Information Security Policy

Version	4
Date Approved by Board	30 March 2020
Date of previous approval	15 May 2018 8 March 2016 4 February 2014
Date of next Review	March 2022

You may also be interested in the following policies:

Accessible Information
Publication Scheme
Information Security Policy
Records Management
File Retention and Disposals Policy

1. Introduction

Providing assurance; meeting our obligations

1.1. This Information Security Policy is based upon The Executive Office (TEO) Information Security Policy and has been revised appropriately to reflect the organisational structure of the Commission for Victims and Survivors. It describes in detail the context, governance arrangements and actions that are required to provide assurance that the Commission fully meets its obligations in this important area.

One-stop reference manual

1.2. The specific purpose of the document is to bring together into a single source an overview of the various policies, procedures and structures that have been put in place to ensure the delivery of a safe environment for the handling of the information and data required by the Commission to carry out its responsibilities.

1.3. The following areas are explained in detail:

- The **legislative context** in which the Commission is obliged to operate;
- The **accountability and governance** arrangements which are in place to monitor and control performance and provide assurance that information is being handled securely;
- Specific **responsibilities and roles** that are mandated or deemed to be best practice are outlined;
- The **controls, monitoring practices and processes** that mitigate against data loss and provide assurance are described;
- The various **data handling procedures** and policies that are in place within the Commission are outlined;
- The requirement for staff to be fully cognisant of their **personal responsibilities** is also addressed together with an outline strategy to achieve this; and
- Key current relevant **policies** are outlined and links are provided to the full documents.

1.4. Effective information security is a key priority for the Commission for Victims and Survivors (the Commission). It is vital for public confidence and for the efficient, effective and safe conduct of public business. In carrying out its duties effectively the Commission obtains, processes and manages a broad range of information from both the business community and the citizen. Many of the services provided by the Commission involve the collection and handling of personal or business sensitive data and information directly which must be managed appropriately and securely.

1.5. The Commission 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 held on clients, associates, employees, suppliers, contractors and the citizens. The Commission is committed to ensuring that all the sensitive information entrusted to it is managed lawfully and appropriately.

1.6. Legislation including The Official Secrets Act, EU Data Protection Regulation (2018), Freedom of Information Act 2000, Computer Misuse Act 1990 and The Human Rights Act 1998 set the legal framework within which the Commission must operate and ensure the safe storage and handling of information. The Commission fully appreciates and will take the necessary actions to ensure that it continues to comply with all legislation regarding its management of personal data and other information.

1.7. While the gathering and analysing of information is essential to the provision of effective public services and the development of relevant and meaningful Government policies, it is clear, nonetheless, that this must be done in a way that ensures the security of that information and preserves the individual's right to privacy. As a Non-Departmental Public Body of TEO, the Commission accepts fully that it is its responsibility to manage safely the information with which it is entrusted and to this end the Commission has in place a range of information security policies and corporate governance and accountability structures to deliver and maintain effective information security.

1.8. The Commission accepts fully the need for transparent accountability and explicit assurance that we will continue to maintain high standards of information security. **This responsibility is not limited to the Commission but equally applies to its delivery partners, contractors, suppliers and any other third party organisation established to support the Commission in its delivery of services**.

1.9. Therefore, the Commission ensures that effective corporate governance arrangements are in place to continually manage and assure all aspects of its approach to data security. The specific purpose of this document is to bring together into a single source an overview of the various policies, procedures and structures that have been put in place to ensure the delivery of a safe environment for the handling of the information and data required by the Commission to carry out its responsibilities. It also provides a single point of access to the information security policies and procedures in place within the Commission. In particular this document sets out:

- The accountability and governance arrangements which are in place to monitor and control performance and give assurance that information is being handled securely;
- The controls and monitoring practices and processes that mitigate against data loss; and
- The various data handling procedures and policies that are in place within the Commission.

2. Policy Statement

2.1. The Commission regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between the Commission and those with whom it transacts business and the public in general.

2.2. The Commission fully endorses and adheres to the personal data as laid out in the General Data Protection Regulation (GDPR). Personal data should be:

a) processed lawfully, fairly and in a transparent manner,
b) collected for specified, explicit and legitimate purposes,
c) adequate, relevant and limited to what is necessary,
d) accurate and where necessary kept up to date,
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and
f) processed in a manner that ensures appropriate security of the personal data.

2.3. Accountability is central to GDPR. The Commission takes care to adhere to these principles, being responsible for compliance with the principles, and able to demonstrate this to data subjects and the regulator.

2.4. The Commission seeks to foster a culture that values, protects and uses information for the public good through a range of methods and arrangements.

