Northern Ireland
Fire & Rescue Service

NIFRS ICT SECURITY POLICY

February 2016

Protecting Our Community

CONTENTS		Page
1	Objective	1
2	Scope	1
3	Background	1
4	Legislation	1
5	Risks & Implications	2
6	Roles & Responsibilities	2
7	Policy/Procedure in Operation	3
8	Issue & Circulation	11
9	Training	12
10	Equality	12
11	Revision & Review	12
12	Further Information & Guidance	12

VERSION CONTROL	
Version Number:	1.1
Original Issue Date:	01/02/2016
Reviewed and Revised:	06/08/2019
S75 Screening Date:	11/08/2016

Linked Policies & Guidance Documents

This NIFRS ICT Security Policy should be read in conjunction with, but not limited to, the following NIFRS documents:

- Criminal Justice Secure Mail Service User Guide
- Information Governance Strategy & Policy
- Disciplinary Policy & Procedure

The above policies/guidance documents can be accessed via NIFRS Global Drive/Document Management System.

1. OBJECTIVE

1.1 The data stored and processed within NIFRS information systems represents one of NIFRS most valuable assets. There is a need to develop and maintain an environment within which information systems and networks are secure, efficient and where staff are aware of potential threats. This policy aims to provide direction in relation to safeguarding the integrity and confidentiality of information held on NIFRS systems.

2. SCOPE

2.1 This policy applies to all NIFRS staff, contractors, temporary employees and third party associates with privileges, regardless of religious belief, political opinion, gender, race/ethnic origin, age, sexual orientation, political opinion, disability, marital status.

3. BACKGROUND

3.1 The purpose of this policy/procedure is to:

(a) Ensure a consistent and high standard of ICT security across NIFRS;

(b) Mitigate against potential threats; these can be internal, external, deliberate or accidental;

(c) To provide awareness of individual responsibilities in securing the Business, Operational and Management Information Systems.

4. LEGISLATION

4.1 The following statutory legislation is linked to this policy/procedure. This list is not exhaustive:

- Data Protection act (1988)
- Freedom of Information act (2000)

5. RISKS AND IMPLICATIONS

5.1 Any breach of this policy can result in disciplinary action which may result in dismissal. A breach is considered to be an attempt to circumvent any security control, whether successful or not.
Non-compliance could damage the reputation of NIFRS, exposing NIFRS and the individual to potential legal liabilities.

It must be noted, that use of NIFRS computing resources for illegal activity is grounds for disciplinary action. Management will co-operate with any legitimate law enforcement agency investigating alleged violations of policy or law. Any misuse or abuse of ICT Systems is also a disciplinary matter and will be dealt with in accordance with the NIFRS disciplinary procedures.

6. ROLES & RESPONSIBILITIES

NIFRS IT Department

NIFRS IT Department are responsible for:

- Undertaking research as appropriate to inform policy development and review;
- Ensuring that approved policies are forwarded to the Planning, Performance and Governance Directorate for inclusion in the Organisational Policy Database;
- Maintaining the published policy, revising as necessary;
- Present the final version of the draft policy to the relevant Director;
- Acting as the point of contact for the policy, dealing with queries that may arise.

Corporate Management Team

The Corporate Management Team (CMT) is the body responsible to the NIFRS Board commenting on and approving draft policies and proposed changes to existing policies. These are then forwarded to the appropriate Board Committee for approval and the NIFRS Board for ratification.

Board Members

Board Members are responsible for the review and approval of draft policies, including proposed changes to existing policies. In addition to this, members of the

NIFRS Board may participate in policy development, either acting as chairs or as members of policy working groups.

7. STAFF GUIDELINES FOR THE APPROPRIATE USE OF NIFRS IT RESOURCES

7.1 Reason for Guidelines

(i) As an emergency services provider, NIFRS creates, integrates, transfers and applies its information and knowledge through the use of computers, e-mail and the internet.

(ii) Use of information technology must be consistent with the NIFRS Mission, Vision, Values, ICT Strategy and Security Policies. Each employee is expected to protect the integrity of all computing resources; adhering to NIFRS rules, regulations and guidelines for their appropriate use. Policies that govern personal conduct also apply to the use of IT resources.

