NORTHERN IRELAND
MUSEUMS
COUNCIL

Information Technology Security Policy

Approved: Audit & Risk Assurance Committee, 18 August 2020
Approved: NIMC Board of Directors, 29 September 2020
Review date: September 2021

Policy Title	Information Technology Security Policy
Policy Sponsor & Owner	Director
Committee	Audit & Risk Assurance Committee
Date Approved	Audit & Risk Assurance Committee – 18 August 2020 Board – 29 September 2020
Review date	September 2020
Related Policies	Data Protection Policy Raising Concerns Policy Safeguarding Policy
Related Procedures	Information Technology Security Procedures Business Continuity Plan
Related Guidance	General Data Protection Regulation 2018 Freedom of Information Act 2000 Data Protection Act 1998 Computer Misuse Act 1990 Official Secrets Act 1989 Copyright, Designs and Patents Act 1988

Revision Control	
Revision date	**Details**

1. Introduction

1.1 This policy applies to all employees whether full-time or part-time, seconded staff, temporary staff, agency staff, contractors, IT Suppliers, consultants and associates.

1.2 The objective of information security is to ensure the business continuity of NIMC and to minimise risk of damage by preventing security incidents and reducing their impact.

1.3 This policy aims to provide direction and guidance to users of NIMC information and information systems, and the security controls that are to be implemented and require user compliance.

1.4 NIMC is committed to maintaining and improving security within all aspects of NIMC business.

1.5 All staff, third parties, contractors and users must abide by the policy.

2. Purpose

2.1 The purpose of this policy is to ensure that NIMC's Information Technology (IT) system operates effectively; that it serves operational needs; that it is protected as far as possible from external threats and breaches of security; and, that it is managed in such a manner as to ensure that NIMC is compliant with prevailing legislation, guidelines and regulations, including:

- General Data Protection Regulation 2018
- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000

3. What is Information Security?

3.1 Information is an asset which has a value to the organisation and consequently it needs to be protected.

3.2 Information can include details that fall within the definition of 'personal data'.

3.3 Information security protects information from a range of threats to safeguard members, customers and staff, ensure business continuity, minimise business damage and maximise operational efficiency.

3.4 Information can exist in several forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of how information is shared or stored, it should always be appropriately protected and is subject to the provisions of this policy.

3.5 Information security ensures:

- *Confidentiality* – information is restricted to authorised users

- *Integrity* – information held is accurate and can only be altered by authorised users
- *Availability* – NIMC's systems are available as and when required by authorised users

3.6 NIMC staff and their IT Suppliers will take all necessary steps to prevent, detect and recover any loss or incident, whether accidental or malicious, including error, fraud, damage and disruption to, or loss of computing or communications facilities.

3. Supply and Service

3.1 NIMC maintains an annual contractual agreement for the supply and maintenance of computer equipment and troubleshooting. This contractual agreement sets out the terms and scope of the service provided.

4. Protection of Data

4.1 Asset Management

All hardware owned and used by NIMC is listed on the Asset Register.

Assets are assigned an owner which is also listed on the Asset Register.

The purchase and disposal of hardware will be done in line with Northern Ireland Civil Service Guidelines.

The IT Support Provider with NIMC will produce an annual verification report listing equipment, warranty arrangements, equipment end of life position and licensing and registration requirements.

4.2 Physical Security

All assets will be protected physically against misuse.

All business equipment, including the server, telephone and broadband connections, sited outside of the main NIMC Office will be sited in a secure area which is not accessible the general public and accessed by authorised personnel only.

All equipment will be protected against all forms of malware and virus by appropriate means as agreed between the Director and IT Support Service.

No computer equipment is to be removed from the NIMC offices without the approval of the Director, except for portable equipment which is the responsibility of each allocated individual user. All portable equipment when not in use must be kept securely within the NIMC offices. Security of equipment is the responsibility of NIMC and its staff.

Staff must not introduce any personal or unauthorised software onto the NIMC systems, including the server, personal computers, Ipads or laptops. The deliberate introduction of malicious software onto a system is a criminal offence under the Computer Misuse Act 1990.

Only NIMC's IT Support Provider may upload new or upgraded software, as this will ensure consistency within the system, ensure NIMC's compliance with associated legal requirements, and avoid the inadvertent introduction of any contamination or virus.

Staff must not to enter or adjust any of the programme files on the system but report any suspected software malfunctions to the Business Executive Officer.

4.3 Communications and Operations Management

Daily back-ups of the information are taken with a copy kept in secure off-site storage.

All equipment and the network will be protected against all forms of malware and virus software as appropriate.

Maintenance of the system and information security by the IT Support Provider.

The IT Support Provider will provide a six-monthly security/audit report/Penetration Test on all firewall technology and list any recommendations.

The designated System Administrators are the Director and the IT Support Provider.

