Information Security Policy

Implementation date: 04 October 2016

Control schedule

Approved by	Corporate Policy and Strategy Committee
Approval date	04 October 2016
Senior Responsible Officer	Neil Dumbleton, Enterprise Architect Kevin Wilbraham, Information Governance Manager
Author	Henry Sullivan, Information Asset Manager Sarah Hughes-Jones, Information Compliance Manager
Scheduled for review	October 2017

Version control

Version	Date	Author	Comment
0.1	07-07-2016	Henry Sullivan Sarah Hughes-Jones	Initial draft created and circulated for comment
0.2	29-07-2016	Kevin Wilbraham Henry Sullivan	Revisions made and incorporated
0.3	04-08-2016	Kevin Wilbraham Sarah Hughes-Jones	Further revisions made and incorporated
0.4	22-08-2016	Kevin Wilbraham	Consultation version circulated
0.5	24-08-2016	Henry Sullivan	Revisions in light of ICT Solutions consultation
0.6	03-09-2016	Henry Sullivan	Draft versions agreed with Head of Strategy (Interim)
1.0	04-10-2016	Kevin Wilbraham	Agreed by CP&S

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30-09-2014	Corporate Policy & Strategy	Information Governance Policies	Minute
04-10-2016	Corporate Policy & Strategy	Information Governance Policies	Minute

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Information Security Policy

Policy statement

1.1 The Council has statutory responsibilities to make sure that the data and information it creates or receives is kept safe and used appropriately.

1.2 The Council depends on the confidentiality, integrity and availability of its information to such an extent that a serious breach of information security could impact on the Council's ability to deliver a wide range of statutory services.

1.3 The Council also has contractual obligations to ensure sound security if it is to use the Government's Public Services Network (PSN); meet Payment Card Industry Data Security Standards (PCI DSS), or receive or share information with partner agencies under information sharing arrangements.

1.4 In setting out the Council's information security arrangements, this policy confirms the Council's commitment to its citizens, visitors, employees and business partners that Council information and data will be properly protected, valued and secured.

1.5 The Council's information security arrangements are based on the provisions of the ISO/IEC 27000 series (the industry standard for information security) and the development and maintenance of an Information Security Management System (ISMS), consisting of this policy and associated standards and protocols.

1.6 The Council requires that its Directorates, Localities, staff and partners operate and deliver its services in compliance with the ISMS and associated standards.

1.7 Failure to comply with this policy may result in sanctions up to and including dismissal or contract termination, as well as the possible involvement of law enforcement and relevant external regulators.

Scope

2.1 This policy and related protocols, procedures and guidance under the Council's ISMS applies to:

2.1.1 All data and information created, received and managed in the course of Council business.

2.1.1 All permanent and temporary Council employees, volunteers, people on work placements and elected members when acting as officers of the Council

2.1.1 All third parties, contractors and suppliers accessing or handling Council information, equipment, network or systems.

Definitions

3.1 **BS ISO/IEC 27001:2013:** This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation, such as the Council.

3.2 **Data:** the raw input from which information of value is derived.

3.3 **Information** means any information recorded in any form.

3.4 **Information asset:** a body of information defined and managed as a single unit or aggregate so it can be understood, shared, protected and exploited effectively.

3.5 **Information asset owners:** Heads of Service involved in managing a business area(s) with responsibility for the information assets within their respective business area(s).

3.6 **The Information Council (IC)**: has delegated responsibility, through the SIRO and the Council Leadership Team, for the development and delivery of effective information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure information governance compliance.

3.7 **Information security**: ensures that Council information is not compromised by unauthorised access, modification, disclosure or loss.

3.8 **Information Security Management System**: preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to internal and external stakeholders that risks are adequately managed.

3.9 **Information sharing**: ensures that Council information is shared in a compliant, controlled and transparent manner.

3.10 **Organisational controls**: are measures that instruct and define responsibilities and expected behaviours and practices in terms of information security (e.g. policies, procedures, guidance)

3.11 **Privacy impact assessment**: a risk management method that reduces the risks of harm to individuals through the misuse of their personal information, and can help with the design of processes for handling personal data. It is used when projects, or changed service activities, or new ICT impact on the privacy of individuals.

3.12 **Security impact assessment**: ensures that necessary security controls are integrated into the design and implementation of a project.

3.13 **Senior Information Risk Owner**: the Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation.

3.14 **Technical controls**: are measures that limit and define access and action via network and system configuration in terms of information security (e.g. account management, back up cycles, encryption and firewalls)

Policy content

Strategic approach

4.1 The Council's strategic approach to information security is based on:

4.1.1 The continued development and implementation of an information security strand within the Council's Information Governance Framework.

4.1.2 The alignment of all elements of information security with ISO 27000 (Information Security Management), which is the industry standard for information security and HMG Security Policy Framework

4.1.3 A documented Information Security Management System (ISMS) which details the Council's information security management arrangements and the application of control measures in detail.

