# Data Handling Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. [List of applicable compliance frameworks and requirements]
2. NIST SP 1800-39:<https://csrc.nist.gov/pubs/sp/1800/39/iprd>
3. NIST 800-88: <https://csrc.nist.gov/pubs/sp/800/88/r1/final>
4. NIST 800-122: <https://csrc.nist.gov/pubs/sp/800/122/final>
5. ISO/IEC 29134: <https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-2:v1:en>
6. ISO/IEC 27701: <https://www.iso.org/standard/71670.html>
7. NIST IR 8496:<https://csrc.nist.gov/pubs/ir/8496/ipd>
8. ISO/IEC TS 38505-3:<https://www.iso.org/standard/56643.html>
9. GDPR Articles 5, 35
10. ISO/IEC 27001:2022: A.5.9, A.5.10, A.5.12, A.5.13, A.5.34, A.8.10, A.8.11, A.8.12
11. NIST 800-53 rev. 5: AC-4, AC-4(21), AC-20(1), AC-21, AC-22, CA-3, CM-5(5), CM-12, CM-12(1), IA-6, PS-3(3), RA-2, RA-3, SI-12
12. CIS v8: 3.1, 3.2, 3.7, 3.12, 3.13, 16.1
13. PCI DSS 4.0: 3.2.1, 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.3, 3.4.1, 3.4.2, 6.5.5, 6.5.6, 7.2.3, 9.4.2, 9.4.5, 9.4.5.1, 9.4.7, 10.1.1, 12.3.1
14. AICPA SOC 2 TSC: C1.1, C1.2, CC2.1, CC6.1, CC6.5, CC6.7, CC8.1, PI1.1, PI1.5, P3.1, P3.2, P4.1, P4.2, P6.1

## Document ownership

<(Choose from)>

* 1. Policy Owner:
     1. [Owner name] ([Owner email]), [Owner title]
  2. Information Security Officer:
     1. [Information officer name], ([Information officer email]), [Information officer title]
  3. System Owner(s):
     1. [System owner name], ([System owner email]), [System owner title]
  4. Process and Operational Owner(s)
     1. [process owner], ([process owner email]), [process owner title]
  5. System Administrator(s):
     1. [System admin name], ([System admin email]), [System admin title]
  6. Required Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT
  7. Optional Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT

## Purpose

The purpose of this Data Handling Policy is to establish a comprehensive framework for the management and protection of data within [Organization]. This policy aims to ensure the confidentiality, integrity, and availability of data by implementing best practices and compliance with relevant laws and regulations. It outlines the responsibilities and procedures for data classification, handling, privacy, minimization, masking, lifecycle management, usage limitation, loss prevention, retention, destruction, transfer monitoring, and the use of test data. By adhering to this policy, [Organization] seeks to protect sensitive information, mitigate risks, and maintain trust with stakeholders.

