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

ICT Incident Reporting Policy

Version Control		
Version	**Date**	**Comments**
Version 1	May 2008	Initial draft of policy
	June 2009	Agreed with Unions
Version 1.1	Jan 2012	Review – small amendments and contact details updated
Version 1.2	May 2013	Review and small amendments
Version 1.2.1	October 2014	Review
Version 1.3	January 2016	Review and contact details updated
Version 1.4	June 2017	Review
Version 1.5	April 2018	Review and update

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

INCIDENT REPORTING POLICY

1. INTRODUCTION

1.1 This document details how the Authority will deal with breaches of Information) security and describes the responsibilities and actions which must be taken by staff and employees with an investigating role.

1.2 The security event could involve employees, elected members or persons with access to Authority information assets, data, computer systems or telephony but could also involve external persons who have no apparent link to the Authority.

2. INFORMATION SECURITY INCIDENTS

2.1 An Information Security Incident can be defined as any event that involves a breach of the principles or procedures laid down in the Information Security Policy, IT Security Policy or supporting policies and guidelines.

2.2 A breach will fall under one or more of the following categories:

- Breach due to negligence
- Breach caused by an accident
- Breach due to an intentional act

The cause of the breach will have a bearing on how the incident is treated.

3. MANAGEMENT RESPONSIBILITIES

3.1 Management should ensure that employees are made aware of this policy.

3.2 Management should ensure that staff allocated to the Investigation Officer role have sufficient experience to enable them to carry out that role.

4. STAFF RESPONSIBILITIES

4.1 Staff are required to report any and all information security breaches to line management, Head of Service, the IT Service Desk or the Business Relations Manager as soon as possible after becoming aware of an information security breach.

4.2 Examples of Information Security breaches include:

- Breaches of physical security e.g. unauthorised persons accessing a secure area
- Pieces of paper identifying an individual being found in a public area
- Access control violations e.g. person attempting or gaining access to systems or facilities to which they should not have access, staff sharing passwords, etc.
- Non-adherence to IT Security Policy or associated policies and guidelines
- IT equipment theft or loss
- Loss of information assets e.g. maliciously deleted data
- Disclosure of sensitive data e.g. loss of removable media or poor disposal of confidential waste
- Virus infection

5. REPORTING CONCERNS

5.1 There are existing procedures in place within the Authority which allow employees to confidentially report any concerns they have i.e. the Whistle Blowing Policy. The principles of the Whistle Blowing Policy will be followed with regard to concerns expressed in relation to incident reporting.

6. INITIAL ACTION

6.1 In the event of an incident the following procedure should be followed:

- The employee must notify a line manager, Head of Service, the IT Service Desk or Business Relations Manager of the suspected security breach.
- If there is the possibility of an ongoing threat, for example, virus contamination or unauthorised system access, the IT Service Desk should be contacted immediately for advice and support.
- If the event is linked to a specific computer or user account then, to retain vital evidence, the machine or user account should not be used until such time as a decision is made on whether or not an investigation is warranted.
- All supporting evidence should be retained for examination by the investigating officer.

7. INVESTIGATION

7.1 If the initial notification is to a line manager or Head of Service, they should ensure that the Head of ICT/Senior Information Risk Officer (SIRO) or Business Relations Manager is informed without delay.

7.2 The following steps will be taken:

- All incidents and allegations will be subject to an initial inquiry. This must be initiated by the relevant manager with support from the Business Relations Manager or nominated officer.
- It will be necessary to establish, as early as possible, whether there is evidence that a breach has occurred.
- If there is evidence of a breach by an individual that could be the subject of a criminal prosecution the procedures laid down in the Authority's Anti-Fraud/Corruption & Malpractice Policy should be followed and access to certain evidence should be restricted e.g. in certain circumstances computer evidence should not be examined.
- If there is evidence of a breach by an individual that could be the subject of disciplinary action the matter should be fully investigated in accordance with the Authority's disciplinary procedures and the policy or policies relevant to the breach.
- All personal information connected with investigations and subsequent reports will be treated confidentially.

8. REPORTING

8.1 Upon completion of the investigation, a report for management will be completed by the Investigating Officer.

8.2 An Incident Report Form will also be produced. The form will be completed by the department reporting the incident with advice and assistance from the Business Relations Manager or nominated officer who will record and document the incident.

8.3 Where relevant information on the incident will be reported to the local WARP (Warning, Advice and Reporting Point) and/or GovCertUK to enable member organisations to learn from (or put in place measures to avoid) the incident.

9. CORRECTIVE ACTION

9.1 The Business Relations Manager and the IT Division will consider any new controls or enhancements that need to be implemented to counter security threats identified by incidents.

10. GENERAL QUERIES

10.1 Any questions regarding this policy or computer security in general should be addressed to Steve John, the Head of ICT/Senior Information Risk Officer (SIRO), on ext. 6218 or Ian John, Business Relations Manager, on ext 6036.