Security, Compliance, and Support Posture of Framez

Executive Summary

This document outlines Framez's approach to security, data privacy, regulatory compliance, and operational support. As a cloud-based AI tool handling potentially sensitive educational content, Framez is designed with a **"security-first" posture** to protect university data and users. Key areas addressed include data handling and PII minimization, encryption and cloud infrastructure security, tenant isolation on Azure, incident response plans, uptime and reliability commitments, SSO and identity management, and organizational measures ensuring sustainable support.

Data Handling and PII Minimization

Framez is explicitly designed to **minimize the collection and exposure of Personally Identifiable Information (PII)**.

- **PII Avoidance:** The platform does not require or store sensitive student PII such as full names, personal emails, or social security numbers. Authentication is handled solely via Single Sign-On (SSO) tokens.
- **Content Focus:** Framez ingests only *course-related material* (e.g., lecture transcripts, course documents) for AI processing, not sensitive student records or grade data from the Learning Management System (LMS). As a defense in depth, Framez PII engine scrubs any potential data from these materials as well, and only saves the scrubbed copy of these materials.
- **Usage Logging:** Student queries and AI responses may be logged for quality improvement, but these logs are institutionally segregated, anonymized, and aggregated when possible, and are never used to profile students. The AI's functionality is based on course content, not student identity.
- **Data Ownership and Retention: The university retains ownership of all content and data** at all times. Data retention policies are strictly enforced, with data (like transcripts and chat logs) only kept for as long as pedagogically necessary. Institutions can request immediate data deletion upon contract termination or at any time. This design aligns with privacy best practices and **FERPA** guidelines.

Encryption and Azure Cloud Security

Framez employs a multi-layered encryption strategy that combines **envelope encryption**, **Azure-managed**

Hardware Security Modules (HSMs), and industry-standard cryptography to protect all institutional data.

All data in transit and at rest is encrypted using best-in-class standards and governed by Azure's enterprise security controls.

- **Encryption in Transit:** All communication between Framez, the LMS (Canvas), media systems (Kaltura), and end-user browsers is protected using **TLS 1.2+**.
  This ensures that data exchanged during LTI launches, API calls, and content ingestion is always transmitted over secure, authenticated channels.
- **Envelope Encryption at Rest:** All stored data, including transcripts, vector embeddings, usage logs, and AI-generated content is protected using an **envelope encryption model**:
  1. **Data Encryption Keys (DEKs)** encrypt data using **AES-256**, stored only in encrypted form.
  2. **Key Encryption Keys (KEKs)**, stored securely in **Azure Key Vault backed by FIPS 140-2 Level 2 validated HSMs**, are used to encrypt and rotate DEKs.
  3. Decryption operations occur **inside the Azure HSM boundary**, meaning raw keys never leave the secured module.
- **Key Management and Rotation:** Azure Key Vault manages all cryptographic keys, secrets, and certificates supporting the platform. The keys are rotated at pre-determined intervals.
- **Infrastructure Compliance :** Microsoft contractually guarantees that customer data—including media derivatives and AI inputs will **not** be mined, analyzed, or used for advertising. By building on Microsoft Azure, Framez inherits protections aligned with:
  - **SOC 2 Type II**
  - **ISO 27001/27017/27018**
  - **FERPA** (supporting institutional compliance)
  - **GDPR infrastructure controls**
- **Access Control and Auditing:** Access to production systems is tightly controlled:
  - Restricted to a small number of senior engineers
  - Enforced through **Azure RBAC**, **MFA**, and Just-In-Time (JIT) access
  - Fully audited through Azure Monitor, Log Analytics, and Key Vault diagnostic logs
  - All access attempts and privileged operations are tracked and retained for compliance review

This comprehensive approach ensures that data is protected not only through encryption, but also through rigorous operational controls and continuous monitoring.

Azure Tenant Isolation and Multi-Tenancy Controls

Framez operates in a secure **multi-tenant** cloud environment, with strict logical and physical separation for each client's data.

- **Data Separation:** We provision a dedicated container (or schemas) for each institution. University A's content and logs are physically or logically segregated from University B's, with application-level checks on every query to prevent intermingling of records.
- **Network Isolation:** The architecture can leverage Azure Virtual Networks and separate App Service instances per institution to ensure isolated compute resources.
- **Dedicated Instances:** For the most stringent governance requirements, Framez supports

deploying a dedicated, single-tenant instance in a separate Azure subscription or on the university's own tenancy.

This level of configurability ensures that security posture scales with institutional requirements, from standard deployments to highly regulated environments

Incident Response and Monitoring

Framez maintains a comprehensive **Incident Response Plan (IRP)** to address security incidents and service disruptions with speed and transparency.

