Information Security Handbook

August 2016

Contents

Foreword

Effective information security is a key priority for Invest Northern Ireland. It is vital for public confidence and for the efficient and effective conduct of our business.

Invest NI holds a wide range of sensitive material, both of a commercial and personal nature, entrusted to us by our customers and stakeholders. This information must be managed appropriately and securely.

Information security must be seen as an integral aspect of Invest NI's customer led service culture, delivering a 'best in class' customer experience. Unauthorised access to information could lead to serious financial or reputational harm to our customers and stakeholders. Such an incident could also lead to serious reputational damage to Invest NI.

This handbook brings together into a single source the various policies, procedures and structures that have been put in place to ensure the protection of information used by Invest NI. For a secure and effective information environment to be maintained, it is essential that all staff should be familiar with and fully apply the policies and guidance set out within this handbook.

This handbook and its associated policies are fully endorsed by me and the Executive Leadership and Senior Management Teams. It is important to highlight that information security is everyone's responsibility and all staff are required to take responsibility for the protection of personal and business information that they manage or access in their daily roles.

Alastair Hamilton

Chief Executive

1 Key Facts: Information Security

What Is It?

- Protecting organisational information against loss and unauthorised or unlawful destruction, alteration, disclosure or access

Why Do We Do It?

- Protecting information entrusted to us by customers, stakeholders & others
- Personal professional integrity
- Protecting organisational reputation
- Legal requirement
- Negative consequences
    - regulatory fines
    - disciplinary action
    - legal action

Who Does It?

- Everyone
- All staff at all levels have personal responsibility to protect organisational information

How Do We Do It?

- Treat information with care, be attentive to how you handle information
- Follow policies & guidance set out in this handbook
- Undertake mandatory Data Protection and security training
- Implementing ISO27001 accreditation requirements

2 Introduction

1. Invest NI recognises that stringent principles of information security must be applied to all information it holds. This includes business and commercially sensitive information and personal data on customers, employees, suppliers, contractors and members of the public.

2. While the gathering and analysis of information is essential to the delivery of Invest NI corporate objectives, it is clear that this must be done in a way that preserves the *confidentiality*, *integrity* and *availability* of the information. To this end Invest NI has in place a range of information governance policies and accountability structures to deliver and maintain an effective information security management system.

3. The Invest NI Information Security Management System (ISMS) is accredited to the information security standard ISO27001. This is an internationally recognised best practice framework for an ISMS which helps Invest NI to identify the risks to our information and put in place the appropriate controls to help reduce the risk.

4. Staff commitment is paramount to successful information security. Invest NI is committed to empowering its staff to make the right decisions in respect of how they handle organisational information. This handbook is a tool to facilitate staff in making the right information security related decisions.

3 Policy Statement

1. Invest NI regards the lawful and correct handling of personal and business sensitive information as essential to its successful operation and to maintaining confidence of those with whom it transacts business.

2. Invest NI is committed to ensuring that all information entrusted to it is managed lawfully and appropriately. Legislation including The Data Protection Act 1998, The Official Secrets Act, The Freedom of Information Act 2000, The Computer Misuse Act 1990, The Human Rights Act 1998 and the common law duty of confidentiality set the legal framework within which Invest NI must ensure the secure processing of information.

3. Invest NI seeks to foster a culture that values, protects and uses information to deliver its corporate objectives through a range of methods and arrangements that embed compliance with information governance into the organisational ethos.

4. Invest NI continues to maintain an Information Security Management System independently certified to the ISO 27001 standard.

5. Information security matters are reviewed by an Information Governance Group headed by the Executive Director of Finance & Operations in the role of Senior Information Risk Owner (SIRO). This group is chaired by the Head of Internal Operations in the role of Departmental Security Officer (DSO).

4 Accountability and Governance

1. Effective accountability and governance arrangements are essential to ensure the proper management and control of information. The Invest NI Information Governance framework is detailed below. This explains the various oversight roles and responsibilities that Invest NI has in place to deliver an effective governance regime to manage Information Security.

Staff Responsibilities

2. The role played by individual staff members is vital in ensuring information is held and managed securely. To that end all staff are responsible for the protection of personal/ business sensitive information that they manage or access as part of their day to day activities.

   Staff must ensure that all personal or business sensitive information in their possession is kept secure against loss and unauthorised or unlawful disclosure at all times. In particular it is the responsibility of staff, regardless of grade, to ensure that they personally read and follow the information security related policies and guidance as detailed at Section 7 of this handbook.

   Staff must also undertake organisational mandatory information security related training (such as the annual Data Protection training) when requested to do so within the required timeframe.

Line Management Responsibilities

3. Line managers have a responsibility to ensure that their teams are aware of and adhere to information security policies and guidance.

