Information Security

Incident Reporting Procedure

Security is everyone's responsibility

Issue	Details
Title:	Incident Reporting Procedure
Version number	Version 1.1
Officer responsible:	Senior Information Risk Owner
Authorisation by:	
Authorisation date:	
Review date:	

What is an information security incident?

An information security incident can be defined as any event or set of circumstances that threaten the confidentiality, integrity or availability of the council's information. This could include but is not limited to:

- Accidental or unlawful destruction of information (destroying or altering information to avoid disclosure)
- Loss of information (including mobile devices)
- Unauthorised alteration of information
- Unauthorised disclosure of information
- Unauthorised access to information (someone's job role does not permit them to access specific information, unauthorised access to building, hacking and ransomware attacks)

In the case of an emergency situation such as fire, bomb threat, medical or personal safety you should refer to the Civic Centre Emergency procedure or follow your site procedures as appropriate.

Breach Management

The following process should be followed to manage the breach:

- Identification – the ability to identify a breach. This can be from staff reporting, client reporting or other monitoring
  Containment – preventing any further disclosure
- Impact analysis – analysing the breach to determine what the impact will be. In terms of customer information, this will be an assessment of the impact on that customer
- Notification – consider whether the breach should be notified to the Information Commissioner and whether the customer(s) should be notified
- Remediation – identification and implementation of any mitigation that prevents a recurrence.

Why should I report an information security incident?

The council is obliged, by law, to report a personal information security incident to the Information Commissioner's Office within 72 hours of having become aware of it if the breach is likely to impact on the rights and freedom of an individual. Failure to report a breach within the 72 hour time limit may result in a fine being imposed on the council. It is therefore vitally important that all actual or potential information security breaches are reported at the earliest opportunity.

How should I report an information security incident?

If you identify an actual or potential breach of the council's information security, report the incident straight away by contacting the Executive Support Unit on extn. 5257 or fill in the online form that can be found here: http://eccintranet/forms/report-a-security-incident/ .

An appropriate member of staff will respond when a matter is reported and it is important to be available for discussion.

Investigation of an incident

On receiving a report the council will need to assess whether the information security incident impacts on the rights and freedoms of any individuals and consider the volume and sensitivity of the information. If the council considers that an individuals' rights and freedoms have been impacted, the council will need to inform the Information Commissioner's Office. The council will also need to consider whether the individual(s) concerned should be informed about the security breach.

Matters reported will always be handled confidentially and investigations will be conducted according to current best practice. The investigation will be undertaken in accordance with guidance issued by the Information Commissioner's Office and will consist of:

- Initial reporting
- Managing the incident
- Containing the data and reducing the effects
- Investigating the cause of the incident and assessing the risks
- Actions to stop the incident from happening again
- Produce final report for review by the Information Governance Forum

Depending on the nature of the incident, the investigation may identify one or more causes or contributing factors:

- problems with working practices or procedures
- council policies or procedures not being followed
- technical weaknesses of IT systems which could lead to security breaches
- attempted or successful technical attacks on IT systems
- inappropriate use of IT systems
- suspected criminal acts involving IT systems

What to consider when assessing the impact on an individual's rights and freedoms

The nature, sensitivity and volume of personal information

Ease of identification of individuals (how easy would it be for a third party to identify specific individuals or match the data with other information to identify individuals)

Severity of consequences for individuals (could the breach result in identify theft, fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm)

Special characteristics (health, child, vulnerable adult, sexuality, religion)

Number of affected individuals (the higher the number the greater the impact)

How long should an investigation take?

The investigation should be completed within 21 working days.

More information

For more information on reporting a security breach, please contact the Data Protection Officer (data.protection@exeter.gov.uk).