London Borough of Enfield

Physical and Environmental Security Policy
CONTENTS

1. Purpose ................................................................................................................ 3
2. Introduction ......................................................................................................... 3
3. Physical Security Areas ...................................................................................... 3
   3.1. Public Areas ................................................................................................. 4
   3.2. General Office Areas ................................................................................... 4
   3.3. Sensitive Areas ............................................................................................ 4
   3.4. Secure Areas ................................................................................................ 5
4. Equipment Siting & Protection ........................................................................... 6
5. Buildings - External Physical Security ............................................................... 6
   5.1. Security Lighting ......................................................................................... 6
   5.2. Doors ........................................................................................................... 6
   5.3. Emergency Exits .......................................................................................... 7
   5.4. Inter-Communicating Doors ........................................................................ 7
   5.5. Windows ...................................................................................................... 7
   5.6. Other Access Points ..................................................................................... 7
   5.7. Public Utilities ............................................................................................. 7
   5.8. Delivery and Loading Areas ........................................................................ 8
   5.9. Perimeter Fence ........................................................................................... 8
6. Fire & Flood Prevention ..................................................................................... 9
   6.1. Fire Prevention ............................................................................................ 9
   6.2. Flood Prevention ......................................................................................... 10
7. Power supplies .................................................................................................. 10
8. Cabling Security ................................................................................................ 11
9. Supporting Utilities ........................................................................................... 11
10. Access Controls ............................................................................................. 11
   10.1. ID Card/Pass System .............................................................................. 11
   10.2. Visitors ................................................................................................... 12
11. Security of Equipment Off Premises ............................................................. 12
12. Security of Paper-Based Information ............................................................ 13
13. Clear Desk Policy .......................................................................................... 13
14. Disposal of Confidential Waste ................................................................. 13
15. Re-Use of Equipment .................................................................................. 13
16. Policy Compliance ......................................................................................... 13
17. Exceptions ...................................................................................................... 14
18. Penalties .......................................................................................................... 14
1. Purpose

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

The purpose of this document is to define the requirements for physical and environmental security that will be applied to maintain the confidentiality, integrity and availability of information and information systems supporting the business functions of the Council.

2. Introduction

Information processing facilities supporting Council business activities must be located within a secure area to protect them from unauthorised physical access and damage.

This policy applies to:

- all buildings, sites and locations used by the Council, whether or not owned by it
- all premises used by the Council’s partners to house any IT systems directly connected to Council resources
- All Council employees, including temporary and agency workers, independent consultants and contractors.
- Members
- Suppliers/contractors responsible for managing premises housing Council information systems, computer and network facilities.

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 the Council’s Information Security Officer.

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

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

- Acceptable Use Policy
- Access Control Policy
- Information Handling and Protection Policy
- Business Continuity Management Policy

3. Physical Security Areas

Just as it is essential to identify sensitive information, there is also the need to identify and accord appropriate levels of protection to different areas within buildings. The physical security requirements for areas will depend upon:
The value and sensitivity of the information and information assets to be protected
Likely or associated security threats and risks
Existing safeguards and protective measures
The Council has identified four such areas and the physical protection procedures required:

3.1. Public Areas
These are areas that are freely accessible to the public. Here, the value of IT assets is either low (usually a desktop PC in reception) or the assets are physically large (e.g. a self-service kiosk). Access to information may be unrestricted (e.g. to publicly accessible web pages) or for a designated individual (e.g. to enable a customer to pay their Council Tax bill).

All equipment not specifically for public access should be sited to minimise the risks of unauthorised access or compromise of information.

Publicly accessible systems used to display confidential information should be sited in such a way as to prevent another member of the public viewing the displayed data.

All publicly accessible kit should be appropriately defended against vandalism, modification and theft.

3.2. General Office Areas
These are the typical office areas that are normally accessible only to employees and admitted guests (including commercial/business people, members of the public, etc.) Here, the value of IT assets is not excessive (usually desktop PCs and laptops) and access to sensitive information (e.g. a specific individual’s council tax account, rent arrears reports, etc.) 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. Visitors must only be granted access for specific, authorised purposes

All employees are required to wear visible identification

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

3.3. Sensitive Areas
These are also typical office environments with desktop PCs and laptops. However, the sensitivity of the information processed is high (e.g. Child Protection Register, personal information).
Sensitive areas must be protected by appropriate entry controls to ensure that only authorised employees are allowed 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.

