Technical Security Policy

We are One Council We are Winners We take Responsibility

We Dare to be Different We are Proud

www.doncaster.gov.uk

Doncaster
Metropolitan Borough Council

Technical Security Policy

Contents

1. Introduction

The Council has an obligation to collect and process information about people with whom it deals. These include current, past and potential employees, suppliers and clients/customers of services provided to and by the Council.

In addition, it is crucial that business information gathered is available at all times to ensure the Council can function efficiently and provide effective services to its customers.

Principle seven of the Data Protection Act 1998 makes it mandatory for the Council to take appropriate measures against unauthorised and unlawful processing of personal data and against accidental loss, destruction of or damage to personal data.

The International Standard for Information Security, ISO 17799:2005, defines controls that must be implemented to ensure the full security of all types of information held by the Council.

2. Scope

This policy identifies the controls necessary to ensure the requirements of the Information Security standard, ISO 17799:2005, are applied that ensure the Council controls access to its information, equipment and buildings and puts measures in place to protect against unauthorised access.

This policy is primarily aimed at the central ICT function within Information and Communication. However, there will be elements of the policy that will apply to system administrators throughout the Council.

3. Aims of the Policy

The aims of the Policy are to:

- define the criteria and controls that must be applied throughout the Council to ensure the technical and physical security of information and processing equipment
- ensure the required processes are identified and implemented to ensure the security of both information and the equipment used to process it
- identify the responsibilities in complying with the requirements of the International Standard for Information Security, ISO 17799:2005, and other relevant legislation, for example, the Data Protection Act 1998

4. Responsibilities

Information and Communication members of staff are responsible for ensuring that the technical procedures are implemented to safeguard the Council's information and equipment in line with this policy and the standard for information security, ISO 17799.

5. Management and Security of Assets

To ensure the security of the Council's assets, measures must be implemented to prevent unauthorised physical access, damage or interference to the Council's information, software, equipment and premises.

There are many types of assets, including:

- information e.g. databases, contracts, agreements, system documentation, user manuals, business continuity plans, audit trails
- software e.g. application software, development tools, system software
- physical e.g. computer and communications equipment, removable media
- services e.g. computing and communications services, general utilities
- people and their qualifications, skills and experience
- intangibles such as reputation and image of the organisation.

All assets should be accounted for and have a nominated owner. Assets should be clearly identified and an inventory of all important assets drawn up and maintained. The asset inventory should include all information necessary in order to recover from a disaster, for example:

- type of asset
- format
- location
- backup information
- license information.

Rules for the acceptable use of information and assets associated with information processing are documented within the **Acceptable Use Policy**, **E-mail Usage Policy** and **Internet Usage Policy**. Specific guidance should be specified, documented and implemented by the relevant departments.

6. Physical and Environmental Security

Secure Areas

To prevent unauthorised physical access, damage and interference to the Council's premises and information, critical or sensitive information processing facilities should be housed in secure areas.

Any area housing critical or sensitive information processing facilities should be designated as a secure area and should be protected by a secure perimeter with appropriate entry controls and security measures.

The entry controls and security measures should ensure that access is properly authorised and should adhere to the following:

- employees of the Council, including support staff who are authorised.
- persons who are not employed by the Council should have their details recorded and be supervised

Security Perimeter

All secure areas are to have a security perimeter, which shall be:

- clearly defined and should be sited depending on security requirements identified as a result of a risk assessment
- physically sound with control mechanisms, bars, alarms and locks, where applicable, in place

and shall have

- a staffed reception area, or employ other means, to control physical access to the secure area
- restricted access to authorised personnel only
- physical barriers which extend from the real floor to real ceiling to prevent unauthorised entry and environmental contamination such as that caused by fire and flooding
- fire doors, which are alarmed and slam shut.

Entry Controls

Secure areas are to be protected by appropriate entry controls to ensure that only those personnel who should have access are allowed access.

