ENERJİSA RESPONSIBLE ARTIFICIAL INTELLIGENCE GOVERNANCE POLICY

Publication Date: 21.01.2025

Table of Content

1. INTRODUCTION

Through this Policy, Enerjisa commits to the development, deployment, use, and commercialization of artificial intelligence models and/or systems in alignment with fundamental ethical principles. To this end, Enerjisa adopts the Responsible Artificial Intelligence Governance Policy, a structured approach for the safe, reliable, and ethical development, evaluation, and dissemination of artificial intelligence models and/or systems. In fulfilling this commitment, Enerjisa particularly emphasizes the "Ethics by Design" approach in its development and commercialization actions. This approach integrates the principle of "compliance with universal legal principles and local laws" into its framework. By embedding ethical principles into the development and use processes from the very beginning, the Ethics by Design approach ensures that ethical considerations are addressed as early as possible. It also defines actionable tasks to be implemented using protective development methodologies (e.g., TDSP[1], CRISP-DM[2]). It is recognized, however, that the ethical risks and the corresponding actionable tasks for each Artificial Intelligence implementation will vary.

Enerjisa promotes the development and use of high-quality Artificial Intelligence models and/or systems through responsible, ethical, and holistic Artificial Intelligence governance. This governance ensures effective management of data, impact, risk, and compliance throughout the lifecycle of Artificial Intelligence models and/or systems.

2. PURPOSE

The purpose of the Enerjisa Responsible Artificial Intelligence Governance Policy ("Policy") is to ensure that development, deployment, commercialization and use of Artificial Intelligence models and/or systems are conducted in full compliance with Enerjisa's ethical principles, legal obligations and corporate values. This is achieved through continuous monitoring and improvements across the lifecycle of Artificial Intelligence models and/or systems, supported by technical, legal, and organizational processes as well as governance.

Additionally, the Policy aims to clearly define the roles and responsibilities associated with all aspects of Artificial Intelligence governance, leaving no room for ambiguity.

3. SCOPE

This Policy applies to:

- All employees of Enerjisa, including members of the Board of Directors,

---

[1] TDSP (Team Data Science Process) is a methodology designed for planning, implementing, and managing predictive analytics solutions and artificial intelligence applications.
[2] CRISP-DM (Cross-Industry Standard Process for Data Mining) is a defined reference model for conducting data mining projects.

- Suppliers that provide goods and services to Enerjisa, as well as consultants, stakeholders, lawyers, external auditors and other individuals and organizations acting on behalf of Enerjisa (business partners).

Thus, all Enerjisa employees, stakeholders, suppliers, shareholders, business partners and customers involved in the development, deployment or use of artificial intelligence models and/or systems are required to comply with these rules. The binding effect of the Policy is ensured through legal measures such as contracts, agreements and written commitments as the relevant situation requires.

The Policy applies to all current and future artificial intelligence models and/or systems, including predictive and generative artificial intelligence applications.

The Policy establishes responsible artificial intelligence governance as a core component of Enerjisa corporate culture. Enerjisa senior management leads the implementation of responsible artificial intelligence governance and ensures alignment with corporate values, Enerjisa Code of Business Ethics and Enerjisa Artificial Intelligence Manifesto.

The Policy has been formulated in accordance with the corporate governance principles approved by the company's Board of Directors and as well as Enerjisa code of business ethics publicly disclosed. It is based on national and international legal framework, guidelines, reports, and recommendations of relevant institutions and organizations at both national and international levels. The Policy is implemented alongside Enerjisa policies, procedures, rules on personal data protection, privacy and confidentiality, information security, human rights, ethics and sustainability.

The procedures and principles related to the concept of responsible artificial intelligence constitute integral parts of the Policy.

4. DEFINITIONS

Artificial Intelligence Manifesto: Document that outlines the core ethical principles adopted by Enerjisa in the field of artificial intelligence.

Artificial Intelligence Model and/or System: A model and/or machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

Enerjisa Artificial Intelligence Board: An authorized corporate body responsible for governing, overseeing, and ensuring the proper implementation of the Policy.

Common Model: A model is designed to be used across multiple tasks.