## Scope

This policy applies to all employees, contractors, and third-party service providers of [Organization] who handle or have access to organizational data. It covers all types of data, including but not limited to personal data, confidential information, intellectual property, and financial records. The policy encompasses all data handling activities, including collection, storage, processing, transmission, and destruction, across all departments and systems within the organization. This policy is mandatory and must be followed in conjunction with other relevant organizational policies, standards, and procedures.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner],  Operational owner title] |  |
| Information Systems Administrators | System Administrators | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users | End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
  2. Management has reviewed and approved this policy.
  3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
  4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
  2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Data Classification: The process of categorizing data based on its sensitivity and importance. Common classifications include Public, Internal, Confidential, and Restricted.
  2. Data Handling: The management and processing of data according to its classification level, ensuring proper labeling, access control, encryption, and training.
  3. Data Privacy Impact Assessment (DPIA): An assessment conducted to identify and mitigate privacy risks before processing personal data in any new project or process.
  4. Data Minimization: The principle of limiting the collection and processing of personal data to what is directly relevant and necessary for the specified purpose.
  5. Data Masking: Techniques used to protect sensitive data, such as credit card information and passwords, by obscuring the data from unauthorized access.
  6. Data Lifecycle Management: The management of data from creation to deletion, including defining retention schedules, ensuring secure disposal, and monitoring data access and changes.
  7. Data Usage Limitation: Ensuring that data is used strictly for the purposes for which it was collected, with controls in place to prevent unauthorized use or disclosure.
  8. Data Loss Prevention (DLP): A strategy to prevent unauthorized access, transfer, or destruction of data, typically involving the deployment of DLP tools and policies for detecting and responding to data breaches.
  9. Data Retention: The process of defining and enforcing schedules for how long data should be kept, based on legal, regulatory, and business requirements.
  10. Data Destruction: The secure and irreversible disposal of data that is no longer needed, using methods such as shredding, degaussing, or data wiping.
  11. Data Transfer Monitoring: The practice of monitoring and securing data transfers to detect and prevent unauthorized transfers, often involving encryption and logging mechanisms.
  12. Test Data: Data used in testing environments, which should be anonymized or masked to prevent exposure of sensitive information.
  13. Encryption: The process of converting data into a code to prevent unauthorized access, commonly used to protect data in transit and at rest.
  14. Access Control: Mechanisms to restrict access to data based on roles and responsibilities, ensuring only authorized personnel can access sensitive information.
  15. Tokenization: A data protection method that replaces sensitive data with a unique identifier or token that retains essential information without exposing the original data.
  16. Degaussing: A method of data destruction that uses a magnetic field to erase data stored on magnetic media.
  17. Data Wiping: The process of overwriting data on a storage device to ensure it cannot be recovered.
  18. Shredding: Physically destroying paper documents or electronic media to ensure data cannot be reconstructed.

## Policy

#### Data Classification

[Responsible Party] shall classify all data based on its sensitivity and importance, categorizing it as Public, Internal, Confidential, or Restricted.

* + 1. Implement a standardized classification scheme.
    2. Review and update data classifications regularly to reflect changes in sensitivity or importance.

#### Data Handling

[Responsible Party] is required to manage and process data according to its classification level.

* + 1. Ensure proper labeling of data.
    2. Restrict access to classified data based on roles and responsibilities.
    3. Encrypt data in transit and at rest where necessary.
    4. Train employees on the appropriate handling of different data types.

#### Data Privacy and Data Protection Impact Assessment

[Responsible Party] shall protect personal information (PII, PHI) in accordance with applicable laws and regulations

* + 1. Identify and mitigate privacy risks before processing personal data.
    2. Conduct and document a Data Protection Impact Assessment
    3. Update DPIAs periodically or when there is a significant change in data processing.
    4. Regularly review data collection processes to ensure they align with data minimization principles.
    5. Remove or anonymize data that is no longer needed.

#### Data Masking for Credit Cards and Passwords

[Responsible Party] is required to apply data masking techniques to sensitive data such as credit card information and passwords.

* + 1. Implement masking at the database level and during data transmission.
    2. Use tokenization or encryption to protect sensitive data in applications and storage.

#### Data Lifecycle Management

[Responsible Party] shall manage data through its entire lifecycle, from creation to deletion.

* + 1. Define and enforce data retention schedules based on legal, regulatory, and business requirements.
    2. Ensure data descriptions are accurate and up-to-date to facilitate proper retention management.
    3. Regularly audit data stores to ensure compliance with retention policies.
    4. Ensure secure disposal of data that is no longer required.
    5. Monitor and log data access and changes throughout its lifecycle.

#### Data Loss Prevention Strategy

[Responsible Party] is required to implement a Data Loss Prevention (DLP) strategy.

* + 1. Deploy DLP tools to monitor and protect data across endpoints, networks, and storage.
    2. Establish policies for detecting and responding to data breaches.
    3. Conduct regular audits and assessments of DLP effectiveness.
    4. Implement controls to prevent unauthorized use or disclosure of data.
    5. Regularly review data usage to ensure compliance with stated purposes.

#### 

#### Use of Test Data

[Responsible Party] shall ensure that test data is anonymized or masked to prevent exposure of sensitive information.

* + 1. Use synthetic or anonymized data for testing purposes.
    2. Implement strict access controls for environments where test data is used.
    3. Regularly review and sanitize test data to remove any sensitive information.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
  2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
  3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
     1. Policies
     2. Procedures
     3. Standards
     4. Documentation
     5. Regulations
     6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
  2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
     1. The Information Security Officer
     2. Officer of the [Organization name] Leadership Team
  3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |