SECURITY REQUIREMENTS FOR DUE DILIGENCE

ABSTRACT

The following security requirements are a necessity for a due-diligence (DD) assessment.

Due diligence is the investigation or exercise of care that a business or person is expected to take before entering an agreement/contract with another party

Please review and confirm these requirements and attach the relevant files. This is a necessary step for the DD assessment and will allow an efficient completion of the assessment.

GENERAL

Please provide an in-depth description of your various environments and solution architecture:

SECURITY REQUIREMENTS

1. Policies and Regulations

- In case of compliance with any regulations or certificates such as ISO-27002, PCI-DSS, SOC2 and so on, specify which regulations/certificates.
  In case of a regulation with certification, please attach the latest documentation regarding the certification.

2. Passwords and Encryption

Please verify these requirements and attached the relevant documentation:

- Sensitive data classification
- Encryption guidelines
- Password and encryption keys management
- Password policy (office, cloud, application, etc..)
- MFA (if exists)

3. Account Management

Please verify these requirements and attached the relevant documentation:

- User creation/removal procedure.
- Permissions granting/revoking process.

- Identity and access management – who can access the following:
  - Admin access to servers/endpoints
  - DBs
  - Cloud production environment
  - Code repositories

4. Backups and Recovery

Please verify these requirements and attached the relevant documentation:

- Backup and restoration policy
- Periodic restoration tests procedure
- DR policy and procedure

Comment:	Click or tap here to enter text.

5. Audit and Monitoring

Please verify these requirements and attached the relevant documentation:

- Logging and audit policy (application, security systems, cloud systems, etc..)
- SIEM/SOC architecture and policy

6. Network and Server Hardening

Please verify these requirements and attached the relevant documentation:

- Server hardening policy/baseline
- Endpoint hardening policy/baseline
- Change procedure and patch management
- Firewall rules authorization process
- Developer access to production environment and data
- Data and network segregation

7. Secure Development Lifecycle (SDLC)

Please verify these requirements and attached the relevant documentation:

- Security development guidelines document
- Code deployment procedures
- Developer security training history (syllabus, etc..)
- Past security code reviews results/reports
- Code management and authentication guidelines and policies
- QA procedures

8. Personal Security Policy

Please verify these requirements and attached the relevant documentation:

- Clean desk policy
- Data destruction policy
- Mobile policy
- Wireless policy

9. Physical Security Policy

Please verify these requirements and attached the relevant documentation:

- Physical access control
- Badging and identification
- Video surveillance and alarm systems
- Security stuff and awareness training
- Logging

In addition to the requirements stated above, please attach the following files:

- ☐The latest penetration testing report
- ☐Updated open sources list in your system
- ☐Technical documentation (Architecture diagram, IT stack)
- ☐API documentation
- ☐Data flow diagram
- ☐System architecture