Technical Security Specifications for Services

Purpose and Scope

This document defines the technical and organizational measures implemented by unihelper.io to ensure the confidentiality, integrity, and availability of data processed within its Services.

It applies to all unihelper.io infrastructure, software systems, integrations, and personnel with access to production environments or customer data.

This specification operates in conjunction with and supports the following documents:

- Information Security Policy
- Systems Management Policy
- Incident Response Plan
- Business Continuity and Disaster Recovery Plans
- Data Processing Agreement

Hosting and Infrastructure Security

- **Data Center Compliance:** Unihelper.io Services are hosted in ISO 27001 and SOC 2 certified data centers located within the European Union.
- **Network Security:** Firewalls, virtual private cloud (VPC) isolation, and intrusion detection/prevention systems protect all environments.
- **Environment Segregation:** Development, staging, and production systems are logically separated.
- **Patch and Vulnerability Management:** Regular vulnerability scans, patching, and security assessments are performed in accordance with the Systems Management Policy.
- **Availability:** 24/7 infrastructure monitoring ensures service reliability and early detection of performance issues.

Data Encryption

- **Data at Rest:** All stored data, including backups, is encrypted using AES-256 or stronger algorithms.
- **Data in Transit:** All data transmitted between clients, APIs, and systems is encrypted using TLS 1.2 or higher.
- **Password Security:** User credentials are hashed and salted using industry-standard algorithms (e.g., bcrypt).

Access Control

- **Role-Based Access Control (RBAC):** Access to systems and data is granted according to job role and business necessity, following the principle of least privilege.
- **Session Management:** User sessions expire automatically after a defined period of inactivity.
- **Access Reviews:** All permissions are reviewed quarterly in accordance with Systems Management Policy, and immediately revoked upon role change or offboarding.
- **Audit Logging:** All privileged access is logged, retained for a minimum of 12 months, and reviewed regularly.

Application Security

- **Secure Development Lifecycle (SDLC):** Development follows the Unihelper.io SDLC Policy, incorporating code review, dependency scanning, and change control.
- **Code Review and Testing:** All changes are tested using E2E testing in a production-like environment before deployment.
- **Dependency Management:** Third-party libraries are continuously monitored for vulnerabilities.
- **API Security:** APIs employ OAuth 2.0 and token-based authentication.
- **OWASP Compliance:** The platform incorporates protections against OWASP Top 10 vulnerabilities, including SQL injection, XSS, and CSRF.
- **Penetration Testing:** Annual third-party penetration tests are conducted, and all findings are tracked through the Change Management Process (Systems Management Policy).

Monitoring, Logging, and Incident Response

- **Centralized Logging:** Application and infrastructure logs are aggregated and monitored continuously.
- **Alerting:** Automated alerts trigger for suspicious activities, including repeated failed logins, data exports, and privilege escalations.
- **Retention:** Operational logs are retained for 90 days; security event logs are retained for 12 months.
- **Incident Handling:** All incidents are managed according to the Incident Response Plan 2025, with breach notifications made within 24 hours in line with DPA.
- **Evidence Preservation:** Logs and artifacts related to incidents are preserved for forensic analysis as defined in the Incident Response Plan.

Data Retention, Anonymization, and Deletion

- **Retention Periods:** Data is deleted as required for contractual or legal obligations defined in the DPA.
- **Anonymization:** When a course or customer account is archived, all personal data is anonymized in accordance with the Services Anonymization Methodology and DPA.

- **Deletion:** Upon termination or request, personal data is securely deleted or returned within 30 days, following NIST SP 800-88 standards.
- **Verification:** Deletion completion is documented and certified.
- **Backups:** Encrypted backups may contain deleted data until expiry of the retention schedule, after which they are purged automatically.

Backup, Business Continuity, and Disaster Recovery

- **Backups:** Daily automated backups of all production databases are performed.
- **Encryption:** Backups are encrypted using AES-256.
- **Recovery Objectives:**
    - **Recovery Point Objective (RPO):** 12 hours
    - **Recovery Time Objective (RTO):** 24 hours
- These objectives mirror those in the Disaster Recovery Plan and are validated annually during Business Continuity Plan reviews.

Third-Party and Sub-Processor Security

- **Vendor Evaluation:** All third-party providers and sub-processors undergo risk assessment before onboarding, per Systems Management Policy and DPA.
- **Contractual Controls:** Security, confidentiality, and audit obligations are embedded in all vendor contracts.
- **Sub-Processor Register:** Maintained and updated in accordance with DPA Annex II.
- **Monitoring:** Vendors are reviewed annually for continued compliance with GDPR and Unihelper.io's security requirements.

Compliance and Governance

- **Standards Alignment:** Unihelper.io aligns its information security framework with ISO 27001, GDPR, and FERPA principles.
- **Policy Integration:** This document operates in conjunction with Unihelper.io's Information Security, Systems Management, and Data Protection policies.
- **Audit and Review:** All technical controls are reviewed annually or following material changes to the platform, coordinated with the ISO 27001 internal audit cycle and documented in the Change Management Register (Systems Management Policy).
- **Change Control:** Updates are approved by the Data Protection & Information Security Officer (DPISO) and recorded in the document revision history.