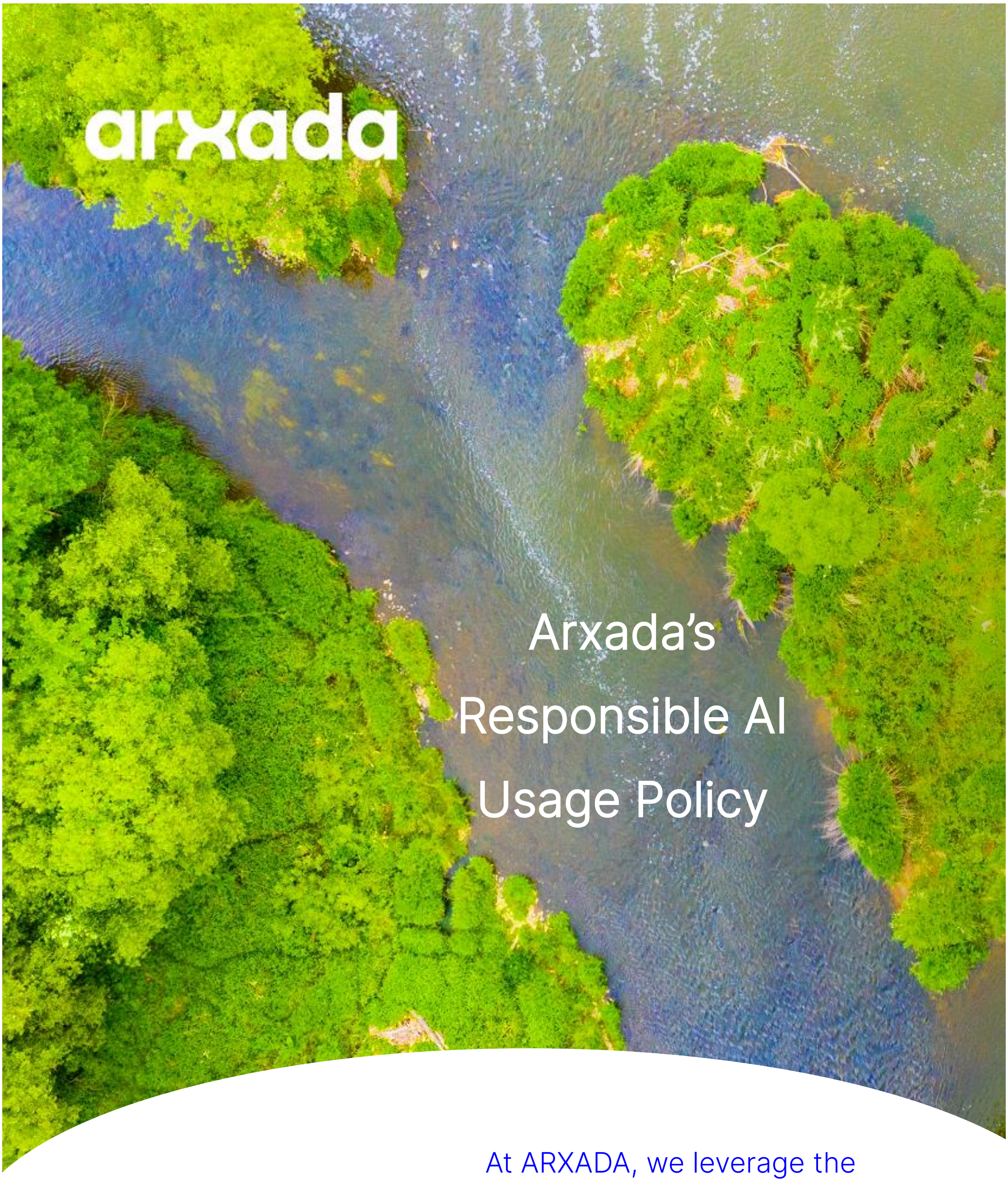

Arxada's Responsible AI Usage Policy

At ARXADA, we leverage the transformative power of Artificial Intelligence (AI) tools to enhance efficiency, decision-making, and innovation.

arxada.com

Introduction

Artificial Intelligence (AI) tools are transforming the way we work by automating tasks, enhancing decision-making, and providing valuable insights into our operations. However, the use of AI tools also presents new challenges related to information security, privacy and data protection.

This Responsible AI Usage Policy (the "Policy") outlines the principles and best practices for the appropriate use of AI tools within ARXADA and emphasizes responsible and secure practices, especially when it involves the handling of potentially sensitive company, employee, and customer information. This Policy must be observed in addition to other applicable policies, guidelines and instructions,

Purpose

The purpose of this policy is to establish guidelines for the appropriate use of Artificial Intelligence (AI) tools at ARXADA. It aims to ensure that all associates utilize AI in a secure, ethical, and confidential manner, in alignment with the company's values and compliance obligations.

This Policy also defines the requirements associates must follow when engaging with AI tools, including:

- Assessing and mitigating security and privacy risks.
- Assessing and mitigating the legal risks of infringement of third-party intellectual property rights and other risks.
- Ensuring the protection of information or data that is the property of Arxada, such as information pertaining to business operations and strategies, pricing and marketing information, technology, trade secrets, customer names and contact details, information pertaining to customers, and any other information that Arxada maintains as confidential ("Confidential Data").
- Adhering to legal and regulatory requirements concerning data usage.

