

Information Security Incident Management Procedure

Reference: DSP DOC 00-27

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 02/03/2021

Organisation Issue Date:

1. Scope

All Users (whether Employees/Staff, contractors or temporary staff, and third-party users) and all Owners of Organisation Name information security assets or systems are required to be aware of and to follow this procedure.

2. Responsibilities

2.1 Users and Owners of Organisation Name information security assets are required to follow this procedure for reporting information security weaknesses or events.

2.2 Information security events and weaknesses are reported to the Chief Information Security Officer (CISO).

<<2.3 removed for sample purposes>>

3. Procedure

3.1 Reporting information security events and weaknesses

3.1.1 Information security weaknesses, events and incidents are reported immediately when they are seen or experienced to the Chief Information Security Officer (CISO), using the agreed format. The person making the report will email a copy of the completed form to the Chief Information Security Officer (CISO). The email will be flagged 'Urgent', and where possible will be preceded by a telephone call to the Chief Information Security Officer (CISO). All reports should also be followed up by a telephone call to the Chief Information Security Officer (CISO).

3.1.2 Users are not allowed to continue working on an affected system until an identified possible weakness or information security event has been resolved and they are authorised to resume working by the Chief Information Security Officer (CISO).

<<3.1.3 removed for sample purposes>>

3.2 Responding to information security incidents

3.2.1 All information security weaknesses, events and incidents are, immediately upon receipt, assessed and categorised. As part of closing out the event or incident, this assessment is documented.

3.2.2 Initially, there are four categories: events, weaknesses, incidents and unknowns.

- <<Content removed for sample purposes>>

3.2.3 The 'unknowns' are subject to further analysis to allocate them to one of the other three categories as soon as possible.

3.2.4 When there are multiple event reports in each category, the Chief Information Security Officer (CISO) prioritises responses in the light of the criticality of the business systems and information assets at risk and the danger of further compromise to Organisation Name's information security.

3.2.5 The NHS places specific requirements on incidents involving personal data and information security including cyber attacks.

<<Content removed for sample purposes>>

It is expected that the type of incidents reported would be of a serious enough nature to require investigation by Organisation Name. These types of incidents could include:

- <<Content removed for sample purposes>>

Guidance on reporting using the DSPT IG Incident Reporting Tool should be followed for all SIRIs.

3.2.6 Once the incident is contained, and the required corrective action is completed, the Chief Information Security Officer (CISO) reports to the Information Security Manager with a summary of the incident, where necessary identifying the cause of the incident and analysing its progress, trying to identify how Organisation Name could have responded earlier or more effectively, or preventive action that might have been taken in advance of the incident, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out.

3.2.7 The Chief Information Security Officer (CISO) is responsible for closing out the incident. This includes any reports to external authorities, initiating disciplinary action

as appropriate by referring the incident to the Information Security Manager, planning and implementing preventive action to avoid any further recurrence, initiating any action for compensation from software, service or outsource suppliers by referring the incident to the Information Security Manager, and communicating with those affected by or involved in the incident about returning to normal working and any other issues.

<<3.2.8-3.2.9 removed for sample purposes>>

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).