Deployer: A natural or legal person who makes artificial intelligence available to be used on a system by users and other programs. In line with the definition provided in the European Union Artificial Intelligence Act, it also refers to a natural or legal person, public authority, agency, or other entity using an artificial intelligence system under their authority, except when the artificial intelligence system is used in the context of a personal or non-professional activity.

Fundamental Ethical Principles: A set of core ethical principles that must be adhered to during development deployment, and use of artificial intelligence models and systems.

Fundamental Rights Impact Assessment: A systematic process that evaluates potential impacts of the development, deployment, and use of artificial intelligence models and/or systems on human rights, fundamental freedoms and democratic values throughout their lifecycle.

Generative Artificial Intelligence: A category of artificial intelligence capable of creating new content such as text, images, videos and music.

Human-in-the-Loop: The ability for human intervention within the decision-making cycle of an artificial intelligence model and/or system.

Human-on-the-Command: The ability to oversee overall operation of an artificial intelligence model and/or system (including its broader economic, social, legal and ethical impacts) and to decide when and how the system should be used. This includes, but is not limited to, the ability to refrain from using the artificial intelligence system in specific cases, set levels of human discretion during the system's operation or override decisions made by the artificial intelligence system.

Mainstream Business Unit: Each of the core business lines that carries out distribution, sales, customer solutions, e-mobility, fleet management or any other business activities as determined by Enerjisa articles of association.

Developer: A natural or legal person that develops Artificial Intelligence Models and/or Systems or that puts Artificial Intelligence Models and/or Systems into service under its own name or trademark, whether for payment or free of charge. In the context of the European Union Artificial Intelligence Act, the term 'Provider' is used to define this scope.

Responsible Artificial Intelligence Principles: A set of ethical, technical and operational principles outlined in the Policy to ensure that artificial intelligence models and/or systems are developed, deployed and used in alignment with fundamental ethical principles, legal requirements and societal and corporate values.

Responsible Artificial Intelligence Governance: Structured management of artificial intelligence models and/or systems, as defined by the Policy, to ensure their development, deployment and use complying with fundamental ethical principles, legal requirements and societal and corporate values in order to minimize/eliminate potential risks and create/maximize benefits.

Responsible Artificial Intelligence Procedures and Principles: Document that outlines the implementation procedures and principles for responsible artificial intelligence governance as defined in the Policy.

User: A natural or legal person that uses Artificial Intelligence Models and/or Systems or that are affected by outputs of those Artificial Intelligence Models and/or Systems.

5. ESTABLISHING AN ETHICAL FRAMEWORK FOR "ETHICS BY DESIGN" IN ARTIFICIAL INTELLIGENCE

Enerjisa aims to develop, deploy and use Artificial Intelligence Models and/or Systems that respect human rights with a human-centered approach, prioritize fundamental rights and freedoms, human dignity and autonomy, take into account all necessary measures to protect privacy and personal data, in a way which is transparent, traceable, explainable, robust, reliable, environmentally friendly, sustainable, responsible, accountable, fair, inclusive and that positively affects social transformation under human supervision and control.

5.1. Principle of Human Oversight

Enerjisa Artificial Intelligence Models and/or Systems are subject to appropriate human oversight and intervention. The rights and freedoms of individuals affected by Enerjisa Artificial Intelligence Models and/or Systems take precedence over any benefits derived from these systems.

In this regard:

- Human oversight is ensured through an appropriate governance mechanism with clearly defined roles and responsibilities. This may include mechanisms such as Human-in-the-Loop or Human-on-the-Command, among others.

- For each Artificial Intelligence Models and/or Systems, the form of human oversight is determined based on the context of its use, the state of the technology, risks of infringing on the rights and freedoms of affected individuals and legal liability of Enerjisa.

- Human oversight extends beyond reviewing system's decisions and includes examination of the procedures and tools used during the development process, the creation of logs accessible to humans for the internal processes of Artificial Intelligence Models and/or Systems and similar elements.

5.2. Principle of Privacy and Personal Data Protection

Throughout the entire lifecycle of the Artificial Intelligence Models and/or Systems, measures are implemented to ensure confidentiality and protect trade secrets, personal data and all critical data, in full compliance with Enerjisa Personal Data Protection Policy. Additionally, personal data of all individuals whose information is processed is safeguarded and processes are adopted to ensure transparency regarding such data in accordance with their right to information.

