We Make IT Work

Braver®

THIRD-PARTY VENDOR CYBERSECURITY QUESTIONNAIRE

The Third-Party Vendor Cybersecurity Questionnaire is a concise set of questions aimed at evaluating a vendor's cybersecurity practices. Covering key areas like security policies, access controls, incident response, and more, it provides businesses with essential insights to ensure the security and compliance of their external partners.

Security Policies and Procedures:

- Does the vendor have a written cybersecurity policy that is regularly updated and reviewed?

Access Controls:

- Does the vendor have a policy for monitoring and managing user access?

Endpoint Security:

- How often does the vendor update EDR solutions, and how often are security patches deployed?
- What is the vendor's integration process for anti-virus protection, and how do they ensure compatibility with the existing security setup?

Network Security:

- What measures are in place to vet and monitor third-party vendors for security compliance?
- What encryption protocols are utilized for data in transit?

Incident Response and Reporting:

- Does the vendor have a response plan in place in the event of a breach?
- How quickly can the vendor's team respond to and report a cybersecurity incident?
- Does the Vendor have 24x7 Live SOC for monitoring and remediation of security issues?

Data Protection:

- Does the vendor have a data protection strategy in place?
- Describe the vendor's data backup and recovery processes.
- Security Training and Awareness:
- Outline the vendor's employee cybersecurity training programs.
- How does the vendor ensure ongoing awareness of the latest security threats?

Vulnerability Management:

- Does the vendor regularly conduct security audits and vulnerability assessments?
- How does the vendor identify and address vulnerabilities in their systems?
- What is the frequency of vulnerability assessments?

Third-Party Security:

- How does the vendor ensure the security of third-party applications and services they integrate?

Regulatory Compliance:

- Provide information on the vendor's compliance with relevant cybersecurity regulations.
- How does the vendor stay abreast of changes in regulatory requirements?

Security Incident History:

- Has the vendor experienced any significant cybersecurity incidents in the past two years?
- If yes, provide details on the incidents and the measures taken to address them.

Insurance Coverage:

- Does the vendor have cybersecurity insurance, and what does it cover?
- What does the coverage amount in case of a data breach?
- Future Security Enhancements:
- What plans does the vendor have for enhancing cybersecurity measures in the future?
- How does the vendor stay ahead of emerging cybersecurity threats?

Organizational Structure:

- Does the vendor have a dedicated cybersecurity team and/or a chief information security officer?
- How often does the vendor update EDR solutions, and how often are security patches deployed?