The following should be adhered to:

- visitors to secure areas are to be supervised or cleared and their date and time of entry and departure recorded. They are only to be granted access for specific**,** authorised purposes and should be issued with instructions on the security requirements of the area and on emergency procedures
- access is to be controlled and restricted to authorised persons only
- an audit trail of all access is to be securely maintained
- all personnel shall be required to wear some form of visible identification and be encouraged to challenge unescorted strangers and anyone not wearing visible identification
- access by third party support service personnel must be authorised and monitored and, where appropriate, supervised
- access rights to secure areas are to be regularly reviewed and updated
- access points such as delivery and loading areas where unauthorised persons may enter must be controlled.

Security Measures

Security measures must be implemented to physically protect processing facilities against damage from fire, flood, explosion and other forms of disaster.

To achieve the required level of security the following controls are also to be implemented:

- buildings that host significant ICT infrastructure or host processing of personal information should not advertise that fact
- support functions and equipment, e.g. photocopiers, fax machines, are to be sited appropriately within the secure area to avoid any demands for access which could compromise information confidentiality
- doors and windows are to be locked when the secure area is unattended
- windows are to be properly protected, particularly at ground level
- suitable intruder detection systems, covering all external doors and accessible windows, are to be installed to professional standards and regularly tested
- unoccupied areas are to be alarmed at all times

- hazardous or combustible materials are to be stored securely at a safe distance from a secure area
- bulk supplies such as stationery are not to be stored within a secure area until required
- fallback equipment and back-up media are to be sited at a safe distance to avoid damage from a disaster at the main site.

Working in Secure Areas

Physical protection and guidelines for working in secure areas should be designed, documented and implemented. Consideration must be taken to include:

- informing personnel of the controls that are in place regarding working in secure areas
- working out of normal business hours and requiring access to IT facilities must be authorised in advance
- unsupervised working in secure areas is not to be allowed both for safety reasons and to prevent opportunities for malicious activities
- vacant secure areas are to be physically locked and periodically checked.

Equipment Security

Controls must be documented and implemented to prevent loss, damage, theft or compromise of equipment.

The following guidelines should be considered to protect equipment from physical and environmental threats:

- equipment should be sited to minimise unnecessary access into work areas
- information processing facilities handling sensitive data should be positioned with the viewing angle restricted to prevent unauthorised viewing of the information
- controls should be implemented to minimise the risk of potential physical threats e.g. theft, fire, smoke, water, electrical supply interference
- environmental conditions such as temperature and humidity should be monitored
- lightning protection should be installed in buildings that contain processing facilities
- power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage
- equipment should be correctly maintained to ensure its continued availability and integrity
- security should be applied to off-site equipment taking into account the different risks of working outside the Council's premises.

Disposal or Re-Use of Equipment

All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Procedures must be implemented to ensure:

- devices containing sensitive information are either physically destroyed or the information destroyed, deleted or overwritten using techniques to make the original information non-retrievable
- information cannot be compromised through careless disposal or re-use of equipment
- media containing Council information or data, regardless of format e.g. paper, CD, is disposed of in a confidential manner
- media containing sensitive information is stored and disposed of securely and safely, e.g. by incineration or shredding, or erased of data for use by another application
- media for use by another application within the Council is emptied of data
- disposal of sensitive items is logged where possible in order to maintain an audit trail
- where appropriate, inventory of equipment is updated.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.

7. Communication and Operations Management

Operating Procedures

The operation of information processing facilities must be correct and secure.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development and maintenance of appropriate operating procedures.

The operating procedures should specify detailed instructions for the execution of each job including:

- processing and handling of information
- backup
- scheduling requirements
- instructions for handling errors or other exceptional conditions which may arise during job execution
- support contacts in the event of unexpected operational or technical difficulties
- special output or media handling instructions e.g. use of special stationery
- system restart and recovery procedures
- the management of audit-trail and system log information.

All operational faults must be recorded and corrective action taken.

