Information Security Policy

Contents

1. Introduction 2
2. Purpose....2
3. Governance and responsibility for information security....3
4. Risk Management 4
5. Asset Management and Classification....4
6. Human resources security....4
6.1 Culture, education and awareness 5
7. Access control....5
8. Physical and environmental security 5
9. Communications and operations management....5
10. Information systems acquisition, development and maintenance 6
11. Information security incident management 7
12. Business continuity management....7
13. Compliance 7
14. Further Information....7

Version Control

Version	Description	Release Date	Issued By
1.0	Final Version	April 2009	Information Security Officer
2.0	Annual Review. Addition of version control, amendment to Introduction and Purpose and renumbering.	July 2011	Information Security Officer
3.0	Annual Review. Amendment to section 5 to reflect changes in information asset management & classification. Added Appendix for documents published or under draft	July 2012	Information Security Officer
4.0	Annual Review. Updated Appendix 1 to reflect current status of Information Security Policies.	September 2014	Information Security Officer
4.1	Minor revision to update Information Security contact details and to adjust terminology in line with GDPR.	May 2018	Information Security and Digital Risk Officer Chief Officer - Legal & Procurement
5.0	Included reference to Charter, Statement of Intent and DPIA's, incorporated links, included explanation of terms, added section 6.1 and 12.2. Removed Appendix 1.	October 2018	Information Security and Digital Risk Officer
6.0	Included reference to departmental responsibility for 3rd party security policy compliance (refer to point 3.2), included reference to data team (refer to point 3.5)	October 2020	Information Security and Digital Risk Officer
7.0	Updated links for Data Sharing and DPIA information in line with changes by DPO (refer to point 10.4)	September 2021	Information Security and Digital Risk Officer

1. Introduction

1.1 Information plays a critical role in the lives of East Renfrewshire Council customers, employees, and business; as a result information systems and physical assets, including supporting processes, systems, networks and equipment, need to be appropriately protected to ensure that the Council can continue to operate and provide its service delivery.

1.2 Information Security efforts do not solely focus on the protection and maintenance of IT systems which process and store information, the information itself is of primary importance, regardless of how it is handled, processed, shared, transported, stored or destroyed, including:

- Physical access to electronic and paper-based information assets: by implementing the use of physical barriers such as visitor management, secure building and office access, staff and visitor ID badges, lighting, motion detectors, CCTV, alarms, locked cabinets, locking away electronic data storage devices such as USB keys and laptops, locking computer screens, protecting computing equipment and devices etc.
- Logical access to data, systems, applications and databases: by implementing logical controls such as user credentials and profiles, managing starters, leavers and movers, applying effective passwords/passphrases, controlling remote access to systems, maintaining audit logs, applying time-of-day or geographical restrictions, providing least privilege to undertake job functions etc.
- System hardening and technical controls to ensure networks, devices, peripherals, systems, databases and applications are configured to reduce security risk by eliminating potential attack vectors.
- External and internal access to the network and all other computing resources.
- Legislation impacting information and IT systems in all Council locations, business units, and teams
- Compliance requirements and standards set out by the Government, partners, and regulatory bodies.
- Council, partner, and customer privacy rights, regulations, and laws.
- Contractual obligations where a 3rd party holds or processes information on the Council's behalf

1.3 Information Security therefore, addresses the universe of risks, benefits, processes involved with information, and takes account of business needs for sharing or restricting information and the business impacts associated with such needs. Information security is assisted by the implementation of an appropriate set of controls comprising policies, standards, procedures, guidance, structures and technology configurations.

1.4 The Council's 'Charter for Protecting Information' and 'Information Security Statement of Intent' state the Council's position and support of the Information Security Policy.

2. Purpose

2.1 The purpose of Information Security is to protect the information of East Renfrewshire Council, our customers, and our employees through the implementation of appropriate policies, standards, processes, and technology.

2.2 This Information Security Policy provides the strategic position and sets out the foundations and a framework for appropriate, cost effective, and efficient information security as a fundamental aspect of corporate governance.

2.3 This policy applies to all aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store, process, transmit or receive information.