4.1.4 The regular review of the ISMS to identify improvements, and to ensure on-going maintenance and implementation of the system.

4.1.5 The continuing availability of specialist information governance/security advice to support the implementation process for information security, and the other areas within the Information Governance Framework.

4.2 In line with the requirements of the Data Protection Act of 1998, the Council has both organisational and technical measures to secure its information. The development, implementation and assurance of these measures are divided between ICT Solutions (Technical) and the Information Governance Unit (Organisational).

Organisation of the Information Security Management System

4.3 The Council's information security management system will consist of protocols, procedures and guidance, all underpinned by this policy.

4.4 This management system will conform to the ISO 27001 standard and will cover the following areas of control:

4.4.1 Human Resources Security and Supplier Management

4.4.2 Information Asset Management

4.4.3 Access Management

4.4.4 Cryptography

4.4.5 Physical and Environmental Security

4.4.6 Business & ICT Operations Security

4.4.7 Protective Marking and Information Handling

4.4.8 Mobile Devices and Removable Media Management

4.4.9 Business Continuity Management

4.5 Each area of control within the management system will have a protocol that outlines compliance requirements. Protocols will be supported by procedures and additional guidance.

4.6 The Council requires that its Directorates, Localities, staff and partners operate and deliver its services in compliance with these standards.

4.7 The Head of ICT Solutions and the Head of Strategy and Insight are the owners of this management system and are responsible for its implementation, maintenance and performance.

4.8 Change control and oversight of process and documentation within the management system will be the responsibility of the Information Council and supported by the Information Governance Unit and ICT Solutions.

4.8.1 Final versions of all documentation of the management system will be maintained by the Information Governance Unit.

4.9 Delivery of the information security management system will be carried out in partnership between the Council and its ICT Provider, CGI Ltd.

4.9.1 The relevant ICT roles and responsibilities and management structure within CGI have been identified in the Security Management Plan arising from Schedule 2.4 of the Council's IT Procurement Contract.

Monitoring of the Information Security Management System

4.10 The Information Council will routinely review the management system's performance to ensure that it meets the Council's statutory and business requirements and its overall strategic objectives.

4.11 The management system will also be reviewed in response to significant incidents or changes to legislation or regulation.

4.12 To support this, the management system will be monitored for effectiveness and non-compliance by an Information Security subgroup of the Information Council made up of the following Council service areas:

4.12.1 ICT Solutions

4.12.2 Information Governance Unit

4.12.3 Facilities Management

4.12.4 Human Resources

4.13 This group will produce reports for the Information Council and SIRO (as appropriate), including:

4.13.1 An annual report detailing the system's effectiveness, resourcing, changes and risks

4.13.2 Quarterly reports detailing security incidents

Communicating the Information Security Management System

4.14 The management system will be broadly communicated to staff and partners through the Council's annual information governance communications plan.

4.15 Communications around specific incidents or threats will be managed by ICT Solutions and CGI (IT incidents and threats) and the Information Governance Unit (organisational incidents and threats), with coordination from the information security subgroup and assistance from Council's Communications service as required.

Risk assessment & management process

4.16 Information security will be risk assessed, documented, managed and mitigated within the Council's wider Risk Management Framework, with regular reporting to the relevant Council risk committees.

4.17 ICT Solutions and the Information Governance Unit will monitor and support managers in identifying, evaluating and mitigating information security risks.

4.18 They will also undertake periodic audits and risk assessments in their own right, reporting to managers and information asset owners as appropriate.

4.19 Identified information security risks can be escalated to the SIRO and be reviewed and managed through the IC if required by the SIRO.

Incident management

4.20 Information security breaches must be reported via the Council's Information Security Incident Management Procedure as soon as possible by the individuals who have caused or discovered the breach.

4.21 While it is appropriate for staff to initially report an incident to their manager where they are available, this must then be reported according to the Information Security Incident Management Procedure as quickly as possible.

4.22 While individual incidents will be handled by the most relevant Council service area, the Information Security subgroup will coordinate and monitor all Council information security breaches.

Information Security in Project Management

4.23 Council projects that involve the handling and sharing of information are covered under the Council's information security arrangements.

4.24 These projects will require a Security Impact Assessment to be undertaken by the relevant project manager or officer with the support of ICT Solutions and the Information Governance Unit, as appropriate.

4.25 Council projects that impact on the privacy of individuals will also require a privacy impact assessment to identify and document appropriate governance controls required to manage the privacy risks associated with new or changed processes that involve personal data.

Training

4.26 This policy and associated protocols will underpin all information security training, both mandatory and refresher training. Training will be supported by further detailed guidance on the Council's intranet.

Implementation

5.1 Implementation of this policy will be undertaken through the continued development, roll out and maintenance of a Council-wide information security management system.

5.2 The information security management system will itself be implemented and continuously improved by the member service areas of the Information Security subgroup through the information security work stream of the Information Council's annual plan.