Faults reported by users regarding problems with information processing or communications systems must be logged and dealt with in accordance with a defined and documented policy which includes:

- the review of fault logs to ensure that faults have been satisfactorily resolved
- the review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorised.

Change Management

Changes to information processing facilities and systems should be controlled. Operational systems and application software should be subject to strict change management control. The following should be considered:

- identifying and recording of significant changes
- planning and testing of changes
- impact assessments should be carried out
- formal approval procedures
- communication of change details to all relevant parties
- procedures for aborting and recovering from unsuccessful changes
- audit log identifying all relevant information.

Separation of Development, Test and Operational Facilities

Development, test and operational facilities should be separate to reduce the risk of accidental change or unauthorised access to operational software and business data.

The following controls are to be applied:

- rules for the transfer of software from development to operational status are to be defined and documented
- development and operational software, where possible, should be run on different computer processors, or in different domains or directories
- development and testing activities are to be separated as far as possible
- compilers, editors and other system utilities should not be accessible from operational systems when not required
- different log-on procedures are to be used for operational and test systems with users instructed to use different passwords for these systems and menus displaying appropriate identification messages
- sensitive data must not be copied into the test system environment
- development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Such passwords are to be changed after use.

Virus Protection

To protect the integrity of software and information, controls must be introduced to prevent, detect and remove malicious code.

Information & Communication must implement controls and procedures that will:

- load anti-virus software onto all PCs, laptops and relevant servers
- configure anti-virus software so that it is permanently active and cannot be deactivated by users
- protect the configuration facilities by password, which is limited to be on a need to know basis
- ensure the Council is aware of new viruses at the earliest opportunity
- update anti-virus software following the report of a new virus as soon as an update is available

- inform users as soon as possible that there is a new virus with instructions for dealing with the virus
- load all applications onto PCs or advise on the loading of applications onto PCs ensuring the media is properly virus checked and authorised for use prior to loading
- maintain a record of all viruses as reported by users
- review the record of reported viruses on a regular basis and implement the virus outbreak procedure where the pattern of viruses is a cause for concern.

Virus Outbreak Procedures

Where the record of reported viruses indicates the pattern of viruses is a cause for concern Information & Communication must take immediate action as follows:

- identify and isolate the equipment infected
- identify other potentially infected equipment (e.g. PCs sent e-mail from an infected PC)
- investigate the reasons for the infection
- take action to eliminate the infection and prevent re-infection
- document details of all investigations carried out and the resulting actions taken.

Information Back-Up

To maintain the integrity and availability of information and information processing facilities, routine procedures should be established to implement the agreed back-up policy and strategy.

These procedures must consider and, where appropriate, take account of the following:

- back-up copies of software should be taken on initial installation and following any subsequent upgrades
- back-up copies of essential business information should be taken regularly in accordance with a documented strategy
- back-up media and arrangements for individual systems must be regularly tested
- restoration procedures must be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery
- back-up copies together with accurate and complete records of the copies and documented restoration procedures should be stored in a remote location which is:
    - at a sufficient distance to escape any damage from a disaster at the main site
    - physically secure
    - protected from environmental hazards
- at least three generations or cycles of back-up information must be retained for important business applications
- back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements for business continuity plans
- the retention period for essential business information, and also any requirement for archive copies to be permanently retained, is to be established and documented.

8. Access Control

Information Access

Appropriate measures must be established, documented and implemented to ensure controlled access to information. These shall include:

- the business requirements for access to each type of information
- the access rules to be applied to each user or group of users
- the security requirements of each type of information or business area
- relevant legislation and any contractual obligations regarding protection of access to information
- standard user access profiles for common categories of job
- procedures for the management of access rights in a distributed and networked environment recognising all the types of connections available
- procedures to ensure personal and business information is not held on the ‘C’ drive of any PC. Where this is unavoidable, full security back ups of the information must be made regularly and retained away from the work area
- controls to ensure there is a consistency between information access controls and the different types of information, business areas, applications and networks.