In this regard:

- The end-to-end confidentiality of the data used as input for Artificial Intelligence Models and/or Systems, the data generated and the data interacting with the model and/or system is ensured. For this purpose, critical data groups, such as trade secrets and sensitive personal data are classified based on their importance as well as corresponding levels of confidentiality and protection are set.

- The accuracy and integrity of the data used in Artificial Intelligence Models and/or Systems are ensured. However, if the data used is provided by the user, the user is responsible for the accuracy, timeliness and integrity of the data, as well as for any outcomes resulting from its use. Accountability for these outcomes lies with the relevant

business unit owning the data. Provisions related to this are governed by the relevant measures to be documented (e.g., user agreements, customer contracts, employment agreements) between Enerjisa and the user.

- In cases where personal data and/or customer data which are specifically regulated due to sector-specific requirements, are shared with the Artificial Intelligence Models and/or Systems, such data is processed in compliance with electricity market regulations, personal data protection laws and confidentiality rules.

5.3. Principle of Robustness and Reliability

Artificial Intelligence Models and/or Systems undergo necessary security reviews either periodically or as needed on ad-hoc basis by Cyber Security Department and/or Group Compliance&Legal Directorate depending on the context of the review. Mechanisms and security tests are implemented to prevent malicious use of data or uncontrolled data extraction outside the company.

In this regard:

- A risk analysis and action plan are prepared to prevent security breaches or to mitigate and eliminate their impact if they occur.

- Security measures are established to enable back-up recovery plans in the event of a security breach.

- To ensure reliability and high accuracy of the Models and/or System, tests are conducted to verify that identical inputs consistently produce the same outcomes and that new inputs yield outputs consistent with previous results. This ensures that the Artificial Intelligence Models and/or Systems deliver intelligent, repeatable, and consistent results. Additionally, if conditions evolve over time, retrospective updates may be applied to generate new results, improving historical data, memory and future outcomes.

- Considering that Enerjisa operates in a regulated sector, all necessary administrative and technical measures are taken to protect personal data and data categorized as critical.

5.4. Principle of Transparency and Explainability

Artificial Intelligence Models and/or Systems including algorithms, all utilized data, how the data is collected, how decisions are reached, data sets and processes that influence the decisions of Artificial Intelligence Models and/or Systems are all managed transparently in accordance with the state-of-the-art standards. For any Artificial Intelligence Models and/or Systems, inputs, parameters, and interpretation of outputs are clearly and explicitly defined. Additionally, individuals interacting with the Models and/or Systems are informed about the use of artificial intelligence at the start or, at the latest, during the initial interaction.

In this regard:

- Traceability,

- Explainability, and

- Communication of Information

are implemented to ensure transparency.

5.5. Principle of Fairness, Impartiality, and Inclusivity

Enerjisa encourages the development, deployment, and use of Artificial Intelligence Models and/or Systems that supports sustainability goals such as energy efficiency optimization, AI-driven insights for climate resilience, predictive analytics for circular economy initiatives through environmentally friendly practices, ensuring their contribution to social welfare and the public good within the defined governance structure. Social and governance aspects such as fairness, inclusivity, transparency and human rights are referred under previous sections.

In this regard:

- From the design phase through to implementation and monitoring, Artificial Intelligence Models and/or Systems are developed using resources and processes that promote diversity and inclusivity, ensuring the representation of all groups to eliminate bias at every stage.

- Artificial Intelligence Models and/or Systems must not be designed to serve solely the interests of a specific group or produce results favoring one group in violation of Fundamental Ethical Principles. Developments are made to guarantee equal access and active participation for all employees and stakeholders including consideration of job impacts and upskilling needs of Enerjisa workforce. This does not preclude the development of Artificial Intelligence Models and/or Systems tailored to the specific needs of particular groups/business units required by the nature of the work, provided that such development is reasonably justified and adheres to the Fundamental Ethical Principles.

- Artificial Intelligence Models and/or Systems are shaped and refined with suggestions and feedback from all stakeholders who are directly or indirectly affected throughout their lifecycle.

5.6. Principle of Responsibility and Accountability

Roles and responsibilities related to Artificial Intelligence Models and/or Systems as well as the Policy itself are clearly defined and documented. All processes associated with Artificial Intelligence Models and/or Systems are recorded to ensure accountability and traceability.

