Network Security Policy

1 Version History details and author

1.0	02/03/2011	Completed for Distribution	Jo White
1.0	31/03/2011	Agreed by Information Governance Group	Jo White
2.0	28/03/2012	Reviewed by Information Governance Group	Jo White
3.0	22/04/2013	Reviewed by Information Governance Group and changed to a policy from procedures.	Jo White
4.0	19/05/2014	Reviewed by Information Governance Group	Jo White
5.0	15/06/2015	Reviewed by Information Governance Group.	Jo White
6.0	11/07/2016	Reviewed by Information Governance Group. Amendment to third party access.	Jo White
7.0	07/08/2017	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	10/09/2018	Reviewed by the Information Governance Group. No changes.	Jo White
9.0	08/10/2019	Reviewed by Information Governance Group. Juniper Access changed to Direct Access. Network Manager changed to Data Centre Manager.	Jo White
10.0	03/11/2020	Reviewed by the Information Governance Group. No changes.	Jo White
11.0	11/01/2022	Reviewed by the Information Governance Group. Data Centre locations removed and acronyms expanded.	Jo White
12.0	07/02/2023	Reviewed by the Information Governance Group. Review changed to at least annually for logs etc.	Jo White
13.0	09/04/2024	Reviewed by the Information Governance Group. ISO27001 controls updated. Reviewed by server team.	Jo White

This document has been prepared using the following ISO27001:2022 standard controls as reference:

A.5.3 - Segregation of duties
A.5.8 - Information security in project management
A.5.15 - Access control
A.5.17 - Authentication information
A.5.18 - Access rights
A.5.29 - Information security during disruption
A.5.35 – Independent review of information security
A.5.37 - Documented operating procedures
A.6.3 - Information security awareness, education and training
A.7.8 – Equipment siting and protection
A.8.2 - Privileged access rights
A.8.6 - Capacity Management
A.8.7 - Protection against malware
A.8.8 - Management of technical vulnerabilities
A.8.9 – Configuration management
A.8.12 – Data leakage protection
A.8.15 - Logging
A.8.19 - Installation of software on operational systems
A.8.20 - Networks security
A.8.22 - Segregation in networks
A.8.24 – Use of cryptography
A.8.29 – Security testing in development and acceptance
A.8.30 - Outsourced development

A.8.31 - Separation of development, test and production environments
A.8.32 – Change management
A.8.33 – Test information
A.8.34 – Protection of information during audit testing

2 Introduction

Derbyshire County Council has a large and complex ICT infrastructure. The foundation of this structure is the Data and Communications Network which is facilitated and supported by many types of hardware including extensive cabling and supporting systems installed throughout the Council's various buildings and offices across Derbyshire.

The Council relies heavily on its Data and Communications Network infrastructure which enables it to:

- Carry out its business functions and activities using connected IT systems
- Communicate via integrated telephony systems
- Facilitate Video Conferencing technologies
- Provide wireless "Hot Spot" access zones and ICT connected services to the public

3 Purpose

The purpose of this policy is to ensure the security, integrity and availability of the Council's Data and Communications Network and to establish professional good working practices and procedures.

4 Scope

The scope of this policy extends to all administration, installation and configuration of the Council's Data and Communications Network equipment and associated systems which form part of the Council's IT infrastructure and which falls under the responsibility of the Network Support team. This policy must be undertaken in line with all existing Council policies and procedures.

5 Policy Statement

The Council's Data and Communications Network equipment is maintained and installed across most Council buildings and locations. The Council's main Data Centre houses most of the Data and Communications Network equipment and serves as the main access area to the Council's ICT Infrastructure. A second Data Centre has been established as a standby or failover location in the event that the main Data Centre is inoperable.

The Council has appointed a Head of Service who manages the data and communications network.

To secure the data and communications network, the Head of Service must ensure:

1. All visitors to the Data and Communications Network environment are issued with an authorised Council visitors badge and are signed in/out using the correct procedures (Data Centre's Physical Access Control Policy)
2. Any visitors to the Data and Communications Network environment area must be accompanied at all times by authorised Council personnel
3. Any person not known to Network personnel must be challenged in order to establish who they are and whether authorisation has been provided for them to be there
4. Access to and knowledge of door lock codes are restricted to authorised personnel only and must not be shared with any unauthorised person.
5. Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the Data Centre Manager in line with ISO27002

code of practice and immediately when an employee (who has access to sensitive ICT areas) ceases to be employed by the Council.

