Philip Seccombe
Police and Crime Commissioner
for Warwickshire

OPCC INFORMATION SECURITY INCIDENT PROCEDURE

May 2018

Office of the Police and Crime Commissioner for Warwickshire

Procedure Title	**OPCC Information Security Incident Procedure**
Responsible Party	**OPCC Chief Executive and Monitoring Officer**

Security Classification	**Public**
Disclosable under Freedom of Information Act 2000	Yes

Policy Implementation Date	**25 May 2018**
Next Review Date Prior To	**25 May 2020**

Revision record

Version number / date	**Nature of revision**

OPCC Information Security Incident Procedure

Contents

1. Introduction 3
2. Purpose 3
3. Scope 3
4. Identifying Incidents 4
5. Reporting Incidents 5
6. Incident Classification 5
7. Notifications 6
8. Incident Management 7
Appendix A- Incident Levels 8
Appendix B- Incident Reporting Form 10
Appendix C- Incident Flowchart 12
Appendix D - Reporting to the Information Commissioner's Office 12

1. Introduction

1.1 The Office of the Police and Crime Commissioner ('OPCC') is committed to the protection of information and has in place a number of technical and organisational measures to safeguard the information it owns. This includes technical security ranging from secure passwords and system encryption, and organisational safeguards ranging from physical building and office security to procedural standards and requirements for the safe handling and storage of information. This procedure covers reporting of actual or suspected data security incidents that may be data breaches.

1.2 These procedures are **mandatory** and must be followed by all staff of the OPCC. All staff should be aware of what a security incident is in order to recognise when an actual or a suspected breach has occurred, and must take all reasonable steps to prevent the occurrence of information security incidents.

2. Purpose

2.1 The OPCC recognises that from time to time 'things go wrong' and there may be a breach of security involving information or equipment holding information. The purpose of this procedure is to ensure that all actual or potential information security incidents are reported centrally to enable the OPCC to react quickly and effectively to minimise the impact.

2.2 The aims of the procedure are as follows:

- Timely advice on containment and risk management
- Determine whether further controls or actions are required
- Consider whether the incident is required to be notified to the Information Commissioner's Office and the individual(s) affected by the incident
- Evaluate lessons learnt and areas for improvement

2.3 All information security incidents will be dealt with by the OPCC Monitoring Officer who will review and advise on incidents and make recommendations on appropriate follow up and corrective action. Specialist input will be sought from WCC Legal Services and / or ICT Service Provider where necessary.

3. Scope

3.1 This procedure applies to all OPCC staff, contractors, agency staff, volunteers and third party suppliers.

3.2 The OPCC requires organisations or individuals that provide commissioned services involving the holding or processing information on its behalf (i.e.

acting as data processors), to at least have in place internal reporting requirements equivalent to this procedure, and for any third party breaches to be reported immediately to the OPCC Data Protection Officer at Warwickshire Legal Services using this procedure.

4. Identifying Incidents

4.1 The General Data Protection Regulation (Regulation (EU) 2016/679) defines a data breach as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" Information security incidents can therefore cover a multitude of situations, but generally it will involve an adverse event which results, or has the potential to result in the compromise, misuse, or loss of OPCC owned or held information or assets. Data breaches can be categorised according to the following three information security principles:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data
- Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data
- Integrity breach – where there is an unauthorised or accidental alteration of personal data

4.2 Information in this procedure is used as a collective term and may include personal or sensitive / special category personal data as defined under the data protection legislation and also business information.

4.3 Some examples of information security incidents include (but are not limited to):

- the loss or theft of information or equipment,
- incorrect handling of protectively marked information
- poor physical security,
- hacking,
- information disclosed in error,
- unauthorised use or access to information or systems.

4.4 The impact of a security incident can vary greatly depending on the type of information or asset involved. It may for instance lead to an infringement of privacy, fraud, financial loss, service disruption or reputational damage. The

purpose of reporting an incident is not to apportion blame but to ensure that any impact is minimised and lessons learnt can be identified and disseminated.

4.5 The principles of this procedure also apply to cyber incidents i.e. any incident that could or has compromised information assets within the OPCC's digital network as provided to the OPCC by Warwickshire Police, e.g. phishing emails or hacking attacks. Any cyber related incident will be handled in accordance with police policies on cyber security.

