The Nine AI Governance Domains for Higher Education

A Framework for Responsible AI Adoption in Higher Education

Joe Sabado

CampusAIExchange.com

March 2026

Version 1.0

Table of Contents

Executive Summary

Artificial intelligence is reshaping every dimension of higher education: teaching, learning, research, student services, administration, and campus operations. Yet governance has consistently struggled to keep pace with the speed of adoption. Most institutions have addressed AI policy only in the teaching and academic integrity space, leaving significant governance gaps across research, student services, data security, procurement, employee competency, and institutional oversight. The result is a landscape where AI tools are widely used but unevenly governed, creating institutional risk that grows with every new deployment.

This document presents The Nine AI Governance Domains for Higher Education, a comprehensive policy architecture designed to help institutions govern AI responsibly, equitably, and effectively across their entire operational scope. The framework is the product of extensive research into existing higher education AI policies, governance frameworks, regulatory requirements, and institutional practice, refined through iterative analysis and expert review.

The framework organizes higher education AI governance into nine distinct domains, grouped into three super categories:

Domains 1 through 4: Academic Core and Student Outcomes. Teaching, Learning, and Assessment; Research and Scholarship; Institutional Algorithmic Decision-Making and Student Services; and Student AI Literacy, Career Readiness, and Workforce Preparation.

Domains 5 through 7: Infrastructure, Risk, and Vendors. Data, Security, Privacy, and AI-Enabled Systems; Fairness, Transparency, Accountability, and Algorithmic Oversight; and Procurement, Vendors, and Legal.

Domains 8 and 9: People and Governance. AI Literacy and Role-Based Competency (Employees); and Governance, Oversight, and Continuous Review.

Each domain is organized using a five-part policy instrument taxonomy: Policies (binding, with enforcement), Standards (specific requirements and benchmarks), Guidelines (advisory, recommended practices), Enablement Mechanisms (innovation support, sandboxes, incentives), and Governance Mechanisms (structural processes, bodies, and review cycles). Each domain also specifies delegation of authority, defining which elements require full shared governance approval and which can be updated on faster cycles by delegated bodies.

The framework includes a cross-domain coordination map that explicitly assigns ownership for shared governance concerns such as shadow AI, algorithmic bias, data security in vendor relationships, agentic AI, application development, campus operations, and innovation. An institutional AI risk-tiering standard (assistive, operational, and consequential) and an institutional AI system inventory standard provide the mechanisms that calibrate governance intensity to actual risk.

A recommended implementation sequence offers a phased approach: Phase 1 establishes a minimum viable governance stack (Domains 1, 3, 5, 7, and 9), and Phase 2 extends to the full framework once governance infrastructure is operational. The domain applicability matrix differentiates recommendations by institution type, covering community colleges, regional comprehensive universities, R1 research universities, minority-serving institutions, online and distance education institutions, and health sciences institutions and academic medical centers.

This framework is designed to be adopted in phases, adapted to institutional context, and sustained over time. It is not a compliance checklist. It is an operating design for responsible AI governance in higher education.

About This Framework

This framework was developed through scholarly research, direct participation in AI governance at the campus and university system levels, leadership within a national higher education technology community, and practitioner engagement across community college systems, R1 research universities, private universities, a health sciences institution, an accreditation agency, and industry associations. It is further informed by a comprehensive review of existing governance frameworks, academic literature, policy documents, regulatory guidance, and institutional practice across a wide range of institutions.

Existing frameworks and institutional policies tend to address specific dimensions of AI governance, most commonly teaching and academic integrity, with varying attention to ethics, data privacy, or procurement. No single framework available today covers the full scope of institutional AI governance across all nine domains identified in this document. This framework was designed to close that gap by providing a comprehensive, integrated architecture that institutions can adopt in phases and adapt to their own context and mission.

The nine-domain structure, policy instrument taxonomy, cross-domain coordination model, and risk-tiering architecture are original contributions designed to address structural gaps identified through that work.

Framework Architecture

The Nine Domains

The framework organizes higher education AI governance into nine domains, each representing a distinct area of institutional responsibility. The domains are grouped into three supercategories that reflect how universities are organized and how governance responsibilities are distributed.

Supercategory	Domain	Focus
Academic Core and Student Outcomes	1. Teaching, Learning, and Assessment	Course-level instructional practice, academic integrity, assessment
	2. Research and Scholarship	AI in research, IP, disclosure, funder compliance
	3. Institutional Algorithmic Decision-Making and Student Services	Consequential AI decisions affecting people
	4. Student AI Literacy, Career Readiness, and Workforce Preparation	Program-level student outcomes, workforce readiness
Infrastructure, Risk, and Vendors	5. Data, Security, Privacy, and AI-Enabled Systems	Data governance, shadow AI, app development, campus operations
	6. Fairness, Transparency, Accountability, and Algorithmic Oversight	Impact assessments, bias audits, ethics, accountability
	7. Procurement, Vendors, and Legal	Vendor risk, contracts, compliance, rapid pilots
People and Governance	8. AI Literacy and Role-Based Competency (Employees)	Employee acceptable use, competency, professional development
	9. Governance, Oversight, and Continuous Review	Governance body, risk tiering, inventory, agentic AI, review

Policy Instrument Taxonomy

Each domain organizes its elements into five functional categories that serve different purposes and move at different speeds within institutional governance:

Policies are binding requirements with enforcement mechanisms. They require full shared governance approval and are designed to be principles-based and technology-agnostic so they survive multiple generations of AI tools.

