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

ICT Incident Reporting Policy

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

INCIDENT REPORTING POLICY

1. INTRODUCTION

1.1 This document details how the CJC 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 CJC information assets, data, computer systems or telephony but could also involve external persons who have no apparent link to the CJC.

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. STAFF RESPONSIBILITIES

4.1 Officers, elected members and agents of the CJC are required to report any and all information security breaches to the Monitoring Officer 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

4. INITIAL ACTION

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

- The individual must notify the Monitoring Officer of a suspected security breach.
- If there is the possibility of an ongoing threat, for example, virus contamination or unauthorised system access, the Monitoring Officer 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.

5. INVESTIGATION

7.1 The following steps will be taken:

- All incidents and allegations will be subject to an initial inquiry. This must be initiated by the Monitoring 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 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 CJC'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.

6. REPORTING

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

8.2 An Incident Report Form will also be produced.

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.

7. CORRECTIVE ACTION

9.1 The Monitoring Officer will consider any new controls or enhancements that need to be implemented to counter security threats identified by incidents.

8. GENERAL QUERIES

10.1 Any questions regarding this policy or computer security in general should be addressed to the Monitoring Officer.