Incident Management Policy

Introduction

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

Purpose

The aim of this policy is to ensure that SG Systems Global reacts appropriately to any actual or suspected security incidents relating to information systems and data.

Scope

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

Definition

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

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.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

Risks

SG Systems Global 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.

Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by an the company CFO combined. It is vital for the company CFO to gain as much information as possible from the business users to identify if an incident is occurring.

For full details of the procedure for incident handling please refer to Appendix 3.

Policy Compliance

If any user is found to have breached this policy, they may be subject to [Council Name'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 [name appropriate department].

Policy Governance

The following table identifies who within SG Systems Global 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	CEO
Accountable	CFO
Consulted	CTO
Informed	All Company employees.

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 company CEO & CFO.

References

The following SG Systems Global 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.

Key Messages

- All staff should report any incidents or suspected incidents immediately by email info@sgsystemsglobal.com
- 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 department head, of the company CFO.

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' by mistake.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on SG Systems Global 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.
- Theft / loss of any SG Systems Global computer equipment.

Procedure for Incident Handling

1.1 Reporting Information Security Events or Weaknesses

The following sections detail how users and IT Support Staff 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.

1.1.1 Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from IT Support Staff.
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the company CFO through info@sgsystemsglobal.com

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 the company CFO for the impact to be assessed.

The Information Services Helpdesk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must 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.

1.1.2 Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to the company CFO. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by Information Services.

1.1.3 Reporting Information Security Events for IT Support Staff

Information security events and weaknesses must be reported to a nominated central point of contact within Information Services as quickly as possible and the incident response and escalation procedure must be followed.

Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Non compliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human errors.

The reporting procedure must be quick and have redundancy built in. All events must be reported to at least two nominated people within Information Services who must both be required to take appropriate action. The reporting procedure must set out the steps that are to be taken and the time frames that must be met.

An escalation procedure must be incorporated into the response process so that users and support staff are aware who else to report the event to if there is not an appropriate response within a defined period.

Incidents must be reported to the Business Continuity Management teams should the incident become service affecting.

1.2 Management of Information Security Incidents and Improvements

A consistent approach to dealing with all security events must be maintained across the Council. The events must be analysed, and the Security Advisor must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Council on continuing operation during the incident.

All incidents should be reported to the company CFO.

1.2.1 Collection of Evidence

If an incident may require 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. If in doubt about a situation, for example concerning computer misuse, contact the company CFO for advice.

1.2.2 Responsibilities and Procedures

Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. The security advisor from Information Services must decide when events are classified as an incident and determine the most appropriate response.

An incident management process must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the Council to those affected.

The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

The actions required to recover from the security incident must be under formal control. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

1.2.3 Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the company CFO, to look for any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

The information, where appropriate, should be shared with the Warning, Advice and Reporting Point (WARP) to aid the alert process for the region.