AI POLICY

Effective Date: ___________, *20___*

This AI Policy ("Policy") is issued by ______________________________ ("Company") and is intended to govern the responsible use of Artificial Intelligence ("AI") technologies by employees, contractors, and third-party partners (collectively, "Users"). This Policy outlines expectations, limitations, governance, and enforcement to ensure legal compliance, data protection, fairness, and ethical integrity in all AI-supported operations.

1. Purpose. The purpose of this Policy is to:

- Ensure the ethical, legal, and secure use of AI tools within the Company's operations.
- Provide clear guidance to Users on acceptable AI usage.
- Prevent misuse or overreliance on automated systems in sensitive or regulated contexts.
- Protect Company and customer data and intellectual property from improper exposure or influence through AI tools.
- Promote transparency, accountability, and continual oversight in the implementation of AI technologies.

2. Scope.

2.1 Applicability. This Policy applies to all Users engaging with AI tools in the course of their work with the Company.

2.2 Definitions.

- "PII" means Personally Identifiable Information, including but not limited to names, addresses, identification numbers, financial account details, biometric data, and any information that could reasonably be used to identify an individual.
- "Confidential Information" means non-public information including trade secrets, business plans, customer data, financial information, and any information designated as confidential.
- "AI-Generated Content" means any output produced partially or wholly by an AI system, including text, images, code, audio, video, or data analysis.
- "High-Impact AI Decision" means any AI-supported process that affects employment, financial status, legal rights, or access to essential services.

2.3 Approved AI Tools. Only AI tools that have been:

- Evaluated and approved by the Company's AI Governance Committee.
- Reviewed for compliance with applicable laws and internal controls may be used.

The following AI tools are approved for use:

AI Tool	Date of Approval

This list shall be maintained by the AI Officer and updated ____________ [e.g., quarterly]. Users must verify a tool's approved status before use.

2.4 Evaluation of New AI Tools. Before introducing new tools:

- Users must complete a Request for Evaluation Form.
- The Company will assess the tool’s accuracy, reliability, vendor data policies, and ethical impact.
- Tools involving third-party services will be scrutinized for security certifications and compliance with Company standards.

3. Policy.

3.1 General Principles. All use of AI tools must reflect:

- Integrity in application and outputs
- Compliance with Company values
- Non-malicious and non-deceptive intent

3.2 Responsible Use.

- AI tools must be used only for legitimate, job-related purposes.
- Users shall avoid excessive automation or using AI to circumvent normal processes.
- No AI-generated content may be presented as human-authored unless explicitly permitted.

3.3 Legal Compliance.

Users shall strictly adhere to all applicable laws, regulations, and legal requirements governing the use of Artificial Intelligence (AI) technologies. Compliance obligations include, but are not limited to, the following areas:

- Data Protection and Privacy:
    - Users must comply with global data protection laws that regulate the processing of personal data using AI systems, including:
        - California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) (US): Respecting data subject rights and ensuring data privacy in AI applications affecting California residents.
    - Users shall implement measures to protect Personally Identifiable Information (PII) when using AI tools, including anonymization or pseudonymization where appropriate.
    - Users must ensure that data processing agreements are in place when utilizing AI tools provided by third parties.

- Intellectual Property (IP) and Copyright Compliance:
  - Users must respect all intellectual property rights when using AI tools, in compliance with:
    - Copyright Act of 1976 (US): Avoiding the unauthorized use of copyrighted material in AI-generated outputs.
    - Digital Millennium Copyright Act (DMCA) (US): Ensuring AI systems do not circumvent copyright protection technologies.
  - Users shall not use AI tools to generate content that infringes on patents, trademarks, or other IP rights.
  - Users must verify that any datasets used for training AI models are either licensed for use or fall within the scope of permissible use under applicable IP laws.
- Licensing and Contractual Obligations:
  - Users must abide by all licensing terms, end-user agreements, and contractual obligations established by AI tool providers, including:
    - Verifying the scope of permissible uses as specified in the license agreement.
    - Refraining from reverse engineering or modifying AI tools in ways prohibited by the license.
    - Ensuring compliance with software licensing requirements, particularly for open-source AI systems.
  - The Company shall maintain records of licensing agreements and update them in line with vendor changes or new deployments.
- Fairness, Accountability, and Transparency:
  - Users must adhere to fairness and anti-discrimination laws when using AI for decision-making, including:
    - Equal Employment Opportunity (EEO) Laws (US): Ensuring AI-driven hiring practices do not lead to biased outcomes.
    - Title VII of the Civil Rights Act (US): Prohibiting AI systems from making discriminatory employment decisions.
    - Algorithmic Accountability Act (Proposed, US): Promoting transparency in high-impact AI systems.
  - Users shall document the logic and decision criteria used by AI systems, ensuring traceability and accountability.
- Information Security and Risk Management:
  - Users must adhere to information security laws and standards to protect AI systems from unauthorized access, including:
    - Cybersecurity Information Sharing Act (CISA) (US): Maintaining cybersecurity practices to safeguard AI models.
    - National Institute of Standards and Technology (NIST) AI Risk Management Framework (US): Implementing risk-based approaches to AI deployment.
    - ISO/IEC 27001: Ensuring information security management when integrating AI with sensitive data.

