Procedure for Correction and Corrective Action

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	First Draft	27/07/2018
V 1.0	Andrew Clarke	CISO approval	06/08/2019

Document Approval

The contents of this document are classified as Protect to Brunel University London (University) information classification. Proprietary information presented in this document may not be used without written consent from University and remains the exclusive property of University unless otherwise agreed to in writing.

This document requires the approval from University as defined in the ISMS Compliance document.

A Clarke	Mick Jenkins
Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

The purpose of this document is to define the procedure for dealing with non-conformities and/or discrepancies for the purpose of taking correction and/or corrective action in order to identify improvement opportunities within the overall Information Security Management System.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
All staff	• To identify and report any non-conformities / improvement opportunities • To provide information and/or assist with root cause analysis
Business Process Owners Information Asset Owners Line Managers	• To carry out root cause analysis • To feed all improvement opportunities to the management specialists
Management Specialists	• To carry out root cause analysis • To provide resolution for any NCR disputes • To provide NCR details to Cyber & Information Security manager
Cyber & Information Security Manager	• To ensure the details are logged in the Non-Conformance & Improvements Report Log
Internal Auditors	• To periodically Audit schedule REC 18MS-1A Internal Audit Schedule and formally evaluate, identify and report to management all improvement opportunities

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A.18 – Compliance
ISO 27001:2013 Conformance Control	Information backup A.18.2.2 Compliance with Security Policies & Standards

1.4 Scope

This procedure applies to all items which are not conforming to the criteria contained within the documented requirements of the information security management system.

The information security management system shall undergo continual improvement and review. In order to do this it is necessary to take actions to change existing practices, processes, policies, procedures etc. This is generally done as a result of identifying improvement opportunities and acting upon them.

The purposes of the following processes are to ensure that any requirement(s) are not being fulfilled are identified and controlled and that corrective and/or preventive (correction) action is taken in order to improve the overall delivery of the information security management system.

An improvement opportunity which happens prior to an event is known as a 'preventive action' and one that occurs post event is generally known as a 'Correction'. This procedure covers correction & preventive (corrective) actions.

Corrective action can be taken to prevent NCR happening again in the future.

1.5 Identification

Correction: action to eliminate a detected nonconformity.
Corrective action: action to eliminate the cause of nonconformity and to prevent recurrence.

Corrective Actions could be identified from (but is not limited to);

- Feedback (compliment or complaint)
- Management Meetings
- Staff suggestions
- External Audits
- Internal Audits
- Security and Business Continuity events
- Non-conforming (defective) products or services
- Breaches of SLAs
- Results of measurements and metrics
- Service / Maintenance Reports
- Inspections and Testing
- Software development
- Risk assessment
- Management review
- Audits
- Business continuity plan testing
- Staff / student suggestions
- Market intelligence analysis
- External environment / competitor analysis
- Future planning exercises / workshops

2.0 Correction and Corrective Process

Examples of non-conformances are detailed in the sections above. When staff or third parties become aware of any non-conformance they must be communicated to line managers, the information asset owner or management specialists by means of a non-conformance report (NCR). This can be either verbally, by email or by completing a Non-Conformance Report.

The line manager, information asset owner or management specialist competes the Non-Conformance Report and submits this to the Cyber & Information Security Manager to be logged in the Non-Conformance & Improvement Report Log along with other information, including the;

- Name of the person raising the NCR
- Date raised
- Log number
- Details of the non-conformity

The process for dealing with correction shall include:

- Investigating & identifying the cause of the specific non-conformity
- Use appropriate techniques to analyse the data available
- Specifying the actions taken to remove the non-conformity
- Identifying actions to prevent the recurrence of the non-conformity
- Ensuring appropriate authority for dealing with customer complaints

The process for preventive/corrective actions shall include:

- Identifying causes for potential non-conformities
- Use appropriate techniques to analyse the data available.
- Specifying the actions taken to prevent potential non-conformities
- Identifying the actions necessary to prevent the occurrence of a non-conformity

All actions must be agreed with the owner(s) of their function(s) (or the representative) and an appropriate timeframe agreed for completion.
Once completed the record shall be signed off.
Any action required that is not implemented is to be escalated to the Chief Information Security Officer for resolution.

In all the above, the following points will be applied:

- Record all actions on the Non-Conformance & Improvement Report Log and communicate the result to all concerned
- Retention period for non-conformance reports are defined in the Record Control Procedure
- Validate that identified corrective measures / actions including code fixes or bypasses, design updates, documentation corrections, process changes, and customer notifications are applied appropriately

- Monitor & review the implementation of the above actions
- NCRs are also provided to the auditors during internal audits for the follow up purposes to measure the effectiveness of the corrective actions taken.

3.0 Management review

Corrective actions will be reviewed as part of the Management Review.

As a result of analysing the inputs at management review meetings, management may decide to take actions to further address the root causes of non-conformities.

These further actions to eliminate root cause shall also be recorded in the corrective action log Non-Conformance & Improvement Report Log.

4.0 Deliveries

- The Non-Conformance Report Log
- The record control procedure
- The management review procedure