Overall Assessment Report

Summary Report for: SAMPLE Mock - Assessment

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |
| --- |
| The overall summary report provides an overall score for each of the categories designed to show the overall health and compliance of your IT systems. Scores are weighted based on their respective importance to keeping your business in optimal range. |

|  |  |  |
| --- | --- | --- |
| Category | Description | Score |
| Policy and Procedure |  | 79 |
| MSP Tools Review |  | 83 |
| Internal Network |  | 86 |
| Business Continuity |  | 83 |

|  |  |
| --- | --- |
| Overall Score | 83 |

Category: Policy and Procedure

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |  |
| --- | --- | --- |
| Item | Summary | Score |
| MSP - Cyber Security / HIPAA Training Review | All team members have performed HIPAA training in the last 12 months. Employees nearing expiration of 2019 training have been scheduled for 2020 training.  | Satisfactory |
| MSP - Incident Response Policy | No defined incident response policy is in place within the MSP, leaving room for errors or poor judgment in incident response.  | At Risk |
| MSP - Employee Onboarding and Separation Procedure | MSP has formal Onboarding/Separation processes, and those policies use templates or checklists to ensure that proper access to sensitive company information is granted/removed during the proc | Satisfactory |
| MSP - Use of encryption to protect sensitive data, PHI, PII, ect. | All company systems including portable storage devices are encrypted and the state of encryption is monitored for change.  | Satisfactory |
| MSP - Critical Systems Management | One or more critical systems have a single dedicated administrator.  | Needs Attention |
| MSP - Electronic Funds Transfer Policy | MSP does not have an established EFT Policy | At Risk |
| MSP - 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.  | Satisfactory |
| MSP - 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 | Satisfactory |

|  |  |
| --- | --- |
| Policy and Procedure Score | 79 |

Category: MSP Tools Review

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |  |
| --- | --- | --- |
| Item | Summary | Score |
| MSP - 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 comp | Satisfactory |
| MSP - Multi-Factor Authentication | MFA is deployed on all critical systems including workstations, servers and MSP tools.  | Satisfactory |
| MSP - Patch management and system updates | Line of business applications and device firmwares are patched/updated frequently and according to a scheduled process.  | Satisfactory |
| MSP - SIEM / Centralized Logging | SIEM solution is not deployed on the MSPs internally hosted tools.  | At Risk |

|  |  |
| --- | --- |
| MSP Tools Review Score | 83 |

Category: Internal Network

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |  |
| --- | --- | --- |
| Item | Summary | Score |
| MSP - Internal Wireless | Internal wireless is separated but authentication is a preshared key,  | Needs Attention |
| MSP - Servers | Servers are not approaching EOL or warranty expiration. | Satisfactory |
| MSP - Intrusion Detection & Prevention | MSP tools are behind a firewall with IPS/IDS configured and monitored by a 24/7 third party SOC.  | Satisfactory |
| MSP - Network Documentation | Network documentation is incomplete and needs attention.  | Needs Attention |
| MSP - Zero Trust | Threatlocker is deployed on all of the MSPs critical systems to prevent execution of unknown and/or untrusted applications and services.  | Acceptable Risk |
| MSP - Audit Firewall Rules/Configuration | Firewall configuration is audited quarterly to ensure that outdated rules have been removed or disabled.  | Satisfactory |

|  |  |
| --- | --- |
| Internal Network Score | 86 |

Category: Business Continuity

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |  |
| --- | --- | --- |
| Item | Summary | Score |
| MSP - Backup Review and Testing | Backups are being checked by the helpdesk team but no policy exists to standardize those checks.  | Needs Attention |
| MSP - 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.  | Satisfactory |

|  |  |
| --- | --- |
| Business Continuity Score | 83 |

Focus Area: Not Applicable Items

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |
| --- | --- |
| Item | Summary |

Focus Area: Unknown Items

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |
| --- | --- |
| Item | Summary |

Focus Area: At Risk Items

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |
| --- | --- |
| Item | Summary |
| MSP - Electronic Funds Transfer Policy | MSP does not have an established EFT Policy |
| MSP - Incident Response Policy | No defined incident response policy is in place within the MSP, leaving room for errors or poor judgment in incident response.  |
| MSP - SIEM / Centralized Logging | SIEM solution is not deployed on the MSPs internally hosted tools.  |

Focus Area: Needs Attention Items

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |
| --- | --- |
| Item | Summary |
| MSP - Critical Systems Management | One or more critical systems have a single dedicated administrator.  |
| MSP - Internal Wireless | Internal wireless is separated but authentication is a preshared key,  |
| MSP - Network Documentation | Network documentation is incomplete and needs attention.  |
| MSP - Backup Review and Testing | Backups are being checked by the helpdesk team but no policy exists to standardize those checks.  |

Focus Area: Acceptable Risk Items

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |
| --- | --- |
| Item | Summary |
| MSP - Zero Trust | Threatlocker is deployed on all of the MSPs critical systems to prevent execution of unknown and/or untrusted applications and services.  |

Focus Area: Satisfactory Items

Prepared for: Delaware Micro-Computer

Date Prepared: Not Specified

Assessment Template: MSP Internal Assessment

|  |  |
| --- | --- |
| Item | Summary |
| MSP - 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 |
| MSP - Cyber Security / HIPAA Training Review | All team members have performed HIPAA training in the last 12 months. Employees nearing expiration of 2019 training have been scheduled for 2020 training.  |
| MSP - Employee Onboarding and Separation Procedure | MSP has formal Onboarding/Separation processes, and those policies use templates or checklists to ensure that proper access to sensitive company information is granted/removed during the proc |
| MSP - 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.  |
| MSP - Use of encryption to protect sensitive data, PHI, PII, ect. | All company systems including portable storage devices are encrypted and the state of encryption is monitored for change.  |
| MSP - Multi-Factor Authentication | MFA is deployed on all critical systems including workstations, servers and MSP tools.  |
| MSP - 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 comp |
| MSP - Patch management and system updates | Line of business applications and device firmwares are patched/updated frequently and according to a scheduled process.  |
| MSP - Audit Firewall Rules/Configuration | Firewall configuration is audited quarterly to ensure that outdated rules have been removed or disabled.  |
| MSP - Intrusion Detection & Prevention | MSP tools are behind a firewall with IPS/IDS configured and monitored by a 24/7 third party SOC.  |
| MSP - Servers | Servers are not approaching EOL or warranty expiration. |
| MSP - 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.  |