London Borough of Enfield

Third Party Access and Management Policy
## Contents

1. **Purpose** .......................................................................................................... 3  
2. **Introduction** ..................................................................................................... 3  
3. **Accounts and Remote Access** ........................................................................ 4  
4. **User Account Creation and Naming Conventions** ........................................... 5  
5. **Physical Access** .............................................................................................. 6  
6. **Identification of risk related to external parties** ................................................ 6  
7. **Addressing Security when dealing with Customers** ......................................... 7  
8. **Third Party Service Delivery Management** ...................................................... 7  
9. **Changes to Council Systems** ........................................................................... 8  
10. **Security Policy Requirements** ......................................................................... 8  
11. **Staff Screening** ............................................................................................... 8  
12. **End Point Anti-virus and Malware Management** ............................................. 8  
13. **Security Incident Management** ....................................................................... 9  
14. **Information Confidentiality** ............................................................................ 9  
15. **Media Handling** ............................................................................................ 9  
16. **Removal of Property** ...................................................................................... 10  
17. **Clear Desk and Clear Screen Policy** ............................................................... 10  
18. **Use of Council Internet and e-mail Systems** .................................................. 10  
19. **Audit and Monitoring** .................................................................................... 10  
20. **Policy Compliance** ......................................................................................... 10  
21. **Exceptions** .................................................................................................... 10  
22. **Penalties** ....................................................................................................... 11
1 Purpose

This policy aims to ensure that access to Council facilities, systems and information assets by third parties is appropriately controlled so that confidentiality, integrity, availability and accountability of information remain intact.

Any loss, compromise or misuse of Council information systems or information assets, however caused, could have potentially devastating consequences for the Council, could impact on the services the Council is responsible for providing, and could result in legal action or financial loss.

Access to Council systems, facilities and information by third parties poses a potential threat to the Council and as such needs to be controlled.

2 Introduction

A third party is an organisation or individual (non-permanent employee) external to the Council. This will include:

- Customers
- On-site contractors
- Agency staff
- IT and building facility suppliers
- Service providers, suppliers, partners

The policy covers the following aspects of third-party relationships:

- Third party risk assessments
- Contracts
- Network service provision
- Authorisation of connections
- Security of access by non-permanent employees (both physical and logical)

It is applicable to all Council activity, locations and employees and includes all Council information assets and infrastructure.

Compliance with this policy is required for all Council employees responsible for negotiation, initiation, authorisation, implementation and maintenance of third-party relationships and services pertaining to the Council.

Factors relating to:

- Legal and regulatory requirements
- Contractual obligations
- Security policy requirements
- Information governance requirements
- Network operations must be identified, understood and approved via a risk assessment.

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

Third Party Access and Management Policy.docx

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.
• Acceptable Use Policy
• Access Control Policy
• Information Classification and Handling Policy
• Code of Conduct for Council Staff
• Information Security Policy

3 Accounts and Remote Access

All account and access management will adhere to the Access Control Policy.

Access to LBE systems, and systems used to manage LBE systems, will only be granted based on defined operational roles.

All role-based access will provide the minimum access and privileges required to perform the responsibilities required of the designated role.

Access will only be granted on confirmation (or approval) by direct line-management and by the role-owner (if applicable) that the user has been assigned to the identified role.

Changes to role-based access (i.e. affecting all persons within that role) must be made via a formal change control, and be approved by the role-owner, and all affected account managers.

Allocation, modification, deactivation/reactivation or removal of role-based access will only be processed as part of the following processes:

• Employee Life-Cycle Management Process (for starters, movers, and leavers)
• Security Event/Incident Management Process (e.g. for loss of access tokens, account compromise, account inactivity, abnormal account usage)
• User Provisioning Process (for user accounts only)
• Formal Change Request (for other access changes, e.g. those required as part of system change, commissioning and decommissioning).