7.2 Passwords

Passwords must not be shared with anyone including a line manager or ICT staff.

Passwords should always be changed immediately on suspicion of any compromise. The longer a password remains unchanged, the more opportunity a potential intruder will have to discover it. Any such incidents must be reported to the IT Helpdesk.

Staff should follow the following basic security password principles:-

- YOUR PASSWORD MUST BE KEPT CONFIDENTIAL;
- Do NOT write down your password;
- Do NOT reveal a password in an email message;
- Do NOT talk about a password in front of others;
- Do NOT hint at the format of a password;
- Do NOT reveal a password on questionnaires or security forms;
- Do NOT share a password with family members;
- Do NOT reveal a password to a colleague before you go on leave.

• It should contain at least one character from each of the following four groups:-

- Uppercase letters (A, B, C …);
- Lowercase letters (a, b, c …);
- Numerals (0, 1, 2, 3 …);
- Symbols, meaning all characters not defined as letters or numerals (including ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).

When creating a password avoid the following as their use makes it easier for someone to work your password out, either by guessing it or by using a password cracking tool:-

• **Avoid using basic personal information**. This can include:
  • Names of family members, close friends, or pets;
  • Birthdays, anniversaries, dates of birth;
  • National insurance numbers, NIFRS service number, pin numbers, account numbers;
  • Current or previous addresses, phone number;
  • Car make, model and registration.

• **Avoid using any portion of your username**. Variations of the username are the first things generic password hacking software will attempt.

• **Avoid sequences**. Ensure that you do not use 'abcdefg' or '123456′. Also avoid keyboard sequences, such as 'qwerty' or 'asdf1234′.

• **Avoid keeping default passwords**. This is important because identity thieves can often find out how popular sites generate their random passwords (or at least the format). It's essential to change these as quickly as possible.

• **Avoid complete words, especially common ones** - The most basic password hacking software often checks databases of common dictionary words (even in foreign languages). Spelling words backwards does not get around this and should also be avoided.

7.3 Patching and Anti-Virus

Staff must allow security and functionality software updates to deploy when connected to the network; where this does not impact on critical business use. Otherwise this should be at the next earliest convenience.

Staff that are assigned PCs, which are not regularly connected to the network, must make special arrangements to connect their device to the network, at least once per month, to allow for security patches and anti-virus software to be updated.

7.4 **Secure Storage/Protection of Equipment**

Portable devices including laptops, smartphones, tablets, etc. must be stored in locked furniture when left unattended.

PCs left unattended at any time must be at least locked using the Windows Lock Computer facility (Windows Logo Key +L). Alternatively use Ctrl-Alt-Delete and then Enter.

7.5 **Protection of Data**

Under no circumstances should sensitive data be stored on personal equipment such as home PCs, laptops, smart phones, tablets or removable USB devices.

All NIFRS provided laptops will have encryption software, e.g. Becrypt or Microsoft BitLocker, installed and can therefore be removed from official premises.

Remember, DO NOT write down your password and keep it with your laptop/tablet, as to do so removes the protection afforded by the encryption software in the event that the equipment is lost or stolen.

7.6 **Mobile Working**

If an NIFRS provided PC is used outside of official premises it should be used only by an authorised member of staff.

Staff carrying or using a PC off the organisation’s premises must take all reasonable steps to guard against their theft, loss or damage, and against unauthorised use.

Laptops must not be left unattended in an unsecure area. When a laptop is removed from a secure location it must, whenever practical, be kept out of sight when not in use.

DO NOT write down a password and keep it along with a laptop or other mobile device. This negates NIFRS security measures and permits access to the information contained on the device.

7.7 **NIFRS use of E-mail**

E-mail is a corporate communication business tool, and e-mail communications must be used in a suitable and professional manner.

To prevent unauthorised access to your e-mail from your workstation, you must ensure that it is secured (i.e. locked) while you are away from the workstation.