    - Users must report data breaches involving AI systems as required by applicable data protection laws.

- Maintaining Awareness and Adapting to Legal Changes:

    - The Company is committed to staying updated on evolving legal standards related to AI, including emerging regulations and judicial interpretations.
    - The AI Governance Committee shall monitor legislative developments and recommend updates to AI practices as needed.
    - Users will receive periodic training to ensure awareness of new legal obligations and compliance standards.

3.4 Transparency and Accountability.

- Legal Requirements and Best Practices:

    - Disclosure: The requirement to disclose AI-generated content aligns with the EU AI Act and the U.S. AI Bill of Rights, both of which emphasize transparency in automated decision-making.
    - Traceability: Maintaining traceability is consistent with the OECD AI Principles, which stress accountability and traceability in AI deployments.
    - Intellectual Property (IP): The assignment of IP rights to the Company aligns with the Copyright Act of 1976 and relevant case law establishing employer ownership of employee-created work products.
    - Ownership of AI Outputs: Preventing personal claims over AI-generated content is also aligned with the Digital Millennium Copyright Act (DMCA) to avoid copyright disputes.
    - A requirement for users to log and document instances where AI-generated content is used, especially for high-impact decisions.
    - A clause specifying that users must include disclaimers when AI content could be interpreted as human-authored, in line with the EU AI Act's transparency obligations.
    - A statement that AI-generated content, when presented as factual or authoritative, must undergo human verification, particularly in regulated sectors (e.g., healthcare, finance).

3.5 Data Security and Confidentiality.

- No PII, client data, financial records, or proprietary material shall be submitted into public or cloud-hosted AI tools unless explicitly approved.
- AI tools may not store, transmit, or generate outputs from confidential information unless processed within secure, Company-controlled environments.

3.6 Bias and Fairness.

- Users must critically evaluate AI outputs for bias, stereotypes, or unfair outcomes.
- Any observed harm or error must be documented and reported.

3.7 Human Oversight.

- Final responsibility for decisions rests with human Users.

- AI is to augment—not replace—human judgment, especially in domains affecting safety, legality, or rights.

3.8 Training and Education. The Company shall ensure that all Users are properly trained to use AI tools responsibly and in accordance with this Policy.

All Users must complete: (Check all that apply)

☐ Basic AI Literacy Training
☐ Tool-Specific Training
☐ Refresher Courses on AI Ethics
☐ High-Risk AI Training
☐ Data Privacy and Security Training
☐ Incident Reporting and Risk Management
☐ Training Record Maintenance
☐ Post-Implementation Training
☐ ____

Training completion shall be documented and reported ___________ [e.g., quarterly] to the AI Governance Committee.

3.9 Third-Party Services.

- All external AI vendors must enter into Data Processing Agreements (DPAs) that comply with applicable data protection laws, including but not limited to the: (Check all that apply) ☐ General Data Protection Regulation (GDPR) ☐ California Consumer Privacy Act (CCPA) ☐ Health Insurance Portability ☐ Accountability Act (HIPAA), and any relevant jurisdiction-specific AI regulations.
- Vendors shall commit to compliance with all applicable laws governing AI use, data privacy, security, and intellectual property rights. Vendors must notify the Company promptly of any governmental or regulatory investigations, breaches, or legal actions related to their AI tools or data handling practices.
- Vendors must maintain current security certifications such as ISO/IEC 27001, SOC 2 Type II, or equivalent, and implement industry-standard technical safeguards including encryption of data at rest and in transit.
- Data breach notifications must be provided to the Company within regulatory timeframes.
- Vendor contracts must explicitly grant the Company the right to audit AI tools, data handling, and compliance procedures, and include termination rights for cause, including but not limited to breaches of security, data privacy, or ethical obligations.
- Vendors are required to provide transparency regarding AI model training data sources, methodologies, and any bias mitigation efforts, with documentation and audit results available to the Company upon request.
- Vendors must implement and document business continuity and disaster recovery plans to ensure resilience and uninterrupted service.
- The Company requires that vendors disclose any subcontractors involved in AI development or data processing and ensure that subcontractors comply with equivalent legal, security, and ethical standards.
- Intellectual property rights, including ownership and licensing of AI models, outputs, and derivatives, must be clearly defined. Vendors shall indemnify the Company against any

intellectual property infringement claims arising from the use of the AI tools.

