

VENDOR SECURITY QUESTIONNAIRE

INSTRUCTIONS

This questionnaire is designed to assess the security posture and risk profile of third-party vendors. Please provide complete and accurate responses to all questions. Where applicable, attach supporting documentation such as certifications, audit reports, or policy documents. If a question is not applicable, please indicate "N/A" and provide a brief explanation.

SECTION 1: VENDOR INFORMATION

1.1 Vendor Legal Name:

1.2 Vendor Primary Contact Name and Title:

1.3 Vendor Primary Contact Email:

1.4 Vendor Primary Contact Phone:

1.5 Service Type/Description:

Please describe the services to be provided in detail

1.6 Contract Start Date (if known):

1.7 Contract Duration:

1.8 Number of Employees:

1.9 Primary Business Locations:

List all relevant locations

1.10 Years in Business:

SECTION 2: DATA PROTECTION & PRIVACY

2.1 Data Handling

2.1.1 What types of data will you collect, process, or store on our behalf?

Include personal data, sensitive data, financial data, intellectual property, etc.

2.1.2 Where will our data be stored (geographic locations)?

2.1.3 Will our data be transferred across borders? If yes, which countries?

2.1.4 Do you use sub-processors or third parties to process our data? If yes, please provide details.

2.1.5 What is your data retention policy?

2.1.6 What is your data disposal/destruction process?

Include methods and timeline

2.2 Encryption & Data Security

2.2.1 What encryption standards do you use for data at rest?

Specify algorithm (e.g., AES-256) and key management practices

2.2.2 What encryption standards do you use for data in transit?

Specify protocols (e.g., TLS 1.3)

2.2.3 How are encryption keys managed and stored?

2.2.4 Do you support client-side encryption or bring-your-own-key (BYOK)?

2.2.5 Are backups encrypted? If yes, using what method?

2.3 Privacy & Compliance

2.3.1 What privacy regulations do you comply with?

E.g., GDPR, CCPA, PIPEDA, LGPD, etc.

2.3.2 Do you have a Data Protection Officer (DPO) or privacy lead?

2.3.3 What is your breach notification timeline?

How quickly will you notify us of a data breach?

2.3.4 Do you have cyber insurance? If yes, what is the coverage amount?

2.3.5 Will you sign our Data Processing Agreement (DPA)?

SECTION 3: ACCESS CONTROLS & AUTHENTICATION

3.1 What authentication methods are supported?

E.g., password, MFA, SSO, biometrics

3.2 Is multi-factor authentication (MFA) available? Is it mandatory?

3.3 Do you support single sign-on (SSO)? Which protocols?

E.g., SAML 2.0, OAuth 2.0, OpenID Connect

3.4 What is your password policy?

Include minimum length, complexity requirements, expiration

3.5 How are privileged accounts managed?

3.6 What role-based access control (RBAC) capabilities do you provide?

3.7 How frequently are access rights reviewed?

3.8 What is your user deprovisioning process?

How quickly are accounts disabled after termination?

3.9 Do you maintain audit logs of user access and activities?

3.10 How long are audit logs retained?

3.11 Can we access our audit logs? If yes, how?

SECTION 4: NETWORK & INFRASTRUCTURE SECURITY

4.1 Describe your network architecture and segmentation strategy.

4.2 What perimeter security controls are in place?

E.g., firewalls, IDS/IPS, DDoS protection

4.3 Do you perform regular vulnerability scanning? How frequently?

4.4 Do you conduct penetration testing? How frequently?

4.5 When was your last penetration test and what were the findings?

4.6 How are identified vulnerabilities remediated and tracked?

4.7 What is your patch management process and timeline?

Critical, high, medium, low vulnerabilities

4.8 Do you use a Web Application Firewall (WAF)?

4.9 What anti-malware/endpoint protection solutions do you use?

4.10 Do you maintain separate development, testing, and production environments?

SECTION 5: BUSINESS CONTINUITY & DISASTER RECOVERY

5.1 Do you have a documented Business Continuity Plan (BCP)?

Please attach a copy or executive summary

5.2 Do you have a documented Disaster Recovery Plan (DRP)?

Please attach a copy or executive summary

5.3 When were these plans last tested?

5.4 What is your Recovery Time Objective (RTO)?

5.5 What is your Recovery Point Objective (RPO)?

5.6 Where are backup data centers/sites located?

5.7 How frequently are backups performed?

5.8 How frequently are backup restorations tested?

5.9 What is your guaranteed uptime/availability?

E.g., 99.9%, 99.99%

5.10 Do you have redundant infrastructure for critical systems?

5.11 What is your incident escalation process?

SECTION 6: COMPLIANCE & CERTIFICATIONS

6.1 What security certifications do you hold?

E.g., ISO 27001, SOC 2 Type II, PCI DSS, HITRUST, FedRAMP

6.2 When do these certifications expire?

6.3 Please attach current certification reports or letters of attestation.

6.4 What industry-specific regulations do you comply with?

E.g., HIPAA, GDPR, PCI DSS, SOX, GLBA

6.5 Do you undergo regular third-party security audits?

6.6 When was your last audit and what was the outcome?

6.7 Do you have an independent audit of your controls (e.g., SOC 2)?

Please provide the most recent report

6.8 Are you compliant with industry-specific frameworks?

E.g., NIST CSF, CIS Controls, PCI DSS

SECTION 7: INCIDENT RESPONSE & SECURITY OPERATIONS

7.1 Do you have a documented Incident Response Plan?

Please attach or provide summary

7.2 Do you have a dedicated security operations center (SOC)?

7.3 What security monitoring tools and processes do you use?

E.g., SIEM, log aggregation, threat intelligence

7.4 How do you detect and respond to security incidents?

7.5 What is your incident notification process and timeline?

How quickly will you notify customers of incidents?

