Highland Council

Information Security & Assurance Policy

Contents

1. Document Control

1.1 Version History

Version	Date	Author	Change
V1	28/08/2013	Philip Mallard	Information Security Policy created and approved by FHR Committee.
V1.1	25/02/2015	Philip Mallard	IM Policy Framework Annual Review. Approved by Resources Committee.
V2	23/11/2016	Philip Mallard Information & Records Manager	Approved by Resources Committee. IM Policy Framework Annual Review Change to title from Information Security Policy to Information Security & Assurance Policy to better reflect scope. ICT Security Policy for Mobile & Flexible Working merged into Policy.
V3	17/10/2022	Miles Watters FOI & Data Protection Manager	Policy Framework Review Approved at Corporate Resources Committee 01/12/2022

1.2 Document Approval

Name	Title	Role
	Corporate Resources Committee	Approval
Kate Lackie	ECO Performance & Governance (Senior Information Risk Owner)	Review and acceptance
	Information Governance Board (IGB)	Review and acceptance

2. Introduction

The Information Security & Assurance Policy sets out the Council's management commitment and approach to ensuring the confidentiality, integrity and availability of its information.

It provides high level rules, responsibilities and roles that apply to members, staff, partners (such as High Life Highland), and those working on behalf of the Council or handling Council Information. The Information Security & Assurance Policy is part of the Information Governance Policy Framework, and together these set out the information security requirements.

More detailed operational requirements are set out in in the Council's Information Security Management System (ISMS).

3. Definition of Information Security

Information is an asset of the Council, and the Council needs to manage it as such, ensuring it is adequately protected. This is especially important in the increasingly interconnected and shared business environment.

Information can exist in many forms e.g. It can be printed or written on paper or stored electronically. Whatever form the information takes, or the means by which it is shared or stored, it should be appropriately protected.

Information security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to protect confidentiality, integrity and availability.

Information security is achieved by implementing a suitable set of controls, including the use of policies, processes, procedures, organisation structures, software and hardware. These controls need to be established, implemented, monitored, and reviewed (and where necessary improved), to ensure that the security and business objectives of the Council are met.

Information security requirements and the Data Protection legislation need not be a barrier to appropriate sharing of information. Through effective security controls and careful consideration of legal obligations we can be more confident in sharing information where appropriate.

4. Highland Council Commitment to Information Security

The Council is committed to effective Information Security through the management of information security risks that occur through both internal and contracted out activities.

The Council will implement and operate appropriate countermeasures and procedures to manage those risks down to an acceptable level, as determined by specialists within the Council, and in line with best practice.

The aim is to ensure business continuity, minimise business risks whilst maximising the return on investment and enabling business opportunities.

Through the Information and Data Strategy, supporting policies and the Information Governance Programme the Council will work to put in place the changes that are required to support the ISMS and effective information security.

The Council recognises that effective information security is achieved through a combination of policy, procedures, a risk based approach, security controls such as building security and most importantly staff information security awareness and skills. This requires an on-going commitment to continual improvement and change that can only be achieved through the support of all staff and those involved in handling Council Information Assets.

5. Policy, Legal & Standards Framework

The Council recognises that it works within a legal framework that places legal obligations on both the Council and its staff in relation to the management of information. The Council has an Information and Data Strategy and a framework of information governance policies that set out how we work to fulfil both the statutory obligations and our duty of care to people and organisations whose information we hold.

The legislation, policy and standards set out below are particularly relevant to the Information Security Policy, but there may be others that also have some relevance and the omission from this list in no way diminishes the Council's commitment to follow its obligations to comply with any statutory requirements and to work within best practice.

