Health and Social Care

Northern Ireland Fire & Rescue Service

Information Security

1.05 Clear Desk and Screen All User Standard

Approval

Document Reference	Information Security - 1.05 Clear Desk and Screen - All User Standard
Version	0.2
Last updated	07th March 2021
Owner	
Approval by	

Contents

1. INTRODUCTION

Health and Social Care (HSC) and Northern Ireland Fire and Rescue Service (NIFRS) (herein HSC will refer to all HSC and NIFRS organisations) Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

A common source of information loss originates from information being left insecure and unattended in their work area. To mitigate this risk, the confidentiality and integrity of information must be ensured when staff are not physically present. A further risk occurs when using computer screens, as overlookers could have visual access to information that they should not have access.

2. PURPOSE

The purpose of this policy is to protect Health and Social Care (HSC) and Northern Ireland Fire and Rescue Service (NIFRS) information from unauthorised disclosure, loss or damage. It establishes minimum requirements for a clear desk and screen environment, addressing the protection of hardcopy information, removable media and on-screen information.

3. SCOPE

This Information Security Standard applies to:

- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC or NIFRS [1], including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - Third Party Contractors;
    - Any other party making use of HSC ICT resources;
- HSC information stored, or in use, on HSC or externally hosted systems;
- Information in transit across the HSC networks;
- Information leaving HSC networks; and
- ICT Systems belonging to or under the control of HSC.

This Standard applies throughout the entire information lifecycle from acquisition/creation through utilisation to storage and disposal.

[1] Northern Ireland Health & Social Care organisations include Health & Social Care Board (HSCB), Public Health Agency (PHA), Health & Social Care Trusts, NI Ambulance Service (NIAS), Business Services Organisation (BSO), Patient & Client Council (PCC), Regulation & Quality Improvement Authority (RQIA), NI Guardian Ad Litem Agency (NIGALA), NI Blood Transfusion Service (NIBTS), NI Social Care Council (NISCC), NI Practice and Education Council for Nursing and Midwifery (NIPEC), NI Medical and Dental Training Agency (NIMDTA), GP Practices and other Independent Contractors to HSC, and Northern Ireland Fire and Rescue Service (NIFRS).

4. STANDARD NON-COMPLIANCE / BREACH

See the Information Security Policy for details of what to do in the event of non-compliance or a breach of an Information Security Standard. For an information Security Breach or Incident, see the Information Security Incident Identification and Reporting All User Standard.

5. CLEAR DESK AND SCREEN

5.1. PHYSICAL ENVIRONMENT

Desk and Office Environment

5.1.1. All staff must ensure personal information or business sensitive information is not left in view or unattended at any time. This includes personal information or business sensitive information contained within hard copy documents or notes left on desks, printers, on top of filing cabinets etc. in addition to being visible on computer screens. Where the use of screen reading software for employees with sight loss is required, headphones or a private area must be provided to avoid potential disclosure of personal or confidential material.

5.1.2. When hard copy information is no longer required, all staff must either dispose of or secure the information (e.g. secured in a locker or shredded).

5.1.3. Ensure digital content on screen is not available or accessible to others when not attended (e.g. use a privacy screen during use and locking the screen when unattended).

5.1.4. Staff must make use of collaboration equipment, including but not limited to whiteboards, flipcharts, post-it walls, in a manner that ensures the protection of any personal information or sensitive business information. This may be to use the equipment out of view of unauthorised individuals and erasing the content when it is no longer required or is to be left unattended, unless it can be secured and made non-visible.

5.1.5. Portable devices, such as mobile phones, that contain personal information or business sensitive information must be secured in line with local device policy, including but not limited to the use of encryption, a strong passcode, and not leaving the device unattended or unlocked.

5.1.6. Workplace furniture shall be positioned so that personal information or business sensitive material is not visible from either the windows or the hallway. Where this is not possible, compensating controls, such as closing blinds or using privacy screens, must be implemented.

5.1.7. Equipment in public areas must be locked with an approved locking cable or locked away in a drawer when left unattended.

5.1.8. Where audio or video conferencing is used, it should take place in a non-public

area with staff avoiding personal information or business sensitive information being seen or heard by unauthorised individuals.

5.1.9. Staff must only store information in hardcopy form if absolutely necessary. Where appropriate, documents should be scanned, or information transferred, and stored digitally within an appropriate HSC Information System. Hardcopy versions must be disposed of in line with local record management policies and procedures.

5.1.10. Where information is stored in hardcopy form, it must be stored in line with the local Records Management Policy. Staff must label the information in accordance with the local classification policy, and store it in a way that is commensurate to the classification of the information.

Use of Locked Areas

5.1.11. Staff must securely store hardcopy information in a locked location inaccessible to unauthorised individuals when it is not in use or when it is left unattended.

5.1.12. Where lockable cabinets are not available, staff must store paper and removable media out of sight in a room which is locked when left unattended.

5.1.13. Locked areas must be secured when not in use or unattended.

5.1.14. Staff must store cabinet and cupboard keys securely, preferably in a combination safe or cabinet. Keys must not be left in locks.

Printers, Fax Machines and Photocopiers

5.1.15. Staff must only print personal information or business sensitive information if it is in line with the execution of their official duties and in accordance with local policy.

5.1.16. Staff must remove printouts, especially those containing personal information or business sensitive information, from the printer immediately.

5.1.17. Where applicable, access controls must be implemented on printers, fax machines and photocopiers to ensure staff are present during the print process.

5.2. COMPUTER ENVIRONMENT

5.2.1. All staff must protect authentication information and devices from unauthorised disclosure.

5.2.2. Staff must not leave removable media unattended.

5.2.3. Staff must lock devices when leaving them unattended, and automatic time-out screen locks must be enabled – see Information Security 1.05 Clear Desk and Screen Standard for more information.

5.2.4. Digital Information Systems must be configured to identify and authenticate users, in accordance with the Accounts and Password Policy.

6. MONITORING

Staff must be aware that any data on the organisation's systems and equipment remains the property of HSC. HSC reserves the right to monitor and record any use of organisation information and systems to ensure they are used for legitimate purposes, and that policies and standards are being complied with.

All monitoring must be undertaken in accordance with the appropriate legislation such as Regulation of Investigatory Powers Act (2000), Human Rights Act (1998), and good practice guidance such as "Employment Practices Code Part 3: Monitoring at Work" issued by Information Commissioners Office.

HSC may at any time, and without notice, conduct clear desk and screen compliance checks or audits, and may remove any information or equipment that is in breach of this policy. All users must co-operate fully with any such audit.

7. REVIEW CYCLE

This policy will be subject to annual review or following any significant incidents, changes to applicable UK or EU legislation or changes to the HSC structure or functional responsibilities.

<<Add Name>>.

<<Add Role>> Date: 25/02/2020

<<Add Name>>.

<<Add Role>> Date: 25/02/2020