



Responsible AI Policy

Ensono's policy on the responsible development, deployment, and operation of artificial intelligence.

SECTION 1

Purpose



Ensono uses artificial intelligence – including generative and agentic AI – to enhance service delivery, operational resilience, security, and innovation, while maintaining human accountability, customer trust, and regulatory compliance.

This policy describes Ensono's responsible approach to AI for customers, partners, vendors, and the public. It sets out the positions Ensono takes on the responsible development, deployment, and operation of AI throughout the AI lifecycle.

SECTION 2

Scope



This policy applies to:

- All AI systems Ensono develops, deploys, or operates in connection with services delivered to customers.
- All AI systems used internally by Ensono associates in support of customer engagements, including approved generative AI tools.
- Third-party AI components and services that Ensono integrates into, or uses to deliver, customer services.
- All Ensono associates, contractors, and subcontractors who develop, deploy, or operate AI on Ensono's behalf.

This policy applies across the AI lifecycle: design, development, deployment, operation, monitoring, and retirement. It applies in addition to Ensono's information security, privacy, data protection, and code-of-conduct obligations.

SECTION 3

Definitions



For the purposes of this policy:

TERM	DEFINITION
Artificial intelligence (AI)	Computer systems and software that perform tasks ordinarily associated with human intelligence, including reasoning, learning, perception, and decision support. Includes machine learning, generative AI, and agentic AI.
Generative AI	AI that produces new content – text, code, images, audio, or other media – typically by drawing on a foundation model trained on large datasets.
Agentic AI	AI systems that plan, call tools, and act on behalf of a user or another system within a defined scope, and that may take a sequence of actions to achieve an objective.
Foundation model	A large AI model trained on broad data and adaptable to many downstream tasks. Foundation models may be operated by Ensono, by a customer, or by a third-party provider.
Customer confidential information	Customer information designated as confidential under contract. Includes personal data and customer application data.
System, operational, or management data	Data generated through Ensono's delivery and management of services – for example, telemetry, log data, performance metrics, ticketing records, and capacity data – that is not customer application data and that Ensono uses to operate, monitor, and improve its services.

Principles for Responsible AI

Ensono's use of AI is guided by the following principles, applied throughout the AI lifecycle (design, development, deployment, operation, and retirement).

4.1 Human-Centered and Accountable

AI is used to augment human expertise, not to replace it. Meaningful decisions that materially impact customers, services, or compliance remain subject to human judgment, oversight, and accountability.

4.2 Transparency and Trust

Ensono is transparent about the use of AI in service delivery. Where AI is used, Ensono is prepared to explain the role AI plays, the type of tools involved, and the safeguards in place, consistent with security obligations.

4.3 Privacy and Data Protection

Protecting customer data is foundational. Ensono uses AI in accordance with applicable data protection and privacy laws.

- Customer confidential information – including personal data and customer application data – is not used to train shared or foundation AI models.
- Ensono may use system, operational, or management data generated through the delivery and management of services, and may analyze certain customer information for service delivery and analytical purposes (including retrieval-based analysis), in each case subject to applicable legal requirements.
- Customer data remains governed by applicable law and the terms of the applicable customer agreement throughout the AI lifecycle, including how it is used, retained, and handled at the conclusion of an engagement.
- The availability, access, and sharing of data generated in connection with services are governed by applicable law and customer agreements

4.4 Security and Resilience

AI systems are treated as production systems and are subject to Ensono's information security program, including controls for confidentiality, integrity, availability, and resilience. Ensono monitors for AI-specific threats – including prompt injection and data-poisoning indicators – and integrates AI events into enterprise logging and incident response. AI solutions are designed to reduce risk, not to introduce unmanaged exposure.

4.5 Fairness and Risk Awareness

Ensono manages AI use through a risk-based governance approach designed to identify and address material risks, including potential unintended outcomes.

Ensono applies a risk-based approach that scales governance, controls, and review to the nature and sensitivity of each AI use case. Bias risk is assessed before an AI system enters production and reassessed over the course of its operation.

4.6 Reliability and Quality

AI-assisted outputs are tested, monitored, and continuously improved. AI is not represented as authoritative without appropriate validation, and outputs are subject to human review consistent with their use and impact. Where AI cannot meet the resilience or accuracy bar of the system it touches, Ensono does not deploy it.

