Data Security & Encryption Statement

At BeneluxSoft B.V., we take information security seriously. As a technology-driven company delivering cloud transformation, AI solutions, cybersecurity consultancy and EU-funded project services, we are committed to implementing industry-leading standards to protect the confidentiality, integrity and availability of all data processed through our systems and services.

This statement outlines the key security principles, controls and encryption practices we apply across our infrastructure and operations, in line with ISO/IEC 27001, GDPR Article 32, and recognised cybersecurity frameworks.

1. Security Governance & Compliance

We design and operate all systems following internationally recognised security frameworks, including:

ISO/IEC 27001 – Information Security Management Principles

Although not all company units are “formally certified”, we align our internal controls with ISO 27001 clauses covering:

- Access Control
- Cryptographic Controls
- Operations Security
- Physical & Environmental Security
- Supplier Security
- Backup & Continuity Management
- Logging & Monitoring

GDPR Article 32 – Security of Processing

Our technical and organisational measures comply with GDPR requirements for:

- Pseudonymisation & encryption
- Ensuring ongoing confidentiality, integrity and availability of systems
- Regular testing & evaluation of security measures
- Incident identification & response procedures

NATO & EU Cybersecurity Expectations

For collaborations involving defence-related innovation, secure software engineering or governmental digital transformation projects, we follow:

- NATO STANAG-referenced basic security practices
- EU Cybersecurity Framework (ENISA)
- CERT & NCSC Coordinated Vulnerability Disclosure guidelines

These principles ensure that sensitive project, client or research data is handled in a secure and compliant manner.

2. Data Encryption Standards

We use strong encryption to safeguard data both in transit and at rest.

Encryption in Transit

All communication between your browser, our website and cloud services is encrypted using:

- TLS 1.2+ or TLS 1.3
- Forward secrecy ciphers
- HSTS (HTTP Strict Transport Security)
- Secure DNS (DNSSEC where supported)

This ensures that no third party can intercept or modify data exchanged between endpoints.

Encryption at Rest

Depending on the system, data is stored using:

- AES-256 encryption for databases, storage buckets and backups
- Encrypted volumes for servers and cloud workloads
- Key rotation policies applied regularly
- Strict access control enforced at storage level

We ensure that encryption keys are not stored alongside encrypted data.

3. Infrastructure Security

Our infrastructure is designed according to zero-trust principles.

Secure Hosting Environment

We host our systems on reputable cloud providers with:

- ISO 27001 / ISO 27017 / ISO 27018 certified datacenters
- Physical access controls
- Redundant power & cooling
- 24/7 monitoring

Network Security

We apply layered network security controls:

- Firewalls and WAF (Web Application Firewall)
- DDoS protection
- Network segmentation
- IP/port restrictions on sensitive systems
- Continuous vulnerability scanning

Application Security

Our development and deployment practices include:

- Secure coding standards
- Code reviews
- Dependency vulnerability scanning
- API security hardening
- Secrets management
- Regular patching and updates

For AI and ML-based systems, we apply additional safeguards to prevent model extraction attacks, prompt injection and data leakage.

4. Access Control & Identity Management

We enforce strict access control rules across all systems:

- Role-Based Access Control (RBAC)
- Strict “least privilege” principle
- Multi-factor authentication (MFA) wherever possible
- Password policies aligned with NIST & ENISA guidelines
- Session timeout and device restrictions for admin roles
- Privileged access logs and security alerts
- Administrative access is restricted to authorised personnel only.

5. Data Backup & Business Continuity

We maintain secure and redundant backup systems to ensure operational continuity:

- Regular automated backups of critical systems
- Encrypted backup storage
- Geo-redundant backup locations (where applicable)
- Continuous recovery testing
- Documented incident recovery procedures

This ensures service continuity even in the event of failure or disruption.

6. Monitoring, Logging & Threat Detection

To ensure system integrity and early detection:

- Security logs are stored in protected environments
- Suspicious activity is automatically flagged
- IDS/IPS and anomaly detection tools may be used
- Audit trails are maintained for sensitive actions
- Regular risk assessments and penetration tests

Logs are reviewed in accordance with GDPR and data minimisation principles.

7. Supplier & Third-Party Security

We work only with reputable suppliers and cloud providers who:

- Adhere to ISO 27001 and GDPR

- Provide DPAs (Data Processing Agreements)
- Undergo regular security audits
- Offer clear data retention & deletion guarantees

Third-party access is tightly restricted and continuously monitored.

8. Incident Response & Vulnerability Handling

We maintain internal procedures for identifying, assessing and responding to security incidents.

Incident Response Capabilities Include:

- Immediate containment actions
- Forensic investigation
- Root-cause analysis
- System recovery & hardening
- Notification to authorities and affected users when required by law (GDPR Article 33 & 34)

Coordinated Vulnerability Disclosure

BeneluxSoft follows recognized CERT / NCSC CVD guidelines, allowing ethical researchers and partners to report vulnerabilities safely.

A dedicated Responsible Disclosure Policy is published separately.

9. Data Retention, Minimisation & Deletion

We ensure:

- Only necessary data is collected (GDPR data minimisation principle)
- Retention limits follow legal and operational requirements
- Secure deletion using industry-standard sanitization
- Anonymisation where full deletion is not possible

Data retention details for personal data are outlined in our Privacy Policy.

10. Your Responsibilities

Security is a shared responsibility. We ask users to:

- Keep their systems updated
- Use strong passwords
- Avoid sharing sensitive information over unsecured networks
- Report suspicious activity
- Follow secure practices when interacting with our services

11. Contact Information

For any security-related questions or concerns, please contact us at: https://beneluxsoft.com/contact/

Email: erhan.akkilik@beneluxsoft.com

Phone: +32 484 53 00 39

Authorized Signatory:

Name: Aden Joseph OZSOY

Title: Co-Founder

Year : 2024