IT Nation Secure MSP+ Cybersecurity Framework

v2020.D-1.2

WISE TOGETHER RISE TOGETHER

IT NATION SECURE
cybersecurity by ConnectWise

Legal Disclaimer

Please note that these playbooks are provided only as examples and are for reference purposes only. In many instances, your existing procedures may suffice. Prior to implementing or adopting these sample playbooks, ConnectWise strongly encourages any organization to consult with its legal counsel, accounting, financial and/or human resource professionals. By doing so, this will assist your organization in developing policies and procedures that reflect its organizational philosophy and that are appropriate to their specific circumstances and that are consistent with applicable federal, state, and local laws.

These are provided as a free resource and are provided "as is" without warranty of any kind and ConnectWise makes no legal representation concerning the adequacy of these playbooks or its compliance with federal, state, or local laws.

Never use sample policies and procedures that you find online as-is, as any policy you adopt needs to reflect the actual practices in your company. They must also be in compliance with all applicable laws and regulations, and there can be significant differences in state and local compliance requirements. You should always consult with a licensed attorney with experience specific to employment law prior to finalizing policies and procedures, whether they are individual documents or combined to form an employee handbook or procedures manual.

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Governance Program	Should have the following policies in place, communicated, and employee acknowledged at a minimum: - Acceptable use policy - Antivirus and malware policy - Data access and password policy - Data backup policy - Facility security policy - Perimeter security and administration policy - Telecommuting policy - System configuration policy - Vulnerability identification and system updates policy	Customized set of most policies for business Measuring some policy effectiveness (Based upon shared IT Nation Secure Security Policy Templates)	Full set of customized policies Measurement of all policies
Define Privacy Program	Informal Internal Privacy Policy, if storing, handling, or processing PII - Must be posted for internal consumption - Documented review of security controls in place, monitoring and actively protecting PII Informal Protocol for Data Retention - Data Retention Policy, if storing, handling, or processing PII - Retention is a manual process with documented procedures - Retention guidelines match those for federal, state, local or compliance and regulatory requirements Employees trained on Internal Privacy Policy and Data Retention	Formal Internal Privacy Policy - Protocols Defined for Data Retention - Employees Trained - Ongoing Improvements Informal External Privacy Policy - Available for external consumption - Documented review of security controls in place, monitoring and actively protecting PII Guidelines for a Breach Response Plan - Informal Breach Response Plan - Initial Training and Awareness for the Breach Plan for both employees and clients impacted	Privacy Officer (Optional) Formal Internal / External Privacy Policy Annual Employee Training Privacy by Design (processes & systems) Formal Breach Response Plan Formal Protocol for Data Retention Privacy Assessments

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Security Program	Security Awareness Training (Minimum Modules / Topics): - Phishing - Social Networks - Malware - Mobile Devices - Data Security - Privileged User - Social Engineering - Passwords - Browsing Safely Physical Security Measures - Safeguards and protections for Server room (Cypher locks minimum) - Clean Desk Policy - Visitor Escort Program Perimeter Security Solutions (Firewall) - NSA or CISA Hardening Guidelines implemented Endpoint Protection - Solution implemented, managed, and monitoring Event Log collection - Servers, Workstations, IDS/IPS, AV, etc. - SIEM Aggregated and Monitored Backup Solution (critical systems) - Audit Collection, SIEM, EDP, PII, etc. - 3-2-1 Tiered Backup Solution implemented - Tested Monthly Flat Network Design (Internally), in most cases - Planning for multiple VLAN segmentation (minimum) - Working with clients to implement segmentation in their environments	Security Awareness Training (Must have all of the Fundamentals and the following): - Insider Threat - Cloud Services - Physical Security - Working Remotely - Encryption - Help Desk Specialized Roles - Senior Leadership Specialized Roles Security becoming part of culture System Auditing (critical systems) Physical Security Measures System Hardening (critical systems) Perimeter Security Solutions (Firewall / IPS) Endpoint Protection Managed Detection & Response (MDR) - (Optional) Ad-Hoc Risk Management Practices 3-2-1 Tiered Backup Solution Documented Security Plan VLAN Segmented Design, Internally and with some Clients	Security Awareness Program Executive Support (Optional) Security as Part of Culture (by design) Identity & Access Management (IAM) System Auditing Physical Security Measures System Hardening Requirements Perimeter Security Solutions (Firewall / IPS / DMZ) Endpoint Protection & Response (EDR) Managed Detection & Response (MDR) Formal Risk Management Program Security Operations Center (SOC) - (Optional) 3-2-1 Tiered Backup Solution Documented Security Plan DR / BCP Metrics for the IT security program are established VLAN Segmented Design, Internally and with all Clients

