Information Security Handbook

August 2025

Contents

Foreword

'Our Future in Focus' recognises organisational excellence as one of the foundations to the delivery of our strategic priorities. Information security is a cornerstone of organisational excellence, as it safeguards the integrity, confidentiality, and availability of information that underpins critical decision-making and service delivery.

For this reason, ensuring effective information security is fundamental to the success of Invest Northern Ireland. It is vital for public confidence and for the efficient and effective operation of our business.

Invest NI is entrusted with a wide range of sensitive material, of both a commercial and a personal nature. It is our responsibility to ensure this information is handled appropriately and securely.

Information security is not a procedural formality; it is a critical enabler of our operations. Any unauthorised access or misuse of data could lead to serious financial or reputational harm to our clients and stakeholders whilst also leading to significant reputational damage to Invest NI.

This handbook provides a single source overview of the key policies, procedures and governance structures that underpin the security of the information used by all of us within Invest NI. In today's hybrid working environment, it is more important than ever that all staff understand and consistently apply the guidance it contains.

I fully support the principles outlined in this handbook, along with the associated policies and annual mandatory training. Information security is a shared responsibility and each of us plays a crucial role in safeguarding the personal and business data we manage, handle and access.

Kathryn Hill

Chief Operating Officer

1 Key Facts: Information Security

What Is It?

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

Why Do We Do It?

- Protecting information entrusted to us by clients, stakeholders and others
- Personal professional integrity
- Protecting organisational reputation
- Legal requirement
- Avoid negative consequences
    - regulatory fines
    - disciplinary action
    - legal action
    - client relationship difficulties
    - bad press

Who Does It?

- All of us
- 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 and guidance referenced in this handbook
- Undertake mandatory Data Protection and Information Security training
- Implementing ISO27001 certification requirements

2 Introduction

1. Invest NI recognises that robust principles of information security must be applied to all the information it holds. This includes business and commercially sensitive information and personal data on clients, 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 recognised 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 and accountability structures to deliver and maintain an effective information security management system.

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

4. Staff commitment is vital 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.

5. This handbook applies to all Invest NI employees, contractors and temporary staff working in Invest NI regardless of geographical location.

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 the 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 2018, The UK General Data Protection Regulation, The Official Secrets Act, 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 fosters 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 security into the organisational ethos.

4. Invest NI continues to maintain, and is committed to continual improvement of, an Information Security Management System independently certified to the ISO 27001 standard.

5. Information security objectives, and progress against these, are set and reviewed by an Information Governance Group headed by the Chief Operating Officer 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 Security framework detailed below sets out 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 is vital in ensuring information is held and managed securely. To that end all staff are responsible for the protection of the personal/ business sensitive information that they manage or access as part of their day-to-day activities regardless of location.

3. 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 all staff, regardless of grade, to ensure that they follow the information security related policies and guidance as detailed at Section 7 of this handbook.

4. There are additional risks when working in a mobile manner, and staff are responsible for the security of equipment and information in their possession, including the transportation of such information.

5. Staff must also undertake mandatory annual organisational Information Security awareness training and Data Protection awareness training when requested to do so within the required timeframe.

Line Management Responsibilities

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

Senior Management Responsibilities

7. 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 ultimately 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.

8. 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 assurance to the CEO that appropriate divisional arrangements are in place to ensure compliance with data management and data security policies.

Organisational Governance

9. The Senior Information Risk Owner (SIRO) for Invest NI is the Chief Operating Officer. 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.

10. 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 direction, support and consideration to the management of information security initiatives and information risk management and is responsible for the maintenance of the ISO27001 certification.

11. The Information Governance Group is chaired by the Head of Internal Operations (the DSO). Its members also include the SIRO, the Executive Director of People & Culture, the Performance Compliance and Co-ordination Director, the Head of Information Governance (Data Protection Officer), the Information Governance Manager, the ICT Manager, the Cloud,

Security & Infrastructure Manager, the Risk Manager and the Contracts and Facilities Manager.

