Supplier Information Security Policy

Document Control

Title	Supplier Information Security Policy
Description	Measures to ensure suppliers adhere to Council security requirements
Created by	Claire Schweidler
Maintained by	Richard Bray
Created	January 2025
Last modified	27 August 2025
Review date	June 2027

Revision History

Version	Date	Detail of change/purpose	Author
1.0	28/03/2025	New Policy	C Schweidler
1.1	27/08/2025	Minor changes following external review	C Schweidler

Contents

Introduction

The business of Kirklees Council operates across a wide range of services to the local area and effective relationships with suppliers are critical to the continued success. To provide these services, information security is an essential factor to ensure the safety of the citizens and their dependents.

This policy aims to ensure suppliers and service providers that handle the Council's information understand the expectations and requirements of best practice information security practice and to demonstrate the importance placed by the Council on the maintenance of effective controls to reduce risk.

Scope of Policy

This policy applies to all consultants, business partners, third party suppliers and their subcontractors that enter into agreements with the Council that involve the handling of any Council data. This includes all information shared with service providers as well as information held in the Council's IT systems (both on premise and cloud).

Related Documents

- Supplier Assurance Procedure
- Supplier Security Agreement
- Cloud Computing Policy
- Cloud Security Due Diligence Questionnaire
- Supplier Assurance Form

Policy Statement

In general, information security requirements will vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

The following will apply.

- The information security requirements and controls must be documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract
- Separate Non-Disclosure Agreements must be used where a more specific level of control over confidentiality is required
- Appropriate due diligence must be completed in the selection and approval of new suppliers before contracts are signed
- The information security provisions in place at existing suppliers (where due diligence was not undertaken as part of initial selection) must be checked against the Supplier Assurance Form by the business and application owners and agreed improvements made where necessary
- Remote access by suppliers must be via approved methods that comply with the Council's access management procedures
- Access to Kirklees Council information must be limited according to clear business need
- Basic information security principles such as least privilege, separation of duties and defence in depth must be applied
- The supplier will be expected to exercise adequate control over the information security policies and procedures used within sub-contractors who play a part in the supply chain of delivery of goods or services to Kirklees Council
- Kirklees Council will have the right to audit the information security practices of the supplier and, where appropriate, sub-contractors

- Incident management and contingency arrangements must be put in place based on the results of a risk assessment
- Awareness training will be conducted by both parties to the agreement, based on the defined processes and procedures

The selection of required controls to mitigate any issues must be based upon a comprehensive risk assessment considering information security requirements, the product or service to be supplied, its criticality to the organisation and the capabilities of the supplier.

Cloud Service Due Diligence

Cloud service providers (CSPs) must be clearly recognised as such so that the risks associated with the CSP's access to, and management of Kirklees Council cloud data may be managed appropriately.

When acting as a CSP, Kirklees Council will clearly set out the relevant information security measures it will implement as part of the agreement. Kirklees Council will also ensure that information security objectives are set for third parties who provide components of the cloud service to customers and that they conduct adequate risk assessment to achieve an acceptable level of security.

Addressing Security within Supplier Agreements

Once a potential supplier has satisfactorily completed the due diligence process, information security requirements of Kirklees Council must be included in the written contractual agreement.

This agreement should include:

- the classification of any information being held or processed by the supplier (including any required mapping between Kirklees Council classifications and those in use within the supplier),
- relevant legal and regulatory requirements
- additional information security controls required by the Council

Where the supplier accesses the Council network for the purposes of software application support and maintenance, the supplier must adhere to the Council's controls for managing access as detailed in the System Security Agreement.

For cloud service contracts, information security roles and responsibilities must be defined in areas such as backups, incident management, vulnerability assessment and cryptographic controls.

Monitoring and Review of Supplier Services

Suppliers to the Council will attend regular contract review meetings. The frequency of these meetings will vary but should be held at least annually.

Each supplier will have a designated contract manager within the relevant Council service who is responsible for arranging, chairing, and documenting the review meetings.

In addition to contract performance items, these review meetings should include agenda items concerning Information Security and Vulnerability Management of the application and the future roadmap for the solution and any changes that may impact its security.