STAFFORDSHIRE COMMISSIONER
Police | Fire and Rescue | Crime

Data Breach and information Security Incident Policy & Procedure

1 Introduction

1.1 Data breaches will happen to every organisation, in most cases, it is human error and could have been avoided. Some breaches will not lead to risks beyond possible inconvenience to those who need the data or equipment to do their job, for example, USB sticks, loss of laptop, or loss of information.

1.2 Other breaches may be more serious including theft of data, documents, crime information or information that is not intended for the public domain. High risk data or sensitive information, that is lost, unauthorised deletion, or has been stolen, could lead to criminal prosecution.

2 Aims and Scope of this Policy & Procedure

2.1 The purpose of this policy is to set out the procedure that should be followed to ensure that a consistent and effective approach is in place for managing data breaches and information security incidents across the Commissioner's Office. This policy applies to all of the Commissioner's staff, contractors and third-party agents handling of its information assets. The Commissioner's Office also has obligations to those systems or information that is accessed through police services or owned by them when breaches are caused by Commissioner's employees or, contractors or third-party agents.

2.2 This policy is related to the following Commissioner's office policies and forms:

- Data Incident Report
- Data Protection Policy
- Risk Management Policy

3 Definition of an incident

3.1 An incident in the context of this policy is an event which has caused or has the potential to cause damage to the Commissioner's office information assets or information compliance. Examples include:

- Accidental loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)

- Unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee)
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to Commissioner's office information or information systems

4 Responding to Breaches

4.1 In the first instance, the Data Protection Officer (DPO) should be notified, who has the responsibility to investigate compliance issues and also initiate an incident response plan to wider breaches or losses of information assets. The initial report should include full and accurate details of the incident, including who is reporting the incident, what type of incident it is, if the data relates to people, and how much data are involved.

4.2 The DPO will act as the single point of contact and will manage the issue and will inform the Commissioner's office Chief Executive, as Senior Information Risk Owner (SIRO) and also communicate to line managers and external bodies as authorised by the SIRO.

4.3 The DPO will assess whether a notification to the Information Commissioner's Office is necessary based data upon whether the breach is likely/unlikely to result in a risk to the rights and freedoms of natural persons.

4.4 The DPO's contact details are: David Morris, Office of the Police Fire and Crime Commissioner for Staffordshire, Block 9, Staffordshire Police HQ, Weston Road, Stafford, Staffordshire, ST18 0YY. The DPO can also be contacted at dpo@staffordshire-pfcc.gov.uk

4.5 The Data Incident Report Form should also be completed by the person reporting the incident and forwarded to the DPO. The DPO maintains a log of incidents which is retained for two years.

5 Time Limits

5.1 The Commissioner's office requires that once an incident is first known it should be notified to the DPO as soon as reasonably possible, but not more than 24 hours.

5.2 There is a statutory requirement for the Information Commissioner's Office to be notified of serious breaches within 72 hours of the organisation first learning of the breach. A report needs to be provided to establish the basics of the compromise or the implications of data loss, who is affected, how many, type of information. The ICO will require the name of the DPO, and for that reason the incident report needs to have already been completed.

6 Investigation and Risk Assessment

6.1 Depending on the type of incident, the DPO will instigate the relevant management actions to investigate the incident. An investigation will be started within 24 hours of the incident being discovered, where possible.

6.2 The investigation will establish the nature of the incident, the type of data involved, and where personal data is involved, who the subjects are and how many personal records were breached.

6.3 The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident, for instance whether harm could come to individuals or whether data access or IT services could become disrupted or unavailable.

6.4 The DPO will ensure that the Senior Information Risk Owner (SIRO) will be regularly updated.

7 Containment and Recovery

7.1 The DPO will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting Staffordshire Police of the incident or relevant staff for shutting down critical equipment, such as laptops or tablets.

7.2 Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

8 Notification

8.1 If a breach involving personal data has occurred, depending on whose data it is, and who the data controller is for it, other parties will need to be made aware such as Staffordshire Police, for example. The DPO will contact the ICO and communicate to the ICO the nature of investigation, outcomes or referrals to the Police / CPS.

9 Review

9.1 Once the incident is contained, a review of the event will be undertaken by the DPO and reported to the SIRO (Chief Executive). The report will detail the root cause of the incident and any contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement. Recommended changes to systems, policies and procedures will be

Policy Version Control

Date Approved: **10 April 2018**

Review Date: **Three years from approval**

Policy Lead: **David Morris**

Document Owner
Staffordshire Commissioner's Office for Police, Fire and Crime

Document Author David Morris – Data Protection Officer
Date of Approval 10 April 2018
Date of Review 1/8/2027

Version	Date	Name	Revision	Description
1.2	1/8/2024	David Morris	Update for Review and approval at IAB	Review
1.1	5/9/2018	David Morris	Change of details	Office details from OPCC to PFCC
1.0 Policy	10/4/2018	David Morris	Policy	Data Breach policy
0.1 Draft	4/4/2018	David Morris	Initial Draft	Data Breach policy

Attachments:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf