LANWORKS™

Preliminary Vulnerability Assessment
REPORT CARD

This report is tabled to provide you with an insight of your IT Security Operations in highlighting any issues that may need to be addressed to mitigate potential cyber security breaches, threats, attacks, and data loss.

Customer	

1.0 Active Directory and Passwords

- ☐ Password Policies (>8 Characters + Number + Special Character)
- ☐ Change Intervals (60 – 90 Days)
- ☐ Privileged Accounts *(other than Admin)*
- ☐ Local Admin Access
- ☐ 5 Failed Logins Locks Account (Failed Login Monitoring)
- ☐ Stale Accounts (user/computer)
- ☐ Non-expiring User Account Password
- ☐ Inactive Computer Lock Policy
- ☐ Other _____

2.0 Backup/Recoverability

- ☐ Separate/Non-Domain Login Credentials for Backup & Storage
- ☐ 3 Copies of Data *(3-2-1 Rule)*
- ☐ Defined RTO/RPO
- ☐ Offsite Copy
- ☐ Standard Operating Procedures for Backup and Recovery
- ☐ Regular Integrity/Recovery Checks
- ☐ Other Corporate Business Continuity Insurance _____

3.0 Supported Operating Systems

- ☐ Servers on Current OS
- ☐ Servers on Current Patch Level (last patch date)
- ☐ Workstations on Current OS
- ☐ Workstations on Current Patch Level (last patch date)
- ☐ RDP Enabled
- ☐ SOP for Patch Management
- ☐ Uninstall Unused Applications
- ☐ Other _____

4.0 Email

- ☐ Email Security Product Installed (versions if local)
- ☐ Two Factor Authentication
- ☐ Monitoring of Failed Login Attempts
- ☐ Other _____

5.0 AntiVirus

- ☐ Endpoint Protection on all Nodes
- ☐ Endpoint Monitoring
- ☐ Servers AntiVirus
- ☐ Advance Threat Protection

- ☐ Endpoint Detection and Response
- ☐ Disk Encryption
- ☐ Other _____

6.0 Remote Access

- ☐ Monitoring
- ☐ Two Factor Authentication
- ☐ Failed Attempt Lockout
- ☐ RDP opened to Outside
- ☐ Reporting
- ☐ Other _____

7.0 Firewall

- ☐ OS is Supported and Current
- ☐ Inbound Policies are Valid
- ☐ No Console Access from Untrust
- ☐ Next Gen Features Enabled
- ☐ Firewall Logs and Monitoring
- ☐ Other _____

8.0 Wireless

- ☐ Corporate Network Secured
- ☐ Access Control in Place
- ☐ No Personal Devices on Corporate VLAN
- ☐ Other _____

9.0 Network

- ☐ Current Licenses and Maintenance on all Equipment
- ☐ Segregation of Server and Users VLANs
- ☐ Isolation of IoT Devices
- ☐ Method to ensure authorized devices on Corp network (802.1x)
- ☐ Other _____

10.0 User Education/Awareness

- ☐ Awareness Training
- ☐ Recurring Reminders
- ☐ Periodic Phishing Tests
- ☐ Other _____

11.0 Office 365

- ☐ Password Policy
- ☐ Two Factor Authentication
- ☐ Security Score Dashboard
- ☐ Stale Accounts (user/computer)
- ☐ Backup
- ☐ Other _____

12.0 Documentation

- ☐ Network diagram
- ☐ Application activation keys
- ☐ Media off Network
- ☐ Server Names, IP's, and Functionalities
- ☐ Other _____