In the case of support accounts all access will be granted for the minimum period required to execute duties as outlined as part of an incident response or pre-planned piece of work. Details of such duties must be submitted prior to approval of access if the work is pre-planned or included in the incident record if in response to an incident call.

User access to LBE systems, and systems used to manage LBE systems, will only be allocated at the user-level (i.e. access will not be granted based on IP address or other non-user-based identification).

All access will be revoked once the access is no longer required – this will be carried out by the disabling of accounts within Active Directory.

All user accounts will conform to LBE account and password standards.

Support accounts will be granted to personnel for individual use only – no generic shared accounts will be authorised, unless the third party is able to produce a full audit record of users who are accessing LBE systems remotely and only after approval by the ICT Security Analyst or other nominated LBE or Enfield IT member of staff in their absence.

Allocation of accounts (and associated tokens) will be recorded, and a scheduled review of account will be performed to ensure that all accounts are still required.
Initial passwords will conform to relevant password standards and be changed by the user at first use.

User accounts will be disabled/deactivated for a set period prior to deletion to enable consistency with current audit and protective monitoring activity.

User accounts will be disabled after a pre-defined and agreed period of inactivity.

Records will be made of all account, and account access modifications, deactivations, and deletions.

All 3rd-party, contractor and temporary accounts will be flagged (or named) to allow easy identification (as per section 4 of this document).

All account management activities will be performed by a designated team(s) within service delivery or CIT departments.

All third parties must have accepted and agreed to the Acceptable Use Policy as well as reading and accepting any role-specific security responsibilities, before the account can be used.

All third parties must confirm that they understand their responsibilities for maintenance of the account and password/token, and that they understand the relevant processes and procedures around the management and maintenance of the account, before the account can be used.

Passwords and account resets must only be performed upon verification of the users’ identity.

All remote access will be via 2-Factor authentication made via Microsoft MFA, RSA or Secure Envoy Token.

4 User Account Creation and Naming Conventions

3rd-party accounts are to take the following naming convention forms:

- 3XXX-<username> {for non-administrative accounts}
- 3XXX-ad-<username> {for administrator accounts}
- 3XXX-da-<username> {for domain administrator accounts}

Where XXX is a 3-letter organisation code representing the 3rd-party (e.g. CAN for Canon), and <name> is the username as per the Active Directory Design Document. Where multiple organisations have the same initial 3 letters then the 3rd-letter will be replaced by a single incremental digit (e.g. CA2) or, at the discretion of the ICT Security Analyst, an alternate code (that should be documented as referring to the third party in question during the account creation process and noted in the comments field of the user).

In circumstances where generic accounts are permitted the account name must include a pre-fix identifier of ‘GEN’ or ‘EX’ that shows the account is generic, for example:

- GEN-LaganTraining01
- 3CAN-GEN-Support01
- EX-Northgatehousing

The following information fields in Active Directory MUST be entered for all accounts:

- User Name
- Full Name
- Email Address
- Administrator(s)
• Given Name, Surname. If the person is not known by their given name, the name by which they are known must also be recorded
• Manager (name of the direct line manager), see below
• Department
• Organisation information
• Contact phone number
• Contact e-mail address
• Information/Details (see below)
• Flag indicating if the account is a contractor or permanent member of staff

For 3rd-party accounts, the line manager information must be the primary 3rd-party contact point (and not necessarily the line manager of the person).

The information/detail will include the following:
• For user accounts it will include the service desk request identifier from which the account was requested
• For support/3rd-party accounts it will include information around which systems are being supported by this account

5 Physical Access

Should any third party require physical access to any area deemed business critical (that could include any of the following: communications rooms, server rooms or document storage facilities) they must be accompanied by a member of LBE staff or personnel responsible for maintaining that business area (for example, a member of the Enfield IT network team when a third party requires access to a communications room).

In circumstances where this is not possible approval for access should be sought from the ICT Security Analyst or other nominated LBE or Enfield IT member of staff in their absence.