All employees are required to wear visible identification.

Employees supplying or maintaining support services will be granted access to sensitive areas only when required and authorised. Where appropriate, their access will be restricted and their activities monitored.

Sensitive areas must be physically locked outside office hours and checked periodically.

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

3.4. Secure Areas

These are communication rooms and computer rooms, rooms accommodating servers, etc. that support critical and/or sensitive activities, and areas housing vital information and documents that require a higher level of physical security compared to other operating environments.

Secure areas must have a higher level of physical and environmental security protection to minimise the possibility of damage from fire, flood, explosion, terrorism, and other forms of natural or man-made disaster. Officers must determine and designate the area(s) within their operating environment according to the above classification and ensure the relevant physical protection mechanisms are implemented.

Access will be controlled by an access control device, preferably one with an audit trail (i.e. something other than a key or a keypad). If such a device is not fitted then a manual log of entry and exit must be maintained.

When unattended, or where the support employees are remote, rooms should be kept locked and an access and egress log maintained.

The fire control system must meet BS6266 - Code of Practice for Fire Protection for Electronic Data Processing installations, and the following must be in place:

- appropriate sited and approved fire extinguishers
- fire alarms that are wired to the main building fire alarm system
- place smoke, fire, and unusual water flow detection devices that are regularly tested
All computer rooms should undergo cleaning of all surfaces at least every six months by personnel experienced in the cleaning of electronic equipment.

Where equipment requires environmental control, rooms must be air-conditioned with humidity set at 50-55% and temperature at 65°F. Means of monitoring the environment and an alarm on the conditioning equipment must be installed. All such environmental controls must meet the requirements of BS7083 - Recommendations for the Accommodation of Operating Environment of Computer Equipment.

4. Equipment Siting & Protection

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.

CCTV may be a useful aid to monitor the activities of the public/visitors in publicly accessible areas.

5. Buildings - External Physical Security

The physical security requirements for areas will, at least to some extent, depend upon the security classification of the areas that they contain.

5.1. Security Lighting

Security lighting can offer a high degree of deterrence to the potential intruder in addition to providing the illumination necessary for effective surveillance. The standard of lighting should, however, meet the minimum requirement and its installation be appropriate to the site conditions.

- Lighting which illuminates perimeter boundaries should be installed
- All dark and blind spots should be eliminated
- Under low light conditions lighting should be activated automatically
- Consideration should be given to illuminating roofs, fire escapes and emergency exits
- Lights installed should be resistant to interference

5.2. Doors

External doors should provide some resistance to forced attack. Keys to external doors be held under secure conditions but should be
readily accessible to authorised persons. External doors that are never used and which are not emergency exits should be bricked up or permanently secured.

External doors leading to areas other than public areas must have an unauthorised access control mechanism. These should normally be locked outside of normal working hours.

5.3. 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.

5.4. Inter-Communicating Doors

Doors communicating with other parts of a building designated as being of a different security classification in general provide a degree of security similar to that of external doors. Doors leading to sensitive or secure areas may need to be protected with intruder alarms.

5.5. 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. Intruder alarms should be considered for windows in secure or sensitive areas.

Where it is necessary to secure a window more effectively than by the use of lock, catch or bolt (e.g. secure areas), the use of bars, grilles or shutters should be considered along with the use of intruder detection sensors.

Double-glazing can provide excellent protection against covert attack and some protection against forced attack. It is unobtrusive, may draw less attention to a sensitive area and is more acceptable than bars or grilles. Double-glazing can also be alarmed.

5.6. Other Access Points

Roofs and roof doors should be periodically surveyed to see whether there is access on to them from adjoining buildings, nearby buildings, trees, fire escapes, window cleaning equipment, etc.

Access to the upper floors of a building or from the roof may often be afforded by way of rainwater or soil down-pipes. Such access may be restricted by boxing in the pipes or by treating them with anti-climb paint - this should be applied at heights above 8 feet to avoid accidental contact by passers-by.
5.7. Public Utilities

Gas, electricity and water supply installations within buildings may offer potential vulnerability access points. Where possible, cables and pipes within buildings should enter the building underground. Public service meters should, wherever possible, be so sited that access to them does not require entry into secure or sensitive areas.

