Information Security

Glasgow
CITY COUNCIL

Information Security Policy

Updated September 2024

Document Control

Document Information

Document Owner	Kenny Meechan, Head of Information & Data Protection Officer (Acting Senior Information Risk Owner)
Date First Approved for Publication	19 August 2013
Review Period	Annual
Date of Last Review	September 2024
Date of Next Review	August 2025
Relevant to	All council Services, Arms Length External Organisations (ALEOs) and CGI

Document History

Version	4.5
Date Issued	September 2024
First Approved By	Glasgow City Council Executive Committee on 26 September 2013
Latest Version Approved By	TBC

1. Definition of Information Security

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

2. Aims 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
- **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 spoken, printed or handwritten; stored on paper or stored electronically, including data stored in the cloud; sent by post or transmitted electronically, carried on PCs, laptops, tablets, iPads, mobile phones, USB devices, cameras or spoken in conversation.

Other members of the council family may adopt stricter standards than outlined in this policy. If not, then the Glasgow City Council standard applies. For further information contact your relevant Service/ALEO Information Risk Owner (SAIRO). A list can be found here.

CGI, the council's IT service provider, has delegated authority through its contract with the council to develop, monitor and apply IT technical security standards and policies to comply with the statements set out in this document.

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

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

5.2 A risk-based approach must be adopted.
It is important that controls are applied in a proportionate way in order that business process is not hampered and costs/benefits are optimised. The council has a separate **Information Security Risk Policy** which can be found here that sets out this approach.

5.3 Information security must be a priority in all partnerships.
Good security is crucial to building trust with partners and those with whom we share information. All new data sharing initiatives must consider security at the outset. Where it is proposed that personal data is shared, risks must be identified and assessed via the Data Protection Impact Assessment (DPIA) process, information about which can be found here. All data sharing must be governed by formal written agreements.

5.4 Access levels and users' rights must be clearly defined and controlled through formal processes.
Regular reviews of user access rights must be carried out and access rights withdrawn or changed promptly when staff leave or change roles. More on the leavers process can be found here.

5.5 Plan for the unexpected.
Regardless of vigilance, vulnerabilities will be found, new attack techniques will be developed and the surprising will happen. Processes must be flexible enough to cope with the unexpected, security defences must be layered (defence in depth) 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.

5.6 Design security for the whole lifecycle.
Security must be built in from the start, not bolted on later, to avoid expensive redesign or security being left out. During its operational life processes and procedures must be maintained, resources monitored, future capacity needs planned for and changes strictly controlled. At the end of an asset's life it must be disposed of carefully as insecure disposal can expose confidential information. Sensitive and/or personal data must be disposed of securely.

5.7 **All staff, and all those working or volunteering in the council family who do not have a permanent employment contract, must be accountable for their actions.** Information security responsibilities must be clearly defined and communicated for all. Training provision should be in accordance with corporate arrangements.

5.8 All user access accounts must be identifiable with an individual. Generic logon accounts must only be used in exceptional circumstances, and only where approved by the relevant SAIRO.

5.9 Segregation of duties is an important information security control mechanism that should be used where appropriate.

5.10 **All staff, contractors, consultants, agency workers, students, voluntary workers, interns, apprentices, skill-seekers and any other person working for the Glasgow Family** must act in accordance with this and the other policies and guidance listed in Appendix 3. Failure to do so may result in disciplinary action or termination of working or volunteering arrangements. All breaches of these policies must be fully investigated. Managers bringing in contractors, consultants etc. must ensure that these people are aware of their obligations to comply with these policies **before** they are given access to Council/ALEO systems or data.

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 are available.

6.2 **Senior Information Risk Owner (SIRO)**
The SIRO has delegated authority from the Corporate Management Team with specific responsibility for information risk and mitigation, including risks involving the Council's data. Currently the Head of Information & Data Protection Officer is the Council's Acting Senior Information Risk Owner (SIRO), but this is under review.

6.3 **Service/ALEO Information Risk Owner (SAIRO)**
A Service or ALEO Information Risk Owner (SAIRO) is the senior officer in each Service or ALEO with responsibility for information security risks relating to data processed and managed within that Service. SAIROs or their representatives attend the Extended Information Security Board.

6.4 **The Information Security Board (ISB - Core & Extended)** is chaired by the Senior Information Risk Owner. The Board champions information security by providing strategic leadership and is supported by the SAIROs or nominated senior representatives from all council Services, ALEOs and CGI. The ISB receives reports on information security risk management and information security incidents, and ensures appropriate control objectives and key controls are established to address any weaknesses identified. The ISB is responsible for the development of information security policy, guidance, communications and training, along with making sure that all staff, contractors, consultants, agency workers, students, voluntary workers, interns, apprentices, skill-seekers are made aware of these. The ISB will make sure this and other supporting policies as listed in Appendix 3 are reviewed annually.

