Northern Ireland
Fire & Rescue Service

NIFRS ICT SECURITY POLICY

Document Version Number:	2
Reviewed and Revised:	July 2011
Prepared by:	M. Blair and A. Reilly (ICT Dept)

INDEX

1 Executive Summary

Despite the quality and range of today’s security products, high-profile security breaches and denial-of-service attacks continue to plague and concern the increasingly ICT reliant, if not dependent, business world. It is apparent that employing security technology in itself is not enough to secure the network.

There are many ICT solutions to safeguard the network from external threats such as passwords, firewalls, anti-virus software and encryption. In theory this should provide an environment sufficiently impenetrable for most business purposes, but it is only addressing part of the problem.

“Security is essentially a business decision, not a technology question,” says Joe Pato, chief technology officer at Hewlett-Packard’s (HP’s) Internet security business. “You need to take a holistic view of security otherwise you end up with a false sense of safety to the security management problem.”[1]

Internal threats are as dangerous, if not more so than external threats. The Post-it Note with the password stuck to the side of the monitor for all to see dangerously exposes the network to accidental or malicious attack. User awareness of the risks to the business, clarity of their individual responsibility and guidelines on acceptable usage will significantly reduce what many in the ICT industry regard as the weakest link and greatest threat to the network – the user base itself.

It is essential therefore to develop and implement a well-rounded security policy for the network that not only provides effective and efficient layers of defence against unauthorised access but also is published, known, fully supported and active within the organisation.

[1] Computer Business Review CBR Research Paper Security Imperatives 2001

2 Mapping the Security Policy to the ICT Strategy

Security and network management has been identified in Section 6.7 of the ICT Strategy[2] as one of the most crucial and broadest strategic issues facing management today. A security policy is regarded an essential contributor to the successful implementation of the ICT Strategy and related Business Plans with its focus on assessing the level of risk, identifying the threats to the network and approaching security as a business-risk-management decision.

The IS element of the ICT Strategy defines the information and system needs for the business while the IT element defines how these needs will be met. The security policy in turn will provide the framework by which the cost of ensuring the confidentiality, availability and integrity of the network can be balanced against the risks to the business it aims to address.

3 The ICT Security Framework

Layers of protection through prevention, detection, response and education measures are the key features of the security policy. The aim is to establish what we need to protect, why we need to protect it, how we are going to protect it in terms of:

- People
- Procedures
- Products (Hardware & Software Protection)

Bill Wylie, chairman of the UK chapter of the American Society for Industrial Security and the validation board for the UK Security Institute, says people come first in any strategy, and make you feel secure or insecure. “After that you need protection, the things you can buy to make you feel more secure. Then you formulate the procedures to link them together.”

[2] NIFRS ICT Strategy “Doing More With Less” – January 2011

4 Roles & Responsibilities

It has been clearly established that security is not simply a technology issue. Indeed it is “naïve” says Schneier, industry commentator and founder of consultants Counterpane Internet Security, to be a panacea for security issues. “If you think technology can solve your security problems, then you don’t understand the problems, and you don’t understand the technology.”[3]

It is important therefore to identify the ICT security issues facing the organisation and to define the roles and responsibilities of the key people in a position to implement the ICT security policy in response. Please refer to Table 1 below:

ICT SECURITY ISSUES FOR NIFRS
To identify external & internal threats and vulnerabilities to the Business, Operational and Management Information Systems
To decide which combination of prevention, detection and response best suits each threat and vulnerability
To prepare an action plan, prioritising the order of work, allocating funding and assigning staff resources
To obtain the support of the Chief Fire Officer to the principles and goals of the ICT Security Policy and commitment to its adherence
To provide awareness of individual responsibilities in securing the Business, Operational and Management Information Systems

Table 1

[3] MIS (UK) July/August 2001 – “Your security can’t save you” – By Grant Heinrich

5 Threats & Vulnerabilities Identified

"Everybody has vulnerabilities, and if you try to shut these down you're shutting down your business. You want to have a system where you have identified the vulnerabilities and have decided which ones you are willing to accept, and for the ones you are not willing to accept you put in place the appropriate policies, procedures and monitoring."[4]

Table 2 overleaf identifies the threats and vulnerabilities facing the Business, Operational and Management Information Systems and the combination of actions necessary to reduce the associated risks to an acceptable level for NIFRS. The assessment is based on the standards required to attain BS7799 which from October 2005 has the international number ISO 27001 and is the international best practice information security management standard, defining and guiding Information Security Management System (ISMS) development.