5.1 Council Information Governance Policy Framework

- Information Management Policy
- Records Management Policy
- Records Retention & Disposal Policy
- Information Security and Assurance Policy
- Data Protection Policy

5.2 Other relevant Council Policies

- ICT Acceptable Use Policy

5.3 External Standards

- ISO/IEC 27001/2 and ISO27000 Series

5.4 Legislation / regulation

- Data Protection Act 2018
- UK General Data Protection Regulation
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA), Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and other connected legislation.
- Copyright, Designs & Patent Act 1988 & other Intellectual Property Rights legislation
- Re-use of Public Sector Information Regulations 2015 and INSPIRE (Scotland) Regulations 2009

6. The Information Security Management System (ISMS)

The Councils approach to the management of Information Security is defined in the Information Security Management System (ISMS). This aims to coordinate and continuously improve the management of risk to information and sets out our approach to the application of our Information Security and Information Governance Policies. It commits the Council to design, implement and maintain a coherent set of policies, processes, and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The ISMS provides the means to understand risk, develops ways of managing that risk, monitors how effective that has been and identifies potential areas of improvement and how it needs to adapt to the changing business environment.

The Highland Council ISMS is based upon the international information security standard ISO/IEC 27001 and the implementation of the controls of ISO/IEC 27002. These standards are referred to as the “ISMS Family of Standards” and are recognised as the International de-facto Security Standards.

The ISMS will support management in ensuring that available security resources are spent on the areas that will deliver the greatest improvement in the management of information and reduction in risk e.g. are finances better invested in implementing additional security measures to the network or would investing in the security training of personnel be more effective?

The ISMS is supported by this Policy, and the other polices that make up the Information Governance Policy Framework. The Information and Data Strategy sets out the Council’s overall strategy for the management of its information which includes Information Security.

7. Information Security Policy Statements (in support of the ISMS)

The following are statements of Council Policy on issues that are important to the delivery of effective Information Security. The Council ISMS sets out operational details of how these are applied by the Council and further guidance will also be provided as appropriate to those affected by these policy requirements.

7.1 Encryption Policy - Cryptographic Controls and Key Management

Staff and any person working with Council Information Assets may only use encryption products that are authorised for use by ICT Services.

Only encryption products that include and make use of central key management should be used by the Council. Any exceptions to this must be approved by the Head of ICT & Digital Transformation and will require additional controls to be in place to ensure the encryption technology is appropriately managed. This must include (but not be limited to) the corporate retention of keys to enable decryption in the event of the Council being required to do so.

Technical controls and measures required for safe, secure and legally compliant use of encryption products will be maintained as part of the ISMS documentation and will be maintained by ICT Services.

The design and configuration of all Council ICT systems and those from third party providers used by the Council to store Council Information must adhere to this Encryption Policy and to the technical controls and measures that are set out as part of the ISMS. All contracts with providers and contractors must set out this requirement.

7.2 Physical / Building Security

It is the responsibility of the relevant Responsible Premises Officer (RPO) to ensure that a building used by the Council is adequately secure for the storage of the information that is held within it.

Managers and Information Asset Owners should ensure that any building they use for the storage of information (on paper or electronic storage) is adequate for the type of information they are holding. If there are any weaknesses in the building security then this must be reported to the RPO. Any other physical security issues such as a lack of local lockable storage must be dealt with by the Manager / Information Asset Owner responsible for that Information Asset.

7.3 Confidentiality Agreements & Data Sharing Agreements

Prior to any systematic, routine sharing of personal information there must be a data sharing agreement put in place. A copy of the data sharing agreement must be added to the Corporate Data Sharing Register.

Highland Council employment contracts will include confidentiality clauses.

Any third party that is provided with access to Council Information Assets must sign a confidentiality agreement that sets out their obligations and requires compliance with this Policy, ICT Acceptable Use Policy and all other relevant Council Policies (including those in the Information Governance Policy Framework).

7.4 Management of ICT Systems

All ICT systems must follow the requirements and controls set out in the Council ISMS and any supporting ISMS Policy documents. This should include but not be limited to the appropriate set up, management of systems, implementation and documentation of access controls.

All System Owners must ensure compliance with the Council ISMS and should create and maintain appropriate documentation to support management in accordance with the ISMS.

System Owners must be able to provide documentation as and when requested by ICT Services and Internal Audit that demonstrates their compliance with the ISMS.

