# Policy and Procedure Document

# Information Security Incident Management Policy and Procedure

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Information Security Incident Management Policy |
| **Author** | Mark Hanwell |
| **Filename** | Information Security Incident Management Policy. doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Information Security Incident Management Policy |
| **Protective Marking** | Unclassified |
| **Review date** | 23/08/2011 |

## Revision History

| Revision Date | Revisor | Previous Version | Description of Revision |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Document Approvals

This document requires the following approvals:

| Sponsor Approval | Name | Date |
|---|---|---|
| Head of Business Transformation | Deborah Poole | 23rd August 2011 |
| | | |
| | | |

## Document Distribution

This document will be distributed to:

| Name | Job Title | Email Address |
|---|---|---|
| | | |
| | | |
| | | |

## Contents

## 1 Policy Statement

Redditch Borough Council will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the Council.

## 2 Purpose

The aim of this policy is to ensure that Redditch Borough Council reacts appropriately to any actual or suspected security incidents relating to information systems and data.

## 3 Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who use Redditch Borough Council IT facilities and equipment, or have access to, or custody of, customer information or Redditch Borough Council information.

All users **must** understand and adopt use of this policy and are responsible for ensuring the safety and security of the Council's systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

## 4 Definition

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the ICT helpdesk. The ICT Helpdesk enables ICT to identify when a series of events or weaknesses have escalated to become an incident. It is vital for ICT to gain as much information as possible from the business users to identify if an incident is occurring.

## 7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Redditch Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or ICT.

## 8 Policy Governance

The following table identifies who within Redditch Borough Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

| | |
|---|---|
| **Responsible** | ICT Transformation Manager |
| **Accountable** | Head of Business Transformation |
| **Consulted** | Corporate Management Team |
| **Informed** | All Council Employees, All Temporary Staff, All Contractors etc |

## 9 Review and Revision

This policy, and all related appendices, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Transformation Manager.

## 10 References

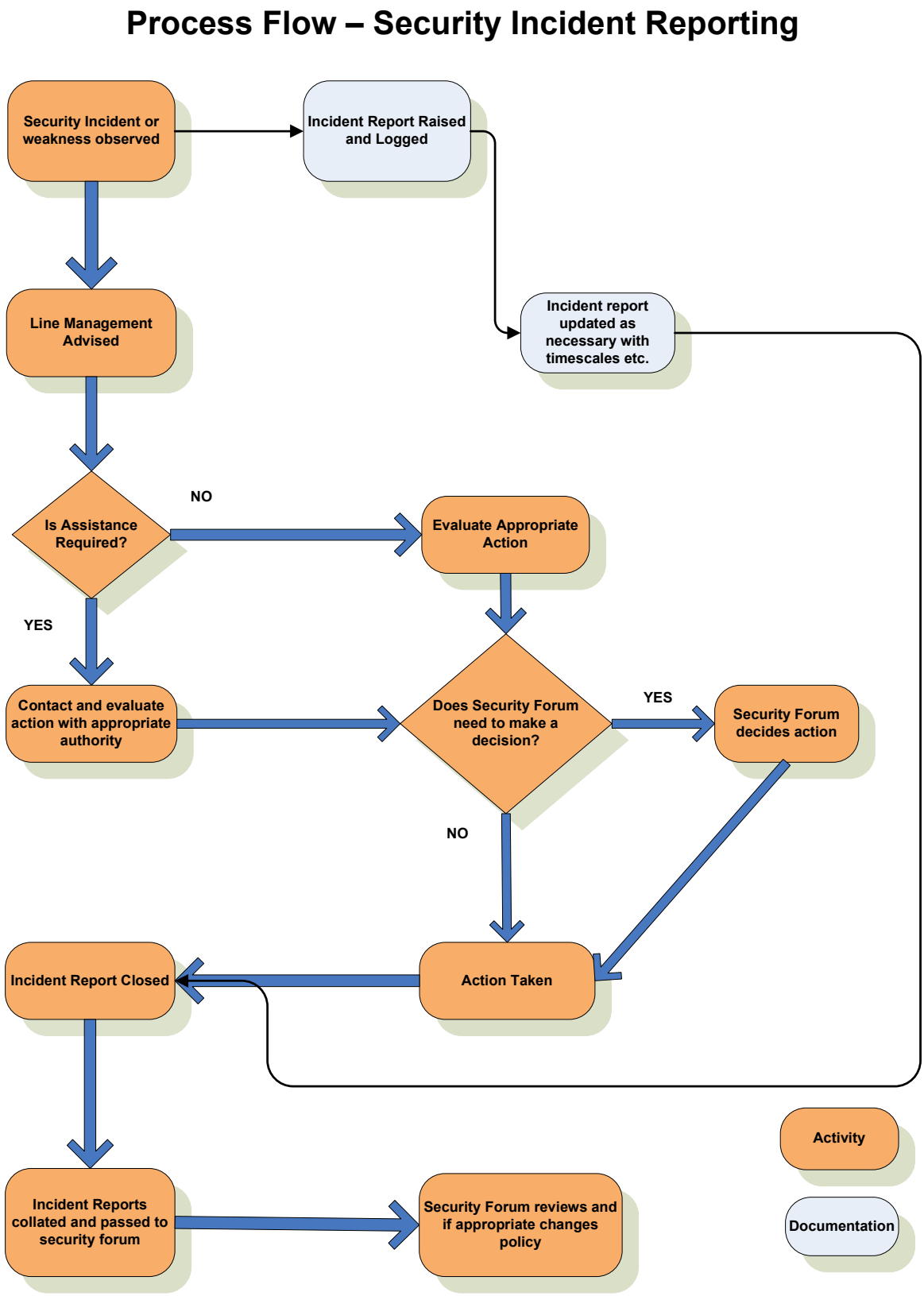
The following Redditch Borough Council policy documents are directly relevant to this policy:

- Email Policy.
- Internet Acceptable Use Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Remote Working Policy.
- IT Access Policy.
- Legal Responsibilities Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- IT Infrastructure Policy.
- Communications and Operation Management Policy.

## 11 Key Messages

- All staff should report any incidents or suspected incidents immediately by reporting them to the ICT helpdesk.
- We can maintain your anonymity when reporting an incident if you wish.
- If you are unsure of anything in this policy you should ask for advice from your line manager or ICT.

## 12 Appendix 1 – Process Flow; Reporting an Information Security Event or Weakness



## 13 Appendix 2 – Examples of Information Security Incidents

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

**Malicious**

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff'.
- Receiving solicited mail of an offensive nature.
- Receiving solicited mail which requires you to enter personal data.
- Changing data without authorisation.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others other than the ICT helpdesk.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

- Use of unapproved or unlicensed software on Redditch Borough Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

**Theft / Loss**

- Theft / loss of a hard copy file through negligence.
- Theft / loss of any Redditch Borough Council computer equipment e.g. laptops, memory sticks and CDs through negligence.

# 14 Appendix 3 - Procedure for Incident Handling

Please report all incidents to help.desk@redditchbc.gov.uk

## 14.1 Reporting Information Security Events or Weaknesses

The following sections detail how people must report information security events or weaknesses. Appendix 1 provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

### 14.1.1 Reporting Information Security Events for all Employees

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to your line manager and the Information Manager for the impact to be assessed.

All suspected security events should be reported immediately to the ICT Helpdesk.

The ICT Helpdesk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information should be supplied:

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

### 14.1.2 Collection of Evidence

Upon a potential incident the authority may need to collect evidence. This could include all data for example personal information, deleted files, and emails from any equipment owned by Redditch Borough Council.