Standards define specific, measurable requirements and benchmarks. They require governance body approval, often with faculty senate consultation, and are updated on an annual or biannual cycle.

Guidelines are advisory best practices and recommended approaches. They are updatable by designated committees or operational leaders without full shared governance approval, enabling rapid iteration as technology evolves.

Enablement Mechanisms support innovation, experimentation, and adoption. They include sandboxes, grants, approved tool lists, training, and peer learning communities. They are administered by operational leaders and are the framework's answer to the critique that governance frameworks are too defensive.

Governance Mechanisms are structural processes, bodies, and review cycles that ensure policies, standards, and guidelines are implemented, enforced, and kept current. They include governance bodies, review cycles, audit processes, and accountability structures.

This taxonomy allows institutions to move at different speeds: policies change slowly through deliberative governance, while guidelines and enablement mechanisms adapt quickly to a rapidly evolving technology landscape.

Domains 1 through 4: Academic Core and Student Outcomes

Domain 1: Teaching, Learning, and Assessment

Scope: This domain governs what happens inside courses: instructional practice, course design, assessment, and classroom AI use. It covers faculty pedagogy, academic integrity, and the student experience within individual courses. It does not govern institution-level or program-level student AI literacy outcomes, which belong to Domain 4. The university library is a named partner in this domain given its role in AI literacy instruction and the evolution of information literacy in AI-prevalent environments.

Policies

AI academic integrity policy (principles-based, technology-agnostic). AI acceptable use policy for instructional contexts. AI-assisted grading and feedback policy.

Standards

AI disclosure and citation standards for student work. Course-level AI use expectations framework (Green/Yellow/Red tiers). Course AI statement requirement (each course syllabus must include an explicit AI use expectations statement aligned with the institutional Green/Yellow/Red framework). Authentic assessment design standards for AI-prevalent environments. AI-assisted learning analytics data use standards. Accessibility and Universal Design for Learning standard for AI tools required in courses (any AI tool required for coursework must meet institutional accessibility requirements).

Guidelines

Faculty guidance on teaching with AI. AI-enhanced pedagogy and course design guidance. Equitable assessment design guidance (addressing differential student access to AI tools). Guidance on AI-generated or AI-assisted course materials.

Enablement Mechanisms

Faculty innovation grants and course redesign incentives for AI-enhanced pedagogy. Teaching-focused AI sandbox access for faculty experimentation. Peer learning communities and communities of practice for AI in teaching. Recognition pathways for faculty AI teaching innovation. Library partnership for AI literacy integration into course-level information literacy instruction.

Governance Mechanisms

Faculty development pathway for AI in teaching. Annual review cycle for course-level AI expectations. Faculty senate or academic council role in AI teaching policy (limited to Policies and Standards; Guidelines updatable by designated committee on a faster cycle). Integration with accreditation and learning outcomes assessment.

Delegation of Authority

Policies require full shared governance approval. Standards require governance body approval with faculty senate consultation. Guidelines are updatable by the AI governance body or

designated academic committee without full senate vote. Enablement Mechanisms are administered by the provost's office or center for teaching and learning.

Cross-Domain Coordination

AI-assisted learning analytics encountered by faculty in the LMS/LTI context are governed by Domain 5 data governance standards and must comply with FERPA and ADA requirements. This cross-reference is surfaced here because faculty encounter these analytics in their teaching environment, not in a data governance document.

Domain 2: Research and Scholarship

Scope: The university library is a named stakeholder in this domain as a steward of research discovery tools and AI-enabled academic databases, with specific attention to licensing terms and data practices for AI-powered research platforms.

Policies

AI in research acceptable use policy. IP ownership policy for AI-assisted scholarship and invention. AI disclosure policy for publications and grant applications. Prohibition on AI-assisted peer review of confidential grant applications and manuscripts (aligned with NIH, NSF, and other funder requirements).

Standards

AI research integrity and disclosure standards. Data provenance standards for AI-assisted analysis. AI use standards for systematic reviews and meta-analyses. Confidentiality standards for pre-publication research in AI environments. Compliance standards for funder-specific AI restrictions.

