Vulnerability / Patch Management Policy

MMF Consulting Grp (Pte. Ltd.)

October 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC7.1

Table 2: Document history

Date	Comment
Oct 15 2024	Initial document
Nov 30 2024	Policy updates and improvements

1 Vulnerability / Patch Management Policy

Field	Value
ID	VULNP-002
Effective Date	October 15, 2024
Last Revised	November 30, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This System Maintenance and Security Update Procedures policy establishes requirements for identifying, assessing, and remediating security vulnerabilities across all MMF Consulting Grp (Pte. Ltd.) information systems. This policy applies to all hardware, software, operating systems, and applications used in business operations, including laptops, servers, cloud services, and third-party applications.

1.2 Background

Effective vulnerability management is critical for maintaining the security of MMF Consulting Grp (Pte. Ltd.)'s systems and protecting sensitive client data. As new security vulnerabilities are discovered daily, systematic identification and remediation processes ensure that security exposures are minimized before they can be exploited. This policy leverages Microsoft Defender for Business capabilities while establishing clear procedures for comprehensive vulnerability management.

1.3 Policy

1.3.1 Vulnerability Management Framework

1.3.1.1 Scope of Coverage

- **Operating Systems**: Windows 11 on all company laptops and workstations
- **Microsoft 365**: Exchange Online, SharePoint, Teams, and related cloud services
- **Box.com Platform**: Cloud storage and collaboration service
- **Business Applications**: Audit software, analysis tools, and productivity applications
- **Network Infrastructure**: Assets managed per Asset / Device Management Policy (ASSETP)
- **Mobile Applications**: Approved business applications on personal devices

1.3.1.2 Vulnerability Sources

- **Automated Scanning**: Microsoft Defender for Business vulnerability assessments
- **Vendor Notifications**: Security bulletins from Microsoft, Box.com, and other vendors
- **Threat Intelligence**: Industry security alerts and vulnerability databases
- **Penetration Testing**: Annual third-party security assessments
- **Internal Discovery**: Employee reporting and system monitoring

1.3.2 Vulnerability Assessment Procedures

1.3.2.1 Continuous Monitoring

- **Microsoft Defender Dashboard**: Daily review of vulnerability reports and security recommendations
- **Windows Update Status**: Weekly verification of patch installation across all devices
- **Cloud Service Monitoring**: Regular review of Microsoft 365 and Box.com security advisories
- **Application Monitoring**: Tracking updates for business-critical applications
- **Network Scanning**: Periodic vulnerability scans of network infrastructure

1.3.2.2 Risk Assessment and Prioritization

- **Critical Vulnerabilities**: CVSS score 9.0-10.0 - Immediate action required (within 7 days)
- **High Vulnerabilities**: CVSS score 7.0-8.9 - Action required within 30 days
- **Medium Vulnerabilities**: CVSS score 4.0-6.9 - Action required within 90 days
- **Low Vulnerabilities**: CVSS score 0.1-3.9 - Address during regular maintenance cycles
- **Zero-Day Threats**: Emergency response procedures for actively exploited vulnerabilities

1.3.2.3 Business Impact Assessment

- **System Criticality**: Priority based on business importance and client impact
- **Data Sensitivity**: Higher priority for systems handling confidential client data
- **Exploitation Probability**: Assessment of likelihood of successful attack
- **Compensating Controls**: Evaluation of existing security measures
- **Downtime Tolerance**: Consideration of business continuity requirements

1.3.3 Patch Management Procedures

1.3.3.1 Operating System Updates

- **Automatic Updates**: Windows Update enabled for all company devices
- **Monthly Patch Cycle**: Second Tuesday of each month for routine Windows updates
- **Critical Patches**: Emergency patching within 7 days for critical security updates
- **Testing Procedures**: Validation on test systems before widespread deployment
- **Rollback Plans**: Documented procedures for reversing problematic updates

1.3.3.2 Application Updates

- **Microsoft 365**: Automatic updates managed by Microsoft with monitoring
- **Box.com**: Cloud service updates managed by vendor with notification
- **Business Applications**: Scheduled updates during maintenance windows
- **Security Software**: Microsoft Defender updates automatically with monitoring
- **Browser Updates**: Automatic updates enabled for Microsoft Edge and approved browsers

1.3.3.3 Third-Party Software Management

- **Approved Software List**: Maintained per Asset / Device Management Policy (ASSETP)
- **Update Coordination**: Vendor notification monitoring and update scheduling
- **License Compliance**: Verification of licensing before applying updates
- **Compatibility Testing**: Validation that updates don't interfere with business operations
- **End-of-Life Management**: Migration planning for software reaching end-of-support

