WEST LOTHIAN COUNCIL
INFORMATION SECURITY
POLICY
Document Control Sheet

DATA LABEL: PUBLIC

AUTHOR: Roberto Riaviz
TITLE: Information Strategy & Security Manager
DOCUMENT TITLE: WLC Information Security Policy

Approval History

<table>
<thead>
<tr>
<th>Date</th>
<th>Approved By</th>
<th>Version Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>30/03/2017</td>
<td>Information Management Working Group (IMWG)</td>
<td>3.1</td>
</tr>
<tr>
<td>22/05/2017</td>
<td>ICT Programme Board</td>
<td>3.1</td>
</tr>
<tr>
<td>28/04/2017</td>
<td>P&amp;RPDSP</td>
<td>3.1</td>
</tr>
<tr>
<td>20/06/2017</td>
<td>Council Executive</td>
<td>3.1</td>
</tr>
</tbody>
</table>
# CONTENTS

1. INTRODUCTION.................................................................................................................. 4
2. MAIN OBJECTIVES ............................................................................................................. 4
3. LEGISLATION ..................................................................................................................... 5
4. SCOPE ................................................................................................................................ 5
5. STANDARDS ....................................................................................................................... 5
6. RESPONSIBILITIES ........................................................................................................... 5
7. ASSET MANAGEMENT ....................................................................................................... 8
8. INFORMATION CLASSIFICATION .................................................................................... 8
9. PHYSICAL AND ENVIRONMENTAL SECURITY ............................................................... 9
10. USER ACCESS MANAGEMENT .................................................................................... 9
11. EQUIPMENT SECURITY ................................................................................................. 9
12. NETWORK SECURITY MANAGEMENT ......................................................................... 10
13. MOBILE COMPUTING AND TELEWORKING ............................................................... 10
14. PUBLICLY AVAILABLE INFORMATION ..................................................................... 10
15. EXTERNAL PARTIES ...................................................................................................... 10
16. HUMAN RESOURCES .................................................................................................... 11
17. DISCIPLINARY PROCESS .............................................................................................. 11
18. PROTECTION AGAINST MALICIOUS CODE (VIRUSES) ........................................... 11
19. INFORMATION HANDLING ........................................................................................... 12
20. EXCHANGE OF INFORMATION/INFORMATION SHARING ......................................... 12
21. ENCRYPTION (CRYPTOGRAPHIC CONTROLS) ............................................................ 12
22. ELECTRONIC COMMERCE SERVICES AND PCI DSS ................................................ 12
23. ICT OPERATIONAL MANAGEMENT ........................................................................... 12
24. BUSINESS CONTINUITY ............................................................................................... 13
25. INFORMATION SECURITY INCIDENT MANAGEMENT .............................................. 13
26. INFORMATION SECURITY POLICY RESPONSIBILITY .............................................. 14
27. INFORMATION SECURITY WITHIN THE INFORMATION MANAGEMENT WORKING GROUP AND ICT PROGRAMME BOARD ............................................................ 14
28. CYBER SECURITY .......................................................................................................... 15
29. MONITORING & REPORTING ..................................................................................... 16
30. REVIEW .......................................................................................................................... 16
1. **INTRODUCTION**

The services delivered by West Lothian Council are becoming increasingly information dependent. Effective management, understanding and sharing of this information can offer service improvements and efficiencies. However, such information is increasingly subject to legislation, Government guidelines, scrutiny, audit, risks and threats.

Information within the Council takes many forms and includes data stored on computers, transmitted across networks, presented on web pages, printed or written on paper, sent by fax, stored on tapes, CDs, DVDs or spoken in conversation or over the telephone.

The potential impact of damage or loss of this information includes disruption to services, risk to citizens, damage to reputation, legal action, personal distress, loss of confidence, and may take considerable time and cost to recover.

The risk of damage or loss is mitigated by applying Information Security controls intended to prevent or minimise the impact of such events.

Information security management within West Lothian Council is concerned with preserving the: Availability (protecting against loss or damage and ensuring maximum uptime and reducing service outages); Confidentiality (ensuring compliance with the Data Protection Act); Integrity (ensuring accuracy and completeness) of information by protecting against unauthorised access or modification.

