Information Security Governance Framework

Introduction

Information is a vital asset for the provision of services to the public and for the efficient management of the Council's resources. The Council recognises the increased threat of a cyber-attack which seeks to access and compromise its information and the consequences to the Council's residents, staff and reputation in the event of a successful attack.

It is essential that the Council has a robust information security governance framework in place to ensure that information, particularly personal, sensitive and confidential information is effectively managed with accountability structures, governance processes, policies, procedures, staff training and appropriate resources in place.

A key part of the governance framework is to support a consistent and empowered approach to risk management across the Council, with ultimate responsibility residing at SLT level. The Council has an approved Risk Management Strategy and Framework in place which defines how risks are managed by the Council at corporate and Service area level. It provides guidance on the processes, procedures, roles and responsibilities for risk and sets out how risks are managed.

This Information Security Governance Framework has been drafted to specifically control and direct the Council's approach to information and cyber security risk. It should be read in conjunction with the Information Security Policy and corporate Risk Management Strategy and Framework.

Roles and Responsibilities

The following section sets out the strategic overview of roles and responsibilities in relation to information security governance. Specific roles and responsibilities relating to information security generally are clearly set out in the Information Security Policy.

Elected Members

1. Cabinet has responsibility for overseeing performance and approving policy documents.

2. The Deputy Leader and Portfolio Holder for Resources and Reputation is the lead Elected Member responsible for information and communications technology.

Chief Executive and Senior Leadership Team

3. The Chief Executive is the Head of Paid Service who leads the Council's staff and advises on policies, staffing, service delivery and the effective use of resources.

4. The Chief Executive, together with the Deputy Chief Executive and Directors form the Council's Senior Leadership Team (SLT).

SLT will:

- Ensure the delivery of an effective Council wide information governance approach
- Agree what risks the Council is willing to tolerate and what is unacceptable
- Regularly review risks that may arise from an attack on technology or systems used
- Promote and drive a risk management culture across the Council.

Senior Information Risk Owner (SIRO)

5. The Director of Organisational Development and Democratic Services is the Council's Senior Information Risk Owner (SIRO).

   The SIRO is responsible for:

   - Managing information risk in the Council.
   - Chairs the Data Security Group.
   - Fosters a culture for protecting and using information within the Council.
   - Ensures information governance compliance with legislation and Council policies.
   - Is responsible for risk at SLT level, ensuring that risk is properly identified, managed and that appropriate assurance mechanisms exist.
   - Prepares an annual information risk assessment for the Council.
   - Gives strategic direction to the work of the Data Protection Officer (DPO).

Data Protection Officer

6. The Service Manager, Legal Services is the Council's Data Protection Officer (DPO).

   The DPO is responsible for:

   - Advising, monitoring and reporting the Council's compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).
   - Raising awareness of data protection requirements.
   - Leading information audits.
   - Advising on and reviewing data protection impact assessment and information sharing agreements.
   - Investigating data breaches and incidents.
   - Cooperating with the Information Commissioner's Office.

Directors

7. Each Director is accountable for identifying, understanding and addressing risks to the information assets within their directorates as well as ensuring good information governance.

Service Managers

8. Each Service Manager is responsible for the information assets and wider information governance within their service area.

   They must:

   - Ensure information is held, stored and shared appropriately.
   - Support the Director to address risks to the information and safeguard assets.
   - Promote good information governance practice amongst their staff.
   - Ensure that service specific procedures and processes are in place and conform to best practice as advised by the Data Security Group.
   - Ensure all staff attend training events and read training materials provided.

9. The Service Manager for Customer Services and Communications has specific responsibility to ensure appropriate ICT security arrangements are in place to protect the Council's electronically held information assets.

System Owners

10. All information systems within the Council will have an assigned System Owner.

    System Owners are ultimately responsible for those systems.

    System Owners will:

    - Ensure system operating procedures are in place and are followed.
    - Recognise actual or potential security incidents.
    - Ensure that information is accurate and up to date.
    - Ensure that only authorised access is granted.
    - Ensure the system delivers the required solutions.

Staff

11. All staff will:

    - Ensure that they comply with the requirements of the Information Security Policy and Personal Data Security Commitment Statement.
    - Follow security controls and local processes and procedures in place to protect the Council's information assets.
    - Attend data protection and cyber security training

Key Governance body

12. The Data Security Group (DSG) comprises the Director of Organisational Development and Democratic Services (Chair), Service Manager responsible for ICT, Service Manager responsible for Audit and Risk, Data Protection Officer or Deputy, and the Research and Development Manager (IT Support).

The overarching remit of the group is assist the Council to fulfil its obligations to appropriately protect paper and electronic 'data' and to ensure that everyone who has authorised access to 'data' is aware of their 'data handling' responsibilities.

The DSG will:

- Ensure comprehensive and current Information Governance Framework is in place and operating effectively throughout the Council.
- Maintain the Information Security Policy.
- Lead the organisation's approach to controlling and managing information and cyber risk.
- Consider and address issues arising from reports of the Data Protection Officer.
- Coordinate information governance activities (data protection, information requests, security, quality and records management) across the Council.
- Monitor information handling and breaches, implement assurance controls (including audits as required) and take corrective actions.
- Ensure data protection and cyber security training is provided to all staff including regular refresher training.
- Communicate and promote information governance and security awareness across the Council.
- Advise on best practice for procedures and processes for the handling and transfer of personal and confidential data to comply with statutory requirements, current government policy and recognised standards.
- Ensure Corporate Policies, procedures and processes are communicated to staff and the safeguards in place to ensure they are adhered to.
- Ensure these procedures and processes are sufficient to ensure the confidentiality of personal data and identify how they may fail.

Key policies

13. The key policies in this Information Security Governance Framework are:

- Information Security Policy.
- Data Protection Policy.
- Records Management Policy.
- Records Retention and Disposal Policy.
- Risk Management Strategy and Framework.

These policies are supported by procedures, guidelines and templates.

Resources

14. The following service areas have a role in supporting the Council's Information Security Governance Framework.

15. **The ICT team**

- Is lead for cyber security management and advice on the Council's IT infrastructure.
- Arranges the annual IT health check, Disaster Recovery testing and maintains PSN (Public Sector Network) Compliance.
- Provides training and guidance on cyber security matters.

16. **Legal Services**

- Provides legal advice on information governance matters to all service areas.
- Provides training and guidance to staff on data protection, freedom of information and Environmental Information Regulations matters.
- Supports and advises departmental FOI representatives.
- Provides records management services.

17. The audit function provides independent assurance of the Council's approach to risk management, control and governance.

Training and Guidance

18. Data protection and cyber security training for all staff will be mandatory as part of induction and periodically thereafter. Further detailed training as appropriate to the role will be available as necessary.

Awareness sessions may be given to staff as required, at team meetings or other events.

Regular reminders on data protection and cyber security topics are made through corporate and local team briefings, staff news and emails.