7.6 Who is the primary contact for security incidents?

Provide 24/7 contact information

7.7 Have you experienced any security breaches in the past 3 years?

If yes, please describe

7.8 Do you conduct security awareness training for employees?

7.9 How frequently is security training conducted?

7.10 Do you have a bug bounty or vulnerability disclosure program?

SECTION 8: PHYSICAL & ENVIRONMENTAL SECURITY

8.1 Who owns/operates your data centers?

If using third-party (AWS, Azure, GCP), please specify

8.2 What physical security controls are in place at data centers?

E.g., biometric access, 24/7 guards, CCTV

8.3 What environmental controls are in place?

E.g., fire suppression, temperature/humidity control, power redundancy

8.4 Do data centers have redundant power sources?

8.5 Are data centers in flood zones or other high-risk areas?

8.6 What physical security controls are in place at office locations?

8.7 How is physical media (hard drives, tapes) secured and disposed of?

SECTION 9: APPLICATION SECURITY

9.1 What secure software development lifecycle (SDLC) practices do you follow?

9.2 Do you perform static application security testing (SAST)?

9.3 Do you perform dynamic application security testing (DAST)?

9.4 Do you conduct code reviews? Are they peer-reviewed or automated?

9.5 How do you manage third-party libraries and dependencies?

E.g., vulnerability scanning, updates

9.6 What is your software update and patching process?

9.7 How much advance notice do you provide for updates and changes?

9.8 Do you maintain a software bill of materials (SBOM)?

9.9 How do you secure APIs?

E.g., authentication, rate limiting, input validation

9.10 Do you use secure coding standards?

E.g., OWASP Top 10, SANS Top 25

SECTION 10: VENDOR MANAGEMENT & PERSONNEL SECURITY

10.1 Do you conduct background checks on employees?

If yes, what type and frequency?

10.2 Are employees required to sign confidentiality/NDA agreements?

10.3 What is your employee onboarding security process?

10.4 What is your employee offboarding security process?

10.5 Do you use contractors or offshore resources?

If yes, in which countries?

10.6 How do you vet and manage your subcontractors?

10.7 Do you have security requirements in contracts with subcontractors?

10.8 What percentage of your workforce is remote?

10.9 What security controls are in place for remote workers?

SECTION 11: SERVICE LEVEL AGREEMENTS

11.1 What are your guaranteed service levels (uptime, performance)?

11.2 What are the penalties for not meeting SLAs?

11.3 What is your standard support response time?

Critical, high, medium, low priority

11.4 Do you offer 24/7 support?

11.5 What support channels are available?

E.g., phone, email, chat, portal

11.6 What is your planned maintenance window schedule?

11.7 How much advance notice is provided for planned maintenance?

11.8 Do you provide a status page for service availability?

SECTION 12: DATA RIGHTS & PORTABILITY

12.1 Who owns the data we provide to you?

12.2 What data export capabilities do you provide?

Formats, frequency, automation

12.3 What is your process for returning or deleting our data upon contract termination?

Include timeline

12.4 Do you retain any data after contract termination? If yes, why and for how long?

12.5 Can you provide data in a structured, machine-readable format?

12.6 What is your data portability process?

12.7 Do you support customer-initiated data deletion requests?

SECTION 13: ADDITIONAL INFORMATION

13.1 Are there any current or pending lawsuits against your organization?

13.2 Are there any current or pending regulatory actions against your organization?

13.3 Have you experienced any financial difficulties in the past 3 years?

13.4 Do you have business interruption insurance?

13.5 What is your process for communicating security updates to customers?

13.6 Do you have a customer security advisory board or council?

13.7 Will you allow us to conduct our own security assessment?

E.g., questionnaires, audits, site visits

13.8 What frequency of security reviews/assessments do you allow?

SECTION 14: ATTESTATION & SIGNATURE

I hereby certify that the information provided in this questionnaire is complete, accurate, and true to the best of my knowledge. I understand that this information will be used to assess our organization's security posture and that any misrepresentation may result in disqualification from consideration or termination of contract.

Name: _____

Title: _____

Company: _____

Date: _____

Signature: _____

REQUIRED ATTACHMENTS

Please attach the following documents with your completed questionnaire:

- Current security certifications (ISO 27001, SOC 2, etc.)
- Most recent third-party audit report or executive summary
- Business Continuity Plan (executive summary acceptable)
- Disaster Recovery Plan (executive summary acceptable)
- Incident Response Plan (executive summary acceptable)
- Data Processing Agreement (DPA) template
- Cyber insurance certificate
- Any other relevant security documentation