Senior Management Responsibilities

4. Executive Directors, Divisional Directors and Head of Divisions, are the Information Asset Owners (IAOs) for all information managed or accessed within their Divisional teams. They are responsible for the secure

management of information within their business areas. This role requires them to raise the profile of information governance policies and related training. They are the primary liaison contact point for the SIRO and the Information Governance Group on information security matters, including performance reporting; incident reporting; audit and accountability matters. Every quarter the IAOs provide written confirmation to the CEO that appropriate divisional arrangements are in place to ensure compliance with data management and data security policies.

Organisational Governance

5. The Senior Information Risk Owner (SIRO) for Invest NI is the Executive Director for Finance and Internal Operations. The SIRO is responsible for managing information risk within Invest NI and leads the organisational response. The SIRO is the focus for the management of information risk at Board level. The SIRO provides an annual assessment of information risk performance to the Accounting Officer for inclusion in the annual report. This assessment draws on material from the IAOs and the Information Governance Group.

6. The SIRO heads the Information Governance Group (IGG), whose role it is to create, implement and monitor an Information Governance Framework for Invest NI. The IGG provides clear direction, support and consideration to the management of information security initiatives and information risk management and is responsible for the maintenance of the ISO27001 Accreditation.

7. The Information Governance Group is chaired by the Head of Internal Operations (the DSO). Its members also include the SIRO, the Executive Director of Human Resources, the Head of Information Management and Governance, the Information Governance Manager, the ICT Manager, the ICT Infrastructure Manager, the Risk Manager and the Contracts and Facilities Manager.

8. The IT Security Officer (ITSO) manages the information security of Invest NI ICT systems.

5 Controls and Monitoring

1. Effective controls, monitoring and reporting procedures are necessary to ensure that efficient information security standards are in place and are being maintained. A range of measures provide assurance that information security and associated business risks are effectively managed. These apply both internally, on how Invest NI manages its own information, and externally, on how others manage the information we share with them.

Delivery Partners (including EDOs), Consultants, Contractors, Suppliers and Stakeholders

2. Invest NI will from time to time enter into arrangements with a range of other organisations to support it in delivering its services. Such organisations will often be contracted to provide services or undertake work which will require them to access, handle, store or dispose of information.

3. It is essential that, in entering into contractual arrangements with such organisations, Divisions ensure that appropriate information governance (security & ownership) standards are maintained and protected.

4. Therefore, it is the responsibility of each Division to ensure that when entering into a contract with an outside organisation:

    - information security is accurately reflected in the contract (for example CPD standard contract provisions); and

    - periodic assurance is provided in respect of its compliance with information security contractual requirements (see 'Contract Management – Information Security Compliance template' available on the intranet).

5. This will also apply to Delivery Partners classified as External Delivery Organisations (EDOs). Please see the specific EDO engagement process guidance available on the intranet.

6. The contract in place will be dependent upon how the services were procured (see Procurement intranet webpage). Where no services are procured and information is being shared, such as in a one off situation, then the 'Third Party Data Processing Agreement' (available on the intranet) must be signed. This agreement should be signed on behalf of Invest NI by a Director/ Divisional Head. A copy of the signed form should be sent to privacy.officer@investni.com .

Risk Management

7. A sound system of internal control relies on thorough and regular evaluation of the nature and extent of risks that the organisation is exposed to. The Invest NI Risk Management Strategy and Risk Management policy detail the approach the organisation takes to managing risk.

8. It is the policy of Invest NI to comply with all regulatory or legislative requirements placed upon the organisation. Therefore the minimum level of risk tolerated in respect of protecting personal and business sensitive information will be full compliance.

Internal Monitoring

9. Invest NI has a variety of controls in place to monitor compliance with Information Security policy and practices. Regular periodic compliance checks with the 'Clear Desk Policy' are conducted on behalf of the Information Governance Group. Information Security Incidents and associated risk assessments are also reported to the Information Governance Group at each meeting.

10. All Invest NI resources, including corporate email, are provided for business purposes. Our systems enable us to monitor e-mail, internet and other communications. For business reasons, and in order to fulfil our legal obligations in our role as an employer, use of our systems is continually recorded. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes. Any information stored on an Invest NI owned PC, server, hard drive, USB device, mobile device etc. may be subject to scrutiny by Invest NI. This

monitoring can help establish the extent to which staff comply with information security related policies (such as the 'ICT Systems Acceptable Usage Policy' and the 'Policy on Sending Information outside Invest NI').

11. Invest NI's Information Security Management System is also monitored by DfE Internal Audit Service on an annual basis. This auditing supports external audits of Invest NI's accreditation to ISO 27001 certification for information security management.

6 Training and Communications

1. Invest NI recognises that effective training and good communications are essential if a secure data environment is to be maintained. Therefore, a range of approaches are used to ensure that all staff have the necessary knowledge, awareness and skills to ensure that Invest NI delivers a safe environment for the management of the information it holds.

