North Hampshire
Clinical Commissioning Group

South, Central and West Commissioning Support Unit

Security Incident Handling Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Philip Evans - Director of IT Services
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Next Review date:	25/05/2018
Target audience:	All NHS South, Central and West CSU staff

Document Control Sheet

Title	**ICT Security Incident Handling Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Philip Evans
Date Created	29/12/2015
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
1.1	29.12.15	Philip Evans	Re-write specifically for SCW CSU
1.2	5.2.2016	Philip Evans	Updated to final following IG Steering Group review
1.3a	08.09.2016	Arif Gulzar	Updated the policy review date
1.3b	04.10.2016	Arif Gulzar	Policy signed off by Information Governance Steering Group
2.0	29.11.2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14.12.2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	Title and contact
Philip Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1 Introduction

This document forms part of the NHS South, Central and West Commissioning Support Unit (SCW CSU) Information Security Management System.

This document provides detailed policies that govern the handling of reported security breaches.

1.1 The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that:-

- Set out the governance of IT security;
- Provide high level policy statements on the requirements for managing IT security;
- Define the roles and responsibilities for implementing the IT security policy;
- Identify key standards, processes and procedures to support the policy;
- Define security architectures that encapsulate the policy and support the delivery of secure IT services.

1.2 Document Purpose

This document provides the detailed security event handling policy statements that support the overall IT security objectives of SCW CSU as set out in the security statement in the ISMS.

2 Security Incident Handling Policy

2.1 Objective

All information security breaches must be reported. Once reported all security breaches must be handled in a consistent manner by recording, investigating and providing an appropriate response.

This document provides a framework for handling security breaches within SCW CSU. It outlines the steps to be taken after a security breach has been reported.

2.2 Security Incident

A breach in information security is defined in terms of the three levels of information security i.e. a weakness, event or incident. For the purposes of this policy, all such breaches will be referred to as a security incident.

2.3 Handling Policy Overview

The management of each security incident (once it has been reported) requires that the following procedural steps must be followed:

- Recording: Create an Security Incident log
- Investigate: Investigate the incident
- Respond: Resolution identified
- Resolution implemented (where applicable)
- Report produced (where applicable)
- Appropriate documentation updated
- SCW CSU senior management advised
- SCW CSU staff advised (e.g. procedural changes, additional training)

In all cases, progress and outputs will be recorded within the security incident record.

3 Procedure for suspected Incident

Once reported, all the relevant details corresponding to a security incident will be recorded, either in the service desk reporting systems or on a secure log maintained by the Information Security Manager.

The format of the Security Incident log is listed in Appendix A.

4 Investigation of a Security Incident

When a security incident is reported or received, a decision will be made as to whether an investigation into the incident will be carried out and who will be tasked to carry out the investigation. Within SCW CSU, the Information Security Manager and the senior management team are authorised to conduct security incident investigations.

All investigations will be treated in confidence and disclosure. Appropriately trained individuals with the relevant knowledge will advise on appropriate course of action and further actions to be taken.

Security investigations must address the following:

- What happened and its impact?
- Why it happened and how?
- What needs to be done immediately to prevent further damage and facilitate initial recovery?
- What needs to be done in the longer term to prevent a further occurrence or what risks need to be acceptable by the business?
- Identify if any person is culpable and whether disciplinary action is necessary?

4.1 Security Investigation Records

For all SCW CSU investigations, an investigation record or incident log must be maintained throughout the time of the investigation and the resolution of the breach. All investigations will be classified as confidential and handled accordingly.

Investigation records must include details of the nature of the breach:

- When, how and who discovered the breach
- To whom and when was the breach escalated
- Details of recommended actions
- Details of actions taken or risks accepted, when, and by whom, together with results
- Details of any emergence measures implemented to contain the exposure
- Details of agreed permanent solution impact assessment

4.2 Collection of Evidence

Paper Documents

Any paper information retained as evidence must be kept securely, with a record of the individual who found the document, where the document was found, when it was found and, if applicable, who witnessed the discovery. This information must be recorded in an investigation log. Any original documentation retained, as evidence, must not be tampered with.

Information Held Electronically

Mirror images or copies of any removable media (hard disks or in memory) should be taken to ensure availability. A log of all actions during the copying process should be made in an incident log. The copy process should be witnessed by a suitable line manager. The original image (or mirror/copy image) including log should be kept securely and untouched.

5 Responding to a Security Incident

5.1 Report and Retention

On completion of every investigation, a report is to be submitted by the investigator to the SCW CSU senior management team and held centrally in a secure repository and retained for a period of not less than three years.

5.2 Learning from Incidents[5]

Once an information security incident has been closed, it is important that the lessons learned from the handling of the information security incident are quickly identified and acted upon. This could include:

- Implementation of additional controls (physical, technical or procedural)
- Raising security awareness
- Changes to the information security incident management process

The Information Security Manager will need to look beyond a single information security incident and check for trends/patterns and report to the SCW CSU senior management team

on possible safeguards. In the event of an IT oriented information security incident, it is strongly advised to conduct information security testing, particularly vulnerability assessments.

Information contained within an information security incident database or incident log should be analysed on a regular basis in order to:

- Identify trends/patterns
- Identify areas of concern
- Analyse where preventative action could be taken to reduce the likelihood of future incidents.

5.3 Identification of Security Improvements

During the review process of a security incident, additional controls may need to be implemented by SCW CSU. The recommendations or related additional controls may not be feasible (financially or operationally) to implement immediately, in which case a Risk Assessment should be conducted and the actions added to the SCW CSU Risk register for acceptance and implementation by management.

6 Review of Policy

6.1 Review Timetable

As part of the Information Security Management System this policy will be reviewed on an ongoing basis by the SCW CSU IT Services senior management team.

Appendix A - Example of a 'security incident log'

Unique reference	
Date	
Heat Reference	
Severity (1 to 5)	
User details	
Description	
Assignee	
Action Taken	
Date Fixed	
Control Updated / Implemented	

ISO27001 Cross Reference

[1] ***A 13.1.1 Reporting information security events***

[2] ***A 13.1.2 Reporting security weaknesses***

[3] ***A 13.2.1 Responsibilities and procedures***

[4] ***A 13.2.3 Collection of evidence***

[5] ***A 13.2.2 Learning from information security incidents***