Information Access Controls

Access controls must be established and be based on the premise 'What must be generally forbidden unless expressly permitted' rather than the weaker rule 'Everything is generally permitted unless expressly forbidden' and shall identify:

- controls that must always be enforced
- controls that are optional or conditional
- changes in user permissions that are initiated automatically by an information system
- changes in user permissions that are initiated by an administrator
- controls which require administrator or other approval before enactment, and, those which do not.

User Access Management

User access to applications, operating systems, networks and database management systems shall only be allowed where the user has been formally registered as a user and access shall not be provided until the authorisation procedure has been followed.

All users shall be allocated a unique user ID so that users are protected and also made responsible for their actions.

The registration procedure shall be as follows:

- all users and their level of access to be authorised in writing
- a record of all users and their level of access to be maintained
- users only to be granted access to those parts of the application, operating system or network where they have a demonstrable business need taking account of the classification of data being held or processed
- specific authorisation, from the appropriate Strategic Director or Headteacher, is obtained when the use of group ID’s cannot be avoided
- users to be given a written statement of access rights and conditions of access
- an annual check of all users to ensure access rights should continue
- the removal of access on leaving the business area.

Privilege Management

A privilege is any feature or facility which enables the user to override system or application controls. The allocation and use of privileges must be restricted and controlled.

The privilege management procedure shall be as follows:

- the privileges associated with each application, operating system, network and database management system, and the categories of staff to which they are to be allocated are to be identified and documented
- privileges should be allocated to individuals on a need-to-use basis and on an event-by-event basis, i.e. the minimum requirement for their functional role only when needed
- an authorisation process and a record of all privileges allocated should be maintained in accordance with the registration procedure detailed
- privileges must not be granted until the authorisation process is complete
- privileges are to be assigned to a different user identity from those used for normal business use
- privileges are to be reviewed every 6 months.

User Password Management

A formal password registration procedure must be implemented to ensure appropriate authorisation is obtained before creating and issuing passwords.

The system owners and system managers must issue passwords:

- to authorised users only
- to new users or users forgetting their password as a temporary password which they must change immediately
- only when they have been provided with positive identification of the user
- in a secure manner, this excludes the use of third parties and unprotected (clear text) electronic mail messages

Passwords should never be stored on a computer system in an unprotected form.

Passwords should never be published in user instructions and system documentation unless adequate controls are applied to protect the documentation

9. Network Access Control

Users are only to be provided with direct access to networks and network services after they have been specifically authorised to do so by the certifying officer (normally the Network Manager).

- the authorisation procedure shall be that detailed in the User Access Management referred to earlier in this policy
- the authorisation is to specify the networks and network services which the user is to be allowed to access
- the certifying officer must ensure that authorising the relevant information access controls are fully and correctly applied.

Network Controls

In addition to ensuring that only authorised users are able to access networks and network services, the following controls are also to be applied:

- all access by remote users is to be authenticated **(external connections)**
- connections to remote computer systems are to be authenticated **(node authentication)**
- access to diagnostic ports is to be secured **(diagnostic port protection)**
- a documented risk analysis is to be undertaken in respect of all networks and network services to determine, when taking account of the relevant information access control policies, whether or not to:
  - establish controls that restrict the route between a user terminal and the computer services the user is authorised to access (**enforced path)**
  - introduce controls within the network to segregate groups of information services, users and information systems **(network segregation)**.

External Connections and Node Authentication

Authentication methods include:
- cryptographic based techniques
- hardware tokens
- a challenge/response protocol
- dedicated private lines
- network user address checking facilities
- dial-back procedures.

Dial-back procedures must not be used with network services which include call forwarding or, if they are, the features must be disabled. Also the call back process must ensure that an actual disconnection occurs so as to prevent the remote user holding the line open and pretending that call back verification has occurred. Call back procedures and controls are to be thoroughly tested for this possibility.

Diagnostic Port Protection

Access to a dial-up remote diagnostic facilities is to be controlled in accordance with the **Third Party Access Controls** detailed below in this policy.