Induction

2. It is important that all new staff joining Invest NI be made aware of the organisation's information security standards and policies. To this end the staff induction process contains a section on information security which emphasises the importance attached to information management in the public sector in general and Invest NI in particular. All new staff are required to complete Data Protection, Information Security and FOI e-learning training. However, the effective induction of new staff also relies heavily on the training processes within teams. Therefore, it is incumbent on all line managers to ensure new staff are familiar with the relevant policies and all specific guidance and procedures (which are available on the intranet).

Data Protection Training

3. Invest NI will ensure that all new and existing staff are fully trained in data protection requirements. To this end, Data Protection training is mandatory and all staff must complete on an annual basis within the specified timescale

to comply with the organisational Data Protection Policy.

4. Some business areas in Invest NI have greater access to sensitive information and as such the basic induction training may not be sufficient. Where this is the case, line management should request advice and guidance from the Learning & Development Team on development of tailored training for key staff.

Records Management training

5. Effective management of records can ensure information is handled correctly. Generic training will be available on Records Management but in the meantime staff are referred to the Records Management Policy and Guidance documents as well as to their Information Co-Ordinators who will provide hands-on training. The Information Management and Governance team will provide advice and guidance on specific issues.

Other Information Governance training

6. Mandatory Information Security training will also be rolled out across the organisation at suitable intervals. Every other year, staff will also be required to complete training on the Freedom of Information (FOI) legislation.

Communicating the Information Security message

7. Invest NI is committed to maintaining an appropriate profile on information security matters and will use internal communications activities to ensure the message is delivered to all staff. The intranet is also used to disseminate organisational information management, data protection and information security policies and guidance to staff.

7 Internal Policies and Guidance

The following is a list of all the current information security related policies in force within Invest NI. If a secure and effective information environment is to be maintained within Invest NI it is essential that all staff should be familiar with and fully apply the policies and advice set out in these documents.

These documents can be found on the Invest NI intranet via a document search.

1. **ICT Systems Acceptable Usage Policy**

   The objective of this policy is to make users aware of their responsibilities towards the security of all electronic and communications systems.

2. **Data Protection Policy**

   The Data Protection Act 1998 provides a framework to ensure that personal information is processed lawfully. All aspects of how Invest NI handles personal information are governed by the requirements of the Act.

3. **Clear Desk Policy**

   The Clear Desk Policy sets guidelines which reduce the risk of a security breach, information theft and fraud caused by documents/equipment being left unattended in Invest NI premises.

4. **Policy on Sending Information outside Invest NI**

   This policy sets guidelines to ensure the security and confidentiality of information whilst it is being sent to appropriate parties outside Invest NI.

5. **Visitor Care Policy and Procedures**

   This policy details the correct procedure that must be followed to ensure visitors present no information security risk to Invest NI held information.

6. **Records Management Policy**

   This policy sets out the principles that apply to the management of records, both physical (paper) and electronic, across the organisation.

7. **Information Security Incident Management Policy**

This policy aims to ensure that information security incidents are identified and reported to minimise any potential risk and impact that may occur.

8. **Third Party Data Processing Agreement**

Non contracted 'third parties' who require access to Invest NI personal and business sensitive information for processing purposes must complete the this Agreement. This form is designed to ensure we are providing adequate protection for data subjects when data is being shared.

9. **Risk Management Policy**

This document outlines the processes that should be used in the management of risk and the structures through which risk should be communicated and reported upon.

10. **Privacy Impact Assessment guidance and procedure manual**

Internal Projects that involve collecting and/or using personal information give rise to data protection concerns. A Privacy Impact Assessment (PIA) is used to assess risks and identify mitigating measures.

11. **Guidance on Protective Marking**

Protective marking is the method by which the originator of a document indicates the levels of protection required.

12. **Guidance on Document Control**

Document version control contributes to the integrity of a document by ensuring its currency is clearly marked and confirms to readers which version they are reading /reviewing.

13. **Contract Management – Information Security Compliance Template**

Template to be used to record periodic assurance from service providers/ contractors in respect of compliance with information security requirements.

Version Control

Author: Danny Smyth
Issue Date: August 2016
Issue Number: 6.0
Approver: Information Governance Group
Status: Approved
Next Review Date: Aug 2018

Version	Author / Reviewer	Review Date	Approved by
1.0	DETI / Danny Smyth	14 March 2011	IGG
2.0	Danny Smyth	14 March 2012	IGG
3.0	Danny Smyth	11 March 2013	IGG
4.0	Danny Smyth	04 April 2014	IGG
5.0	Danny Smyth	20 April 2015	IGG
6.0	Danny Smyth	19 August 2016	IGG

Information Management &
Governance Team

Email : privacy.officer@Investni.com