Appendix 1

West Dunbartonshire Council

(Information Security Policy Framework)
Information Security Policy

Contents

Version Control

Version	Description	Release Date	Issued By
0.1	First Draft of Information Security Policy to replace the old Corporate Information and Communication Technology Acceptable Use & Security Policy (ISP - 4.8)	June 2019	ICT Security Officer
0.2	Various updates following SLG feedback	July / August 19	ICT Security Officer
1.0	Final Draft	August 19	ICT Security Officer

1. Introduction

1.1 Information plays a critical role in the lives of West Dunbartonshire Council citizens, 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 service delivery.

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

- Physical access to electronic and paper-based information assets;
- Logical access to data, systems, applications and databases;
- External and internal access to the network and all other computing resources;
- Legislation impacting information and technology 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 citizen privacy rights, regulations, and laws; and
- 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 "Information Security Statement of Intent" states the Council's position and supports the Information Security Policy.

2. Purpose

2.1 The purpose of Information Security is to protect the information held by West Dunbartonshire Council, relating to our citizens, 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 processes, systems (manual and electronic), 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 policies, guidance and standards relevant to information security;

- Assist West Dunbartonshire Council employees in protecting the confidentiality, integrity, and availability of Council information;
- Ensure that all information, particularly personal and citizen information, is treated appropriately at all times;
- Ensure compliance with all relevant legislation and regulations regarding Council information assets; and
- Enable West Dunbartonshire 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 employees and individuals with access to Council information 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 Council service areas will be expected to adhere to the requirements of this policy in the way that they work.

3.3 The Senior Information Risk Owner (SIRO) has overall responsibility for ensuring implementation of this policy and is assisted in fulfilling this role by the Council's senior management team.

3.4 Additionally, a number of roles and groups within the Council will be expected to manage compliance with this policy as part of their remit. These include:

- Managers;
- ICT Security Officer;
- Data/Information Protection Officer;
- Network Security Analyst;
- ICT employees;
- System administrators within service teams;
- Information Security Forum; and
- ICT Board.

3.5 Services must nominate one or more senior officer (member of Council's Senior Management Network (SMN) to represent them at Information Security Forum meetings as and when required. The forum is chaired by ICT Security Officer and has been in place for several years, reviewing breaches and identifying and auctioning improvement measures.. Permanent members of the Forum are as indicated in the Information Security DPA forum charter.

3.6 The Forum meets at quarterly intervals throughout the year to review information security across the Council. Special meetings may be held to examine a specific security issue problem.

4. Risk Management

4.1 Assessing information risk is required for the protection of information assets throughout their lifecycle. This framework guidance 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 the use of personal data as outlined in the Records Management and Data Protection documents.

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; and

e. Ensure an Information Security Risk Register is maintained by relevant Service Manager and ICT Manager is responsible for Corporate ICT Risk register.

5. Asset Management and Classification

5.1 Appropriate measures are in place to ensure the protection of information assets and information processing as detailed in this clause 5. Each Service is responsible for maintaining their information asset entries within the Council's Information Asset Register which was introduced by Regulatory Services in 2018. The register contains an inventory of information assets and identifies a range of details including the service name of the information asset owner, whether personal information held, location of the assets and the legal basis for processing.

5.2 The Government Security Classification scheme is under review by Regulatory Services and this incorporates the handling of information assets. The Information Handling and Classification Procedure assists employees in judging what information requires to be marked, how to reach this decision and what security is required.

5.3 The Records Management guidance covers how information assets are used and stored in different scenarios and throughout their lifecycle.

