Information Risk Policy

1 Introduction

1.1 The Cabinet Office's June 2008 'Data Handling Procedures in Government' report set out measures to strengthen information assurance within the public sector. Those measures included the identification of the information assets held by an organisation, the allocation of those assets to a responsible owner, and an annual assessment process to inform the Governance Statement. This policy has been developed to implement these measures in order to safeguard the information held by NILGOSC.

1.2 Information is a key asset and its proper use is fundamental to the delivery of NILGOSC's services. Members, pensioners and all other stakeholders are entitled to expect NILGOSC to protect their privacy by using and handling information professionally and sensitively to ensure that private information is protected.

1.3 NILGOSC will aim to do this by effectively managing all risks to the integrity, availability and confidentiality of all information it holds, both on paper and electronically. It will ensure controls are in place, in line with those set out for 'Official' documents as per the Cabinet Office policy 'Government Security Classifications – April 2014[1]'.

1.4 The purpose of this policy is to define how NILGOSC will manage information risk and safeguard its information assets.

2 Scope

2.1 Everyone in NILGOSC has a role to play in the effective management of information. This policy applies to all sections within NILGOSC and all Committee Members and staff. 'Staff' refers to all staff, regardless of occupation, including, but not restricted to, permanent, temporary, voluntary, students and agency workers.

2.2 The policy also applies to any contractors, suppliers, advisers or other third parties that collect, transmit, retain or use information on behalf of NILGOSC in any form.

2.3 This policy should be read in conjunction with the following NILGOSC policies, procedures and other documents:

- Information Security Policy
- Information Asset Register
- Risk Management Policy
- Risk Evaluation Guidance
- Risk Register
- Document Management Policy
- Code of Conduct for Committee Members
- Data Protection Policy and Procedures
- Freedom of Information Policy and Procedures
- Anti-Bribery Policy

[1] This replaces the Government Protective Marking Scheme.

- Anti-Fraud Policy
- Software Policy
- Information Strategy
- Secure Desk Guidance
- NILGOSC Retention and Disposal Schedule
- Internal Control Framework

2.4 In line with Cabinet Office guidance, NILGOSC has also developed an Information Charter, which sets out the standards that the public can expect when NILGOSC requests or holds personal information; how people can access their personal data and what is required to keep information up to date. A copy of the Information Charter is attached at Appendix A.

2.5 These policies and documents have been prepared in line with the following legislation:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

3 What is Information Risk and Assurance?

3.1 Information risks are vulnerabilities and threats to the information resources used by an organisation to achieve its business objectives. Risks may include inappropriate disclosure or non-disclosure of information, loss, theft or fraud, information being wrongly destroyed, staff acting in error and a failure to use information for the public good.

3.2 Information Assurance is defined in HMG IA Standard No. 2 Risk Management and Accreditation of Information Systems (v 3.1 October 2008) as, *'the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under control of legitimate users.'* Determination of the measures to protect a system and the information it holds must take into account the confidentiality, integrity and availability (CIA) of the information, as defined below:

- Confidentiality: ensuring that information is only available to those who are authorised to access it;

- Integrity: safeguarding the accuracy and completeness of information and the methods that are used to process it;

- Availability: ensuring that users have access to the data and/or systems as and when required.

3.3 NILGOSC has taken these three aspects into consideration to establish and maintain a secure environment for the protection of information. The measures to protect information include a combination of physical, technical, personnel and procedural controls, as set out below:

- Clearly defined roles and accountability
- Appropriate vetting of staff and contractors
- Controls based on cost effective assessment of risk
- Awareness training for staff
- Development and review of relevant policies and procedures
- Mechanisms for monitoring and reporting security incidents
- Business continuity planning
- HR policies reinforce the importance of data management by reminding staff that the misuse or poor control of personal data could constitute gross misconduct.

4 Information Asset Register

4.1 In line with Cabinet Office guidance, NILGOSC has developed an information asset register (IAR). This is a register of information or collections of information, held electronically or in hard copy, which have (usually) not been published or made publicly available.

4.2 An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Each asset has an Information Asset Owner who is responsible for safeguarding it and using it appropriately. Further details on the Information Asset Owner role are provided in 6.7 below, and in Appendix B.