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Measurement Program	Some documented security capabilities (AV, malware, identification of future security enhancements) Metrics around: Infrastructure Measurements Servers - Vulnerability scanning - Patching (OS and applications) - Standard secure configuration (Configuration Mgmt.) Client Devices - Standard secure configuration - Endpoint protection - Patching (OS and applications) Perimeter Security - Secure firewall configuration - Monitoring and alerts Governance Measurements Policy Compliance - Policy review - Personnel security Security Awareness Training - End user training - Executive and management training Password Compliance (Includes MFA) - Complexity - Age - MFA enabled - Security vs. infrastructure budget - Risk assessments (Against a framework, like CSF)	Developing metrics for security capabilities Metrics for security awareness Identify any security gaps (Annual Assessments)	Monitor and measure current security capabilities Identify any gaps in systems, processes, and operations for improvement Developing data-driven metrics for decision makers Developing data-driven metrics for operations Optimizing security program with metrics and KPIs Establishing security response and operations efficiency to reduce risk

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Security Life-Cycle / Review	Security life-cycle management profiles are documented May not be communicating existing security risk at the business level Develops business case for new security products and services Approach to managing security / risk has not been established	Ad-hoc security / risk management life-cycle policies Efforts underway to establish security / risk management objectives and environment baseline Awareness of existing security risk at the business level Implementing security procedures with adequate workforce and resources	Formalized security life-cycle procedures are regularly updated Changes based upon risk, requirements, or threats Well-trained security workforce Documented security/business dependencies Collaborates with business partners to make risk-based management decisions
Define Risk Management Program	Risk Management - Working to define for the organization - Approach to managing risk has not been established - Vulnerability identification and patching make up the majority of this program Minimal security strategy program Sell security products to customers (land and expand) Limited awareness of existing security risk at the business level	Efforts underway to establish risk management objectives Ad-hoc risk management life-cycle policies Limited understanding of business security and security risks Understanding of existing threat environment Initial security strategy program underway for critical systems/services Implementing risk management procedures with adequate resources	Formalized risk management procedures are regularly updated Security strategy exists across many business operations Changes based upon risk, requirements, or threats Well-trained risk management workforce Documented security/risk/business dependencies Collaborates with business partners to make risk-based management decisions
Define Vulnerability Management / Assessment Program	Documented procedures in accordance with the vulnerability identification and system updates policy Annual vulnerability scan of limited scope	Documented vulnerability management program Limited input from threat intelligence Threats and risk not aligned with business goals Few critical systems and threat vectors are occasionally scanned	Working vulnerability management program Input gathered from threat intelligence Threats and risk partially aligned with business goals Critical systems and threat vectors are scanned and prioritized Developing metrics and processes aligned to understand trends and to enhance business processes

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Patch Management Program	Documented procedures for patching in accordance with the vulnerability identification and system updates policy Patching should be on a regular cadence (minimum monthly) Includes all operating systems and application updates Patching without strategy or organized structure Limited change management processes	Regular patching of all systems and applications Ad-hoc configuration management program Documented patch management plan and processes Change management processes are followed Limited patch testing / regression testing	Documented inventory and regular patching of systems Formalized configuration management program Detailed patch management plan and processes Developing change management program Ad-hoc patch testing/regression testing
Define Business Continuity/ Recovery Planning (DR/BCP)	Identify vital resources, facilities and data for DR/BCP Documents access required for vital resources, facilities and data for DR/BCP Identify workforce personnel roles needed for implementing DR/BCP Backups occasionaly tested and rarely restored	Developing Disaster Recovery (DR) & Business Continuity Plan (BCP) Ad-hoc measures to safeguard vital resources, facilities and data Ad-hoc measures to ensure access vital resources, facilities and data Identify workforce personnel roles needed for implementing DR/BCP 3-2-1 Tiered Backups with testing	Disaster Recovery (DR) Plan integrated with Business Continuity Plan (BCP) Conducts Business Impact Analysis across critical systems Measure ability to perform essential functions through test, training and exercise, identifying gaps and solutions Document measures to safeguard vital resources, facilities and data Document measures to ensure access vital resources, facilities and data Ensure emergency continuity resource requirements, agreements/contracts remain current Identify, train & prepare workforce personnel to relocate to alternate sites / remote (WFH) 3-2-1 Backups fully tested and periodically restored