6 The Role of the Strategic Information Systems Planning Group (SISP)

The SISP Group was established in May 2000 at the request of the Assistant Chief Fire Officer (Technical Services) as an authoritative group to facilitate and co-ordinate the development, management and support of ICT within NIFRS. The Group is chaired by the Assistant Chief Fire Officer.

It is essential therefore that the threats and vulnerabilities facing the Business, Operational and Management Information Systems and the combination of actions necessary to reduce the associated risks as identified in Table 2 are planned, prioritised and progressed by the Group.

[4] MIS May 2001 - Securing Your Network Environment - Section 4 – Jan Babiak, Ernst & Young

Threats & Vulnerabilities Identified	Actions Required to Reduce Risk
Failure to make the business user base aware of the importance and necessity for IT security	Security Policy drawn up, approved by management and communicated to the user base
Lack of ownership of information and equipment	Maintain a Fixed Asset and Inventory syster for classification & accountability
Unauthorised access, damage and interference	Physical controls: Systems level to Desktop environment
Unauthorised access to information, networks, operating systems and applications	Logical access controls for all parties with access to the business network infrastructure
Unauthorised disclosure of information and lack of built in security for systems and applications	Fully defined systems development and maintenance procedures
Incorrect and insecure operation of information processing facilities	Fully defined communications and operations management
Failure to prepare for the effects of major disasters and the provision of Business Continuity Management	The preparation and regular testing of a Business Continuity Plan for business critical hardware platforms and software applications
Legal threats to the business	To ensure compliance with the legal requirements and obligations of any business

Table 2

7 Support for the ICT Security Policy

A successful ICT Security Policy is dependent, in no small way on the support for security from all levels of the organisation, but the support of the highest level of management is critical.

It is essential that the Chief Fire Officer as Chief Executive support the goals and principles of the policy and its review, approval and enforcement procedures.

8 Communicating the ICT Security Policy

"People will take a lot of responsibility once they understand the risk."[5] Says Jan Babiak at Ernst & Young. One of the biggest weaknesses and criticisms of IT security policies is their focus on the technical infrastructure that supports the business at the expense of creating an informed, educated and supportive user base. The user base must be aware for example, as to why they need to keep their password confidential and change it regularly.

The user base must be aware that the ICT Security Policy addresses the threats posed by the nature of the business and establishes a management framework through which high-level principles can be formulated and administered. In addition, **"User Guidelines for the Appropriate Use of Information Technology Resources",** a sub-section of the policy document itself, is enclosed overleaf and provides a concise briefing for users on how to work within the security guidelines of the ICT Security Policy.

[5] MIS May 2001 - Securing Your Network Environment - Section 3 – Jan Babiak, Ernst & Young

9 User Guidelines for the Appropriate Use of Information Technology Resources

9.1 Reason for Guidelines

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

(ii) Use of information technology must be consistent with the Mission, Vision and Values of NIFRS and its ICT Strategy and Security Policies within its role as a public sector organisation. Each employee is expected to protect the integrity of all computing resources and to know and adhere to NIFRS rules, regulations and guidelines for their appropriate use. Policies that govern personal conduct also apply to the use of IT resources.

9.2 General Guidelines of Acceptable Usage

(i) Access to NIFRS ICT resources is a privilege granted to both a uniformed and non-uniformed user base. Members of this user base carry the responsibility of using these resources for NIFRS related activities, exercising common sense and decency;

(ii) Authorisation for use of ICT facilities is provided to each individual for his or her own business use. Users must protect the confidentiality of their personal passwords and are expected to exercise care to ensure that others cannot use their accounts;

(iii) Users may not alter or intentionally damage software or data belonging to another or interfere with someone’s authorised access to ICT resources;

(iv) No-one must attempt to disrupt or damage NIFRS networks or computers in any way;

(v) Should users wish to transfer files via any media from external sources, they must have the media virus-checked by the Information Technology Department; and

(vi) Users are expected to report possible policy violations to the Information Technology Department at NIFRS Headquarters.

9.3 Implications for the Use of E-Mail under the Freedom of Information Act 2000

(i) An increasing amount of NIFRS business is now transacted by E-Mail. Under the Freedom of Information Act 2000, E-Mail communications relating to the conduct and content of NIFRS business, constitute public records. As from 1 January 2005, the public is entitled to access existing E-Mail communications to the same extent as any other public record, subject to the exceptions of disclosure described under NIFRS's Freedom of Information Publication Scheme.