This policy sets out the overall security principles that apply to information management and all other information security documentation within the Council e.g. Corporate and service based guidelines and procedures.

2. **MAIN OBJECTIVES**

- To ensure that the Council complies with information related legislation and government guidance.
- To maintain effective but proportionate security controls that are designed to protect information and give confidence to information subjects, owners, users and auditors.
- To ensure that everyone with access to the Council’s information systems are aware of information security responsibilities and good practice.
- To ensure that the Council’s information assets and associated technologies are protected from all known threats, including internet (cyber) threats on a cost/benefit basis that is relative to the associated risks.
- To ensure that all breaches in information security, actual or suspected are reported, investigated, reviewed and acted upon.
3. **LEGISLATION**

The Council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to staff and agents of the Council, who may be held personally accountable for any breaches of information security where they are personally responsible. The Council shall comply with the following legislation and other legislation where appropriate:

- The Data Protection Act (1998)
- The Freedom of Information (Scotland) Act 2002
- The Public Records (Scotland) Act 2011
- The Computer Misuse Act (1990)
- The Health & Safety at Work Act (1974)
- The Human Rights Act (1998)
- The Regulation of Investigatory Powers (Scotland) Act 2000
- The Re-Use of Public Sector Information Regulations 2005
- The Environmental Information (Scotland) Regulation 2004
- The Insurance Act 2015

4. **SCOPE**

The Information Security Policy applies to all employees and Elected Members of West Lothian Council, consultants, contractors, agents and partner organisations provided with authorised access to the Council’s equipment, systems, information and paper records.

5. **STANDARDS**

Information Security Management within West Lothian Council will comply with the British Standard: **BS ISO/IEC 27001:2013**

This standard specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the Council's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of the Council. ISO27032 and The Government’s [Cyber Essentials](#) provide security standards for the Internet (referred to as “Cyberspace” or “Cyber”).

6. **RESPONSIBILITIES**

The Chief Executive and Corporate Management are ultimately responsible for Information Security Management within West Lothian Council:

The Chief Executive is the Senior Information Risk Officer (SIRO) for the council. Depute Chief Executives and Heads of Service are responsible for:

- ensuring that this policy is communicated to all individuals, including third parties, who are authorised to use information facilities;
- ensuring that information security principles and standards of operation are consistently enforced, in line with the terms of this policy, across all service areas;
ensuring service-level representation on the Information Management Working Group;
applying higher level access for staff where it is appropriate for business purposes.

Service Managers

Service Managers are responsible for:

- Information created, held, stored, processed and destroyed in their service;
- Owning and managing risks associated with information, systems and applications in their service;
- ensuring that business continuity plans are in place that covers the loss of information and systems within their service;
- ensuring that appropriate information handling arrangements are in place within their service;
- determining, on the basis of business needs, those staff who require access to information to assist them in the performance of their duties;
- ensuring that appropriate local access controls are in place (e.g. application passwords, lockable storage etc.);
- ensuring appropriate resources for the response/investigation/management/resolution of security incidents in their service areas.

Line Managers

Line Managers are responsible for:

- ensuring that authorised users are given appropriate training and are fully briefed in good practice, legitimate and lawful use of the systems in accordance with the standards set down in this policy;
- new employees are appropriately vetted and made aware of this policy during their induction training;
- ensuring that authorised users are made aware of the possible disciplinary and/or legal consequences of any breach of this policy and any associated procedures or codes of practice;
- reviews are carried out to ensure compliance with the terms of this policy;
- complying with procedures for removing or amending the access rights of their staff who change jobs or leave the Council;
- reporting security incidents to the IT Service Desk;
All authorised users (including Elected Members, staff, consultants, contract and agency staff)

General responsibilities of any and all authorised users:

- comply with the terms of this policy in relation to good practice and legitimate and lawful use of West Lothian Council information systems and physical records;
- manage the security of their own work in accordance with the Council’s Data Protection and Information Security Procedures;
- ensure they exercise security (in line with guidelines) of all personal or sensitive information they handle on behalf of West Lothian Council;
- comply with all other guidelines relating to information security including password use, clear desk/clear screen guidelines, anti-virus guidelines, internet and email use policy etc;
- must not circumvent or alter security facilities (such as anti virus software), access control facilities (e.g. network passwords, firewall rules etc.) without prior permission;
- report all suspected cases of misuse/breach of this policy to their line manager.