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Third-Party / Vendor Risk Program	Accept default contracts without understanding impact to the business No to minimal involvement from the business with third parties There is no standard third-party risk assessment methodology Reviews are limited to single categories of third-party risk Lack of central repository can result in repetitive / duplicate information	The business is reluctantly involved in processes There is no standard risk assessment methodology Reviews are limited to single categories of third-party risk There are sporadic instances of duplicate efforts on similar vendors	The business is engaged, ensuring their third-party risk is acceptable Third parties are monitored periodically Standard sets of questions / questionnaires are used based on the third parties' inherent risk level Multiple risk categories are assessed for each third party Assessments are completed within a technology (online) portal
Define Incident Management Program	Break/fix mindset Engineering / administrators know need for IR plan Ad-hoc assignment of workforce personnel for IR Manual capabilities may exist to analyze incidents	Business executives know need for IR plan Incident response policy, plan, and procedures created Identify workforce personnel for incident response Manual capabilities may exist to analyze incidents Reactive / ad-hoc IR communications for identified internal / external parties Limited reporting to regulatory, compliance, and legal entities	Business executives promote IR plan and enhanced capabilities Incident response policy, plan, and procedures created and followed Identify, train, and prepare workforce personnel for incident response Capabilities exist to automatically detect and analyze incidents Ability to contain, eradicate, and recover from an incident Lessons learned are incorporated into IR plans and procedures Actively conducts remediation training (post-incident) Up-to-date IR communication plan for identified internal/external parties Formalized reporting procedures for regulatory, compliance, and legal entities

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define Executive/ Board/Owner Oversight	Business executives partially aware of needs	Business executives know need for IR plan	Business executives promote IR plan and enhanced capabilities
Define Roles and Responsibilities	Ad-hoc assignment of workforce personnel for IR	Identify workforce personnel for incident response	Integrated workforce personnel for formalized incident response program
Define Team Training for Incident Response	Limited training / publicly available material from Internet	Limited training and preparation for IR	Train and prepare workforce personnel for incident response
Define Communication Plan	No comprehensive communication plan or limited to few contacts	Documented IR communication plan for some identified internal / external parties	Up-to-date IR communication plan for all identified internal / external parties
Incident Response Life-Cycle	Reactive and ad-hoc response in dealing with IR issues	Documented aspects of several elements of the IR life-cycle: preparation, detection, analysis, containment, eradication, recovery, and post-incident activities	Formalized IR life-cycle of preparation, detection, analysis, containment, eradication, recovery, and post-incident activities
Define Security Architecture	Very few components / disorganized ad-hoc Basic attempts have been made to define the security architecture Limited documentation of security architecture and network diagrams	Basic understanding of best practice with several objectives, strategy and tools in place The security architecture is defined at critical layers and is reasonably effective Security architecture is defined and a need for monitoring and measurement has been identified, but not realized	Effective and Integrated security architecture based upon a standards framework Detailed business requirements with controls mapped to the standards framework Business drivers are measured against security architecture and monitored for meeting requirements Business has seen improvements from the implementation of security architecture Security architecture provides consistent and effective management controls

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Reference Architectures/Case Studies	Limited documentation of security architecture / network diagrams Management awareness of enterprise architecture needs / some level of effort	Documented network / security architecture and process flows Management actively supports enterprise architecture standards	Published reference architecture with supporting business use cases Periodic re-examination of business drivers and review of security architecture
Product Security	Some applications and appliances Few resources are allocated to address product security	Resources are learning security and getting hands-on experience	Advocates secure coding practices and has a SDLC
Product Compliance	Default compliance/settings No single system for purchasing Multiple purchasing channels	Follows a well-defined purchasing policy with some internal controls Processes in place to authorize/approve purchases of product/services Limited resources for measuring compliance and controls	Controls are fully documented in the form of the purchasing policy Some automation with procurement systems Procurement systems may be siloed (contracts/purchase orders/invoicing) Dedicated workforce for auditing and measuring compliance with the controls
People and Process	Very few components / disorganized roles and responsibilities Understands need for security program and compliance program	Documented most roles and responsibilities for existing security initiatives Understands security program maturity and compliance objectives	Documented roles and responsibilities for security and compliance program Implemented components of a security program and compliance framework Aware of actions to better protect organizational data and IT systems and have corrective action plans