4.6 In the event that a cyber incident also involves a data breach then it shall remain subject to this procedure and the OPCC Monitoring Officer will work in conjunction with the police cyber security team.

5. Reporting Incidents

5.1 The OPCC Monitoring Officer should always be made aware of any information security incident and the incident reported in line with this procedure.

5.2 All information security incidents should be reported immediately (and in any event within 4 hours) after a member of staff is aware of a potential or actual incident. Incidents should be reported by telephone (01926 412118) to the OPCC Monitoring Officer followed by the completion of an incident reporting form (see Appendix B) and once complete should be emailed to the Monitoring Officer.

5.3 Any incidents involving lost or stolen equipment or a network security issue should also be reported to the ICT Service provider's service desk immediately. For the purposes of this procedure lost or stolen hardware will be logged and may be subject to further investigation depending on the circumstances giving cause to the incident.

5.4 The Police should be notified immediately of any incidents involving stolen information or equipment and a crime reference number obtained. It is the member of staff who has had the equipment stolen who is responsible for notifying the police.

6. Incident Classification

6.1 The severity of an information security incident will be determined in accordance with the incident levels set out in Appendix A.

6.2 An incident will be rated in accordance with a risk classification based on agreed criteria for assessing the likelihood, severity and impact of risk. Matters to consider will include:

- The nature, sensitivity and volume of personal data
- Ease of identification of individuals
- Severity of consequences for affected individuals
- Special characteristics of people that may be affected (e.g. age, vulnerabilities)
- The number of affected individuals
- Nature of breach (e.g. error, mistake or intentional action and malicious)
- Financial or legal implications and reputational damage.

A traffic light approach will be used to plot risk whereby red is 'high' risk, amber is 'medium' risk, green is 'low' risk and for the purposes of this procedure white is 'no' risk.

6.3 It is difficult to provide a definitive list of incidents by level as each case varies depending on the circumstances, including containment and recovery, which may reduce or escalate the level at any given point. An initial incident rating will be awarded upon incident notification and may change once the facts and impact of risks has been determined.

6.4 Generally the less serious incidents will involve encrypted data or low level data including near misses whereby the severity is reduced due to swift remedial action. The more serious incidents will involve high level data which poses actual or potential high risk to people's rights and freedoms or to the organisation e.g. through the loss or release of highly sensitive personal or confidential business information.

7. Notifications

7.1 Aside from the initial reporting mentioned above the Monitoring Officer will determine whether any internal notifications or external stakeholder notifications are required to be made.

7.2 Any incidents categorised as high risk may amount to a 'serious' breach under the General Data Protection Regulation and require notification to the Information Commissioner's Office (ICO) within 72 hours. Please see Appendix D for details of what needs to be reported to the ICO.

7.3 The Monitoring Officer having sought legal advice will provide instructions on any other notifications as appropriate for e.g. affected people (data subjects).

8. Incident Management

An incident flowchart can be found in Appendix C

8.1 **Stage 1: Incident Notification**

- Any actual or suspected incidents must be promptly reported (and in any event **within 4 hours**) after becoming aware of the incident, by using the incident reporting form. The notifying officer is also responsible for reporting any incidents involving lost or stolen equipment or a network security issue to the ICT Security Desk.
- The incident reporting form requires the notifying officer to provide key details of the incident including what happened, when it occurred, what information or assets were compromised, number of people affected and any immediate action taken.
- Once the incident reporting form is received the incident will be logged centrally by the Monitoring Officer.
- The Monitoring Officer will report any breaches of personal data to ICO. Where a member of the public, information sharing partner or supplier notifies the OPCC Data Protection Officer (DPO) of a breach, it will be the DPO's responsibility to notify the Monitoring Officer.

8.2 **Stage 2 – Incident Assessment**

- The severity of an incident will be determined by the incident rating.
- Upon notification an initial assessment of risk will be undertaken by the Monitoring Officer to determine a provisional incident rating and appropriate notifications will be made as per the applicable rating. Where incidents are rated as high risk consideration shall be given if a data security breach is to be notified to the ICO. This assessment will be made as soon as possible to ensure that any breach will be reported within a 72 hour deadline (the 72 hours beginning from when the individual is aware of the breach). Any reporting to the ICO will involve prior consultation with the OPCC's Data Protection Officer.
- An incident rating may change once the full facts and impact of risks has been determined and the status of the incident will be kept under review accordingly. In addition, this may involve updating any reports to the ICO and/or other external bodies and internal persons accordingly.

