To: NDSU IT Security Office
From: Liszt Team (Kyle Vanderburg)
Subject: Security Review Documentation for Liszt

Contact Information:

IT Security Contact
Kyle Vanderburg
Email: kyle@noteforge.com
Phone: 701-960-4569
Address: PO Box 10893, Fargo ND 58106

Contents

Statement of which regulation or standards the company complies with

Liszt is designed with FERPA compliance in mind and adheres to best practices derived from NIST 800-53, CIS Critical Security Controls, and the Higher Education Community Vendor Assessment Toolkit (HECVAT).

Liszt is developed with a strong focus on educational data privacy and security, and is designed to support compliance with the Family Educational Rights and Privacy Act (FERPA). Although Liszt is not a system of record, it handles student attendance data, competency tracking, and limited personally identifiable information (PII), all of which are treated with FERPA-level sensitivity.

To ensure FERPA compliance and a strong security posture, Liszt incorporates the following design principles and operational safeguards:

FERPA Compliance Measures

- **Data Ownership and Control:** Institutions retain full ownership of all data submitted to Liszt. Access to data is controlled by institutional identity providers (e.g., Microsoft Azure AD).
- **No Re-disclosure:** Liszt does not share or re-disclose any education records or PII except at the direction of the institution or as required by law.
- **User Identification:** All users authenticate via institution-controlled OAuth providers, ensuring that only authorized individuals access FERPA-covered information.
- **Data Residency:** All data is stored in cloud infrastructure located in the United States.
- **PII Deletion on Request:** Liszt provides institutions with tools and support to delete user data, including submission history and identifying information.
- **Separation of Commercial and Educational Use:** Liszt does not use student data for advertising, profiling, or any commercial purpose.

Alignment with NIST 800-53 (Low Baseline)

While Liszt is not formally certified under NIST 800-53, its infrastructure and development lifecycle align with the Low-Impact Baseline Controls, including:

- **Access Control (AC):** Role-based access enforced within the app; user identity governed by institutional SSO.

- **System and Communications Protection (SC):** TLS 1.2+ for all traffic in transit; AES-256 encryption for data at rest.
- **Identification and Authentication (IA):** OAuth authentication using Microsoft and other SSO providers; no passwords stored locally.
- **Contingency Planning (CP):** Nightly encrypted backups; infrastructure-as-code-based recovery; data restore testing every 30 days.
- **System Integrity (SI):** Regular OS patching, dependency updates, and log monitoring for anomalous behavior.
- **Audit and Accountability (AU):** Logging of access and system actions retained for audit purposes.

HECVAT Best Practice Adoption

Liszt's security planning is modeled on the Higher Education Community Vendor Assessment Toolkit (HECVAT). Specific HECVAT-aligned practices include:

- **Clear role delineation** for access to institutional and student data
- **Data classification and retention guidance**
- **Data storage and encryption policies** reviewed annually
- **Ongoing internal assessments** based on HECVAT Lite and Full questionnaires

Company Security Policies

Liszt follows a defense-in-depth approach to security, applying industry-standard practices in encryption, access control, system hardening, and patch management. The system is built to meet the security expectations of higher education institutions while maintaining operational simplicity and transparency.

Application & Data Security

- **Encryption in Transit and at Rest:** All user data in transit is secured using TLS 1.2 or higher. Data at rest, including database storage and nightly backups, is encrypted using AES-256, ensuring that sensitive information remains protected.
- **OAuth-Based Authentication:** Liszt delegates authentication to institutional identity providers (e.g., Microsoft Azure AD), meaning passwords are never stored or managed by Liszt. This model supports institution-**enforced multifactor authentication (MFA)** and account lifecycle policies.
- **Role-Based Access Control (RBAC):** Application roles govern user access to features and data within each institution. Students, faculty, and admins are granted only the permissions necessary for their roles.

