VULNERABILITY & PATCH MANAGEMENT POLICY [VPMP]

DOCUMENT CONTROL PAGE

Document ID	SCG/VPMP/011/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/S2RAS/113/1.0			SOC2 Asset Scope
SCG/RMF/015/1.0			Risk Management Policy

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective

Our Vulnerability & Patch Management Policy [VPMP] provides definitive information on the prescribed measures used to manage information security-related risk at [SecureCyberGates]. The main objective of the VPMP is to detect vulnerabilities to reduce possible exposure to harm in a timely manner.

[SecureCyberGates] is committed to protecting its employees, partners, clients, and [SecureCyberGates] Assets from damaging acts that are intentional or unintentional. Protecting company data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure availability, integrity, confidentiality, and safety.

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.
- Safety – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated to cause physical impact by nefarious actors.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Overseeing the implementation and enforcement of this policy [Review and Approve VPMP Policy]
IT/Security Team	1. Responsible for ensuring VPMP requirements are in place. 2. Responsible for enforcing these requirements.
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve VPMP Policy]
Employees / Contractors	1. Read this VPMP Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates] including:

- All employees / Contractors.
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

Each and every one of us are responsible for ensuring that we follow this policy, and we will be held accountable for upholding our commitments to this Vulnerability and Patch Management Policy.

4) Vulnerability & Patch Management

4.1) Objective

The organization develops, implements, and governs processes and documentation to facilitate the implementation of an enterprise-wide vulnerability and patch management policy, as well as associated standards, controls, and procedures to promote healthy vulnerability/patch management practices and other preventative best practices.

4.2) Scope

The scope of the VPMP encompasses all [SecureCyberGates] networks and geographic locations, regardless of what entity "owns" or maintains the asset(s)

[SecureCyberGates] controlled environments

Corporate

- Devices [Firewall, Servers, Laptops, Printers etc]
- Web application, Mobile Application, O.S, Network, Database, Desktop Apps.
- Server Room Assets
- Development environment Assets
- Test environment Assets
- Stage environment Assets
- Production environment Assets

Physical Infrastructure

- Heating, Ventilation and Air Conditioning (HVAC) systems
- Physical access control systems (e.g., proximity badges)
- Alarm & video surveillance systems

3rd party-controlled environments

- Service providers
- Cloud hosting [Azure, AWS, OCI]
- 3rd party developers / Software's

For detailed scoping kindly refer to **Document Name :** SCG_ASSET-RISK-SCOPING_113_V1.0.xls **Document ID** "SCG/S2RAS/113/1.0"

5) Vulnerability & Patch Management Program

5.1) Key Activities

Vulnerability management for [SecureCyberGates] is comprised of the following key activities:

- Manage the asset inventory
- Categorize assets
- Identify vulnerabilities
- Assess risks
- Remediate flaws.

5.1.1) Manage the Asset Inventory

Without a current and accurate asset inventory, it is ad hoc and problematic to properly address applicable vulnerabilities since a comprehensive understanding of the environment is not known. Only through proactive management of asset inventories will Asset Owner know what is applicable and how exposed those assets are to exploitation. Inventories are more useful when categorized into meaningful classes of systems:

System	Comments
Server-Class Systems	Servers taken care by [SecureCyberGates].
Workstation-Class Systems	Laptops / Desktops handled by [SecureCyberGates].
Network Devices	Firewalls / Routers / Switches etc. Networking devices managed by Company
Mobile Devices	Applicable Mobile devices where Company data is stored
Databases	Oracle, MySQL and other DB taken care by [SecureCyberGates].
Minor Applications	Minor or Pre-requisites apps like PHP, Java etc.
Major Applications	All Major [SecureCyberGates] Products [Web Based Apps , Mobile based Apps]

5.1.2) Categorize Assets

Asset categories or zones should be created from asset inventories of [SecureCyberGates] but the categorization should also address criticality and exposure. These categories allow for vulnerability scan customization, addressing asset or business requirements, and assist with assigning risk rankings.

5.1.3) Identify Vulnerabilities

There are internal and external components to identifying vulnerabilities. This includes, but is not limited to:

- Security Audits [Internal as well as External]
- Vulnerability assessments [VA]
- Penetration testing [PT]
- Threat feeds from Special Interest Groups [OWASP Top 10, Security, Support etc.]
- Risk assessments
- Incident Response Team incidents. [IT Team]
- Vulnerabilities raised during Security Monthly meeting.