6. Electronic access tags must be issued to authorised staff on an individual basis. Staff issued with access tags must have their names and employee numbers recorded against the registered access tag number including date and time of issue
7. Access tags should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's tag if available with permission of the line manager and the recorded user must either be present or be made aware that their tag is being used. Any such use must be recorded and maintained in a logging system for this type of event and be securely stored with restricted access.
8. Access to the Data Centre area, including any adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms
9. Access tags issued to personnel who no longer work for the Council must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system
10. Doors which provide access to Data and Communications Network equipment must not to be left/wedged open unless for the purpose of taking delivery of new equipment, to accommodate the movement of existing equipment, transportation of maintenance or cleaning equipment – an authorised member of staff must be present at all times to supervise access when doors are left open
11. All Council/Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this policy
12. Personal, special access visits from relatives or acquaintances of personnel are not permitted within the secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure
13. Any issues to do with official authorisation of access to the Data Centre Area should be sought from the Data Centre Manager – in the absence of the Data Centre Manager, clearance should be requested from the Assistant Director of ICT Services or the Information Security Manager

All staff must abide by the Data Centre's Physical Access Control Policy which is available from the Data Centre manager

ENVIRONMENT

The Data Centre accommodates ICT infrastructure equipment from both the Network and Server support teams. Access to the Data Centres given by personnel from either team to visitors must be formally authorised by the Data Centre Manager as any access given will be providing access to both Network and Server infrastructure equipment. In the absence of the Data Centre Manager, formal clearance must be requested from the Assistant Director of ICT Services or the Information Security Manager.

It is important to maintain a high level of professionalism to ensure the security, integrity and safety of the Council's Data and Communications Network and supporting environment. The Data Centres are sensitive ICT areas and as such, require a high degree of physical and environmental controls. The Data Centre's **Physical Access Control Policy** describes these controls.

All authorised personnel must ensure that they comply with the policies, procedures and best practice specific to the Data and Communications Network and Data Centre working environment.

CONFIGURATION AND MAINTENANCE

Administration, maintenance and support for the Council's ICT Network infrastructure is normally provided by a dedicated team of Network Support personnel.
The following must be considered in order to protect the security, integrity and reputation of the Council:

1. All Data and Communications Network devices must be installed and maintained according to the manufacturer's guidelines in-line with all relevant Council policies and procedures. This will also include the relevant power supplies to Data and Communications Network devices.
2. All Data and Communications Network hardware and software should be purchased/obtained via the Council's approved procurement procedures.
3. Adequate levels of staffing should be provided at all times – particularly for call-out purposes or systems requiring out-of-hours support
4. Firmware updates/upgrades to Data and Communications Network hardware must only be undertaken if there is an identified requirement or need to do so in line with the documented maintenance procedures
5. Any visitors, contractors or vendors carrying out hardware/software installations and/or maintenance are not left unattended while working - unless authorised by the Data Centre Manager or an appropriate supervisor Access within the building should also be limited to areas where the work is to be carried out
6. Data and Communications Network devices must be located in physically secure areas (locked communications rooms or cabinets) to protect against unauthorised access, removal, disconnection, interference and/or damage.
7. All unnecessary services running on network devices must be disabled wherever possible
8. Controls must be implemented to prevent direct unauthorised communication with network devices (Infrastructure ACLs).
9. Logical separation of the network must be implemented at Layer 2 (VLANs) and layer 3 (subnets) with access controls implemented (Private VLANS, ACLs, firewalls).
10. All routing protocol exchanges must be authorised and verified.
11. All security devices deployed must be EAL4 compliant
12. Data cables should be individually identifiable through the application of a labelling scheme to ensure cables are not removed or re-patched in error
13. Standardised cable colours should be used where practical to differentiate between cables carrying DCC data and cables carrying partner data or external (service provider) connections
14. Configuration details and any other potentially sensitive information relating to network management must not be circulated to any party outside the Network Support team.
15. Disaster recovery procedures must be in place in the event of loss of the Council's Data and Communications Network infrastructure and procedural documentation must be regularly updated, at least annually, to include any changes/updates to existing procedures or processes involved