System and Infrastructure Security

- **Minimal Attack Surface:** Liszt is deployed on hardened Linux servers with only necessary services exposed. Public-facing services are restricted to HTTPS; administrative access is via SSH with key-based authentication.
- **Firewall Controls:** Host-level firewalls are configured to allow only required traffic. Ingress and egress rules are regularly reviewed.
- **SELinux Enforcement:** Liszt is in the process of migrating all hosting environments to SELinux-enforcing Linux distributions to enhance mandatory access controls and contain unauthorized process behavior.

Patch and Vulnerability Management

- **Timely Updates:** System packages and application dependencies are patched regularly. Security-related patches are applied within 48 hours of disclosure when feasible.

- **Vulnerability Monitoring:** The Liszt codebase and hosting stack are monitored for common vulnerabilities and exposures (CVEs) using package manager tools (dnf, composer audit) and community threat advisories.
- **No Containerization:** Liszt does not currently use Docker or container orchestration; services are deployed on traditional virtual machines for maximum transparency and auditability.

Policy Management and Logging

- **Change Management:** Application and configuration changes are tracked in version-controlled repositories. Production deployments are reviewed and logged.
- **Logging and Monitoring:** System logs, application errors, and access records are collected and retained for internal review and incident response purposes.
- **Annual Policy Review:** Security policies and practices are revisited annually or after any significant infrastructure change.

Company Privacy Policy

Liszt is committed to protecting the privacy and security of its users and institutional clients. The platform is designed with educational use and FERPA compliance as core priorities, and no student or institutional data is ever used for marketing, analytics, or third-party profiling.

Key principles of Liszt's data privacy policy include:

- **No Sale or Sharing of Data:**
  Liszt does not sell, share, or re-disclose any user data to third parties. This includes personally identifiable information (PII), institutional records, and usage metadata.
- **Access by Permission Only:**
  Liszt staff may access institutional or user data solely for the purposes of support, troubleshooting, or maintenance, and only with explicit permission from the institution or user when appropriate. All such access is logged and reviewed periodically.
- **Institutional Data Ownership:**
  All data entered into Liszt by a participating institution or its users remains the property of that institution. Liszt functions as a data processor on behalf of each institution, with no claim to data ownership.
- **Minimal Data Collection:**
  Liszt only collects the minimum necessary information to support its core features. Authentication is handled by the institution's identity provider, and no passwords are stored or managed by Liszt.
- **United States Data Residency:**
  All Liszt data is stored and processed within data centers located in the United States.
- **Data Deletion and Export Support:**
  Institutions may request the export or deletion of data at any time. Liszt provides tools and support for complying with user data requests in accordance with institutional policies.

The full privacy policy is available at:
https://noteforge.com/legal/privacy-policy/

Company Administrative Logical and Physical Control Policies:

Liszt implements layered administrative, logical, and physical controls to protect data and infrastructure from unauthorized access and ensure institutional compliance with FERPA and standard security expectations.

Administrative Controls

- **Role-Based Administrative Access:** Access to system administration, application configuration, and institutional data is granted strictly on a need-to-know basis. Only authorized Liszt administrators have access to sensitive system functions, and access is reviewed periodically.
- **Principle of Least Privilege:** All administrative accounts are provisioned with the minimum necessary permissions for their operational responsibilities.
- **Change and Access Review:** System-level access and application-level role assignments are logged and reviewed regularly to detect unauthorized elevation or privilege misuse.

Logical Controls

- **Authentication Security:** Server-level access is restricted to designated administrative personnel via SSH key-based authentication. Password-based logins are disabled.
- **Separation of Environments:** Development and production environments are logically separated to reduce the risk of data leakage or misconfiguration.
- **Data Access Segregation:** Institutional data is logically isolated by tenant, preventing cross-institutional access within the shared application infrastructure.
- **Encryption and Logging:** All sensitive operations are logged. Logs include access records, error conditions, and authentication events, and are retained for monitoring and incident response.

