Digilangua Security Policy

Reference Code: `DGL-SP-K01`
Prepared by: Digilangua Security Team

1. Introduction

At Digilangua LLC, we take data privacy and security seriously. Our digital language learning platform is designed with the privacy of students, teachers, and educational institutions in mind. This security policy outlines the measures we have implemented to ensure compliance with state and federal regulations such as FERPA, COPPA, and local Student Data Privacy Agreements.

2. Hosting Infrastructure

- Digilangua is hosted on **Amazon Lightsail (Ubuntu LTS)** servers.
- All infrastructure is located in **U.S.-based data centers**.
- Access to production servers is limited to authorized personnel via **SSH key-based login only**.
- All unused ports are blocked using a host-level firewall (`ufw`).
- **fail2ban** is used to detect and block repeated unauthorized access attempts.

3. Data Encryption

- All web traffic is served over **HTTPS** using **TLS 1.2+**.
- Passwords are stored using **strong one-way hashing** (PBKDF2, Django default).
- Backup archives and sensitive exports are **encrypted at rest** using GPG or encrypted S3 storage.
- Sensitive operations in the application are only accessible over encrypted channels.

4. Authentication and Access Control

- All developer and admin accounts are protected with **Two-Factor Authentication (2FA)**.
- Django Admin access is restricted to approved staff accounts with 2FA enabled using **TOTP (Google Authenticator)**.
- **No shared credentials** are used — all users authenticate with unique usernames.
- Role-based access control (RBAC) is implemented to ensure the principle of least privilege.

5. Patch and Vulnerability Management

- **Automatic system security updates** are enabled using `unattended-upgrades`.
- Dependencies are reviewed monthly. We use tools like `safety` and `bandit` to detect vulnerable Python packages.
- Only security-critical Python packages are updated immediately in production environments, after safe testing.

6. Monitoring and Logging

- All server-level activity and application logs are recorded and retained for **a minimum of 30 days**.
- Access logs, error logs, and login attempts are monitored regularly.
- Alerts are configured for suspicious activity using `fail2ban` and external monitoring tools like **Sentry**.

---

7. Backups and Disaster Recovery

- Daily automated backups of databases and uploaded files are performed.
- Backups are stored securely in an encrypted storage solution.
- Backup restoration procedures are tested **monthly** to ensure recoverability.

---

8. Incident Response Plan

- Digilangua maintains a **documented Incident Response Plan (IRP)**.
- All security incidents are triaged and logged internally.
- In the event of a data breach affecting student or teacher information, we will notify the affected LEAs and districts **within 72 hours** of discovery or sooner as required by law.

---

9. Data Collection and Retention

- Digilangua collects only **minimal necessary information**:
  - Student: name, email, password
  - Teacher: name, email, password, Stripe account (if applicable)
- We do **not** collect biometric, behavioral, health, or geolocation data.
- Data is retained only for the duration of the educational use agreement. Upon termination, data is deleted within **60 days** unless otherwise instructed.

---

10. Subprocessors and Third-Party Services

- Digilangua uses trusted subprocessors including:
  - **Amazon Web Services** (hosting, backup storage)
  - **Stripe** (teacher payments)
- All subprocessors are under strict contractual agreements to comply with equivalent privacy and security obligations.

---

11. Staff Policies and Training

- All staff and developers with access to student or teacher data:
  - Undergo **criminal background checks**
  - Receive annual **FERPA and data privacy training**
  - Are subject to strict internal access control and confidentiality agreements

---

12. Compliance Framework

Digilangua aligns with the **CIS Critical Security Controls v8 (Implementation Group 1)**, focusing on:

- Secure configurations
- Account access control
- Patch and vulnerability management
- Incident response
- Data protection and audit logging

We commit to continuously improving our security posture and reviewing this policy **annually** or upon any material changes.

Note: Some of the features are under development or under maintenance.

13. Contact

For questions about this policy or to report a security concern, please contact:

Digilangua Security Team
✉ info@digilangua.co 📞 (518)593-9881