IAPF07

Security Incident Management Policy

Purpose

This policy is part of the council's information assurance framework and establishes the security incident management requirements necessary for the council to implement its strategic objectives for information governance in accordance with the Information Governance Policy.

Information security incidents pose a significant risk to the council should they occur. The loss of information assets or impact upon services may lead to legislative or reputational repercussions. This includes punitive or enforcement action against the council or individuals by the Information Commissioner for breaches of the Data Protection Act 1998.

The specific objective of this policy is to define standards for managing information security incidents and requirements for reporting that minimise damage and allow lessons to be learnt following an incident.

Standards are required so that the council can meet its obligations under the Data Protection Act 1998 and other legislation and to meet its commitments to partner organisations and members of the public regarding the custody of information.

The standards defined allow for the establishment of effective, risk based procedures and guidelines for implementing information assurance and reinforce the council's commitment to ensuring that its information assets are protected and secure.

Scope

This policy applies to all employees, contractors and, as appropriate, third party staff who have access to council premises, information assets and associated systems and storage devices.

The policy applies to any incident that has an information security implication. This includes:

- A breach of confidentiality or an unauthorised disclosure of data (data loss or leakage).
- A loss of integrity to data or an information system.
- A temporary or permanent loss of records, information or information systems.
- Compliance failures with policies and relevant legislation, in particular the Data Protection Act and the Freedom of Information Act.

This definition may bring in incidents and problems which may normally be regarded as another type of incident e.g. a serious fire. This policy is not necessarily intended to change how those are managed but an incident report may be required so that the information assurance implications can be properly assessed.

Suspected breaches, near misses, clear weaknesses in systems or procedures and risks that cannot be addressed locally, or require input from another party, e.g. One Connect Limited come within the scope of this policy and must be reported.

Risk Assessment

The main categories of risk within the council are:

- Emerging issues affecting the council and its services.
- New projects and service developments.
- Current issues or developments within the council's existing services.
- Monitoring of performance measures.
- On-going provision of the council's services.

The Information Governance Policy defines how the management of each risk category should be evidenced and each category should be considered in applying appropriate information handling standards.

Breaches of information security can occur in a many ways and whilst often easily preventable they can have extremely serious consequences. Reported information is also useful in assessing weaknesses and corporate priorities such as training and areas for inclusion within the annual improvement programme.

In the event that the Information Commissioner's Office investigates an information security breach involving personal data, the Information Commissioner will expect to see evidence that the council implemented a robust and effective management response.

It is therefore important that any incident or possible incident as defined within the scope of this policy is reported regardless of the apparent risk. This will ensure the council has an effective means of reporting and managing risks and breaches; limiting potential negative impacts and; implementing remedial measures to prevent reoccurrence.

Standards

Once a breach of information security is identified, employees must notify their manager immediately.

If there is any indication of serious misuse or abuse that may necessitate disciplinary or possible criminal action exceptional care must be taken care to maintain the integrity of any computer related evidence. Managers must ensure that:

- ***The subject PC/Laptop or other device is not turned on or operated in any way. Do not switch off any device but isolate it, pending advice from the IG Lead.***

- ***There is no attempt to access data held on any computer media.***
- ***Any media that may be provided as evidence should be placed in an envelope or bag and immediately sealed, signed and dated. This should then be stored and locked away until required by the designated investigator. Who obtained the evidence, secured it and had control of it should be documented.***
- ***The number of people who know of the suspicions is kept to a minimum – all actions taken should be kept confidential. The original suspect may have accomplices or may be innocent of the allegations.***

The manager must ensure that the Information Security Incident Reporting Form on the intranet is completed as soon as possible. This automatically notifies the Information Governance (IG) Lead and the Data Protection Officer of the incident.

The following reporting standards apply depending upon whether the breach relates to a data protection, other security incident or a reported issue.

Data Protection Incident Reporting

If necessary the reporting manager or employee will be issued with an **Information Security Incident Investigation Report.**

The report must be completed as a matter of urgency, with as much detail as is possible. The checklist on page four of the form must be completed fully.

The completed report must be sent to the Chief Executive, the Executive Director of the affected Directorate, the IG Lead and the Data Protection Officer no later than seven days after the date of the incident to which the report refers.

The Data Protection Officer will advise the Chief Executive on whether the incident should be reported to the Information Commissioner. If this is required, the report will be issued by the Data Protection Officer.

