Ver 1.0

The ASCII Group Community:

The set of questions below are being provided to vet potential vendors on their security posture. This document is based on feedback received by fellow ASCII MSPs who reside on the ASCII Security Committee. By each member reinforcing the ideals below, our collective voice will help push the industry forward.

Existing Compliance:

Do you adhere to one or more of the following cybersecurity standards or frameworks?

NIST CSF
NIST 800-53 specify revision
NIST 800-171 specify revision
CIS Top Controls
CMMC, specify level
ISO 27001/27002
FedRAMP

Product Development:

Do you follow a standard SDLC (secure development lifecycle)?
What protocols are in place regarding third party access to client data?
Is two-factor authentication available on admin access?
What controls are in place regarding your supply chain for patches and updates?
What protocols are in place for test accounts? Access? Removal?
Do developers have access to production data?

Product Testing:

Do you have a Vulnerability Disclosure Program (VDP) in place? – If so, please provide a link.
Does your VDP contain a bug bounty program?
Does your bounty program require an NDA on items submitted via it?
Has your code base been reviewed by a third party? If so, please provide a report or link to a report on their findings.
Do you have a system in place for MSPs to report security concerns?

Internal Security:

Do you have an internal security awareness training program?
If your workforce is remote, what safeguards are in place for access to code base and client data?
Are workstations for remote access to your back-end systems private or corporate controlled?
Do you have a CISO on staff? As part of your corporate structure, do you plan to hire a CISO on staff?
Do you have an incident response plan to handle incidents involving one/multiple customers?
Is this incident response plan practiced?

Product Security:

Where is your data stored? Who has access to the data? Where are they located?
Is the data encrypted at rest and in transit? If so, is this keyed per client, etc.?
Do you have two-factor authentication for all parties? Can we integrate SAML/OIDC authentication?
Does your product ship a default secure configuration with regards to encryption and authentication?
Do these security measures require 3rd party products?

Third-Party Risk:

Do you use 3rd party platforms as part of your solutions?
Do you outsource any technical or cybersecurity operations outside the United States? If so, where?
Do you outsource any development outside the United States? If so, where?
Do you have a vendor risk management process in place for your critical vendors?
What insurance coverages do you require of your critical vendors?
What contractual requirements do you have for your critical vendors relating to notification of breach?

Cloud Service Provider:

What protocols do you have in place that limit internal access to the MSP's client data?
Do you have audit logs specific to employees accessing the MSP's client instances?

About The ASCII Group, Inc:

The ASCII Group is the premier community of North American MSPs, VARs and solution providers. The Group has over 1,300 members located throughout the U.S. and Canada. Founded in 1984, ASCII provides services to members including leveraged purchasing programs, education and training, marketing assistance, extensive peer interaction and more. For more information, please visit www.ascii.com.