4.4 Network Security and Access Control

For all types of access, the principle of least privilege will be applied.

Password Management controls will be in place to ensure that passwords are of a suitable complexity and require changing at 60-day intervals. Sharing of passwords is strictly prohibited. Network controls will be implemented and maintained to ensure the security of NIMC and protect against unauthorised access.

No external or personal computer device should be attached to NIMC's network. Staff are not permitted to access the web using any protocol that may allow internet users access to NIMC's network and information.

Facilities are in place to allow the transfer of information into and out of the NIMC environment by memory stick and other removable media including CDRom, flash drive and memory card. Automatic anti-virus procedures are in place around such transfers.

NIMC information can only be saved onto encrypted devices.

Remote access to NIMC's network will be securely controlled.

4.5 Internet Security

All emails will be filtered to remove undesirable content such as viruses and inappropriate material and content.

4.6 Cyber Security Reviews & Departmental Security Health Checks

NIMC will conduct, where possible, an independent Cyber Security Review every **three** years.
NIMC will participate in the annual Departmental Security Health Checks which should be validated, where possible, by the Audit & Risk Assurance Committee.

5. NIMC Staff – Acceptable Use

5.1 E-mail

Users where appropriate will be provided with individual email accounts to use for communication with other NIMC staff, NIMC members and other interested parties who have provided consent. E-mail to and from external parties is permitted for any user in carrying out their NIMC duties.

5.2 Web browsing

Users are permitted to browse the internet to research relevant and potentially relevant information sources in carrying out their NIMC duties.

Users must use the service in an acceptable manner to reduce the risks of accessing inappropriate material.

5.3 Newsgroups, bulletin board and social media

Users are permitted to be part of Newsgroups, use bulletin boards and social media that are associated with NIMC business.

Details of what defines **Acceptable Use** is outlined in the Information Technology Security procedures.

Unacceptable use of NIMC's Information Technology services including email, internet and social media may lead to disciplinary proceedings. Guidance on Unacceptable Use is outlined in the Information Technology Security procedures.

5.4 Personal Use

Personal use is defined as any use of internet or email facilities that does not stem from a requirement directly relating to the staff member's official duties.

Any access or use which is unrelated to official duties, for example, personal banking, online purchasing, accessing general news and shopping sites, travel information, sending or receiving personal emails, would be classified as personal use.

NIMC permit staff to use official facilities for personal use, **in their own time**, providing that such use does not compromise the security of NIMC information and data. Result in increased costs or delays or have any negative impact on the NIMC network or on the effective discharge of official business.

Own time is when an individual is not on duty, such as before signing in or after signing out, or during lunch or other officially sanctioned breaks.

Users are reminded that all internet and email use is subject to monitoring. Such monitoring does not differentiate between official and personal use.

Use of NIMC facilities for personal use will be deemed as acceptance that usage, and on occasions, content, will be monitored.
Users must not make excessive use of NIMC internet and email facilities to the detriment of their official duties.

6. Information Security Management

Security Incident Management reporting procedures are to be documented and communicated to all staff and third parties.

Loss of equipment, including the circumstances, must be immediately reported to the local police and NIMC Director. Loss and misuse of NIMC equipment may lead to disciplinary action.

All Security Incidents must be reported by employees to the Director in line with the Security Incident Reporting Process.

Any Security Incident concerning an individual not adhering to the practices outlined in this policy and associated procedures, the matter can be raised confidentially with the Director, or through the Public Interest Disclosure procedures operated by NIMC.

7. Business Continuity Management

Information technology is essential to the delivery of NIMC's business. Consequently, it is a key component of NIMC's Business Continuity Plan.

The interface between the Business Continuity Plans for NIMC and NMNI is critical. Communication between the two organisations is essential to ensure the seamless delivery of plans and procedures.

8. Accountability and Responsibility

The NIMC Director owns this policy and is responsible for information security within NIMC and is the initial point of contact for all queries regarding information security and the content of this policy.

The Business Executive Officer is responsible for co-ordinating NIMC's computer systems.

All users of and providers of services to NIMC are responsible for ensuring that they are aware of and comply with this policy at all time.

All users are required to agree to a Compliance Statement when accessing the NIMC network.

All NIMC employees whether full time or part time, seconded staff, temporary staff and agency staff, contractors, consultants and associates are required to be aware of policy details and to comply with these at all times.

Access to the Museums systems may be withdrawn and the Museums disciplinary procedures will be invoked where a serious or deliberate breach of the policy is made.

9. Monitoring and Review

9.1 The Director is responsible for monitoring and reviewing this policy.

9.2 The Director reports on Information Security at NIMC's Accountability Meeting with the Department for Communities.

10. Authority

10.1 Policy Sponsor, Owner and Contact

The Director, as Accounting Officer for the NIMC, is responsible for the policy development, its effective operation and associated procedures.