In this regard:

- All processes related to artificial intelligence governance can only be executed by authorized personnel, and log records of all actions are maintained.

- The Enerjisa Artificial Intelligence Manifesto and this Enerjisa Responsible Artificial Intelligence Governance Policy are published, and the processes outlined in all associated documents are continuously improved and kept up to date.

5.7. Principle of Sustainability

Enerjisa encourages the development, deployment, and use of Artificial Intelligence Models and/or Systems that supports sustainability goals such as energy efficiency optimization, AI-driven insights for climate resilience, predictive analytics for circular economy initiatives

through environmentally friendly practices, ensuring contribution to social welfare and the public good within the defined governance structure.

In this regard:

- The impact of Artificial Intelligence Models and/or Systems on sustainability projects are acknowledged, and Artificial Intelligence Models and/or Systems are designed to positively influence and support stakeholders' social skills. Efforts are made to avoid adverse social, economic, and environmental impacts.

- Measures are taken to ensure that the entire lifecycle of Artificial Intelligence Models and/or Systems are in alignment with Enerjisa Climate Strategy and decarbonization targets, preserves energy and natural resources, promoting environmentally friendly practices.

6. STEPS FOR IMPLEMENTING THE ETHICAL FRAMEWORK

6.1. Evaluation

Within the scope of the Ethics by Design approach, the objectives of the Artificial Intelligence Models and/or Systems are assessed by Enerjisa Artificial Intelligence Board against the Fundamental Ethical Principles (outlined in Section 5, "Ethical Framework"). If any violation of these principles is identified, the Artificial Intelligence Models and/or Systems are deemed unethical. Following this, improvements made by the business owner, the overarching objectives of the application are to be reevaluated. Only the Models and/or Systems complying with the Fundamental Ethical Principles, proceed to the next step which is "Modeling".

6.2. Modeling

The Fundamental Ethical Principles are translated into specific features tailored to the respective Artificial Intelligence Model and/or System. These features guide the identification of ethical design requirements, considering the development methodology, organizational structure, business units' use cases, and the nature of the specific Artificial Intelligence Models and/or Systems.

6.3. Mapping

Within the scope of the Ethics by Design approach, implementing ethical design requirements for Artificial Intelligence Models and/or Systems developed or deployed by Enerjisa or third parties requires a structured mapping process. This mapping aligns ethical requirements with specific procedures and actions, encompassing various methods such as system functionality, data structures, and organizational measures.

In certain cases, ethical requirements may necessitate additional functionalities; in others, they may impose restrictions on certain functionalities. For instance, to avoid algorithmic bias, a formal bias assessment of the data is conducted before the Artificial Intelligence Models and/or Systems are deployed.

6.4. Implementation

Each ethical requirement must be addressed explicitly within its respective methodology and context. During the development or deployment process, Ethical Design requirements are applied in accordance with the "Mapping" step. The Ethics by Design approach provides a comprehensive development model where Fundamental Ethical Principles are transformed into artificial intelligence-specific requirements. Accordingly, existing Common Models and Artificial Intelligence Models and/or Systems developed by third parties must be reviewed to ensure alignment with the Ethics by Design methodology.

7. ROLES AND RESPONSIBILITIES

Enerjisa acts consciously of liability, within the scope and to the extent mandated by local laws, for any harm caused to its employees or third parties due to actions or operations of the Artificial Intelligence Models and/or Systems, it uses or makes available that violate Fundamental Ethical Principles.

In cases where legal responsibility arises from a contractual relationship, the "Principle of Utmost Care in Design" is applied during the contract drafting phase. Provisions are included to preclude or minimize Enerjisa's liability to the greatest extent possible and to establish appropriate recourse clauses. These measures are implemented from the outset, adhering to the ethical framework and risk assessments outlined in the preceding sections.

For non-contractual liabilities, such as strict liability or torts, Enerjisa not only applies utmost care in the design, implementation, and supervision of the Artificial Intelligence Models and/or Systems but also evaluates the impact, scope, and affected parties of the violation. All necessary measures are promptly taken to address and remedy the harm to the fullest possible extent as quickly as possible.

The responsibilities of Enerjisa based on its different roles in the Artificial Intelligence Models and/or Systems are as follows:

(i)   Developers of Enerjisa Artificial Intelligence Models and/or Systems:

- Design Artificial Intelligence Models and/or Systems that adhere to the Responsible Artificial Intelligence Principles and the Fundamental Ethical Principles.