16. Data and Communications Network Infrastructure Fault Tolerance and Redundancy procedures must be in place and tested for effectiveness on a regular basis, at least annually. Procedural documentation must be regularly updated to include any changes or updates
17. Network Management procedures must be in place for the administration of all critical network functions including firewall maintenance, Intrusion Detection System management and maintenance of Internet activity logs
18. Any new hardware or systems to be installed as part of the Council's Data and Communications Network must be provided with documentation detailing running environment specification, installation procedures and details of any known issues which could adversely affect the security and integrity of the Council's ICT infrastructure – these requirements must be formally identified and included in system documentation and service agreements on procurement of the hardware or system
19. Configuration changes to the Data and Communications Network must be passed through the Council's Change Control Procedure and any planned work to be scheduled should include a notification to all parties affected via the Change Control Procedure
20. Emergency Changes will follow the agreed Emergency Change Procedure which requires emergency changes to be approved by designated staff and for the changes to be documented and submitted retrospectively
21. In the event of inappropriate activity or network misuse being identified by the Network Team this should be reported immediately via the Security Incident Reporting protocol and where there is suspected fraud or serious system misuse reported to Internal Audit

ADMINISTRATION

1. Administrative access for the management of Data and Communications Network devices is permitted only from authorised management workstations defined by the Network Support team
2. Authorised personnel with administrative access to Data and Communications Network devices and/or Servers must have their account disabled immediately on cessation of employment with the Council
3. Administrative access for the management of network devices is permitted only for authorised personnel. All administrative management access must be monitored (including failed access attempts) and event logs must be checked for events such as unauthorised access attempts
4. Only authorised personnel are provided with full administrative access to network infrastructure devices – read-only access may be made available to other parties where necessary
5. All interfaces used for system administrative management must be appropriately secured
6. All administrative/management sessions and data must be protected through the use of secured protocols in accordance with industry best practice
7. All passwords in the network device configuration must be encrypted.
8. Local device passwords must be changed quarterly and must conform to the Council's Password Policy wherever possible
9. Password recovery must be disabled on all devices - backup configurations must be readily available in case of emergency
10. Copies of backup passwords must be kept in secure locations both onsite and offsite and easily accessible to authorised staff when required

11. Notifications which display acceptable (authorised) use including warnings for unauthorised use must be presented to any user connecting to infrastructure network devices
12. All Data and Communications Network equipment which may require local logon privileges for configuration and maintenance i.e. Routers etc… must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of the Council's Password policy wherever possible
13. All administrative, privileged systems account passwords (not individual user accounts) must be stored using encryption which utilizes a minimum of 128 Bit AES encryption and must only be accessible to Network Support personnel

MONITORING AND EVENT LOGGING

1. Network events which include the following, must be logged and recorded to a centrally secured location:
    - Security events
    - Network device access
    - Systems warnings errors or critical alerts
    - CPU and memory threshold alerts
    - Routing change events
    - Network topology changes

2. Servers which are used to log events/data files must be appropriately secured against unauthorised access in line with the Council's Server Security procedures
3. Logging events to individual network devices must be disabled
4. Log files must be routinely analysed to ensure anomalies, failures, unexpected changes or any other significant events are reported under the Council's incident/event management process
5. All network device clocks must be synchronised with a central time source (NTP Server)
6. Network traffic profiles must be monitored and analysed for capacity management and anomaly detection

REMOTE ACCESS

1. Procedures must be in place to ensure that any external remote connections enabled for third party software/system support to the Council's Network/Servers are setup to connect via the Council's secure Remote Access Portal (RAP).
2. The Network Support team must ensure that the correct procedures and processes are in place to facilitate and enable third party vendors to provide support for the Council's software and systems using the most secure methods available

3. Remote access provided for third party support must be managed through a secure Remote Access Portal (RAP) shared session with a member of the Data Centre/Network Team and/or an appropriately authorised Council staff member who is responsible for and in control of elevating/revoking privileges within the shared session and for the remote support account.

Documentation detailing this process must be developed and disseminated to relevant areas such as the ICT Service's Service Desk in order to protect the Council's Network and Server infrastructure

4. The Network Support team should facilitate Council staff accessing the Council Network/Servers remotely and the team should ensure users are restricted to using the most secure protocols and tunnelling mechanisms available
5. Network Support staff working remotely or from home must observe the same controls and procedures as when working within the Council campus in order to ensure the security, integrity and to prevent loss and/or damage to Council assets and reputation

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.
All Council employees, elected members, partner agencies, agency staff, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.