Artificial Intelligence (AI) Policy

Document Control

Policy version number	**v03**
Policy version with revision dates	**v03 August 2026**
Policy revision frequency	**Every Two Years**
Policy review due date	**July 2028**

Target Audience: All students, Faculty Members, Researchers, Administrative Staff, IT Staff, and External Partners, and Guest Scholars.

Effective Date: September 1, 2026

1. Purpose & Scope

This policy establishes guidelines for the ethical, secure, transparent and compliant deployment of Artificial Intelligence (AI) technologies across academic instruction, research, administrative operations, and student learning environments at STI Myanmar University. It aims to foster innovation while protecting academic integrity, data privacy, institutional governance, and human oversight.

Scope

This policy applies to:

- All full-time and adjunct faculty, administrative and support staff, undergraduate/graduate students, student researchers, and guest scholars.
- All hardware, cloud infrastructure, local compute clusters, software licenses, and API services owned, leased, or managed by the institution.
- Any AI system, generative model, automated pipeline, or autonomous agent utilized for university work, coursework, research projects, or administrative functions—regardless of whether accessed via institutional or personal credentials/devices.

2. Core Principles

1. **Academic Integrity & Transparency:** AI must be used as a tool to enhance learning and research, not to bypass authentic intellectual effort. Disclosure of material AI assistance is required where specified by applicable academic, research, or administrative requirements.
2. **Data Stewardship & Privacy:** Student records, financial data, health/medical information, and proprietary institutional research must be protected against unauthorized disclosure or training set exposure.
3. **Human-in-the Loop and Accountability**: AI systems may assist in administrative and academic processes, but critical decisions (academic grading, admissions, hiring, research validation) must retain ultimate human oversight and accountability.
4. **Equity & Fairness**: AI implementations must actively guard against algorithmic bias, ensuring equitable access and fair treatment for all students, staff, and faculty.
5. **Operational Resilience:** Maintain locally hosted, resilient AI capabilities alongside commercial cloud tools to ensure continuity during vendor disruptions or network outages.

3. Classification of AI Projects & Risk Levels

To ensure proportional governance, all university AI activities are categorized into four distinct risk tiers:

Tier	Risk Level	Description & Examples	Mandatory Approval & Controls
Tier 0	**Permitted/Minimal Risk**	Standard spelling/grammar correction tools, approved learning tools, routine search/summarization without sensitive data.	Standard Acceptable Use Policy compliance; no specialized review needed.
Tier 1	**Low Risk**	Non-sensitive administrative workflows, public dataset processing, classroom demonstration of generative models using vetted institutional tools.	Faculty/Department Chair notification;adherence to data privacy guidelines.
Tier 2	**Moderate Risk**	Processing restricted student/institutional data, customized fine-tuning of open-weight models, integration with institutional databases/APIs.	IT Security and/or Data Privacy review; Ressearch Ethics/IRB review where applicable.
Tier 3	**High/Critical Risk**	Autonomous agents, high-risk research (e.g., cyber capabilities, biological modeling), high-performance cluster fine-tuning, automated scoring or admissions tools.	AI Governance Committee approval

4. Academic & Pedagogy Guidelines (Student & Faculty Perspectives)

A. Coursework & Student Guidelines

- **Syllabus Explicit Rules:** Course instructors must explicitly state the permissible scope of AI tool usage in their course syllabus for each assignment type.
- **Disclosure & Citation:** If generative AI is used to brainstorm, draft, outline, or debug code, students must acknowledge the tool (e.g., tool name, version, prompt, date) and include an **AI Declaration Form/Statement** with their submission.
- **Unpermitted Generative AI Use:** Submitting AI-generated text, code, or media as original work without explicit instructor approval or proper citation may constitute constitutes academic dishonesty, plagiarism, or another academic integrity violation, subject to the University's applicable procedures.
- **Assessment Validation:** Instructors reserve the right to verify student work through oral defenses, in-class viva assessments, or monitored written evaluations.