Guidelines

Guidance on using proprietary AI tools with confidential research data. AI in human subjects research guidance (IRB jurisdiction). Grant agency AI compliance guidance (NSF, NIH, DOE requirements). Guidance on AI authorship and attribution in scholarly publishing (aligned with disciplinary norms including COPE guidelines, ICMJE recommendations, and major publisher AI authorship policies, so that institutional expectations are consistent with what faculty encounter in their professional communities). Guidance on AI-enabled research discovery tools and academic database licensing (developed in partnership with the university library, addressing data practices, training data provisions, and copyright implications of AI-powered research platforms).

Enablement Mechanisms

Research computing access and AI infrastructure provisioning. Institutional AI platforms and sandboxes for research use. Seed funding or internal grants for AI-augmented research. Support for interdisciplinary AI research collaboration. Library-curated guidance on AI-enabled research tools and discovery platforms.

Governance Mechanisms

Research office AI review process. IRB AI-specific review protocols. Technology transfer and licensing review for AI-assisted inventions. Cross-institutional research data sharing agreements for AI contexts.

Delegation of Authority

Policies require shared governance and research office approval. Standards are set by the research office in consultation with the AI governance body. Guidelines are updatable by the research office. Enablement Mechanisms are administered by the VP for Research or equivalent.

Domain 3: Institutional Algorithmic Decision-Making and Student Services

Scope: This domain governs the use of AI and algorithmic systems wherever they make or inform consequential decisions about people, including students, prospective students, donors, alumni, employees, and community members. Student services is the largest and most regulated area within this domain, but the governance principles apply equally to advancement and alumni relations (predictive analytics, donor capacity modeling, wealth screening), HR analytics, and any other institutional function using AI to make decisions that affect individuals. Consequential decisions include, but are not limited to, those affecting admission, financial aid level, academic standing, retention interventions, employment, housing, and disciplinary outcomes. This domain also governs AI used in external communications, recruitment marketing, and institutional brand representation. AI used in student-led co-curricular contexts that affects other students is subject to the same transparency and fairness principles.

Policies

AI in student services acceptable use policy. Algorithmic decision-making transparency and disclosure policy. Student rights and appeals policy for AI-influenced decisions. Right to human alternative policy (any individual subject to an AI-assisted consequential decision may request human review or a human interaction pathway).

Standards

Bias review standards for AI systems affecting admissions, financial aid, retention, and academic standing. FERPA compliance standards for AI-assisted student analytics. ADA and accessibility standards for AI-enabled student services. Notification standards (when and how individuals are told AI is involved in decisions affecting them, including the availability of human alternatives). Bias review standards for AI in advancement, fundraising, and donor analytics. AI in external communications and recruitment marketing standards (disclosure when AI-generated content is used in public-facing institutional communications, human review of AI-generated recruitment and marketing materials before publication, prohibitions on fabricated representations of campus diversity, student experience, or institutional facilities in AI-generated imagery, accuracy verification and hallucination mitigation requirements for AI-powered public-facing chatbots with escalation to human staff, risk classification of public-facing AI communications under the institutional risk-tiering standard).

Guidelines

Guidance on AI-assisted advising and early alert systems. Guidance on predictive analytics in enrollment management. Guidance on AI chatbots and virtual assistants in student-facing roles. Guidance on AI in advancement and alumni relations (donor privacy, prospect research ethics, wealth screening transparency). Guidance on AI in institutional marketing and recruitment communications. Guidance on AI use in student-led co-curricular contexts.

Enablement Mechanisms

Pilot approval process for new AI-assisted student service tools. Data-sharing agreements that enable responsible analytics while protecting individual rights. Cross-functional collaboration between student affairs, advancement, and institutional research on responsible AI use.

Governance Mechanisms

Predictive analytics ethics and bias review process. Student appeals process for AI-influenced decisions. Student-facing communication templates for disclosures and appeals (developed and

maintained as concrete artifacts). Title VI/IX and Title VII compliance review for AI-assisted decisions. Periodic audit cycle for AI systems making or informing consequential decisions about any population. Donor and alumni data privacy review process.

Delegation of Authority

Policies require institutional leadership and shared governance approval. Standards are set by the AI governance body in consultation with affected divisions (student affairs, advancement, HR, marketing and communications). Guidelines are updatable by divisional leadership. Enablement Mechanisms are administered by the relevant division with AI governance body oversight.

Cross-Domain Coordination

Algorithmic bias review coordinates with Domain 6, which owns the institutional algorithmic impact assessment standard. Data privacy dimensions coordinate with Domain 5. Vendor-supplied AI tools are governed through Domain 7 procurement processes. AI systems classified as consequential under the institutional risk-tiering standard (Domain 9) trigger the full governance requirements in this domain. AI in external communications connects to Domain 6 (transparency) and Domain 7 (marketing technology vendor procurement).

Domain 4: Student AI Literacy, Career Readiness, and Workforce Preparation

Scope: This domain governs institution-level and program-level student outcomes related to AI literacy, employability, and career readiness. It does not govern course-level instructional practice or classroom AI use, which belong to Domain 1. The bright line is that Domain 1 governs what happens inside individual courses; Domain 4 governs what programs and institutions do to ensure students graduate with AI-relevant competencies. The university library is a named contributor, building on its existing information literacy mission.

