**Risk assessment: MSP Internal Assessment**

Administered by: Date:

|  |  |  |  |
| --- | --- | --- | --- |
| Description | Not Started | In Progress | Completed |
| **Cyber Security/HIPAA Training Review:** All teams have performed HIPAA training in the last 12 months.  |  |  |  |
| **Incident Response Policy:** A clearly defined incident response policy is in place and an Information Security Officer is defined. Response policy is reviewed and/or practiced on a regular basis. |  |  |  |
| **Employee Onboarding and Separation Procedure:** MSP has formal Onboarding/Separation processes, and those policies use templates or checklists to ensure that proper access to company information is granted/removed during the process. |  |  |  |
| **Encryption of Sensitive Data:** All company systems including portable storage devices are encrypted and the state of encryption is monitored for change. |  |  |  |
| **Critical Systems Management:** All critical systems are protected with 2FA, are patched to a secure version, and have at least two designated administrators. All critical systems have been assessed for security in the last 90 days. |  |  |  |
| **Electronic Funds Transfer Policy:** MSP has an established EFT policy, updates it regularly, and reviews it with staff annually. |  |  |  |
| **Remote Access Policy:** MSP has a remote access policy that outlines the requirements for secure remote access, what data can be accessed, and who can utilize that access from what devices. |  |  |  |
| **Controlled Access/Least Privilege Policy:** The MSP has a defined policy in place to limit access rights for users to the bare minimum permissions they need to perform their work. |  |  |  |
| **Password Policy/Password Manager:** Password policy is up to date and requires the use of unique passwords for all apps/services. Each team member has access to a password manager and is trained on how to use it in accordance with compliance. |  |  |  |
| **Multi-Factor Authentication:** MFA is deployed on all critical systems including workstations, servers and MSP tools. |  |  |  |
| **Patch management and system updates:** Line of business applications and device firmwares are patched/updated frequently and according to a schedule process. |  |  |  |
| **SIEM/Centralized Logging:** All on-premise or private clouds have a centralized and monitored SIEM solution deployed |  |  |  |
| **Internal Wireless:** Internal wireless is separated into vlans to separate trusted and untrusted subnets. Authentication on the trusted subnet is backed by Radius authentication and BYOD devices are not allowed.  |  |  |  |
| **Servers:** Servers are not approaching EOL or warranty expiration. |  |  |  |
| **Intrusion Detection and Prevention:** MSP tools are behind a firewall with IPS/IDS configured and monitored by a 24/7 third party SOC.  |  |  |  |
| **Network Documentation:** Network documentation is performance and updated regularly by the MSP. Access to the documentation is limited and secured behind 2FA. |  |  |  |
| **Zero Trust:** Threatlocker is deployed on all of the MSPs systems, even non-critical ones, to prevent the execution of unknown and/or untrusted applications and services. |  |  |  |
| **Audit Firewall Rules/Configuration:** Firewall configuration is audited quarterly to ensure that outdated rules have been removed or disabled. |  |  |  |
| **Backup Review and Testing:** A policy is in place and being followed to monitor all backup products daily and perform test restores in accordance with customer agreements. Test restores are being completed without issue in most scenarios. |  |  |  |
| **Business Continuity Planning:** A business continuity plan exists and all team members are aware of their responsibilities. The MSP should be able to remain functional in the event of a disaster. |  |  |  |

**Action items:**