Corporate Information Governance Group

Information Governance Policy Framework

Incident Management Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Incident Management Policy

Background

Legislation and Compliance obligations require a robust and documented methodology to deal with Information Incident Management. This policy will ensure the council's react appropriately to any actual or suspected incidents relating to information systems and information within the custody of the councils. All staff must be aware of this policy and how to report an incident.

The CIGG will review incident reports and take appropriate action to prevent similar incidents occurring and/or improve systems for the protection of data.

Key Messages

All staff should report any incidents or suspected incidents immediately by informing the ICT Helpdesk via 01227 862043 or by emailing ictservicedesk@ekservices.org

See Appendix 1 for the Incident Management Process flow chart

All incidents that result in the unauthorised disclosure of personal or sensitive data must be reported to the CIGG. The responsible Senior Information Risk Officer, may inform the Information Commissioner's Office.

Incidents that result in a breach to the network may be reported by the EK Services Network and Security Manager to appropriate bodies.

Risks

The CIGG recognises that there are risks associated with users accessing and handling information in order to conduct official council business.

This policy aims to mitigate these 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.

Policy Detail

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.

An “information management security incident” is an adverse event that has caused or has the potential to cause damage to the 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. It may include ICT equipment but also applies to paper records, letters and any other way data is stored or processed.

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.

The record of all incidents will be managed by EK Services ICT. Anyone involved in an incident are required to work with ICT to produce that record so that it may be reported to the CIGG.

Resolution of Incidents that do not involve ICT will be managed by the organisations Senior Information Risk Officer.

Resolution of Incidents involving ICT will be managed EK Services ICT.

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

Incidents need to be reported at the earliest possible stage as they need to be assessed by a member of the IT Services team.

Responsibilities

All staff should report any incidents or suspected incidents immediately by informing the ICT Service Desk via 01227 862043 or by emailing ictservicedesk@ekservices.org.

EK Services ICT will manage the incident reporting mechanism, where an incident involves ICT equipment; ICT will manage the incident to its operational conclusion.

All incidents that result in the unauthorised disclosure of personal or sensitive data must be reported to the CIGG. The responsible Senior Information Risk Officer, may inform the Information Commissioners Office.

Incidents that result in a breach to the network may be reported by the EK Services Network and Security Manager to Gov-Cert UK, Kent Warp or PSN SIRO.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

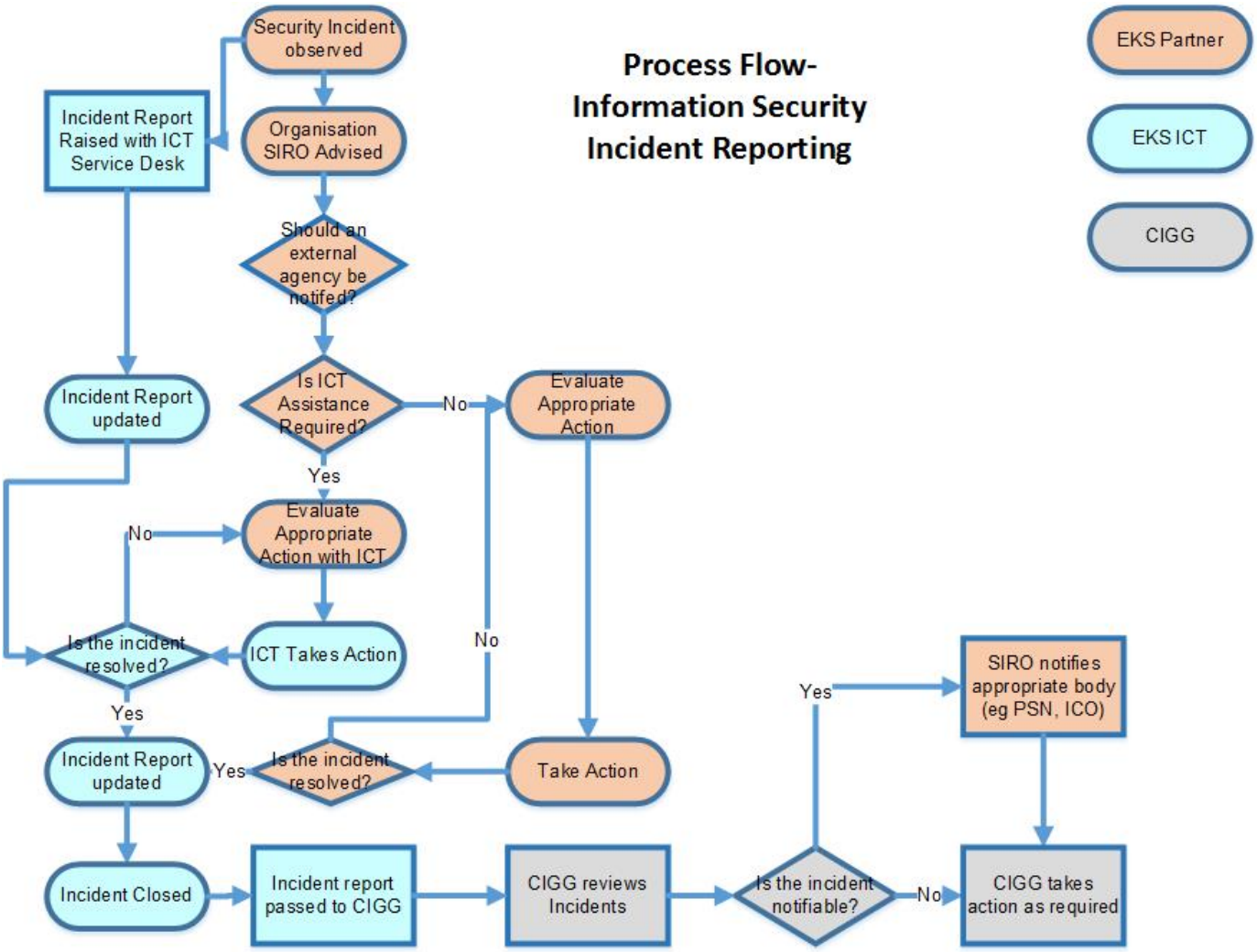
- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

