# Artificial Intelligence 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 obligations.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. ISO/IEC 42001:2023
2. NIST AI RMF
3. ISO/IEC 27001:2022: A.5.10
4. NIST 800-53 rev. 5: PL-4, PL-4(1)
5. CIS v8: 14.5, 14.8
6. AICPA SOC 2 TSC: C1.1

## 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 Artificial Intelligence (AI) Policy is to establish a comprehensive framework that governs the ethical, secure, and effective use of AI technologies within the organization. This policy aims to ensure the confidentiality, integrity, and availability of protected data, particularly when such data is used in conjunction with Generative AI tools and other AI technologies. The policy seeks to comply with relevant legal and regulatory requirements, uphold ethical standards, and enable the organization to leverage AI to achieve its business objectives.

## Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other individuals who interact with AI technologies on behalf of the organization. It encompasses:

* 1. All AI technologies used within the organization, including Generative AI, Machine Learning, Natural Language Processing, Computer Vision, and other AI systems.
	2. Both internally developed AI tools and those acquired from third-party vendors.
	3. All data processed, stored, or transmitted by AI systems, particularly protected data such as Personally Identifiable Information (PII), Protected Health Information (PHI), financial data, and other sensitive information.

## 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. Artificial Intelligence (AI):
		1. The simulation of human intelligence in machines that are programmed to think and learn. AI can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation.
	2. Machine Learning (ML):
		1. A subset of AI that involves the use of algorithms and statistical models to enable machines to improve their performance on a task through experience. ML systems learn from data and can make predictions or decisions without being explicitly programmed for each specific task.
	3. Generative AI:
		1. A type of AI that can create new content, such as text, images, music, or code, based on the data it has been trained on. Examples include language models like GPT-4, which can generate human-like text.
	4. Natural Language Processing (NLP):
		1. A field of AI that focuses on the interaction between computers and human language. NLP enables machines to understand, interpret, and generate human language in a way that is both meaningful and useful.
	5. Computer Vision:
		1. An area of AI that enables machines to interpret and make decisions based on visual data from the world, such as images and videos. Applications include facial recognition, object detection, and image classification.
	6. Protected Data:
		1. Information that is safeguarded by legal, regulatory, or contractual requirements. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), financial data, and other sensitive information.
	7. Personally Identifiable Information (PII):
		1. Any data that can be used to identify a specific individual, either directly or indirectly. Examples include names, addresses, social security numbers, and email addresses.
	8. Protected Health Information (PHI):
		1. Any information about health status, healthcare provision, or healthcare payment that can be linked to an individual. This is covered under laws such as HIPAA in the United States.
	9. Data Anonymization:
		1. The process of removing personally identifiable information from data sets, so that individuals cannot be readily identified. This helps protect privacy while still allowing for data analysis.
	10. Data Encryption:
		1. The process of converting data into a code to prevent unauthorized access. Encrypted data can only be read or decrypted by someone who has the correct decryption key.
	11. Bias in AI:
		1. The presence of systematic errors or prejudices in AI systems that can lead to unfair outcomes. Bias can occur due to biased training data, algorithmic design, or other factors, and it can affect decisions made by AI systems.
	12. Algorithm:
		1. A set of rules or instructions given to an AI system to help it learn from data and make decisions. Algorithms are the foundation of AI and ML, guiding how data is processed and analyzed.
	13. Model Training:
		1. The process of teaching an AI system to make predictions or decisions by feeding it large amounts of data and adjusting the algorithm to improve its performance over time.
	14. Overfitting:
		1. A modeling error in machine learning where an algorithm performs well on training data but fails to generalize to new, unseen data. This occurs when the model learns the details and noise in the training data to an extent that it negatively impacts its performance on new data.
	15. Data Privacy:
		1. The aspect of data protection that concerns the proper handling of data – focusing on compliance with data protection laws, regulations, and best practices to ensure that individuals' data is kept confidential and secure.
	16. Explainability in AI:
		1. The extent to which the internal mechanics of an AI system can be explained in human terms. Explainability is important for understanding how AI systems make decisions and for ensuring transparency and accountability.
	17. Ethical AI:
		1. The practice of designing and using AI in a manner that is fair, transparent, and respectful of users' rights and freedoms. Ethical AI involves considerations of bias, fairness, privacy, and overall impact on society.
	18. Data Governance:
		1. The overall management of the availability, usability, integrity, and security of data used in an organization. Effective data governance ensures that data is accurate, consistent, and used responsibly.

## Policy

The [responsible party] shall ensure the ethical and responsible use of AI, including Generative AI, by aligning its use with security and privacy commitments.

#### Data Privacy and Security

To protect data privacy and security, the [responsible party] shall:

* + 1. Implement Safeguards: Establish and maintain comprehensive safeguards for data collection, storage, processing, and sharing to protect sensitive information.
		2. Prohibit Inappropriate Data Input: Restrict employees from entering private or personal information into AI systems, especially third-party or public AI tools.
		3. Maintain Confidentiality: Ensure that company trade secrets, personal data, and sensitive information are protected and not inadvertently exposed through AI applications.
		4. Regular Risk Assessments: Conduct regular risk assessments and audits of AI systems to identify and mitigate potential security and privacy risks.

#### Ethical Use and Bias Prevention

The organization is committed to the ethical use of AI. It shall:

* + 1. Establish Ethical Standards: Outline principles for the ethical use of AI, including fairness, accountability, and transparency.
		2. Detect and Mitigate Bias: Implement measures to detect and mitigate biases in AI systems, ensuring they do not produce discriminatory outcomes.
		3. Promote Diversity and Inclusion: Ensure AI tools support the organization’s diversity goals and comply with anti-discrimination laws.

#### Compliance with Legal and Regulatory Requirements

The organization shall:

* + 1. Adhere to Relevant Laws and Regulations: Ensure compliance with relevant data protection laws such as GDPR, CCPA, and sector-specific regulations.
		2. Monitor Regulatory Updates: Stay informed about evolving AI regulations and adjust the policy as needed to remain compliant.

#### Accountability and Governance

To establish effective governance, the organization shall:

* + 1. Define Roles and Responsibilities: Clearly define the roles and responsibilities of various stakeholders, including IT, legal, data science, compliance, and HR teams.
		2. Form an AI Ethics Committee: Establish an AI ethics committee to oversee ethical considerations and guide AI governance frameworks.
		3. Implement Continuous Monitoring: Establish procedures for the ongoing monitoring and evaluation of AI systems to ensure they adhere to established standards and ethical guidelines.

#### Training and Awareness

The [responsible party] shall provide training and awareness programs to educate employees about AI use and compliance:

* + 1. Conduct Regular Training: Provide regular training sessions on AI best practices, ethical use, and data protection.
		2. Promote Awareness: Implement awareness initiatives to keep employees informed about the latest developments in AI governance and compliance requirements.

#### Transparency and Documentation

To ensure transparency and accountability, the [responsible party] shall:

* + 1. Maintain Comprehensive Documentation: Keep detailed documentation of AI models, data sources, and decision-making processes.
		2. Ensure Transparency: Ensure stakeholders understand how AI systems function and make decisions.

#### Consequences and Enforcement

The [responsible party] shall clearly outline the consequences of policy violations:

* + 1. Define Repercussions for Violations: Specify the repercussions for violating the AI policy, which may include disciplinary actions or legal consequences.
		2. Establish Reporting Channels: Set up channels for employees to report potential policy violations or ethical concerns related to AI use.

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