Physical Controls

- **U.S.-Based Hosting Infrastructure:** Liszt is hosted in geographically redundant, SOC 2-certified data centers operated by trusted cloud providers (e.g., DigitalOcean), located exclusively within the United States.

- **Physical Security Measures (inherited from hosting provider):** These facilities implement 24/7 security monitoring, biometric access controls, video surveillance, and environmental controls (power, cooling, fire suppression).
- **No On-Premise Data Storage:** Liszt maintains no physical servers or storage devices at developer offices or administrative sites. All infrastructure is virtualized and managed through secure cloud platforms.

How and to whom NDSU data may be disclosed to and why:

NoteForge, the developer and operator of Liszt, maintains a strict policy regarding the confidentiality and handling of institutional and user data.

No Unauthorized Disclosure:

- NoteForge does not disclose, transmit, or share any data belonging to NDSU (or other institutions) with third parties unless:
    - **Explicit written authorization** is provided by the institution, or
    - **Disclosure is required by law**, such as in response to a valid subpoena or court order.
- **No Advertising, Analytics, or Sale of Data:**
  Institutional and user data is never used for advertising, marketing, profiling, or analytics, nor is it sold or shared with data brokers or advertisers.
- **Subprocessors and Infrastructure Providers:**
  NoteForge does not use third-party subprocessors to process education records. Core infrastructure providers (e.g., cloud hosting platforms such as DigitalOcean) are used solely for storage and compute purposes, and these providers do not have access to application-level data.
- **Access Bound by Confidentiality and Purpose:**
  Any access to institutional data by NoteForge staff is purpose-limited (e.g., support, maintenance) and performed only with institutional awareness or request.
- **FERPA Alignment:**
  Liszt operates as a data processor on behalf of each institution. All data remains under the control of the institution, in alignment with FERPA's directory and nondirectory information restrictions.

Company Data Classification

Data Classification:
NoteForge treats all institution-stored data as “Confidential – Institutional Use” and applies appropriate safeguards accordingly.

NoteForge classifies all data stored or processed within the Liszt platform in accordance with its sensitivity and institutional ownership. The default classification applied to all institution-related data is:

Confidential – Institutional Use Only

This classification reflects the potential impact of unauthorized disclosure, modification, or loss of the data, and guides how data is secured, accessed, and retained.

Classification Scope Includes:

- **User Profile Information** (e.g., name, email, institutional role)
- **Attendance Information** (e.g., swipe records)
- **Submission Records** (e.g., files uploaded for applied juries)
- **Authentication Metadata** (e.g., institutional ID tokens, access logs)
- **Institution-Specific Configurations** (e.g., degree requirements, advising templates)

Associated Protections:

- **Encryption in Transit and at Rest** using TLS and AES-256 respectively
- **Role-Based Access Controls (RBAC)** to ensure only authorized users access institutional records
- **Logical Tenant Isolation** preventing data leakage across institutions
- **Access Logging and Review** to detect unauthorized access attempts
- **Support-only Access Model** to reduce surface area of internal exposure

If a more granular data classification schema is required (e.g., distinguishing FERPA-protected, public, and internal-use-only data), NoteForge is prepared to align with institution-specific data governance frameworks.

Company Data Dictionary:
A detailed data dictionary is included with this submission.

Network Firewall and IPS Policies:

Liszt uses DigitalOcean Managed Databases, which provide AES-256 encryption for data at rest and enforce TLS 1.2+ for all data in transit. Tenant data is logically separated by design in the application layer, ensuring that users can only access records relevant to their institution.

Data Encryption and Isolation Policies

Liszt employs strong encryption standards and logical data isolation techniques to protect institutional data both in transit and at rest. These safeguards are designed to ensure confidentiality, integrity, and tenant-specific access control, consistent with FERPA and HECVAT expectations.