Policies

AI literacy requirements policy (institutional or programmatic level).

Standards

AI literacy learning outcomes framework (what students should know and be able to do, aligned with recognized external frameworks such as foundational generative AI literacy, data literacy, and human-AI collaboration skills to ensure portability and employer recognition). AI competency integration standards for career and workforce programs. Industry-aligned AI skills benchmarks for applied and technical programs.

Guidelines

Guidance on AI in career and workforce curricula. Guidance on experiential learning with AI tools (internships, capstones, co-ops). Guidance on industry partnerships for AI skills alignment.

Enablement Mechanisms

Student-facing AI labs and experimentation spaces. Partnerships with employers for AI skills exposure and applied projects. Curricular rapid-update pathways for AI content. Library-supported AI literacy programming and resources.

Governance Mechanisms

AI literacy credential or certificate framework. Employer advisory board input on AI workforce readiness. Program review cycle incorporating AI literacy expectations. Alignment with accreditation standards for workforce programs.

Delegation of Authority

Policies require shared governance approval. Standards are set by academic programs with AI governance body consultation. Guidelines are updatable by program faculty. Enablement Mechanisms are administered by academic affairs and career services.

Domains 5 through 7: Infrastructure, Risk, and Vendors

Domain 5: Data, Security, Privacy, and AI-Enabled Systems

Scope: This domain governs institutional data practices, security posture, privacy compliance, and the technical implementation of AI-enabled systems. It includes two named subdomains: Application Development and AI-Enabled Systems, and Campus Operations and Operational AI. AI use by student organizations, residential life, and co-curricular programs using institutional data or infrastructure is within scope of this domain's shadow AI risk management policy.

Policies

AI data governance policy. Shadow AI risk management policy (scope includes AI use by student organizations, residential life, and co-curricular programs operating on institutional data or infrastructure). AI records retention policy.

Standards

AI-specific data classification standards. AI vendor data use agreement requirements. Data minimization and retention standards for AI applications. Cross-border data transfer controls for AI. Audit trail and logging standards for AI systems processing institutional data.

Guidelines

Guidance on institutional data in commercial AI tools. Guidance on de-identification and anonymization for AI training data. Guidance on AI-related incident reporting and breach notification.

Subdomain: Application Development and AI-Enabled Systems

This subdomain governs how AI-enabled systems are built, tested, deployed, and maintained within the institutional technology environment. It applies to custom-built institutional applications, integrations, and any system where AI capabilities are developed or embedded by institutional staff or contractors.

Standards: AI-assisted development tool standards (acceptable use and data exposure rules for tools such as Copilot, Claude Code, and AI pair programming environments). Code review and security standards for AI-generated code. Model selection and deployment standards for custom AI implementations (including open-source and locally hosted models). API governance and integration standards for AI services. Testing and validation standards for AI-enabled applications (including bias testing, edge case handling, and regression testing for AI components). Low-code/no-code AI platform governance standards. Logging and audit trail requirements for AI-enabled systems. Agentic system development and deployment standards (human-in-the-loop requirements, action boundaries, escalation triggers, agent-to-agent interaction controls; aligned with the agentic AI governance standard in Domain 9).

Guidelines: Guidance on responsible use of AI coding assistants in institutional development work. Guidance on AI model lifecycle management (versioning, retraining, deprecation). Guidance on documentation standards for AI-enabled systems (including decision logic, training data provenance, and known limitations).

Subdomain: Campus Operations and Operational AI

This subdomain governs AI and algorithmic systems deployed in campus facilities, physical infrastructure, and operational environments.

Standards: Smart building AI standards (HVAC optimization, energy management, space utilization analytics). AI-enabled security and surveillance standards (including camera analytics, access control, and behavioral monitoring, with explicit privacy and civil liberties protections). Operational predictive maintenance standards. Environmental and sustainability optimization standards for AI systems. Data retention and access standards for operational AI systems.

Guidelines: Guidance on transparency and notification for AI systems operating in shared campus environments. Guidance on balancing operational efficiency with privacy in smart campus deployments. Guidance on community input and review for AI-enabled surveillance and security systems.

Cross-domain trigger: Any campus operations AI system that affects individual rights, fairness, or human impact triggers the algorithmic impact assessment and accountability requirements in Domain 6. Community consultation is required before deployment of AI-enabled surveillance or security systems.

Enablement Mechanisms

Institutionally provisioned AI platforms that meet data governance requirements. Approved AI tool list published, maintained, and promoted as a campus-facing resource organized by data classification level (this must be a living, visible, easily searchable resource). Streamlined data access request processes for legitimate AI use cases. Development sandboxes and staging environments for AI-enabled application testing. Access to institutional AI infrastructure (compute, model hosting, API endpoints) for authorized development teams.

