Falkirk Council

INFORMATION SECURITY POLICY

Date: 14/04/2019

Contents

1. Definition of Information Security

Information security is the protection of information (in any form including hand-written, typed, video, paper based or electronic) from a wide variety of threats. The purpose of this is to minimise business risk, ensure business continuity, support information sharing, achieve organisational objectives, develop business opportunities and protect information relating to people.

2. Aim of the Policy

The purpose of this policy is to ensure:

- **Confidentiality of information:** making sure that information is accessible only to those authorised to have access.
- **Integrity of information:** safeguarding the accuracy and completeness of information and data processing methods.
- **Availability of information:** making sure that authorised users have access to information and assets when required.
- **Protection of people:** making sure personal information is safe.
- **Regulatory compliance:** making sure that the Council meets its regulatory and legislative obligations. See Appendices 1 and 2.

3. Policy Scope

This policy concerns information in all forms printed, handwritten or verbal; stored on paper or stored electronically; transmitted by post, fax or transmitted electronically, carried on paper or on PCs, laptops, tablets, smartphones, blackberries, or USB devices.

This policy applies to all employees and elected members whether working in Council premises, working at home, or when mobile working. It also applies to employees of external organisations who use, or access, the Council's Information and Communications Technology (**ICT**).

4. Policy Statement

Information security is an essential enabler in helping the Council meet its objectives. Security risks must be managed effectively, collectively and proportionately to achieve a secure and assured working environment. The Council's processes and procedures must reflect the principles, governance and responsibilities set out below.

5. Principles

Data must have an appropriate level of protection applied at all times.

5.1 Much of the information handled by the Council relates directly to individuals and it is important their information is protected from loss or theft either accidentally or deliberately.

A risk based approach must be adopted.

5.2 It is important that controls are applied in a proportionate way so that information is protected in a way which does not hamper business process and costs/benefits are optimised.

Information security must be a priority in all partnerships.

5.3 Good security is crucial to building trust with partners and those with whom we share information. All data sharing initiatives should consider security at the outset and, where personal data is involved, take a *data protection by privacy and design* approach. This will include the use of data protection impact assessments at the outset of initiatives where there is a high risk to the privacy of individuals. All data sharing will be governed by formal written agreements.

Ownership, and access to information and rights to it, must be clearly defined, controlled and reviewed through formal processes.

5.4 Owners of information must carry out regular reviews of user access rights and in particular must withdraw rights promptly when staff leave or change roles. A hierarchy of information ownership should be created in the event that information owners leave or change roles so that continuity of information ownership is maintained.

Plan for the unexpected.

5.5 Regardless of vigilance, vulnerabilities will be found, new attacks will take place and the surprising will happen. Processes must be flexible enough to cope with the unexpected. Security defences must be layered so as to provide cover should one layer fail and risks from single points of failure must be managed. Business continuity plans must be prepared and tested where appropriate.

Security by design for the whole lifecycle.

5.6 Security should be built in from the start, not bolted on later, to avoid expensive redesign or vulnerabilities. All initiatives must consider security at the outset and, where personal data is involved, take a *data protection by privacy and design* approach, including the use of data protection impact assessments at the outset where there is a high risk to the privacy of individuals. During the operational life of an asset, processes and procedures should be maintained, resources monitored, future capacity needs planned for and changes strictly controlled. At the end of an asset's life it should be disposed of carefully as insecure disposal can expose confidential information.

All employees and elected members are accountable for their actions.

5.7 Information security responsibilities must be clearly defined and communicated. Training provision should be in accordance with corporate arrangements. All user access accounts must be identifiable with an individual. Segregation of duties is an important information security control mechanism that should be used where appropriate. Individuals must act in accordance with this policy, and the other policies listed in Appendix 3. Failure to do so may result in disciplinary action. All breaches of these policies will be fully investigated.

6. Governance and Responsibilities

In order to ensure security of information, the following governance arrangements are required within the Council to make sure the organisation meets its business aims and objectives.

6.1 **The Corporate Management Team (CMT)** recognises the importance of information security to the organisation and directs the Council's strategy, setting the overall direction and making sure resources for implementation.

6.2 The Director of Corporate and Housing Services is the Council's **Senior Information Risk Owner (SIRO)** and has lead responsibility to ensure that organisational information risk is properly identified and managed in the Council and that appropriate assurance mechanisms exist. The Council's Financial Regulations provide that the Director of Corporate and Housing Services is responsible for the issue of this policy. Also, in terms of the Financial Regulations, the Director, in consultation with the Chief Governance Officer, is responsible for ensuring that proper privacy and security is maintained in respect of information held on manual or computer records, and that the requirements of relevant legislation are complied with.

6.3 **The Information Management Working Group (IMWG)** is chaired by the Chief Governance Officer and seeks to (i) promote the effective management of all Council information in all formats throughout its lifecycle, to meet operational, legal and evidential requirements, (ii) support the Council in identifying and managing its information needs, risks and responsibilities, and (iii) ensure an information risk management policy and framework is in place and overseen.

6.4 **The IT Security Group** is chaired by the Head of Policy Technology and Improvement and has the following responsibilities - (i) in conjunction with the IMWG, the promotion of Information Security throughout the Council, (ii) the review and recommendation for the approval of all IT-security related policies and procedures, (iii) compliance and certification through external assurance schemes such as PSN and Cyber Essentials, (iv) review and monitoring of IT security incidents, their cause, resolution and future prevention, and (v) providing technical input to the DPIA assurance process.

6.5 **The Head of Performance, Technology and Improvement** has overall responsibility for the security of the Council's corporate technology systems and network.