Encryption in Transit

- All communication between users and the Liszt application (web browsers, API requests) is encrypted using TLS 1.2 or higher.
- Internal service communication (e.g., between application and database) also uses encrypted connections via TLS, as enforced by DigitalOcean Managed Databases.
- Only HTTPS traffic is permitted over the network; all HTTP traffic is redirected or blocked.

Encryption at Rest

- All institutional and user data is encrypted at rest using AES-256, including:
    - Managed database storage
    - Uploaded files and submission content
    - Backup archives stored offsite
- Backup data is also encrypted both during transmission and on disk, using encrypted volumes or cloud-native encryption policies.

Data Isolation

- Liszt is a multi-tenant application that uses a logical isolation model to separate data by institution.
- Every record in the system includes an ownership identifier that enforces strict access boundaries at the application level.

- Application queries are scoped to ensure that users can only access data affiliated with their institution.
- Institutional configurations (branding, policies, permissions) are also isolated, preventing cross-tenant interference.

Administrative Access

- Only authorized Liszt system administrators can access unencrypted data in raw form, and such access is limited to specific support requests or incident response tasks.
- All such access is logged and reviewed, and institutional consent is required for data inspection or recovery operations.

Role or Account Security Policies

Liszt uses OAuth-based authentication, delegating login and account security to each institution's identity provider. Role-based access is managed within Liszt, but authentication is handled externally, ensuring that security policies (e.g., password strength, login monitoring, SSO) align with each institution's standards.
For NDSU, Liszt integrates with Microsoft Azure Active Directory, which uses Duo MFA for enhanced login security.

Multifactor Authentication Policies

Because Liszt uses OAuth authentication, MFA enforcement is managed at the institution level through the connected identity provider.

At NDSU, Microsoft accounts secured with Duo two-factor authentication are used, ensuring administrative and user-level MFA compliance.

Liszt itself does not store passwords or manage MFA directly, allowing institutions to retain full control over authentication policies.

Summary of Incident Response Plan

Liszt maintains a structured incident response process to identify, contain, and mitigate security threats while ensuring transparency and institutional accountability.

Incident Handling Process

All incidents are handled according to a severity-based framework, inspired by industry standards such as NIST 800-61:

Identification:
Security events are detected via system logs, authentication failures, server monitoring tools, and user reports.

Classification:
Incidents are categorized by severity:

- **Low:** Minor bug or system anomaly with no impact on confidentiality or availability
- **Medium:** Unauthorized access attempt or elevated risk requiring mitigation
- **High:** Confirmed or suspected breach of institutional or user data

Containment & Investigation:
Upon detection of a high-severity event, steps are taken to isolate affected systems, restrict access, and begin forensic analysis.

Mitigation & Recovery:
Security patches, configuration updates, or rollback procedures are applied to resolve the incident. Data recovery procedures may be initiated if needed.

Notification & Reporting:
In the event of a confirmed or suspected breach involving institutional data, the affected institution (e.g., NDSU) will be notified within 48 hours of initial detection. Notification includes:

- Nature and scope of the incident
- Data types potentially impacted
- Actions taken to resolve or contain the issue
- Recommendations for follow-up by the institution

Postmortem Review:
All significant incidents are followed by an internal review and documentation process. Policy or technical changes may be made to reduce recurrence risk.

Logging and Recordkeeping

- Access attempts, administrative actions, and authentication failures are logged continuously.
- Logs are retained for at least 30 days, with longer retention possible for active investigations.

Summary of Business Continuity Plan

Liszt is designed to ensure high availability and rapid service restoration in the event of disruption, whether due to hardware failure, software issues, cyber incidents, or other unexpected outages. The platform incorporates backup, automation, and redundancy practices that support sustained operations and minimize downtime.

Data Backup and Protection

- **Nightly Encrypted Backups:**
  All institutional data, including application files and managed database contents, is backed up nightly to an offsite storage location. These backups are encrypted using AES-256 and stored in geographically separate infrastructure to reduce risk from localized failures.
- **Retention and Rotation:**
  Backups are retained in accordance with institutional requirements, with older snapshots rotated on a defined schedule to limit exposure while maintaining historical recovery points.