Business Change, Programme and Project Managers

- ensuring that information security (including Cyber Security) is specified and included in project plans and contracts;
- ensuring new implementations and timely upgrades to existing information systems are fully risk assessed, tested and that audit arrangements are put in place;
- ensuring that project and corporate Risk Logs are kept up to date with developments;
- ensuring that all external project staff and suppliers are aware of their information security responsibilities during project implementation and ongoing operations.

IT Manager is responsible for:

- maintaining all security issues associated with central systems facilities such as servers, databases, software and network facilities;
- Identify, monitoring, mitigating and managing system and application vulnerabilities and cyber-attacks in conjunction with services, partners and suppliers.
- providing all ICT based security facilities such as firewalls, anti-virus software, intrusion detection, encryption facilities;
- manage and apply baseline security build and configuration for all approved ICT hardware and devices including security patch management;
- maintaining Internet network security, user accounts and filtered user access, and for monitoring and reporting on inventories and access logs;
• providing backup and disaster recovery facilities for systems (as per service’s business continuity plans);
• providing backup and disaster recovery as well as business continuity facilities for all central systems including email, internet, electronic file storage, firewalls etc.;
• reviewing the technical, operational and security aspects of this policy, in consultation with Service Units;
• issuing procedural guidance and codes of practice in support of this policy;
• providing evidence and log information for periodic audits, ‘code of connection’ requirements and security accreditations.

Information Security Officer

• provision and maintenance of the Information Security Policy, guidelines and procedures;
• provision of ICT Security training material and online content (for all users);
• provision of advice and assistance in planning on security issues to the Information Working Group, ICT Programme Board and across services, programmes and projects;
• sign-off authority on firewall and network security changes and updates.

7. ASSET MANAGEMENT

• Information Assets e.g. Databases, documents etc. will be identified and managed within the Records Management Policy;
• All ICT and information assets will be clearly identified and included in a central inventory (maintained by IT Services);
• All assets will have an identified ‘owner’, either Head of Service or IT Services (for central systems);
• The West Lothian Council Software Use Guidelines are available on the Council’s intranet (IT Pages);


8. INFORMATION CLASSIFICATION

All information within West Lothian Council will be identified and classified by the criteria set out in the Council’s Records Management Plan, Policy and associated Guidelines. Information will be classified and labelled as per each service’s File Plan and the Council’s classification scheme. This will ensure that appropriate levels of protection are afforded when handling information. Higher levels of protection will be applied to personal or sensitive information or where there is a specific legal requirement.

In some instances it will be necessary to adopt even higher levels of security where information relates to Central Government Classifications (Official, Secret and Top Secret). Specific arrangements will be put in place for such information.
9. PHYSICAL AND ENVIRONMENTAL SECURITY

Depending upon the function and the nature of use, accommodation that stores information will be equipped with perimeter barriers, walls, gates manned reception desks, CCTV and entry controls. Public areas, deliveries etc. will be isolated from information processing areas.

Offices that deal with personal and/or sensitive information will have entry controls and lockable storage facilities. The above relates to operational offices and to off-site storage facilities.

10. USER ACCESS MANAGEMENT

All users will be granted/revoked access to systems via a formal user registration and de-registration process. User access will be granted on a role-based, least privilege basis (users will only be granted access to the areas of the network, systems and applications that their job role requires). A Password Management guideline and a Password Management Policy for IT Systems is in place that defines the standards and best practice for ensuring strong passwords. User access rights will be reviewed, monitored and audited on a regular basis (at least annually). User activity will be regularly logged and reviewed for unusual activity.