7.5 Removable Media

Removable media is a data storage device that is not attached to a computer and can be used to hold and transfer information from one computer to another. This includes CDs, DVDs, Memory Sticks, Portable hard drives, memory cards (e.g. SD cards), and any electronic device that has internal storage (e.g. digital cameras and recording devices).

Removable media should only be used for the temporary storage and transportation of data. Where sensitive or personal data is being held on removable media the data and/or device must be encrypted and done so in accordance with the Encryption Policy (As set out in section 7.1). Handling of removable media must be appropriate to the type of information held on it and not be used to transfer Council information to personal devices as this use is contrary to this Policy and ICT Acceptable Use Policy.

Only removable media that has been approved for use by ICT Services may be used.

7.6 Disposal of Information held on ICT Equipment, Removable Media and Paper

All Computer media or paper that may contain personal or confidential data must be securely destroyed. Personal and Sensitive data must be removed from ICT equipment prior to destruction or recycling.

All ICT equipment and media must be disposed via an appropriate Council approved disposal service. This can be accessed by contacting the ICT Service Desk.

Paper containing personal or other confidential information must be disposed of using the Council confidential waste paper disposal bins or other approved method as defined in the Council's Confidential Paper Waste Procedure. If you do not have access to appropriate disposal services then you should contact your RPO to locate the nearest confidential waste paper disposal bin.

7.7 Clear Desk & Clear Screen Policy

All staff, those working on behalf of the Council, or handling Council Information must ensure that they lock their screen when computer equipment or mobile devices are left unattended and ensure that their screen cannot be read by others when they are in use.

All staff, those working on behalf of the Council, or handling Council Information must ensure that they leave their desk or working area clear of all personal or confidential information / documents when they are away from their desk (unless adequately managed on their behalf or the room is locked).

Laptops must be stored out of sight and not left out at the end of the working day. If possible, they should be stored in a locked cupboard or cabinet.

This section applies whether staff are working in a Council Building, when travelling on behalf of the Council or working from home.

7.8 Password Policy

System Owners must follow the ISMS Password Policy rules when defining requirements, and implementing systems.

Passwords used must be complex. The Council will ensure that any ICT systems use available technical controls to force complex passwords as appropriate to the information being held within the system.

All ICT users must ensure that they follow Council password guidance to create a complex password for each ICT System they access.

Passwords must be treated as confidential and not shared with others. Intentional sharing of passwords is a breach of the ICT Acceptable Use Policy.

If a password does become known to another person or there is a suspicion that a password has been compromised then this must be reported as a security incident by contacting the ICT Service Desk.

7.9 Intellectual Property Rights (IPR)

The Council will respect Intellectual Property Rights when handling information, working to ensure it complies with its legal obligations.

The Council's own IPR will be protected, whilst supporting re-use where appropriate. The Information Management Policy sets out the principle that Information will be reused and shared where appropriate. This includes allowing re-use both internally and externally of information that is non-personal and non-commercially sensitive. In particular, the Council shall work towards making its data open and available for re-use, in compliance with its obligations under the Re-use of Public Sector Information Regulations 2015 and INSPIRE (Scotland) Regulations 2009.

7.10 Vulnerability Assessment and Penetration Testing

The Council will carry out Vulnerability Assessment and Penetration Testing on its network infrastructure.

The Council will risk assess the need to carry out penetration testing and vulnerability assessment on its ICT Systems. It is the responsibility of each System Owner to assess the need for this based on the type of system and the information held within it.

7.11 Hybrid working

All handling and storage of Council electronic information must be done using ICT that has been authorised for this purpose. This requirement is further expanded in the ICT Acceptable Use Policy. Generally that will mean ICT equipment provided and managed by the Council's ICT Services team. However, some access to certain resources, such as M365 and Assure, is also made available for staff to access on personal devices. This is more limited and with higher levels of protection than for Council-supplied equipment. For instance, multi-factor authentication is likely to be mandated for such access.

All handling and storage of paper based Council information must be in accordance with this Policy, the Information Governance Policy Framework policies and local procedures. Paper based Council information must only be removed from Council premises where this has been authorised and appropriate arrangements are in place to protect the confidentiality, integrity and availability of this information.

