Northern Ireland Blood Transfusion Service **POLICY DOCUMENT**

Document Details

Document Number: POL:00:IP:005:04:NIBT **No. of Appendices:** None
Supersedes Number: POL:00:IP:005:03:NIBT

Document Title: NIBTS COMPUTER SECURITY POLICY

ISSUE DATE: 17TH MAY 2024 **EFFECTIVE DATE: 31ST MAY 2024**

Document Authorisation

Written By: David Moore, IM& Manager

Signature: David Moore IM&T Manager **Date:** 30.04.2024

Authorised By: Glenn Bell Finance Manager

Signature: G Bell, Finance Manager **Date:** 30.04.2024

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998.

CROSS REFERENCES

This Policy refers to the following documents:

Doc Type	Doc. No.	Title
Policy	IP:001	NIBTS Email and Internet Acceptable Use Policy
Policy	IP:003	NIBTS Management of User Accounts and Passwords
Policy	IP:004	NIBTS Controls Against Malicious Software

Key Change from Previous Revision:

Amendments to provide upstream reference to wider HSC Information Security Policy.

1. STATEMENT

Aims of the policy

The Information Security Policy details the organisation's approach to Information Security Management and is aligned to the HSCNI Information Security Policy which applies across the wider HSC.

This policy, and any associated Information Security standards, lay down a range of principles and expectations which will ensure a consistent and high standard of Information Security management across the organisation from all significant threats whether internal, external, deliberate or accidental.

2. OVERVIEW

2.1. The Information Security Policy will set out the expected standards for both user behaviour and technical controls to ensure a robust Information Security posture is maintained in the organisation. This policy is supported by an acceptable use policy (AUP), user account management policy and security controls policy (IP001, IP003 and IP004 respectively).

This policy applies throughout the entire information lifecycle from acquisition or creation, through utilisation to storage and disposal.

Breaches of this policy may result in disciplinary action being taken.

3. RESPONSIBILITY

3.1. It is the responsibility of all staff with access to IT systems in NIBTS to ensure that the policy as detailed below is followed to ensure safe and secure access to such systems. Any breach in relation to this policy or subordinate policies should be reported to the staff member's line manager and the IT Security Officer or IM&T Manager to ensure that the safety and security of systems and data is maintained.

4. POLICY

4.1. NIBTS recognises the importance of effective information security controls given the level of donor and patient information which the organisation processes. As a special agency of the HSC, it is appropriate to ensure alignment with adopted HSC standards and processes in regards to Information Security in order to provide a robust, unified approach across the whole HSC.

4.2. NIBTS will employ appropriate administrative and technical control mechanisms to provide assurance that information security controls are being appropriately managed and are effective. These work together to ensure a robust approach to information security is attained.

4.3. Examples of policy or procedural controls would include the following:

- Third party management
- Data classification and records management
- Data encryption
- Information asset and system management
- Standards for use of email and internet services
- Information flow and data transfer
- Management of user accounts and passwords
- Remote working arrangements
- Controls against malicious software
- Vulnerability and patch management
- Security training and awareness
- Backup and business continuity
- Security incident management
- Physical and environmental security
- Clear desk and screen
- Risk management
- Audit and accountability

4.4. Users are required to comply with the organisation's relevant acceptable use policy and exercise care in the use or transport of any equipment that is either assigned to them or to which they have access.

4.5. Examples of exercising due care and attention would include:

- Never sharing logon credentials, no matter whom it may be.
- Not leaving workstations unattended while logged in – users should either 'lock' the screen or logoff.
- Appropriate handling of laptop computers and equipment during transport and use – taking particular care that they not be left unattended in vehicles or when used remotely.

4.6. Users should not seek to change, deactivate or otherwise interfere with existing controls. Attempting to do so may introduce vulnerabilities to the security and integrity of systems in use within NIBTS.

Any such interference may result in disciplinary action being taken.

5. EQUALITY SCREENING OUTCOME

This policy has been drawn up and reviewed in light of the statutory obligations contained within Section 75 of the Northern Ireland Act (1998). In line with this statutory duty of equality this policy has been screened against particular criteria. If at any stage of the life of the policy there are any issues within the policy which are perceived by any party as creating adverse impacts on any of the groups under Section 75 that party should bring these to the attention of the Head of HR & Corporate Services.

The Northern Ireland Blood Transfusion Service is committed to the promotion of equality of opportunity for staff, donors and service users. We strive to ensure that everyone is treated fairly and that their rights are respected at all times. We believe that it is important that our policy is understood by all those whose literacy is limited, those who do not speak English as a first language or those who face communication barriers because of a disability. On request it may be possible to make this policy available in alternative formats such as large print, Braille, disk, audio file, audio cassette, Easy Read or in minority languages to meet the needs of those not fluent in English.

6. TRAINING REQUIREMENTS

All staff who make use of IT systems in NIBTS are required to read this policy and confirm that they have read and understood its content.

Additional assistance in relation to the use of NIBTS IT systems will be made available for those members of staff who may require it.