SkillsOS Security Whitepaper

Version 1.0 | December 2024

Executive Summary

SkillsOS is an enterprise-grade platform designed specifically for higher education institutions to navigate curriculum transformation, workforce alignment, and credential management. Security and compliance are foundational to our architecture, ensuring that student data, institutional information, and operational processes are protected at every level.

This whitepaper provides a comprehensive overview of our security architecture, compliance certifications, and data protection practices.

Table of Contents

1. Security Architecture Overview

Defense in Depth

SkillsOS employs a defense-in-depth security strategy with multiple layers of protection:

Layer	Protection Measures
Network	WAF, DDoS protection, TLS 1.3 encryption
Application	Input validation, CSRF protection, secure headers
Data	AES-256 encryption at rest, field-level encryption for sensitive data
Identity	MFA, SSO integration, role-based access control
Monitoring	24/7 security monitoring, anomaly detection, audit logging

Secure Development Lifecycle

Our development process incorporates security at every stage:

- **Design Review**: Security architecture review for all new features
- **Code Review**: Mandatory peer review with security checklist
- **Static Analysis**: Automated security scanning in CI/CD pipeline
- **Dependency Scanning**: Continuous monitoring for vulnerable dependencies
- **Penetration Testing**: Annual third-party penetration tests

2. Data Protection

Encryption Standards

Data at Rest:

- AES-256 encryption for all stored data

- Encrypted database backups
- Secure key management using cloud KMS

Data in Transit:

- TLS 1.3 for all communications
- HSTS enforcement
- Certificate pinning for mobile applications

Data Classification

Classification	Examples	Protection Level
Confidential	Student PII, credentials	Encrypted, access-logged, MFA required
Internal	Curriculum data, analytics	Encrypted, role-based access
Public	Marketing content	Standard protection

Data Retention and Deletion

- Configurable retention policies per institution
- Secure deletion with cryptographic erasure
- Right to deletion compliance (GDPR, CCPA)
- Automated purging of expired data

---

3. Access Control

Authentication

- **Single Sign-On (SSO)**: SAML 2.0 and OAuth 2.0 support
- **Multi-Factor Authentication**: TOTP, SMS, and hardware key support
- **Password Policy**: Configurable complexity requirements
- **Session Management**: Automatic timeout, concurrent session limits

Authorization

Role-Based Access Control (RBAC):

Role	Permissions
Institution Admin	Full access to institution settings, user management
Program Manager	Curriculum management, program analytics
Faculty	Course management, credential issuance
Viewer	Read-only access to dashboards

Audit Logging

All access and modifications are logged with:

- User identity
- Timestamp (UTC)
- Action performed
- Affected resources
- IP address and user agent

---

4. Infrastructure Security

Cloud Infrastructure

SkillsOS is hosted on enterprise-grade cloud infrastructure:

- **Provider**: Vercel (frontend), Supabase (database), AWS (storage)
- **Certifications**: SOC 2 Type II, ISO 27001
- **Geographic Redundancy**: Multi-region deployment
- **Availability**: 99.9% uptime SLA

Network Security

- **Web Application Firewall (WAF)**: Protection against OWASP Top 10
- **DDoS Mitigation**: Automatic traffic analysis and filtering
- **Network Segmentation**: Isolated production environments
- **Intrusion Detection**: Real-time threat monitoring

Backup and Disaster Recovery

Component	RPO	RTO	Backup Frequency
Database	1 hour	4 hours	Continuous
File Storage	24 hours	8 hours	Daily
Configuration	1 hour	1 hour	Continuous

---

5. Compliance Certifications

FERPA (Family Educational Rights and Privacy Act)

SkillsOS maintains full FERPA compliance:

- Student education records protected as required
- Disclosure controls and consent management
- Annual FERPA training for all employees
- Data Processing Agreement available for institutions

SOC 2 Type II

Independent audit verification of:

- Security controls
- Availability measures
- Processing integrity

- Confidentiality protections

GDPR (General Data Protection Regulation)

For institutions with EU students and staff:

- Data subject rights implementation
- Privacy by design architecture
- Data Protection Impact Assessments
- EU-US data transfer mechanisms

HECVAT (Higher Education Community Vendor Assessment Toolkit)

Pre-completed HECVAT Lite questionnaire available for streamlined procurement processes.

WCAG 2.1 AA

Web Content Accessibility Guidelines compliance:

- Screen reader compatibility
- Keyboard navigation
- Color contrast requirements
- Alternative text for images

CCPA (California Consumer Privacy Act)

For California-based users:

- Right to know
- Right to delete
- Right to opt-out
- Non-discrimination

6. Incident Response

Response Process

1. **Detection**: Automated monitoring and alerting
2. **Triage**: Severity assessment within 15 minutes
3. **Containment**: Immediate threat isolation
4. **Investigation**: Root cause analysis
5. **Remediation**: Fix deployment and verification
6. **Communication**: Stakeholder notification per SLA
7. **Post-Incident**: Review and improvement

Notification SLAs

Severity	Initial Response	Customer Notification
Critical	15 minutes	1 hour
High	1 hour	4 hours
Medium	4 hours	24 hours
Low	24 hours	72 hours

---

7. Vendor Management

Third-Party Risk Assessment

All vendors undergo security assessment including:

- SOC 2 or equivalent certification review
- Security questionnaire completion
- Contract review for data protection terms
- Annual reassessment

Current Subprocessors

A complete list of subprocessors is maintained and available upon request. Key categories include:

- Cloud infrastructure providers
- Authentication services
- Analytics platforms
- Communication services

---

8. Contact Information

Security Team Email: security@skillsos.org

Vulnerability Reporting Email: security@skillsos.org Subject: Vulnerability Report

Compliance Inquiries Email: compliance@skillsos.org

Data Protection Officer Email: dpo@skillsos.org

This document is updated quarterly. Last review: December 2024.