

Third Party IT Access Policy



EAST RIDING
OF YORKSHIRE COUNCIL

Lead Directorate and Service:	Corporate Resources - Digital Change and Technology
Effective Date:	December 2022
Contact Officer/Number:	David Cox - ICT Security Manager
Approved By:	Cabinet

Contents

Third Party IT Access Policy

1. Introduction.....	1
2. Scope.....	1
3. Policy Statement.....	Error! Bookmark not defined.
4. Corporate Requirements	1
5. Policy Development Including Consultation	1
6. Links with Other Policies	1
7. Policy Implementation	2
8. Third Party responsibilities	2
9. Arrangements for Contractors.....	3
10. Policy Compliance.....	3
11. Financial Implications	3
12. Review	3

Third Party IT Access Policy

1. Introduction

East Riding of Yorkshire Council (ERYC) are making ever increasing use of Information and Communication Technology (ICT) and customer information held by the Council and other public sector organisations. The information that ERYC holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

To ensure the continued availability and integrity of our IT systems we must ensure they are properly maintained and serviced. It is not possible to have experts in all systems so, on occasion, it is necessary to allow third party organisations access to our systems to carry out service and maintenance tasks.

Access to systems by third parties must be controlled in such a way as to maintain the confidentiality, integrity and availability of the IT systems being accessed. This policy defines the policies that must be followed when we require third parties to access Council IT systems for business purposes.

2. Scope

This Policy applies to all employees, councillors, committees, partners and contractual third parties and agents of ERYC who access and utilise Council ICT owned facilities and equipment.

3. Policy Statement

This policy applies to all IT systems and software owned, leased or operated by the Council or operated on the Council's behalf.

4. Corporate Requirements

ICT Security is vital to the effective operation of ERYC. All ICT equipment used by the Council must adhere to the highest standards of ICT security at all times so that:

- The public and all users of the Council's information systems are confident of the confidentiality, integrity and, availability of the information used and produced.
- Business damage, interruption and reputation caused by security incidents are minimised.
- All legislative and regulatory requirements are met.
- The Council's ICT equipment and facilities are used responsibly, securely and with integrity at all times.

5. Policy Development Including Consultation

This Policy has been developed in consultation with:

- Corporate Management Team.
- Senior Management Team.
- Information Governance Management Board.
- Portfolio Holder.
- Head of Digital, Change & Technology
- Head of Legal and Democratic Services and Senior Information Risk Owner (SIRO).
- Head of Human Resources.
- Data Protection Team.
- ICT Management Team
- ICT Security Manager.

6. Links with Other Policies

The following East Riding of Yorkshire Council Policy documents are directly relevant to this Policy and are referenced within this document:

- Information Management Strategy
- ICT Strategy and Technical Framework
- ICT Security Policy.
- Data Protection Policy.

7. Policy Implementation

Advice must be sought from the appointed service area Business Analysts prior to engaging with any potential third parties regarding accessing IT systems for service and maintenance purposes.

Third-party access to the council's network and IT systems potentially exposes the council infrastructure to risk. Therefore, arrangements must be in place to assure the third-party operating processes and policies meet the council's security requirements prior to approving access. Therefore third-parties, including suppliers of systems, must be denied access to Council IT systems by default, any exceptions to this should be agreed by the Information Asset Owners and the council Senior Information Risk Owner on a case by case basis.

A register of all third-party connections should be maintained for each on premise system. This will be completed by the system administrator, either within the ICT application team or the service area if the system is not supported by the councils ICT teams. As a minimum, the register must contain the following information:

- Name of the system
- service area contact details
- Third party company name
- Key contacts at the Third Party for the system

- Names of third-party personnel requiring access and their level of access
- Type of access Required
- End/review date of the arrangement with the Third Party

All third-party access arrangements must be reviewed and verified at least annually by the Business Analysts and the IT Security team, or when this policy changes.

Access details and log on credentials must not be issued until IT Services has received appropriate approval, in writing, from the Business Analysts following the normal service request process.

Where access is approved, IT Services will implement mechanisms to prevent access except when the third-party is required to access Council systems to fulfil the service and maintenance requirements of the Council. If access is required to be available from the third-party on a continuous basis then this will be approved from the relevant Information Asset Owner (IAO) for the service and the Council SIRO.

Mechanisms for remote connections to the Council's IT systems are maintained by IT Services. The preferred connection methods are through the Councils VPN solution or Citrix Access Gateway solution. Where these methods cannot be used, the use of an alternative access solution must be documented and approved by the IT infrastructure and Security Team.

IT Services will maintain a log of third-party access to Council IT Systems, including dates and times of access. These logs will be retained for a period of six months for audit and forensic purposes.

8. Third Party Responsibilities

It is essential that the third-party immediately informs IT Services of any security incidents that impact on the

third-party systems, or systems that the third-party is supporting or has access to, where this could lead to a possible information security incident for the council

Third-parties must securely manage (for their staff) any usernames, passwords and access information issued to them by IT Services, and must put in place suitable measures to ensure usernames, passwords and access information issued to them cannot be used to gain unauthorised access to council IT systems.

9. Policy Compliance

Contractors, including external consultants, other Public Serving agents, and agency staff, are required to abide by the council's policies, procedures and guidance, and that failure to do so may result in termination of their contract, legal action, or both. Upon receipt of this agreement the relevant Information Asset Owner, or their delegated substitute, can approve the creation of relevant IT accounts, and access to relevant systems. Contractors can then be managed as if they were employees.

10. Policy Compliance

Failure to comply with the Security Policy Framework could harm the council's ability to achieve its security objective and/or damage the professional reputation of the organisation.

If you do not understand the implications of this Policy or how it may apply to you, seek advice from your line manager, the IT Service Desk or the ICT Security Team

11. Financial Implications

The requirement to ensure appropriate protection of the Council's corporate infrastructure is one that can be managed within existing budgets.

12. Review

This policy will be reviewed on an annual basis unless there is a major changes or security-event, then the policy will be reviewed after the event has been resolved.