Western Digital.

D034-000251-000000

Artificial Intelligence (AI) Policy

Revision No: 01

1. Purpose

This policy establishes governance, appropriate use, and risk management expectations for all forms of Artificial Intelligence ("AI") technologies including Machine Learning (ML), Generative AI (GenAI), AI Agents, Agentic AI systems, and other AI capabilities as the technology continues to evolve. It promotes the responsible, ethical, and secure development, deployment, and usage of AI systems, protecting the company from legal, regulatory, reputational, and operational risks while empowering our workforce to safely innovate and integrate AI technologies in support of our business objectives.

2. Scope

This policy applies worldwide to all Western Digital employees, contractors, vendors, business partners, and other third parties (hereinafter collectively referred to as "you" or the "workforce") using, developing, modifying, procuring, or managing AI-related systems, services, or data on behalf of Western Digital. In this Policy, "Western Digital" or "Company" refers to Western Digital Corporation and all its majority-owned subsidiaries.

Any violation of this Policy may result in disciplinary action, up to and including termination of employment or contract.

2.1 Exclusions

Not Applicable

2.2 Definitions

- **Artificial Intelligence (AI):** Technologies that simulate human intelligence functions.
- **Machine Learning (ML):** Systems that learn from data without being explicitly programmed.
- **Generative AI (GenAI):** Systems that can create new content (e.g., text, images, audio, video, code) from input prompts. Output is based on patterns learned from its training data or external context provided.
- **AI or Digital Assistants:** Systems that can automate routine tasks based on direct requests and user input.
- **AI Agents:** Autonomous software that can perform tasks or achieve goals on behalf of a user.
- **Agentic AI:** Autonomous systems that can make independent, contextual decisions and adapt to changing conditions to achieve pre-defined goals without human involvement.
- **Model Drift:** The degradation of model performance over time due to changing data patterns.
- **Prompt Injection:** A type of attack that manipulates GenAI behavior through malicious inputs.

- **Data Lineage:** Ability to trace the origin, movement, transformation, and use of data throughout the entire AI lifecycle.
- **Explainability:** Ability to describe and validate how an AI system produces its decisions, predictions, or recommendations.

3. Corporate Policy

3.1 Overview

Artificial Intelligence offers opportunities to accelerate innovation, streamline operations, and reimagine how we work. It also introduces new risks that require thoughtful and intentional management. This policy is designed to strike a balance by providing reasonable guardrails that are necessary to protect our people, data, and reputation while enabling teams to responsibly explore the transformative potential of AI. This document exists not to limit progress, but to empower it with clarity, accountability, and confidence.

3.2 Workforce Responsibilities

Western Digital's Acceptable Use Policy (AUP) covers the general responsibilities and expectations of our workforce plus other important policy topics regarding the handling of Company information and information systems assets. For AI technologies, you must also adhere to the following.

1. **Approved Systems Only:** Only Company-approved AI systems may be used to process Company data, including but not limited to typing, uploading, connecting to, or otherwise entering such data via prompts or other AI interfaces.
2. **Personal Account Use Restriction:** You must not procure or use personal AI accounts and subscriptions for Company business. Further, you must not use free AI services or accounts to process Company data. You are responsible for complying with the terms of any free AI service you use.
3. **Per-User Subscriptions:** Any commercial AI product requiring user-level subscription must be reviewed and approved by Information Security and Legal before using it to process Company data.
4. **Prompt Safety:** You must not enter or expose regulated, confidential, customer, partner, personal, or other Company data in prompts unless the AI system has been formally approved for such data classes.
5. **Prompt Behavior:** You must not attempt to manipulate an AI system through prompt injection to obtain information or outcomes that are not intended to be available from the AI system.
6. **Agent Limitations:** AI agents and Agentic AI with task or goal autonomy must be governed by defined constraints to prevent unauthorized system changes, data access, or external communications.
7. **Human Oversight:** Decisions that impact safety, legal obligations, finance, potential ethical matters, third parties, sensitive personal data, or employment must involve human review, often referred to as "human-in-the-loop" controls and processes.

8. **Trade Compliance:** All AI use, development, training, and deployment by Company personnel must comply with the Global Trade Policy and applicable trade compliance laws. Do not provide AI systems, models, datasets, or related technical information to any sanctioned or restricted party without legal authorization and Trade Compliance approval. Do not upload, input, or share export-controlled or otherwise restricted technical data in public or third-party AI tools without prior written approval from Trade Compliance.

   Note that Western Digital's Information Security team will partner with our Legal and Procurement organizations for appropriate risk identification, handing, and treatment recommendations.

