UNIVERSITY INNOVATION ALLIANCE

AI Contract Decision Guide for Presidents & Chancellors & Provosts

Protecting Your Institution While Navigating AI Enterprise Offers

Purpose: This guide was designed to help you identify red flags and make informed decisions before signing long-term AI partnerships, particularly when evaluating enterprise AI platforms such as Google Gemini, OpenAI ChatGPT Enterprise, Microsoft Copilot, Anthropic Claude Enterprise, and emerging enterprise AI providers.

When to Use: Before any commitment involving student or institutional data, especially when facing pressure to sign quickly.

Time Required: 15 minutes for presidential review; 2-4 hours for full institutional assessment.

Note: We hope this guide will generate new questions and insights that you will contribute to help us evolve this shared resource and identify best practices for the broader field in support of non-UIA campuses, particularly those who are significantly under-resourced.

⚠️ **Critical Tool for Multi-Year Contract Decisions**

UNIVERSITY INNOVATION ALLIANCE

Executive Summary: What You Need to Know

The Reality:

Enterprise AI providers are aggressively marketing multi-year contracts to universities right now. Their sales teams are skilled at creating urgency around limited-time pricing and features. However, the AI landscape is changing monthly, and what seems like a good deal today could lock you into outdated technology or unfavorable terms tomorrow.

Key Risk: Most standard contracts give vendors permission to train their AI models on your institutional data, even if sales reps say otherwise verbally.

Four-Question Gut Check

Before reading further, answer these four questions:

1. **Data Control:** Can you confirm in writing that your institution retains full ownership of all data inputs AND outputs, with zero vendor rights to use them for training?
2. **Exit Strategy:** If you need to leave in 18 months because a better option emerges, can you export all your data and models without penalty?
3. **Compliance Verification:** Has your General Counsel confirmed FERPA compliance for student data, and do you have audit rights to verify ongoing compliance?
4. **Future Flexibility:** Can this contract accommodate future AI models without requiring us to renegotiate or replace the agreement?

If you cannot answer 'YES' with documentation to all four questions, DO NOT SIGN.

What Makes This Different Than Other Tech Contracts

AI contracts are fundamentally different from traditional software licensing:

- **Your data becomes training material:** Unlike traditional software where your data stays yours, AI systems can legally use your inputs to improve their models for everyone unless explicitly prohibited.
- **Students can't consent:** Student data protected under FERPA cannot be used for AI training, but many contracts don't clearly prohibit this.
- **Bias and fairness:** AI systems can perpetuate or amplify biases in ways that affect admissions, financial aid, or academic outcomes.
- **Rapid technology change:** Today's cutting-edge AI may be obsolete in 12 months, but you're signing 3–5-year contracts.
- **Unclear regulatory landscape:** AI regulations are evolving rapidly. What's legal today may be restricted tomorrow.

UNIVERSITY INNOVATION ALLIANCE

Quick Decision Framework: Stop, Caution, or Proceed

Use this framework to quickly assess where you stand. If you hit any STOP criteria, halt the process immediately.

🛑 STOP	Do not proceed if ANY of these are true:

- Contract allows vendor to use your data for AI training (even de-identified)
- No written FERPA compliance certification provided
- Data will be stored or processed outside the U.S. without clear legal protections
- No ability to delete data upon contract termination
- Vendor refuses to provide list of subprocessors who will access your data
- Sales rep says 'we'll work that out later' to critical data protection questions
- Your legal team has not reviewed and approved the privacy terms
- Contract term exceeds 24 months without clear exit clauses
- The contract contains exclusivity provisions or unnecessarily limits the institution's ability to use competing AI platforms.

⚠️ CAUTION	Proceed only with additional safeguards if ANY of these are true:

- Vendor has not provided SOC 2 Type II or ISO 27001 certification
- Contract lacks specific data retention periods and deletion timelines
- No audit rights to verify compliance with data protection terms
- Unclear intellectual property rights for custom-trained models or prompts
- No documentation on bias testing or model explainability
- Breach notification window exceeds 72 hours
- Sales pressure includes 'limited time' discounts or 'sign today' urgency
- Vendor roadmap, pricing model, or licensing structure is changing rapidly without contractual protections for existing customers.
- Other universities in your state or network haven't reviewed the vendor

✓ PROCEED	You may proceed if ALL of these are true:

- Written confirmation: No data used for AI training, with clear contractual prohibitions
- Full ownership retained for institutional data, prompts, outputs, workflows, custom assistants, and other institutional intellectual property.
- FERPA compliance certified by vendor's legal team, reviewed by yours
- Data stored in U.S., with encryption at rest and in transit
- Clear data deletion and exit procedures, with certification process
- All subprocessors disclosed, with approval rights for future additions
- Your CIO, CISO, and General Counsel have jointly approved
- Pilot phase completed successfully with de-identified data
- Annual compliance audits required, with your institution's audit rights

UNIVERSITY INNOVATION ALLIANCE

Ten Critical Questions for Presidents, Chancellors & Provosts to Ask

Ask these questions directly to the vendor's executive team (not just sales reps) and demand written answers before any signature. If they cannot answer clearly, that's a red flag.

1. **Who owns the data?** Get specific: Who owns the prompts our faculty, staff and students create? Who owns AI-generated outputs? Who owns custom assistants, institutional GPTs, workflows, agents, retrieval indexes, and any fine-tuned models? Demand the contract explicitly states the university retains 100% ownership.
2. **Can you use our data to train your AI?** The answer must be an unequivocal 'no' in writing. Watch for wiggle words like 'de-identified' or 'aggregate' data, which still means your institutional knowledge is being used to benefit competitors.
3. **Where is our data physically stored and who can access it?** Demand a data flow diagram showing where data enters, where it's processed, where it's stored, and who has access. Include countries, data centers, and any subcontractors.
4. **How do you ensure FERPA compliance?** Require a written FERPA compliance certification from their legal department, not marketing materials. Your General Counsel should review and confirm.
5. **What happens if you're acquired or change your business model?** Google and OpenAI are both active in M&A. What happens to your data if they're acquired by a company with different privacy standards? Demand data return rights and termination clauses.
6. **How can we verify you're doing what you promise?** Require audit rights: your team should be able to independently verify data handling, access logs, and compliance claims at any time, not just during scheduled audits.
7. **What's your data breach protocol?** Require notification within 48 hours maximum, not the legal minimum of 72 hours. Confirm they maintain cyber insurance of at least $10M. Get the name and contact info for their security incident lead.
8. **How do we leave if we need to?** Can you export all institutional data, prompts, custom assistants, workflows, agents, vector databases, retrieval indexes, and any custom models in standard formats? What's the process? What's the timeline? Are there penalties? Test this during a pilot phase.
9. **How do you handle AI bias and transparency?** If you use AI for decisions affecting students (admissions, financial aid, academic placement), you must be able to explain and audit those decisions. Demand model documentation and bias testing protocols.
10. **I'm talking to your competitor, what question should I ask them that I have not asked you?** Listen carefully to what they say about their competitors' weaknesses.

UNIVERSITY INNOVATION ALLIANCE

Specific Questions for individual enterprise AI providers.

10 vendor-neutral questions.

1. Does your platform support multiple foundation models, or does it lock us into a single model ecosystem?
2. Who owns our institution's data, prompts, outputs, custom assistants, workflows, agents, and other AI assets? Can all of them be exported if we leave?
3. How are AI agents governed, monitored, and audited? What administrative controls exist for managing agent behavior and permissions?
4. Can institutional knowledge be exported independently of the underlying AI model? What is the migration process if we change vendors?
5. What administrative controls exist for departments, colleges, faculty, staff, students, and external partners? Can permissions be managed at a granular level?
6. How does your platform integrate with our identity management, LMS, SIS, HR, CRM, cloud storage, and research systems? What data moves between systems?
7. What contractual protections exist if your pricing, licensing model, product roadmap, ownership, or strategic direction changes during our agreement?
8. How do you communicate significant model updates that could affect institutional workflows? Can institutions evaluate or delay major changes before deployment?
9. How do you support interoperability with other enterprise AI platforms if our institution adopts a multi-vendor strategy?
10. We're evaluating multiple enterprise AI platforms. If you were in our position, **what is the single most important question you would ask your competitors that we haven't asked you?**

For Google Workspace / Gemini

1. How does Gemini's integration with Gmail, Drive, Docs, Calendar, Meet, and Classroom affect data access, and how can those permissions be managed by an organizational unit or user group?
2. How does adding Gemini change our existing Google Workspace data protection agreement and administrative controls?
3. Can Gemini capabilities be disabled or restricted for specific organizational units, such as financial aid, health services, legal counsel, research administration, or other high-risk areas?
4. What existing Workspace content is available to Gemini by default, and what administrative controls exist to limit or audit that access?
5. How does Google separate enterprise customer data from consumer Google services, and what contractual guarantees prevent enterprise data from being used to improve public models?