Automated Recovery and Redeployment

- **Infrastructure-as-Code (IaC):**
  Core Liszt services are defined using configuration files and deployment scripts (e.g., shell scripts, version-controlled server setup routines), allowing the entire platform to be redeployed on new infrastructure within hours.
- **Environment Reproducibility:**
  System dependencies, environment variables, file permissions, and security controls are documented and reproducible across staging and production environments to ensure consistency.

Business Continuity Testing

- **Regular Simulations:**
  Periodic internal recovery drills are performed to verify the completeness and reliability of backup data and deployment processes.
- **Monitoring and Alerts:**
  Uptime monitoring tools are used to detect outages and automatically alert technical staff in the event of downtime or degraded performance.

Disaster Recovery Plan

Liszt is equipped with a disaster recovery plan to ensure that services and institutional data can be restored in the event of a catastrophic failure, such as data center outages, infrastructure compromise, or major configuration corruption.

Redundant Hosting

- **Cloud-Based Architecture:**
  Liszt is hosted on cloud infrastructure that allows for geographically distributed resource allocation. While primary systems operate in a U.S.-based region, snapshots and backup data are stored offsite in separate physical availability zones.
- **Scalable Deployment Model:**
  Core application services can be migrated to alternate cloud nodes or providers using reproducible deployment procedures, minimizing disruption even in the event of provider outages.

Data Resilience

- **Backup Strategy:**
  All production data is backed up nightly and stored encrypted at rest. Backups include user data, configuration files, and metadata critical to full application restoration.
- **Verification Schedule:**
  Backup data is verified every 30 days through test restores and checksum validation to ensure file integrity and successful redeployment capability.

Documentation and Review

The disaster recovery plan is documented, reviewed annually, and updated as infrastructure, data volume, or service dependencies evolve.

Summary of Employee Background Check Policies

NoteForge is operated solely by its founder, Kyle Vanderburg, who is the only individual with access to production systems. As the sole proprietor, no additional employee background checks are applicable. If additional staff or contractors are brought on in the future, NoteForge will require appropriate background screening as a condition of access to institutional data.

Summary of Employee Confidentiality Agreement Policies

While there are currently no other employees, all future staff and contractors with access to sensitive systems or institutional data will be required to sign a confidentiality agreement and FERPA non-disclosure acknowledgment. Internal policies restrict data access to only what is necessary for operations and support.

Summary of Employee Training

NoteForge commits to ongoing professional development in areas of data privacy, FERPA compliance, and information security. As the developer of Liszt, Kyle Vanderburg conducts annual reviews of FERPA guidelines, incident response procedures, and higher ed compliance standards (e.g., via EDUCAUSE, NACUA, and NIST guidance). Security policies and data handling practices are reviewed and updated at least twice per year.

A letter of attestation of the company's latest Vulnerability/Pentest Attestation

FERPA Attestation

NoteForge affirms the following:

- We will not re-disclose FERPA-protected information without NDSU's permission or FERPA exceptions.
- NDSU retains ownership of all data; audit access is granted.
- All data is stored exclusively in the United States.
- NDSU has direct control over the deletion of personally identifiable information (PII).
- NDSU will be notified before any changes affecting data handling.
- Educational data is never used for commercial purposes.

Breach Notification Protocol:

In the event of a breach involving NDSU data:

- Liszt will notify NDSU within 48 hours of breach confirmation.
- A report including the scope, mitigation, and impact assessment will be delivered.
- Follow-up updates and a postmortem will be provided.
- A remediation plan will be implemented in coordination with NDSU if needed.

Please let us know if additional details or documentation is required.

Sincerely,
Kyle Vanderburg
NoteForge, LLC
liszt.app