5.3 Progress and performance will be monitored by the Information Council and reported to the SIRO as appropriate.

5.4 The protocols and guidance of the management system will need to be implemented by managers into business processes and other local documentation. The Information Security Team and Information Governance Unit will support this process, as required.

Roles and responsibilities

6.1 The Information Governance Policy provides a detailed explanation concerning overall roles and responsibilities around information governance. This section provides a summary of those responsibilities, but also outlines specific responsibilities in relation to compliance with the Council's Information Security Management System.

Council Leadership Team

6.2 The Council Leadership Team has overall responsibility for Information Governance. This involves providing high-level support to ensure that directorates and localities apply relevant information governance policies and

controls, including compliance with the Council's Information Security Management System.

Senior Information Risk Owner

6.3 The Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation, including technical and organisational risks around information security.

Deputy Senior Information Risk Owner

6.4 The Information Governance Manager deputises for the SIRO as required and ensures that the Information Governance Framework is compliant with the Council's overall approach to corporate governance.

Information Asset Owners

6.5 Heads of Service are nominated information asset owners with overall responsibility for identifying and addressing any information risks relating to the information assets within their areas, including technical and organisational risks around information security.

Information Council

6.6 The Information Council has delegated responsibility, through the SIRO and the Council Leadership Team, for the development and delivery of effective information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure compliance with the Council's Information Security Management System.

ICT Security Manager - CEC

6.7 The Council's ICT Security Manager is part of ICT Solutions and is the operational lead on technical IT risks and is responsible for overseeing and implementing appropriate controls, in line with best practice, compliance frameworks and this policy. The Information Security service works closely with the Information Governance Unit and the ICT partner to ensure that information governance policies, standards, rules and assurance are applied and assured.

ICT Security Manager - CGI

6.8 CGI's IT Security Manager provide an independent view of IT security across the City of Edinburgh Council ICT Transformation Environment and co-ordinates operational security activities across the various CGI provided programmes and

services in accordance with Information Security Management System and associated plans.

Information Compliance Manager

6.9 The Council's Information Compliance Manager is the operational lead on organisational risks around information security. They are responsible for:

6.9.1 Coordinating and implementing appropriate organisational controls and measures, in line with best practice, compliance frameworks and this policy, and in conjunction with Facilities Management, ICT Solutions and Human Resources.

6.9.2 Assessing and reporting on those controls in line with the Council's Information Security Management System.

6.9.3 Receiving and managing relevant breach and incident reporting and ensure remedial actions have been undertaken and completed, in conjunction with ICT Security.

Facilities Management

6.10 Facilities Management will undertake the routine operation of physical security controls within the Council's estate.

Human Resources

6.11 Human Resources will monitor and provide assurance on organisational security controls in relation to staffing issues.

Managers and supervisors

6.12 Managers and supervisors have a number of responsibilities in relation to information security, and information governance more generally. These are set out in the protocols that form part of the Council's Information Security Management System and the Council's Information Governance Framework. These must be followed at all times.

6.13 In particular, managers and supervisors are responsible for ensuring that all permanent and temporary staff, contractors, partners, suppliers and customers of the Council who have access to Council Information Systems, or information used for council purposes have read and understood this policy (including associated protocols and guidance), and undertaken mandatory training in information governance and information security.

All staff

6.14 Information security is the responsibility of all staff. Individuals must ensure that they have read and understood this policy (including associated protocols and

guidance), and undertaken mandatory training in information governance and information security.

Related documents

Council Policy

7.1 Archives Policy

7.2 Data Quality Policy

7.3 ICT Acceptable Use Policy

7.4 Information Governance Policy

7.5 Information Rights Policy

7.6 Managing Personal Data Policy

7.7 Records Management Policy

Codes, Guidance, Procedures and Strategy

7.8 Employee Code of Conduct

7.9 In addition to the above there will be a suite of protocols, procedures and guidance on information security developed and published as part of the Council's Information Security Management System

Legislation

7.10 Computer Misuse Act, 1990

Standards

7.11 *ISO/IEC 27000 series – Information technology — Security techniques — Information security management systems*

Equalities impact

8.1 There are no equalities issues arising from this policy.

Sustainability impact

9.1 There are no sustainability issues arising from this policy.

Risk assessment

10.1 The principles of information security are underpinned by legislation, and the consequences of a serious breach of information security are severe.

10.2 The risks of not implementing this policy include:

10.2.1 Distress or harm to individuals or organisations.

10.2.2 Reputational damage to the Council.

10.2.3 Financial loss or monetary penalty imposed.

10.2.4 Detrimental impact on Council business and service delivery.

10.2.5 Non-compliance with legislation and potential litigation.

Review

11.1 This policy will be reviewed annually or more frequently if required by significant changes in legislation, regulation or business practice. It will be reviewed by the Information Council and presented to Council committee annually, in line with the Council's Policy Framework.