Governance Mechanisms

AI security risk assessment process. Shadow AI discovery and remediation process (discovery function owned by this domain; vendor remediation coordinated with Domain 7; reporting to Domain 9). AI records retention schedule. Data governance committee AI review function. Vendor data use agreement review and renewal cycle. AI-enabled application review and approval process. Institutional AI system inventory maintenance (technical implementation and ongoing updates owned by this domain; inventory standard defined by Domain 9; inventory updated as a mandatory step in deployment approval).

Delegation of Authority

Policies require institutional leadership approval. Standards are set by IT security and data governance in consultation with the AI governance body. Application development subdomain standards are set by IT leadership with AI governance body review. Campus operations subdomain standards are set by IT and facilities leadership with AI governance body review and Domain 6 consultation for systems affecting individual rights. Guidelines are updatable by IT security, the privacy office, IT development leadership, and facilities leadership. Enablement Mechanisms are administered by IT.

Cross-Domain Coordination

Shadow AI discovery is owned by this domain; vendor remediation coordinated with Domain 7; escalation flows to Domain 9. Data requirements for AI vendor contracts are defined here and enforced through Domain 7. AI-assisted coding tools as employee competency questions coordinate with Domain 8. Agentic system development practices are governed here; the agentic AI governance standard (policy level) is owned by Domain 9. AI-enabled applications

making consequential decisions trigger Domain 6 algorithmic impact assessment and Domain 3 notification and appeals requirements. Campus operations AI affecting individual rights triggers Domain 6 review. The institutional AI system inventory is maintained here per Domain 9's standard. AI-assisted learning analytics in LMS/LTI environments are governed here, with cross-reference surfaced in Domain 1.

Domain 6: Fairness, Transparency, Accountability, and Algorithmic Oversight

Policies

Human oversight requirements for AI-assisted consequential decisions. AI transparency disclosure policy (when AI must be disclosed to affected individuals).

Standards

Algorithmic impact assessment standard (required before deployment of consequential AI systems; institutions may align with the NIST AI Risk Management Framework Map/Measure/Manage/Govern structure as a recognized methodology). Bias audit requirements and schedules for consequential AI systems. Explainability standards for AI-assisted decisions.

Guidelines

AI ethics principles (institutional values statement). Guidance on equitable AI deployment across diverse student and employee populations. Guidance on community engagement and stakeholder input in AI deployment decisions.

Enablement Mechanisms

Algorithmic impact assessment templates and support resources. Equity-centered design guidance for AI deployments. Community feedback channels for AI system experiences.

Governance Mechanisms

Equity impact review process for AI deployments. Appeals and redress process for individuals affected by AI-assisted decisions. Accountability assignment framework (who is responsible when AI-assisted decisions cause harm). Periodic bias audit and impact assessment review cycle.

Delegation of Authority

Policies require institutional leadership and shared governance approval. Standards are set by the AI governance body. Guidelines are updatable by the AI governance body or designated ethics committee. Enablement Mechanisms are administered by the AI governance body with support from institutional equity and compliance offices.

Cross-Domain Coordination

This domain owns the institutional algorithmic impact assessment standard and bias audit methodology. Domain 3 applies these standards to student services, institutional analytics, and public-facing AI communications. Domain 5 triggers these for AI-enabled applications and campus operations AI affecting individual rights. Domain 7 incorporates them into vendor evaluation. Domain 8 incorporates fairness considerations into employee-facing AI.

Domain 7: Procurement, Vendors, and Legal

Scope: The university library is a named procurement stakeholder for AI-enabled academic databases and discovery platforms, where licensing terms increasingly include AI training data provisions that require governance attention.

Policies

AI procurement policy. Open-source AI model use policy. IP provisions for AI-assisted institutional work product.

Standards

AI vendor risk assessment standard. AI contract requirements checklist (training data provenance, model behavior, data use restrictions, indemnification, liability, audit rights; any vendor product classified as consequential under the institutional risk-tiering standard must provide the vendor's own algorithmic impact assessment and bias documentation as a condition of contract). Acceptable use restrictions in vendor terms. State and federal AI legislation compliance standards (CCPA/CPRA ADMT, state AI bills, sector-specific regulations). AI-enabled academic database and discovery platform licensing standards (developed in consultation with the university library).

Guidelines

Guidance on evaluating AI vendor claims and capabilities. Guidance on contract negotiation for AI-specific provisions. Guidance on managing AI vendor relationships over time (model updates, data retention, contract termination).

Enablement Mechanisms

Rapid-cycle pilot approval process for low-risk AI tools (distinct from full procurement review, with defined risk thresholds and time-limited approvals). Pre-approved AI tool list maintained and updated regularly. Streamlined procurement pathway for tools that meet established data governance and security standards.