- Upon termination or expiration of the vendor agreement, vendors must securely return or delete all Company data and AI-generated outputs in accordance with Company data retention policies and applicable law
- All third-party AI providers will be documented in a vendor risk register maintained by the Company, which will be regularly reviewed to monitor compliance, risk exposure, and contractual performance.

3.10 Department-Specific Guidelines. (Optional)

Department	**Guidelines**

3.11 Emergency Procedures.

In case of AI system failure, Users shall: (Check all that apply)

☐ Document the nature and time of the failure, including any error messages, logs, or symptoms observed.
☐ Notify the AI Officer within ____ hours, providing a summary of the issue and any immediate impacts.
☐ Follow the Company's Incident Response Plan, which may include isolating affected systems or disabling integrations.
☐ Coordinate with IT support for a comprehensive diagnostic and resolution plan.
☐ Conduct a post-incident analysis to determine root causes and document lessons learned.
☐ Implement corrective actions to prevent similar failures in the future.
☐ Update the AI Governance Committee on the failure, impact assessment, and mitigation steps taken.
☐ ____

For suspected security breaches or harmful outputs: (Check all that apply)

☐ Immediately cease using the affected tool
☐ Preserve evidence of the incident
☐ Follow the Company's Incident Response Plan
☐ ____

The Company shall maintain backup procedures for all critical functions supported by AI tools.

3.12 Risk Assessment Framework.

All AI applications shall be classified as:

- Low Risk: Tools with minimal potential for harm
- Medium Risk: Tools that influence but don't determine outcomes
- High Risk: Tools that automate decisions affecting rights, health, or finances

High-risk applications require: (Check all that apply)

☐ Formal impact assessment before deployment
☐ Regular auditing
☐ Enhanced human oversight protocols
☐ Documented testing for bias and accuracy
☐ ____

The AI Governance Committee shall maintain risk assessment templates and review criteria.

3.13 Cross-Border Considerations. (Optional)

Users shall strictly comply with the following requirements when using AI tools that involve cross-border data processing or international deployments: (Check all that apply)

☐ General Data Protection Regulation (GDPR): Ensuring data minimization, purpose limitation, and lawful basis for processing personal data. Specific provisions apply to automated decision-making and profiling.

☐ Personal Information Protection and Electronic Documents Act (PIPEDA): Protecting personal data when using AI for data analysis or automated decisions.

☐ Transparency obligations include clearly indicating when content or decisions are AI-generated, as mandated by regional AI regulations.

☐ Adhere to all relevant jurisdictional regulations mandating that data be stored, processed, or maintained within specific geographic boundaries, including but not limited to the: (Check all that apply) ☐ EU General Data Protection Regulation (GDPR) ☐ China's Cybersecurity Law ☐ __________________, and other applicable local data residency laws.

☐ Verify that AI systems hosted or managed by third-party vendors comply with regional data localization mandates before deployment.

☐ Ensure that all cross-border data transfers comply with applicable data protection frameworks, including: (Check all that apply)

☐ GDPR (Chapter V): Implement Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or obtain explicit data subject consent for transfers outside the EU/EEA.

☐ California Consumer Privacy Act (CCPA): Maintain appropriate data transfer agreements when processing data outside of California.

☐ APEC Cross-Border Privacy Rules (CBPR) System: For transfers within the Asia-Pacific region.

☐ Berne Convention for the Protection of Literary and Artistic Works (International): Avoiding infringement of copyrighted works in global contexts.

☐ Maintain documentation of transfer mechanisms used, such as adequacy decisions, data processing agreements, and compliance with international data protection agreements.

☐ Country-Specific AI Regulations and Disclosure Requirements: (Check all that apply)

☐ Familiarize with and adhere to AI-specific legislation and disclosure mandates, including: (Check all that apply)

☐ EU AI Act: Requirements for transparency, risk assessments, and data protection when deploying AI within the EU.