12. The Technical Security Manager (TSM) 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
    - assurance is provided in respect of its compliance with information security and data protection contractual requirements (see 'Contract Management – Protective Measures Assurance Form' 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 are procured (see Procurement intranet webpage).

7. Where no services are procured and information is being shared, such as for the delivery of a collaborative programme with another public body, then a relevant Data Sharing Agreement (DSA) must be signed. The agreement should be signed on behalf of Invest NI by a Director/ Divisional Head. Template DSAs can be found on the intranet. A copy of the signed DSA should be sent to the Information Governance Team via, privacy.officer@investni.com .

Risk Management

8. 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 Framework details the approach the organisation takes to managing risk.

9. It is the policy of Invest NI to comply with all regulatory or legislative requirements placed upon the organisation. Therefore, a breach of such requirements would be perceived as high risk, with the organisation adopting an 'averse' risk appetite in respect of protecting personal and business sensitive information.

10. All projects and activities that involve collecting and/or using personal or commercial data give rise to risks related to data protection compliance and security. To enable Invest NI to address these concerns, these projects and activities must undergo a Data Protection Impact Assessment (DPIA) screening exercise, to determine if a full assessment is required. Further information can be found in the Data Protection Impact Assessment Guidance and Procedural Manual available on the intranet.

Internal Monitoring

11. 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.

12. All Invest NI resources, including corporate email and M365 tools are provided for business purposes. Our systems enable us to monitor e-mail, Teams messages, 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 device 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 'Information Systems Acceptable Usage Policy' and the 'Policy on Sending Information outside Invest NI').

13. Invest NI's Information Security Management System is also reviewed by DfE Internal Audit Service on an annual basis. This auditing supports external audits of Invest NI's 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 they are enabled to play their role in protecting corporate data.

Induction/ Staff Onboarding

2. It is important that all new staff joining Invest NI are made aware of the organisation's information security standards and policies. To this end all new staff are required to complete Data Protection and Information Security e-learning training on day one of their employment. 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 it on an annual basis within the specified timescale to comply with the organisational Data Protection Policy.

Records Management training

4. Effective management of records can ensure information is handled correctly. Mandatory Records Management Awareness Training will be made available to all staff, including at induction. Short, helpful user guide videos are available via the intranet on using ECM, the main corporate repository for records. Divisional Information Co-Ordinators can also provide hands-on training. The Records Management team will provide advice and guidance on specific issues.

Information Security Awareness training

5. Mandatory Information Security awareness training is also required to be completed across the organisation on an annual basis. All staff must complete within the specified timescale to comply with the organisational commitment to protecting corporate data.

Communicating the Information Security message

6. 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

1. The following is a list of all the current information security related policies within Invest NI. To maintain a secure and effective information environment within Invest NI, it is important that everyone knows and follows the policies and guidance set out in these documents.

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

- **Information 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.

- **Data Protection Policy**

Data Protection legislation 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 legislation.

- **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 by Invest NI staff.

- **Data Transfer Policy**

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

- **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.

- **Records Management Policy**

This policy sets out the principles that apply to the management of records,

both physical (paper) and electronic, across the organisation.

- **Data Breach 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.

- **Risk Management Framework**

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.

- **Data Protection Impact Assessment guidance and procedure manual**

New activities that involve using personal information give rise to data protection concerns. A Data Protection Impact Assessment (DPIA) is used to assess risks and identify mitigating measures.

- **Guidance on Protective Marking**

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

- **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.

- **Contract Management – Protective Measures Assurance Form**

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

- **Access Procedures**

Procedures followed when a staff member or a third party joins, moves or leaves the organisation to ensure appropriate access to Invest NI systems and buildings.

Version Control

Author: Danny Smyth
Issue Date: August 2025
Issue Number: 10.0
Approver: Information Governance Group
Status: Approved
Next Review Date: August 2027

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
7.0	Danny Smyth	28 August 2018	IGG
8.0	Danny Smyth	14 May 2021	IGG
9.0	Danny Smyth	17 May 2023	IGG
10.0	Danny Smyth	14 August 2025	IGG

Information Governance Team

Email : privacy.officer@Investni.com