

Breach Reporting & Response Policy



EICH CYNGOR arleinamdani
www.sirgar.llyw.cymru

YOUR COUNCIL doitonline
www.carmarthenshire.gov.wales

Breach Reporting and Response Policy

Contents

1. Purpose
 2. Scope
 3. Reporting breaches
 4. Procedure for responding to breaches
 5. Other policies and procedures
 6. Compliance measurement
 7. Sponsor
 8. Custodian
 9. Ensuring equality of treatment
- Appendix 1
- Appendix 2

1. Purpose

1.1 This Policy sets out Carmarthenshire County Council's requirements for ensuring that personal data breaches are reported and responded to in a timely and effective manner.

1.2 Data Protection legislation places an obligation on the Council to document all personal data breaches, in effect, to maintain an internal register of such incidents.

1.3 The Council is also required report breaches which are likely to result in a risk to the "rights and freedoms" of individuals to the Information Commissioner's Office (ICO) and in certain cases, inform the individuals whose personal data has been affected.

2. Scope

2.1 This policy applies to all employees of the Council, including:

- Temporary employees and agency workers
- Volunteers
- Contractors acting as data processors

2.2 The legal definition of the term breach, as used in this policy, is as follows:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

This policy therefore covers incidents where the confidentiality, integrity or availability of personal data, in any format, is compromised.

2.3 Examples of breaches include, but are not limited to:

- Loss or theft of ICT equipment such as laptops, tablet devices, smartphones, USB drives containing personal data
- Loss or theft of paper records, such as files, individual documents, notebooks containing personal data
- Loss or theft of financial information such as payment card details
- Accidental disclosure of information such as emails or letters sent to the wrong recipients and containing personal data
- Accidental deletion of records, affecting service delivery and potentially impacting on individuals' wellbeing
- Unauthorised access to IT systems, cyber and ransomware attacks

3. Reporting breaches

3.1 Breaches are most likely to come to light as a result of:

- A complaint or representation by a member of the public or external organisation
- A report via IT helpdesk
- Staff becoming aware of an issue during the course of their duties
- A data processor informing the Council of an incident

3.2 In order to ensure that breaches can be acted upon they should be reported by employees to their line manager immediately. Within the same time limit, the breach must also be reported to the Breach Response Team via a central mailbox:

databreaches@carmarthenshire.gov.uk

3.3 Out of office hours, breaches must be reported via Careline (0300 333 2222).

3.4 The response to data security breaches will be co-ordinated by the Breach Response Team, comprised of the:

- Digital Security Officer
- Information & Data Protection Officer
- Manager – Information Systems, Security

Depending on the nature of the breach, one or more of these officers will lead on the co-ordination of the response.

4. Procedure for responding to breaches

4.1 The response to a breach will follow the following steps:

- Containment and recovery
- Assessment of risk
- Notification of a breach (where necessary)
- Evaluation and response

4.2 Upon being made aware of a breach, the Breach Response Team will record the details of the breach on the Breach Report template (attached as **Appendix 1**) and notify the manager and Head of Service of the department where the breach occurred.

4.3 Where the breach is believed to relate to financial information such as bank account details, payment cardholder's information or of a system related to the Payment Card Industry (PCI), the Breach Response Team must implement the **PCI Breach Response Plan** immediately (attached as **Appendix 2**)

4.4 The manager will be responsible for initiating an immediate investigation into the cause(s) of the breach and identifying and implementing necessary containment & recovery actions, which must be clearly documented in the Breach Report. Examples of such actions include, but are clearly not limited to:

- Attempting to locate and retrieve lost paper records
- Finding a missing item of ICT equipment
- Ensuring that a wrongly addressed email has been deleted
- Informing the Police in the event of a theft
- Changing door access codes

4.5 The manager will then undertake an assessment of the risk(s) posed by the breach and record this in the Breach Report. This assessment must take into account:

- The type of data involved, its nature, sensitivity and volume
- Whether the subject(s) could be harmed by the breach, for example, identity theft, fraud or damage to reputation
- Who the individuals are, for example, children or other vulnerable people such as social care clients
- The number of individuals' personal data affected

4.6 Once these steps have been completed and recorded, the Breach Report will be returned to the Breach Response Team to be referred to the Senior Information Risk Owner (SIRO), or Deputy SIRO in their absence.

