# Privacy 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 and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. GDPR ICO Checklist: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>
2. HHS HIPAA Guidance: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>
3. NIST 800-122: <https://csrc.nist.gov/pubs/sp/800/122/final>
4. ISO/IEC 27701: <https://www.iso.org/standard/71670.html>
5. ISO/IEC 29134: <https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-2:v1:en>
6. ISO/IEC 27001:2022: 6.1.2, 6.1.2.a, A.5.10, A.5.14, A.5.18, A.5.34, A.8.26
7. NIST 800-53 rev. 5: AC-4, AC-4(21), AC-6(7), AC-20(1), AC-21, AC-22, CA-3, PL-2, PS-3(3), PS-6, PS-7, RA-3, SA-4, SA-9(5), SA-11, SA-15(3)
8. 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, 3.4.2, 7.2.4, 7.2.5.1, 12.3.1, 12.8.2, 12.9.1
9. CIS v8: 3.1, 6.8, 15.4
10. AICPA SOC 2 TSC: C1.1, CC2.1, CC5.2, CC6.2, CC6.3, CC6.7, CC9.2, P3.1, P3.2, P4.1, P4.2, P4.3, P5.1, P5.2, P6.1, P6.4, P6.5, P7.1, PI1.5

## 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 Privacy Policy is to establish clear guidelines and procedures for the collection, use, storage, and protection of personal information by the organization. The policy aims to ensure compliance with relevant data protection regulations and to uphold the highest standards of privacy and data security. It outlines the organization's commitment to safeguarding personal data, maintaining user trust, and providing transparency regarding data handling practices. By implementing this policy, the organization seeks to protect the rights and privacy of individuals and to foster a culture of accountability and responsibility in data management.

## Scope

This Privacy Policy applies to all employees, contractors, and third parties who process personal data on behalf of the organization. It covers all personal information collected, processed, stored, and shared by the organization, regardless of the medium or format. The policy is applicable to all business units, departments, and operations within the organization, including but not limited to:

* Websites, mobile applications, and online services operated by the organization
* Customer relationship management (CRM) systems and databases
* Marketing and communication activities
* Vendor and supplier engagements
* Product and service development initiatives

The scope of this policy extends to the implementation of data protection measures, user consent management, data subject rights, and privacy impact assessments. It encompasses all stages of the data lifecycle, from collection and processing to storage and deletion, ensuring comprehensive protection of personal data.

## 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. Cookie: A small piece of data stored on the user's device by a website to remember information about the user, such as login status or preferences.
  2. Consent: A clear affirmative action signifying the user's agreement to the processing of their personal data.
  3. Personal Identifiable Information: Any information relating to an identified or identifiable natural person.
  4. Withdrawal of Consent: The act of a user revoking their previously given consent for the processing of their personal data.
  5. Data Minimization: The principle of collecting only the personal data that is strictly necessary for the purposes for which it is processed.
  6. User Access Request: A request made by a user to obtain a copy of their personal information held by the organization.
  7. Correction Request: A request made by a user to update or correct their personal information held by the organization.
  8. Data Exchange Agreement: A contract between the organization and a third party outlining the terms and conditions for sharing personal data.
  9. Vendor and Supplier Agreement: A contract between the organization and its vendors or suppliers that includes privacy and data protection clauses.
  10. Data Protection Impact Assessment (DPIA): A process to identify and mitigate privacy risks in new projects or significant changes to existing systems.
  11. Third Party: An entity other than the organization that processes or stores personal data on behalf of the organization.
  12. Data Deletion: The process of removing personal data from the organization's systems and records.
  13. Anonymization: The process of removing or altering personal data so that individuals cannot be identified.
  14. Privacy Requirements: The standards and obligations related to the protection of personal data as defined by laws, regulations, and organizational policies.
  15. Data Protection: The measures taken to safeguard personal data from unauthorized access, disclosure, alteration, or destruction.
  16. Explicit Consent: A type of consent given by a clear affirmative action, indicating agreement to the processing of personal data for specific purposes.
  17. Data Usage: The manner in which collected personal data is processed, stored, and used by the organization.
  18. Technical and Organizational Measures: The security practices and controls implemented to protect personal data, including encryption, access controls, and staff training.
  19. Privacy Standards: The set of guidelines and best practices for ensuring the protection of personal data.
  20. User Preferences: The choices made by users regarding the collection and use of their personal data, such as cookie settings and consent options.
  21. Data Protection Clauses: Provisions included in contracts to ensure that all parties adhere to data protection requirements.
  22. Privacy Principles: The fundamental concepts and rules that guide the handling of personal data, such as transparency, accountability, and fairness.
  23. Audit: A systematic review of policies, procedures, and practices to ensure compliance with data protection and privacy requirements.