6.6 **The Data Protection Officer** is responsible for monitoring the Council's compliance with data protection legislation and with its policies in relation to the protection of personal data.

6.7 **The Corporate Risk Management Group (CRMG)** is chaired by the Head of HR and Business Transformation (who is also a member of CMT). The CRMG receives regular reports on information asset and cyber security risk management and makes sure that appropriate control objectives and key controls are established to address any weaknesses identified.

6.8 **Information Asset Owners (IAOs)** are identified as Directors or Heads of Service at a service area level and will be accountable for ensuring that the risks in relation to the assets are identified and managed according to the appropriate level of security. This includes user access management. IAOs must also clearly define data retention and disposal requirements.

6.9 **Internal Audit** will regularly review information security matters through its audit programme. This will serve to inform the risk management approach and promote continuous improvement of policy.

6.10 **All staff and elected members** are responsible for protecting information in accordance with this policy.

7. Information Security Incidents

An information security incident is an event that has, or could have, resulted in loss or damage to information, or an event which is breach of this policy. This includes but is not limited to:

- The loss of an unencrypted memory stick
- Theft or loss of data held in electronic format
- A break-in to Council premises
- Paper files going missing
- Disclosure of confidential information
- Unauthorised access to a system
- Unauthorised use of information
- Cyber attack

Information security incidents must be reported as set out in the Information Security Incident Reporting Procedure.

8. Review of Policy

This policy will be reviewed every 3 years or sooner if required by changes to legislation, technology or Council policy.

The SIRO will be responsible for ensuring the review of this policy.

APPENDIX ONE

Legislation

Information security is managed in accordance with the following legislation.

The Copyright, Designs and Patents Act 1988	UK copyright law which gives creators of literary, dramatic, musical and artistic works the right to control how their material may be used.
The Computer Misuse Act 1990	This was created to criminalise unauthorised access to computer systems and to deter the more serious criminals from using a computer or the data it stores by inducing a computer to perform any function with intent to secure access. The act has been modified by the Police and Justice Act 2006.
Data Protection Legislation as defined by the Data Protection Act 2018	The main piece of legislation that governs protection of personal data in the UK. It provides a way that individuals can enforce the control of information about themselves.
Human Rights Act 1998	This act governs interception or monitoring of communications, especially article 8 which guarantees respect for an individual's private and family life, their home and correspondence. Public authorities can not interfere with these rights unless it's justifiable to do so.
Regulation of Investigatory Powers Act 2000 and Regulation of Investigatory Powers (Scotland) Act 2000	Aims to make sure that various investigatory powers available to public bodies are only exercised in accordance with the Human Rights Act 1998. The act legislates for using methods of surveillance and information gathering to help the prevention of crime and terrorism.
Electronic Communications Act 2000	Gives legal recognition for electronic signatures and makes it simpler to amend existing legislation that could hamper the development of internet services.

Telecommunications Act 2003	Governs fraudulent and improper use of telecommunications equipment

Freedom Of Information (Scotland) Act 2002	Provides the right of access to recorded information of any age held by public sector bodies in Scotland. There is a duty on all local authorities to adopt and maintain a publication scheme approved by the Scottish Information Commissioner.
The Privacy and Electronic Communication (EC Directive) Regulations 2003	Replacing the Telecommunications (Data Protection and Privacy) regulations 1999 and amendments 2000, these cover issues relating to privacy of electronic communications including telemarketing and cookies.
Public Records (Scotland) Act 2011	The council must prepare a records management plan setting out arrangements for the management of the authority's public records.

APPENDIX TWO

Standards

Information security is managed in accordance with the following standards.

STANDARD	DEFINITION
Information Technology Infrastructure Library (ITIL)	A set of concepts and techniques for managing information technology, infrastructure, development and operations.
ISO/IEC 27001 and 27002	International standards for information security management.
National Information Assurance (IA) Strategy (2007)	This outlines an approach for the UK in adopting information risk management by making sure the correct level of professionalism, education and training; availability of IA products and services as well as compliance and adoption of standards.

Payment Card Industry Data Security Standards (PCI DSS)	Standard developed by major credit card companies as a guideline to help organisations that process card payments to prevent fraud and other security vulnerabilities and threats.
Public Services Network (PSN) Code of Connection	The PSN is a private wide area network across which secure interactions between connected organisations can occur (previously known as GSX).
Security Policy Framework (SPF)	The SPF describes the principles and approaches that central government have established to protect its assets, whether they be people, infrastructure or information and at the same time assist in the delivery of public services. The SPF applies to all organisations associated with the delivery of public services.
Scottish Government (SG) Cyber Security Action Plan	The action plan, developed in partnership by the SG and the National Cyber Resilience Leaders Board (NCRLB), sets out the action the SG intends to take in order to make progress towards the 3rd outcome of the Cyber Resilience Strategy, "We have confidence in, and trust, our digital public services."
Cyber Essentials Accreditation	Accreditation against a set of basic technical controls to help organisations protect themselves against common online security threats.

APPENDIX THREE

Supporting Documents

To make sure the objectives of this policy are met all staff must comply with the following guidelines. Senior management must ensure the material is understood and adherence appropriately monitored.

- Acceptable Use Policy (including Email Guidelines and Social Media Guidelines)
- Corporate Information Security Guidelines
- Data Protection and Confidentiality Guidelines
- Information Security Incident Reporting Procedure
- Data security breach management procedure
- Mobile flexible working guidance
- Code of Conduct for Employees

Version	Purpose/change	Author	Date
1.0	Approved by Executive	Murat Dilek	06.03.2020