Governance Mechanisms

Cross-functional AI procurement review team (legal, IT security, privacy, academic governance, with library representation for academic database acquisitions). AI compliance register. Shadow AI inventory and risk rating process (vendor remediation function owned by this domain; discovery coordinated with Domain 5). Vendor contract renewal and audit cycle. Mandatory AI system inventory update as a step in the procurement approval process.

Delegation of Authority

Policies require institutional leadership approval with legal counsel review. Standards are set by procurement and legal in consultation with the AI governance body. Guidelines are updatable by procurement and legal. Enablement Mechanisms are administered by procurement with AI governance body oversight for risk threshold definitions.

Cross-Domain Coordination

Shadow AI vendor remediation is owned by this domain; discovery coordinated with Domain 5. Data governance requirements in vendor contracts are defined by Domain 5 and enforced here. Algorithmic impact assessment requirements for vendor-supplied AI are defined by Domain 6 and applied here during procurement review. High-risk vendors must supply their own impact

assessments and bias documentation. Marketing technology vendors with AI capabilities are governed here, with Domain 3 providing the standards.

Domains 8 and 9: People and Governance

Domain 8: AI Literacy and Role-Based Competency (Employees)

Policies

Employee AI acceptable use policy. AI in performance management policy.

Standards

Role-based AI competency framework (defined expectations by job family and level). AI professional development requirements (minimum training expectations by role). AI competency assessment and credentialing standards.

Guidelines

Guidance on AI-augmented work practices by functional area. Guidance on workforce transition planning and reskilling. Guidance on AI use in hiring, evaluation, and promotion processes.

Enablement Mechanisms

Employee-facing AI sandbox for experimentation and skill building. AI tool access provisioned by role with appropriate training. Peer learning communities and communities of practice by functional area. Dedicated time allocation for AI skill development.

Governance Mechanisms

Integration of AI literacy into new employee onboarding (role-specific expectations defined at the point of hire, not deferred to later professional development). AI professional development delivery and tracking infrastructure. Competency framework review and update cycle. Connection to institutional HR classification and compensation systems.

Delegation of Authority

Policies require institutional leadership and HR approval. Standards are set by HR in consultation with the AI governance body. Guidelines are updatable by HR and divisional leadership. Enablement Mechanisms are administered by HR and IT in partnership.

Domain 9: Governance, Oversight, and Continuous Review

Policies

AI governance charter (authority, membership, scope, relationship to shared governance). AI incident response policy.

Standards

Agentic AI governance standard (autonomous systems, agent-to-agent interactions, human-in-the-loop requirements). AI risk register standards. Annual AI policy review standards. Institutional AI risk-tiering standard (three-tier classification: assistive/low-risk AI requiring compliance with acceptable use policies and approved tool lists; operational/moderate-risk AI requiring data governance review and departmental approval; consequential/high-risk AI requiring full algorithmic impact assessment, bias audit, human oversight, notification, and appeals). Institutional AI system inventory standard (comprehensive catalog of all approved and deployed AI systems capturing purpose, owner, vendor or model, data categories, affected populations, decision criticality, risk tier, human oversight point, audit schedule, and retirement owner; technical implementation delegated to Domain 5; inventory entry triggered during procurement approval in Domain 7 and deployment approval in Domain 5). Governance evidence package standard for consequential AI systems (requiring maintenance of algorithmic impact assessments, exception approvals, validation and testing results, bias audit results, review dates, responsible officials, and incident history).

Risk-Tiering Examples by Domain

Assistive/low-risk: AI writing assistants used for drafting and editing (Domain 1). AI-assisted literature search tools (Domain 2). AI chatbots providing general campus information with no decision authority (Domain 3). AI-powered career exploration tools (Domain 4). AI-assisted code completion in development environments with no access to production data (Domain 5). AI grammar and style tools used by procurement staff (Domain 8).

Operational/moderate-risk: AI-assisted grading tools providing feedback on student work (Domain 1). AI tools analyzing research datasets containing de-identified data (Domain 2). AI-powered donor prospect research tools (Domain 3). AI-generated recruitment marketing content with human review before publication (Domain 3). AI-assisted scheduling and space optimization (Domain 5 campus operations). AI vendor evaluation scoring tools (Domain 7). AI-assisted resume screening for staff hiring (Domain 8).

Consequential/high-risk: AI systems informing student academic standing decisions (Domain 1/Domain 3). AI tools processing confidential pre-publication research or clinical trial data (Domain 2). Predictive analytics determining financial aid eligibility or retention interventions (Domain 3). AI-powered public-facing admissions chatbots providing policy guidance without human oversight (Domain 3). AI-enabled surveillance and security systems with behavioral monitoring (Domain 5 campus operations). AI systems making or recommending employment decisions (Domain 8).

Guidelines

Guidance on AI governance body composition and operation. Guidance on elevating emerging AI risks to institutional leadership. Guidance on board education and reporting on AI governance. Guidance on applying the risk-tiering standard across institutional contexts.