The provisions of the Data Protection Act 1998 (and any related legislation), the Freedom of Information Act 2000 and the organisation's policies and procedures relating to Data Protection, Freedom of Information and Confidentiality also apply to e-mail communications and the content of those communications. This means that e-mails may be disclosed to individuals or outside agencies, as required by current Data Protection and Freedom of Information legislation or as required by any other statutory or legal duty imposed on the organisation.

Personal Use

NIFRS will permit employees to access NIFRS e-mail facilities for personal use. Access will be permitted outside working hours e.g. after work or at meal breaks and/or at the discretion of line management.

All aspects of these guidelines apply also to personal use and each employee is expected to respect this privilege afforded by NIFRS. Personal e-mails will not express opinion on behalf of NIFRS and will carry a disclaimer to this effect.

Staff must not register their NIFRS e-mail account with websites for personal use e.g. Amazon, Groupon etc. Private email accounts should be used in these cases as use

of nifrs.org mailboxes could potentially increase the amount of spam sent to NIFRS. Where a member of staff has already registered their NIFRS e-mail account they should take steps to remove this immediately.

Prohibited Use

The e-mail system must NOT be used to:

- Transmit pornographic, obscene, offensive, illegal or damaging material. Staff must not take deliberate steps to receive pornographic, obscene, offensive, illegal or damaging material;
- Transmit threatening material or material intended to frighten, harass or bully;
- Transmit defamatory material;
- Infringe copyright;
- Harass or intimidate others or to interfere with the ability of others to conduct NIFRS business;
- Attempt unauthorised access to other networks or systems;
- Introduce viruses, spyware or malware onto NIFRS equipment or network;
- Represent personal opinions as that of the organisation;
- Illegally distribute any personal identifiable or business sensitive material.

Where sensitive, confidential or protectively marked information has to be sent to an e-mail address not ending in 'nifrs.org', the Criminal Justice Secure Mail Service (CJSM) is available. Should you require a CJSM account, contact the IT Helpdesk for further information.

Spam / Phishing

Spam e-mail, also known as 'junk' or 'bulk' e-mail, is sent to millions of e-mail addresses every single day. The messages usually contain information on purchasing such things as prescription drugs, holidays and financial services.

Phishing is the process of attempting to acquire details from users such as usernames, passwords and banking details i.e. account numbers or credit card information by masquerading as a trustworthy source. This is usually done by

presenting people with e-mails that look legitimate but direct users to sites that are not.

The NIFRS network is protected by spam and phishing filters which capture the vast majority of this e-mail traffic. However they cannot guarantee 100% success. New spam and phishing assaults are developed everyday so the filters have to react to them in the same way the anti-virus vendors operate.

Therefore:-

• Particular attention must be given to e-mails, especially containing attachments or zip files, from unknown or dubious sources. Where there is doubt or suspicion, advice should be sought from the IT Helpdesk before any such e-mail is opened;

• Seeking information by deception is increasingly being used to gain access to sensitive and personal information. Staff must never respond to e-mail requests from unknown or external sources asking them to divulge personal information or sensitive corporate information;

• In order to ensure appropriate corrective action is taken, and no unnecessary panic is caused by hoaxes, staff must report any virus incidents immediately or any other apparent breach in security, to the IT Helpdesk. It is recommended that staff should not take it upon themselves to issue warnings to staff within or outside this organisation.

7.8 **NIFRS use of Internet**

Internet access is not permitted on any networked machine except via the NIFRS network; thus ensuring internet traffic is routed via NIFRS managed security controls and web filtering policies.

Direct access through modems (includes broadband services) is not permitted except with the authorisation of the IT Security Manager. This will only be granted in exceptional circumstances.

Personal use

NIFRS will permit employees to access the internet via NIFRS IT equipment for personal use. Access will be permitted outside working hours e.g. after work or at meal breaks and/or at the discretion of line management. Access will be subject to NIFRS security controls and web filtering policies.

