Mid Devon District Council

Information Security Incident Policy

Policy Number: IM 002

November 2024

Version Control Sheet

Title: **Information Security Incident Policy**

Purpose: **To inform Staff and Elected Members of Mid Devon District Council (MDDC) of the requirements for proper reporting and management of any potential Information Security Incidents.**

Owner: **Head of Digital Transformation & Customer Engagement**

Date: **November 2024**
Version Number: **4.1**

Review Frequency: **Every three years**

Next review date: **November 2027**

Consultation: **This document was sent out for consultation to the following:**
IT and Information Governance Board
Cabinet

Document History

This document obtained the following approvals.

Title	**Date**	**Version Approved**
IT & Information Governance Board	Nov 2024	V4.1
Cabinet	Jan 2025	V4.1

Contents

Information Security Incident Policy

1 Introduction

1.1 Information Security Incidents are a growing issue for both public and private sector bodies. Whether they are caused by accidental misuse of data or intentionally by malicious actors. The impact on Local Authorities like Mid Devon District Council (MDDC) and the wider public has the potential to be significant. As the use of data increases, so will these potential impacts. The Information Commissioner for this reason has high expectations of Local Authorities and has used robust enforcement actions in cases of severe data breaches.

1.2 MDDC has a statutory responsibility to monitor all potential information security incidents that occur within the organisation. All potential incidents need to be identified, reported, investigated, or actioned based on type and severity and monitored thereafter. Only by adopting this approach can MDDC ensure that the appropriate lessons are learned from the incidents and the appropriate frameworks are put in place to ensure similar incidents do not re-occur.

2 Related Documents

- IM001 Information Security Policy
- IM006 Data Protection Policy
- ICT003 Mobile Device Policy
- ICT004 Email Us Policy

3 Scope

3.1 This Policy applies to all MDDC employees (whether permanent or temporary), Councillors, Partners, Contractual third parties and Agents of MDDC who have access to Information Systems or information used for Council purposes.

3.2 This may involve staff reporting observed or suspected incidents or actions of others where security is threatened. You may wish to also read MDDC's Anti-Fraud and Corruption Policy and the Whistle Blowing Policy.

4 Definition

4.1 An information security incident occurs when information/data is transferred, or is at risk of being transferred, to somebody who is not entitled to receive it; or where information/data is at risk from corruption. This includes a breach or suspected breach of confidentiality which could be anything from computer users sharing passwords to a piece of paper identifying an individual being found in a public area.

4.2 Breaches of security and/or confidentiality are events that could compromise business operations, result in embarrassment to MDDC or loss of trust in the organisation by a client or the public. Each could be a threat to the personal safety or privacy of an individual(s) and/or could lead to legal or financial penalties.

4.3 A range of examples of incident types are set out in section 9.

5 When to report

5.1 Any potential data breach should be reported as soon as any officer has identified an event that may have resulted in the potential loss of data, breaches of confidentiality, unauthorised access or any misuse of data including but not limited to changes to systems should be reported as soon as they happen. For examples of what may constitute a potential data breach please see section 9.

5.2 Every potential breach will be taken seriously and reported according to the process identified in this document. If there is any doubt about what constitutes a security incident, you should contact the Operations Manager for ICT or the Senior Information Officer (SIO). Please use DPO@middevon.gov.uk

6 Action on becoming aware of the incident

As soon as you become aware of any potential Incident you should log this in one of two ways:

- Report the potential incident immediately via the ICT Helpdesk under Security; or
- email DPO@middevon.gov.uk directly with the details specified in 7.3.

7 How to report

7.1 Log the call under Security and answer the required questions on the ICT Helpdesk, the call will be assigned to the Information Management team who will follow up the report.

7.2 If you do not have computer access please advise your line manager or Customer First who can log the call on your behalf.