4.3 The creation of an IAR was a government initiative designed to facilitate greater openness to information held by public bodies. The IAR does not provide direct access to the information holdings themselves. It is a means of alerting the public to the existence of the unpublished information and whom to contact.

4.4 To sustain its usefulness, the IAR will be formally reviewed in line with this policy, but updated as regularly as required as new information assets are identified.

4.5 NILGOSC has also prepared a Freedom of Information Publication Scheme, which aims to reduce the number of information requests by proactively publishing the information most likely to be requested. The Publication Scheme does not include all of NILGOSC’s information resources, either due to the sensitivity of the information, or the fact that it is not considered of interest to the public. As the IAR lists all information resources, including unpublished information, it will complement the Publication Scheme in terms of managing the demand for information.

5 Information Risk Management

5.1 Information risk management is the process of identifying vulnerabilities and threats to the information assets used by an organisation to achieve its business objectives, and deciding what controls, if any, to put into place based on the value of the information asset.

5.2 The identification and assessment of risks relating to NILGOSC's information assets will be carried out in line with the Risk Management Policy and the Risk Register.

5.3 All risk owners are required to complete a quarterly Statement of Assurance (SoA) to confirm that the controls outlined in the Risk Register have been reviewed. The SoA comments on how effectively those controls are operating, and notes any new risk areas or control weaknesses identified during the quarter. Results from this process are reviewed by the Senior Management Team and by the Audit & Risk Assurance Committee.

5.4 NILGOSC is responsible for maintaining a sound system of internal control and risk management. The Accounting Officer will report in the annual Governance Statement on whether information risks are being managed effectively and on any significant incidents relating to the security of information during the reporting period.

5.5 NILGOSC recognises that the aim of information risk management is not to eliminate risk totally, but rather to provide an effective infrastructure to identify, prioritise and manage the risks involved. It requires a balance between the cost of managing and treating risks, and the anticipated benefits to the business.

6 Responsibilities

6.1 All NILGOSC Committee Members and staff have a duty to manage information effectively, and to identify and help to address potential risks in their area. However, the staff listed in paragraphs 6.3 to 6.7 have specific information assurance responsibilities.

6.2 The Cabinet Office's June 2008 'Data Handling Procedures in Government' report established mandatory minimum measures to protect information. These measures have been included in the information assurance roles within NILGOSC as set out below. The specific responsibilities for each role are provided in Appendix B.

6.3 *Accounting Officer*

6.3.1 This role is undertaken by the Secretary in NILGOSC.

6.4 *Senior Information Risk Owner (SIRO)*

6.4.1 This role is undertaken by the Deputy Secretary in NILGOSC.

6.5 *Information Risk Manager*

6.5.1 This role is undertaken by the Information & Compliance Manager.

6.6 *Information Security Officer*

6.6.1 This role is undertaken by the IT Systems Manager.

6.7 ***Information Asset Owners (IAOs)***

6.7.1 This role is undertaken by Senior Managers in respect of the information assets and systems under their control.

6.8 ***Internal Audit***

6.8.1 Internal Audit also has a role to play in providing assurance on the effectiveness of the management of information risks within NILGOSC and should carry out regular reviews of the systems in place to provide information assurance. Those systems include the various roles and specific responsibilities, the effectiveness of the policies and procedures and compliance with best practice.

7. Incident Management

7.1 An information security incident is any real or suspected event that has, or could have, resulted in information loss, unauthorised disclosure or damage to NILGOSC information assets or which breaches the Information Security and/or other relevant policies. This can include anything from a forgotten password to the successful access of confidential corporate data by a hacker.

7.2 Computer security incidents must be reported to the IT Systems Manager and personal data security breaches must be reported to the Information & Compliance Manager. The relevant manager will make an assessment of the incident and determine an appropriate response. If the incident has potential significant implications for NILGOSC, the SIRO should be informed at an early stage.

