Responsible Generative AI

Purpose

The field of generative artificial intelligence (GenAI) is expanding quickly. Although GenAI can greatly increase an organization's productivity and revenue, there are dangers associated with its use. GenAI requires careful consideration of matters relating to cybersecurity, intellectual property, privacy, third-party/client engagements, legal duties, and regulatory compliance.

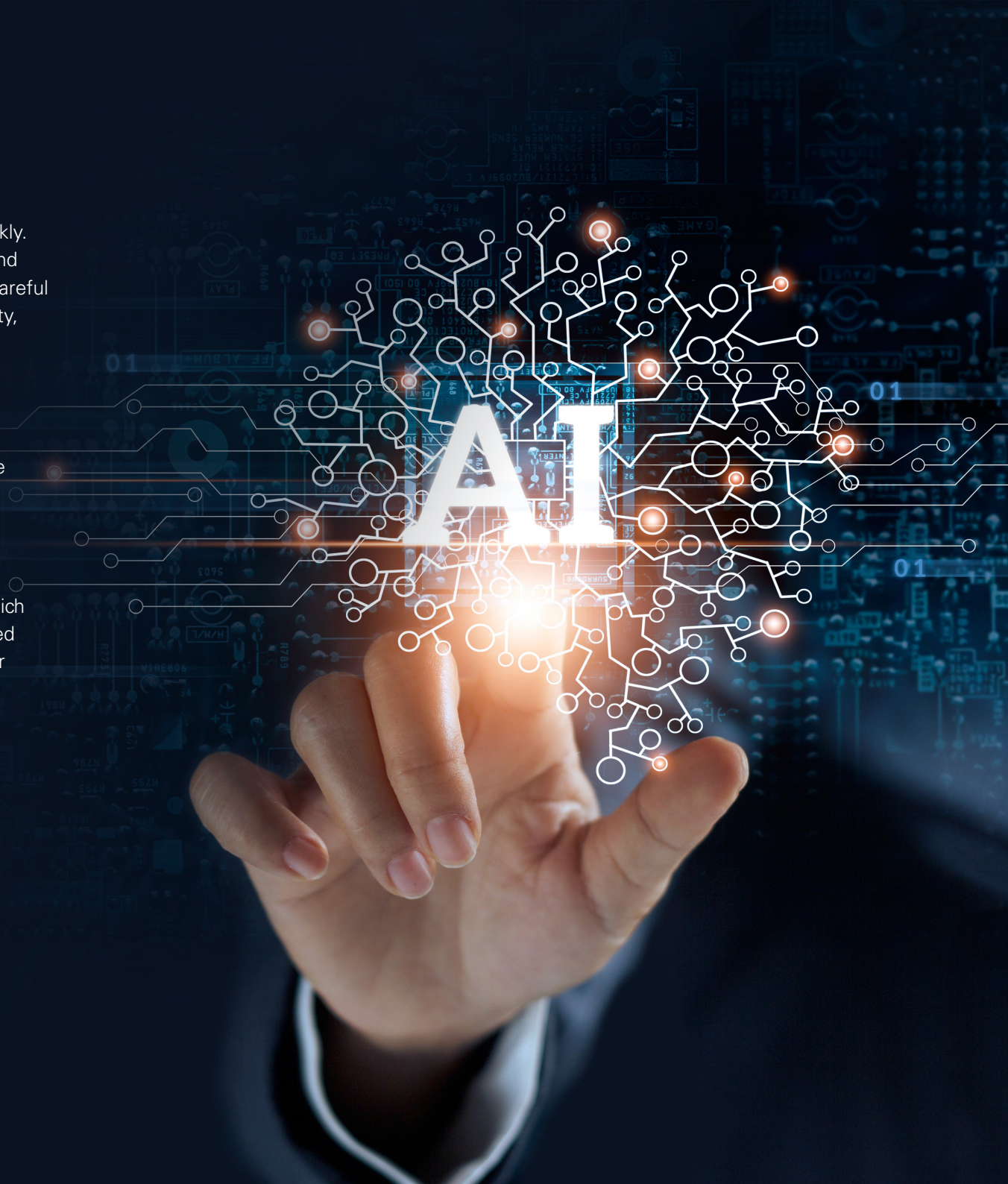
The goal of this policy is to establish responsible usage, deployment, and development of Generative AI within Axtria. This policy also aims to mitigate risks and challenges associated with the technology while maximizing its benefits.