7.3 Whichever approach is taken, the following information must be supplied:

- Contact name and telephone number of person reporting the incident
- The type of data or information involved
- Whether the loss of the data puts any person or other data at risk
- The number of Data Subjects (residents impacted) that may have been affected by the incident
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Date and time we became aware of the incident
- Location of data or equipment affected
- Type and circumstances of the incident;
- Any additional information you may feel could assist in the investigation

7.4 Once the information management team has received a notification of any potential information security incident, it will be logged separately for internal and audit purposes. All Information security incidents will receive a 'DB' reference number. The information collected as outlined in 7.3 will act as the basis for calculating the severity of any potential information security incident. To calculate in a standard way MDDC will apply the ICO endorsed European Agency for Cyber Security (ENISA) Score. This calculates the severity of breach based on three variables:

- Data Processing Context (type of data)
- Ease of identification
- Context of Breach

By calculating this score, we will be able to assess any immediate actions required:

- 0-2, data breach logged and action plan developed
- 2.1-3 Data Breach report drafted for review by line manager
- 3.1+ Data Breach reported to the ICO

7.5 The Report will be made on any breach that scores more than 2.1 on the severity index or represents a noticeable pattern of a particular type of information security incident. The report will provide a detailed explanation of the incident, any potential impacts on data subjects, reasons why the Information Security Incident may not meet the threshold for ICO notification and an agreed action plan. Any agreed action plan will be discussed with department heads of the affected service.

8 What happens after a Report

8.1 The Senior Information Officer will report data breaches quarterly to the IT & Information Governance Board (ITIG).

8.2 All registered incidents will be investigated and appropriate action taken. This could include contacting the ICO and/or the affected Data subjects. This could also be further training and awareness provision or an improvement to existing security and/or confidentiality policies and procedures. Action plans should be based on the specific department and be designed to reduce the likelihood of a breach.

8.3 There may be Security Incidents that highlights a new risk, in this instance the corresponding Data Breach Report will be sent to the Responsible officer for risk registers to review.

8.4 Incidents are regularly assessed to establish whether there are any trends in the incidents being recorded. If there is an influx in incidents of a particular type, or there is a failure to reduce in the volume of each type of incident, then the ITIG board will be alerted by the Head of Digital Transformation & Customer Engagement and further courses of action will be considered.

9 Examples of Information Security / Misuse Incident Protocols

9.1 The list below is not a comprehensive list, and officers should liaise with Information Management for advice on any incident they believe may be an information Security Incident.

Malicious Incident

- Computer infected by a virus or other malware, Ransomware, Phishing etc.
- An unauthorised person changing data
- Social engineering - Unknown people asking for information which could gain them access to Council data (e.g. a password or details of a third party)
- Unauthorised disclosure of information electronically, in paper form or verbally
- Falsification of records or inappropriate destruction of records
- Denial of service, for example
- Damage or interruption to Council equipment or services caused deliberately
- e.g. computer vandalism
- Connecting non-council equipment to MDDC network
- Unauthorised information access or use
- Printing or copying protectively marked information and not storing it correctly or appropriately

Access Violation

- Disclosure of logins to unauthorised people
- Disclosure of passwords to unauthorised people e.g. writing down your password and leaving it on display
- Accessing systems using someone else's authorisation e.g. someone else's user id and password
- Inappropriately sharing security devices such as access tokens
- Other compromise of user identity e.g. access to network or specific system by unauthorised person
- Allowing unauthorised physical access to staff areas of the premises.

Environmental

- Loss of integrity of the data within systems and transferred between systems □ Damage caused by natural disasters e.g. fire, burst pipes, lighting etc.
- Deterioration of paper records
- Deterioration of backup tapes
- Introduction of unauthorised or untested software □ Information leakage due to software errors.

Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Personal use of services and equipment in work time
- Using unlicensed software
- Unauthorised use of data using Artificial Intelligence (AI)

Theft / loss Incident

- Theft / loss of data – written or electronically held.
- Theft / loss of any Council equipment including computers, laptops, mobile phones, PDAs, Memory sticks, CDs.
- Failure to return council equipment above at the end of employment or tenure as councillor

-

Accidental Incident

- Sending an email containing personal information to wrong recipient by mistake.
- Receiving unsolicited mail which requires you to enter personal data or click on a link.

Miskeying

- Receiving unauthorised information.
- Sending information to wrong recipient.

10 Escalation

10.1 Where an incident is determined to be of National value the Operations Manager for ICT will escalate this to NCSC.gov.uk. NCSC as the National Technical Authority for Information Assurance within the UK and is the technical arm of GCHQ.