Information Security Incident Reporting & Data Breach Management Policy

CONTEXT

This policy defines the requirements for reporting and managing information security incidents and/or data breaches at Maldon District Council. It supports the Corporate Information Security Policy.

Definitions

- An Information Security Incident is any event which has resulted, or could result, in:
    - the disclosure of confidential information to any unauthorised individual
    - the integrity of any system or information being put at risk
    - the availability of any system or information being put at risk
    - an adverse impact, for example:
        - embarrassment to the organisation
        - threat to personal safety or privacy
        - legal obligation or penalty
        - financial loss
        - disruption of activities
- An Information Security Problem is a weakness or vulnerability which could be exploited to cause an incident.
- A Data Breach is any event which has resulted in, or could result in:
    - The disclosure of physical records or papers containing personal information
    - The unauthorised removal of data in a physical form (i.e. printouts, letters, etc.)
    - The sharing or distribution of personal data with unauthorised persons
    - Loss or theft of data

AUDIENCE

This guidance is relevant for everyone who uses any of the Maldon District Council ICT systems and/or networks, records, archives and other physical assets where personal data may be held, or acts as a representative of the organisation.

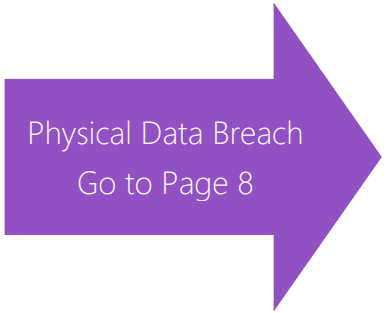
All those who access Maldon District Council ICT systems, networks and physical records may be held personally responsible for any abuse or inappropriate use.

Table of Contents

Incident Response

- All users must report any actual or perceived Information Security Incidents or Data Breach Issues as well as those set out in the Acceptable Use Policy in accordance with the Incident Management Procedures.
- All reported incidents must be assessed and responded to in accordance with Council procedures as quickly as possible.
- Management responsibilities must be established to ensure a quick, effective and orderly response to Information Security incidents.
- A security incident response plan must be formally documented and disseminated to the appropriate responsible parties.
- In case of cardholder data compromise an incident response team must be ready to be deployed.
- Any external organisations or individuals must be notified where appropriate.
- The Council should have a risk recovery policy including a plan covering the Council's media and legal response to an information security incident.
- Significant actual or potential loss of personal information should be reported to the Information Commissioners Office.
- Where the Security Incident is deemed to have either originated from or had a significant impact on the PSN, the Incident Response Team shall report the incident to the relevant bodies as detailed within the PSN Technical Standard document titled "Common Standard for Protective Monitoring, Security Incident Management and Situational Awareness".

Are you responding to an ICT or Physical Data Breach Incident?



ICT Security Breach Protocol

Reporting and Management of ICT Security Incidents

The following procedure has been derived from best practice as defined in the BERR Incident Reporting and Management guidelines.

The Incident Response Team consists of the ICT Manager, Data Protection Officer (DPO) and Head of Resources (SIRO), plus additional organisational resources as required.

A Security Incident is a situation where the security of a device, a server, a system, an application or the network itself has or may have been compromised, and may be from either an internal or external source. It could also be the introduction of a virus to a device or server and/or the network, or access to the network by an unauthorised user.

Incident Reporting

Incidents should be reported by telephone to a member of the ICT Team as soon as they happen.

ICT will record the incident in the ICT Helpdesk to track and monitor the incident and kept a record of what happened, the steps taken and the resolution.

The DPO & SIRO will be notified of the incident and kept up to date.

If the impact and severity warrants it the ICO will be notified within 72 hours. This will be decided on by the incident management team including the SIRO who has ultimate responsibility to decide to report or not.

Informing data subjects

The ICO has produced guidance on when a data subject(s) should be informed of a data breach. The Security Incident Team will establish the likelihood and severity of the resulting risk to people's rights and freedoms.