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

Document Control		
Title/Version	-	Incident Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
12/12/2015	Will Causton	1.0	Initial Version
15/03/2016	Will Causton	1.1	Draft following CIGG Consultation
23/09/2016	CIGG	1.2	Final Review

Appendix 1


Process Flow-
Information Security
Incident Reporting
EKS Partner
EKS ICT
CIGG
Security Incident observed
Incident Report Raised with ICT Service Desk
Organisation SIRO Advised
Should an external agency be notifed?
Incident Report updated
Is ICT Assistance Required?
No
Evaluate Appropriate Action
Yes
No
Evaluate Appropriate Action with ICT
Is the incident resolved?
ICT Takes Action
No
Yes
Incident Report updated
Yes
Is the incident resolved?
Take Action
Yes
SIRO notifies appropriate body (eg PSN, ICO)
Incident Closed
Incident report passed to CIGG
CIGG reviews Incidents
Is the incident notifiable?
No
CIGG takes action as required

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 email or letter to the wrong person.
- 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 council equipment.
- Accessing a computer 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 council computer equipment.

Appendix 3

Procedure for Incident Handling

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.

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.
- If a computer virus infection is suspected, the computer must be immediately powered down or disconnected from the network.
- 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 ICT Service Desk via 01227 862043 or by emailing ictservicedesk@ekservices.org.

If the Information Security event does not involve ICT equipment, or example personal information files that may have been stolen from a filing cabinet, this must be reported to the organisations Senior Information Risk Officer as well as the ICT Service Desk.

The ICT Service Desk 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.

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 ICT Service Desk. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by EK Services ICT reporting outcomes to the CIGG.

Reporting Information Security Events for ICT Staff

Information security events and weaknesses must be reported to the Technical Systems Manager and/or the Network and Security Manager as quickly as possible. A work order must be opened immediately in the ITSM system and the affected organisations SIRO notified, (see Appendix 4).

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.

Responsibilities and Procedures

Management responsibilities and appropriate procedures must be established to ensure an effective response against security events.

For incidents that do not involve ICT, The Senior Information Risk Officer must decide when events are classified as an incident and determine the most appropriate response. EK Services will record and report the Incident to the CIGG on behalf of the SIRO.

For incidents that involve ICT, EK Services ICT Management will decide when events are classified as an incident and determine the most appropriate response. EK Services will record and report the Incident to the CIGG on behalf of the SIRO.

The incident management process must 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 officer responsible for an incident should risk assess the incident based on the Risk Impact Matrix (please refer to Appendix 4). If the impact is deemed to be high or medium this should be reported immediately to organisation SIRO.

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 CIGG and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted in the minutes of the CIGG

Appendix 4

Senior Information Risk Officers by Organisation.

Thanet District Council, EK Services:
Tim Howes Director of Corporate Governance & Monitoring Officer
tim.howes@thanet.gov.uk
Deputy Siro

Canterbury City Council:
Velia Coffey, Deputy Chief Executive
Velia.Coffey@canterbury.gov.uk
Deputy Siro
Matthew Archer: matthew.archer@canterbury.gov.uk

Dover District Council, EK Human Resources
David Randall, Director of Governance
David.Randall@dover.gov.uk
Deputy Siro
Colin Cook: Colin.Cook@dover.gov.uk

Appendix 5 Impact Matrix: To decide on the potential or actual impact of an information security incident, the impact matrix below should be used

Type of Impact	Reputational Media and Member Damages	Reputational Loss within Government and / or Failure to Meet Statutory / Regulatory Obligations	Contractual Loss	Failure to meet Legal Obligations	Financial Loss / Commercial Confidentiality Loss	Disruption to Activities	Personal Privacy Infringement
Low	None	None	None	None	None	None	None
	Contained internally within the council Unfavorable council member response	Internal investigation or disciplinary involving one individual	Minor contractual problems / minimal SLA failures/	Civil lawsuit / small fine - less than £10K	Less than £100,000	Minor disruption to service activities that can be recovered	Personal details revealed or compromised within department
Medium	Unfavorable local media interest Unfavorable council member response	Government authorised investigation by nationally recognised body or disciplinary involving 2 to 9 people	Significant client dissatisfaction. Major SLA failures. Failure to attract new business	Less than £100K Damages and fine	£100,000 - £500,000	Disruption to service that can be recovered with an intermediate level of difficulty. One back up not backing up for 2 or more days	Personal details revealed or compromised internally within authority. Harm mental or physical to one members of staff or public
High	Sustained local media coverage, extending to national media coverage in the short term	Government intervention leading to significant business change. Internal disciplinary involving 10 or more people	Failure to retain contract(s) at the point of renewal	Greater than £100K damages and fine	£500,000 - £1,000,000	Major disruption to service which is very difficult to recover from. Two or more systems not being backed up for two or more days	Severe embarrassment to individual(s)
	Sustained unfavorable national media coverage	Service or product outsourced through Government intervention	Client contract(s) cancelled	Over £1M damages and / or fine Custodial sentence(s) imposed	More than £1,000,000	Catastrophic disruption - service activities can no longer be continued	Detrimental effect on personal & professional life OR large scale compromise affecting many people. Harm mental or physical to two or more members of staff or public