Server Security Policy

1 Version History details and author

1.0	25/01/2011	Completed for distribution	Jo White
1.0	02/03/2011	Approved 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 and privileged account 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 Information Governance Group. No changes.	Jo White
9.0	08/10/2019	Reviewed by Information Governance Group. Juniper Access changed to Direct Access. Server Support changed to Data Centre.	Jo White
10.0	03/11/2020	Reviewed by Information Governance Group. No changes.	Jo White
11.0	11/01/2022	Reviewed by 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.5.7 – Threat intelligence
A.5.8 - Information security in project management
A.5.10 – Acceptable use of information and other assets
A.5.15 - Access control
A.5.16 – Identity management
A.5.17 - Authentication information
A.5.18 - Access rights
A.5.19 – Information security in supplier relationships
A.5.23 – Information security for use of cloud services
A.5.29 - Information security during disruption
A.5.30 – ICT readiness for business continuity
A.5.34 - Privacy and protection of pii
A.5.35 – Independent review of formation security
A.5.37 - Documented operating procedures
A.6.3 - Information security awareness, education and training
A.7.4 – Physical security monitoring
A.7.8 – Equipment siting and protection
A.7.10 – Storage media
A.8.2 - Privileged access rights
A.8.3 – Information Access Restriction

A.8.6 - Capacity management
A.8.7 - Protection against malware
A.8.8 - Management of technical vulnerabilities
A.8.9 – Configuration management
A.8.10 – Information deletion
A.8.11 – Data masking
A.8.12 – Data leakage prevention
A.8.13 - Information backup
A.8.15 - Logging
A.8.16 – Monitoring activities
A.8.19 - Installation of software on operational systems
A.8.20 > 8.22 - Networks security
A.8.23 – Web filtering
A.8.24 – Use of cryptography
A.8.32 - Change management
A.8.33 – Test information
A.8.34 – Protection of information systems during audit testing

2 Introduction

Derbyshire County Council has a large and complex ICT infrastructure. Servers form a key part of this infrastructure - providing essential services, access to computer applications, security and data storage. The Council's ICT network would be unable to function or provide its critical services without the availability of Servers.

All administration, installation and configuration of Servers and associated systems which form part of the Council's IT infrastructure and which falls under the responsibility of the Data Centre team must be undertaken in line with all existing Council policies and procedures.

3 Purpose

The following, details the security implications and measures required to ensure the Council's Server infrastructure is protected through effective and well managed procedures and practices.

4 Scope

This policy applies to all Council servers which are maintained and installed within secure Council buildings and locations. The Council's main Data Centre houses most of the Server and 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.

5 Policy Statement

The Council has appointed a Head of Service who manages the Server Infrastructure.
To secure the Data Centres the Head of Service must ensure that:

1. Appropriate mechanisms are in place to record the names, dates, times and signatures for the signing in and out of visitors (including Council personnel) to the Data Centre. All visitors must be issued with an authorised Council visitors badge when signing in
2. Any visitors to the Data Centre area must be accompanied at all times by authorised Council personnel
3. Any person not known to Data Centre 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 professional best 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

8. Access to server rooms 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 the Servers/rooms are 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 to 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 made available to Data Centre personnel and can be requested from the Data Centre manager

ENVIRONMENT

Servers are physically stored/located in the Data Centre areas. The Data Centre accommodates ICT infrastructure equipment from both the Server and Network 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 Server and Network 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.

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 Centre working environment:

CONFIGURATION AND MAINTENANCE

The Council's Network Domain IT Infrastructure is built on and around the Microsoft Windows environment. All Servers which include critical infrastructure functions (excluding any alternative/legacy Servers running disparate operating systems), are installed with Microsoft Windows Server based operating systems. Administration of these Windows based Servers is normally provided by a dedicated team of Data Centre personnel.

