Third Party Connection 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	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. Correction of document name.	Jo White
7.0	10/07/2017	Reviewed by Information Governance Group. Amendments to council point of contact.	Jo White
8.0	06/08/2018	Reviewed by Information Governance Group. Data Protection Act changed to 2018.	Jo White
9.0	10/09/2019	Reviewed by Information Governance Group. No changes.	Jo White
10.0	06/10/2020	Reviewed by Information Governance Group. No changes.	Jo White
11.0	02/11/2021	Reviewed by Information Governance Group. Updates to legislation.	Jo White
12.0	06/12/2022	Approved by Information Governance Group. No changes.	Jo White
13.0	09/04/2024	Approved by Information Governance Group. No changes.	Jo White

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

A.5.3 - Segregation of duties
A.5.4 - Management responsibilities
A.5.19 - Information Security in Supplier Relationships
A.5.20 - Addressing information security within supplier agreements.
A.5.21 - Managing information security in the ICT supply chain
A.5.22 - Monitoring, review and change management of supplier services
A.6.2 - Terms and conditions of employment
A.8.31 - Separation of development, test and production environments

2 Introduction

Derbyshire County Council permit connections to Third Party organisations, via the RAP Portal, to promote partnership working, information sharing, service provision and support arrangements with Third Party organisations or service providers. This policy is specific to the Council's requirements when establishing new links between the Council and Third Party organisations and makes reference to additional Council security policies and procedures.

3 Purpose

The purpose of this policy is to clarify the procedures and responsibilities with regard to initiating a new connection between the Council and a Third Party organisation or service provider in order to maintain confidentiality, integrity and availability.

4 Scope

Third parties are:

(a) any individuals not employed directly by the Council,
(b) any other organisation with which the Council has entered into a Contract or Agreement,
(c) other partner organisations such as the NHS, police or other local authorities; and
(d) suppliers who require access to the Council's network to provide remote support.

This policy applies to all existing and new permanent or temporary connections and applies to any connection agreement with a third party. Any sanctions and obligations specified within the contract may be imposed as part of the third party connection agreement.

5 Policy Statement

The overall security of the Council's infrastructure, systems and data takes precedence over any individual requirements for a Third Party connection.

A specific business purpose must exist and be defined for a Third Party connection to be considered. For each Third Party connection agreement, named lead persons responsible for the system and information concerned must be appointed by both the Council and Third Party.

A risk assessment should be conducted, prior to implementation of any connection, to identify specific requirements. It will be the responsibility of the named Council lead person to carry out the assessment. The risk assessment will consider:

- A description of the participants in the assessment.
- The type of access required and the data that needs to be available to the Third Party.
- The value and sensitivity of information and information systems that may be exposed to unauthorised access
- The threat and vulnerability (the risk) to information and information systems and the impact if the threat were to take place
- The controls required to protect information and information systems. An overview of the users

- The controls required to monitor or halt the movement or sharing of information.
- How to prevent unauthorised transmission or sharing of information.
- How the Third Party organisation manages and controls information security and where the data is stored
- Details of how the Third Party will secure their ICT equipment and networks
- Details of how the third party assesses and addresses vulnerability management on their ICT infrastructure
- The method of access required – physical and logical connectivity between information systems.
- Dates of when the access is required from and a cessation date if a temporary arrangement. If a permanent arrangement is required, then an annual review must be incorporated in the agreement.
- Security incident management
- Legal requirements affecting stakeholders
- A statement assessing and listing all risks.
- An overall conclusion

Any Third Party Organisation with which the Council enters into a connection agreement must be able to demonstrate compliance with the authority's information security policies and enter into binding agreements that specify the performance to be delivered and the remedies available in the event of non-compliance.

The Council point of contact will:-

- Draft a non-disclosure agreement in conjunction with Legal Services for any organisation or named individuals accessing the services/information provided by the connection.
- Be responsible for gaining approval for the third party access from relevant stakeholders such as SRM's , senior management, Information asset owners.
- Be responsible for facilitating remote access by ensuring a written application has been made and recorded/actioned via a Halo request.
- Act as a point of liaison both with the Third Party and the Council's Digital services.
- Be responsible for liaising with the Third Party point of contact to ensure background checks (such as DBS and Baseline Personnel Security Standard) are made for Third Party access to Council systems, information and data, wherever the Council deems it necessary.
- Ensure a regular review of access roles and permissions
- Ensure a regular audit of accounts and delete accounts when no longer required.
- Ensure all relevant bodies are informed when the connection is no longer required.

