9. GOVERNANCE

Policy 9. 21

IT INFRASTRUCTURE SECURITY

Version 1

9. GOVERNANCE

9.21 IT INFRASTRUCTURE SECURITY POLICY

1. OBJECTIVES

The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council's information, in line with section A9 of ISO/IEC/27001.

In order to ensure the continued protection of the personal, confidential and RESTRICTED information that Lithgow City Council holds and uses, and to comply with legislative requirements, and information security best practice access to Lithgow City Council's information equipment and information must be protected.

The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access.

2. SCOPE

All Lithgow City Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council with access to Lithgow City Council's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Council's equipment and the information that they use or manipulate.

3. DEFINITION

This policy applies to all users of the Council's owned or leased / hired facilities and equipment. The policy defines what electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of information within the custody of the Council.

This policy should be applied whenever a user accesses Council information or information equipment. This policy applies to all locations where information within the custody of the Council or information processing equipment is stored, including remote sites.

4. RISKS

Lithgow City Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Negligent or malicious acts of employees
- Targeted attacks, theft and destruction of data by criminal hackers
- Accidental damage and distribution of data
- System malfunction
- Loss of data stored by Third Party providers
- System infection through malicious email campaigns
- Cyber extortion or ransomware

- Denial of service attacks
- Stolen and lost devices

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

5. APPLYING THE POLICY

5.1 Secure Areas

PROTECT and RESTRICTED information **must** be stored securely.

Physical security must begin with the building itself. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Access control mechanisms fitted to all accessible doors
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g. fire, flood, vandalism.

As an example, access to secure areas such as the server room must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff should challenge unknown persons if seen in staff only areas. Each department must ensure that doors and windows are properly secured.

Access passes (e.g. keys, entry codes, HID tags etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times. A Council IT employee must monitor all visitors accessing secure IT areas at all times.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately.

A. EQUIPMENT SECURITY

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have data stored on the local hard drive. Data should be stored in business systems such as ECM where appropriate. File server locations such as T drive can be used to save non sensitive working documents. For working documents of sensitive nature, “My Documents” should be used. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from IT department.

All items of equipment must be recorded in IT Asset database. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of. Disposed items are to be recorded in the It Asset Disposal log. The record is to include the date, description of the item, the IT asset number, means of disposal and be signed by both the It officer disposing of the item and another member of the IT team.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the IT asset database. Monitors are not individually numbered, but are regarded as part of the PC.

B. CABLING SECURITY

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

C. EQUIPMENT MAINTENANCE

The IT department must ensure that all of Lithgow City Council’s ICT equipment is maintained in accordance with the manufacturer’s instructions and with any documented internal procedures to ensure it remains in working order. Staff involved with maintenance should:

- Retain all copies of manufacturer’s instructions.
- Identify recommended service intervals and specifications.
- Enable a call-out process in event of failure.
- Ensure only authorised technicians complete any work on the equipment.
- Record details of all remedial work carried out.
- Identify any insurance requirements.
- Record details of faults incurred and actions required.

A service history record of equipment should be maintained so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs.

D. SECURITY OF EQUIPMENT OFF PREMISES

The use of equipment off-site must be formally approved by the IT Manager. Equipment taken away from Lithgow City Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be password protected.

Any losses / damage must be reported to the IT Manager.

E. SECURE DISPOSAL OR RE-USE OF EQUIPMENT

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

F. DELIVERY AND RECEIPT OF EQUIPMENT INTO THE COUNCIL

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.
- Holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

G. REGULAR AUDIT

There should be an audit information security arrangements regularly to provide an independent appraisal and recommend security improvements where necessary.

6. POLICY COMPLIANCE

If any user is found to have breached this policy, they may be subject to Lithgow City Council disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

7. POLICY GOVERNANCE

The following table identifies who within Lithgow City Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IT Manager
Accountable	Chief Financial & Information Officer
Consulted	Executive Management Team, Councillors
Informed	Council Staff, Contractors, Members of the Public

8. REVIEW AND REVISION

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 4 years.

Policy review will be undertaken by the IT Manager.

Maintained by Department:	Finance & Assets	**Approved by:**	Council	**Exhibition Date:**	
Reference:	Policy Register	**Council Policy No:**	9.21	**Effective Date:**	
Min No:		**Version No:**	1	**Reviewed Date:** **Next Review Date:**	
Attachments:					