7.3 The following organisations should also be informed if the incident is significant:

- GovCertUK – this is the Computer Emergency Response Team (CERT) for UK Government. It assists public sector organisations in the response to computer security incidents and provides advice to reduce the threat exposure. The IT Systems Manager is responsible for reporting computer security incidents in line with *GovCertUK Incident Response Guidelines* as follows:

    - All incidents of electronic attack, actual or suspected, should be reported initially by telephone on 01242 709311 and followed by an e-mail to incidents@govcertuk.gov.uk (attaching the completed incident report template, available on the GovCertUK website). This includes malware incidents that have significant effects, disruption of service and other events that may reflect electronic attacks, whether attempted or successful.

    - Due to the inherent sensitivity of cryptographic items, incidents involving cryptographic equipment and/or the associated key material (e.g. encrypted laptops, secure telephones) should be reported to CINRAS (Comsec Incident Notification Reporting and Alerting Scheme) at cinras@cesg.gsi.gov.uk.

- Information Commissioner's Office (ICO) – this is the UK's independent authority founded to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. All significant personal data breaches should be reported by the Information & Compliance Manager to the ICO in line with the *ICO Guidance on Data Security Breach Management* and recorded on NILGOSC's Personal Data Breach Log.

7.4 Security breaches will be managed as 'incidents' with appropriate action taken in terms of escalation, reporting, recovery and subsequent review of existing controls, policy and procedures.

8. Monitoring and Review

8.1 The Information & Compliance Manager has overall responsibility for monitoring the effectiveness of, and compliance with, this policy.

8.2 This policy will be reviewed at least every three years, and may also be revised in response to changing circumstances, technology, operational or legislative requirements.

Published:	May 2010
Reviewed:	August 2012, June 2015
Next review due:	June 2018

Information Charter

NILGOSC needs to handle personal information about you in order to provide better services for you. This Information Charter sets out the standards you can expect from NILGOSC when it requests or holds personal information; how you can access your personal information and what NILGOSC requires in order to keep your information up to date.

When NILGOSC asks you for personal information, it undertakes:

- to make sure that you know why we need it;
- to ask only for what we need - not to collect too much information, or any irrelevant information;
- to protect the information and to make sure that only authorised people can access it;
- to let you know if we share the information with other organisations to give you better public services, and if you can say no to this;
- to make sure that we do not keep information for any longer than necessary;
- not to make your personal information available for commercial use without your permission.

In dealing with your personal information, NILGOSC will also:

- value the personal information entrusted to it and ensure that trust is respected;
- abide by the law relating to the handling of personal information;
- consider the privacy risks when planning to use or hold information in new ways, such as introducing new systems;
- provide training to staff who handle personal information and respond appropriately if personal information is not used or protected properly.

In return, NILGOSC asks you:

- to give us accurate information; and
- to tell us as soon as possible about any changes, such as a new address.

This will help to keep your information reliable and up to date, and will make it easier for NILGOSC to contact you if necessary.

Please contact NILGOSC if you would like further information about any of the following:

- how to find out what information is held about you, and how to ask NILGOSC to correct any mistakes;
- the information sharing agreements NILGOSC has with other organisations;
- the circumstances under which NILGOSC can pass on your personal information without telling you, for example, to prevent and detect crime, or to produce anonymised statistics;
- NILGOSC's instructions to staff on how to collect, use and delete your personal information;
- how NILGOSC checks whether the information we hold is accurate and up to date; and
- how to make a complaint.

Contact Details

For further information on any of the above, or to request a hard copy of this Information Charter, please contact the Information & Compliance Manager using the details provided below:

Address: NILGOSC
Templeton House 411
Holywood Road Belfast
BT4 2LP

Phone: 0345 3197 320
Fax: 0345 3197 321
E-mail: info@nilgosc.org.uk

Independent advice

For independent advice about data protection, privacy and data-sharing issues, you can contact the Head Office of the Information Commissioner at:

Address: Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Phone: 0303 123 1113 (local rate) or 01625 545 745 (national rate)
Fax: 01625 524510
Website: www.ico.org.uk

Alternatively, you can contact the Northern Ireland Information Commissioner's Office at:

Address: 3rd Floor
14 Cromac Place
Gasworks
Ormeau Road
Belfast
BT7 2JB

Phone: 028 9027 8757 or 0303 123 1114
E-mail: ni@ico.org.uk

Key responsibilities of Information Assurance Roles

1. Accounting Officer (Secretary)

a) To have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

b) To sign the annual Governance Statement, which explicitly covers information risk, and includes:
- the number of information risk incidents reported to the Information Commissioner;
- the numbers of people potentially affected;
- actions taken to contain the breach and prevent recurrence.

c) To share and discuss the information risk assessment with the Audit & Risk Assurance Committee and the Management Committee.