11. EQUIPMENT SECURITY

In order to mitigate the risks of loss, damage, theft or compromise of equipment and to protect equipment from environmental threats and hazards, and opportunities for unauthorised access:

- Central equipment (servers, network equipment, storage etc.) will be protected from power failures and disruptions caused by failures in supporting services;
- Power and telecommunications cabling shall be protected from interception or damage;
- All equipment shall correctly maintained to ensure correct (specified) operation and uptime;
- Secure disposal of equipment – all items containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal;
- Security settings and software must not be altered without prior permission from IT Services;
- Equipment, information or software shall not be taken off-site without prior authorisation;
- Security shall be applied to off-site equipment taking in to account the different risks of working outside the Council’s premises; and
- Specific guidance and procedures will be issued by IT Services.
12. NETWORK SECURITY MANAGEMENT

IT Services will specify, implement manage and maintain central network management facilities e.g. cabling, switches, wireless devices, hubs, firewalls and intrusion detection systems.

IT networks will be protected against internal and external cyber threats and attacks and security controls will be monitored and tested.

Networks will be adequately managed and controlled in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or by a third party.

Users will only be permitted access to areas of the network they have been specifically authorised to use.

Appropriate authentication methods will be used to control access of remote users.

Automatic equipment identification will be maintained as a means of authenticating connections. Physical and logical access to diagnostic and configuration ports will be controlled. Networks will be segregated to ensure security between groups of users.

Routing controls will be maintained to ensure security of business applications.

All network connections and third party access must comply with this policy and have been approved by IT Services.

Network security will be compliant with the requirements of key external networks e.g. the ‘Code-of-Connection’ agreements of the ‘Janet’ and ‘PSN’ (Public Services Network), SWAN (Scottish Wide Area Network) networks.

13. MOBILE COMPUTING AND TELEWORKING

Mobile working and teleworking will be supported but will also be subject to prior approval and must conform to guidelines and procedures.

The guidelines/procedures include specific and appropriate security measures for the protection from the specific risks of cyber threats, teleworking, mobile computing and communication facilities.

14. PUBLICLY AVAILABLE INFORMATION

The integrity of information being made available on publicly available system (e.g. the Council’s Web Site) will be protected to prevent unauthorised modification or loss. Information published on behalf of the Council must follow agreed publishing procedures.

15. EXTERNAL PARTIES

To maintain the security of the Council's information and information processing facilities that are accessed, processed, communicated to or managed by external parties:
The risks to the organisation’s information and info processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

All identified security requirements shall be addressed before giving customer access to the organisation’s information or assets.

A documented third party access agreement will be required of all service providers providing any aspect of information management and must cover all security requirements, including those relating to cyber security.

Service delivery agreements will be regularly monitored and reviewed and will cover the security controls and standards required. All services will be reviewed upon significant change or upgrade.

16. HUMAN RESOURCES
Managers will ensure that all staff, contractors and third party users understand their responsibilities with regard to information security. User will be required to sign network access agreements as part of their employment. Line managers must ensure all employees completing appropriate awareness training and regular updates as relevant to their job function. In high risk areas, it will be necessary to conduct screening and background verification checks (conducted by Human Resources). This Information Security Policy forms part of the Council’s employment policy framework as referenced in Council contracts of employment. Upon termination of employment line managers must ensure the return of assets and the removal of all access rights.

17. DISCIPLINARY PROCESS
Any misuse of information or information systems will be investigated under the Council’s Disciplinary Procedure. Any resulting disciplinary action, and the level of that action, will depend on the extent of misuse identified in each case. However, serious misuse including knowingly accessing or attempting to access systems or information without authorisation, handling security marked information (such as personal information) without regard to guidelines or procedures or deliberately causing security incidents will be treated as gross misconduct in accordance with the Council’s Disciplinary Code.

In certain circumstance, breaches of this policy may be deemed unlawful and the individual(s) concerned will become subject to criminal proceedings.

