Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

Security Concept

Date: 01-04-2024.

1. Objectives

To ensure the confidentiality, integrity, and availability of Brytend Software and its data, and to comply with applicable legal, regulatory, and contractual obligations. This security concept outlines the principles, practices, and controls implemented to protect the software platform and its users.

2. Scope

This security concept applies to all components of the Brytend SaaS platform, including internal systems and infrastructure, employees and subcontractors, and third-party integrations and APIs. It encompasses both technical and organizational measures to safeguard data and services.

3. Security Principles

Brytend Software adheres to the following security principles:

- Least Privilege: Access is granted only as needed.
- Defense in Depth: Multiple layers of security controls are implemented.
- Zero Trust: Continuous verification of users and devices.
- Privacy by Design: Data protection is embedded into the system architecture from the outset.

4. Access Control

Access to systems and data is managed through role-based access control (RBAC). Multi-factor authentication (MFA) is enforced for administrative and privileged accounts. All access attempts are logged and monitored. Access is revoked immediately upon role change or termination of employment.

5. Data Protection

All data in transit is encrypted using TLS 1.2 or higher, and sensitive data at rest is encrypted using AES-256. Regular backups are performed and stored securely offsite. Data retention and deletion policies are aligned with GDPR and other applicable regulations.

6. Application Security

Brytend Software follows a secure development lifecycle (SDLC) that includes code reviews and automated security testing. Regular vulnerability scans and penetration tests are conducted. The application is designed to comply with the OWASP Top 10 security risks. APIs are protected with OAuth 2.0 authentication.

7. Infrastructure Security

The platform is hosted on secure cloud infrastructure with network segmentation and firewall rules to isolate environments. Continuous monitoring is in place with intrusion detection and prevention systems (IDPS). Patch management and automated updates ensure systems remain secure.

8. Incident Response

A documented incident response plan (IRP) is maintained. The system is monitored 24/7 with alerting mechanisms. Roles and responsibilities for incident handling are clearly defined. Post-incident reviews and root cause analyses are conducted to prevent recurrence.

9. Third-Party and Subcontractor Management

All vendors and subcontractors undergo security assessments. Data processing agreements (DPAs) are in place. Access to customer systems is granted only with prior written consent and is limited to what is necessary for contract performance. The End User is notified immediately if access roles change.

10. Compliance

Brytend Software aligns its practices with GDPR, ISO 27001, and NIS2. Regular internal audits are conducted. A Data Protection Officer (DPO) is appointed to oversee compliance and data protection efforts.