5.8. Delivery and Loading Areas

At each site an isolated delivery and loading area is provided for supplies and equipment deliveries. It is sited to reduce the opportunities for unauthorised access to the working areas and secure offices. The following controls are implemented:

Access to a delivery and loading area from outside of the building is restricted to identified and authorised personnel.

The delivery and loading area is designed so that suppliers can be unloaded without delivery personnel gaining access to other parts of the building or location.

Where relevant, the external doors of a delivery and loading area are secured when the internal doors are opened.

Relevant employees are given advance notice of incoming deliveries. Any deliveries arriving without clear destinations or advanced warning are turned away.

Incoming material is inspected for potential threats before goods are moved from the delivery and loading area to the point of use.

Incoming material is registered on entry to the site.

Incoming and outgoing consignments are physically segregated where possible.

5.9. Perimeter Fence

Given that, in many cases, the public will have access to buildings, a perimeter fence is unlikely to be generally acceptable. However, as it does form a useful barrier and delay to the opportunist intruder it may be most appropriate to protect secure areas.

Where installed, the following features are desirable:

- Height of fence should be commensurate with degree of physical deterrence required.
- Access should not be possible under the fence, or through drains, culvert etc.
- The whole of the fence area should, wherever possible, be run in straight lines for ease of surveillance.
- The ground on both sides of the fence should be cleared to remove cover for an intruder.
• Anti-climbing devices such as barbed wire should be used on top of the fence.
• Perimeter Intruder Detection Systems (PIDS) may be used on perimeters to enhance the level of security offered by the fence.
• Likewise CCTV can be used to monitor the perimeter barriers and particularly gates.

6. Fire & Flood Prevention

6.1. 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.
• The air ducts which enter the computer room must be fitted with dampers, power vents or other means to prevent smoke entering from external fires
• All furnishing in the computer room should be non-combustible
• 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 computer rooms
• Computer rooms must be fitted with appropriate fire extinguishing equipment
• Signal panels must be designed and placed to make it possible to ascertain immediately where the smoke or fire has been detected
• Ensure that fire services are notified immediately when the fire alarm sounds
• 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
• All printed material must be removed from the computer rooms regularly.
6.2. 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
- Water detection and alarm systems should be installed under information systems
- Where appropriate, pumps and a water/vacuum cleaner should be available to remove water accumulation
- Electrical hook-up points should be placed at least 10 cm 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.

7. Power supplies

Information processing equipment should be protected from power failures or other electrical anomalies. A suitable electrical supply is to be provided that complies with the equipment manufacturers specifications. Options to achieve continuity of power supplies include:

- Multiple feeds to avoid a single point of failure in the power supply
- Uninterruptible power supply (UPS)
- Back-up generator

A UPS to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Contingency plans cover the action to be taken on the expiry of the UPS. UPS equipment is regularly tested in accordance with manufacturer’s instructions.

A back-up generator should also be available for equipment supporting critical business operations in order to continue any processing in case of prolonged power failure. Where generators are in place they should be regularly tested in accordance with the manufacturer’s instructions.

For further information on business continuity requirements, please refer to the Business Continuity Management Policy.
Lightning protection is applied to all buildings and lightning protection filters are fitted to external communications lines.

8. Cabling Security

Power and telecommunications cabling carrying data or supporting information services are protected from interception and damage.

Within Council office working areas, power and telecommunications lines into information processing facilities are hidden/underground and avoid routes through public areas.

Power cables are segregated from communication cables to prevent interference.

9. Supporting Utilities

All supporting utilities, such as electricity, water supply, sewage, heating, ventilation, air conditioning should be adequate for the systems they are supporting. Supporting utilities should be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

10. Access Controls

Control of entry into Council buildings, sites and locations is important for the security of our information systems (both computerised and manual) and their employees. Appropriate entry controls must be provided to ensure that only authorised employees are allowed access. This can best be achieved through an ID card/pass system. This system of access control must be rigidly enforced in buildings and areas housing sensitive information assets. In buildings where IT facilities are located and where there is public access, special measures for the enforcement of the access control system should be taken, particularly after normal office hours.

