Health and Social Care

Northern Ireland Fire & Rescue Service

Information Security

1.02 Removable Media

All User Standard

Approval

Document Reference	Information Security 1.02 – Removable Media - All User Standard
Version	0.3
Last updated	1st 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.

Removable Media by its very nature allows digital data to be removed from the controls of the HSC computer systems and moved internally and/or externally to HSC premises – this results in many risks to the security of HSC Data and ICT systems.

Removable Media is considered as digital storage that can be removed from a computer system and includes, but is not limited to:

- USB Storage, or Storage using a different hardware interface, (e.g. Flash Drives, USB/Thunderbolt External Hard Disks);
- Optical Media (e.g. CD's and DVD's);
- Memory Cards (e.g. SD Cards);
- Mass Storage Devices (e.g. Mobile Phone Storage, wireless storage devices);
- Tape Drives (e.g. Backup media.).

2. PURPOSE

This Information Security Standard is in place to ensure HSC and NIFRS organisations are able to use removable media in a manner that is effective for the business need, whilst reducing the risk of any losses related to the Confidentiality, Availability or Integrity of HSC or NIFRS Information Assets and Systems.

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 and 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

[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).

- 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.

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. REMOVABLE MEDIA

5.1. USE OF REMOVABLE MEDIA

5.1.1. All HSC organisations must ensure that processes and standards are in place to govern the secure use, handling and destruction of removable media.

5.1.2. All staff should be aware that:

- Only organisation approved Removable Media Devices shall be used to store, download or transport organisation and client information; and
- When Removable Media is needed to support the business, it shall be limited to the minimum amount of data and users required.
- Unknown removable media must not be connected to a HSC computer system (e.g. a USB Flash Drive found internally or externally to HSC Premises) but should, instead, be handed to the ICT Service Desk.

5.1.3. Encryption must be used when storing HSC data on removable media. See Encryption Standard for more information.

5.1.4. Portable Storage Media devices should be secured in locked storage overnight or when not in use in HSC's premises.

5.1.5. All personnel shall comply with the Information Security 1.07 Data Transfer Standard when using Removable Media to transfer HSC information to others.

5.1.6. Removable media should not be the primary or sole storage location for HSC information.

5.1.6.1. All HSC organisations must ensure that processes and standards are in place to ensure backup copies of information are made and tested regularly. The requirement to backup, i.e. the information, the frequency and the extent, will be determined according to risk, regulation and business needs.

5.1.6.2. Information governance activities (i.e. security controls, retention and handling procedures) must be considered and implemented, in addition to the Information Security Policy, throughout the data storage and backup processes.

5.2. PROTECTING HSC DEVICES

5.2.1. All staff shall ensure all necessary precautions are undertaken to protect HSC removable media, and the data stored, both internally and externally to HSC premises.

5.2.2. HSC equipment shall be used for HSC business purposes in line with local policy.

5.3. LOST OR STOLEN INFORMATION AND PORTABLE STORAGE MEDIA DEVICES

5.3.1. All staff should report all data (electronic or hardcopy) and device losses (including portable storage media devices and any other firm equipment) to your line manager and your local ICT Service Desk and if applicable a DATIX incident must be raised.

6. MONITORING

6.1.1. Staff must be aware that any data on the organisation's systems 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.

6.1.2. 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.

7. REVIEW CYCLE

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

7.1.2. All HSC organisations are responsible for ensuring their own local Security Policies, Standards, Procedures and Guidance are subject to regular review and take into account any changes to the HSC Information Security Policy and Standards.

<<Add Name>>.

<<Add Role>> Date:

<<Add Name>>.

<<Add Role>> Date: