Managing Information Security Incidents

1. Introduction

1.1 Community Justice Scotland (CJS) must take steps to protect the information and systems for which it is responsible from theft, loss, unauthorised disclosure (intentional or not), damage and destruction.

1.2 Information security incidents may involve information held in any format, for example paper, electronic, sound, visual or audio on any CJS system.

1.3 Information security incidents can cause real harm, damage or distress to children and families. They can also damage the reputation of CJS and, in some cases, where the incident involves personal data, can result in the serving of a monetary penalty notice of up to £500,000 by the Information Commissioner's Office (ICO).

2. Purpose and scope

2.1 The following procedure sets out what staff and Board Members must do in the event of an information security incident. It explains how to report suspected weaknesses or vulnerabilities in processes and systems to CJS and sets out what CJS will do in the event that an information security incident has been reported. It applies to all information and systems for which CJS is responsible.

2.2 The purpose of this procedure is to ensure that all information security incidents are reported in a correct and timely manner to allow the incident, suspected incident or weakness or vulnerability to be assessed and swift action to be taken. It is also necessary in order to ensure that all information security incidents are handled in a consistent manner with the following objectives:

a) to identify the cause of the incident, contain and recover information where possible,
b) to identify where weaknesses/risks lie and to put in place measures to address these and prevent future incidents, and
c) to ensure CJS complies with applicable legislation and regulatory guideline.

2.3 This procedure covers all circumstances where information for which CJS is responsible is stolen, lost, disclosed without authorisation (intentionally or not), damaged or destroyed, or it is suspected that any of the above has occurred. All suspected weaknesses or vulnerabilities in CJS systems or processes which may result in the above must also be reported using this procedure.

3. Reporting information security incidents

3.1 CJS must be contacted at info@communityjustice.scot within 2 working days in the following circumstances:

a) an information security incident has occurred
b) it is suspected that an information security incident may have occurred or
c) it is suspected that there are weaknesses or vulnerabilities in processes and systems which may lead to an information security incident.

3.2 If an incident has occurred, you suspect an incident may have occurred or you have noticed a vulnerability or weakness, don't assume someone else will report it. You should contact CJS directly as soon as you become aware of the incident, vulnerability or weakness.

3.3 The following information should be provided when reporting an information security event:

a) the nature of the incident/suspected incident/weakness or vulnerability;
b) the information/systems that are involved; and
c) who is involved (for example users of the information/who the information is about).

3.4 The Chief Executive, as Senior Information Risk Owner (SIRO) will nominate a lead officer who has responsibility for leading the investigation into an information security incident and ensuring an audit trail of all action taken is kept. This will normally be the Data Protection officer (DPO). Annex four contains a template to use to record all actions taken as part of the investigation.

4. Classifying a security incident

4.1 If a security incident has occurred, it is suspected that an incident has occurred or vulnerabilities in systems/processes have been identified, CJS should be contacted immediately.

4.2 If it is ascertained that an incident has occurred it must be classified as one of the following:

Event – events are occurrences that after analysis have no or very minor importance for CJS's information security

Vulnerability – weaknesses that after analysis have clear weaknesses compromising CJS's information security
Incident – occurrences of events (or a series of events) that have a significant probability of compromising CJS's information security. This category includes breaches of the Data Protection Act.
Unknown – reported events/vulnerabilities that after initial analysis are not capable of allocation to one of the four categories. Any unknowns are subject to further analysis to allocate them to one of the other three categories as soon as possible.

If there are multiple incidents to respond to, the prioritisation for action and response is:

1. Incidents
2. Unknowns
3. Vulnerabilities
4. Events

4.3 A summary of the security incident and classification should be recorded in the Security Incident Summary Log.

5. Assessment, containment and recovery

5.1 CJS will undertake an investigation in the event of an information security incident, using the forms attached in annexes one, two (where there is personal data involved) and three. The DPO will normally take the lead in investigating the incident, securing the assistance of other members of CJS staff where necessary.

5.2 Information security incidents will require an initial response to investigate and contain the situation and a recovery plan including, where necessary, damage limitation. This may involve input from specialists across CJS and its shared service business partners, such as IT. In some situations it may be necessary to seek legal advice or to contact external stakeholders and suppliers.

5.3 The Head of People will be responsible for ensuring adequate support is provided to Staff members involved in the incident. They will also be responsible for managing conduct issues in relation to the incident.

5.4 Depending on the nature of the incident, it may be necessary to suspend a staff member until the investigation is complete. If a suspension is recommended, business continuity arrangements must be put in place. If information has been lost or stolen, the DPO, with assistance from other members of CJS staff, will try to recover the information.

5.5 The CJS Senior Management Team (or representatives from the team) will approve any action taken.

6. Notification of an incident

6.1 CJS must consider who to notify in the event of an information security incident. Who to notify will be considered on a case by case basis. For example, if the incident involves personal data we may need to notify the data subject(s), the police and/or the ICO. We may also need to inform the system providers, such as Microsoft.

6.2 The DPO will inform the Senior Management Team immediately in the event of a security incident. The CJS Board and the Scottish Government Sponsor Team will be notified when the incident has been classified and assessed.

6.3 The template attached in annex three should be used to assess whom to notify, how and when.

7. Evaluation and response

7.1 It is essential to evaluate the effectiveness of our response to any information security incident. If an information security incident occurs CJS should:

- review CJS's Information Asset Register to ensure all risks are captured and the appropriate mitigating controls are in place
- review information governance policies, procedures, guidance and information sharing protocols and
- review awareness raising and training provided to CJS staff and Board members.

Annex one
Information security incident – assessment, containment and recovery

Date of event/ vulnerability/ incident	Date discovered	Date notified CJS	ID number	Classification: Event/ vulnerability/ incident	Description of event/ incident/ vulnerability	Has there been a breach of the Data Protection Act?*

*If yes, complete annex two

Description of information and/or systems involved	What is the risk to CJS?	Who should be informed of the event/incident /vulnerability?	What containment action has been taken?	How effective was the containment action?	What recovery action has been taken?	How effective was the recovery action?	What further action is recommended?	Timescales for further action

Annex two
Information security incident – for incidents involving personal data

The ICO's Guidance on Data Security Breach Management will be used to guide this process

Date of event/vulnerability/incident	
Date discovered	
Date notified CJS	
ID number	
Description of information	
Is the data sensitive personal data?	
What could the data tell a third party?	
Who does the information belong to?	

Who was involved in the breach?	
How did the breach happen?	
Who has seen the information and what have they done with it?	
Has any action been taken? Is the affected individual(s) /organisation(s) aware of the breach?	
What harm could come to the individual(s)/organisation(s) (e.g. physical safety, reputation, financial loss)	
What is the risk to CJS?	

Annex three Information security incident – notification

The ICO's Guidance on Notification will be used to guide this process

Date of event/vulnerability/incident	
Date discovered	
Date notified CJS	
ID number	

Notifying third parties

Who do we require to inform?	
What is their role?	
Are there any legal or contractual requirements to notify third bodies?	

If the information breached is personal data the following steps should also be taken:

Notifying the individual(s)

Would notifying the individual help them (could the individuals act on the information you provide to mitigate any risks e.g. change a password)?	

Notifying the ICO

What is the potential detriment to the individual? (emotional distress as well as both physical and financial damage)	
What is the volume of data that has been breached?	
What is the sensitivity of the data that has been breached?	

Annex 4
Security Incident Response – Record of Events

ID XXX	
Date	
Action	

This document was last update July 2020