- Implement data management practices that prioritize Responsible Artificial Intelligence Principles.

- Ensure that data pipelines are designed to reduce bias and protect against undesirable outcomes.

- Implements data management practices that prioritize the Responsible Artificial Intelligence Principles and the Fundamental Ethical Principles from the design phase onward.

- Verify that data pipelines are designed to minimize bias and safeguard against undesirable outcomes.

- Conduct feature engineering to enhance model performance while avoiding risk-related concerns.

- Develop Artificial Intelligence algorithms, models and/or systems that align with the Responsible Artificial Intelligence Principles.

- Create models and/or systems to monitor models for deviations and biases post-deployment.

- Test the Artificial Intelligence Models and/or Systems to ensure compliance with regulatory requirements.

- Identify and report potential biases, errors, and undesirable outcomes in the Artificial Intelligence Models and/or Systems.

- Validates Artificial Intelligence models against performance criteria and ensures the fairness and transparency of Artificial Intelligence Models and/or Systems through detailed testing to guarantee their reliability.

(ii)   Deployer of Enerjisa Artificial Intelligence Models and/or Systems:

- Implement automated deployment pipelines that integrate Responsible Artificial Intelligence practices.

- Ensure that Artificial Intelligence models are deployed securely, with appropriate protective measures and feedback loops in place.

- Apply security measures to protect Artificial Intelligence Models and/or Systems from malicious attacks and unauthorized access, ensuring that Artificial Intelligence deployments adhere to security standards and best available practices.

(iii)   Users of Enerjisa Artificial Intelligence Models and/or Systems:

- Comply with legal requirements and Enerjisa policies, procedures, rules, and guidelines related to the responsible use of artificial intelligence.

- Avoid using confidential data (e.g., personal data or trade secrets) when interacting with Artificial Intelligence Models and/or Systems.

- Report observed inconsistencies in Artificial Intelligence Models and/or Systems (e.g., bias, discrimination, hallucinations) through designated channels.

- Participate in training programs that promote responsible artificial intelligence practices and enhance understanding of Responsible Artificial Intelligence usage.

(iv)   <u>Business Units or Internal Customers</u> Requesting the Development or Procurement of Artificial Intelligence Models or Systems:

- Ensure that artificial intelligence use cases are aligned with the [Responsible Artificial Intelligence Principles](#), the [Fundamental Ethical Principles](#), and corporate values from the design phase onward.

- Prioritize artificial intelligence use cases that comply with the [Responsible Artificial Intelligence Principles](#) and the [Fundamental Ethical Principles](#).

- Define methods to measure the impact of developed or procured Artificial Intelligence initiatives on business outcomes.

- Record Artificial Intelligence use cases from the design phase to enable risk assessments and share this information with relevant stakeholders for evaluation.

- Ensure the creation and maintenance of documentation for all aspects related to use cases, including model and data information.

(v)   <u>Employees, Stakeholders, or Third Parties</u> Developing, Deploying, Commercializing, or Using Enerjisa Artificial Intelligence Models and/or Systems:

- Are responsible for any harm caused to Enerjisa or a third party, whether intentionally or negligently, through actions or behaviors that violate laws, the [Responsible Artificial Intelligence Principles](#), or the [Fundamental Ethical Principles](#).

- Are accountable for any actions that harm an individual's honor and dignity.

- Are held liable for administrative fines and all material and moral damages imposed on Enerjisa due to violations of personal data protection, data privacy, transparency, or security laws.

- Are held accountable for any violations of Capital Markets Law, Competition Law, Intellectual and Industrial Property Law, or Consumer Rights Law.

- Are accountable for violations of product safety regulations.

- Must ensure compliance with electricity market regulations and the boundaries established by relevant institutions and organizations for regulated sectors throughout the end-to-end process of designing and using Artificial Intelligence Models and/or Systems.

(vi)   Enerjisa Artificial Intelligence Board:

- Oversees the high-level management of Enerjisa Artificial Intelligence Models and/or Systems.

- Leads digital transformation primarily covering Artificial Intelligence Models and/or Systems.

- Is responsible for ensuring the proper implementation of the Policy.