2. Senior Information Risk Owner (Deputy Secretary)

a) To own the Information Risk Assessment and the Information Risk Policy.

b) To act as an advocate for information risk at Committee meetings and in internal discussions.

c) To provide written advice to the Accounting Officer on the content of the annual Governance Statement with regard to information risk.

d) To understand risks to the IT system, have an awareness of the overall risks and how the risks may affect strategic goals.

e) To approve any changes relevant to information risk in the security clauses for procurement contracts.

f) To ensure that information risk awareness training is provided to all data users on appointment and at least annually thereafter.

g) To ensure that appropriate information risk management training is provided to all Committee Members and managers on appointment and refresher training provided on a regular basis.

3. Information Risk Manager (Information & Compliance Manager)

a) To produce, maintain and monitor compliance with NILGOSC's information management policies.

b) To produce and maintain the Information Asset Register.

c) To conduct privacy impact assessments as required.

d) To conduct at least an annual review of information risk and the effectiveness of the information risk policy. The risk assessment must examine potential changes in services, technology and threats.

e) To assess compliance with the arrangements for handling personal information on paper and on IT systems, including testing whether access rights have been removed if necessary, and whether paper and electronic information has been disposed of appropriately.

f) To advise the Senior Information Risk Owner on Information Risk Assessment and Information Risk Policy, and to assist in the provision of risk awareness training.

4. Information Security Officer (IT Systems Manager)

a) To have day to day responsibility for all aspects of information security, including the implementation and dissemination of the information security policy, and the provision of staff training on information security.
b) To manage the process of information security incident reporting and resolution.
c) To ensure that IT systems handling official information are protected using either: FIPS certified encryption; foundation grade encryption; or appropriately assured[2], commercially available security products and service offerings.
d) To undertake a review of IT systems when systems undergo significant change or at least every 3 years.
e) To ensure that any IT contracts for services, or any IT clauses in other contracts, clearly specify the security requirements.
f) To put into place arrangements to log data users' activity in respect of electronically held personal information, and to share summary records of this activity with the relevant senior manager.
g) To avoid the use of removable media, including laptops, USB memory sticks and PDAs etc, where possible.
h) Where it is not possible to avoid the use of removable media, to take action to manage the risk to the information, by minimising access to the data, by minimising user rights to copy files onto and from removable media, and via encryption of data.

5. Information Asset Owners (Senior Managers)

a) To know what information is held in their area, and in what form, what is added and removed, how information is moved, who has access, and for what purpose.
b) To understand and identify risks to the information assets and systems in their area, and assess and respond to those risks as appropriate.
c) To identify and keep a record of staff and contractors with access to, or involved in handling, individual records containing personal data.
d) On a quarterly basis, to assess risks to the confidentiality, integrity and availability of information in their area. At least once a year, the risk assessment must examine potential changes in services, technology and threats.
e) To provide information on an annual basis to support completion of the Governance Statement in respect of the security and use of the information assets under their control.
f) To determine what information they or their delivery partners hold which falls into the personal information category.
g) To ensure that all personal information is handled, processed and stored as if it were marked OFFICIAL.'
h) To ensure that personal data is disposed of in a controlled manner, e.g. via shredding or confidential waste.

[2] Assurance will normally be delivered through industry led (but independent) assessments under the CESG Commercial Product Assurance (CPA) Scheme (Foundation Grade).

i) To define and document users' access rights to personal data in their area. Access rights should be set at the minimum level possible in terms of the pool of records accessible, the number of records viewed, the nature of information available, and the level of functionality required.

j) To check users' activity in respect of electronically held personal information to ensure that this is being done appropriately, with particular focus on staff who work remotely, or who have higher levels of functionality.

k) To approve and minimise transfers of information whilst achieving the business purpose.

l) To approve disposal mechanisms.

m) To approve arrangements for transfer of data, e.g. on removable media.