[organization logo]

[organization name]

**PROCEDURE FOR CORRECTIVE ACTION**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415655775)

[2. Reference documents 3](#_Toc415655776)

[3. Corrections and corrective actions 3](#_Toc415655777)

[3.1. Nonconformities and corrections 3](#_Toc415655778)

[3.2. Corrective actions 3](#_Toc415655779)

[3.3. Implementation of corrective actions 3](#_Toc415655780)

[4. Managing records kept on the basis of this document 4](#_Toc415655781)

[5. Validity and document management 4](#_Toc415655782)

[6. Appendices 5](#_Toc415655783)

# Purpose, scope and users

The purpose of this procedure is to describe all activities related to the initiation, implementation and keeping of records of corrections, as well as corrective actions.

This procedure is applied to all activities implemented in the Information Security Management System (ISMS) [Business Continuity Management System (BCMS)].

Users of this document are all employees of [organization name].

# Reference documents

* ISO/IEC 27001 standard, clause 10.1
* ISO 22301 standard, clause 10.1
* BS 25999-2 standard, clause 6.1
* Information Security Policy
* Business Continuity Policy
* Internal audit procedure
* Incident management procedure

# Corrections and corrective actions

## Nonconformities and corrections

A nonconformity is any failure to meet the requirements of the standards, internal documentation, regulations, contractual and other obligations within the ISMS. Nonconformities can be identified during an internal or external audit, based on results of the management review, after incidents, during normal business operations or on any other occasion.

An employee who notices a nonconformity must take immediate action to control it, contain it and correct it, and to deal with its consequences; if an employee is not responsible for such nonconformity he/she must forward information about that nonconformity to a responsible person, who must make a correction.

## Corrective actions

Said responsible person must evaluate the need to eliminate the cause of nonconformity and prevent its recurrence by taking corrective actions. The main difference is that corrective actions eliminate the cause of a nonconformity, whereas the correction focuses only on controlling the nonconformity and dealing with direct consequences.

Corrective action may be initiated by any employee or (where appropriate) client, supplier or outsourcing partner of the organization. Corrective action may require that changes be made to any document, process or arrangement within the ISMS.

## Implementation of corrective actions

Corrective action is implemented in the following way:

|  |  |
| --- | --- |
| ***Step*** | ***Person responsible for implementation*** |
| 1. Reviewing the nonconformity | Anyone with a role in the ISMS |
| 1. Determining the cause of nonconformity | Person responsible for the area where the nonconformity has been identified |
| 1. Identify if similar nonconformity already exists | Person responsible for the area where the nonconformity has been identified |
| 1. Evaluating the need for action to eliminate the nonconformity | Person responsible for the area where the nonconformity has been identified |
| 1. Determining the actions needed to eliminate the causes of nonconformity and to ensure that nonconformities do not recur | Person responsible for the area where the nonconformity has been identified |
| 1. Implementation of planned actions | Person in charge of implementation, appointed by the person responsible |
| 1. Reviewing whether the action taken resulted in the elimination of causes of nonconformity | [job title] |
| 1. Informing all persons concerned that corrective action has been implemented | Person in charge of implementation, appointed by the person responsible |
| 1. Making changes to the ISMS, if necessary | Person who is in charge of coordinating the ISMS |

Each of the above steps must be recorded in the corrective action form.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
| Corrective action form | [name of filing folder, in which cabinet] [intranet folder name] | [job title] | After all data has been recorded, any new additions or editing must be disabled | 3 years |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number of initiated corrective actions
* number of incomplete corrective actions
* number of corrective actions taken without having been recorded in a designated form

# Appendices

* Appendix – Corrective Action Form

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]