8.3 **Stage 3 – Incident Investigation**

- Not all incidents will require an in depth investigation to establish the facts and determine what went wrong.

- If any additional information is required then the Monitoring Officer will contact the notifying officer or any other persons involved in the incident to seek clarification or further information.
- Any incidents rated as medium or high risk may require a full scale investigation in which case a nominated officer will be asked to investigate the incident.
- As mentioned in Stage 2 above, where an incident is high risk and may require reporting to the ICO the Monitoring Officer will consult with the Data Protection Officer and the Cyber security/IT team (as appropriate) to further assess the risk and identify any recommendations/actions. T
- The investigation should be completed and returned to the Monitoring Officer as soon as possible, taking into account the severity of the incident..

8.4 **Stage 4 – Incident Resolution**

- The completed incident reporting form and any additional information or investigation report will be reviewed by the Monitoring Officer.
- A final incident report will be produced **within 5-10 days** setting out the Monitoring Officer's (i) observations and conclusions about any information governance non-compliance issues, risks, adverse consequences or implications; and (ii) remedial recommendations to mitigate the risks and impact including preventative measures to address areas for improvement and training needs with target dates for completion.
- Any repeat or previous similar incidents will be flagged in the final incident report and may result in additional or escalated action.
- This procedure is independent of a locally commissioned disciplinary investigation but the final incident report may inform any consequential action taken or considered.

8.5 **Stage 5 – Incident Closure**

- An incident will only be closed when the recommendations have been implemented.

8.6 **Incident Flowchart**

- A flowchart setting out the incident management process as described above, is set out in Appendix C.

Appendix A- Incident Levels

An incident rating will be awarded upon reporting and may change once the full facts or impact of risk has been determined.

Levels	Description
No Risk	No breach as data protected and no impact.
Low Risk	Breach of personal or business data but low risk and impact to individuals.
Medium Risk	Breach of sensitive personal or confidential personal or confidential business data and medium risk and impact to individual(s). The personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons.
High Risk	Breach of sensitive personal or confidential personal or confidential business data and high risk and impact to individual(s). The personal data breach is likely to result in a risk to the rights and freedoms of natural persons **Decision if to report to ICO** **Decision if to report to data subjects**

Additional points to consider when assessing the incident breach rating

-The nature, sensitivity and volume of personal data

- Ease of identification of individuals

- Severity of consequences for individuals

-Special characteristics of people that may be affected (e.g. age, vulnerabilities)

-The number of affected individuals

-Nature of breach (e.g. error, mistake or intentional action and malicious

-Financial or legal implications and reputational damage

Appendix B- Incident Reporting Form

Security Incident/Breach reporting form

For Office use Only:

Incident Reference	
Incident Level	

Section 1: Details of Incident (to be completed by the Notifying Officer immediately (and in any event within 4 hoursof incident occurrence)

Notifying Officer's Name		Post	
Reporting Date		Incident Date	
DPO's Name			
DPO's Contact Details			
Brief Outline of Incident			
Whose data has been compromised / placed at risk by the incident?			
How many individuals have been affected by this incident?			
Which categories of personal data have been breached?			
Are they a:	Member of the Public YES/NO Customer Yes/No Partner YES/NO		
How many individuals have had access to the data?			
Are they a:	Member of the Public YES/NO Customer Yes/No Partner YES/NO		
Has the data been lost / disclosed outside of OPCC			YES / NO
What exactly has been compromised? (include description or a copy of data if possible)			
Description of likely consequence of data breach			
What immediate action (if any) has been taken or proposed to deal with the data breach, including			

measures taken to mitigate adverse effects.	