- **24/7 Monitoring:** Continuous monitoring via Azure Security Center and Application Insights ensures immediate alerts for suspicious activity. An on-call rotation of engineers provides 24/7 coverage for critical alerts.
- **Containment & Remediation:** The IRP prioritizes swift containment (e.g., isolating a compromised component) and rapid remediation (e.g., security patching, restoring data from backups).
- **Transparent Communication:** In the event of a significant incident or data exposure, customers are notified within a targeted window (e.g., within 24 hours), provided with a summary of the impact, and informed of the steps taken.
- **Post-Incident Review:** Every major incident is followed by a post-mortem analysis, with a report shared with the client to detail root causes and preventative measures for continuous security improvement.

Uptime Guarantees and Reliability

Framez is built for reliability, committing to an objective of at least **99.9% availability** (less than approximately 45 minutes of unplanned downtime per month).

- **Redundant Infrastructure:** We utilize Azure's geo-replication and multiple availability zones. Critical components have failover instances to minimize single points of failure.
- **Autoscaling:** The platform automatically scales compute resources during peak usage (e.g., exam periods) to prevent slowdowns or outages due to high load.
- **Disaster Recovery (DR):** Daily backups of critical data are stored in a separate region. Our DR plan is designed to restore service within a few hours in the event of a region-wide outage or major corruption.
- **Planned Maintenance:** Scheduled maintenance is conducted during off-peak hours and communicated in advance, often using zero-downtime deployment strategies.

Single Sign-On and Identity Management

Framez fully supports **Single Sign-On (SSO)**, integrating with the university's existing identity management systems for seamless and secure access.

- **Authentication:** Users authenticate via trusted campus credentials (e.g., Okta, Azure AD) through the LMS (Canvas LTI launch). Framez never handles or stores user passwords.

- **Protocol Support:** We support major federation protocols including **SAML2** and **OIDC** for admin access outside of the LMS, and are tested with **Azure AD/Entra ID, Google Oauth etc**.
- **Role Mapping:** User roles (instructor, student, TA) are received via SSO/LTI, and permissions are strictly enforced within Framez (e.g., only instructors can access course configuration).
- **Automated Provisioning:** Access is dynamically managed via LMS enrollment. If a student is removed from a course or leaves the institution, their access to Framez is automatically revoked, minimizing the risk of orphaned accounts.

Compliance with Educational Regulations

Framez proactively ensures its operations support university compliance with key educational and data protection regulations.

- **FERPA:** Framez acts as a "school official" under contract, committed to the confidentiality of student Q&A logs and course content. We avoid PII ingestion to maintain institutional control over educational records.
- **GDPR:** We adhere to GDPR principles of data minimization and support data deletion upon request, with Azure providing infrastructure-level GDPR compliance.
- **Accessibility:** We are committed to IT accessibility standards (e.g., **WCAG 2.1 AA**). The Canvas interface is designed to be screen-reader friendly and keyboard navigable.
- **Security Assessments:** Framez is prepared to complete the **Higher Education Community Vendor Assessment Toolkit (HECVAT)** to provide comprehensive evidence of our security, privacy, and compliance controls to campus IT offices.
- **Audits and Testing:** We support university audits with necessary documentation (e.g., SOC 2 report summaries, data flow diagrams) and regularly perform third-party security audits and penetration tests.

Operational Support and Financial Sustainability

Framez is committed to being a reliable, long-term partner through robust support and a sustainable business model.

- **Support Services:** We provide responsive support through a structured ticketing system, emergency contact channels for outages, and direct engineering engagement for urgent issues. Faculty and IT teams receive onboarding assistance to ensure a smooth deployment.
- **Escrow/Exit Strategy:** Framez is also open to escrow arrangements for critical components or data, giving universities confidence that their instructional materials and derived datasets remain accessible even under unlikely scenarios.
- **Continuous Improvement:** Our team continually monitors developments in AI and security, integrating new best practices and ensuring regular software updates to maintain compatibility and security posture.

In conclusion, Framez combines a conservative security posture with an innovative instructional platform. By minimizing PII ingestion, integrating through LMS-based identity flows, leveraging Azure's robust cloud security, maintaining strong tenant isolation, providing transparent incident response, and offering a sustainable support structure, Framez ensures that universities can adopt AI-enhanced teaching tools without jeopardizing privacy, security, or operational stability.

The result is a platform designed not just for powerful AI-driven learning experiences, but for long-term trust and responsible partnership with higher-education institutions.