The GDPR guidance states: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

The individual(s) concerned only need to be informed if there is a 'high risk' that they may be adversely affected, therefore the threshold for informing individuals is higher than that for informing the ICO of a breach. However, the decision and reasons not to inform an individual should be documented.

Incident Management

Having received an Information Security Report, the Incident Response Team will initially qualify the incident – i.e.: determine whether the event is actually a Security Incident that needs to be managed. The key determinant will be whether there has been (or is now) a threat to the organisations business assets or a breach of regulatory requirements or organisational policy. If there has then the full incident response process will commence.

Virus and Malware incidents will be managed in accordance with the BERR five stage response process detailed below:

The BERR Five Stage Process

Containment

- Record the time, duration and location of the incident.
- Isolate systems and logons to the affected system. For example, introduce new passwords and review system access rights
- Determine whether the system should be isolated or access paths removed to prevent further damage
- Preserve the scene. For example, take photographs, save logs, record evidence, take notes of system connectivity, etc.
- Create a forensic backup of relevant data or systems. For example, imaging of computer systems
- Identify what records or logs exist for the incident
- Identify other evidence. For example, witnesses, CCTV, manual systems
- Determine who should be notified internally
- Determine who should be notified externally

Assessment

- Determine the extent of damage or penetration
- If an attempt was unsuccessful, establish why it failed
- Establish the value and relevance of evidence
- Interview witnesses or relevant parties
- Perform crime scene analysis
- Gather supporting evidence. For example, carry out penetration tests, network reviews, and risk assessments
- Gather staff evidence. For example, Human Resources records
- Perform a business impact assessment

Countermeasures

- Perform appropriate technical upgrades, patches and a configuration review
- Harden network protection
- Review intrusion detection devices and policy
- Adjust server loads and access
- Revise policy and review staff training
- Determine HR and contractual issues (to include external suppliers)
- Review outsourcing agreements (as appropriate) and revise or negotiate liability clauses and warranties
- Manage PR and publicity issues. For example, inform Members
- Involve appropriate external parties. For example, the local police force.
- Does the incident need to be reported to the police?

Appraisal

- Ask "should we disclose to statutory bodies?"
- Review assessment and countermeasures
- Determine whether we have had an internal or external attack
- Address disciplinary issues
- Consider legal proceedings
- Address contractual issues

Physical Data Breach Protocol

Reporting and Management of Physical Data Breach Incidents

Where physical records may have been breached, the DPO should be informed immediately in order for the matter to be investigated and the ICO to be informed if required.

An Incident Response Team will be convened if necessary consisting of the DPO, SIRO, Head of the Service for the incident, plus additional organisational resources as required.

Incident Reporting

Incidents should be reported by telephone to the DPO as soon as they happen.

The DPO will record the incident in the Data Breach Log to track and monitor the incident and kept a record of what happened, the steps taken and the resolution.

The SIRO will be notified of the incident and kept up to date.

If the impact and severity warrants it the ICO will be notified within 72 hours. This will be decided on by the Incident Response Team.

Incident Management

Having received an Information Breach Report, the Incident Response Team will initially qualify the incident – i.e.: determine whether the event is actually a Data Breach that needs to be managed. The key determinant will be whether there has been (or is now) a threat to the organisation's business assets, an individual's personal data, a breach of regulatory requirements or organisational policy.

Informing data subjects

The ICO has produced guidance on when a data subject(s) should be informed of a data breach. The Security Incident Team will establish the likelihood and severity of the resulting risk to people's rights and freedoms.

The GDPR guidance states: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

The individual(s) concerned only need to be informed if there is a 'high risk' that they may be adversely affected, therefore the threshold for informing individuals is higher than that for informing the ICO of a breach. However, the decision and reasons not to inform an individual should be documented.

Further information

Also see **Information Security Policy, Acceptable Use Policy**

Contact Chris Wall, ICT Manager

To report concerns, contact the ICT team on 875795 or 875770