


Clackmannanshire and Stirling

Strategic Plan

Clackmannanshire and Stirling Integration Joint Board

Information Security Incident Reporting

2016 - 2019

Health and Social Care Partnership

Clackmannanshire and Stirling Health and Social Care Partnership ('the IJB')
Information Security Incident Reporting

1. **Purpose**

1.1. The purpose of this document is to describe the procedures for identifying and reporting, responding to, monitoring and learning from the loss or potential loss of information and ICT hardware e.g. Laptops, netbooks, iPads, smartphones, USB keys/data sticks, Vasco/Citrix tokens, or hard copies of files or documents.

1.2. The objective of Information Security Incident Reporting is to record, investigate and resolve any actual or potential breaches of information security and to take actions that will avoid or reduce the impact or probability of a similar incident in the future.

2. **Scope**

2.1. This process is applicable to all areas of the IJB.

3. **Overview**

3.1. All information and ICT equipment will be subject to formal incident reporting and escalation procedures where a loss or potential loss or other breach has occurred.

3.2. The incident reporting will be used to log all information security events including 'near misses'.

3.3. A security incident is an event which causes or could potentially cause:

- loss of equipment
- loss of system or information availability
- unauthorised disclosure of confidential information
- corruption of information
- disruption of an activity
- financial loss
- reputational damage
- legal action/breach of legislation

3.4. Examples of incidents include:

- loss of portable equipment e.g. laptop or tablet
- loss of removable media e.g. USB key
- loss of paper files containing personal and/or sensitive information
- unauthorised accessing or use of an ICT system

3.5. As soon as possible after an incident occurs, the following should be established:

- when and where the incident took place
- when the incident was discovered
- who is reporting the incident
- who was involved in the incident
- where the incident took place e.g. an address or 'in the post'
- whether this is an actual incident or a 'near miss'
- what the cause of the incident is e.g. theft, accidental loss

- the type of data (how sensitive) involved and details of who is involved if this relates to personal data
- the type of asset involved (if appropriate)
- who has been made aware of this
- who the Information Owner is and if they have been advised
- whether this has been or should be reported to Police Scotland and a crime number received

3.6. Whilst every employee is responsible for ensuring that no information security breaches occur as a result of their actions, all employees should be aware of their responsibility to report any potential suspected or actual incidents.

3.7. Information security breaches which are caused deliberately or by reckless behaviour or non-compliance with any IJB Information Management Policy and associated guidelines may result in disciplinary action.

4. Responsibilities

4.1. Users are responsible for reporting incidents promptly and providing any additional information as requested.

4.2. The Chief Officer is responsible for:

- ensuring all incidents are logged and allocated a reference number
- initiating investigation of all reported incidents timeously
- escalating to the SIRO as appropriate
- ensuring that a resolution is agreed, achieved and recorded
- approving closure of incidents

4.3. The Chief Officer is responsible for:

- ensuring that all recorded incidents are reported, where appropriate, to the IJB
- reviewing recorded incidents and making recommendations for change to processes or procedures to reduce risk of similar breaches in the future
- for agreeing the proposed reporting process and any procedure changes to reduce risk

4.4. SIRO is responsible for ensuring that the IJB is

- aware of any serious breaches
- provided with statistics on Information Compliance issues
- aware of the notification of breaches to Information Commissioner (ICO)

5. Procedure for Reporting Security Incidents

5.1. The above details should be reported to the Chief Officer as soon as possible providing as much information as possible.

5.2. Incidents will be prioritised according to their severity and impact (or potential impact) on the organisation or on the people whose data has been the subject of the incident. These priorities will be High, Medium and Low.

5.3. It is recognised that information security incidents vary that where immediate action is necessary to prevent something happening incidents may require to be resolved prior to being reported. However, such incidents should be reported as soon as possible.

5.4. Every incident, however minor, should be recorded to ensure that the risk of recurrence is avoided, reduced or mitigated.

5.5. Incidents deemed to be ‘near misses’ should also be recorded to identify areas where we may wish to improve controls or processes for the future.

5.6. Resolution of incidents will be agreed and allocated by the Chief Officer.

5.7. Where incidents may have a direct effect on individuals, these will be advised to the SIRO.

5.8. Where incidents are deemed to be notifiable to the ICO, the Chief Officer will ensure that these are processed and addressed timeously and that notification takes place as soon as possible.

5.9. Incidents will remain open until satisfactorily resolved. This may include referral to the IJB or action required by the SIRO.

5.10. All incidents will be reviewed to ensure that the risk of recurrence is mitigated.