5.4 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 business and service delivery. The Council undertakes to provide appropriate information security training for employees, elected members and third parties as appropriate. Service Managers must ensure that:

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

b. All employees with access to information assets undertake the appropriate information security training provided by their Service area;

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

d. All employees understand their obligations to both protect special category information (e.g. in line with Records Management Policy) and business sensitive information and ensure openness and transparency in decision-making (e.g. in response to freedom of information requests or any other request to release information into the public domain;

e. All users of ICT (employees, elected members and partners) are familiar with the system security operating procedures governing system use, receive appropriate training as defined by the relevant Strategic Lead, and are aware of Reporting of Information Security Concerns policy; and

f. Strategic Leads should ensure that employees 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 actions may lead to disciplinary or criminal proceedings.

5.5 Further user responsibilities are defined in the Acceptable Use Policy.

6. Human Resources Security

6.1 Strategic Leads must ensure that West Dunbartonshire Council's Recruitment and Selection Policy is complied with during all stages of the recruitment process, ensuring that appropriate recruitment checks and controls (e.g. Disclosure Scotland and PVG – Protecting Vulnerable Groups) are in place before access to information assets is permitted. This includes all recruitment, (both internal and external), change of role (e.g. secondment, acting up arrangements) and termination of employees and third parties. Further guidance on can be found via HR Online.

7. Access Control

7.1 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 as follows. This includes physical and ICT 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 remote or home working.

8. Physical and Environmental Security

8.1 Appropriate measures exist and will continue to be implemented as needed 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.

In the event that ICT equipment is lost or stolen, this must be reported directly to a service manager, ICT security officer or ICT management team and can also be logged via the ICT service desk.

Information Assets also include hardware hosting Information and these hardware assets must be handled and disposed of in line with the Acquisition and Disposal of ICT policy.

9. Information Systems Acquisition, Development and Maintenance

9.1 West Dunbartonshire 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 (purchased or developed) appropriate steps must be taken by all involved to ensure that

- New systems correctly process information;
- Any necessary cryptographic controls are implemented;
- The security of system, hosting and software application files is considered;

- Security during development stage is adhered to;
- Support and maintenance processes are properly managed; and
- that consideration is given to patch and vulnerability management.

9.2 Strategic Leaders will further comply with the requirement to assess potential privacy risk and impact in line with the Councils Data Protection Policy.

9.3 Further advice on procurement processes can be found on the Council's Intranet.

10. Information and/or Security Incident Management

10.1 The appropriate service manager must be notified immediately when;

- Unauthorised use of internet access has taken place or is suspected of having taken place;
- Passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed;
- Unusual system behaviour occurs, such as missing files, frequent system crashes or misrouted messages;
- Sensitive WDC information is lost, disclosed to unauthorised parties or suspected of being lost or disclosed to unauthorised parties; and
- In instances where personal or sensitive data may have been compromised, a senior officer within the service should immediately notify the Strategic Lead Regulatory Services, the Data Protection / Information Protection Officer and the ICT Security Officer to seek guidance. Report a Data Breach

10.2 It is the responsibility of all employees, elected members and partners to report any suspected irregularities / fraud to their Strategic Lead, or nominated senior officer, thereafter the Audit and Risk Manager, as soon as possible.

10.3 A log will be maintained by the ICT security officer of all reported ICT security incidents.

11. Business Continuity Management

11.1 Measures already exist within each service area to counteract interruptions to business activities, to protect critical business processes from the effects of major failures or disasters and maintain core services. Services must ensure they retain up to date Business Continuity Plans to manage interruption in service delivery such as an IT incident. This process is coordinated by the Council's Civil Contingencies Service (CCS).

12. Compliance

12.1 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 2016/679;

c. Freedom of Information (Scotland) Act 2002 (including relevant decisions);

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 1992 (Display Screen Equipment) and Health and Safety (Display Screen Equipment) Regulations 1992;

k. Re-use of Public Sector Information Regulations 2005;

l. Civil Contingencies Act 2004 and The Civil Contingencies (Contingency Planning) (Scotland) Regulations 2005; and

m. Any other relevant legislation as may be enacted from time to time.

13. Further Information

13.1 Information Security policies and standards are available on the West Dunbartonshire Council Intranet. For further advice, please contact ICT Security Officer.