**Physical Security Policy**

* 1. **Overview**

In order to comply with elements of law (Data Protection, Computer Misuse acts etc.), Central Government and industry best practice, (Information Management etc.) and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Government Connect secure network, access to ***<Company Name>’s*** equipment and information must be protected.

The aim of this policy is to prevent unauthorized access to both physical and electronic information. In summary, the policy requires the following to be protected: 

* Sensitive paper records
* IT equipment used to access electronic data
* IT equipment used to access the Council network

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the ***<Company Name>’s*** IT data center. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorized access. Each department is responsible for assessing the level of protection required for their teams and locations.

* 1. **Policy Statement**

The purpose of this policy is to establish standards in regard to the physical and environmental security of the ***<Company Name>’s*** information. All ***<Company Name>’s*** employees, contractors and users with access to ***<Company Name>*** equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the ***<Company Name>***’***s*** equipment and the information that they use or manipulate.

* 1. **Scope of the Policy**

This policy applies to all users of the ***<Company Name>’s*** owned leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to the organization 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 organization’s information.

* 1. **Secure Areas**

Critical or sensitive information must be stored in secure areas protected by appropriate security controls. A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored. Examples of secure areas for protection are:

* A room with sensitive paper based information, 
* A machine room containing IT fileservers.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there, these could include: 

* Alarms fitted and activated outside working hours 
* Window and door locks 
* Window bars on lower levels 
* Access control mechanisms fitted to all accessible doors (where codes are utilized they should be regularly changed and known only to those people authorized to access the area / building) 
* CCTV cameras 
* Staffed reception area 
* Protection against damage e.g. fire, flood, vandalism

As an example, access to secure areas such as the data center and IT equipment rooms, must be adequately controlled and physical access to buildings should be restricted to authorized persons. Staff working in secure areas should be ready to challenge anyone not known to them and/or not wearing a badge. Each department must ensure that doors and windows are properly secured.

Badges, keys, (should be signed for/regularly audited) entry codes etc. must only be held by officers authorized 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 and are required to wear an identification badge. An IT/IS 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 keys, badges etc. should be recovered from the staff member and any door / access codes should be changed immediately.

* 1. **Paper Based Data Security**

Paper based (or similar non-electronic) information must be assigned an owner and a classification If it is classified as personal or confidential, information security controls to protect it must be put in place. A risk assessment should identify the appropriate level of protection for the information being stored. Paper in an open office must be protected by the controls for the building in Section 1.4 and other appropriate measures that could include: 

* Filing cabinets that are locked with the keys stored away from the cabinet 
* Locked safes 
* Stored in a Secure Area protected by access controls
  1. **Equipment Security**

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

* Reduce risks from environmental hazards, for example, heat, fire, smoke, water, dust and vibration. 
* Reduce the risk of theft, for example, if necessary items such as laptops should be physically attached to the desk 
* Facilitate workstations handling sensitive data being positioned so as to eliminate the risk of the data being seen by unauthorized people.

Desktop PCs must not have data stored on the local hard drive; data must be stored on the network file servers. This ensures that information lost, stolen or damaged via unauthorized access can be restored with its integrity maintained. Information concerning network drives and the appropriate place to store Council information can be found on the intranet.

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 authorization from Information Services.

All items of equipment must be recorded on an inventory, both a Departmental and the Information Services inventory. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of. All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the inventories.

* + 1. **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.

* + 1. **Equipment Maintenance**

Information Services, all department’s representatives and third party suppliers must ensure that all of ***<Company Name>*** 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 must: 

* Retain all copies of manufacturer’s instructions 
* Identify recommended service intervals and specifications 
* Enable a call-out process in event of failure 
* Ensure only authorized 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, for example HP servers are under a support and maintenance agreement.

* + 1. **Security of Equipment off Premises**

Your line manager must formally approve the use of equipment off-site. Equipment taken away from organization’s premises is the responsibility of the user and must: 

* Be logged in and out 
* Not be left unattended 
* Concealed whilst transporting 
* Not 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 encrypted if carrying personal or confidential information 
* Be password protected 
* Be adequately insured

Users should ensure, where necessary and required that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the IS Department and the Insurance Section (if applicable), losses or damage to equipment must be recorded in the inventories.

Staff should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act.

* + 1. **Secure Disposal or Re-use of Equipment**

Equipment that is to be reused or disposed of must have all of its data and software removed/destroyed. If the equipment is to be passed onto, another organization (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools.

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

All equipment being disposed of must be prepared for release within the mandated criteria of ***<Company Name>*** recycling policies.

* + 1. **Delivery and Receipt of Equipment into the *<Company Name>***

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

* An authorized individual using an auditable formal process must sign for equipment deliveries. This process should confirm that the delivered items correspond fully to the list on the delivery note. 
* Loading areas and holding facilities should be adequately secured against unauthorized access and all access should be auditable. 
* Subsequent removal of equipment should be via a formal, auditable process.
  1. **Policy Compliance**

If you are found to have breached this policy, you may be subject to the ***<Company Name>’s*** disciplinary procedure. If you have broken the law, you may be subject to prosecution. If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Services Department.

**Source:** [**http://modgov.sefton.gov.uk/moderngov/Data/Cabinet%20Member%20-%20Corporate%20Services%20(meeting)/20080305/Agenda/Item%2004A.pdf**](http://modgov.sefton.gov.uk/moderngov/Data/Cabinet%20Member%20-%20Corporate%20Services%20(meeting)/20080305/Agenda/Item%2004A.pdf)