6.5 **The Strategic Information, Innovation and Technology Team (SIIT)** makes sure CGI and the ICT functions of ALEOs fulfil their information security responsibilities. It also acts as the intelligent client for the Glasgow Family in identifying solutions that meet the requirements of the business, and arranges with our IT service providers for these to be delivered. SIIT will make sure that information security requirements are specified and communicated to IT service providers for inclusion in solution development. SIIT is also responsible for making sure that our IT service providers provide day to day services to the Glasgow Family which effectively address information security requirements.

6.6 **Information Asset Owners (IAOs)** are identified at the Service area level and are 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.

6.7 **CGI** must operate an Information Security Management System (ISMS). The ISMS must reflect the requirements of BS ISO27001 and its scope should include all of the services CGI provides to Glasgow City Council and ALEOs. ALEOs are responsible for developing and operating similar systems for their own IT services that are not received from CGI.

6.8 **Internal Audit** regularly reviews information security matters through an annual programme of audits. This serves to inform the risk management approach and promotes continuous improvement of policy.

6.9 **Managers** are responsible for ensuring that their staff and any non-staff individuals such as contractors, consultants etc. are given access only to systems and data they need to have access to for their current role, and that this access is removed when the member of staff or other individual no longer needs it. This includes following the leavers’ process when a member of staff leaves the organisation.

6.10 **All staff, contractors, consultants, agency workers, students, voluntary workers, interns, apprentices, skill-seekers and any other person working for the Glasgow Family** are responsible for protecting information in accordance with this policy. The persons listed must not seek to circumvent this and other related policies. Managers bringing in contractors, consultants etc. must ensure that these people are aware of their obligations to comply with this policy. All information security incidents must be reported via databreach@glasgow.gov.uk.

7. Further Information

For more information about this policy, you can contact the Head of Information and Data Protection Officer **by emailing AssetGovernance@glasgow.gov.uk**

OFFICIAL

APPENDIX ONE

Legislation

Information security is managed in accordance with the following legislation.

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.
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.
Data Protection Act 2018	This Act replaced the Data Protection Act 1998, and, along with the UK GDPR, forms the data protection regime which applies in the UK following the UK's exit from the European Union. Many of the detailed rules covering the application of the GDPR are found within the schedules of this Act.
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.
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.

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.
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, cookies, and unsolicited marketing emails (i.e. spam). They were updated in 2018 and 2019.
Public Records (Scotland) Act 2011	The council has a Records Management Plan setting out arrangements for the management of the authority's public records as required by the Act.
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.
UK General Data Protection Regulation	The UK General Data Protection Regulation (GDPR) is a provision made under the European Union (Withdrawal) Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendment) Regulations 2019. These laws continue in force the provisions of the EU GDPR following the withdrawal of the UK from the European Union. Both the EU and UK GDPRs place greater obligations on how organisations handle personal data. The UK GDPR needs to be read alongside the (amended) Data Protection Act 2018.

APPENDIX TWO

Standards

Information security is managed in accordance with the following standards.

STANDARD	DEFINITION
Code of Practice on Records Management issued under section 61 of the Freedom of Information (Scotland) Act 2002	Recommends security marking be applied to records.
Strategic Framework for a Cyber Resilient Scotland and associated Action Plan	This Action Plan sets out the key actions that the Scottish Government and its partners will take to help address issues relating to, and make sure of, confidence in standards of cyber resilience in Scotland's public bodies, and the Strategic Framework for a Cyber Resilient Scotland 2021-2023 .
Government Security Classification Policy	The GSCP is the Government scheme for protectively marking documents (both paper and electronic) to indicate how sensitive the contents are and what the appropriate level of security is. The council has adopted GSCP as part of its own protective marking policy. GSCP replaced the previous Government Protective Marking Scheme (GPMS).
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.
Government Cyber Security Strategy 2022 to 2030	The strategy sets out the vision and actions required to make sure that by 2030 the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

OFFICIAL

STANDARD	DEFINITION
Payment Card Industry Data Security Standards (PCI DSS)	**Standards 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). Please note, this is no longer used for secure email.
Her Majesty's Government 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.

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.

All guides can be found on the council intranet Connect.

- Acceptable Use of IT Policy
- Access Control Policy
- Data Protection Guides and Factsheets
- Data Security Incident and Breach Procedure
- GCC Code of Conduct for Employees
- GCC Code of Discipline for Employees
- Guidelines for staff using email and messaging services
- Information Security Risk Policy
- Information Security Staff Guidelines
- Information Use and Privacy Policy
- Physical Security
- Policy Statement on Bullying and Harassment
- Privacy Statement
- Protective Marking Policy
- Risk Management Policy and Framework
- Staff Guidance on the Use of Photography, Filming & Voice Recording