Should access be required in an emergency, approval for access can be made by Facilities Management, Architectural Services or the Building Controller.

At all times an audit log of entry should be kept (this can be in the form of electronic entry monitoring or physical logbook held at the location).

Access to rooms where locked communications and server cabinets are located can be made without the need to consult Enfield IT as long as entry audit logs are maintained.

6 Identification of risk related to external parties

Where there is a requirement for a third party to access Council facilities, information or information systems, a security risk assessment shall be conducted by the ICT Security Analyst to identify any additional security requirements or additional controls required. The risk assessment shall be performed before the granting of additional services/connectivity and should take into account the following issues:

• The information processing facilities the third party is required to access
• The type of access required to information and information processing facilities, for example:
  • Physical access (computer rooms, cabinets, offices, etc)
• Logical access (database, general information)
• Network connectivity between the Council and third party (e.g. permanent connection, remote access)

• Value and sensitivity of the information to the Council and its operations
• What controls are deployed by the third party for storing, processing, communicating and sharing information belonging to the Council
• Security measures employed by the third party
• Contractual obligations and legal/regulatory compliance requirements
• Security management controls, including compliance with client security policies, confidentiality agreements
• Practices and procedures to deal with information security incidents
• Ownership of software and information must be clearly defined.

7 Addressing Security when dealing with Customers

The following terms should be considered to address security before giving customers access to any of the Council’s information and information assets.

• Asset protection, including:
  • Procedures to protect the organisation’s assets, including information and software
  • Management of known vulnerabilities
  • Procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred
  • Integrity
  • Restrictions on copying and disclosing information

• Description of the product or service to be provided
• The different reasons, requirements and benefits for customer access
• Access control policy, covering:
  • Permitted access methods, and the control and sue of unique identifiers such as user IDs and passwords
  • An authorisation process for user access and privileges
  • A statement that all access that is not explicitly authorised is forbidden
  • A process for revoking access rights or interrupting the connection between systems
  • Arrangements for reporting, notification, and investigation of information inaccuracies (for example: of personal details), information security incidents and security breaches

8 Third Party Service Delivery Management

The Council will nominate an individual to liaise with appropriate third parties to ensure that services are being operated in accordance with service level agreements and that any security incidents affecting the Council are reported in a timely manner. The nominated representative should consider the following:

• Monitoring the service level performance
• Review of appropriate service reports provided by the third party
• Agreement of regular meetings to discuss service agreements, performance, adopting of Council policies and procedures
• Problem identification and resolution including any disputes
• As part of the information security schedule, all third-party services will be subject to an annual risk assessment of services provided.

9 Changes to Council Systems
Changes to Council information systems by third parties must adopt the Council’s change control process. The Information Security Manager and Change Manager must address any changes to services and the security consequences of such changes.

10 Security Policy Requirements
All third parties must follow the following information security requirements. These set out the security measures that must be implemented and maintained by the Council in relation to all aspects of information security and all associated supporting processes. They determine the minimum level of security the Council requires to be achieved by the third party.

All third parties must ensure that they do not breach any of the information security management system statements at any time during their contract with the Council.

11 Staff Screening
Confirmation of identity and qualifications of permanent, temporary or contact staff, when requiring access to Council buildings, systems and information, is the responsibility of all third parties. In addition, the third party is responsible for ensuring that all permanent, temporary or contract staff sign a confidentiality/non-disclosure agreement that protects the confidentiality of Council information, and information provided to the Council by other third parties.

The Council reserves the right to request that third parties provide the appropriate evidence to show that the activities have been undertaken and also to undertake occasional audits of agencies to verify that adequate checks are taking place.

12 End Point Anti-virus and Malware Management
All workstations, desktop computers and servers with access to the Council’s network must be installed with appropriate and virus software, active and kept up to date. This includes all third party’s own equipment.

The responsibility for the provision of antivirus measures for Council owned assets should be clearly established.