2.4 The key objectives of this Information Security Policy are to:

- Provide the framework for sub-policies, guidance and standards relevant to information security
- Assist East Renfrewshire Council employees in protecting the confidentiality, integrity, and availability of Council information.
- Ensure that all information, particularly personal and customer information, is treated appropriately at all times.
- Promote compliance with all relevant legislation and regulations regarding Council information assets.
- To enable East Renfrewshire Council to maximise the benefits of the information it holds through making the best use of information and information sharing whilst managing the risks and being cognisant of the information security requirements.

3. Governance and responsibility for information security

3.1 The Council will ensure that suitable frameworks exist to initiate and control the implementation of information security both within the Council and between itself and external organisations.

3.2 All staff and individuals with access to Council information must appreciate that they have an individual responsibility to ensure that information is handled appropriately. As well as employees, Elected Members and 3rd parties who access council information, all departments will be expected to adhere to the requirements of this policy in the way that they work and ensure compliance of any 3rd party they engage with the Supplier Information and Cyber Security Policy.

3.3 The Chief Executive, as Senior Information Risk Owner (SIRO) has overall responsibility for ensuring implementation of this policy and is assisted in fulfilling this role by Directors and Heads of Service.

3.4 Additionally, a number of individuals have direct responsibility and are required to apply this policy as part of their remit. These include:

- Managers;
- Information Security and Digital Risk Officer;
- Data Protection Officer;
- IT support and project staff;
- System administrators;
- Information Security Forum.

3.5 Departments must nominate one or more senior officers to represent them at Information Security Forum meetings. Permanent members of the Forum include subject matter experts from IT, Human Resources, Data Team and Audit.

3.6 The Forum meets at least twice a year to review security within Departments. Special meetings may be held to examine a specific security issue problem.

 Refer to Information Security Forum information

4. Risk Management

4.1 Assessing information risk is required for the protection of information assets throughout their lifecycle. The Information Risk Management Policy defines the baseline standards to:

a. Manage the threat of a compromise of confidentiality, integrity or availability of information held on systems or manual records and a strategy to address that threat or reduce the impact;

b. Manage compliance with Data Protection obligations in use of personal data;

c. Manage the risk of removal of information from controlled environments, sharing of data from a Council repository or exchanges of data with third parties;

d. Ensure changes of existing services or facilities or introduction of new ones are only carried out on completion of a risk assessment;

e. Ensure an Information Security Risk Register is maintained.

5. Asset Management and Classification

5.1 Appropriate measures are in place to ensure the protection of information assets and information processing. Each Department is responsible for maintaining their information asset entries within the Council's Information Asset Register. This contains an inventory of information assets and identifies a range of details including the name of the information asset owner, classification level, where the assets are stored and who they are shared with.

5.2 The Information Handling Procedures and Classification Procedures cover how information assets are used and stored in different scenarios and throughout their lifecycle.

5.3 Managers will ensure that all information used by their staff, is allocated a classification level (also known as Protective Marking) where required to identify the requirement for protection. The Information Classification Procedure and Guidelines assist managers in judging what information requires to be marked, how to reach this decision and what security is required.

 Refer to Information Management and Classification information

6. Human resources security

Departments must ensure that:

a. Employment and personnel security policies are complied with during all stages of the employment process, ensuring that appropriate checks and controls (e.g. PVG – Protecting Vulnerable Groups) are in place before access to information assets is permitted. This includes the recruitment, employment, change of role and termination of staff and third parties.

 Refer to Recruitment and Selection Procedures

6.1 Culture, education and awareness

Fostering a professional culture and developing a positive attitude toward security is critical. Security must be seen as an integral part of and a key enabler to, effective departmental business. The Council undertakes to provide appropriate information security training for staff, Elected Members and third parties as appropriate.

Departments must ensure that:

a. Appropriate information assurance education and awareness is provided to all staff on Service induction, and that staff receive training appropriate to their role and access to information.

b. All staff with access to information undertake information security training provided within MyInsider.

c. Appropriate information security education and awareness is provided to staff when undertaking a new post or role within the Council.

d. All staff understand their obligations to both protect special category information (e.g. in line with data protection principles) and business sensitive information and ensure openness and transparency in decision-making (e.g. in response to freedom of information requests or by proactively publishing non-sensitive datasets on the Council's open data portal).

e. All users of ICT are familiar with the security operating procedures governing their use, receive appropriate training, and are aware of processes for reporting issues of security concern.

f. Staff that have privileged access to key Council assets (e.g. system administrators) should be given enhanced training about their responsibilities and be aware that inappropriate behaviours may lead to disciplinary or criminal proceedings.