SECTION 5

Use of AI in Client Services

Ensono uses AI to deliver better customer outcomes across managed services, including improved reliability, faster issue resolution, stronger security, and continuous service optimization. AI enables Ensono teams to anticipate issues, automate routine tasks, surface actionable insights, and direct human expertise where it delivers the most value.

AI may be embedded within the tools and platforms Ensono uses to deliver services, in support of:

- Proactive operations through predictive monitoring, anomaly detection, and root-cause analysis.
- Faster and more consistent execution through intelligent automation and workflow optimization.
- Improved security and resilience through advanced detection, response, and risk analysis.
- Data-driven optimization that continuously improves performance, availability, and customer experience.

Ensono's approach combines automation with deep platform expertise and human oversight, enabling AI to scale safely across complex, mission-critical environments.

SECTION 6

Client Protections and Transparency

Alongside the benefits AI delivers, Ensono applies strong protections to maintain customer trust:

- Customer-specific AI configurations and customer-specific predictive models are isolated to the customer's environment and decommissioned at the end of the engagement.
- AI use is governed by customer contracts, including confidentiality, data protection, and security obligations.

- Ensono does not rely solely on AI to make decisions that materially affect customers or service outcomes; human review and accountability remain integral.
- Material changes to AI use within a customer's services are subject to Ensono's established change-management practices, applied in a manner appropriate to the nature and risk of the change.
- Customer data residency, sovereignty, and retention obligations are honored throughout the AI lifecycle.

WHAT CUSTOMERS CAN EXPECT

Ensono segregates customer-specific models, honors data residency and sovereignty obligations, and requires human authorization for consequential actions.

SECTION 7

Third-Party and Vendor AI

Ensono works with technology partners and vendors that incorporate AI into their products and services. All third-party AI used in connection with Ensono services is subject to Ensono's vendor risk management, security, privacy, and responsible AI requirements.

Vendors are required to:

- Comply with applicable laws and Ensono policies, including Ensono's standards for security, data protection, and responsible use of AI.
- Disclose material AI use relevant to the services they provide, in sufficient detail for Ensono to assess risk.
- Support Ensono's commitments to customers, including those concerning the use of customer data and the training of shared or foundation models.
- Cooperate with Ensono's incident response and audit processes for AI-related events.

Where a third-party AI offering cannot meet Ensono's requirements – for example, if it cannot exclude the use of customer data for retraining – Ensono will require a private deployment or will not use the offering for customer work.

SECTION 8

Regulatory Alignment

Ensono actively monitors evolving AI-related laws and regulatory frameworks and aligns its practices with applicable requirements. Ensono seeks consistency across jurisdictions while allowing appropriate adaptations where local laws require them.

Ensono aligns relevant aspects of its responsible AI practice to the following external frameworks and standards:

- **EU AI Act** – including emerging requirements related to risk classification, documentation, and notification for higher-risk systems.
- **NIST AI Risk Management Framework**, including the Generative AI Profile.
- **ISO/IEC 42001** – AI Management Systems. Ensono aligns its practices to this standard; formal certification is under evaluation.
- **ISO/IEC 27001** – Information Security Management. Ensono operates a certified Information Security Management System that provides the security spine on which its AI practice runs.

Where customer-specific regulatory obligations apply – for example, sector-specific rules in financial services, healthcare, or the public sector – Ensono works with the customer to apply additional controls consistent with those obligations.

SECTION 9

Governance and Oversight

AI at Ensono is governed through established enterprise governance processes that integrate Legal, Security, Privacy, Technology, and business leadership. These functions collectively set direction, review AI design and deployment decisions, manage risk, and ensure accountability across the AI lifecycle. Ensono applies centralized oversight, risk-based review, and ongoing monitoring of AI use to ensure alignment with internal policies, customer commitments, and applicable laws. This governance model is designed to enable responsible innovation while maintaining trust, safety, and compliance.

AI use is subject to risk-based evaluation and ongoing oversight appropriate to the nature and sensitivity of the use case. Where issues are identified, Ensono applies established incident and remediation processes.

All Ensono associates, contractors, and subcontractors involved in the development, deployment, or operation of AI are required to complete applicable training and maintain awareness of this policy and related standards.

Associates and other personnel who identify concerns regarding AI use – including suspected bias, errors, security issues, or misuse – are expected to report such concerns through Ensono's established escalation and incident reporting channels.