Enforced Path

An enforced path may be imposed by any of the following:
- allocating dedicated lines or telephone numbers
- automatically connecting ports to specified application systems or security gateways
- limiting menu and sub-menu options for individual users
- preventing unlimited network roaming
- enforcing the use of specified application systems and/or security gateways for external network users
- actively controlling allowed source to destination communications via security gateways, e.g. firewalls
- restricting network access by setting up separate logical domains, e.g. virtual private networks, for user groups within the organisation.

Network Segregation

Where it is decided to segregate networks they are to be divided into separate logical network domains each protected by a defined security perimeter. The perimeter is to be

implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. The gateway is to be configured to filter traffic between the domains and to block unauthorised access.

Shared Networks beyond the Organisational Boundary

Shared networks extending beyond the organisational boundary are to incorporate controls to restrict the connection capability of the users. Such controls are to be implemented through network gateways to enable traffic to be filtered by means of pre-defined tables or rules.

The restrictions applied should be based on the **Information Access Controls.**

Examples of applications to which restrictions should be applied are:

- electronic mail
- Internet access
- one-way file transfer
- both-ways file transfer
- interactive access.

Routing controls are also to be applied based on positive source and destination address checking mechanisms.

10. Information Systems Acquisition, Development and Maintenance

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services and user-developed applications.

Security requirements must be identified and agreed prior to the development and/or implementation of information systems.

Security controls must be specified in statements of business requirements for new information systems or enhancements to existing information systems.

Appropriate controls should be designed and documented into applications to ensure correct processing, for example:

- validation of data input to applications
- message integrity in applications must be authenticated
- validation of output data.

Procedures must be implemented to control the installation of software on operational systems.

Test data should be selected carefully, protected and controlled. Live data should not be used as test data.

Access to program source code should be restricted.

Where software development is outsourced or software packages are purchased, the following points should be considered:

- licensing arrangements, code ownership and intellectual property rights
- escrow arrangements in the event of failure of the third party
- contractual requirements for quality and security functionality of code
- testing before installation to detect malicious code.

11. Information Security Incident Management

A reporting and escalation procedure must be implemented to ensure all security events and weaknesses associated with information systems are processed in a timely manner.

All security incidents will be reported through the Helpdesk.

Security incidents will be assigned to the Information Management Team.

Information & Communication Information Management Team shall:

- monitor and update security incidents recorded on the Information & Communication helpdesk system
- contact the appropriate Responsible Officer when a security incident is reported to offer advice and guidance, if required
- recommend the actions to be taken to correct any security weakness
- follow up reported incidents to ensure actions have been taken and that measures have been put in place to prevent further similar breaches
- publish on the intranet advice and guidance provided as a result of reported security incidents
- provide Management with appropriate statistics from the helpdesk system on a regular basis.

12. Business Continuity Management

A business continuity management process should be implemented to counteract interruptions to business activities and to protect critical business processes from the effects of major failure to information systems or disasters.
A managed process should be developed and maintained for business continuity throughout the Council that addresses the information security requirements needed for the Council's business continuity.

13. Third Party Access

Where a third party requires access, then it is the responsibility of the relevant department / section to ensure that the relevant procedures are in place.

Access to secure areas by third party support services personnel is to be restricted, authorised, controlled and monitored.

The Council's officers are responsible for ensuring that:

- third party access is in accordance with a written contract and the contract should include this policy and a reference to it

