures are applicable to staff employed by and/or working for and/or delivering services to or on behalf xxxxxxxxxxxxxxxxxxx

This policy applies to the following group(s) of staff:

|  |  |
| --- | --- |
| **Staff Group** | **Yes** |
| Head Office |  |
| Clinical Staff |  |
| Non-clinical staff |  |
|  |  |
|  |  |
|  |  |

**Signed on behalf of xxxxxxxxxxxxxxxxx**

**Chief Executive Date:**

# POLICY STATEMENT

1.1. This document defines the Network Security Policy for xxxxxxxxxxxxxxxxx

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.

1.3. This document: sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network, establishes the security responsibilities for network security and provides reference to documentation relevant to this policy.

# OBJECTIVE

2.1. The objective of this policy is to define controls implemented within the realm of IT to ensure the security of the organisation’s network.

# SCOPE OF POLICY

3.1. This policy does not form part of any user’s contract of employment and it may be amended at any time.

# RESPONSIBILITIES

4.1. Each of the following roles are responsible for compliance with this policy:

## Chief Executive

The Chief Executive of xxxxxxxxxxxxx has overall responsibility within the organisation for compliance with data protection requirements. The development, implementation of, and compliance with this policy is delegated to the Data, Information and Communication Officer.

## Data Controller

The Data Controller will ensure that the Chief Executive is kept up to date and briefed on all information governance and information security issues which affect the organisation.

## Information Governance Lead

The IG Lead will act as the first point of contact for training, advice and support for all users on matters relating to information governance and data protection which may arise within the organisation. In addition they will lead any investigation of any suspected breaches of this policy.

## IT Officer

The IT Officer will have responsibility for managing the equipment and devices within the organisation, utilising technical controls as described in this policy.

## User Responsibilities

Every employee in the organisation (whether employed, self-employed, consultant, locum, contractor or agency) has individual responsibility for complying with this policy. All users should therefore ensure that they take the time to read and understand it fully.

# TECHNICAL CONTROLS

5.1. The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables or wirelessly. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

5.2. This policy applies to all networks within the organisation 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 nonclinical or clinical data or images.

5.3. The overall Network Security Policy the organisation is described below: The network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. In order to achieve this, the following controls and counter-measures are in place:

* Network computer equipment is housed in a controlled and secure environment in the Stationery Cupboard in Head Office and remote servers provided by Beyond Networks.
* Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
* Critical or sensitive network equipment will be protected from power supply failures.
* All visitors to secure network areas must be signed in and accompanied by the IT Lead. Visitors must be logged in and out of the computer room. The log will contain name, organisation, purpose of visit, date, and time in and out.
* Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. This is controlled using ????? by Beyond Networks.
* User access will only be granted on receipt of a New User/Equipment Request form.
* Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
* All users to the network will have their own individual user identification and password.
* Users are responsible for ensuring their password is kept secret and not shared under any circumstances.
* User access rights will be immediately removed or reviewed for those users who have left the organisation or changed jobs.
* Remote access to the network is not available
* All computer hardware is protected from unauthorised access by ???????? disk encryption
* All computer hardware is protected from virus activity using ??????????
* All incoming and outgoing email is filtered using ???????? email content filtering.
* All web traffic is monitored using ????????????? web content filtering.
* Windows critical updates are pushed out to users machines using ??????????????? Microsoft WSUS services.
* Network data is backed up using ????????????????.
* Maintenance contracts are in place for all critical infrastructure components
* IT Equipment is securely disposed and certifcates of destruction are obtained for disk drives disposed of in this way.
* Change logging is in place for network and server changes
* A risk register is maintained for all operational IT risks
* Regular penetration tests/security audits are undertaken to ensure appropriate network protection.

# MONITORING

6.1. IT resources and communications systems and their contents may be the property of the organisation. Therefore, users should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

6.2. The organisation reserves the right to monitor, intercept and review, without further notice, user activities using our IT resources and communications systems, to ensure that our rules are being complied with and for legitimate business purposes and users consent to such monitoring by their use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

6.3. Copies of such data or communications may be stored for a period of time after they are created, and may be deleted from time to time without notice.

6.4. Users must not use our IT resources and communications systems for any matter that they wish to be kept private or confidential from the organisation.

# MONITORING AND REVIEW OF THIS POLICY

7.1. The Information Governance Lead will be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

7.2. For questions regarding this policy from an IT perspective, please contact the Data, Information and Communications Officer.

7.3. For questions regarding this policy from an information governance perspective, please contact the Head of Information Governance

References

Key references e.g. national guidance or legislation used in developing the policy/procedure

* Data Protection Act 1998

Document Control:

|  |  |  |
| --- | --- | --- |
| Version number: | Date: | Supersedes version number: |
| V1 |  |  |
|  |  |  |
|  |  |  |