- Promotes the adoption of Responsible Artificial Intelligence Principles within the company and fosters awareness, culture, and necessary competencies related to Artificial Intelligence.

- Identifies, prioritizes, and evaluates the development, deployment, use, and commercialization of Enerjisa Artificial Intelligence Models and/or Systems from technical and legal perspectives; formulates short, medium, and long-term roadmaps accordingly.

- Proactively identifies and assesses risks and opportunities in Artificial Intelligence projects, determines measures to prevent risks or mitigate their impacts, and ensures the implementation of these measures.

- Makes decisions on the implementation of Artificial Intelligence Models and/or Systems based on cost-benefit analyses.

- Evaluates the objectives of Artificial Intelligence Models and/or Systems for compliance with the **Fundamental Ethical Principles**.

- Encourages innovative projects, research, and development activities in the field of Artificial Intelligence.

- Resolves disputes or differences in interpretation regarding responsibility for Enerjisa Artificial Intelligence Models and/or Systems.

- Ensures that non-compliances with Enerjisa Responsible Artificial Intelligence Principles are reported to the Artificial Intelligence Board and takes necessary actions to address these non-compliances.

- Is responsible for the creation and consolidation of an Artificial Intelligence inventory.

- May for establish subcommittees specific purposes.

8. GOVERNANCE

8.1. General

Governance processes are established to ensure that Enerjisa Artificial Intelligence Models and/or Systems comply with the Policy.

Each use case is carefully analyzed using different evaluation methods, with responsibilities defined under the Policy. After categorizing the use cases, control checkpoints are defined, and, if necessary, additional research is conducted before the Artificial Intelligence Model and/or System is deployed or released to the market. Efforts are made to ensure that the application has been developed as intended before it is made accessible to a broader user base.

Every Artificial Intelligence Model and/or System developed, deployed, used, or commercialized by Enerjisa is subject to an ethical evaluation in line with the [Fundamental Ethical Principles](#). Based on the evaluation results, different action plans are applied:

- Minimal or low-risk use cases: These include all Artificial Intelligence Models and/or Systems that are not prohibited and not classified as high-risk. The development, deployment, commercialization, and use of the Artificial Intelligence Model and/or System is subject to permission by the Enerjisa Artificial Intelligence Board during the design phase.

- High-risk use cases: These include Artificial Intelligence Models and/or Systems that pose a significant risk to health, safety or fundamental rights. If an Artificial Intelligence Model and/or System is classified as high-risk, the Enerjisa Artificial Intelligence Board assesses the risk and makes a definitive decision on whether the risk will be accepted during the design phase.

- Prohibited use cases: These include Artificial Intelligence Models and/or Systems that violate fundamental rights. If an Artificial Intelligence Model and/or System is classified as prohibited, its development, deployment, commercialization, and use are not permitted by the Enerjisa Artificial Intelligence Board during the design phase.

The security, stability, and compliance of Artificial Intelligence Models and/or Systems with laws, [Responsible Artificial Intelligence Principles](#), and [Fundamental Ethical Principles](#) are periodically assessed by the Digital Business Management and Business Intelligence Group Department and the Group Compliance and Legal Directorate depending on the scope of assessment. The frequency of these reviews is determined based on the risk categorization.

8.2. Impact Management

The development of an Artificial Intelligence Model and/or System begins with an impact assessment as required by [the Responsible Artificial Intelligence Procedures and Principles.](#) This assessment is done by the **Enerjisa Artificial Intelligence Board** that identifies potential risks, the associated harms, and the measures required to prevent or mitigate these risks.

In critical situations that may jeopardize individuals' fundamental rights, such as performance deterioration due to changing input data characteristics, discrimination arising from underrepresentation, or unlawful processing of sensitive personal data, the [Fundamental Rights Impact Assessment](#) is conducted.

The Treasury, Risk, Investor Relations and Tax Directorate and the Group Compliance and Legal Directorate are jointly responsible for overseeing all processes under this section.

8.3. Risk Management

A Risk Management System (RMS) for Artificial Intelligence Models and/or Systems is implemented, documented, and monitored through the existing system. The Artificial Intelligence risk assessments identify risk sources, determine their likelihood of occurrence, and measure their impacts.