☐ U.S. State-Specific AI Regulations: governing biometric data and automated decision-making.

☐ AI Ethics Guidelines: Including the OECD AI Principles and UNESCO’s Recommendation on the Ethics of AI when operating in global contexts.

☐ Clearly disclose to data subjects when their data may be processed by AI systems across borders, including potential risks and data protection measures in place.

☐ International Data Transfer Management: (Check all that apply)

☐ Obtain approval from the AI Governance Committee before engaging in cross-border data transfers involving AI tools.

☐ Document cross-border data flows in the Company’s Data Transfer Registry, including the legal basis for transfers and any safeguards implemented.

☐ Conduct regular compliance audits to ensure that cross-border data processing activities align with evolving legal requirements.

☐ Conduct DPIAs for AI systems that process personal data across borders to identify risks related to data privacy, compliance, and potential data breaches.

☐ Include risk mitigation measures in the DPIA, particularly when using cloud-hosted AI solutions that may store data in multiple jurisdictions.

☐ ____

- ____
- ____
- ____

International data transfers involving AI systems must be: (Check all that apply)

☐ Approved by the AI Governance Committee, following a formal risk assessment and review of compliance with applicable regulations.
☐ Documented in the Company's Data Transfer Registry, including the purpose of the transfer, data categories involved, transfer mechanisms (e.g., SCCs, BCRs), and the receiving jurisdiction.
☐ Supported by Appropriate Safeguards, such as encryption, pseudonymization, data minimization practices, and contractual commitments from recipients to maintain data security and privacy.
☐ Assessed for Legal Adequacy, ensuring the receiving country offers a comparable level of data protection (e.g., under GDPR adequacy decisions).
☐ Reviewed for Data Subject Rights, ensuring that data subjects are informed of the transfer and their rights under applicable data protection laws.
☐ Monitored for Compliance, with periodic reviews to ensure that cross-border data processing remains lawful and consistent with the original risk assessment.
☐ Accompanied by Data Protection Impact Assessments (DPIAs) where the transfer poses a high risk to the rights and freedoms of data subjects.
☐ Regional Variations in AI Regulations Shall Be Documented and Communicated to Affected Users, including any additional obligations or restrictions specific to the jurisdiction.
☐ Securely Managed, ensuring that data is protected against unauthorized access during transit and at rest, especially when using cloud-based AI services hosted internationally.
☐ Reassessed Annually or When Regulations Change, to maintain ongoing compliance with evolving data protection and AI governance standards.

4. Implementation and Monitoring.

4.1 AI Governance Committee.

- A cross-functional team will oversee policy implementation, perform risk assessments, and advise on high-impact AI projects.
- The Committee shall meet at least quarterly or upon request following incidents.

4.2 Designated AI Officer. Point of contact for questions, tool approvals, and incident reports:

Name: ___________________________
Email: ___________________________
Phone: __________________________

Name: ___________________________
Email: ___________________________
Phone: __________________________

Name: ___________________________
Email: ___________________________
Phone: __________________________

4.3 Reporting Incidents. Users must immediately report:

☐ Unauthorized AI use
☐ Security breaches involving AI tools

☐ Harmful, biased, or noncompliant outputs
☐ ____

4.4 Violations. Any violation of this Policy may result in:

☐ Written warnings
☐ Revocation of AI access
☐ Disciplinary action, up to termination
☐ Referral to legal or compliance authorities if applicable
☐ ____

4.5 Enforcement. The Company reserves the right to audit system logs, restrict access, suspend tools, or take legal measures if this Policy is breached.

4.6 Version Control. The Company shall maintain records of: (Check all that apply)

☐ AI system versions in use
☐ Dates of deployment and retirement
☐ Significant changes between versions
☐ ____

Users shall: (Check all that apply)

☐ Document which version of an AI tool was used for significant outputs
☐ Report unexpected changes in AI behavior that may indicate version changes
☐ Verify version compatibility when integrating multiple AI systems
☐ ____

Change management procedures for AI tools shall include testing, user notification, and training updates.

5. Review and Amendments.

5.1 Review.

- This Policy shall be reviewed no less than annually by the AI Governance Committee.
- Material changes may occur in response to legal updates, technological advances, or internal audit findings.

5.2 Amendments. No amendment to this Policy shall be valid unless made in writing and formally adopted by the AI Governance Committee.

ACKNOWLEDGMENT

I have read, understood, and agree to abide by the terms of the Company’s AI Tool Usage Policy.

Signature: ___________________________
Name: _________________
Date: ____________, 20___