BREACH-MANAGEMENT PLAN

1.0 Introduction

1.1 The Commission recognises that, as it processes personal data, it must take appropriate measures against the unauthorised or unlawful processing of personal data and against the accidental loss, destruction or damage to such data. One of those measures is the adoption of a plan which deals with any data-security breaches.

1.2 A data-security breach can happen for a number of reasons, including:

- Loss or theft of data or equipment on which data are stored
- Inappropriate access controls allowing unauthorised use of data
- Equipment failure
- Human error
- Unforeseen circumstances, such as a fire or a flood
- Hacking attack
- "Blagging" offences (where information is obtained by deceiving the organisation which holds it)

1.3 There are four elements to the Commission's breach-management plan:

- Containment and recovery
- Assessment of ongoing risk
- Notification of the breach
- Evaluation and response

Those elements are set out in detail below.

2.0 Containment and recovery

2.1 The Commission will decide who should take the lead in investigating the breach of security (the person concerned will depend on the nature of the breach), and will ensure that he or she has the appropriate resources to investigate the breach.

2.2 It will establish who needs to be told about the breach and what they are expected to do to assist in the containment exercise – which could be isolating or closing a

compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.

2.3 It will establish whether there is anything it can do to recover any losses and limit the damage the breach can cause. For example, the recovery might involve the physical recovery of equipment or the use of back-up tapes to restore the lost or damaged data.

2.4 It will inform the police, where appropriate.

3.0 Assessment of ongoing risk

3.1 Before deciding the steps that need to be taken further to the immediate containment of the breach, the Commission will assess the risks associated with the breach – for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. In making those assessments, the Commission will take into account the following factors:

- The type of data involved and its sensitivity
- If data have been lost or stolen, whether there are any protections in place, such as encryption
- What happened to the data (where data have been stolen, they could be used for purposes which are harmful to the individuals to whom they relate; whereas damaged data pose a different type and level of risk)
- What the data could tell a third party about the individuals concerned
- The number of individuals whose personal data are affected by the breach
- The individuals whose data have been breached – whether, for example, they are Board Members, staff, applicants or witnesses
- The harm that could come to those individuals – whether there are, for example, risks to their physical safety or reputation
- The wider consequences, such as the loss of public confidence in the Commission

4.0 Notification of breach

4.1 The Commission recognises that informing individuals and organisations that it has experienced a data-security breach can be an important element in its breach-management strategy, but that informing them about a breach is not an end in itself. In deciding whether to inform individuals and organisations about a breach, and whom to inform, the Commission will take into account the following factors:

- Whether there any legal or contractual requirements

- Whether notification will help the Commission meet its obligations under the seventh data protection principle

- Whether notification will help the individual

4.2 Where the Commission decides to inform individuals and organisations about a breach, it will provide them with the following information:

- A description about how and when the breach occurred, the data that were involved and details of the measures the Commission has carried out to respond to the risks posed by the breach

- Clear advice about both the steps they can take to protect themselves and the steps the Commission is willing to take to help them

- The way in which they can contact the Commission for further information or to ask it questions about what has occurred

4.3 Where the Commission decides to notify individuals and organisations about a breach, it will identify the most effective way in which to notify them. Where it needs to notify children or vulnerable adults, it will give specific consideration to the method of notification.

4.4 The Commission will report to the ICO any "serious" breaches of its security which resulted in the loss, release or corruption of personal data. In notifying the ICO of any such breach, the Commission will include details of the security measures and procedures it had in place at the time the breach occurred.

5.0 Evaluation and response

5.1 The Commission recognises that it is important both to investigate the causes of any breach and to evaluate the effectiveness of its response to the breach. Clearly, if the breach had been caused, even in part, by systemic problems, then simply containing the breach and continuing "business as usual" is not an acceptable approach. Similarly, if inadequate policies or a lack of a clear allocation of responsibility hampered the Commission's response, it is important to review and update those policies and lines of responsibility. In evaluating the effectiveness of its response to any breach, the Commission will carry out the following procedures:

- It will re-examine what, where and how personal data are held

- It will establish where the biggest risks lie, and will identify further potential weak points in its existing security measures

- It will ensure that the methods of transmission of data are secure and that it discloses only the minimum amount of data necessary

- It will monitor staff awareness of security issues and look to fill any gaps through training

Date approved	16 August 2013
Date of last review	8 February 2016
Date of next review	8 February 2017