1.3.4 Implementation and Deployment

1.3.4.1 Change Management Integration

- **Change Approval**: Formal approval process for significant system changes
- **Documentation Requirements**: Detailed records of all patches and updates applied

- **Communication Plan**: Notification to affected users before scheduled maintenance
- **Rollback Procedures**: Defined steps for reversing updates that cause problems
- **Post-Implementation Verification**: Testing to confirm successful patch deployment

1.3.4.2 Deployment Strategies

- **Phased Rollouts**: Gradual deployment starting with test systems and non-critical users
- **Emergency Deployment**: Rapid patching procedures for actively exploited vulnerabilities
- **Maintenance Windows**: Scheduled downtime for major updates requiring system restarts
- **Remote User Support**: Procedures for updating devices of remote and traveling employees
- **Client Site Considerations**: Coordination with client IT policies for on-site work

1.3.4.3 Quality Assurance

- **Pre-Deployment Testing**: Validation in isolated test environment before production deployment
- **Pilot Groups**: Small user groups for initial deployment and feedback
- **Performance Monitoring**: Assessment of system performance after patch installation
- **Functionality Testing**: Verification that business applications continue to work properly
- **User Feedback**: Collection and analysis of user reports after updates

1.3.5 Vulnerability Response Procedures

1.3.5.1 Emergency Response (Critical/Zero-Day Vulnerabilities)

- **Immediate Assessment**: Evaluation of threat within 2 hours of notification
- **Risk Mitigation**: Implementation of temporary controls while permanent fixes are prepared
- **Accelerated Patching**: Emergency patch deployment within 7 days
- **Stakeholder Communication**: Immediate notification to Director and affected teams
- **Monitoring Enhancement**: Increased monitoring for signs of exploitation

1.3.5.2 Standard Response (High/Medium Vulnerabilities)

- **Weekly Assessment**: Regular review during scheduled vulnerability management activities
- **Planned Remediation**: Integration into regular patch management cycles
- **Resource Allocation**: Assignment of appropriate personnel and time for remediation
- **Progress Tracking**: Monitoring of remediation progress against established timelines
- **Completion Verification**: Confirmation that vulnerabilities have been successfully addressed

1.3.6 Compliance and Reporting

1.3.6.1 Vulnerability Metrics

- **Time to Detection**: Measurement of how quickly vulnerabilities are identified
- **Time to Remediation**: Tracking of time from detection to successful patching
- **Patch Compliance**: Percentage of systems with current security updates
- **Vulnerability Reduction**: Trending of overall vulnerability exposure over time
- **Critical Finding Resolution**: Specific tracking of high-risk vulnerability remediation

1.3.6.2 Management Reporting

- **Monthly Dashboard**: Summary of vulnerability status and patching activities
- **Quarterly Reviews**: Comprehensive assessment of vulnerability management effectiveness
- **Annual Reporting**: Yearly summary for compliance and audit purposes
- **Incident Correlation**: Analysis of security incidents related to unpatched vulnerabilities

- **Improvement Recommendations**: Identification of process enhancements and resource needs

1.3.6.3 External Compliance

- **Client and Regulatory Requirements**: Meeting applicable security standards and client-specific requirements
- **Audit Support**: Documentation and evidence collection for security audits and assessments
- **Insurance Compliance**: Meeting cyber insurance policy requirements for vulnerability management

1.3.7 Training and Awareness

1.3.7.1 Staff Training

- **Vulnerability Management Training**: Conducted per Security Awareness Training Policy (TRAINP) with role-specific focus on patch management procedures
- **Emergency Response Training**: Procedures for critical vulnerability response and vendor coordination

1.4 Policy Review and Maintenance

This policy is subject to annual review and update by the System Administrator and Director.

1.5 Exceptions

All exceptions to this policy require written approval from the Director, accompanied by documented business justification and formal risk assessment. Exception requests must demonstrate that alternative controls provide equivalent security protection or that the business risk is acceptable given operational requirements. Approved exceptions include specific monitoring provisions and regular review schedules.

1.6 Violations & Enforcement

Violations of this policy are subject to disciplinary action commensurate with the severity of the breach and its potential impact on organizational security. Enforcement measures may include mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Failure to apply critical security patches or deliberately circumventing patch management procedures may result in immediate termination and potential legal action.

2 Authorship and Approval

Last edit made by Bill Li (yushengli.tw@gmail.com) on Mon, 18 Aug 2025 18:37:06 +0800.

Approved by Yusheng Li (YushengLi@users.noreply.github.com) on Thu, 21 Aug 2025 11:54:21 +0800 in commit 8e0c1296a6a80185ef11d1631bbf6ca59ccc896b.