Email Security

1. Do you prescreen emails for potentially malicious attachments and links?	Y	N Y

		N
7. How often is phishing/cybersecurity training conducted to all staff?		Never Monthly Quarterly Annually Ad Hoc
8. Can your users access email through a web app on a non-corporate device?	Y	N
If Yes: do you require and enforce Multi-Factor Authentication?	Y	N
9. Do you use Office 365 in your organization?	Y	N
If Yes: do you use the o365 Advanced Threat Protection add-on?	Y	N

10. Do you implement PowerShell best practices as outlined in the Environme
Recommendations by Microsoft?

19. Which systems are patched with the above cadence?	Internal Servers Perimeter Systems Workstations None
20. If you have any end of life or end of support software, is it segregated from the rest of the network?	Y N Partial N/A
21. Have you configured host based and network firewalls to disallow inbound connections by default?	Y N Partial
22. Do you use a protective DNS service (e.g. Quad9, OpenDNS, or the public sector PDNS)?	Y N

23. Do you use an endpoint application isolation and containment technology?

  Menlo Security Isolation Platform Authentic8 Silo
  Symantec Web Security Service Web Isolation CylanceProtect Puffin Secure Browser
  Apozy Bitdefender Browser Isolation Cigloo Remote Browsing Cyberinc Isla
  Passages by Ntrepid WEBGAP Remote Browser Curose Internet Isolation Cyberwall
  Garrison SAVI Light Point Web Morphisec Endpoint Threat Prevention Browser Based
  Randed AGU Other No such Product

24. Do your users have local admin rights on their laptop / desktop?	Y N
25. Do users who have admin rights have separate privileged accounts for daily tasks?	Y N

  If Yes: How are those accounts controlled?

  By an Identity Access Manager (IAM) Solution

     Alliant

32. Is remote access exposed to the internet (RDP, Telnet, SSH), without any controls such as IP whitelisting?	Y	N

33. What elements exist on the segmented network? Select all that apply.
 	
    Demilitarized Zones (DMZs)   Security Network   Guest/Wireless Network
    Sites (Office locations, Industrial Control Systems, etc.) Server Network
    IT Management Network VoIP Network N/A		

Detection & Response Assessment

Back-Up & Recovery Policies

42. Are your backups encrypted?	Y N Partial
43. Œ Ç } µ Œ l µ ‰ • l ‰ š • ‰ Œ š (Œ } u Ç } µ (cloud service designed for this purpose?	Yes-Full Online YesCloud Service YesPartially Offline No
44. Do you use a Cloud synching service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups?	Y N
45. Have you tested the successful restoration and recovery of key serv configurations and data from backups in the last 6 months?	Y N Partial
46. Are you able to test the integrity of backups prior to restoration to be confident it is free from malware?	Y N Partial

47. What is the average time to triage and contain security incidents of workstatioear to date?
     Do not know/do not track
     Less than 30 minutes
     30 minutes t 2 hours
     2-8 hours
     Greater than 8 hours	

Pleasesign below and return this form to your Alliant representative:

Signature: _____

Printed Name: _____

Title: _____

Company: _____

Date: _____