Security Incident Reporting Policy

Policy | Security Incident Reporting Policy
---|---
This policy is authorised by | Information Assurance and Exploitation Committee (IAEC)
This policy applies to | Office for National Statistics (ONS) and UK Statistics Authority
This policy was introduced in | March 2012
Policy Owner | Head of Information Assurance (HIA) Louise Bader-Jones
Other Contacts | IT Security Officer (ITSO)
Next Review | September 2016

Part 1 - Security Incident Reporting Policy
Part 2 - Security Incident Reporting Procedures

1.0 Introduction
2.0 Policy Statement
3.0 Scope
4.0 Definition of a security incident
5.0 Roles and Responsibilities
6.0 Modifications to the policy
7.0 Staff with specific needs
8.0 Failure to comply
9.0 Complaints

1.0 Introduction

The purpose of this policy is to ensure staff within the organisation are able to quickly identify, monitor and rectify any weaknesses in its security regime. Each security incident presents unique circumstances requiring case-by-case examination by the Security Incident Team (SIT).

Back to the top
It is essential that individuals understand how to report a security incident. Security incidents should be reported quickly through the appropriate channel so that they can be dealt with in a swift, consistent and professional manner.

3.0 Scope

All information security incidents, which include’s physical, personnel and information assurance are within scope.

4.0 Definition of a Security Incident

A security incident is defined as ‘non compliance with security policies and procedures, or any fact or event which you think could affect the organisation’s personnel, physical and/or information security’.

5.0 Roles and Responsibilities

5.1 Director Generals (DG)

The Director Generals are responsible for the implementation of this policy across the organisation.

5.2 Executive Directors and Deputy Directors

Executive Directors and Deputy Directors are responsible for:

- implementing this policy on behalf of the DG by ensuring their staff are fully aware of this policy and the operating procedures
- encouraging a ‘responsible’ culture which encourages staff to report all types of incidents
5.3 Security Incident Team (SIT)

The Security Incident Team (SIT) is a fluid structure that is formed on a case by case situation. The team will consist of two or more of the following:

- Senior Information Risk Owner (SIRO)
- Departmental Security Officer (DSO)
- Head of appropriate security regime (for example, Information Assurance (IA), Physical Security, Personnel Security)
- Media Relations
- Executive Director or Deputy Director of the business area affected by the incident

The SIT is responsible for:

- assessing the reported incident and contacting the person who has logged the call to find out more detail before deciding on the appropriate action (if necessary)
- determining who will lead the investigation, if one is required
- examining all of the individual resolution plans submitted by the various representatives involved with remedying the incident and drawing these plans together into a single action plan to ensure that all actions are taken at the appropriate time
- passing the call to the appropriate area for action or closure if an investigation is not needed or it is not considered a security incident
- recording all actions on a timeline record to outline progress made against the action plan and creating a lessons learned paper for implementation

5.4 Human Resources

The Human Resources Department are responsible for the management of any personnel or misconduct matters arising from the investigation of security breaches.

5.5 Line Managers
Managers are responsible for:

- ensuring their staff understand and comply with the organisation’s policies and procedures
- instigating any initial action proportionately with the nature and seriousness of the occurrence and taking measures to secure any assets
- ensuring that incidents and breaches are reported in accordance with operating procedures
- co-operating in any subsequent investigation

5.6 Staff

All staff are responsible for:

- ensuring that they understand and comply with the organisation’s policies and procedures
- reporting any incident in accordance with these procedures
- co-operating fully in any incident investigations

6.0 Modifications to the policy

It is recognised that changing issues and circumstances may require future revision to the policy/procedures.

A formal review will be undertaken every 12 months or after a major incident, though the policy may be modified as appropriate from time to time as agreed by the Policy Owner, Information Assurance and Exploitation Committee (IAEC) and, if appropriate, in consultation with the Departmental Trade Union Side (DTUS).

7.0 Staff with specific needs
Staff with specific needs/requirements in relation to this policy and related procedures will be given consideration on a case-by-case basis.

8.0 Failure to Comply

Failure to report a security incident that you are aware of could result in disciplinary action in line with the organisation’s Discipline policy.

Serious or repeated breaches of security, which include deliberate or damaging behaviour, may lead to the withdrawal of an individual’s security clearance and may also be subject to disciplinary action as detailed in the Discipline Policy.

9.0 Complaints

Staff making a complaint in relation to the application of this policy should refer to the organisation’s Grievance Policy.