18. PROTECTION AGAINST MALICIOUS CODE (VIRUSES)
A central anti-virus security system will be managed by IT Services. This will include malware and activity relating to cyber-attacks, anti-virus updates, monitoring, alerting & responding. This will include all security patching on central servers and systems as well as PC based antivirus. Users will be required to comply with Anti-virus guidelines & requirements.
19. INFORMATION HANDLING

Information handling will be in strict accordance with the Information Handling Guidelines of West Lothian Council. Local procedures will be in place for all removable media and information in transit. Council information, that is subject to the Data Protection Act (1998), must not be stored or transmitted on USB memory drives, removable drives, CDs and DVDs. Only Council approved methods of information transit will be permitted. Electronic data devices such as Laptops, CDs, Memory Sticks and other removable memory devices must be protected, using council approved encryption methods, from unauthorised disclosure, loss or misuse. High risk areas will be identified, recorded on the council’s risk register and additional procedures, staff training and awareness will be applied.

20. EXCHANGE OF INFORMATION/INFORMATION SHARING

Formal guidelines, procedures, protocols and controls must be in place to protect the exchange of information of West Lothian Council and external bodies. Individual exchange agreements must be in place for each instance. These exchange agreements will detail the Council’s information security requirements.

Each service must maintain a register of all information exchanged. This will be recorded in the council’s corporate risk register. The management of these risks will be the responsibility of service managers. All channels will be tested and assessed on an annual basis or where a significant change/upgrade occurs.

21. ENCRYPTION (CRYPTOGRAPHIC CONTROLS)

Procedures and guidelines for the use of encryption technologies will be provided by IT Services in order to protect data both in transit and at rest. These controls will be used, reviewed and kept up to date in accordance with all relevant agreements, legislation and regulations.

22. ELECTRONIC COMMERCE SERVICES AND PCI DSS

Information involved in electronic commerce (such as online payments, electronic purchasing etc.) passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification. All payment card information processed, stored and transmitted will be in accordance with PCI DSS 3.0 (Payment Card Industry Data Security Standard). Where such services are provided by a third party, contracted agreements on security requirements must be in place. Service levels will be monitored and audits will be conducted to ensure compliance with the Council’s security requirements.

23. ICT OPERATIONAL MANAGEMENT

IT Services will ensure documented operating procedures for all ICT (Information and Communications Technology). This includes network equipment, central servers,
backup facilities, central databases, central storage and web facilities. Such equipment and systems will be subject configuration and change management.

Access and areas of responsibility will be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the system. System and administrator passwords will be issued on an individual basis and used in a secure manner to maintain least privilege access control. Access to databases, system files/facilities and operating systems will be strictly controlled.

The capacity of these facilities will be managed and optimised – the use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure required system performance.

Audit logs of activities on servers etc. will be maintained to assist in security monitoring and investigations.

Incidents and system faults will be logged with the IT Service Desk.

Development, Test and operational facilities shall be separated to reduce the risks of unauthorised access. System acceptance criteria will be drawn up to ensure consistent criteria for the testing of new systems/changes/upgrades.

Back-up copies of information, databases, configurations and software shall be taken and tested regularly in accordance with the agreed backup plan.

24. BUSINESS CONTINUITY

Facilities and systems shall be in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters and to ensure their timely resumption.

Business continuity plans, procedures and facilities shall be in place for all of the Council's critical systems. This will be in accordance with the Council's risk management practices. A disaster recovery facility shall be put in place and maintained by IT Services that allows for the full or partial recovery of critical business systems in the event of a disaster at the Civic Centre.

All backup, business continuity and disaster recovery systems will be regularly reviewed and tested. For critical business systems this will be on at least an annual basis and after each significant change or upgrade.

25. INFORMATION SECURITY INCIDENT MANAGEMENT

All staff, contractors and third party users of information systems and services are required to note and report any observed or suspected security weaknesses in systems or services. All must comply with the subsequent requirements and directives in order to rectify or eliminate the security risk.

Security incidents must be logged with the IT Service Desk who will ensure the timely notification to management and the Information Security Officer.
IT Services will give security incidents priority over normal service work until an agreed and acceptable level of security is restored.

All on-going security risks must be recorded on the council's risk register.

Security incident resolutions will be managed by the Council’s Information Security Officer in conjunction with managers and staff in services, as required.

