Physical Security Policy

This policy applies to all companies within the Relyon Group.

Purpose

Any loss, compromise, or misuse of council information and associated assets, however caused, could have potentially devastating consequences for the company and may result in financial loss and possible legal action.

Introduction

Information, buildings keys and access cards relating to any business activities must be located securely to protect them from unauthorised physical access and damage.

This policy applies to:

- All buildings, sites and locations used by the company regardless of whether they are owned/leased or not.
- All company employees, including temporary and agency workers, independent consultants and contractors.
- Suppliers/contractors responsible for handling any client premise information, keys or access cards.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact your line manager in the first instance.

In adhering to these standards, employees must not put themselves at personal risk.

The following policies should be read in conjunction with this policy:

- Data Protection Policy
- IT, Email and Internet Usage Policy
- IT Secure Disposal Policy
- Information Security Policy
- Information Retention Policy

Areas of physical security

In much the same way we identify differing levels of information security, physical environmental security needs to be determined as well. The physical security requirements for areas will depend upon:

- The value and sensitivity of the information assets to be protected.
- Likely or associated security threats including guidance on national security and intelligence which can be subject to change on a regular basis.
- Existing safeguards and protective measures

The council has identified 4 such areas and the physical protection procedures required.

General office areas

These are the typical office areas that are normally accessible only to employees and admitted guests. Here, the value of IT assets is not excessive (usually desktop PCs and laptops) and access to sensitive information is closely controlled.

General office areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

Visitors must be supervised, and their name, company (if relevant), date and time of entry and departure, and person(s) visited must be recorded at all times. Visitors must only be granted access for specific, authorised purposes.

All employees issued with an identification badge **must** have it clearly on display when undertaking work duties in or out of company premises. Only issued corporate staff lanyards are to be used by permanent employees.

Support functions and equipment (for example, photocopiers, fax machines, printers) must be sited to minimise the risks of unauthorised access or compromise of information.

Sensitive areas

These are also typical office environments which may contain desktop PCs and laptops. However, the sensitivity of the information contained within carries greater risk if lost or removed without authority. This could include keys to client premises etc.

Sensitive areas must be protected by appropriate entry controls to ensure that only authorised employees are allowed access.

Authorised employees are classified as those who have undergone security clearance and vetting, and their roles requires them to have access.

Visitors must be supervised, and their name, company (if relevant), date and time of entry and departure, person(s) visited, and the purpose of the visit recorded. Visitors must only be granted access for specific, authorised purposes such as independent auditing on behalf of the SIA.

Sensitive areas must be physically locked when not in use.

Equipment siting

Workstations displaying sensitive data must be positioned to reduce the risk of overlooking.

Where possible, IT equipment must be sited or protected to reduce risks from unauthorised access, theft, and environmental hazards such as fire, flood, dust, chemicals, electromagnetic interference, and loss or fluctuation of power supply.

Doors

External doors should provide some resistance to forced attack and have a minimum of three locks. Keys to external doors are to be held under secure conditions but should be readily accessible to authorised persons.

Emergency Exits

There is often a conflict between demands for security and those of safety when it comes to securing emergency exits. Most emergency exit locks, including those of bar release type, are not fully secure and emergency exits should normally be fitted with intruder detection devices.

Windows

Basement, ground floor and other windows that are readily accessible should have secure fittings. Window catches should be regularly examined, and defective catches replaced. Security grills should be installed for windows in sensitive areas.

Any window or opening described here must be closed and secured when the room or area it could access is unoccupied.

Fire and Flood Prevention

Fire Prevention

The following is a checklist of the various precautions that may be taken against fire:

- Doors should be fire-resistant and equipped with automatic closing devices.
- Back up and other magnetic media should be stored in special fire-resistant rooms or cabinets or stored at another location.
- Automatic smoke and heat detection systems must be installed in server rooms.
- Hand-held fire extinguishers of appropriate type should be mounted at strategic places.
- All employees must be trained in what to do in the event of a fire and fire drills held on a regular basis.
- Schedules should be established for regular inspection and testing of all equipment.
- Cleaning compounds and combustible material must be disposed in fireproof rubbish containers.

Flood prevention

Water damage can easily ruin computers, putting the organisation out of business for a long time. The following is a checklist of the various actions that may be taken as a precaution against flooding:

- Information systems should not be located in areas liable to flooding.
- The floors above the information systems should be sealed to prevent damage.
- Water sprinkler systems should be arranged to minimize damage.
- Where appropriate, pumps and a water/vacuum cleaner should be available to remove water accumulation.
- Electrical hook-up points should be placed at least 10cm above the floor to avoid short-circuiting in case of water leakage.
- Ready access to the main water stopcock should be possible and responsible officers be made aware of where it is.

Security of equipment off premises

Security procedures and controls must cover the security of equipment used outside company premises. IT equipment used outside company premises to support business activities must be subject to the equivalent degree of security protection as office equipment.

The following must be applied:

- When travelling, equipment (and media) must not be left unattended in public places.
- Laptops must be carried as hand-baggage when travelling.
- Laptops must not be left unattended in vehicles.

- Laptops and mobile telephones are vulnerable to theft, loss or unauthorised access when travelling. They must be provided with an appropriate form of access protection (for example, passwords or encryption) to prevent unauthorised access to their contents.

Clear Desk Policy

Employees are required to adopt a clear desk policy to reduce the risks of unauthorised access, loss of or damage to information.