For ChatGPT Enterprise / OpenAI

1. Is ChatGPT Enterprise completely isolated from the public ChatGPT environment for both model training and data storage?
2. How are custom GPTs governed across the institution? Who can create them, share them, approve them, and retire them?
3. Given OpenAI's relationship with Microsoft Azure, what customer data, if any, is shared with Microsoft, and under what contractual terms?

4. If OpenAI introduces new enterprise capabilities or changes its product structure, how will existing institutional GPTs, workflows, and contracts be affected?
5. What happens to our institutional GPTs, custom AI assets, and data if OpenAI's ownership, partnership structure, or business model changes?

For Anthropic Claude Enterprise

1. How does Claude Enterprise ensure institutional data, Projects, Artifacts, and conversations remain isolated from public Claude usage and are never used to train foundation models?
2. How does Claude Enterprise manage institutional knowledge connected through the Model Context Protocol (MCP) or other enterprise integrations? What information is indexed, where is it stored, and how can it be audited or removed?
3. How are Claude's Projects and Artifacts managed as institutional intellectual property, and can they be exported in standard formats if we change platforms?
4. How are Claude's Constitutional AI safety mechanisms applied within the Enterprise environment, and can institutional administrators configure organizational guardrails for different use cases?
5. How will Anthropic communicate significant model or MCP changes that could affect institutional workflows, and can institutions evaluate those changes before deployment?

Detailed Assessment Checklist for Your Team

Give this comprehensive checklist to your CIO, CISO, and General Counsel to complete jointly. They should collaborate on reviewing the vendor's responses, and all three must sign off before you proceed.

Topic	What to Verify	Must Have in Contract
1. Data Ownership	University retains full ownership of all inputs, outputs, and any derivative works	Explicit clause: 'Vendor has zero rights to use, copy, or train on institutional data in any form'
2. Model Training	Vendor cannot use your data to improve general AI models, even if de-identified or aggregated	Clause prohibiting data use for: training, model improvement, benchmarking, or product development
3. Data Residency	Data stored and processed only in approved U.S. data centers, with no cross-border transfers	Data flow diagram + contractual commitment to U.S.-only processing. Written approval required for any changes
4. FERPA Compliance	Written certification that vendor qualifies as 'school official' under FERPA, with limitations on data use	FERPA addendum signed by vendor's legal team. Incident reporting clause for any FERPA violations
5. Security Standards	SOC 2 Type II or ISO 27001 certification current and maintained throughout contract	Encryption at rest (AES-256) and in transit (TLS 1.3+). MFA required. Annual security audits
6. Subprocessors	Complete list of all entities with data access, including overseas contractors	Written approval required before adding new subprocessors. Right to object to specific subprocessors
7. Data Retention	Clear retention schedule and verified deletion process, including backups	30-day retention maximum after termination. Deletion certification provided. No indefinite backups or archives
8. Breach Protocol	Immediate notification of any unauthorized access, with detailed incident response	48-hour maximum notification. $10M minimum cyber insurance. Dedicated security contact with escalation path
9. Bias & Explainability	Model documentation and bias testing for any AI affecting student outcomes	Prohibit AI use in consequential decisions (admissions, financial aid) without human oversight and appeal rights
10. Exit Rights	Full portability of institutional data, prompts, custom assistants, workflows, agents,	Export all institutional data, prompts, assistants, workflows, agents, & custom models in standard formats. Documented

Topic	What to Verify	Must Have in Contract
	and transition support if you change vendors.	migration support for at least 90 days. No penalties for early termination.

Action Steps: Who Does What

Here's your implementation roadmap. Don't skip steps, even if the vendor is pressuring you to move faster.

Before Any Vendor Presentation

1. **President:** Convene your CIO, CISO, General Counsel, and Chief Data Officer (if you have one). Give them this guide and set expectations: no shortcuts on data protection.
2. **President:** Establish a cross-functional AI procurement committee that must approve all AI contracts. No single department should sign alone.
3. **CIO:** Survey which departments are already using AI tools (often shadow IT). Create an AI tool registry to understand current exposure.