2.5. The Commission works closely with its sponsoring Department, TEO, and the Information Commissioner's Office (ICO) to ensure compliance with the legal and regulatory framework. The Commission will maintain open communication with them about the personal information it holds, how it is used, and the rights of those with respect to the use of their information.

3. Accountability and Governance

3.1. Effective accountability and governance arrangements are essential to ensure the proper management and control of information. The following paragraphs detail the various oversight roles and responsibilities that the Commission has in place to deliver an effective governance regime.

Commission Board

3.2. The Commission Board considers issues which affect the corporate governance.

3.3. The Board considers issues which affect the corporate governance of the Commission. These include:

- progress against performance indicators;
- finance issues;
- issues relating to audit and accountability; and
- an overview of major policy issues.

Audit and Risk Assurance Committee (ARAC)

3.4. The ARAC assists the Commission's Board in fulfilling its corporate governance responsibilities and oversees the corporate governance and risk management processes. The ARAC provides a means of independent assurance and objective review of the Commission's financial systems, financial information and internal control mechanisms. Internal control includes risk management which in this context specifically includes information security.

Accounting Officer

3.5. The Accounting Officer has ultimate responsibility for information security within the Commission and is required to provide, in the annual Statement of Internal Control, assurances that information risks are being controlled and managed and that the Commission continues to be a trusted custodian of personal and business sensitive information.

3.6. The Accounting Officer is also charged with the responsibility of performing the following roles within the Commission:

Senior Information Risk Owner (SIRO)

3.7. As the SIRO, the Accounting Officer reports regularly to the Commission's Board on information security matters within the Commission, provides assurances that standards are being maintained and reports any incidents that have been identified in the previous period.

Commission Accreditor / Information Technology Security Officer (ITSO)

3.8. As the SIRO, the Accounting Officer is the Commission's lead on risk management of information security matters and is the primary liaison with TEO on information security matters.

3.9. The Commission's ICT Infrastructure and services are provided and managed by the Equality Commission for Northern Ireland (ECNI) through a Service Level Agreement (SLA). As the SIRO, the Accounting Officer is also the primary liaison with the ITSO in ECNI regarding information security matters.

Information Asset Owner (IAO)

3.10. The Unit Heads within the Commission are the IAOs for their individual business areas and are responsible for the secure management of information within their business areas, and other third party organisations. They are also the primary liaison contact point for the SIRO on information security matters, including performance reporting, incident reporting, raising information security awareness and audit & accountability matters. The IAOs are also responsible for ensuring that all information and records management policies are implemented fully for their business area.

Staff Responsibilities

3.11. The role played by individual staff members is vital in ensuring information is held securely. To that end all staff must take responsibility for the protection of personal/sensitive information that they manage or access as part of their day to day work activities. It is therefore essential that all Commission staff are familiar with the Commission's information security policies. Staff must ensure that all personal or sensitive information in their possession is kept secure at all times against unauthorised or unlawful loss or disclosure.

3.12. In particular it is the responsibility of staff to ensure that:

- paper files and other records or documents containing personal/sensitive information are kept in a secure physical environment in line with the official **Records Management Policy** of the Commission;
- personal/sensitive information held on computers and computer systems is stored in line with the **IT Security Policies**, and
- if they are required to pass information to an organisation outside the Commission, that they follow the guidance as set out in the **"Guide to Document and IT Security."**

3.13. In addition to their responsibilities as members of staff, line managers have a responsibility to ensure there are appropriate procedures in place so that the

required authorisations are secured before any personal/sensitive information is released outside the business area.

3.14. Attached at **Annex A** is a chart showing the Information Assurance governance and reporting structure in the Commission.

4. Controls, Monitoring and Reporting

4.1. Effective controls, monitoring and reporting procedures are necessary to ensure that high information standards are in place and are being maintained. To that end the following range of measures are in place to provide assurance that information security within the Commission is effectively managed and business risks are properly managed.

Statement of Internal Control

4.2. The Statement of Internal Control (SIC) is an annual statement made by the Accounting Officer as part of the Commission's Annual Report and Accounts. In it the Accounting Officer comments on a range of risk and control issues. To adequately make this statement the Accounting Officer needs comprehensive and reliable assurance from managers, internal audit and other assurance providers that risks, including information risks are being managed effectively. The SIC includes a specific reference to the handling of information risk issue within the Commission.

Quarterly Assurance Statements

4.3. The Quarterly Assurance Statements are provided to the Commission's sponsoring Department, TEO. The Assurance Statements provide the Accounting Officer with a valuable source of assurance on internal control systems. Each Assurance Statement contains a completed checklist and a statement signed by the Accounting Officer providing assurance that risks are being managed to a reasonable level. This Assurance Statement includes a specific reference to the management of information security.