   In addition to our AUP, other AI-relevant policies include but are not limited to Confidential Information Policy, Global Privacy Policy, Privacy Statement, Global Trade Policy, Global Code of Conduct, Cyber Security Policy, and Third Party Risk Management Policy.

3.3 Acquisition of AI Systems, Software, or Services

The procurement or subscription of any AI-related products, platforms, tools, agents, connectors, or services for Company use must be reviewed and approved by Western Digital's Information Security, Legal, and Procurement teams. Vendor systems and services must include contract clauses on data rights and protection, model considerations (e.g. training restrictions, change management and disclosure, explainability, auditability, access, and portability), intellectual property ownership, and liability for misuse or data breach.

3.4 Internal Deployment of AI Systems

No AI system or software, nor any system or software that makes use of AI, whether commercial, open source, or internally developed, may be deployed into production without prior risk assessment and validation via the Company's AI Enablement process.

3.5 External Deployment of AI Systems

Risks associated with AI systems or services that are offered to our customers, suppliers, partners, the public, or other third parties are significantly greater than those for AI systems used exclusively by our workforce. They also come with a much greater level of Company liability. Such AI systems or services may require disclosure and other additional measures.

The degree of risk assessment, management, and process scrutiny outlined in the following Policy sections will be elevated for external AI deployments.

3.6 Data Access Security and Governance

AI systems may only access information and data they are explicitly authorized to use and must fully honor each source system's access controls including permissions and retention policies. Users of an AI system must not be granted access to information or data that they do not already have access to through the respective source system.

Internally developed models and AI applications must log all data access and support auditability. Such systems that ingest Company data must ensure data lineage and explainability.

Where feasible, Company data stored or indexed for use by an AI system must be encrypted, typically referred to as encryption at rest. All user interfaces and intersystem connections must be encrypted, typically referred to as encrypted in transit.

3.7 Data Integrity

Data, including external datasets or pretrained models, must be sourced with proper consent and comply with privacy regulations, content licensing, and attribution requirements.

Where feasible, owners of AI systems must implement continuous data monitoring and model drift detection to ensure ongoing accuracy, relevance, and fairness where bias may be a concern, with documented mitigation mechanisms to address any issues that surface.

AI generated content, decisions, or outputs that impact business operations, compliance-sensitive processes, or other critical processes must include appropriate human review before action or publication.

3.8 Inappropriate or Discriminatory Data

The creation, distribution, or use of any content or data that is discriminatory, harassing, biased, or otherwise offensive, is strictly prohibited. This includes, but is not limited to, materials that could reasonably be perceived as creating a hostile, intimidating, or abusive environment.

3.9 Intellectual Property (IP) Rights

To mitigate AI created risks to Western Digital's IP and risks of third-party IP claims:

1. **Input into AI Systems**
   - Company confidential information must be input into approved systems only.
   - No third party (e.g., external partner) confidential information can be input into any AI system without Legal approval.
2. **Output from AI Systems**

- Use of AI generated content in external messaging (e.g., marketing), product designs or code (e.g., development), or as part of an external services must be reviewed and approved by Legal.
- Any AI used in creating an invention must be disclosed in the invention disclosure form.

Any IP or other ownership rights in AI models, prompts, software, tools, systems, and their outputs developed using Company data, resources, or time are Company property. The AI models, prompts, software, tools, systems, and their outputs developed using Company data, resources, or time must also be considered confidential and be handled in accordance with Company policies.

Contributions to external AI projects must be pre-approved by Legal to ensure proper IP handling.

3.10 Incident Response and Reporting

All AI-related incidents (e.g. model failures, unexpected outcomes, prompt injection, suspicion of unauthorized access) must be reported immediately to Information Security for investigation in accordance with the Company's Incident Response Plan outlined in the Cyber Security Policy**.**

If an AI-related incident involves the Company's products, additionally report the incident to the Product Security Incident Response Team (PSIRT) at PSIRT@wdc.com. If you have concerns about a situation that might be a legal violation, unethical conduct, or a violation of this Policy, please contact your manager or any of the following resources:

- Ethics and Compliance team at compliance@wdc.com;
- The Legal Department;

The Ethics Helpline, which is available 24 hours a day and allows anonymous reporting, via www.EthicsHelplineWDC.com

Western Digital.

D034-000251-000000

Artificial Intelligence (AI) Policy

Revision No: 01

4. Revision History

Revision	Date	Changes	Author	Function
01	08/22/2025	Revision 01 publish	Phil Malatras	Information Security

5. Approved By

Title	Name	Date Approved
CISO, VP IT	Phil Malatras	08/22/2025