Laptop users and third-party staff who use PCs for work off site must be supplied with virus detection software and regular updates.

Any employee or third party who attempts to disable, defeat or circumvent applicable security controls will be subject to immediate dismissal or contract termination.

All virus outbreaks infecting the Council environment must be reported immediately to the ICT Service Desk.

Any PC or laptop that might be infected by a virus must be disconnected immediately from all Council networks. Infected machines may not be reconnected to the network until security administrators can verify that the virus has been removed.
13 Security Incident Management
All third parties are required to report any potential or actual breach of security affecting Council information or information systems. A breach of security is unauthorised access to premises, information and information systems connected with the Council.

Examples of possible security incidents may include, but not limited to:

- Loss or theft of computer equipment
- Inappropriate use of the Internet
- Unauthorised access to a Council information system
- Virus outbreak

Any third party who becomes aware of a security breach or attempted breach of Council information or information systems must report it immediately to the relevant system administrator and copy to the Information Security Officer and/or designated security personnel.

The Council will investigate all security breaches.

The Information Security Manager will collate information about security incidents and ensure trends are analysed, so that further controls can be implemented if required.

14 Information Confidentiality
All third parties are required to handle Council information in accordance with the Information Handling and Protection Policy. In particular, employees shall not discuss or disclose Council information with any non-Council employee or third party without explicit authorisation from the Council.

All third parties will sign confidentiality/non-disclosure agreements integrated within their contract of employment with the Council and/or third-party organisation.

All information developed by or on behalf of the Council will remain the property of the Council and shall in no way be sold, copied or used without the express permission of the Council or authorised designate.

15 Media Handling
To protect information from loss, unauthorised disclosure and loss of integrity, all third parties are to create all Council documents and records under version control and adhere to the council’s AUP, including the statements on clear screen and desk policy. Where appropriate, the document should also contain a security classification in line with the Council’s security classification scheme as documented in the Information Classification and Protection Policy.

All media used for data import, export and storage shall be clearly labelled; this includes but is not limited to back up tapes, CDs and USB storage devices.

All media containing Council information that is transported off site must be encrypted to AES 256 bit standard as a minimum and stored in a suitable container. Media that is to be posted should be put into a suitable disk mailer envelope and then into a padded envelope.

Advice should be sought from the ICT Security Manager if there are any doubts as to the validity of encryption methods or media being used to transport data.
Media containing council information shall be disposed of securely either by physical
destruction of the paper or media or by secure erasure of stored data using methods
documented in the council’s Confidential Waste Disposal Policy.

16 Removal of Property

No equipment (hardware or software) shall be removed from Council premises by a
third party without prior written authorisation from the appropriate Council manager.

17 Clear Desk and Clear Screen Policy

A Clear Desk Policy must be adopted for all third parties encountering Council
information.

Further guidance can be found in the Acceptable Use Policy.

18 Use of Council Internet and e-mail Systems

All electronic mail messages composed, sent or received using Council systems
remain the property of the Council.

Third parties with access to the Council’s Internet systems and e-mail systems must
adhere to the Council’s Internet and e-mail Usage Policy (included in the Council’s
Code of Conduct).

Further guidance can be found in the Acceptable Use Policy.

19 Audit and Monitoring

The Council has deployed comprehensive security systems with the capability of
monitoring and recording all Internet and e-mail usage. The Council reserves the
right to monitor and intercept any e-mail activity over its network for any of the
following reasons:

- Record keeping
- Checking compliance with regulations and appropriate Council policy
- Quality control and staff training
- Preventing or detecting crime
- Investigating or detecting the unauthorised use of e-mail
- Checking for viruses or other threats to the system

In addition, Council employees have the ability to inspect any information processed
and stored on the Council network or local disk storage by third parties.

20 Policy Compliance

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

21 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 Information security officer 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.

22 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 ICT Security Analyst 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.