Enablement Mechanisms

AI sandbox and experimentation environment (institutionally provisioned, with defined data governance and risk parameters). Emerging technology horizon scanning process. Innovation intake process (mechanism for faculty, staff, and students to propose new AI use cases for governance review and approval).

Governance Mechanisms

Designated AI governance body with cross-functional membership and defined authority, including explicit student representation (student government or equivalent). AI risk register and review process. Annual AI policy review process. AI incident response plan. Shadow AI monitoring and remediation process (this domain owns the orchestration; discovery is delegated to Domain 5; vendor remediation is delegated to Domain 7). AI audit rights and accountability framework. Agentic AI escalation and review process. Mechanism for surfacing emerging tools and risks to governance body. Annual enablement adequacy assessment (evaluating whether institutional AI platforms, approved tool lists, sandbox environments, and training are meeting demand). Annual equity resourcing assessment (reporting to institutional leadership on whether bias audits, community engagement, appeals processes, and equity-related governance activities are adequately funded and staffed). AI financial sustainability and cost governance (enterprise license management and cost allocation, token and API consumption tracking and chargeback models, total cost of ownership analysis for institutional AI platforms, budget integration for enablement mechanisms, annual cost review as part of the governance body's report to institutional leadership).

Delegation of Authority

The AI governance charter is approved by institutional leadership (president, cabinet) with shared governance consultation. The governance body has delegated authority to update Standards and Guidelines across all domains on defined review cycles without requiring full shared governance approval for each change. Policies across all domains require shared governance approval. The governance body reports annually to institutional leadership and the board on AI governance posture, emerging risks, policy adequacy, enablement adequacy, equity resourcing, and AI financial sustainability.

Cross-Domain Coordination Map

The following map explicitly assigns ownership for governance concerns that span multiple domains. This is the mechanism that prevents cross-domain redundancy from becoming bureaucratic confusion.

Shadow AI

Domain 5 owns discovery and data risk assessment (including AI use by student organizations and co-curricular programs on institutional infrastructure). Domain 7 owns vendor remediation and contract enforcement. Domain 9 owns institutional risk escalation, reporting, and orchestration.

Algorithmic Bias

Domain 6 owns the institutional algorithmic impact assessment standard and bias audit methodology. Domain 3 applies these to student services, advancement, institutional analytics, and public-facing AI communications. Domain 5 triggers these for AI-enabled applications and campus operations AI affecting individual rights. Domain 7 applies them during AI vendor procurement review and requires high-risk vendors to supply their own impact assessments.

Data Security in Vendor Relationships

Domain 5 defines data governance requirements for AI systems. Domain 7 enforces those requirements through procurement contracts and vendor management. Domain 9 monitors compliance and escalates gaps.

AI Literacy

Domain 4 owns student-facing AI literacy as a curricular and workforce preparation function. Domain 8 owns employee-facing AI competency as an HR and professional development function. Domain 1 owns faculty-specific AI teaching competency. The university library contributes across Domains 1, 2, 4, and 7. Domain 9 ensures alignment across all three literacy domains.

Agentic AI

Domain 9 owns the agentic AI governance standard. Domain 5 addresses data and security dimensions and governs agentic system development through its application development subdomain. Domain 7 addresses agentic capabilities embedded in vendor products. Domain 3 addresses agentic systems making or informing decisions about individuals.

Application Development

Domain 5 owns the application development subdomain. Domain 7 governs vendor-supplied development platforms and AI coding tools. Domain 8 addresses AI-assisted coding tools as employee competency questions. Domain 6 provides the algorithmic impact assessment standard for consequential applications. Domain 3 provides notification and appeals requirements.

Campus Operations

Domain 5 owns the campus operations subdomain. Domain 7 governs procurement of smart campus vendors. Domain 6 is triggered when campus operations AI affects individual rights,

with community consultation required before deployment of surveillance and security systems. Domain 9 ensures inclusion in the institutional AI risk register and system inventory.

External Communications and Brand

Domain 3 owns standards and guidelines for AI in external communications, recruitment marketing, and institutional brand. Domain 6 provides the transparency and accountability framework. Domain 7 governs procurement of marketing technology vendors with AI capabilities. Domain 9 ensures classification under the risk-tiering standard.

University Library

The library is a named stakeholder across Domain 1 (AI literacy instruction), Domain 2 (research discovery tools, copyright and fair use expertise), Domain 4 (institutional AI literacy outcomes), and Domain 7 (procurement of AI-enabled academic databases). The library's cross-cutting role should be recognized in the AI governance body's membership or advisory structure.

Risk Tiering

Domain 9 owns the institutional AI risk-tiering standard. All domains apply it. Low-risk AI requires domain-specific acceptable use compliance. Moderate-risk AI requires data governance review (Domain 5) and departmental approval. Consequential/high-risk AI triggers the full governance stack: algorithmic impact assessment (Domain 6), bias audit (Domain 6), human oversight (Domain 6), notification and appeals (Domain 3), governance evidence package (Domain 9), high-risk vendor documentation (Domain 7), and system inventory inclusion (Domain 9, maintained by Domain 5).