Business processes that require information and ICT (that provides access to Council information) to be removed from Council premises shall be risk assessed to ensure security arrangements are adequate for the type of information. It is the responsibility of the relevant Information Asset Owner and Information Asset Manager to ensure that local procedures are produced and are communicated to those handling the information. A clear distinction is made between arrangements

put in place to meet immediate emergency requirements (when staff have to vacate a building to work from home) and longer-term working arrangements. In emergency situations it may not be possible to fully assess and mitigate against security risks, but that assessment should be done as soon as practically possible and certainly if the arrangements become long-term.

Local information handling procedures must be appropriate to the type of information being processed as part of the local business activity. These must include the following controls to protect information:

- Paper based Council information and Council ICT must be kept in sight at all times and be under the control of the Council representative when off site (subject to the exception where the Council is supporting a customer in completing information where the customer is the owner of the information).
- Use of Council ICT must be positioned in a way that complies with the clear screen policy (Section 7.7) and ICT Acceptable Use Policy to prevent unauthorised access to information. This should not prevent appropriate viewing of information by third parties where this is required as part of the business process.
- Council ICT and paper information must not be left in a car unattended during offsite working activity unless this is securely stored (not visible such as in a covered area in the boot of the car).
- Council ICT and paper information must not be left unattended in a car overnight. Exceptions may be made where this is the best possible security available, but in any case the information / ICT must not be visible and a risk assessment must be carried out.
- The Council's clear screen and clear desk policies, detailed in Section 7.7, must be complied with when working from home. Council ICT and paper information must not be left unattended and must be kept secure when not in use.
- Staff working from home must ensure meetings take place in a location where confidential discussions cannot be overheard by third parties.

Authorisation for Council staff to work from home or other locations not within Council Buildings must be captured within the New Ways of Working (NWOW) Teams Agreements. An appropriate information risk assessment must be carried out to understand the risks associated with these arrangements and this must be taken into consideration as part of the decision on whether to allow the hybrid working. Authority for mobile and flexible working shall be in line with the Council Flexible Working Policy.

NWOW Team Agreements should also capture the details of situations where Council information (e.g. paper file) or Council ICT devices that are not specifically designed for mobile use (e.g. Desktop PC) have been removed from Council premised by any person with permission from the relevant Information Asset Manager.

For third parties, such as contractors, any mobile and flexible working must be in accordance with contractual arrangements. It is the responsibility of Council staff to

ensure that these contracts require full compliance with this Policy and all other Council policies.

Any potential information risks associated with the location being used must be declared to the relevant Information Asset Manager at the earliest opportunity. One such risk would be sharing a working location with non-Council staff.

Particular attention must be paid to:

- the policy requirements for Clear Desk and Clear Screen (as set out in section 7.7) to ensure that information is not inadvertently disclosed through others being able to see information on paper and ICT equipment when out of the office.
- the requirements for secure disposal of Council information (as set out in section 7.6), which required that any paper held off site that requires secure disposal must be brought back for disposal using Council provided facilities.
- The requirements around the use of removable media (as set out in section 7.5), ensuring that only Council ICT is used to process Council information, information is not transferred to personal devices and Removable media is only used for the temporary storage and transportation of data.

7.12 Security Classification & Protective Marking

The Council has an agreed security classification scheme and this scheme must be used where a security classification is applied to Council information (this is known as protective marking). The Council security classification scheme is consistent with the government security classification scheme, supporting appropriate sharing of information.

Protective marking shall be used where appropriate to highlight information that is sensitive to support appropriate handling of that information by recipients of the information both within the Council and by partners.

8. Information Security Management Roles & Responsibilities

This section sets out the general and specific responsibilities for information security management, including reporting of information security incidents.

8.1 All Staff and any person working on behalf of the Council

Information Security is everybody's responsibility and is something that should be considered as part of normal everyday working practice. This policy and other policies in the Information Governance Policy Framework set out the information security requirements to be followed by staff at all levels, and further support is provided to staff through guidance and training where necessary.

