ISMS 012, Managing Information Security Incidents

Document Information

Security Classification	Not Protectively Marked
Document Owner	Head of Corporate Support
(M33C) Date Last Review Published Category of amendment Completed by	26 November 2018 Minor amendments due to implications of new legislation [redacted]
(M33A/Factual) Date Last Amendment Published Category of amendment Completed by	
Date of Next Review	4th Quarter 2021
Notes	

In Case of Query Contact	Information Governance and Compliance Officer

PLEASE NOTE THAT IF YOU ARE READING A PRINTED COPY OF THIS DOCUMENT IT MAY BE OUT OF DATE. PLEASE REFER TO THE VERSION AVAILABLE ON THE SERVICE INFORMATION MANUALS INTRANET SITE

Contents

1. Introduction

1.1 The Service has a duty to its employees and the public to ensure that all data and information that is utilised and processed in the course of its business is protected from unauthorised or inadvertent disclosure which may cause personal distress or reputational damage.

1.2 The aims of this procedure are to:

- Ensure staff can identify potential Information Security Incidents and understand how to report them;
- Reduce the impact of Information Security Incidents by ensuring incidents are followed up correctly;
- To help identify areas for improvement in existing Information Security practices.

1.3 What is an Information Security Incident?

An **information security incident** is anything that could impact on the Confidentiality, Integrity and/or Availability (CIA) of our information.

This includes any suspected, attempted or actual threat of unauthorised access to SWFRS information, leading to the loss, unavailability, unlawful/inappropriate use, disclosure, modification, or destruction of information.

This applies to ALL information – paper, electronic and even verbal. It is not simply in relation to IT systems – although, a breach of an IT system would be an example of an Information Security Incident.

1.4 Why is a Procedure Required?

It is vital that we protect our all of our information so as to ensure that our operations run smoothly. Loss of information could prevent us from carrying out our core business functions and could lead to offences under legislation such as the General Data Protection Regulation.

Protecting our information against loss also allows us to fulfil obligations of confidentiality to our staff, partners, suppliers and anyone else who has entrusted us with their information.

2. Corporate Policy

2.1 This Organisational Procedure supports the Corporate Policy CP-06 Information Management and CP-07 Information Communication Technology.

3. Scope and Applicability

3.1 An "Information Security Incident" is defined as *any* occurrence or set of circumstances that would allow SWFRS information to be available to people not normally authorised to see it.

3.2 This includes internal circumstances where information is made available to SWFRS staff who would not normally be authorised to see particular information.

3.3 This procedure applies to:

- *All* data and information held or processed by South Wales Fire and Rescue Service, whether it is generated internally or received from an external source and regardless of whether this is paper, electronic or even verbally communicated information;
- All SWFRS employees, Fire Authority members, contractors and any other individual or company with access to SWFRS information.

3.4 Particular emphasis will be given to personal data and operationally sensitive information.

3.5 All employees are required to adhere to this procedure. Employees should note that any breaches of this procedure may lead to disciplinary action. Serious breaches of this procedure may constitute gross misconduct and lead to dismissal. Please refer to our disciplinary procedure OP-02.007 for further information.

3.6 South Wales Fire and Rescue Service supports an environment of mutual respect and equality of opportunity. In accordance with the Equality Act (2010), this document has been Equality Risk Assessed to ensure all Protected Characteristics are considered. Should an employee perceive that an adverse impact does exist, it is their responsibility to bring it to the attention of the Diversity Officer. This document also complies with other relevant legislation.

4. Roles and Responsibilities

4.1 Individual responsibilities

- Ensuring all information is stored and processed in accordance with prevailing legislation and guidance.
- Reporting any potential or actual Information Security incident, in line with this procedure.

We are all responsible for information security. Should any breach, or potential breach be noticed by anyone, that individual has a duty to report it.

Any intentional incident of Information Security may constitute gross misconduct and will result in disciplinary action that could lead to dismissal, and in some cases could constitute offences under the General Data Protection Regulation (GDPR), the Data Protection Act 2018 or Computer Misuse Act 1990.

4.2 Line Manager Responsibilities

- Communicating this procedure and it's content to all staff
- Monitoring the action of staff to prevent potential incidents
- Reporting of incidents, as appropriate, in line with this procedure
- Assisting the Information Governance & Compliance Officer as required when investigating actual or potential incident

4.3 Information Governance & Compliance Officer (Data Protection Officer)

- Carry out the function of Data Protection Officer (DPO) as specified in the General Data Protection Regulation (GDPR)
- To review each report of an actual or potential Information Security Incident and make recommendations to the relevant department for appropriate action
- In the case of any incident involving the loss/theft or unlawful access of personal data, contact the individual(s) affected is appropriate
- Where appropriate, refer the incident to the Information Commissioner (ICO) within the 72 hour legislative timeframe
- In the case of “serious” incidents, work with the SIRO to create a task group to fully investigate the incident and to take all appropriate action.
- Maintain a log of all actual or potential Information Security Incidents and report to SMT and FAPM on a periodic basis.
- Where incidents may affect service provision, report to the Business Continuity Management team.
- As requested, provide advice and guidance on information and data security matters in relation to storage, processing and transmission.
- Carry out or arrange periodic audit of data and information storage.

4.4 IT Security Officer

- Assist the DPO in the investigation of Information Security Incidents as appropriate.
- In the case of breaches of electronic systems, take appropriate action to prevent any further access to that information.

4.5 Joint Control Room

- Receive and record notifications of Incidents outside normal business hours (defined in this procedure).
- Notify the Senior Risk Information Officer (SIRO) as per these procedures.

5. Procedures

5.1 Identifying an Information Security Incident

If you believe that information has been lost, stolen or is simply not being handled appropriately, this represents a potential Information Security Incident.