Administration, maintenance and configuration of these Servers requires the following considerations in order to protect the security, integrity and reputation of the Council:

1. All Server hardware and software should be purchased/obtained via the Council's approved procurement procedures
2. Adequate levels of staffing should be provided at all times – particularly for call-out purposes or systems requiring out-of-hours support
3. All visitors, contractors or vendors carrying out hardware/software installations and/or maintenance should not be 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
4. Servers must be regularly updated with the latest Windows Operating System security updates and patches using Microsoft Windows update services, usually within a week of being released
5. Servers must be protected from malicious software and viruses using industry standard antivirus and anti-malware software regularly updated with the latest definition and signature files and whenever they become available
6. All Servers must record all logon, system and application activity via Windows event logs which must be archived off and stored securely elsewhere on a regular basis
7. All unnecessary Services, Applications, and Network Protocols should be removed or disabled
8. All unneeded or unnecessary Default Windows Accounts should be disabled
9. Backup and restore procedures and routines must be employed so that systems and data files can be restored and recovered in the quickest, most efficient time possible
10. Disaster recovery procedures must be in place in the event of loss of Server(s) or IT infrastructure and procedural documentation must be regularly updated, at least annually, to include any changes/updates to existing procedures or processes involved
11. Server/Domain Fault tolerance and Redundancy procedures should be in place and tested for effectiveness on a regular basis and procedural documentation must be regularly updated, at least annually, to include any changes or updates
12. Any new software or systems to be installed on the Council's Servers 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 Server infrastructure – these requirements must be formally identified and included in system documentation and service agreements on procurement of the software/system
13. Configuration changes to software, Servers and systems must be passed through the Council's Change Advisory procedure and any planned work to be scheduled should include a notification to all parties affected via the Change Control Procedure
14. Emergency Changes will be reported to the Change Enablement Board during working hours where appropriate. In out-of-hours emergency situations the Assistant Director of ICT Services or the Data Centre Manager will use their professional judgement to decide on the appropriate course of action.

Back-up, Restore and Disaster Recovery procedures are in place and are available from the Data Centre manager.

ADMINISTRATIVE ACCOUNTS

1. All Data Centre staff who are provided with administrator and/or other privileged access by whatever authorised means must ensure at all times that individual passwords are not shared with anyone else – in line with the Council's Password policy
2. Authorised personnel with administrative access and/or other privileged access by whatever authorised means to Servers and ICT devices must have their account disabled immediately on cessation of employment with the Council
3. Authorised personnel with administrative and/or other privileged access by whatever authorised means to Servers for maintenance, installation or configuration must logon with individual usernames and passwords wherever possible
4. All Data Centre staff who are provided with administrator and/or other privileged access by whatever authorised means must ensure their own account passwords are set to expire on a regular basis in line with existing account expiration policies and professional best practice
5. All accounts (other than individual user accounts) which are used solely for the installation, maintenance and configuration of Servers, software and/or other supporting hardware equipment must be disabled prior to and after use – i.e. account only to be enabled when required
6. Groups and accounts added to local Server administrator or other privileged groups must be removed unless absolutely necessary – a record of Groups and accounts which are added to local Server Administrative/ privileged groups must be maintained
7. All ICT devices which may require local logon privileges for configuration and maintenance i.e. SAN appliances 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
8. All Server administrative, privileged, software systems account passwords (not individual user accounts) must be stored using encryption which utilises a minimum of 128 Bit AES encryption and must only be accessible to Data Centre personnel
9. Administrator and/or other privileged access accounts should be reviewed on a regular basis to ensure that unauthorised privileges have not been obtained and that current user access is appropriate for their role.

SERVICE ACCOUNTS

Service accounts can be described as any account that does not correspond to an actual person. These are often built-in accounts that services use to access resources they need to perform their activities. However, some services require actual user accounts to perform certain functions.

The following considerations must be taken into account when working with service accounts and system services:

1. All services must be run using local/system accounts wherever possible

2. New software and systems procured must fulfill the requirement of using local/system accounts to run services with the least privileges wherever possible
3. All Domain accounts currently used to run services must have a password length and complexity in line with the Council's password policy and professional best practice
4. Domain accounts which were configured to run a service/s but which are no longer required must be disabled and/or removed (deleted)

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 Data Centre 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 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 is disseminated to relevant areas such as the ICT Services Service Desk in order to protect the Council's Servers and network infrastructure.
4. The Data Centre team should facilitate Council staff accessing the Council Network/Servers remotely and should be restricted to using the most secure protocols and tunnelling mechanisms available
5. Data Centre staff working remotely or from home must observe the same controls and procedures as when working within the Council campus in order to ensure security and 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, 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.