Section 2: Additional Information

Risk Assessment

(To be completed by the Monitoring Officer)

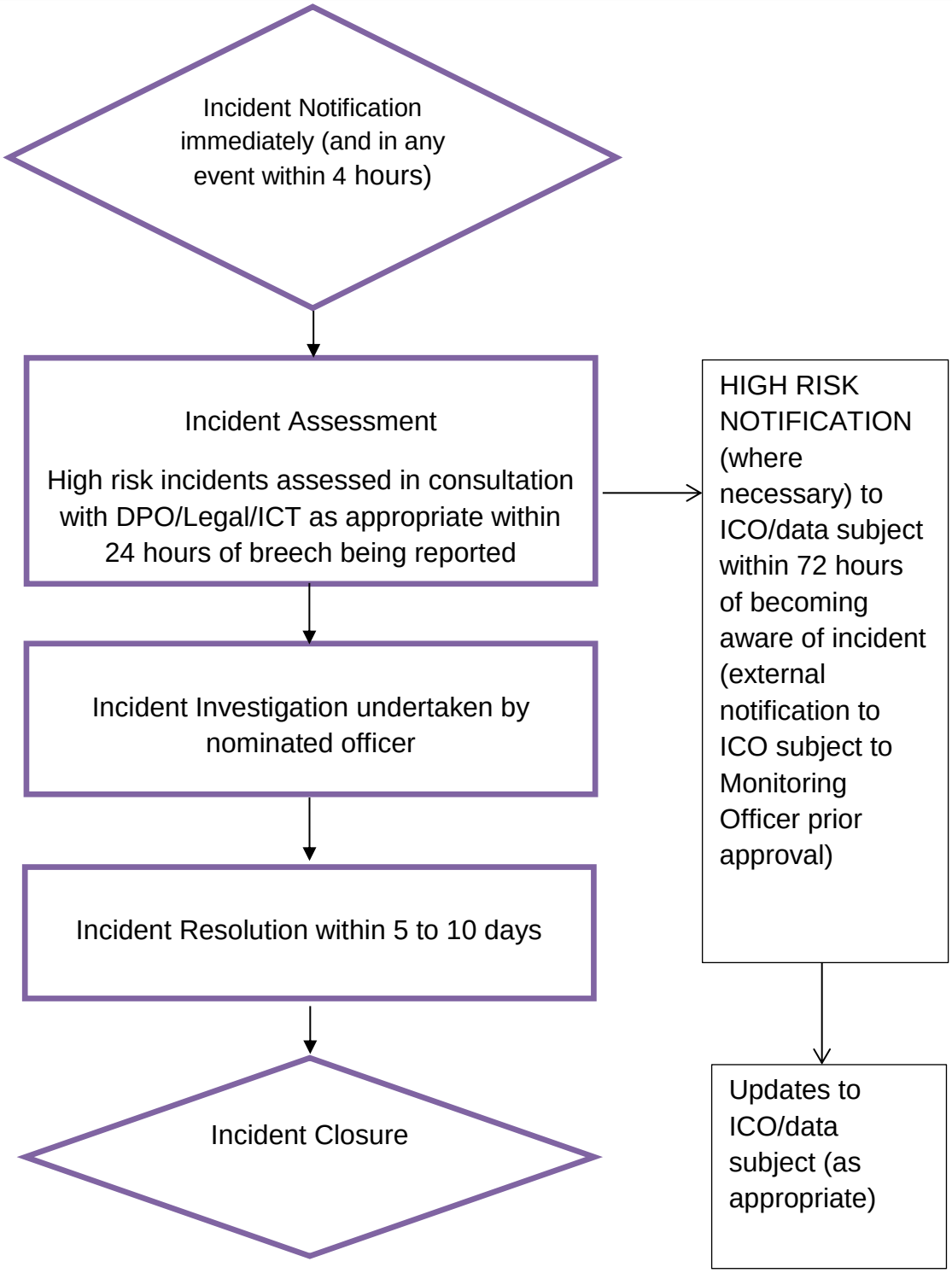
Section 3 (*To be completed by the Monitoring Officer*)

Comments

Recommendations

Recommendations

Appendix C- Incident Flowchart



Appendix D – Information to be Reported to the ICO in the Event of a Data Breach

Breaches of personal data must be reported to the ICO within 72 hours. The personal data breach helpline is available Monday to Friday between 9am and 4:30pm by calling: 0303 123 1113. Outside of these hours, personal data breaches can be reported using the online reporting form. It may be appropriate to use the online form if reporting an incident that has been dealt with appropriately or if more information is being obtained.

The following information will need to be provided:

- What has happened
- When and how you found out about the breach.
- The people that have been or may be affected by the breach.
- What you are doing as a result of the breach.
- Who the ICO should contact if they need more information and who else you have told.