

Questionnaire



Supplier Security Assurance

2023



**Security Assurance Questionnaire**

1. Is your organisation ISO-27001 certified? If yes, please provide the certificate.
2. How does your organisation plan and prepare for a cybersecurity incident? What processes does your organisation have in place to respond to an incident?
3. How does your organisation specifically protect customer information?
4. How does your organisation ensure the protection of *data in transit* and *data at rest*?
5. Does your organisation use TLS and SSH certificates to ensure data exchanges are secure?
6. What are the encryption standards followed by your organisation?
7. Does your organisation install security patches for systems, networks, and software?
8. Where is client data stored and how is it protected?
9. Does your organisation have a disaster recovery policy/periodic tests? Please provide a copy of the policy and an example.
10. Do you have a data retention policy? Specifically, how long is client data stored and how is it made available on-demand?
11. Please provide evidence of adherence to data protection and privacy regulations (for example EU-GDPR) applicable in the region(s) your organisation operates.
12. Please share your Information Security Policy for review (link or attachment).
13. Please provide a Service Level Agreement and Terms of service for review (link or attachment).
14. How do you grant and revoke access to systems and data? Do you implement multi-factor authentication for privileged accounts?
15. Please describe the process for reporting security incidents to our organization promptly and efficiently.
16. Do you have a secure and anonymous channel for reporting potential security vulnerabilities or concerns?
17. Have you conducted any security audits or received compliance certifications from third-party auditors? If yes, please provide the relevant reports.
18. How do you handle data subject access requests and data deletion requests to comply with privacy regulations?
19. What procedures do you have in place for the secure disposal of data, including hardware and media containing sensitive information?