4.7 The SIRO or Deputy SIRO will then determine whether it is necessary to notify the ICO of the breach, taking into consideration the circumstances as documented. In the event that notification is required, the Breach Response Team will provide the ICO with all of the information required under Data Protection legislation.

4.8 Based on the assessment of risk, the Head of Service, in consultation with the manager and Breach Response Team, will then determine whether the data subject(s) affected by the breach are to be notified. Where this is deemed necessary, the information to be communicated to the subject, set out in Data Protection legislation, must be provided in full.

4.9 The steps set out from 4.1 to 4.8 above must be completed within a maximum of 5 working days.

4.10 Finally, in consultation with the manager, the Breach Response Team will identify and document any further recommendations and actions required. For example, if the breach was caused by systemic and ongoing problems, then actions such as the following may be necessary:

- Changes to procedures and systems
- Review of policies
- Staff training/awareness

5. Other policies or procedures

5.1 Where a breach requires further escalation due the circumstances of the case, the SIRO will determine whether to proceed with a formal investigation under the Council's **Investigation Policy**.

5.2 Where the breach constitutes a complaint, a response to the complainant will be provided in accordance with the **Council's Complaints Procedure**.

5.3 Where a reported breach constitutes a breach of any other Council policies, then the requirements of the relevant policy will be followed, which may include initiating disciplinary procedures.

6. Compliance measurement

6.1 Compliance with this Policy is mandatory. Breaches of this policy by staff may lead to disciplinary action being taken.

7. Sponsor

7.1 This Policy is owned by the Corporate Information Governance Group.

8. Custodian

8.1 It is the responsibility of the Digital Security Officer and Information & Data Protection Officer to ensure that this policy is reviewed and updated.

9. Ensuring equality of treatment

9.1 This policy and procedure must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

If you require this document in an alternative format please contact the Information & Data Protection Officer on 01267 224127 or email dataprotection@carmarthenshire.gov.uk

Policy approved by Executive Board on:
Policy review date:
Policy written by: John Tillman and John M Williams

Appendix 1



**DIOGELU DATA
SIR GÂR
CARMARTHENSHIRE
DATA PROTECTION**

PERSONAL DATA BREACH REPORT

Reference:

1. Full details of the breach

2. Containment & recovery action(s) taken

3. Assessment of ongoing risk

Type of data involved:

Number of data subject(s) affected:

Number of records affected:

Risk(s) to data subject(s):

Risk(s) to Authority:

4. Notification of breach required?

Information Commissioner's Office:

Data subject(s):

5. Evaluation & response – recommendations & action(s) required

6. Other considerations (including HR issues)

Lead co-ordinating officer	
Designation	
Department & service	
Date	

Recipients
Senior Information Risk Owner:
Head of Service:
Other:

Appendix 2

PCI Breach Response Plan

In response to a potential breach relating to PCI Data Security Standard (card payments), the Breach Response Team will make immediate contact with the Council's Treasury Management Officer or Head of Financial Services, who must:

- Ensure any compromised systems are isolated from the network;
- Gather, review and analyse the logs and related information from various central and local safeguards and security controls;
- Conduct appropriate forensic analysis of any compromised systems;
- Contact appropriate internal and external departments and entities as appropriate;
- Contact the Police and/or relevant card industry security personnel, making logs and forensic details available to them as required;
- Assist the Police and card industry security personnel in their investigative process including prosecutions;
- Contact the relevant card merchant and carry out the company's specific requirements, when reporting suspected or confirmed breaches of cardholder data.