Audit Role

4.4. Information security will be an integral aspect of the work of Internal Audit when reviewing the processes and procedures within the Commission. Independent audit of the procedures in place is an important element in assuring best practice is being followed and that Commission policies are being adhered to.

Annual Review

4.5. The Commission will carry out an annual data security review aimed at ensuring the Commission is adhering to information management policies and

is handling information, for which it is responsible, safely and securely. The review survey requires each Commission to report to TEO on the management of information within the organisation and covers key aspects in relation to information security. The survey also includes data retention periods and identifies when data should be securely destroyed.

Risk Register

4.6. The assessment and management of risk is central to good corporate governance. This is no less true for the management and securing of information. Therefore the Commission's Risk Register will identify information security related risks and detail how these risks are managed and mitigated. The Risk Register is reviewed on a monthly basis by the Commission's Board and on a quarterly basis by the ARC as part of the risk management system.

Incident Monitoring and Reporting

4.7. An important aspect of the Commission's information security policies is the **effective and timely reporting** of all suspected incidents of misuse of personal/sensitive information or breaches of information security. The "**Procedure in the event of a significant loss or theft of NICS Information or IT equipment**" must be followed when reporting such incidents.

4.8. It is the responsibility of the Accounting Officer to oversee investigations into suspected personal data loss incidents and where necessary:

- inform the Information Commissioner's Office of the suspected incident;
- inform the Commission's sponsoring department, TEO;
- activate a response plan to the incident; and
- report to the Commission's Board and Audit and Risk Committee.

Third Party Organisations

4.9. The Commission may establish Third Party Organisations (TPOs) as an effective means of delivering on its statutory duties and services. While these organisations have autonomy in their operations, the Commission also has a role to monitor and ensure that public information which the TPO maintains is handled securely.

4.10. The Commission will ensure that any TPO for which they are responsible is fully aware of the Commission's information security policies. Each TPO should be in a position to demonstrate that they have appropriate procedures and policies in place to ensure effective information security standards are maintained and monitored.

4.11. Information security should be a standing item on the agenda of all formal meetings between the Commission and TPOs.

Delivery Partners, Consultants, Contractors and Suppliers

4.12. The Commission will from time to time enter into arrangements with a range of other organisations to support it in delivering on its objectives. These may include organisations in the private, community and voluntary sectors. Such organisations may be contracted to undertake services or work which may require them having access to, handling, storing or disposing of information.

4.13. It is essential that, in entering into contractual arrangements with such organisations, the Accounting Officer ensures that the Commission's information security standards are maintained and protected.

4.14. Therefore, it is the responsibility of the Accounting Officer to ensure that when entering into a contract with an outside organisation:

- information security is reflected accurately in the contract;
- the contracted organisation is fully aware of the Commission's Information Security Policy; and
- Information Security will be a standing item on all formal monitoring and reporting mechanisms.

4.15. To assist in the delivery of effective and robust contracts the Commission commits to using the Central Procurement Directorate (CPD) for such procurements and the Commission will continue to work with CPD to ensure information security matters are accurately reflected in these contracts.

Network & Application Controls

4.16. The network controls within CVS will be maintained and controlled by ECNI through the SLA agreement agreed at 3.9 above. Any modifications to network controls follow the ECNI change management procedure after approval from CVSNI.

4.17. Any 3rd party applications are controlled and monitored by CVSNI staff and are configured and updated based on the Best Practice guidance set by the provider.

5. Supporting Legislation and Legislative Context

5.1. There are three main pieces of legislation currently in force that require the Commission to disclose information. Detailed guidance on these can be accessed via the following links: –

- The Freedom of Information Act 2000;
- EU General Data Protection Regulation (2018); and
- The Environmental Information Regulations 2004.

5.2. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC.

5.3. The GDPR places responsibilities on any organisation to process personal data that it holds in a fair and proper way. This is the Commission's policy and statement on the purposes for which it holds personal data about its employees and others who work for it.

5.4. Under the GDPR, the data protection principles set out the main responsibilities for organisations.

5.5. Article 5 of the GDPR requires that personal data shall be;

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

5.6. Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Handling Requests for Information

5.7. As well as having a duty to protect the information the Commission holds, the Commission is also required by certain legislation to make information available to the public on request. In responding to requests from the public, the Commission must ensure that sensitive information is not accidentally or inappropriately released, while at the same time meeting its obligations to disclose. It is therefore important that all staff are made aware of the statutory framework within which the Commission is required to disclose information; are able to recognise requests to which these requirements apply; and are familiar with the Commission's procedures for handling such requests. Advice and practical support on the handling of individual requests is also available by contacting the Information Management & Central Advisory Branch (IMCAB) of TEO.