Prohibited use

The following list is not exhaustive, but provides an indication of prohibited use:-

- Deliberately viewing any pornographic, obscene and indecent material;
- Deliberately viewing any illegal material;
- Deliberately viewing any offensive, sexist, racist, hateful or otherwise offensive/discriminatory material;
- To perpetrate any form of fraud or criminal activity;
- The violation of copyright, license agreements or other contracts (e.g. copying and using software for business purposes from a site where there is a clear limitation for personal use only);
- To send offensive or harassing material to others;
- Bring NIFRS or a colleague into disrepute;
- Any form of defamation;
- Any form of discrimination;
- Any form of harassment or bullying;
- Where it interferes with the work of the individual that is using the internet;
- Where it interferes with the work of a colleague;
- Where it interferes with the business of NIFRS;
- For illegally distributing any business confidential material;
- For hacking or gaining access to unauthorised areas;
- To deliberately waste network resources;
- For the deliberate introduction of viruses, spyware or malware;
- The use of proxy avoidance websites;
- Streaming video or audio for non-business related use;
- Any form of internet based instant messaging;
- For political lobbying;

- To undertake unauthorised trading at work, whether buying or selling, through internet auction sites such as (but not limited to) e-bay. Trading is defined as any activity, buying or selling, connected with a commercial or business interest.

Blocked Web Sites

A web filtering tool is in place to control access to certain categories of sites and file protocol types.

Only if you have a legitimate business reason to be granted access to one of the blocked sites will a review of it be carried out. This does not guarantee that the restriction will be lifted.

Staff should contact the IT Helpdesk, stating the URL (website address) that is blocked (this is displayed on the block page) and the business reason for which access is required.

7.9 **Third party access**

Where system support and maintenance is provided by a third party contractor i.e. not NIFRS IT Department, then their method of access must be authorised by the IT Security Manager.

The third party contractor must comply with NIFRS remote access procedures when providing remote support.

7.10 **Incident Reporting**

Any actual or suspected security incident, including theft or loss of NIFRS equipment, must be directly reported to the IT Security Manager or IT Helpdesk.

7.11 **Monitoring**

Staff should note that, as is permitted by legislation, the NIFRS IT Department will monitor and review internet activity and analyse usage patterns. Use will be routinely monitored from time to time, and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons. This includes the prevention or detection of illegal activities.

Users of NIFRS resources, including internet and e-mail facilities, should be aware, and must accept as a condition of use that their usage of such facilities will be monitored and may be reviewed whether use is for the conduct of official business or for personal use.

8. ISSUE & CIRCULATION

8.1 This document will be issued via Service Circular and will be uploaded onto the Policy folder within the Document Management System within the NIFRS Global drive.

9. TRAINING

9.1 Induction Training (including Substantive Promotions)

Via the Human Resources department, all new employees will be provided with a copy of NIFRS ICT Security Policy as part of the NIFRS Induction Pack.

Where the new start has a functional responsibility (AGC or SO1 and above), formal ICT Security training will be provided by a relevant member of the IT team.

Likewise if a member of staff is promoted into a role in which they now have functional responsibility, formal ICT Security training will be provided by a relevant member of the IT team.

It is the responsibility of the Recruitment Services Manager to ensure processes are in place to notify the IT Department of all new starts/promotions with functional responsibility.

As far as possible induction training will be provided in a group format and will be provided from time set aside for ICT activities. Therefore it is not anticipated that additional costs will be incurred.

9.2 Refresher Training

Refresher training workshops for staff with functional responsibilities will be run as appropriate.

Workshops will be planned in each Operational Area and also at the Training Centre and Headquarters and nominations to these workshops will be based on nominations put forward by the Corporate Management Team (CMT).

Refresher training will be provided from time set aside for ICT activities. Therefore it is not anticipated that additional costs will be incurred.

10. EQUALITY

10.1 NIFRS is committed to equality of opportunity for all employees. This Policy will be reviewed periodically in accordance with Section 75 equality obligations, best practice and with regard to NIFRS statutory obligations to make NIFRS corporate publications and information accessible in alternative formats, where reasonable.

11. REVIEW & REVISION

11.1 This policy/procedure will be reviewed as deemed appropriate, no less frequently than every 12 months.

11.2 Policy/procedure review will be undertaken by Head of IT.

12. FURTHER INFORMATION & GUIDANCE

12.1 Further information and guidance about this policy/procedure can be obtained from:

Head of IT
NIFRS
1 Seymour Street
Lisburn
BT27 4SX