- potential third parties are advised of the policy and the need for compliance during the tender and evaluation process
- any access to the Council's network is subject to the written approval of the Head of Information and Communication
- all access conditions are documented and agreed by the Head of Information and Communication or the appropriate Strategic Director or Headteacher
- an officer or officers are appointed who are authorised to grant third party access to data, networks and applications
- third parties are issued with an access password which is changed at irregular intervals not exceeding 2 months and communicated to the third party in a secure manner as agreed between the Council and the third party
- third party access is not allowed unless and until a request, either verbal or written, has been received and authorised
- an access log is maintained of all third party access requests with details of each request recorded and certified by an authorised officer
- the systems administrator examines the audit log and parameter files within one working day of the access being made, ensures that the activity undertaken by the third party is in agreement with the details of amendments as provided and signs off the access log
- an up to date record is maintained of all third parties, their level of access, responsible managers and associated details
- the third party is assigned to a member of the Council's staff when accessing data, networks and applications using the Council's IT resources and/or when on the Council's property and accompanied where practical
- where access has not been in accordance with these procedures the Officer controlling access shall immediately report the fact to Head of Information and Communication or the appropriate Strategic Director or Headteacher
- review the security arrangements on an annual basis in light of technological or other changes.

Where the procurement of the software, the support of the software and the ongoing arrangements for third party access is made via Information and Communication, then a representative of Information and Communication, in conjunction with the relevant systems administrator, will be responsible for discharging the defined responsibilities.

Where software is procured, supported or the support managed independently of Information and Communication, then the Strategic Director of the directorate concerned or the Headteacher of the school concerned is responsible for ensuring that all the responsibilities in respect of third parties are discharged.

The requirements of third party access shall be covered in a written contract with the third party supplier. The contract shall state that:

- the third party is to ensure the confidentiality of all information and information regarding access
- the third party must ensure that all access to the council's data, networks and applications is in accordance with the written contract requirements
- access means access by any means
- the third party must in no way attempt to access the Council's data, networks and applications without the prior approval of the authorised Council Officer unless so instructed by the authorised Officer or Officers

- the third party must in no way attempt to access the Council's data, networks and applications without confirmation by fax signed by the authorised Officer or by other means as considered secure by the Council
- the third party shall be issued with a password by the Council which should be quoted at the time access is requested
- the Council shall issue an amended password as often as it determines is necessary to ensure security
- the third party must at all times ensure the security and confidentiality of the password. If a record is maintained of the password it must be destroyed immediately on receipt of a new password
- the third party must not attempt to bypass the Council's procedures or security arrangements or to access other than the data or application authorised
- the third party must inform the Council of its preferred/expected method of access
- the third party must inform the Council of any changes to its preferred/expected method of access
- the third party must inform the Council immediately if it suspects that security procedures are compromised in any way
- the Council shall inform the third party in writing of the Officer or Officers so appointed to grant access to data, networks and systems and the data, networks and applications to which they shall be granted access
- the third party shall appoint a Senior Manager or Managers who shall be responsible for informing the Council when the third party access is required.

When contacting the Council to request access the third party shall state:

- the name of the Manager making the request
- the password
- reason for access
- details of all the amendments being undertaken
- time and estimated length of access
- type of access (if more than one possible).

Requests for access made by phone shall be confirmed by receipt of a fax signed by the appointed manager or by other means as considered secure by the Council.

The Council shall reserve the right to impose any other fair and reasonable conditions to safeguard its data, networks and applications.

The Council shall be entitled to request from the third party any information which it feels is required to verify the adequacy of their security procedures.

Delivery and Loading Areas

- delivery and loading areas are to be isolated from information processing facilities to avoid unauthorised access
- access to a holding area from outside of the building is to be restricted to identified and authorised personnel
- the holding area is to be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building
- the external door(s) of a holding area are to be secured when the internal door is opened

- incoming material is to be inspected for potential hazards before it is moved from the holding area to the point of use
- incoming material is to be logged on entry to the site.

14. Further Guidance

Further guidance on the above issues can be found via the **link** on the front page of the Council's intranet site or by placing a call on the Information & Communication helpdesk (73)4356.

Author: M Meakin
Contact: 734369 or maureen.meakin@doncaster.gov.uk

Version	Date of Revision	Amended by	Reasons
1.0	March 2007	M Meakin	Initial version
1.1	May 2007	P Hudson	Amended for Comments from Employee Relations Committee Brief.