

Cyber Incident Response 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

Cyber Incident Response Policy	1
1. Introduction.....	1
2. Scope.....	1
3. Definitions for the Purposes of this Policy	1
4. Policy Statement.....	1
5. Corporate Requirements	1
6. Policy Development Including Consultation	2
7. Links with Other Policies	2
8. Policy Overview.....	2
9. Incident Classification.....	4
10. Policy Compliance.....	5
11. Financial Implications	5
12. Review	5
Cyber Incident Handling Checklist	6

Cyber Incident Response 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.

The goal of the Cyber Security Incident Response Policy is to detect and react to cyber security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

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. Definitions for the Purposes of this Policy

For the purpose of this Policy the key definitions are:

Event

An event is any observable occurrence in a system or network. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorised use of system privileges, unauthorised access to sensitive data, and execution of malware that destroys data.

An event is an exception to the normal operation of IT infrastructure, systems, or

services. **(Not all events become incidents.)**

Security Incident

A security incident is an event that violates or there is an imminent threat of violation to the confidentiality, integrity, or availability of the Council's information systems or data.

4. Policy Statement

This document describes the overall policy for responding to information security incidents at the Council. It defines the roles and responsibilities of participants, characterisation of incidents, relationships to other policies and procedures, and reporting requirements.

5. Corporate Requirements

ICT Security is vital to the effective operation of ERYC. All ICT systems 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.

6. 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 and 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.

7. 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:

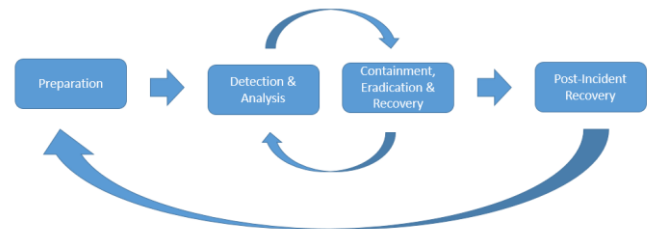
- [Information Management Strategy](#)
- [ICT Strategy and Technical Framework](#)
- ICT Security Policy
- Data Protection Policy
- ICT Acceptable Use Policy
- ICT BYOD Policy
- ICT Firewall Change Management Policy
- ICT Patch Management Policy
- Third Party ICT Access Policy
- Policy and Guidance for Web Application Penetration Testing

8. Policy Overview

This policy outlines the high-level activities for a Cyber Security Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or

channels of communication. These internal guidelines and procedures are subject to amendment as technology changes and must be documented in detail and kept up to date.

The incident response process has several phases as shown below:



Preparation

- Risk assessments.
- Conducting regular review of host security solutions.
- Conducting regular review of network security solutions.
- Ensure Malware solutions are in place.
- Conduct user awareness and training sessions.

Having the tools, resources and plans in place reduce the time to respond to an incident. This includes but is not limited to:

- Incident handling communication plans and contact lists.
- Incident analysis software and hardware.
- Incident analysis documentation, architecture diagrams and asset lists.

It is essential that training is received to ensure that the response to cyber incidents are handled with a consistent approach. To enable this training and awareness sessions will be undertaken and run and led by the following organisations:

- Local Resilience Forum (LRF)
- Yorkshire and Humberside, Warning Alerts and Response Point (YHWARP)
- Cabinet Office
- National Cyber Security Centre (NCSC)
- Disaster Recovery Consultant

Detection and Analysis

While it is not feasible to prepare a detailed action plan for all Incident types, there are several principles that can be followed. As part of the preparation phase the council will need to be prepared to respond to common attack methods. This includes the following:

- Signs that an incident is or has occurred.
- Understanding common precursors to an attack.
- Have an incident analysis process.
- Having an incident document template.
- Have a process for incident prioritisation and notification.

To assist with the incident response process, an incident handling checklist is included as Appendix A.

Containment, Eradication and Recovery

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration, once an incident has been detected.

Containment provides time for developing a remediation strategy, which is an essential part of the remediation process.

As part of the preparation phase, containment activities will need to be created for major incident types. The containment activities will assess the following:

- Potential damage to and theft of data and ICT resources.
- Service availability (eg network connectivity, services provided to external parties).
- Time and resources needed to implement the proposed containment solution.
- Effectiveness of the proposed containment solution (partial containment, full containment).
- Duration of the containment solution (emergency workaround to be removed in hours, temporary workaround to be removed in weeks, permanent solution).

Eradication and recovery should be done in a phased approach so that remediation steps are prioritised. Depending on the size of the incident this can take anywhere from hours to months.

A phased approach includes:

- Containment.
- Increase the overall security with relatively quick changes to prevent future incidents.
- Implement permanent solutions to secure the estate.

Post-Incident Activity

Each Incident will need to be reviewed and documented. All parties involved in the incident are required to provide information on their view of the incident.

Multiple incidents can be covered in a single lesson learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked.

The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed?
- Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organisations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

9. Incident Classification

Incidents will be categorised as a High - Medium - Low designation. Depending on the exposure of confidential Council information or resources. The initial severity rating may be adjusted during incident management execution.

Categorisation of such incident will be determined as per the IT Services incident response policy.

Detected vulnerabilities will not be classified as incidents.

Security incident classification is based on the functional impact, informational impact and the recovery effort required to recover from the incident.

Functional Impact

Category	Definition
None	No effect to the Council's ability to provide all services to all users.
Low	Can still provide all critical services but has lost efficiency.
Medium	Lost the ability to provide a critical service to a subset of system users.
High	no longer able to provide some critical services to any users.

Informational Impact

Category	Definition
None	No information was ex-filtrated, changed, deleted, or otherwise compromised.
Privacy Breach	Sensitive personally identifiable information (PII) was accessed or ex-filtrated.
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information

	(PCII), was accessed or ex-filtrated.
High	Sensitive or proprietary information was changed or deleted.

Recovery Effort

Category	Definition
None	No information was ex-filtrated, changed, deleted, or otherwise compromised.
Privacy Breach	Sensitive personally identifiable information (PII) was accessed or ex-filtrated.
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or ex-filtrated.
High	Sensitive or proprietary information was changed or deleted.

10. Policy Compliance

If any user is found to have breached this policy they will be subject to East Riding of Yorkshire Council's Disciplinary Procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

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 Service.

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.

APPENDIX I

Cyber Incident Handling Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred.	
1.1	Analyse the precursors and indicators.	
1.2	Look for correlating information.	
1.3	Perform research (eg search engines, knowledge base).	
1.4	As soon as an incident has occurred, begin documenting the investigation and gathering evidence.	
2.	Prioritise handling the incident based on the relevant factors.	
3.	Report the incident to the appropriate internal personnel and external organisations.	
Containment, Eradication and Recovery		
4.	Acquire, preserve, secure, and document evidence.	
5.	Contain the incident.	
6.	Eradicate the incident.	
6.1	Identify and mitigate all vulnerabilities that were exploited.	
6.2	Remove malware, inappropriate materials, and other components.	
6.3	If more affected hosts are discovered (eg new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.	
7.	Recover from the incident.	
7.1	Return affected systems to an operationally ready state.	
7.2	Confirm that the affected systems are functioning normally.	
7.3	If necessary, implement additional monitoring to look for future related activity.	
Post-Incident Activity		
8.	Create a follow-up report.	
9.	Hold a lesson learned meeting.	
10.	Update the final report.	
11.	Publish the final report.	
12.	Close the incident.	