Throughout the development lifecycle and prior to deployment, Artificial Intelligence risks are mapped, measured, and managed. Risk mapping serves as a critical first step in assessing and

managing risks associated with Artificial Intelligence, and is repeated throughout the Artificial Intelligence development cycle.

Risk-based priorities are set, and a risk hierarchy framework is established. Efforts are made to deepen understanding of how identified risks arise and to uncover previously unknown risks through targeted analyses of Artificial Intelligence Models and/or Systems.

Cybersecurity and data privacy risks related to Artificial Intelligence, as well as compliance risks with transparency principles inherent to Artificial Intelligence Models and/or Systems, are given priority. Relevant company documents are updated in alignment with advancements in Artificial Intelligence.

The Treasury, Risk, Investor Relations, and Tax Directorate is responsible for overseeing all risk management processes outlined above.

Automated audits are conducted using new software tools tailored for auditing Artificial Intelligence Models and/or Systems. The Treasury, Risk, Investor Relations, and Tax Directorate, in collaboration with the Digital Business Management and Business Intelligence Group Department, is jointly responsible for identifying and implementing artificial intelligence-specific automated auditing tools during the development lifecycle and prior to the deployment of Artificial Intelligence Models and/or Systems.

8.4. Lifecycle Management

Artificial Intelligence Models and/or Systems must remain robust and accurate throughout their lifecycle. Structured process flows are established to manage Artificial Intelligence Models and/or Systems from the design phase to operational deployment.

Proven architectures are implemented for Artificial Intelligence Models and/or Systems. Specific principles, components, roles, and processes are aligned with legal requirements and fully documented. Metadata, input and output data, performance analyses, and traceability data are stored and monitored to ensure transparency and accountability.

Environmental impacts, energy usage and greenhouse gas (GHG) emissions are being assessed, mitigation actions are defined, implemented and monitored.

The Digital Business Management and Business Intelligence Group Directorate, as the relevant Mainstream Business Unit, is responsible for managing the processes under this section.

8.5. Technical Compliance and Conformity Management

Compliance evaluations for Artificial Intelligence Models and/or Systems are conducted based on comprehensive documentation ("technical documentation"). Artificial Intelligence Models and/or Systems deemed compliant are labeled accordingly. If a system is found to be non-compliant or operational issues arise, the Enerjisa Artificial Intelligence Board is notified, and efforts are undertaken to restore compliance.

The Digital Business Management and Business Intelligence Group Department, as the relevant Mainstream Business Unit, is responsible for managing the processes under this section.

9. FINANCIAL EVALUATION

For each Artificial Intelligence Models and/or Systems developed, deployed, or commercialized by Enerjisa, a value and cost-benefit analysis is conducted, from the outset on,during the design phase by the business owner to assess its feasibility, efficiency, and alignment with corporate goals. This analysis ensures that Artificial Intelligence Models and/or Systems provide measurable value while adhering to the Responsible Artificial Intelligence Principles and the [Fundamental Ethical Principles](#). In this regard:

- The analysis considers both tangible and intangible benefits, including financial performance, operational efficiency, and contributions to social welfare and sustainability.
- The analysis may apply different methodologies depending on the specific requirements of the Artificial Intelligence Models and/or Systems. For example, the Feigenbaum PAF Model (which includes four steps: i) Prevention, ii) Appraisal, iii) Internal Failure, iv) External Failure) may be used as a reference.
- Costs includes development, implementation, maintenance, and potential risks associated with non-compliance or ethical concerns as well as contingency funds for unforeseen expenses.
- For high-risk Artificial Intelligence Models and/or Systems, the value and cost-benefit analysis also includes the potential improvement and risk mitigation costs required to address the risks identified during the ethical evaluation and impact assessment.
- Relevant Business Unit and the Business Units Finance Directorate are responsible for ensuring that cost-benefit analyses are completed and documented for all Artificial Intelligence Models and/or Systems.
- The findings of the cost-benefit analysis are presented to Enerjisa Artificial Intelligence Board by relevant Business Unit, the Business Units Finance Directorate including the Digital Business Management and Business Intelligence Group Directorate, and incorporated into the decision-making process for the Artificial Intelligence Models and/or Systems.
- Based on the analysis presented, Enerjisa Artificial Intelligence Board either approves the model or system for implementation or provides recommendations for revision to address any identified gaps.
- Following the submission of revision recommendations, the relevant Business Unit, the Business Units Finance Directorate, and the Digital Business Management and Business Intelligence Group Directorate take the necessary actions to address the identified deficiencies and resubmit the revised analysis to the Enerjisa Artificial Intelligence Board. The Board evaluates the updates and makes a final decision, either approving or rejecting the proposal.
- Regular financial monitoring checkpoints is established during the project lifecycle to compare actual expenditures and performance against projections.
- Models or systems approved by the Enerjisa Artificial Intelligence Board are initially implemented as pilots. The duration of the pilot phase is determined by the Enerjisa Artificial Intelligence Board based on the specific use case. Following the completion of the pilot phase, a post-implementation value and cost-benefit analysis is conducted by the relevant Business Unit and the Business Units Finance Directorate to compare actual outcomes against initial projections. A detailed evaluation report is prepared, outlining successes, discrepancies, and lessons learned, which is then presented to Enerjisa Artificial Intelligence Board for further review and decision-making.

