Mid Devon District Council

Information Security Incident Policy

Policy Number: IM 004

October 2021

Version Control Sheet

Title: **Information Security Incident Policy**

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

Owner: **Operations Manager Performance, Governance and Health & Safety**
cyandle@middevon.gov.uk
01884 234975

Date: **October 2021**
Version Number: **4.0**

Review Frequency: **Every three years**

Next review date: **October 2024**

Consultation **This document was sent out for consultation to the following:**
Corporate Manager for Digital Transformation and Customer Engagement
Leadership Team
Cabinet Member

Document History
This document obtained the following approvals.

Title	Date	Version Approved
Corporate Manager for Digital Transformation and	Oct 2021	V4.0
LeadershipTeam	Oct 2021	V4.0
Cabinet Member		

Contents

Information Security Incident Policy

1 Introduction

1.1 This Policy is about the handling of incidents where there has been a loss of, or breach of security relating to, information belonging to or being processed by Mid Devon District Council (the Council). This document defines an Information Security Incident and the procedure to report an incident.

1.2 The Council has a responsibility to monitor all incidents that occur within the organisation that may breach security and/or confidentiality of information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the Council can ensure that incidents of a particular nature do not re-occur.

1.3 Where 'near misses' occur, these should also be reported to the line manager and a local decision taken as to whether the cause of the 'near miss' is one which could involve the development of a new policy or process. If this is the case, it should be reported using the normal Procedure (see Section 8).

2 Related Documents

- IM 003 Information Security Policy
- IM 001 Data Protection Policy

3 Scope

3.1 This Policy applies to all Employees of the Council (whether permanent or temporary), Councillors, Partners, Contractual third parties and Agents of the Council 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 the Council'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 the Council or loss of trust in the organisation by a client or the public as a whole. Each could be a threat to the personal safety or privacy of an individual(s) and/or could lead to legal or financial penalties.

5 An Information Security Incident

5.1 Examples of these types of incident include:

- the loss or theft of information or data (either manual or electronic)
- the finding of confidential information/records in a public area
- poor disposal of confidential waste
- unauthorised access to information
- unauthorised disclosure of confidential information to a third party (in any format including verbally)
- transfer of information to the wrong person (by email, fax, post, or phone)
- receiving of information (such as by email or fax) meant for someone else
- sharing of computer IDs and passwords.
- attempts (either failed or successful) to gain unauthorised access to information or data storage or a computer system
- changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent
- unwanted disruption or denial of service to a system

5.2 A wider range of examples of incident types are set out in section 10 below

6 When to report

6.1 All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen.

6.2 Every breach must 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 & GMS Services or the Operations Manager for Performance, Governance and Health & Safety (DPO). Please use DPO@middevon.gov.uk

7 Action on becoming aware of the incident

7.1 As soon as you discover something that could be considered as an incident or suspected incident it must be reported immediately via the ICT Helpdesk (Hornbill) under Security.

8 How to report

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

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

8.3 Whichever route you choose, the following information must be supplied:

- Contact name and 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
- Location of the incident

- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of data or equipment affected
- Type and circumstances of the incident.

8.4 The incident and any action plan will be followed up by the SIRO team and line manager as required.

9 What happens after a Report

9.1 The DPO will report all incidents on a regular basis to Leadership Team.

9.2 All registered incidents will be investigated and appropriate action taken. This could be further training and awareness provision or an improvement to existing security and/or confidentiality policies and procedures.

9.3 Incidents will be re-evaluated after a six month period to ensure the type of incident is no longer being reported or the volume of those incidents has reduced. If there is no reduction in the volume of each type of incident Leadership Team will be alerted by the Operations Manager for Performance, Governance and Health & Safety and further courses of action will be considered.

10 Examples of Information Security / Misuse Incident Protocols

10.1 Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

10.2 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 the Council network
- Unauthorised information access or use
- Printing or copying protectively marked information and not storing it correctly or appropriately.

10.3 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.

10.4 **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.

10.5 **Inappropriate use**

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Personal use of services and equipment in work time
- Using unlicensed software

10.6 **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.

10.7 **Accidental Incident**

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

10.8 **Miskeying**

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

11 Escalation

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