Greater Lincolnshire
Combined County Authority

Policy

Security Incident Reporting

Purpose

A security incident is any fact or event that results in the compromise, misuse, or loss of information, ICT assets or ICT services. A security incident can impact the confidentiality, integrity, and, or availability of information.

The purpose of this policy is to:

- Outline the types of security incidents.
- Detail how incidents can and will be dealt with.
- Identify responsibilities for reporting and dealing with incidents.
- Detail procedures in place for reporting and processing of incidents.

Document Owner	Monitoring Officer
Document Version	V1.1
Approved By	GLCCA 29 April 2025

Contents

Scope

The policy applies to:

- Information which is processed by us or on our behalf by a third party;
- Owned or leased ICT such as PCs; laptops; notebooks; smart phones; software; services, storage media and network resources.

What is a Security Incident?

A security incident is any fact or event that results in the compromise, misuse, or loss of information, ICT assets or ICT services.

A near miss is as any fact or event that has happened, or may have happened, but did not result in a security incident.

A suspected incident is where initial information is sparse, and it may be uncertain whether an actual incident has taken place.

A security incident can impact the confidentiality, integrity, and, or availability of information. Examples of security incidents include:

- the loss or theft of information
- unauthorised disclosure of, or access to, information
- loss or theft of ICT, media, or devices
- physical security breaches
- deliberate or accidental breach of security policy
- insecure disposal of information or ICT assets
- malicious software infection or phishing emails
- social engineering, for example a bogus contractor attempting to use a system

General Principles

We encourage an open and transparent reporting system.

Individuals must report all security incidents accurately and without delay.

Individuals are required to assist in any investigation.

We will record all:

- reported security incidents
- potential security incidents
- near misses
- security weaknesses

We will investigate security incidents in a manner commensurate with the potential impact of the incident.

Where we establish a root cause we will consider corrective action to help prevent similar incidents occurring.

We will determine responsibility for the management of an incident after considering the following points:

- the type of incident
- the type of information involved
- the level of impact or potential impact
- the number and type of stakeholders and partnerships
- the personal data involved
- the source of the incident

Actions on Identifying a Security Incident

As soon as you identify, or suspect, that a security incident has occurred you must take the following action:

- Consider immediate action to contain, rectify or minimise the impact of the security incident e.g. asking an unintended email recipient to permanently delete the email.

- Immediately report all security incidents impacting ICT to cybersecurity@northlincs.gov.uk.

- Immediately report all security incidents to IA@greaterlincolnshire-cca.gov.uk

- Complete the online security incident report form here. .

Personal Data Breaches

A personal data breach means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal* data.

Personal data breaches attract several reporting obligations set out in data protection legislation.

All personal data breaches must be recorded.

A personal data breach which is likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office (ICO) no later than 72 hours from the point we become aware of the breach.

A personal data breach which is likely to result in a *high* risk to the rights and freedoms of individuals must be reported to the impacted individuals without undue delay.

Whether or not a breach meets either of these thresholds will be determined on a case-by-case basis as part of the security incident process. The final decision on reporting requirements is the responsibility of the Data Protection Officer.

Further Information

For further information regarding security incidents please contact:

IA@greaterlincolnshire-cca.gov.uk

or write to

Information Assurance (GLCCA),
Lincolnshire County Council,
County Offices,
Newland,
Lincoln,
LN1 1YL