FSA Security Incident Procedure

Published: May 2015
Latest Review: May 2015
Next Review Date: May 2016

Document control

Changes history

Revision No.	Revision date	Purpose of revision and paragraph number	Revised by
1.0	April 2011	Transfer from Policy to a Guidance document	S40 (2) & (3)
1.1	October 2013	Annual Revision	S40 (2) & (3)
2.0	April 2014	Update and change of layout to new Procedure Document	S40 (2) & (3)
2.1	December 2014	Update due to change of Incident form	S40 (2) & (3)
3.0	May 2015	Annual Revision	S40 (2) & (3)

Contents

Introduction

What is the purpose and aim of this document?

The purpose of this document is to provide a framework of procedures, standards and controls to protect the FSA's information from all threats, whether internal or external, deliberate or accidental.

Who is does this document apply to?

This procedure applies to all employees, contractors, consultants and temporary employees working for and on behalf of the Food Standards Agency.

Everyone who works with government information has a responsibility to protect the confidentiality and integrity of any HMG information and data that they access.

What is a Security Incident?

A security incident is an event that may cause the loss of FSA assets, information, or the disclosure of information to someone not authorised. These incidents may be accidental as well as deliberate and include events such as:

- Suspected viruses
- Misuse of internet or email
- Breaches of physical security
- Damage or loss of personal property
- Unauthorised disclosure of Information
- Loss of Assets

What to do if an incident occurs?

Please complete the Incident Reporting form and send to the S40 (2) & (3) mailbox

Who Can Report a Security Incident

Everyone must report possible security incidents, because if incidents are not reported the FSA will be unaware of security breaches and remedial action cannot be implemented. The Agency would be unable to assess trends in security so it can meet the evolving demands of threats and vulnerabilities.

No one will be criticised for raising a security incident report that turns out to be a false alarm. Likewise, if you accidentally cause a breach of security, you should

report the breach so that FSA as a whole can learn from the incident and remedial changes to the system can be made. No one will be criticised for causing an accidental security breach as long as it is reported.

What Happens after the Incident has Been Reported

Users responsible for equipment that has been affected by a security incident should not attempt any action on or with that equipment, but follow the instructions from the Security Manager. Individuals affected by a security incident should document, in writing, as much information about the incident while waiting for a response (do not use affected equipment). Examples of information to document include: date, time, description of suspicious activity, duration of activity, any dialog boxes or messages, system behaviour, or anomalies. Any information provided will aid in responding in an appropriate manner.

The Security Manager in conjunction with appropriately authorised security personnel will determine the course of remediation on a case by case basis.
If at such time an incident has become apparent, and the physical location or responsible user of the affected device cannot be immediately ascertained, the ICT Service Desk may disconnect the network connection.

Who should I contact for further information?

For further information please email the S40 (2) & (3) team: S40 (2) & (3) @foodstandards.gsi.gov.uk

Annex A – Flow Diagram