[Organization logo]

[Organization name]

CHANGE MANAGEMENT POLICY

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

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The purpose of this document is to define how changes to information systems are controlled.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology within the scope.

Users of this document are employees of [organizational units for information and communication technology].

2. Reference documents

- ISO/IEC 27001 standard, clause A.8.32
- Information Security Policy

> **Commented [27A5]:** You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

3. Change management

Each change to operational or production systems must be made in the following way:

> **Commented [270016]:**
>
> **Commented [270017]:**

1. change may be proposed by [specify job functions]
2. ~~Change must be authorized by [job title], who must assess its justification for business with potential negative security impact~~
3. ~~change must be implemented by [job title]~~
4. ~~[job title] is responsible for: checking that the change has been implemented in accordance with the requirement~~
5. ~~[job title] is responsible for testing and verifying the system's stability~~ - the system must not be put into production before thorough testing has been conducted
6. ~~implementation of changes must be reported in the following journal, title will necessary and date~~
7. ~~[job title] is responsible for updating all the document policies, procedures, plans, etc.) that~~ have been affected by the change

~~Change records are kept generally the same of this from, i.e especially a different method for recording changes.~~

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
[Name of change record] – in	[intranet folder	[job title]	Once created, the record cannot subsequently be	3 years

electronic form	name]		changed	

5. 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 changes not made in accordance with the document
- Number of changes where failure to comply caused incidents

[job title]
[name]

_____

[signature]