All security incidents will be reported by the IT Service Desk on a 6 weekly basis to the Information Management Working Group and quarterly to the ICT Programme Board.

The Information Security Incident Procedure will be made available to all parties.

26. INFORMATION SECURITY POLICY RESPONSIBILITY

The Head of Corporate Services will serve as the designated officer responsible for ensuring the development, publishing and maintenance of the information security policy and information security management systems within West Lothian Council.

The IT Manager is responsible for the operation, implementation and resourcing of this policy including operational controls, security systems and the provision of evidence in accordance with the ISO27001 standard.

The Information Strategy and Security Manager will serve as the designated officer responsible for administering the Information Security Policy. Appropriate contacts with professional associations and security forums will be maintained (e.g. SocITM Security Group and CISSP – Certified Information Security System Professional Group).

This policy will be subject to regular audit and review by Internal Audit and external Audit.

27. INFORMATION SECURITY WITHIN THE INFORMATION MANAGEMENT WORKING GROUP AND ICT PROGRAMME BOARD

The group will be kept abreast of Information Security by the Head of Corporate Services. Each Council service will be represented at an appropriate level and may choose to have multiple representatives to suit the services internal structure.

The Group will meet on an annual basis to review and update the Policy.

The group members will meet at two month intervals to review the ongoing implementation and development of the Information Security Policy but specifically:

- To review security incidents
- To approve recommendations of new initiatives relating to Information Security to the corporate management team.
- To review through a process of risk management the Council’s exposure to risk, assessing the risks to Council's information assets. A review of the existing risk register together with the inclusion of new risks to Information Security will be
considered. Risks will be rated on the vulnerability of a system, the likelihood of occurrence of the threat and the potential impact to the Council.

- To ensure that the Information Security Policy is adopted by all Council services.
- The group will review the Council’s legal, statutory, regulatory and contractual requirements for the Council, its suppliers and appointed third parties.
- The group will review Information Processing strategies to ensure that security is central to the processing of information.
- To find and review methods of continually promoting the education of Information Security throughout the Council.
- To assess the adequacy of the security controls implemented for specific new systems and services.
- On a regular basis, to agree and approve reports to Corporate Management Team regarding information security.

28. CYBER SECURITY

In order to protect council systems and information from internet based (cyber) threats, and crime, IT services will lead on the operation of a ‘Cyber Security Strategy’ for the council. This strategy will form part of the council’s ICT strategy and support service areas in the provision of cost effective online digital services. Clearly defined roles and responsibilities will be assigned to security systems and processes. The strategy will encompass the following:

- **Inventory** – Identification of information, systems, applications and hardware assets most at risk from internet borne threats.
- **Risks** - Are recorded and roles assigned i.e. Business Owner (budget holder), Systems Administrator, IT Manager, Suppliers etc. Risk will be recorded in the council’s risk register.
- **Identity Management** – protecting the online identity of council staff and customers though the implementation of effective user access controls and authentication.
- **Threat Analysis and Intelligence** – Identifying the threats to the councils business and systems through network analysis and notifications from internet authorities and reporting forums such as the Cyber-security Information Sharing Partnership (CiSP), Warning Advice and Reporting Point (WARP), Partners and suppliers.
- **Configuration and patch management** – Management of software and updates from suppliers including priority patching where required.
- **Monitoring, Alerting and Reporting** – Monitoring the council’s boundary firewalls, internet gateways and other critical systems to ensure early identification, containment and alerting of cyber based vulnerabilities, risks and incidents.
• **Incident Handling and Recovery** – Appropriately resourced response teams to work systematically with internal teams, suppliers, partners, law enforcement agencies and authorities to recover council systems in the event of incidents and attacks.

29. **MONITORING & REPORTING**

Monitoring activities will be carried out by services on an annual basis. Compliance must be monitored as part of the statement of compliance of the Council within its Code of Corporate Governance. Where non-compliance to this policy is discovered suitable remedial and long term actions will be implemented to ensure resolution.

30. **REVIEW**

Date Last Reviewed:  May 2018
Date of Next Review:  May 2019