AI System Inventory

Domain 9 defines the inventory standard. Domain 5 owns technical implementation and maintenance. All domains ensure their AI systems are registered. Inventory entry is triggered during procurement approval (Domain 7) and deployment approval (Domain 5). The inventory feeds the risk register and annual policy review in Domain 9.

AI Financial Sustainability

Domain 9 owns AI financial sustainability and cost governance, including enterprise license management, token and API consumption tracking, chargeback models, and total cost of ownership analysis. The annual cost review is part of the governance body's report to institutional leadership.

Innovation and Experimentation

Domain 9 owns the institutional AI sandbox and innovation intake process. Individual domains (1, 2, 4, 8) maintain domain-specific enablement mechanisms. Domain 7 provides the rapid-cycle pilot approval process. Domain 5 provides development sandboxes and staging environments.

Recommended Implementation Sequence

Phase 1: Minimum Viable Governance Stack

Domain 9 (Governance, Oversight, and Continuous Review) to establish the governance body, risk-tiering standard, and system inventory. Domain 5 (Data, Security, Privacy, and AI-Enabled Systems) as the most urgent risk domain. Domain 1 (Teaching, Learning, and Assessment) as the most visible and faculty-facing domain. Domain 3 (Institutional Algorithmic Decision-Making and Student Services) to address consequential AI decisions. Domain 7 (Procurement, Vendors, and Legal) to govern vendor relationships and new AI acquisitions.

Phase 2: Full Framework

Domain 2 (Research and Scholarship) once governance infrastructure is operational. Domain 4 (Student AI Literacy, Career Readiness, and Workforce Preparation) integrated into program review cycles. Domain 6 (Fairness, Transparency, Accountability, and Algorithmic Oversight) operationalized through impact assessments and bias audits. Domain 8 (AI Literacy and Role-Based Competency for Employees) integrated into HR and professional development systems.

Domain Applicability by Institution Type

Community Colleges

Priority domains are Domain 1, Domain 3, Domain 4 (especially prominent given the workforce mission), Domain 5 (with lighter application development provisions), Domain 7, and Domain 9. Domain 2 is minimal. Domain 8 is important but may be delivered through simpler structures given smaller staff size. Focus governance resources on student-facing AI in advising and enrollment, AI literacy integration into career programs, and FERPA compliance in vendor relationships. Capacity-building support is essential: shared services, system-level templates, consortial resources, and state-provided tools enable smaller institutions to operationalize this framework without requiring nine dedicated policy owners.

Regional Comprehensive Universities

All nine domains apply. Priority sequencing: begin with Domain 9 to establish oversight structure, then Domain 5 as the most urgent risk, then Domain 1, then Domain 3 and Domain 7. Domain 2 is lighter than R1 but present given graduate programming. Domain 4 applies across both liberal arts and professional programs.

R1 Research Universities

All nine domains at full depth. Domain 2 is co-equal in priority with Domain 1. Domain 5 requires the full application development subdomain given significant institutional development capacity. Governance structure must accommodate decentralized academic units while maintaining minimum standards. Dedicated CAIO or equivalent role, AI ethics board, and cross-functional AI review committee are recommended. Agentic AI governance provisions are essential given research computing infrastructure. The campus operations subdomain is highly relevant given large physical campuses and significant facilities operations.

Minority-Serving Institutions

All nine domains apply with particular emphasis on equity dimensions. Domain 3 carries heightened importance given the equity obligations of MSIs and the documented risks of algorithmic bias in admissions, financial aid, and retention systems. Domain 4 is critical for ensuring equitable access to AI skills and career readiness. Domain 6 should be established early in the governance sequence. Domain 8 should include explicit attention to equitable access to AI professional development. Capacity-building support through shared services, system-level templates, and consortial resources is essential.

Online and Distance Education Institutions

All nine domains apply with particular emphasis on Domain 1 (identity verification, proctoring, and instructional authenticity at scale), Domain 3 (AI in student services delivered entirely online, chatbots and virtual assistants as primary interaction points), Domain 5 (data security for fully digital learning environments, cross-border data considerations for geographically distributed students), and Domain 7 (vendor dependency given heavy reliance on EdTech platforms). Domain 4 must address AI readiness for students who may have limited in-person support.

Health Sciences Institutions and Academic Medical Centers

All nine domains at full depth with additional regulatory overlay. Domain 2 carries HIPAA, FDA, and clinical trial compliance requirements for AI-assisted research. Domain 3 extends to clinical AI systems affecting patient care decisions and clinical education placements. Domain 5 must address health data under HIPAA in addition to FERPA. Domain 7 must address FDA-regulated AI/ML medical devices and clinical decision support tools. The campus operations subdomain applies to AI in clinical and laboratory facilities.