6. Training and Communications

6.1. The Commission 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 the Commission delivers a safe environment for the management of the information it holds.

Information Security Training

6.2. Through the advice of the Commission's sponsoring department, TEO, the Commission will ensure that all centrally mandated information security training is provided to its staff. TEO is currently reviewing the existing training

provision and the generic requirements that may be needed in the future to ensure that a consistent standard of information security training is available to all staff and ALBs.

Commission Staff Induction

6.3. It is important that all new staff joining the Commission are made aware of the Commission's information security standards and policies. To this end the Commission staff induction process contains a section on information security which emphasises the importance attached to information management in the public sector in general and the Commission in particular. During induction training, staff are provided with take away material for future reference. However, the effective induction of new staff also relies heavily on the training processes within Commission. Therefore, it is incumbent on all line managers to ensure their new staff are familiar with this policy and all guidance and procedures.

6.4. Some business areas in the Commission have greater access to sensitive information and as such the basic induction training may not be sufficient. Where this is the case the appropriate Head of Department within the Commission will provide advice and guidance on the development of tailored training for key staff.

Records Management training

6.5. Effective management of records can ensure information is handled correctly. Staff should consider their training needs in this area, along with their line manager and apply for generic training courses as necessary.

Communicating the Information Security message

6.6. The Commission 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.

7. Information Policies and Guidance

7.1. The following is a list of all the current information security related policies in force within the Commission with links attached (coloured blue and underlined). If a secure and effective information environment is to be maintained within the Commission it is essential that staff should be familiar with, and apply fully, the policies and advice set out in these documents.

The NICS Information Assurance Policy

7.2. This policy is based on the Cabinet Office issued Her Majesty's Government (HMG) Security Policy Framework and applies to all NICS Departments, ALBs and other organisations who are connected to NetworkNI.

A Guide to Document and IT Security

7.3. This guide published by TEO is intended to provide a ready reference on matters relating to document and IT security. The standards and procedures in the guide are the minimum which must be applied uniformly throughout all Departments and Agencies.

Key Rules on Securing Sensitive Data

7.4. This document sets the 10 key rules that all NICS, and Commission staff must follow to ensure the security of personal data.

Guide to Internet and E-mail Usage

7.5. A policy is presently in place for all staff in relation to the use of the internet and e-mail facilities on the Commission's Information and Communications Technology (ICT) resources. The Commission's **'Internet and E-mail Policy'** has been reviewed and approved by the Equality Commission Northern Ireland (ECNI) who provide ICT infrastructure services and support to the Commission through an active SLA.

Laptop and Mobile Devices Security Policy - Advice and Guidance

7.6. This document provides advice and guidance to staff on the use of laptop devices.

Guidance for Information Asset Owners

7.7. This document provides summary guidance for IAOs to explain their responsibilities in terms of Information Assurance. IAOs can contact the Departmental Accreditor) for guidance.

Procedure for Disposal or Transfer of IT equipment

7.8. This document sets out the procedure to be followed for disposal or transfer of all IT equipment.

Anti-Fraud Policy & Response Plan

7.9. The Commission's '**Anti-Fraud Policy'** and **'Fraud Response Plan'** covers any fraudulent use of information – personal, sensitive or classified which is held by the Commission.

Clear Desk Policy

7.10. This document details the requirement for all staff to ensure a clear desk at close of the working day with equipment and sensitive material locked away.

Central Procurement Directorate

7.11. Through the Department the Commission has a Service Level Agreement with the Central Procurement Directorate (CPD) in DFP to use its services for tendering and procuring goods and services. ETendersNI must be used for all procurement exercises over £5,000 for services which will include the handling, use, storage or transmission of information.

7.12. Central Procurement Directorate have in place a set of information security related clauses in its standard Terms & Conditions, used for all contracts tendered for through them. It is the responsibility of the Commission's Accounting Officer to ensure that these clauses are sufficient for the services they are planning to procure. If additional safeguards are required as part of the contract the Accounting Officer should speak with the Account Manager in CPD and additionally speak with the TEO ITSO and Accreditor for advice and guidance. The Commission has the right to include additional safeguards in the tender documentation that issues as part of the tendering process for the service being sought.

Risk Management

7.13. It is a mandatory requirement that all ICT systems which store, process, transmit or exchange protectively marked government data are accredited. It is the responsibility of the IAO for the business area, or the SRO for a new project, to engage with the Departmental Accreditor at an early stage to ensure that all such systems are accredited before going live.

Annex A

Information Security Governance and Reporting Structure