9.4 Specific Guidelines for Internet and E-Mail Usage

(i) NIFRS views the Internet as a business tool, provided at significant cost. Users are expected to use the Internet access for business-related purposes, i.e., to communicate with other organisations and suppliers, to research relevant topics and obtain useful business information. Users therefore must at all times conduct themselves honestly and appropriately on the Internet and respect the copyrights, software licensing rules, property rights and privacy of others.

(ii) NIFRS has put in place systems in place to monitor and record all Internet and E-Mails for the prevention and detection of viruses and the management of network bandwidth usage. As a result, Management will actually monitor any and all files on NIFRS ICT systems, including mobile computing, to assure policy compliance;

(iii) Material of a sexually explicit or of a sectarian nature must not be displayed, archived, stored, distributed, edited or recorded using NIFRS's computing resources;

(iv) With the exclusion of the foregoing any software or files downloaded via the Internet into NIFRS's network becomes the property of NIFRS;

(v) No employee may use NIFRS facilities knowingly to attempt to create, download, distribute or import pirated or unauthorised software or data;

(vi) No employee may use NIFRS's Internet facilities to deliberately propagate any type of virus or hostile activity;

(vii) Only those members of staff who are duly authorised to speak to the media on behalf of NIFRS may speak/write in the name of NIFRS to any newsgroup or chat room;

(viii) Employees releasing protected information via a newsgroup or chat room, whether or not the release is inadvertent, will be subject to all penalties under existing data security policies and procedures;

(ix) Employees who require software to be downloaded from the Internet for direct business use must arrange first with the Information Technology Department to have such software properly licensed, registered and virus-checked. Downloaded software must be used only under the terms of its license;

(x) Employees must not upload or distribute any software licensed to NIFRS or data owned by NIFRS without explicit authorisation from the Officer responsible for the software or data;

(xi) Other systems must not be exploited to facilitate the widespread distribution of unsolicited and unwanted E-Mails;

(xii) Employees who allow others to share access to their E-Mail accounts and calendars will be responsible for the content and distribution of this information;

(xiii) Employees must not create, send or distribute E-Mails containing foul or abusive language or any other type of profanity;

(xiv) Employees must not include attachments of non-work-related or suspicious types, including but not limited to the following: .exe (executable programs), .mp3 (MP3 Audio files), .mpeg, .avi, .mpg, .ram (Video files) etc;

(xv) Personal information relating to individuals must not be obtained or disclosed without ensuring that this disclosure complies with the law and in particular, the Data Protection Act. Further information on Data Protection may be obtained from the Information Commissioner's Website:
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

9.5 Access to NIFRS Internet and E-Mail Facilities for Personal Use

(i) NIFRS will permit employees to access NIFRS Internet and E-Mail facilities for personal use. Access will only be permitted outside working hours e.g. after work or at meal breaks; and

(ii) 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.

9.6 Violation of Use

(i) It must be noted, that use of NIFRS's computing resources for illegal activity is grounds for disciplinary action. Management will co-operate with any legitimate law enforcement in 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's disciplinary procedures.

10 Conclusion

10.1 Just as it is clear that technology alone does not ensure system security, so too an ICT Security Policy does not resolve the issues of IT security, but provides the plan that ensures that NIFRS's most critical vulnerabilities receive adequate attention. Security is both a cultural and financial issue, as well as an IT issue and must be viewed and supported as such throughout the organisation.

10.2 With regard to the ICT Security Policy the ICT Department has completed the following action plan

(i) Presented this ICT Security Policy to the NIFRS Board who have approved this policy;

(ii) Obtained the support of the Chief Fire Officer and NIFRS Principal Officers for commitment to the adherence of the ICT Security Policy;

(iii) Distributed the ICT Security Policy User Guidelines to the entire NIFRS user base;

(iv) Ensured that all Internet and E-Mail users are given suitable training to ensure effective implementation of the ICT Security Policy;

(v) Made arrangements to adhere to and comply with ISO 27001 as the standard for information security;

(vi) Defined and included a corporate E-Mail disclaimer on all external E-Mails;

(vii) Continually re-assessed and addressed the threats and vulnerabilities facing the Business, Operational and Management Information Systems through the Strategic Information Systems Planning (SISP) Group; and

(viii) Reviewed the ICT Security Policy in accordance with changes to legal requirements and emerging technologies.