The Third Party point of contact will:-

- Be responsible for managing all aspects of the connection on behalf of the Third Party
- Be the primary point of contact and be able to provide accurate information on all aspects of the Third Party
- Determine the minimum necessary access permissions pertinent to the role.

- Ensure that all Third Party users have received appropriate training and have under-gone appropriate background checks.

Third Party access to the Council's network potentially exposes the Council infrastructure to risk and therefore there must be an agreement in place that assures the Council that any third party connection meets the Council's security standards. The Third Party must consider and address:-

- A description of services and service level agreement
- Reference to relevant Council security policies and legislation
- Requirements for asset protection and access control
- Responsibilities and liabilities
- Monitoring rights and reporting processes
- Conditions for termination and renegotiation of agreements

If a log of third party activity on the DCC network is required as part of the agreement, then the third party will need to retain this log for the period specified in the agreement. Remote access software must be disabled when not in use.

All Third Party access must be facilitated through a method of connection approved by the Council which provides protection to the satisfaction of the authority. All Third Party access must be logged via the Digital Services Service desk and authorised before being permitted onto the Council's network. Once authorisation has been obtained, this will be managed in accordance with pre-agreed arrangements.

Changes to methods of connection must be clearly defined and agreed by the Council and the Third Party.

Third Parties and the Council must inform each other about any security incidents which may impact on the confidentiality, integrity or availability of the third party service or data provided by the service. Incidents originating within the Council must be handled in accordance with the 'Security incident management policy and procedures'. The range of security incidents which will require security awareness procedures include:-

- Computers left unlocked when unattended
- Password disclosures
- Virus warnings/alerts
- Media loss
- Data loss/disclosure
- Misuse/loss/corruption/alteration of Personal information.
- Physical security
- Missing correspondence
- Found correspondence/media
- Loss or theft of IT/information
- Misuse of IT equipment/facilities

Third Parties with whom the Council has a Third Party connection contract are permitted access only to systems and information related to that contract. All other access is prohibited. Any Third Party with access to sensitive council information must be cleared to the same security and human resources checks as Council staff.

6 Responsibilities

It is the responsibility of the Council and each Third Party to ensure that all sections of this policy are adhered to.

Should changes in the requirements of either the Council or the Third Party regarding the connection become apparent, such as:-

- Life span of the service
- Changes in the information required
- Changes in the type of connection
- Changes in any aspect of security
- Changes of key contacts
- Emergency handling procedures

Each party should notify the other as soon as possible and the respective connection agreement should be revised.

7 Breaches of Policy

Breaches of Third Party Connection agreements 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.

The Council will take appropriate measures to remedy any breach of a third party connection agreement. If a breach/security incident relates to a Third Party the County Council reserves the right to immediately terminate the Third Party connection and, subject to the nature of the breach/security incident, seek compensation or take legal action. If it can be determined that the breach/security incident has been caused by an employee of the third party, the Council would retain the right to request the employer to remove their employee from Council premises. If the breach/security incident is determined to have been caused by an individual employed by the Council, the matter may be dealt with under the disciplinary process

8 Compliance with legal obligations

The Council and Third Parties will abide by all UK legislation relating to information storage and processing including:

- The Data Protection Act (2018)
- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act (2000)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)

The Council and Third Parties will also comply with any contractual requirements, standards and principles required to maintain the business functions of the Council including:

- Protection of intellectual property rights;
- Protection of the authority's records;
- Compliance checking and audit procedures;
- Prevention of facilities misuse;
- Relevant codes of connection to Third Party networks and services.

9 Compliance with Council ICT policies

Several Council non-ICT and ICT specific policies need to be considered as relevant within the sphere of any Third Party connection policy.

These include but are not exclusive to:-

- Safe Haven guidance
- Information security policy
- Wireless network policy
- Password policy
- Encryption & Cryptographic Controls policy
- ICT acceptable use policy
- Public internet access policy
- Security incident management policy and procedures
- Supplier Information Security policy

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.