Neath Port Talbot
Castell-nedd Port Talbot
County Borough Council Cyngor Bwrdeistref Sirol

Information Security Breach Policy

Version Control		
Version	**Date**	**Comments**
Version 1	April 2015	Initial draft of policy
Version 1.1	May 2015	Include HoS/SIRO comments
Version 1.2	June 2015	Include DFCS and Head of Legal comments
Version 1.3	June 2017	Review

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

INFORMATION SECURITY BREACH POLICY

1 INTRODUCTION

1.1 The Authority maintains a large portfolio of information, a significant proportion of which is deemed private, and care must be taken to protect these assets and to avoid an information security breach.

1.2 The Data Protection Act 1998 (DPA) makes provision for the processing of information relating to individuals, including the obtaining, holding, use and disclosure of this information. Principle 7 of the DPA states that organisations need to take "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

1.3 The Information Commissioner's Office (ICO) has produced Information Security Breach Guidance Notes which are available here.

1.4 In the event of data being lost or shared inappropriately, this Information Security Breach Policy is to be enacted as soon as possible to minimise any associated risk.

1.5 This document outlines the Authority's policy in relation to the loss of ICT equipment and/or documents and endeavours to:

- Protect the council's information assets against unauthorised access
- Protect the Authority from reputational damage
- Minimise the possibility of a financial penalty being imposed by the Information Commissioner's Office.

2 SCOPE

2.1 This policy applies to all information assets held by Neath Port Talbot County Borough Council regardless of format. A risk-based proportionate approach to handling information security breaches is encouraged. All information security breaches should be evaluated on an individual, case-by-case basis and decisions should be made according to the risk assessment in each particular circumstance.

2.2 This policy applies to all staff who have access to corporately held information and is intended to alert staff of their responsibilities regarding the security of information assets; whether that information is electronic or paper-based.

3 WHEN A BREACH OCCURS

3.1 As soon as an information security breach is identified or suspected the Incident Reporting Policy needs to be followed and the Senior Information Risk Owner (SIRO) must be informed. Dependent upon the information supplied, a decision will be made on the next course of action. This decision will be informed as to whether or not the breach has been contained.

4 TYPES OF INFORMATION SECURITY BREACH

4.1 Information security breaches include:

- Loss of computer equipment e.g. lost or stolen laptop, removable media, mobile device, hard drive
- Loss of paper documents
- Records being released to the wrong person
- Unauthorised access to systems

4.2 It should be noted that for an incident to be classified as a security breach under the DPA the loss must include person identifiable information (PII).

5 CONTAINED BREACH

5.1 If an information security breach is contained the data will normally not have left the Authority.

5.2 If the SIRO is satisfied that the information security breach has been contained, he will immediately instigate an investigation into the incident. A full report will be issued to the SIRO, and, if thought relevant, the Director and Head of Service (Information Asset Owner) concerned. The report will detail:

- The breach
- How the breach occurred
- Mitigation steps to limit the possibility of reoccurrence

5.3 The SIRO will update the Information Security Incident GROUP (ISIG) that an information security breach has occurred. The ISIG will consist of three or more of the following:

- Director of Finance & Corporate Services
- Head of ICT (SIRO)

- Head of Legal Services
- Head of Financial Services
- Head of HR
- Relevant Head of Service

6 NON-CONTAINED BREACH

6.1 A non-contained breach is an information security breach where the information has leaked outside the Authority. This type of breach puts the Authority at risk of reputational damage as well as the possibility of a financial penalty being imposed by the ICO.

6.2 In this situation a meeting of the ISIG must be arranged as soon as possible.

6.3 The purpose of the meeting is to establish the current position and consider the following:

- If the information can be retrieved
- If the ICO needs to be informed
- If the data subjects need to be informed
- If specialist Legal advice is required
- If the media are aware of the incident
- How can the Authority be assured that no further breach can occur in the same manner

6.4 Following the initial meeting of the ISIG the SIRO will initiate a full investigation into the incident. A complete record of the breach and all mitigating actions will be retained. The SIRO will ensure that appropriate officers, including the Chief Executive, if thought relevant, are updated with developments.

6.5 It will be necessary for the group to meet regularly during the course of the incident although the frequency will depend upon the incident. A record of all meetings will be maintained by the SIRO.

6.6 A report of the incident will be taken to the Information Security Group (ISG) and if thought appropriate, to the Corporate Director's Group (CDG).

7 INFORMING THIRD PARTIES

7.1 Once the incident has been investigated and a position established, if third party information is involved a decision needs to be taken to on whether or not to inform the third parties. This decision must be taken by the ISIG.

7.2 When ISIG is considering this decision, the guidance offered by the ICO should be followed. Where the decision made is to notify third parties that their information has been disclosed the responsibility for making contact will rest with the service manager unless the ISIG deem it inappropriate.

7.3 Where the decision is NOT to inform third parties of a data breach the ISIG needs to record the reasons for this decision.

7.4 A decision also needs to be taken by the ISIG as to whether or not the Authority needs to self-report the breach to the ICO.

8 INCIDENT CLOSURE

8.1 The incident will not be deemed to be closed until the SIRO determines that a conclusion has been reached.

9 POLICY REVIEW

9.1 This policy will be reviewed as required.