St.Helens Council

Information Security Incident Management Policy

Version: 1.1

Date: September 2012

Version Control

Date	Version	Comments
November 2011	1.0	First draft for comments to IT Policy & Regulation Group and IMG
January 2012	1.1	Updated version following comments received
June 2012	1.1	Approved at Chief Officer Group
September 2012	1.1	Approved Delegated Executive Decision

Table of Contents

1. Introduction

The purpose of this policy is to ensure that information security events and weaknesses associated with information systems and hard copy documentation are communicated in a way that allows timely, corrective action to be taken, so that St.Helens Council's information and data is protected from any actual, suspected or potential security events.

The definition of an incident 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 in IT is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes. However, an information security event or weakness can also arise through loss, misuse or compromise of hard copy information or data and this policy equally applies to such losses.

1.1. Information & ICT Security Policy Framework

This policy should be read in conjunction with the Information & ICT Security Policy Framework, which sets out the policies and governance in place to protect the Council's information assets.

2. Policy Statement

All St. Helens Council employees, contractors and users with access to St. Helens Council's equipment and information (in any format including electronic and paper records) are responsible for ensuring the safety and security of the Council's systems and the information that they use.

3. Scope

This policy applies to all users of the Council's facilities and equipment. 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. Security Incidents and Weaknesses

An Information Security Incident can be described as an event that results in:

- The disclosure of confidential information to an unauthorised individual.
- The integrity of a system or information being put at risk.
- The availability of a system or information being put at risk.

A weakness is the potential for an incident to occur.

4.1. Reporting Information Security Incidents and Weaknesses

Information security events and weaknesses need to be reported at the earliest possible stage. It is vital that as much information is gained as possible to identify whether reported events or weaknesses are security incidents and to determine any further cause of action.

Security events and weakness that must be reported include :

- Theft or loss of equipment, data or information (including removable media)
- Breaches of physical security arrangements
- Computer infected by a virus or other malware

- Receiving unsolicited mail of an offensive nature or requesting personal data
- Unauthorised disclosure of information including information being faxed, emailed, posted or handed to an unintended recipient
- System malfunctions which may compromise security
- Inadequate disposal of confidential material
- Writing down passwords and leaving them on display or somewhere easy to find
- Non-compliance with policies or guidelines
- Accessing a persons record inappropriately
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).

(Please note this list is not exhaustive).

Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

4.2. Procedure for Reporting Information Security Incidents and Weaknesses

All information security events and weaknesses must first be reported to an individual's Line Manager. In the absence of the individual's Line Manager, an alternative appropriate manager within the Department must be informed.

If the event or weakness concerns personal data relating to a member of staff, a service user or a member of the public, or it contains particularly sensitive or confidential information, then the incident should be reported directly to Internal Audit.

If the information is in relation to Social Care service users, the incident should be reported to Internal Audit who will log the breach and inform the appropriate officers where necessary.

All IT-related events and weaknesses must be reported IMMEDIATELY to the IT Service Desk. If applicable, you must note the symptoms and any error messages on screen and await further instructions from a member of IT.

You can contact the IT Service Desk on 01744 676525, support hours are between 8am to 5.30pm.

Alternatively you can use the IT Service Desk Portal (which can be also be accessed out of hours):

- Via the IT Service Desk Portal link on your desktop
- Via the IT Service Desk Portal link on the Citrix Access Gateway Home Page
- Via the Home Page of the Intranet under 'Applications'

4.3. Action to be taken by IT Support Staff

When an information security event or weakness is reported, the Incident Management Procedure or Major Incident Management Procedure (if appropriate) must be followed. IT Support Staff will not be expected to take specific action over events or weaknesses that arise in relation to hard copy documentation. However, all incidents must be reported to Internal Audit via the IT Service Desk.

All staff involved in incident management will have access to relevant information such as known errors, problem resolutions and the configuration management database (CMDB).

The customer must be kept informed of the progress of their reported incident, and alerted in advance if their service levels cannot be met and an action agreed.

Incidents that are considered service affecting must be reported to the relevant Departmental Management Team and the System Owner, in order to make the necessary Business Continuity arrangements. A summary report will be presented to the IT Policy and Regulation Group.

5. Management of Information Security Incidents and Improvements

A consistent approach to dealing with all information security events must be maintained across the Council.

Information security incidents must be reported and recorded in line with incident management procedures as soon as possible.

Business IT will investigate all IT-related information security events and weaknesses. The Systems and Information Management Officer will investigate incidents resulting in the loss, misuse or compromise of data, if it is considered that a breach of the Data Protection Act may have occurred.

Information Security Incidents will be reported to the IT Policy & Regulation Group for review.

Where an information security event is considered to fall within the notification guidelines issued by the Information Commissioner’s Office (ICO), the Data Protection Officer will, in agreement with the Assistant Chief Executive (Finance), prepare the necessary notification and deal with all correspondence arising from it.

5.1. Collection of Evidence

If an incident requires information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence.

For other incidents, including loss or compromise of hard copy information, as much information as possible on the circumstances of the incident should be collated in order to assist the Systems and Information Management Officer to investigate.

6. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council’s disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, please seek advice from Internal Audit.