Our Responsible AI Pillars

Empowering People & Accountability

AI tools are designed to support, not replace, human judgment. Associates remain accountable for all decisions and actions taken with the assistance of AI.

All associates must ensure that their use of AI aligns with ARXADA's values and complies with all applicable laws and regulations.

Fairness & Ethical Use

Promote fairness: use AI tools in ways that uphold fairness, prevent bias, and support non-discrimination and respect for human rights. Do not use AI to create, alter, or distribute content that could harm individuals or groups, or that misrepresent facts.

Privacy, Security & Confidentiality

Only use AI tools that have been vetted by ARXADA´s IT and Legal Teams.

Transparency

Be clear when AI is used to generate content or make recommendations.

All participants in meetings where AI notetaking/recording tools will be used must be informed that such tools will be used before they are deployed and must consent to being recorded by the AI notetaking and recording tool. AI vetted notetaking and recording tools may be used in any meeting, or any portion of a meeting, unless personal data will be discussed.

Communicate the limitations of AI outputs and provide opportunities for feedback or correction.

Robustness & Safety

Regularly review AI outputs for accuracy, relevance, and unintended consequences, such as bias and discriminatory or offensive content, and edit outputs as required before using the content.

Report any unexpected or unsafe AI system behaviour immediately.

Usage Scope

This Policy applies to all associates, contractors, and third parties who use AI tools within ARXADA's networks and platforms. It covers the use of AI tools involving potentially sensitive company and customer information.

This Policy also applies to anyone using third-party AI tools for work purposes, whether outside ARXADA systems, or integrated into them (e.g., as a widget, plugin or download).

Security Best Practices

The usage of AI tools should be limited to business-related purposes only, subject to the limitations herein. All associates are expected to adhere to the following security best practices when using AI tools:

Data privacy and Confidentiality

Always protect Confidential Data, intellectual property, and confidentiality; only use approved AI Tools. In particular, never input or share confidential company or customer data with not-approved AI Tools. Maintain strong access controls; do not share credentials or grant AI systems unauthorized access.

If unsure about sharing information with an AI tool, ask your manager or the Legal Department first.

Process Recording

Keep records of important AI interactions (such as input prompts and generated outputs) for review and tracing when needed.

Unacceptable Use

Associates **must not engage** in the following activities when using AI tools:

- Unauthorised sharing of Confidential Data, including entering company-protected information (e.g. personal information, trade secrets, or other business information) into unapproved AI tools.
- Using AI tools before they have been evaluated and approved by ARXADA.
- Sharing login credentials or sensitive information with third parties.
- Altering company or other copyrighted material or otherwise violating intellectual property laws.
- Using AI tools to alter an employee or third party's image, speech, or work product without permission.
- Using AI for unlawful, unethical, or discriminatory purposes or to create misleading, biased, or inappropriate content, or for any other unlawful purpose.
- Using any AI system classified as high-risk for the organization.
- Using AI technology to generate or synthesize text, images, audio, video, virtual scenes, and other information for external release, but not actively declaring or labelling it as "AI generated" or "Aided by AI". Use means to delete, tamper with, conceal, or forge the labelling of the AI-generated content.
- Using AI to replace human oversight or to be a substantial factor in critical decision-making processes, including, but not limited to, with respect to making critical employment decisions about applicants or employees, such as decisions about recruitment, hiring, promotions, transfers, and terminations.
- Other illegal uses of AI technology prohibited by local laws and regulations.

Enforcement & Non-Compliance

Any associates found to have violated this policy may be subject to disciplinary action, up to and including termination.

Monitoring

ARXADA reserves the right to monitor all interactions with AI tools to ensure compliance with this Policy.

Incident Reporting

All associates are required to report any security incidents or AI-tool-related issues to their manager or the IT Department immediately, including and up to suspected data breaches.

Compliance Statement

At ARXADA, we are committed to safeguarding company and customer data when using AI tools. We uphold the data management practices outlined by the National Institute of Science and Technology (NIST), the

General Data Protection Regulation (GDPR), Personal Information Protection Law of the People's Republic of China (PIPL) and any other applicable regulations governing our industry.

Follow all standard company security practices, such as using strong passwords, keeping software updated, and following data retention and disposal procedures. Do not give AI tool access or credentials to anyone outside the company without proper approval and completion of security checks.

Non-Interference with Applicable Laws

Nothing in this policy shall be construed to prevent disclosure of Confidential Data as may be required by applicable law or valid legal process. Nothing in this policy prohibits or is intended to restrict or impede the exercise of rights under the U.S. National Labor Relations Act, or disclosure or discussion of truthful information about unlawful employment practices.

Policy Exceptions

Exceptions require approval from the CIO and Legal.

Questions

If any employee has questions about the appropriateness of using AI, contact the Head of AI or Legal for guidance.

Review and Revision

This Policy will be subject to change based on evolving regulatory requirements.