10.1. ID Card/Pass System

To be effective, the following needs to be observed:

- All employees (regardless of grade) and visitors are required to wear their identification badges
- All employees must immediately challenge people not wearing an ID card/pass
- To prevent tailgating, staff should be wary when considering the polite gesture of leaving the door open for person(s) to follow through, unless such person is seen to be wearing the appropriate ID card/pass
- ID cards should be safeguarded and if lost reported to Facilities Management.
• ID cards should be renewed if they become defaced or the photograph no longer resembles the bearer.
• ID cards must be returned to Facilities Management for deactivation when an employee leaves the Council.
• ID cards for temporary employees (included contractors, consultants, agency workers, maintenance employees) must be issued with an ID card that is visibly different to that for permanent employees. These should be issued for a limited period and not exceeding three months.
• ID cards for visitors should be visibly different from those of permanent and temporary employees, be valid only for the date of issue, bear the visitor’s name and be accounted for by a serial number. Visitors must be requested wear the ID Card in a visible fashion at all times whilst on the premises. Visitors must surrender the ID card to Reception on departure from the premises.
• All ID cards must be signed for when issued.

10.2. Visitors

As well as the above conditions relating to ID cards, holders of visitors passes must be escorted by the person visited (or their representative) from and to Reception.

Any person not wearing their ID card should be challenged. Tailgating (allowing a person without proper ID to follow through security doors) is not permitted.

11. Security of Equipment Off Premises

Security procedures and controls must cover the security of equipment used outside Council premises. IT equipment (regardless of ownership) used outside Council 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 and mobile telephones are vulnerable to theft, loss or unauthorised access when travelling. They must be provided with an appropriate form of access protection (e.g. passwords or encryption) to prevent unauthorised access to their contents.
• Removal of property belonging to Council must be authorised in writing by line managers.
12. Security of Paper-Based Information

The same standards of physical and environmental security that are applied to electronic based information should also be applied to paper based information.

Where appropriate, consideration should be given to using fireproof safes for storing ‘vital’ paper based information.

Paper based information should be processed and stored in secluded rooms. However, due to space restrictions, rooms/areas may be shared with other non-sensitive functions and effective physical controls will be difficult to achieve in such conditions. Wherever possible, sensitive information (paper based and electronic) should be processed and stored away from non-sensitive information, so they may be afforded appropriate levels of protection.

Filing cabinets and rooms holding sensitive paper based information, back up disks, video and audio recordings, should be locked outside normal working hours, unless auditable access controls are in place.

13. Clear Desk Policy

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

14. Disposal of Confidential Waste

Council information can be compromised through careless disposal and reuse of equipment.

All disposal of equipment and paper must follow the Confidential Waste Disposal policy.

15. Re-Use of Equipment

All items of equipment containing storage media (fixed or hard disks) are checked to ensure that any sensitive data or licensed software is removed overwritten before disposal.

All re-use of equipment must follow the Confidential Waste Disposal policy.

16. Policy Compliance

The Council expects that all employees will achieve compliance to the directives presented within this policy. This policy will be included within the Information Security Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.
17. Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

If complying with the policy would lead to physical harm or injury to a member of staff

If complying with the policy would cause significant damage to the company’s reputation or ability to operate

If an emergency arises

In such cases, the staff member concerned must take the following action:

Ensure that their manager is aware of the situation and the action to be taken

Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report

Ensure that the situation is reported to the ICT Security Analyst as soon as possible.

Failure to take these steps may result in disciplinary action.

In addition, the ICT Security Analyst maintains a list of known exceptions and non-conformities to the policy. This list contains:

Known breaches that are in the process of being rectified

Minor breaches that are not considered to be worth rectifying

Any situations to which the policy is not considered applicable.

The Council will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

18. Penalties

Non-compliance is defined as any one or more of the following:

Any breach of policy statements or controls listed in this policy

Unauthorised disclosure or viewing of confidential data or information belonging to the Council or partner organisation

Unauthorised changes to information, software or operating systems

The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body

The exposure of the Council or partner organisation to actual or potential monetary loss through any compromise of security
Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information security officer or senior management.

Any violation or non-compliance with this policy may be treated as serious misconduct.

Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.