CyberSecure™ MY BUSINESS
PLAN. PROTECT. RESPOND.

NATIONAL CYBERSECURITY ALLIANCE

SECURITY VENDOR QUESTIONNAIRE

Choosing a vendor to meet your cybersecurity needs is not an easy task. To help you, we have created this checklist with some questions you should consider asking current or potential vendors. it is not exhaustive, but gives you a good start. If you don't understand some or any of these questions, consider having a business partner or colleague help you interview vendors. And always remember to engage in a Service Level Agreement and Contract with the vendor so all expectations are clearly articulated.

☐ Does your company have a pre-employment screening policy for employees and contractors? What is that process? What is your process for training them on security best practices?

☐ Does your company have a written controls plan that contains the administrative, technical and physical safeguards you use to collect, process, protect, store, transmit, dispose or otherwise handle our data (e.g., Information Security Plan)?

☐ Does the system or application which will be storing our company data provide access control mechanisms (e.g., unique user IDs, passwords standards, role based access)? Please elaborate.

☐ How will you help me comply with all applicable privacy and security laws for my business?

☐ What certifications if any does your company have (ex. ISO 27001, SOC, etc.) and can you provide documentation?

☐ Does the system or application provide multi-tenant controls for separation of users and data within the service?

☐ Does your company utilize encryption methods for data in transit and data at rest where technically possible and legally permissible?

☐ Are files and records reviewed, retained and purged in accordance with legal requirements, contractual obligations and service level agreements?

☐ What is your process for purging all files and records and removing accesses upon completion of the service, task, or contract?

☐ What is your commitment to response time if I have a question or emergency? Do you have "off" hours? What is the best way to reach someone

CyberSecure™
MY BUSINESS
PLAN. PROTECT. RESPOND.

NATIONAL
CYBERSECURITY
ALLIANCE

SECURITY VENDOR QUESTIONNAIRE

□ Does your company have written business continuity/disaster recovery Plans, which are tested on a periodic basis? Please elaborate.

□ Does your company ensure adequate steps are taken to guard against unauthorized access to our company Data (e.g., firewall)? Please list the technology and processes that are in place.

□ Does your company maintain up-to-date versions of anti-virus software, anti-malware, antispyware, and operating systems security patches? Please elaborate.

□ What will your company actively do to prevent security incidents or breaches, and how often do you plan to check for vulnerabilities? Please elaborate.

□ Does your company have a written plan to promptly identify, report, and respond to breaches of security related to our company data (e.g., incident response plan)?

□ Would our company retain ownership of its data at all times?

□ Does your company hire an external audit firm to perform a compliance review of your operational controls?

□ Will third party vendors (e.g., subcontractor, managed shared hosting) used by your company be restricted from having access to the system or application data of our company?

□ Does your company provide assurance (in the form of a written report) of your and your third-party vendor's security and controls while customer data is being collected, processed and retained?

□ Can your company, and any relevant third-party service provider your company contracts with, send the results of your last security audit?

□ What specific services are included in my monthly service fee? What services will be an additional fee?

ADDITIONAL RESOURCES

☑ **FTC:** Vendor Security Basics
https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/vendor-security

☑ **NCSA**: Own Your Role in Cybersecurity: Start With the Basics
https://staysafeonline.org/resource/own-your-role-in-cybersecurity/