Scope

This policy is dynamic, reflecting the rapid changes in technology, which we embrace in full accordance with Axtria's values of human-centered design, responsibility, and sustainability, as well as our safeguards for security and privacy.

Responsible AI @ Axtria

To mitigate GenAI risks, Axtria has developed a Responsible GenAI framework consisting of four main pillars.



Pillar 1: Dependable and Secure

- **Security, Privacy, and Compliance** to ensure:
  - Robust data encryption, differential privacy techniques, model isolation, and secure data storage solutions
  - Regular compliance and legal reviews, ensuring the ability to control AI outputs
  - Development and use of the system is within the bounds of global regulations (also as required per U.S. Executive Orders)
  - Regular checking and verifying of model outputs for copyrighted or sensitive data
  - Only subscription-based GenAI models are used for cloud hosting
  - Open-source GenAI models are used only within an Axtria VPC to eliminate security and privacy risks
  - Data collection, use, and retention is done lawfully, securely, and protects consumer privacy
  - Assessment of risk/conformity* to identify risk categories:
    - *Unacceptable Risk:* Prohibited due to their significant harm potential.
    - *High-Risk AI Systems:* Regulated and subject to stringent requirements.
    - *Limited-Risk AI Systems:* Subject to lighter transparency obligations.
    - *Minimal Risk:* Unregulated AI applications, including most existing AI systems on single market (e.g., AI-enabled video games and spam filters).
- **Model robustness**
  - Testing models for robustness from adversarial attacks, data, or concept drift
- **Usage monitoring and assessment**
  - Collecting and analyzing model outputs regularly to ensure model consistency on key metrics.
  - Regularly reviewing and assessing generative model user prompts to ensure usage remains aligned with intent

Pillar 2: Accountability and Governance

- **Documentation and ownership**
  - Documenting the project's relevant compliance check outputs and decision points with appropriate governance
  - Ensuring clear ownership for each stage of the development cycle as well as corporate accountability for potential failures
  - Clearly documenting requirements and specifics of when and how a model output can be used
- **Third-party model governance**
  - Documenting all instances of third-party models in use across systems
  - Providing best practices and limitations to end users interacting with third-party models
  - Reviewing and authorizing third-party models in accordance with governance or responsible AI policies wherever possible
- **Oversights and sign-offs**
  - Assigning roles and requirements for each stage of the AI pipeline, cross-checked against the GenAI project framework and full development cycle
  - Requiring sign-off from relevant parties before moving to the next stage of a pipeline build

* A conformity assessment is mandatory for High-Risk projects/POC at Axtria; also mandatory per the EU AIA Act

Pillar 3: Humane and Equitable

✦ Bias measures

- Documenting potential sensitive attributes in datasets
- Measuring and documenting disparate impacts of sensitive attributes across outcome variables and relevant subpopulations
- Assessing dataset features for potential human bias entry or encoding practices
- Checking system designs and data collection practices for automation, sampling, or confirmation biases

✦ Threshold and acceptable deviations

- Assessing business risk/value of deviation from the selected fairness metrics and documenting acceptable risks of deviation
- Reevaluating metrics and thresholds after model build and before final deployment
- Provide monitoring teams with guidance for preventive risk monitoring

✦ Impact and unintended consequences

- Discussion with relevant stakeholders before development to map out expected impacts and potential unintended consequences
- Measuring model fairness in accordance with set guidelines when the pipeline is in production
- Ensuring collaborative human-AI interactions, prioritizing human override features, and iterative feedback loops

Pillar 4: Transparent and Explainable

Data linage and traceability

- Documenting all datasets used as basics for models according to the principles outlined in the contract, including how the data was collected, whether it is representative of the population of interest, and with what intent it was collected
- Documenting the rationale for using specific datasets and how new features should be used in downstream/alternative pipelines
- Documenting the rationale for and steps taken toward cleansing, transformation, or another feature

Explainability and interpretability

- Use of a dashboard to contextualize individual predictions against all training data and overall feature importance of the selected model
- Document why a given model was selected before deployment, including the rationale for any custom evaluation metrics built into the model

