



IronYun Company Policy for Compliance with the European AI Act

Effective Date: January 3rd, 2025

1. Purpose

IronYun is committed to ensuring compliance with the European Union Artificial Intelligence (AI) Act. This policy establishes guidelines for the responsible development, deployment, and management of AI systems in accordance with EU regulations.

2. Scope

This policy applies to all AI systems developed, used, or sold by IronYun within the EU or impacting EU citizens. It includes internal AI applications, customer solutions, and partnerships involving AI technologies.

3. AI System Classification

IronYun classifies AI systems according to the EU AI Act risk framework:

- **Unacceptable Risk:** AI applications banned by the EU, such as social scoring or biometric categorization.
- **High Risk:** AI systems used in critical infrastructure, employment, law enforcement, and biometric identification.
- **Limited Risk:** AI applications that require transparency and user awareness, such as chatbots and deepfakes.
- **Minimal Risk:** AI solutions with no significant regulatory requirements, such as spam filters and recommendation engines.

4. High-Risk AI Compliance Requirements

For high-risk AI systems, IronYun will ensure:

- **Risk Management:** The company has implemented a documented risk management system.
- **Data Governance:** The company use high-quality, representative, and unbiased datasets.
- **Transparency:** Provide clear documentation and user instructions.
- **Human Oversight:** Ensure human control to mitigate risks.
- **Robustness & Security:** Design AI models that are resilient against attacks and malfunctions.
- **Conformity Assessment:** Conduct internal and external evaluations to verify compliance.



5. Transparency and Explainability

IronYun commits to ensuring:

- Users are informed when interacting with AI systems.
- AI-generated content is clearly labeled.
- AI decisions in high-risk applications are explainable and interpretable.

6. Data Privacy and Security

IronYun follows GDPR and EU AI Act standards for:

- Protecting user data through encryption and access controls.
- Ensuring AI models do not process personal data beyond their stated purpose.
- Conducting regular security audits to prevent data breaches.

7. Ethical AI Principles

IronYun adheres to ethical AI practices by:

- Preventing bias and discrimination in AI models.
- Ensuring AI applications align with human rights and democratic values.
- Conducting impact assessments before deploying high-risk AI systems.

8. Monitoring and Compliance

- Regular audits will be conducted to verify adherence to this policy.
- A compliance officer will oversee EU AI Act-related activities.
- Employees and stakeholders will receive training on AI ethics and regulations.

9. Reporting and Redress

IronYun provides:

- A reporting mechanism for concerns related to AI risks.
- A redress system for users affected by AI decisions.
- A contact point for regulatory bodies regarding compliance inquiries.

10. Policy Review and Updates

This policy will be reviewed annually or as required by regulatory changes. Updates will be communicated to all relevant stakeholders.

For further details or inquiries regarding this policy, please contact sales@IronYun.com