7. Access control

Appropriate measures exist or will be put in place to limit access to information, information processing facilities and business processes to appropriate persons or groups of persons. This includes physical and IT system access control procedures to address, where appropriate, the need for user access management policies, password controls, network access controls, operating system access controls, application access controls, and access security issues pertaining to the uptake of mobile computing and teleworking.

Where access is being provided across the Public Internet additional security will be applied such as 2FA/MFA to assure the identity of the user requesting access.

8. Physical and environmental security

Appropriate measures exist or will be put in place to prevent unauthorised access, loss, theft, damage and interference to the Council's premises and information assets. This will include addressing the physical security needs of buildings, offices, equipment, and supporting utilities and infrastructure.

9. Communications and operations management

Appropriate measures exist or will be put in place to ensure the correct and secure operation of processing facilities, including:

- Media handling;
- Operational procedures and responsibilities;
- Third party service delivery management;
- Change control;

- Protection against malicious software;
- General housekeeping duties;
- Network management;
- Exchanges of information and software;
- Sharing of information from the source repository within Council systems;
- Disposal and decommissioning.

 Refer to Acceptable use Policy Framework

10. Information systems procurement, development and maintenance

10.1 East Renfrewshire Council recognises the need to ensure that security is built into new and proposed IT systems, and is assessed as part of the normal system lifecycle. To properly address the security requirements of new systems appropriate steps must be taken to ensure that new applications correctly process information, any necessary cryptographic controls are implemented, the security of system and software application files is considered, security in development and support processes is properly managed, and that consideration is given to patch and vulnerability management.

All procurement exercises must take cognisance of information security requirements by including the Information Security Schedule into procurement exercises and by engaging with the Information Security Officer where a supplier indicates any non-compliance.

 Information Security Schedule

 Refer to Procurement Guidance

10.2 Departments will comply with the requirement for the Council to undertake continual software patching and security updates across the computing, networking and application estate. Managers will ensure compliance throughout their respective areas and assist IT Services in ensuring users comply.

10.3 The Council will ensure network connected devices are regularly scanned for vulnerabilities / device configuration changes.

10.4 Where Departments have procured applications or systems they must ensure that software updates and patching are maintained and kept up to date. All software and applications must be supported and not utilise any components classed as out of date software.

10.5 Departments will further comply with the requirement to assess potential privacy risk and impact from the collection, use, sharing and disclosure of personal data in line with the Councils Data Protection Policy and Data Protection Impact Assessment procedures.

 Refer to Data Sharing Guidance

 Data Protection Impact Assessment procedures

11. Information security incident management

Information security events and weaknesses associated with information systems will be communicated direct to the Information Security and Digital Risk Officer in a manner allowing timely corrective action to be taken, the background fully investigated and appropriate solutions put in place to reduce the potential of a recurrence.

 Report a data breach

 Report lost/stolen equipment

12. Business continuity management

12.1 Measures exist to counteract interruptions to business activities, to protect critical business processes from the effects of major failures or disasters and maintain core services. Departments must ensure they retain up to date Business Continuity Plans to plan for any interruption in IT service delivery.

12.2 Departments will ensure that Business Continuity Plans take cognisance of the requirement to appropriately protect information during business interruptions.

13. Compliance

Appropriate measures exist or will be put in place to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. Relevant legislation includes:

a. Data Protection Act 2018
b. General Data Protection Regulation
c. Freedom of Information (Scotland) Act 2002
d. Copyright, Designs and Patents Act 1988
e. Computer Misuse Act 1990
f. The Privacy and Electronic Communications Regulations 2003
g. Regulation of Investigatory Powers (Scotland) Act 2000
h. Anti-Terrorism, Crime & Security Act 2001
i. Defamation Act 1996
j. Health and Safety at Work Act 1994 (Computers)
k. Re-use of Public Sector Information Regulations 2015
l. Civil Contingencies Act 2004
m. and any other relevant legislation as may be enacted from time to time.

14. Further Information

Information Security policies and standards are available on the East Renfrewshire Council Intranet. For further advice, contact Cathie Fraser, Information Security and Digital Risk Officer on 0141 577 3644 or cathie.fraser@eastrenfrewshire.gov.uk