Reporting and enablement

- Develop reporting that provides complete documentation of the AI pipeline, all relevant decisions taken during the build, and steps taken as part of the responsible AI framework
- Provide clear guidelines on the intended purpose of an AI system as well as those use cases for which it should not be employed
- Provide a mechanism for recourse if an end user is not satisfied with the consistency

GenAI: Data Security, Privacy, and Compliance Measures in the Axtria Environment

Safeguards and Technical Measures

Axtria has adopted a defensive posture of in-depth security. These measures include the information security pillars of process, people, technology, and the culturally associated components that protect Axtria's environment. These include, but are not limited to:

- **Information Security and Privacy Management System (ISPMS)**
  - Axtria's global ISPMS policy
  - IT processes per the NIST and CIS standard framework
  - Information Security awareness and training
- **Application, Infrastructure, and Data Security**
  - Cloud workload protection using native & OEM security products.
  - Data leak protection through DLP
  - Zero trust security for remote users
  - Periodic Vulnerability Assessment & Penetration Testing for infra and applications.
  - Encryption for endpoints & Data while in transit & at rest
  - Patch management for regular updates of patches to protect against vulnerabilities.
  - Business Continuity Plan/Disaster Recovery and periodic drills
  - OEM products - Nextgen Firewalls, Web Application Firewall (WAF), DDOS
  - Endpoint detection and response (EDR) technology to protect and detect zero-day vulnerabilities
- **Security Operations**
  - NextGen SOC-24X7 monitoring of all infrastructure and applications on the Azure Sentinel SIEM platform
  - Forensic analysis for identifying suspicious patterns
  - Security incident response and management

Accreditations and Certifications - International Standards

- **External Accreditations and Certifications:**

  Axtria has international accreditations and certificates that include:

  - ISO 27001: 2013 (Information Security Management System)
  - ISO 27701: 2019 (Privacy Information Management System)
  - System and Organizational Controls (SOC) - II Type II - Sales IQ
  - Axtria is assessed by CyberVadi, and our score is Gold.

This accreditation confirms that Axtria has reliable, well-defined, and closely monitored policies and procedures. This accreditation acknowledges Axtria's unwavering commitment to system integrity, privacy, confidentiality, and availability.

- **Internal Compliance and Audit:**

Axtria has a dedicated InfoSec team, that conducts internal validations based on industry best practices based on Responsible AI GDPR, HIPAA, Privacy Impact Assessments & NIST 800-53, ISO 42001, NIST AI.100 & EU AIA best practices.

Axtria GenAI Core Committee Governance and Function Responsibilities

Generative AI Core Committee

- Define and govern policy for the responsible use, deployment, and development of Generative AI
- Drive awareness on the responsible use, deployment, and development of Generative AI
- Provide thought leadership and advice on Generative AI technology and Axtria GenAI offerings

InfoSec

- Define cybersecurity controls to protect Axtria infrastructure from probable attack vectors and threats powered by generative AI
- Define security controls to protect GenAI models and associated data against misuse and unauthorized use
- Provide audit and governance
- Ensure GenAI compliance
- Cybersecurity assessments for customer GenAI POCs
- Define a plan to check for usage, deployment, and development of GenAI during account audits
- Define a framework for assessing GenAI use cases that involve the use of personal information
- Provide training and awareness of privacy risks around GenAI

Legal

- Advise whether Intellectual property Rights and liabilities arising from the usage or development of GenAI should be addressed in client, vendor, contractor, and partner contracts

Founded in 2010, Axtria is a global provider of cloud software and data analytics to the life sciences industry. We help life sciences companies transform the product commercialization journey to drive sales growth and improve healthcare outcomes for patients. We continue to leapfrog competition with platforms that deploy artificial intelligence and machine learning. Our cloud-based platforms - Axtria DataMAx™, Axtria SalesIQ™, Axtria InsightsMAx™, Axtria CustomerIQ™, and Axtria MarketingIQ™ - enable customers to efficiently manage data, leverage data science to deliver insights for sales and marketing planning, and manage end-to-end commercial operations. We help customers in the complete journey from data to insights to operations.

For more information, visit www.axtria.com.

Follow Axtria on Twitter, Facebook, Instagram, and LinkedIn.

facebook.com/Axtria

www.axtria.com

connect@axtria.com

Axtria – Ingenious Insights

@Axtria

+1-877-929-8742