All those working within a Council Building or handling Council Information anywhere must ensure that they observe the Clear Desk & Clear Screen Policy as set out in this Policy (section 7.7).

If a potential security issue or incident is identified then this must be reported by the individual or delegated nominee to the ICT Service Desk. This requirement is set out in the ICT Acceptable Use Policy, but this also applies equally to any security issue or incident that involves paper based information or physical security where this could impact on the security of Council Information Assets.

Any remote or mobile working that may involve information handling must be consistent with the requirements as set out in section 7.11 of this policy.

8.2 Managers and Supervisors

Security of information within a business unit or building zone is the responsibility of individual managers and staff who work within those areas.

Managers are responsible for information held within their area. This includes ensuring that the information is held securely, access controls are appropriate and maintaining an accurate and up-to-date a list of Information Assets in the Corporate Information Asset Register.

Managers must promptly report any building physical security issues to the Responsible Premises Officer. The RPO will work with appropriate staff to remove or reduce any information security risk. Managers must report any remaining risks, after risk reduction, through their management chain to their service management team to be considered as part of the Councils approach to risk management.

Managers and supervisors must ensure that all their staff have completed the Information Management online learning module and have understood their obligations under this Policy and other Information Governance Policies. Managers should support their staff in this regard by highlighting relevant parts of policies that apply to the roles being performed by a member of staff.

Managers and supervisors must ensure that their work area and that of their staff is adequately secured including the implementation of the Clear Screen and Clear Desk Policy as set out within this Policy (section 7.7).

8.3 Information Asset Owners & System Owners

An Information Asset Owner (IAO) is a senior manager (head of service or equivalent) who has been identified as being accountable for a Council Information Asset. A System Owner is a person who has been identified as being accountable for a Council ICT system. The Information Asset Owner is supported by an Information Asset Manager (IAM), who has responsibility for management of the information within that Information Asset.

An Information Asset is a collection of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. All Information Assets should be recorded in the Corporate Information Asset Register.

Each ICT system and the information held within it is also considered to be an Information Asset and is recorded as such in the Corporate Information Asset Register.

IAO and System Owners are responsible for ensuring that the security controls applied to their Information are appropriate and that it is held securely with access to the information being provided as appropriate.

IAO and System Owners must ensure that the information recorded in relation to their Information Asset in the Corporate Information Asset Register is correct and up-to-date.

Role descriptions and an accompanying online learning module for IAO and IAM have been developed and approved by IGB. These provide further explanation on the roles and all IAO / IAM must read the role description and undertake the online learning.

8.4 Senior Information Risk Owner (SIRO)

The SIRO is the senior manager responsible for management of information security risks and for reporting this to the Council's Executive Leadership Team. The SIRO role is performed by the ECO Performance & Governance.

The ECO Performance & Governance is the corporate strategic owner of Information Security as part of Information and Data Strategy.

8.5 Freedom of Information & Data Protection Manager

The FOI and DP Manager has operational strategic ownership of Council Information Assurance and Records Management on behalf of the ECO Performance and Governance.

The FOI and DP Manager is responsible for ensuring an operational records management service is in place. The Council Records Management Service is provided by High Life Highland under a service delivery agreement. This service includes the maintenance of the Corporate Information Asset Register, which contains information on the security classification and security controls of Information Assets.

8.6 Head of ICT & Digital Transformation

The Head of ICT & Digital Transformation is responsible for ensuring an operational security management function is in place. Information Security Incident Management

and Investigations are managed by ICT Services on behalf of the Head of ICT & Digital Transformation.

8.7 Data Protection Officer

The Data Protection Officer role is performed by the Freedom of Information & Data Protection Manager who is responsible for providing advice about compliance with the Data Protection legislation, for monitoring Privacy Impact Assessment and for reporting Data Protection Breaches to the Information Commissioners Office (ICO).

The Head of ICT & Digital Transformation is responsible for ensuring the Council's ISMS; Information Management and Security Policies, and Information Security Incident Reporting processes support the Council's compliance with the Data Protection legislation.