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Security Awareness Training	Ad hoc security awareness, training, and education Limited training provided to users accessing data or IT systems at a minimum: - Random monthly email phishing - Annual online or in-person security awareness training **(Minimum Modules / Topics)** - Phishing - Privileged user - Social networks - Social engineering - Malware - Passwords - Mobile devices - Secure browsing - Data security	Limited topics for security awareness, training, and education General training provided to users accessing data or IT systems (including testing/phishing) Required security awareness training conducted annually (or quarterly) Completion of security awareness training is documented (reporting includes exam and phishing result KPIs)	Establish practical guidance for security awareness, training, and education (Roadmap created) Training provided to users accessing data or IT systems (based upon roles and responsibilities)(includes phishing) Required security awareness training conducted annually (at least quarterly and includes testing) Completion of security awareness training is documented and tracked (reporting includes exam and phishing result KPIs)

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Identity and Access Management (IAM)	Internal users (no customers, no suppliers, no partners) One trusted, central directory Basic provisioning, mainly HR-driven, focus on creation of users Little to no role management No authentication beyond the Windows / network operating systems and isolated SSO-solutions Web access management as point solution, no application integration No federation Auditing only on system level No consistent policy-driven approach Only point solutions for compliance (if any)	Internal user, customers, suppliers One consistent view on identities, independent of the type of user Defined processes for creation, change, and deletion of users Basic role management on the provisioning layer Enterprise single sign-on (SSO) Strong authentication for internal users (Two-factor) Multiple access management policies based upon role-based concepts Singular federation implementations Policy-driven control for singular systems, no consistent approach Auditing and compliance solutions on the system level, some degree of integration	Defined identities for both on-prem and cloud service interfaces External / open provisioning workflows Enterprise entitlement approaches in provisioning Enhanced role concepts Authentication service, enabling single sign-on (SSO) for applications Federation as a means for SSO Federation as standard approach for distributed authentication and authorization Centralized federation services for service-oriented applications Consistent policy approach across systems Audit log service interfaces for access to different logs Pre-defined compliance services

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Security Operations (SOC)	Identified a specific area of environment requiring protection or compliance needs Process to manage security / compliance violations may or may not exist Isolated logging and limited insight into threats Lack of people and process for effective threat evaluation and prioritization No formal incident response process Minimal compliance-mandated monitoring and response Limited visibility into (internal and external) threats, many blind spots	Seeking efficiencies and improved assurance for risk and compliance Working on improvements to detect and respond to potential high-impact threats for critical systems Established formal processes and assigned responsibilities for monitoring and alerting Basic, formal processes in place for incident monitoring and response Good visibility into (internal and external) threats, with some blind spots	Highly resilient and effective security, risk and compliance posture Invested in the processes and manpower to significantly improve ability to detect and respond to most threats Functional formal security operations and incident response center (SOC) effectively staffed with trained workforce Actively monitoring logs and alerts and has progressed into proactive threat hunting Implementing and leveraging automated tools to better investigate and response to events Great visibility into (internal and external) threats, detect early and respond quickly
Define MSP+ Education Program	Acceptable	Good	Proactive
ConnectWise Certify for Engineers	Completed ConnectWise Certify Fundamentals for Engineers for all technical staff (100% pass rate) New hires will complete training within 90 days	Completed ConnectWise Certify Advanced for Engineers for all technical staff (50% pass rate or greater) New hires will complete training within 90 days	ConnectWise Certify Master for Engineers
ConnectWise Certify for Sales	Completed ConnectWise Certify Fundamentals for Sales for all sales personnel (100% pass rate) New hires will complete training within 90 days	Completed ConnectWise Certify Advanced for Sales for all sales personnel (50% pass rate or greater) New hires will complete training within 90 days	ConnectWise Certify Master for Sales

MSP+ Cybersecurity Framework Disciplines	MSP Baseline (Fundamentals) Partial / Ad Hoc	MSP+ (Advanced) Risk Informed	SECURE MSP (Master) Repeatable
Define MSP+ Certification	n/a	MSP+ Certification (Self-Attest)	Secure MSP Accredited Partner