B. Teaching & Faculty Guidelines

- **Pedagogical Integration:** Faculty are encouraged to integrate AI literacy into learning outcomes while designing assessments that evaluate critical thinking, analysis, and problem-solving.
- **Assessment Integrity:** Commercial "AI Detectors" must **not** be used as the sole basis for penalizing a student, due to known rates of false positives and bias against non-native English speakers. Allegations of unauthorized AI use require holistic evaluation and dialogue with the student.
- **Automated Grading Restriction:** AI tools may assist in generating feedback or initial rubric evaluations, but final grades must always be reviewed and finalized by a human instructor.

5. Security, Infrastructure & Data Governance

A. Environment Isolation (Air-Gapping) for Autonomous Agents

- **Mandatory Sandbox Isolation:** Any research or operational project involving autonomous AI agents, multi-agent frameworks, or automated code execution must operate within appropriately isolated virtual environments proportionate to the assessed risk.
- **Network Restrictions:** High-capability AI agents under testing must access to internal university databases or external internet protocols only where explicitly authorized through documented IT Security approval and appropriate compensating controls.

B. Machine Identity & Access Management (IAM)

- **Ephemeral Credentials:** Persistent, non-expiring API tokens and cloud root keys are strictly prohibited for automated AI scripts and agents.
- **Velocity & Usage Limits:** Automated scripts and AI agents must operate under rate-limited service accounts configured to lock automatically upon detecting unusual activity or traffic spikes.

C. Data Protection & Model Vetting

- **Prohibited Uploads:** Personally Identifiable Information (PII), student grades, financial records, medical data, and confidential research IP must never be entered into public or unauthorized AI services.
- **Model Scanning:** All open-weight models downloaded from external model hubs (e.g., Hugging Face, GitHub) must undergo appropriate security, provenance, dependency, integrity, vulnerability, and license assessment before deployment.

6. Business Operations, HR & Administrative Uses

- **Vendor Due Diligence:** Administrative departments adopting enterprise software with integrated AI features must ensure vendor agreements explicitly state that institutional data will **not** be used to train vendor foundational models.
- **Employment & Admissions Decisions:** AI tools may not be used to autonomously screen job applicants or evaluate university admissions. AI may provide controlled decision-

support recommendations subject to qualified human review and appropriate fairness safeguards.

- **Intellectual Property (IP):** Research data and intellectual property developed using university resources remain subject to STI Myanmar University's core IP policies. Staff and faculty must ensure commercial AI service terms must appropriately address ownership, licensing, confidentiality, permitted use, retention, and secondary use of University intellectual property.

7. Continuity & Backup Infrastructure

- **Self-Hosted Redundancy:** To safeguard operational continuity during commercial API outages, policy shifts, or service locks, Central IT may maintin a self-hosted or institutionally controlled AI models where determined necessary based on operational requirements, risk, and business continuity needs.
- **Local Compute Allocation:** Compute resources for local open-weight models will be managed by Central IT and prioritized according to risk tier and academic necessity.

8. Roles & Responsibilities

- **Students:** Responsible for adhering to syllabus-specific AI guidelines, properly citing AI tool usage, and maintaining academic honesty.

- **Faculty & Instructors:** Responsible for defining clear AI expectations in courses, designing robust assessments, evaluating potential academic dishonesty fairly, and providing AI literacy guidance.

- **Principal Investigators (PIs):** Responsible for declaring AI usage in grant applications, securing Tier 2/3 approvals, and enforcing sandbox rules within research labs.

- **Chief Information Security Officer (CISO) & Central IT:** Responsible for network monitoring, infrastructure maintenance, model security scanning, credential policy enforcement, and managing self-hosted AI backups.

- **AI Governance Committee:** A joint body comprising faculty representatives, legal counsel, ethics officers, student representatives, and IT personnel responsible for review of Tier 3 proposals and significant Tier 2 proposals as determined by the AI Governance Committee, policy updates, and oversight of institutional AI practices.

9. Non-Compliance & Policy Violations

Violations of this policy—including unauthorized exposure of sensitive student data to public LLMs, unauthorized network bridging of sandboxed models, unauthorized or undisclosed AI usge in coursework where disclosure is reequired by the applicable or assessment rules, or unapproved AI usage in high-risk administrative workflows—may result in:

- Academic penalties (ranging from assignment resubmission to module failure) under the Academic Integrity Policy.
- Suspension of university computing, API, and cluster access privileges.
- Administrative or disciplinary review under institutional staff/faculty ethics protocols.