During Vendor Evaluation

4. **CIO:** Require vendors to complete a written questionnaire from this guide before any demo. No verbal answers. No 'we'll get back to you.'
5. **General Counsel:** Review vendor's standard contract before any pilot. Identify deal-breaker clauses early. Don't wait until you're invested.
6. **CISO:** Conduct security assessment. Review SOC 2 reports, penetration test results, incident history. Call references at similar institutions.
7. **CIO:** Create side-by-side comparison matrix for all enterprise AI platforms under consideration, including existing institutional tools vs. status quo. Include costs beyond subscription (training, integration, support).

Before Pilot Phase

8. **President:** Approve pilot only with synthetic or de-identified data. No student records in pilots. No exceptions.
9. **CIO:** Define pilot success criteria in advance. What must the tool accomplish to justify continuing? Set a firm evaluation date.
10. **General Counsel:** Ensure pilot agreement includes all data protections you'll require in the final contract. Pilots are binding contracts too.
11. **CIO:** Test the exit process during the pilot. Can you actually export data in usable formats? How long does it take? Document everything.

Before Contract Signature

12. **General Counsel:** Red-line the contract with all required changes from this guide. Do not accept vendor's 'standard contract' without modifications.
13. **President:** Require written certification from CIO, CISO, and General Counsel that all checklist items are satisfied. They should sign off jointly.

14. **President:** Consider consulting with peer institutions who have signed similar contracts. Learn from their mistakes.
15. **President:** Limit initial contract to 12-24 months maximum. AI changes too fast for longer commitments. Build in annual review and renegotiation rights.

After Contract Signature

16. **CIO:** Establish an AI governance committee to oversee AI deployment, agents, institutional knowledge, and future enterprise AI adoption.
17. **CIO:** Create usage policies and training for faculty and staff. AI literacy is essential for responsible use.
18. **CISO:** Schedule quarterly compliance audits. Don't wait for annual reviews. Verify vendor promises continuously.
19. **President:** Require annual review meeting where CIO, CISO, and General Counsel present on: compliance status, security incidents, cost vs. value, and whether to renew.
20. **President:** Stay informed on AI policy developments. Regulations are evolving. Your contract may need renegotiation as laws change.

A Final Word: Why This Matters

Your institution's data represents decades of student aspirations, faculty research, stakeholder investment, and relationships. Once that data is used to train an AI model, you can never get it back. The vendor has it permanently, even if you delete your account.

Google and OpenAI are valuable partners with powerful technologies. But their business models depend on data at scale. Your students didn't come to your university to become training data for Silicon Valley.

The sales teams you're meeting with are skilled and well-intentioned, but they have quotas to hit. They will tell you that other universities are signing up rapidly and you'll be left behind. They'll offer 'limited time' discounts that expire this quarter. They'll say privacy concerns are 'theoretical' and point to vague reassurances in marketing materials.

Don't let urgency override due diligence. The right AI partnership can transform your institution. The wrong one can expose you to data breaches, FERPA violations, potential chaos, and loss of institutional knowledge.

AI contracts are no longer simply software agreements. They determine where institutional knowledge lives, how future workflows will be built, and how easily your institution can adapt as AI evolves. The goal is not to predict the winning AI model. The goal is to preserve your institution’s flexibility.

Take your time. Ask hard questions. Demand written answers. Protect your students' data as fiercely as you protect your institution's endowment.

If you have questions about this guide or need support reviewing a specific contract, consider consulting with:

- Your institutional legal counsel
- EDUCAUSE or your regional higher ed IT consortium
- Peer institutions who have completed similar reviews
- Third-party experts in AI ethics and data governance

Document Version: 1.2 July 2026
This guide should be reviewed and updated quarterly as AI technology and regulations evolve

Updates include:

- *Expanded guidance for today’s broader enterprise AI marketplace.*
- *Added protections against vendor lock-in and exclusivity.*
- *Clarified ownership of prompts, custom assistants, workflows, agents, and other institutional AI assets.*
- *Strengthened AI portability and exit planning guidance.*
- *Updated vendor evaluation questions and procurement recommendations.*
- *Refreshed terminology throughout for continued relevance while preserving the original framework.*