8.8 Responsible Premises Officer (RPO)

The RPO is responsible for the physical security of buildings through the effective management of perimeter security and zoning of buildings. Physical security of information within a business unit or building zone is the responsibility of the Information Asset Owners, individual managers and staff who work within those areas.

The RPO must respond promptly to any building physical security issues that are brought to their attention by any member of staff (or visitors) to remove or reduce any information security risk. Any remaining risk must be reported by the RPO to the relevant Information Asset Owners / Managers and Data Protection Officer. These managers must then report this through their management chain to their service management team to be considered as part of the Council's approach to risk management.

8.9 Internal Audit

The Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Information Security Policy, procedures, internal information security controls, their implementation and Corporate and Service compliance with these.

8.10 Information Management Lead Officer

The IM Lead Officer is a senior representative (head of service or equivalent) from each Council Service that represents their Service Director on the Information Governance Board (IGB) and provides a strategic lead for Information Governance and Information Security within each Service.

The IM Lead Officer will be required to attend the IGB meetings, communicate and cascade information within their Service and ensure adoption of working practices that are consistent with Information Governance Policy and Guidance.

IM Lead Officers will be supported in their role through information and guidance provided through the IGB. A Role description for the Information Management Lead Officer has been developed and approved by IGB.

9. Information Security Governance and Process

9.1 Information Governance Board (IGB)

The IGB has been created to oversee the delivery of the Council Information and Data Strategy and govern the implementation of this across the Council. An IM Lead Officer from each of the Services represents their Service's Executive Chief Officer (ECO) on the Board. Each ECO is required to identify a member of their senior management team to act as IM Lead Officer for their Service.

The IGB is chaired by the ECO Performance & Governance as the corporate owner of Information and Data Strategy and the Information Governance Policy Framework and as SIRO.

The primary role of the IGB is to identify priorities for the implementation of Information Governance improvements and the strategic initiatives identified in the Information and Data Strategy Implementation Plan.

The IGB has a duty to consider and make recommendations to the Executive Leadership Team about information governance issues and influence strategy and policy development. It also exists to support delivery of information governance improvements within services.

The IGB will review high level information security risks in support of the SIRO.

9.2 ICT Security Management

Operational ICT Security management is managed by ICT Services and will operate under Service management governance and the Head of ICT & Digital Transformation will report back to the IGB, identifying information risks that require consideration by the IGB. Any technical issues that are ICT Security risks or require ICT changes to manage the risk, will be referred to the appropriate board, following normal ICT Services service management governance.

9.3 Information Security Incident Reporting

Information Security Incidents or concerns about information security must be reported by staff through the ICT Service Desk.

The ICT Acceptable Use Policy sets out the Council's expectations on all ICT Users to report all security incident or concerns. This obligation also applies to any other

user of Council information or those working on behalf of the Council when this concerns paper based information.

9.4 Information Security Incident Management Procedure

The ICT Acceptable Use Policy sets out the monitoring that the Council may undertake of ICT usage. The Council may produce Potential Misuse Reports on the activity of a user or investigate any information security incident, regardless of whether the incident involves information held in ICT systems or on paper. The procedure is set out in more detail in the ICT Acceptable Use Policy.

10. Staff Communication & Training

This policy and other information governance policies are made available to staff through the Intranet and others within scope of the policies through the Council website.

Staff and any person handling Council Information are provided with an online learning module that provides an introduction to the expectations the Council places on those handling information. This includes the information security and data protection issues that staff should be aware of.

All staff must complete the Information Management online learning module and managers must ensure that this has been completed by their staff.

Any other person handling Council information must also complete this training and the relevant Information Asset Owners and the Council manager responsible for the contract, involving third party handling of information, must ensure this takes place.

Further information security online learning modules may be provided to staff and these must be completed where they are relevant to their role. Staff will be informed when they must complete these additional training modules.

11. Review

This policy will be reviewed on a regular basis and adapted appropriately to ensure that it continues to meet the business and service delivery requirements of the Highland Council.