10. AWARENESS AND ARTIFICIAL INTELLIGENCE COMPENTENCIES&LITERACY

Efforts are undertaken to promote awareness, understanding, and literacy in artificial intelligence to ensure informed and responsible decision-making regarding the development, deployment, and use of Artificial Intelligence Models and/or Systems, as well as to mitigate potential adverse effects.

Competency development is encouraged to ensure that individuals involved in developing, deploying, and using Artificial Intelligence Models and/or Systems possess adequate levels of artificial intelligence literacy. These competencies are regulated and structured through the Artificial Intelligence Reference Guide to ensure alignment with responsible artificial intelligence practices.

Digital Business Management and Business Intelligence Group Department and Group Compliance&Legal Directorate are jointly responsible for promoting awareness, developing literacy and competency.

11. MONITORING

Enerjisa reserves the right to monitor and access the use of Artificial Intelligence Models and/or Systems on devices it provides or networks it manages. Monitoring is conducted to ensure compliance with the Policy and to detect and address any unauthorized or non-compliant use of Artificial Intelligence Models and/or Systems. All monitoring activities are carried out in adherence to applicable laws and information security regulations. All employees and other internal stakeholders set out in the Policy are obliged to consent to such monitoring and access by Enerjisa as long as such intervention is proportionate and in compliance with the purpose.

The risk management practices of stakeholders and third parties are continuously monitored, and risks arising from their Artificial Intelligence Models and/or Systems are consistently evaluated by Digital Business Management and Business Intelligence Group Department and Group Compliance&Legal Directorate. This ensures ongoing oversight and mitigation of potential risks associated with third-party and stakeholder artificial intelligence usage.

12. FAILURE TO COMPLY

Users who fail to comply with any provisions of Enerjisa's Responsible Artificial Intelligence Governance Policy may face disciplinary action, including termination of employment. For suppliers, business partners, and customers, such violations may constitute a breach of contract and could result in termination of the agreement. Group Compliance&Legal, in collaboration with the Compliance Directorates of the Main Business Units, ensures that contracts are structured to include proportionate sanctions for any violations. In cases where artificial intelligence related activities violate applicable laws, such violations may be reported to law enforcement authorities if deemed necessary.

If monitoring activities identify a potential policy violation or if a possible breach is reported, the Cyber Incident Response Team will address the violation. Appropriate measures will be taken by the said team to investigate and mitigate the issue, ensuring alignment with company policies and applicable laws.

13. COMMUNICATION

Any end-user or affected individual, whether within or outside Enerjisa, may anonymously raise concerns with the Group Compliance&Legal Directorate regarding the compliance of an Artificial Intelligence Model and/or System with the Policy.

All notifications related to Artificial Intelligence Models and/or Systems are thoroughly reviewed by the Group Compliance&Legal Directorate. If deemed necessary, cases of non-compliance are reported to the Enerjisa Artificial Intelligence Board to ensure that the relevant processes for addressing the issue are initiated. These review and remediation processes are managed transparently, and the individuals who raised the concerns are informed of the outcomes.

Based on the outcomes, controls are strengthened, and improvement activities are implemented to prevent recurrence of similar incidents.

14. ENFORCEMENT

The Policy becomes effective for all Enerjisa companies as of the date it is approved through QDMS by the CEO and CFO, and it is binding on all entities.