
# Data Security Policy

## Confidential Statement

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, by any means electronic, mechanical, photographic, optic recording or otherwise without prior consent, in writing, of the information owner.

## Document Control

| | |
|---|---|
| Document Name | Data Security Policy |
| Document Reference Number | IS 24 Data Security Policy |
| Issue Number | 01 |
| Revision | 00 |
| Document Prepared by | CISO |
| Document Reviewed by | IT |
| Document Approved by | Director |
| Document Classification | For Internal Use only |

**Table of Contents**

# Contents



## 1. Purpose

This Data Masking Policy is established to ensure the protection of sensitive information within our organization, in compliance with the ISO 27001:2022 standard. Data masking is a crucial component of our information security strategy to safeguard confidential data while allowing for legitimate use in non-production environments. This policy applies to all employees, contractors, and third-party entities with access to sensitive information within our organization.

## 2. Definition of Data Masking

Data masking is the process of concealing original data with fictitious or pseudonymous data to protect sensitive information while maintaining its usability for authorized purposes.

## 3. Objectives:

The primary objectives of this policy are:

- To protect sensitive data from unauthorized access in non-production environments.
- To enable legitimate use of data for testing, development, and analysis without exposing sensitive information.
- To comply with ISO 27001:2022 standards related to data protection.

## 4. Data Classification:

All data must be classified based on its sensitivity and criticality. The organization will use a standardized classification system to identify and categorize data.

- Public Data: Information that can be freely shared.
- Internal Data: Sensitive information meant for internal use only.
- Confidential Data: Highly sensitive information that requires the highest level of protection.

## 5. Data Masking Techniques:

The organization will employ industry-standard data masking techniques, such as:

- Substitution: Replacing sensitive data with fictitious data.
- Shuffling: Randomizing the order of data records.
- Tokenization: Replacing sensitive data with randomly generated tokens.
- Noise Addition: Introducing random noise to data to make it harder to discern.

## 6. Data Masking in Non-Production Environments:

Sensitive data must be masked in all non-production environments, including but not limited to:

- Development environments
- Testing environments
- Quality assurance environments


## 7. Access Controls

Access to masked data in non-production environments will be restricted to individuals with a legitimate business need. Access permissions will be reviewed regularly, and any unnecessary access will be revoked.

## 8. Monitoring and Auditing

Regular monitoring and auditing of data masking processes will be conducted to ensure compliance with this policy. Any deviations or incidents will be promptly investigated and addressed.

## 9. Training and Awareness:

All personnel with access to sensitive data will receive training on data masking procedures and their responsibilities in maintaining data security.

## 10. Review and Revision:

This policy will be reviewed at least annually and updated as necessary to address changes in technology, business processes, or regulatory requirements.

## 11. Enforcement:

Failure to comply with this Data Masking Policy may result in disciplinary action, up to and including termination of employment or legal action, as appropriate.

## 12. Document Control:

This policy is a controlled document, and any changes must be approved by the designated authority. The latest version will be made available to all relevant personnel.