Information Governance

Cyngor Sir Gâr Carmarthenshire County Council

Breach Reporting and Response Policy

Contents

1. Purpose

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

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 term breach used in this policy refers to incidents where the security of personal data, or otherwise confidential information, in any format, is compromised.

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

- Loss or theft of ICT equipment such as laptops, tablet devices, smartphones, USB drives etc
- Loss or theft of paper records, such as files, individual documents, notebooks etc.
- Loss or theft of financial information such as payment card details
- Accidental disclosure of information such as emails, letters or faxes sent to the wrong recipients
- Unauthorised access to IT systems

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

3.3 In order to ensure that breaches can be acted upon they should be reported by employees to their line manager immediately, or in any event within 12 hours of the breach occurring. Within the same time limit, the breach must also be reported to the Breach Response Team via a central mailbox:

databreaches@carmarthenshire.gov.uk

3.4 Out of office hours, breaches must be reported via Careline (01267 224466). This telephone number can be accessed by staff on the Council's website.

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

- IT Security Officer
- Information & Data Protection Officer
- CareFirst, Security & Integration Manager

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 steps set out in the Information Commissioner's Office guidance on data security breach management:

- Containment and recovery
- Assessment of risk
- Notification of a breach
- 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 relevant Information Asset Owner (IAO) and Head of Service.

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 IAO 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 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 IAO 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 and its sensitivity
- Whether the subject(s) could be harmed by the loss or theft of data, such as bank account details
- The number of individuals' personal data affected
- Who the individuals are, for example, social care clients

4.6 The Head of Service, in consultation with the IAO and Breach Response Team, will determine whether the data subject(s) affected by the breach are to be notified**.** This will be necessary where notifying the subject has a clear purpose, such as enabling an individual to take steps to protect themselves.

4.7 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).

4.8 The SIRO will then determine whether a referral to the Information Commissioner's Office is required, taking into consideration:

- Potential detriment to the data subject(s)
- The volume of the data affected
- The sensitivity of the information

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 IAO, 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 IT 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 must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, age, gender, gender reassignment, sexual orientation, parental or marital status.

If you require this document in an alternative format please contact the IT Security Officer on 01267 246311 or email **ITSecurity@Carmarthenshire.gov.uk**

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

Appendix 1

DIOGELU DATA
SIR GÂR
CARMARTHENSHIRE
DATA PROTECTION

DATA PROTECTION ACT 1998 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:
Risk to data subject(s):
Risk to Authority:

4. Notification of breach required?
Data subject(s):

Information Commissioner’s Office:

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.