## Policy

#### Cookies

The [responsible party] shall:

* + 1. Implement a cookie consent banner on its website to inform users about the use of cookies and to obtain explicit consent before cookies are set.
    2. Provide clear and comprehensive information about the types of cookies used, their purposes, and the data they collect.
    3. Ensure that users can manage their cookie preferences, including the ability to accept or reject cookies, through a user-friendly interface.

#### Consent to Collect Personal Information

The [responsible party] shall:

* + 1. Obtain explicit, informed consent from users before collecting any personal information.
    2. Provide clear and concise information about the types of personal data collected, the purposes for which the data is collected, and how the data will be used.
    3. Ensure that consent is documented and stored securely for future reference and compliance purposes.

#### Withdraw Consent

The [responsible party] shall:

* + 1. Allow users to withdraw their consent at any time through an easy and accessible process.
    2. Provide clear instructions on how users can withdraw their consent and the consequences of such withdrawal.
    3. Ensure that the withdrawal of consent is promptly reflected in all relevant systems and processes.
    4. Implement procedures to promptly delete or anonymize personal data upon the withdrawal of user consent.
    5. Communicate the deletion process to users, including any exceptions where data may be retained for legal or regulatory reasons.
    6. Ensure that all third parties with whom the data has been shared are informed of the user's request for data deletion.

#### User Access

The [responsible party] shall:

* + 1. Provide users with the right to access their personal information upon request.
    2. Implement a secure and efficient process for verifying user identities and fulfilling access requests.
    3. Provide the requested information in a clear and understandable format within a reasonable timeframe.

#### Correct Personal Information

The [responsible party] shall:

* + 1. Allow users to correct or update their personal information to ensure accuracy and completeness.
    2. Implement a straightforward process for users to submit correction requests and verify their identities.
    3. Ensure that corrections are promptly reflected in all relevant systems
    4. Ensure that corrections are communicated to third parties with whom the data has been shared.

#### Data Minimization

The [responsible party] shall:

* + 1. Limit the collection of personal data to the minimum necessary for the specified purposes.
    2. Regularly review data collection practices to ensure compliance with the principle of data minimization.
    3. Avoid collecting sensitive personal information unless it is strictly necessary and justified.

#### Data Usage Limitation

The [responsible party] shall:

* + 1. Use personal data only for the purposes explicitly stated in the user consent agreement.
    2. Implement controls to prevent the use of personal data for unauthorized purposes.
    3. Regularly review and update consent agreements to reflect any changes in data usage practices.

#### Third-party Agreements

The [responsible party] shall:

* + 1. Include specific privacy and data protection requirements in all data exchange agreements with third parties.
    2. Ensure that third parties adhere to the organization's privacy standards and legal obligations.
    3. Require vendors and suppliers to implement appropriate technical and organizational measures to protect personal data.
    4. Conduct regular audits and assessments to verify third-party compliance with privacy requirements.

#### Data Protection Impact Assessment

The [responsible party] shall:

* + 1. Integrate privacy considerations into the design and development of all products and services.
    2. Conduct data protection impact assessments (DPIAs) for new projects and significant changes to existing systems.
    3. Ensure that development teams receive training on privacy principles and best practices.

## 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** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |