St.Helens Council

Information and ICT Incident Management Policy

Version: 2.0

Date: March 2016

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
September 2015	1.2	Policy subject to full review
December 2015	1.3	Draft approved at IMG
February 2016	1.3	Union Consultation
March 2016	2.0	Approved by Executive Decision

Table of Contents

1 Introduction 4
2 Policy Statement 4
3 Scope 4
4 Security Incidents and Weaknesses 4
5 Reporting Procedure 5
6 Management of Incidents 6
7 Responsibilities 6
Information Management Group (IMG) 6
IT Policy & Regulation Group 6
Business IT 7
System & Information Management Officer (SIMO) 7
Line Managers 7
Employees 7
8 Review and Governance 8
9 Policy Compliance 8

1 Introduction

1.1 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 the Council's information and data is protected from any actual, suspected or potential security events.

1.2 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.

1.3 Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

1.4 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.

2 Policy Statement

2.1 The purpose of this Policy is to ensure that any incidents that affect the daily operations are managed through an established process.

2.2 All Employees have an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

2.3 This Policy provides a framework for reporting and managing:

- Security incidents affecting the Council's information and ICT systems
- Losses of information
- Near misses and information security concerns

3 Scope

3.1 This Policy applies to all Employees and third parties working for or on behalf of the Council with any form of access to a Council computer device or ICT system. For the purpose of this Policy the term 'Employee' refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

3.2 This Policy should be read in conjunction with the Code of Conduct, the Council Comprehensive Equality Policy and other associated relevant policies, procedures and guidance as contained within the Information Management Framework.

4 Security Incidents and Weaknesses

4.1 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.

4.2 Initially, there are four categories: events, weaknesses, incidents and unknowns:

- Events – Occurrences that, after analysis, have no or very minor importance for information security.

- Vulnerabilities – Weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security.
- Incidents – Occurrences of events (series of events) that have a significant probability of compromising the Council's information security.
- Unknowns – Reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.

4.3 A weakness is the potential for an incident to occur.

Incidents and Weaknesses to Report

4.4 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.

4.5 Actions to fix any damage caused by an Incident must be put through Business IT change management process. Any actions should be aimed at fixing the cause and preventing re-occurrence.

4.6 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 an individual's 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 another Employee's credentials (User ID and password), either with or without their authorisation.

(Please note this list is not exhaustive)

4.7 Employees must not attempt to prove/exploit a security weakness as such an action may be considered to be misuse.

4.8 Employees must not attempt to investigate a suspected security breach as such action may compromise any investigation.

5 Reporting Procedure

5.1 All information and ICT security events and weaknesses must first be reported to an individual's Line Manager. In the absence of the individual's Line Manager, the Departmental Information Management Group (IMG) Representative must be informed.

5.2 All events and weaknesses must be reported at the earliest opportunity to the IT Service Desk.

5.3 If applicable, you must note the symptoms and any error messages on screen and await further instructions from a member of IT.

6 Management of Incidents

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

6.2 Business IT will investigate all IT related information security events and weaknesses. The System & Information Management Officer (SIMO) will investigate incidents resulting in the loss, misuse or compromise of personal data (whether real or potential). Information Security Incidents will be reported to the IT Policy & Regulation Group for review.

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

Collection of Evidence

6.4 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.

6.5 For further guidance see the Forensic Readiness and Investigation Policy.

6.6 For other incidents, including loss or compromise of hard copy information, as much information as possible on the circumstances of the incident must be collated in order to assist the SIMO to investigate.

7 Responsibilities

Information Management Group (IMG)

7.1 The role of the IMG is to co-ordinate the approach to every aspect of Information Management, and not just compliance with DPA 1998.

7.2 The group is made up of Departmental Information Management Representatives who are senior managers in each Department and are responsible for a multi-disciplinary approach to the management of information throughout their Departments.

7.3 The IMG is responsible for the overarching governance and implementation of the Policy throughout the Council.

7.4 The IMG is responsible for ensuring that all Employees are fully aware of Council policy and process, and have received appropriate training.

7.5 The IMG is also responsible for the development and monitoring of the adherence to the Policy.

7.6 IMG Representatives are responsible for ensuring any security information incidents reported to them are referred to the IT Service Desk.

7.7 IMG Representatives have a duty to ensure their Department/Service area cooperates fully with Business IT and/or the SIMO with any investigations.

IT Policy & Regulation Group

7.8 The IT Policy & Regulation Group (ITPARG) will review all incidents reported to it and advise on any further action required.

7.9 ITPARG will action any lessons learned from reported incidents/weaknesses to prevent future incidents, this will be recorded within their minutes.

7.10 Where necessary, as part of the review of reported incidents/weaknesses ITPARG may re-classify the event.

Business IT

7.11 Business IT will investigate all ICT security incidents.

7.12 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.

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

7.14 The reporting Employee must be kept informed of the progress of their reported incident.

7.15 The Service must be alerted in advance if their service levels cannot be met and an action agreed.

7.16 Incidents that are considered service affecting must be reported to the relevant Service Manager and System Owner, in order to make the necessary Business Continuity arrangements.

7.17 Incidents should be promptly reported to Internal Audit for information purposes.

7.18 Business IT will present a summary report on ICT security incidents to the IT Policy and Regulation Group.

System & Information Management Officer (SIMO)

7.19 When an information security event or weakness is reported which could potentially involve personal data the SIMO will co-ordinate the investigation alongside the relevant Line Manager or, where appropriate, conduct an investigation

7.20 The SIMO will provide advice and recommendations, where necessary, on actions to be taken following potential/actual data breaches.

7.21 All incidents will be reported to the IMG.

Line Managers

7.22 Line Managers are responsible for ensuring all Employees in their Service area adhere to the Policy.

7.23 Line Managers must report any security event or weakness to the IT Service Desk.

7.24 Where Line Managers conduct an investigation, all outcomes must be reported to the SIMO.

Employees

7.25 Employees must report any security event or weakness at the earliest opportunity to their Line Manager or the IT Service Desk.

7.26 Relevant Employees connected to an incident will be required to supply any necessary information which will help in establishing the events which led to the incident occurring.

7.27 All Employees must cooperate fully with Business IT and/or the SIMO during any investigation. Employees may be interviewed as part of this process.

8 Review and Governance

Policy Governance

8.1 The Policy will be subject to governance through the IMG, and will be formally approved by Chief Officers Group via the Executive Decision Framework.

8.2 The Policy will be subject to at least an annual review, and where changes in legislation require, more frequent.

9 Policy Compliance

9.1 If you are found to have breached this Policy, the matter will be considered and investigated under the Council's disciplinary procedure.

9.2 Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.