HECVAT Lite Questionnaire Responses

Higher Education Community Vendor Assessment Toolkit

Vendor: SkillsOS Version: HECVAT Lite 3.0 Date Completed: December 2024

Company Information

Field	Response
Company Name	SkillsOS (NorthPath Strategies, LLC)
Product Name	SkillsOS Platform
Contact Name	Security Team
Contact Email	security@skillsos.org
Website	https://skillsos.org

QUAL: Qualifications

QUAL-01: Does your organization have a dedicated information security function?

Response: Yes

Additional Information: SkillsOS maintains a dedicated security function responsible for security architecture, compliance, incident response, and security awareness training.

QUAL-02: Does your organization have documented information security policies?

Response: Yes

Additional Information: Comprehensive security policies covering access control, data protection, incident response, acceptable use, and vendor management. Policies are reviewed annually.

QUAL-03: Has your organization completed a SOC 2 Type II audit?

Response: Yes

Additional Information: SOC 2 Type II audit completed annually. Report available upon request under NDA.

QUAL-04: Does your organization carry cyber liability insurance?

Response: Yes

Additional Information: Cyber liability insurance with coverage appropriate for our operations and customer base.

COMP: Compliance

COMP-01: Is your organization FERPA compliant?

Response: Yes

Additional Information: Full FERPA compliance maintained. We act as a “school official” with legitimate educational interest. Data Processing Agreement available.

COMP-02: Is your organization GDPR compliant?

Response: Yes

Additional Information: GDPR compliance for EU data subjects including data subject rights, privacy by design, and appropriate transfer mechanisms.

COMP-03: Is your organization CCPA compliant?

Response: Yes

Additional Information: CCPA compliance for California residents including right to know, delete, and opt-out.

COMP-04: Does your organization comply with WCAG 2.1 AA accessibility standards?

Response: Yes

Additional Information: Platform designed and tested for WCAG 2.1 AA compliance including screen reader support, keyboard navigation, and color contrast requirements.

DATA: Data Protection

DATA-01: Is all customer data encrypted at rest?

Response: Yes

Additional Information: AES-256 encryption for all data at rest in databases and file storage.

DATA-02: Is all data encrypted in transit?

Response: Yes

Additional Information: TLS 1.3 encryption for all data in transit. HSTS enabled.

DATA-03: Can customer data be logically separated from other customers?

Response: Yes

Additional Information: Multi-tenant architecture with logical data separation. Each institution’s data is isolated using organization-level access controls.

DATA-04: Where is customer data stored geographically?

Response: United States

Additional Information: Primary data storage in United States. Data residency options available upon request for specific compliance requirements.

DATA-05: Does your organization have a data retention policy?

Response: Yes

Additional Information: Configurable retention policies. Default: active data retained during service period, deleted within 30 days of termination.

DATA-06: Can customer data be exported?

Response: Yes

Additional Information: Data export functionality available in standard formats (CSV, JSON). Full data portability supported.

DATA-07: Is customer data backed up?

Response: Yes

Additional Information: Daily encrypted backups with geographic redundancy. Point-in-time recovery available. RPO: 1 hour, RTO: 4 hours.

ACCESS: Access Control

ACCESS-01: Does your application support Single Sign-On (SSO)?

Response: Yes

Additional Information: SAML 2.0 and OAuth 2.0 SSO support. Integration with major identity providers (Azure AD, Okta, Google Workspace, Shibboleth).

ACCESS-02: Does your application support Multi-Factor Authentication (MFA)?

Response: Yes

Additional Information: MFA support including TOTP authenticator apps, SMS, and hardware security keys.

ACCESS-03: Does your application implement role-based access control?

Response: Yes

Additional Information: Granular RBAC with predefined roles (Admin, Program Manager, Faculty, Viewer) and custom role support.

ACCESS-04: Are user sessions automatically terminated after inactivity?

Response: Yes

Additional Information: Configurable session timeout. Default: 30 minutes of inactivity. Concurrent session limits available.

ACCESS-05: Are all user activities logged?

Response: Yes

Additional Information: Comprehensive audit logging of all user activities including authentication, data access, and modifications. Logs retained for 7 years.

Mail: Email Security

MAIL-01: Does your organization use email authentication (SPF, DKIM, DMARC)?

Response: Yes

Additional Information: SPF, DKIM, and DMARC configured for all outbound email. DMARC policy set to reject.

MAIL: Vulnerability Management

VULN-01: Does your organization conduct regular vulnerability assessments?

Response: Yes

Additional Information: Continuous automated vulnerability scanning. Weekly scans of production infrastructure.

VULN-02: Does your organization conduct penetration testing?

Response: Yes

Additional Information: Annual third-party penetration testing by qualified security firm. Remediation tracked to completion.

VULN-03: Does your organization have a vulnerability disclosure program?

Response: Yes

Additional Information: Responsible disclosure program. Contact: security@skillsos.org

VULN-04: What is your patch management timeline for critical vulnerabilities?

Response: Critical: 24-48 hours, High: 7 days, Medium: 30 days, Low: 90 days

---

Mail: Incident Response

IR-01: Does your organization have a documented incident response plan?

Response: Yes

Additional Information: Documented incident response plan covering detection, containment, eradication, recovery, and lessons learned.

IR-02: What is your notification timeline for security incidents?

Response: 24-72 hours

Additional Information: Initial notification within 24 hours of discovery. Detailed report within 72 hours.

IR-03: Does your organization conduct incident response exercises?

Response: Yes

Additional Information: Annual tabletop exercises and periodic technical drills.

MAIL: Business Continuity

BC-01: Does your organization have a business continuity plan?

Response: Yes

Additional Information: Documented BCP covering disaster recovery, communication plans, and recovery procedures.

BC-02: What is your guaranteed uptime SLA?

Response: 99.9%

Additional Information: 99.9% uptime SLA with service credits for downtime exceeding SLA.

BC-03: Does your organization have geographic redundancy?

Response: Yes

Additional Information: Multi-region deployment with automatic failover capabilities.

MAIL: Vendor Management

VENDOR-01: Does your organization assess third-party vendor security?

Response: Yes

Additional Information: All vendors undergo security assessment including SOC 2 review, security questionnaire, and contract review.

VENDOR-02: Do you maintain a list of subprocessors?

Response: Yes

Additional Information: Subprocessor list maintained and available. Customers notified of changes.

MAIL: Personnel Security

HR-01: Does your organization conduct background checks on employees?

Response: Yes

Additional Information: Background checks conducted for all employees with access to customer data.

HR-02: Does your organization provide security awareness training?

Response: Yes

Additional Information: Annual security awareness training for all employees. Additional training for technical staff.

Additional Documentation Available

- Security Whitepaper
- Data Processing Agreement (DPA)
- Subprocessor List
- Privacy Policy
- Terms of Service
- SOC 2 Type II Report (under NDA)

Contact for Questions

Security Team: security@skillsos.org **Compliance Team:** compliance@skillsos.org

---

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