It may be necessary to notify affected individuals of a breach of the Data Protection Act. This is particularly important if the breach may leave them vulnerable or compromise their personal safety or security. The Access to Information Team should be contacted for advice.

Other Security Incident and Issues Reporting

The IG Lead will decide upon the appropriate reporting action depending upon the type and possible severity of the reported incident or issue as follows:

Incidents or issues for corporate consideration that require no further investigation will be reported quarterly to CIGG and the SIRO.

Minor incidents will be reported to the relevant CIGG representative immediately and within the quarterly report to CIGG and the SIRO, i.e.

- Incidents or issues that have no immediate or significant impact upon information assurance standards or controls.

- Where, at the outset, there is no expectation of formal or significant disciplinary measures against any employee(s).

Major incidents must be reported immediately to all CIGG representatives and the SIRO. The SIRO will be responsible for informing the relevant Executive Director(s) and the Chief Executive as appropriate.

Other steps to be taken will depend on the nature of the incident, but consideration should be given to the following in all cases:

- In the event that any ICT equipment is lost (laptop, mobile phone, etc.) you should notify One Connect Limited at the earliest opportunity.
- If your staff ID badge is lost, you should notify the Facilities Manager at County Hall at the earliest opportunity.
- If the breach was a result of a criminal act (such as theft from a car, burglary of premises) the Police should be notified immediately and a crime reference number obtained. This should be recorded in the Information Security Incident Reporting Form.

All investigations into an incident of any type must be carried out in accordance with the Security Incident Investigation Protocol.

Emerging risks or incidents requiring remedial action outside of an investigation will be assessed by CIGG at their scheduled meetings for either addendum to the annual improvement programme or consideration for inclusion in subsequent programmes.

References

Data Protection Act 1998

Code of Conduct for Employees
http://lccintranet2/corporate/web/view.asp?siteid=2859&pageid=5795&e=e

Security Incident Investigation Protocol

The council's information assurance policy framework is designed to provide a layered approach to information security and assurance, ensuring that suitable precautions are adopted in all situations. Individual policies should not be considered in isolation but rather as elements of the whole.

Governance and responsibilities

All Managers are responsible for ensuring that relevant policies and supporting standards and guidance are built into local processes and that there is on-going compliance on a day to day basis. Any breaches or suspected breaches of confidentiality or information security must be reported in accordance with this policy.

All reported incidents will be assessed and collated by IG Lead and the Data Protection Officer.

It is the responsibility of all mangers to inform their Executive Directors, at the earliest opportunity, of possible or actual breaches of the Data Protection Act.

Executive Directors must brief the Chief Executive at the earliest opportunity.

All Managers are responsible for the identification of existing or emerging information risks relating to their service area and either addressing or reporting the issues to CIGG for consideration. Where risks cannot be addressed locally, or require input from another party, e.g. One Connect limited, they should be reported to ensure the issue can be considered by CIGG.

The IG Lead and where relevant the Data Protection Officer, in consultation with CIGG and the SIRO will decide upon the type and scale of any investigation and the necessary resources in accordance with the Security Incident Investigation Protocol.

Compliance

Non-compliance with this policy could have significant effects on service delivery and may adversely impact individuals, waste resources and cause reputational damage to the council.

The SIRO and CIGG are responsible for ensuring overall compliance with the Policy.

The council's code of conduct for employees sets out the behavioural standards that must be upheld by all employees of the council and forms part of the council's terms and conditions of employment.

Compliance with this policy is mandatory. Non compliance may result in action being taken under the council's Disciplinary Procedure and could result in dismissal from employment with the council.

A breach of policy involving a partner or third party organisation will be treated as a security incident and investigated in accordance with the Security Incident Management Policy. Appropriate action will be agreed with the SIRO taking into consideration any specific contractual recourse or sanctions available.

Document Control

Organisation	Lancashire County Council
Title	IAPF07 Security Incident Management Policy
Author	Ian Shipcott
Filename	
Owner	County Secretary & Solicitor (SIRO)
Subject	Information Governance
Protective Marking	Not Protectively Marked
Review date	

Revision History

Version	Status	Revision Date	Summary of Changes	Author
0.1	Draft	4/2/13	First Draft	I Shipcott

Review and Approvals

Title	Name	Signature	Date of Issue
IG Project Lead			
CIGG			
SIRO			

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version