This applies whether it is information that you are responsible for, or information which is the responsibility of someone else, and whether that information is held within SWFRS premises, or is being used externally. Whatever the circumstance, this procedure must be followed.

Accidents do happen, things will get lost or left in the wrong place – what is important is that the incident is reported promptly so that it can be investigated quickly and appropriate action taken to:

a) Reduce the risk created by the Incident
b) Prevent, or minimise the potential for, any future recurrence.

5.2 Internal Reporting of Incidents (during "normal" business hours)

For the purposes of this procedure, "normal" business hours are defined as Monday – Friday 08:30 – 17:00. Bank Holidays would be considered to be outside normal business hours.

When any incident is identified, the following action MUST be taken:

1. The individual who identifies the incident must notify the relevant line manager, who may be able to take immediate local action.

2. If you know the information has been stolen (for example, a lap top stolen from a vehicle), you must report this to the police who will give them a crime number.

3. **All** Information Security Incidents (actual or potential) must be reported to the Information Governance & Compliance Officer by e-mail to the "Data Protection" mailbox. (If e-mail is not an available option, reports can be made by telephone on 2213 or 2705).

4. The following information **must** be provided where known:

   a. Contact name and number of person reporting the incident;
   b. The type of information and/or equipment involved;
   c. Location of information and/or equipment when incident occurred;
   d. Asset numbers of any equipment involved;
   e. Whether the incident is likely to put any individual at risk;
   f. Whether the incident could lead to any further Information Security Incidents;
   g. Date and time the incident occurred;
   h. Details of *how* the incident occurred;
   i. Any action already taken by the individual, line manager or any other party;
   j. If the matter has been reported to the police, provide the crime number.

5. In the case of lost or stolen ICT equipment, the individual must also e-mail the ICT Service Desk as soon as possible including the same information. (If you cannot send an e-mail, contact the ICT helpdesk on ext 2323).This should be followed up by completion of Form O-39.

   (Note: without a Police Crime Number any ICT will consider the device lost, not stolen)

6. In the case of loss/theft of an **Airwave Radio** you **MUST** contact Control so that the lost terminal can be temporarily disabled (stunned) **within 1 hour of the discovery** (whatever time of day the incident occurred). If the device is found within 3 hours notify control who can re-enable the device.

   Where a **loss is confirmed**, the terminal **MUST** be permanently disabled “Killed” .

   If theft is suspected, the matter **MUST** be reported to the police and
   a crime number obtained for future reference; The Airwave Custodian **MUST** report the incident to The Home Office **within 4 normal working hours**

   (Loss process is detailed in the **Firelink Code of Practice Version D 2016,** and further advice on the use of Airwave can be obtained from ICT).

All incidents will be logged by the Information Governance & Compliance Officer, who will review the initial report and make recommendations for appropriate action.

5.3 Reporting “Out of Hours” Incidents

For the purposes of this procedure “out of hours” means Monday – Friday nights from 5pm through to 08:30am, weekends and any bank holiday.

Due to the potential impact of any Information Security Incident, incidents must be highlighted as soon as possible.

We also have a legal obligation to formally report certain incidents within 72 hours, therefore prompt reporting internally is essential.

Out of ours, all actual and/or potential Information Security Incidents should be reported to the Joint Control Centre, who will record all details and:

- Notify the SIRO (or the ELT member on call).
- In the case of electronic data – the out of hours ICT engineer will be informed and must take appropriate action to protect data from further harm
- Send details of the incident to the Data Protection mailbox for review the next available working day.

The SIRO (or ELT on call) will conduct an initial risk assessment. In the case of actual or potential “serious” incidents an emergency task group will be established (to include the DPO) to begin the formal investigation.

5.4 Formal Reporting of Personal Information Security Incidents

Under the GDPR, SWFRS has a legal obligation to report any Information Security Incidents involving personal information to the Information Commissioners Officer (ICO).

This currently applies only to incidents considered “serious”.

There is no specific definition of seriousness – it is based potential detriment to the individual concerned and the volume/sensitivity of the information concerned. The seriousness with be assessed by the Information Governance & Compliance Officer in consultation with the SIRO.

5.5 Monitoring of Information Security Incidents

On a monthly basis, a summary of all incidents will be reported to the Senior Management Team. These will be reported in an anonymised basis.

The exception to this will be where any gross misconduct and/or deliberate misuse of information has been identified.

6. Sources of Information and Related Documents

Source of Information
Guidance on Data Security incident management V2.0 July 2011 – Information Commissioner’s Office

Relevant Legislation (this list is not exhaustive):

- General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990

Related Documents

OP-02.007, Discipline Procedure (where data misuse results in breach of legislation)

OP-06.004, Business Continuity Management Planning Procedure
A&E/-52, Mobile Telephones

Appendix 1 – Examples of Information Security Incidents

Some obvious examples would be:

- a lost/stolen lap top or memory stick
- a case containing papers left on a train or in a public area
- allowing a virus to enter SWFRS networks through the use of mobile devices such as USB sticks

Other examples may not be quite so obvious:

- Circulating chain e-mails (these can introduce virus's, block servers and/or be considered offensive);
- Passing personal information about one colleague to another when it is not required as part of their work;
- Sensitive information found lying next to a printer
- a building not being locked or protected when it should be may allow people to have access to information within it
- An e-mail accidentally sent to the wrong people
- Allowing your computer password to be used by someone else – either with or without your knowledge
- Disclosure of information to a third party, without making suitable checks about their identity.

Information can also be lost through things such as equipment failure, or even a fire or flood.

In Summary – an Information Security Incident is any occurrence which has or may allow any SWFRS information (and/or information that we are custodians for) to be accessed by unauthorised users or which prevents SWFRS from accessing information belonging to them.