5.1.4) Assess Risks

Vulnerabilities are assigned a business criticality rating based on Risk Management Policy **Document ID** : SCG/RMF/015/1.0. When a vulnerability is discovered, the vulnerability needs a risk rating assigned to it, and remediation efforts are subsequently prioritized on a risk basis. Based on the degree of exposure, these risk categories help enable [SecureCyberGates] leadership to make informed decisions at the appropriate level of management oversight.

Vulnerability Severity	CVSS Score	Risk Severity
Critical	9.0 – 10.0	Critical Risk
High	7.0 – 8.9	High Risk
Medium	4.0 – 6.9	Medium Risk
Low	0.1 – 3.9	Minor Risk
Informational	0.0 - 0.0	No Risk

Critical Risk:

Extensive financial and long-term brand damage could occur from a critical risk:

- The impact could include extensive damage to [SecureCyberGates]'s reputation.
- The impact could impede [SecureCyberGates]'s systems or business operations.
- The impact could negatively affect [SecureCyberGates]'s long-term competitive position.
- Risk scenarios involving potential physical harm or fatality are included in this category.

High Risk:

Significant financial and brand damage could occur from a severe risk:

- The impact could include significant damage to [SecureCyberGates]'s reputation.
- The impact could impede [SecureCyberGates]'s systems or business operations.

- The impact could negatively affect [SecureCyberGates]'s short-term competitive position.
- This may involve a violation of contractual, statutory and/or regulatory requirements.

Medium Risk:

Minimal damage could occur from a medium risk:

- The impact would not be damaging to [SecureCyberGates]'s reputation or impede business operations.
- The impact could impede core or supporting business systems or business operations.
- This may involve a violation of contractual requirements.
- There are no violations of statutory or regulatory requirements.

Minor Risk:

Minor damage could occur from a Minor risk:

- The financial impact is negligible.
- The impact would not be damaging to [SecureCyberGates]'s reputation or impede business operations.
- There are no violations of contractual, statutory, or regulatory requirements.

No Risk:

False Positive vulnerability.

Severity	CVSS Score	Risk Severity
Critical	Exploitable vulnerabilities which can lead to the widespread compromise of many users.	Vulnerabilities like SQL injections which may compromise the application data, RCE.
High	Based on the existing controls and information processed, there is a certainty that sensitive information will be susceptible to disclosure, tampering and/or disruption to critical infrastructure.	Vulnerabilities like session management can lead to access for the unauthorized user.
Medium	Risk exposure that does not directly compromise the confidentiality, integrity, and/or availability of the areas tested. However, there is a likelihood of intrusion given the current controls, and recommended controls should be implemented to further minimize the risks and constant monitoring should be performed to respond to malicious activities.	Vulnerabilities like missing X-XSS-Protection header which may lead to minor security issues.

Low	Risk exposure that impacts insignificant business processes/information, or the likelihood of occurrence is negligible. The recommended measures may be implemented to enhance the security posture of the overall infrastructure/processes.	Path disclosures, Information Disclosure in a website which enable gathering of information about a site or leak information.
Info	Informational Findings that do not impact the system.	Web Server Default Page enabled in Production, Possible Unwanted Pages, Readme file detected. Etc.

5.1.5) Remediate Risks

Flaw remediation management is the process of identifying, acquiring, installing, and verifying patches for flaws in systems and applications. Patches correct security and functionality problems in software and firmware. From a security perspective, applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Automation of patch deployment helps ensure timely remediation. However, patches may be applied through the following methods:

- User involvement (manual patch install or patch approval).
- All patch **MUST** be first tested in **Lower environments [Development, SIT]** before applying on **UAT / Production.**

5.2) Vendor-Maintained Systems

Vendor-maintained servers and web applications hosted on [SecureCyberGates] network, as well assets hosted on vendor's network, are subject to the same requirements as [SecureCyberGates] maintained assets.

The business unit that contracted the vendor's services is responsible for vendor oversight to ensure the vendor is properly performing vulnerability management activities. The vendor must be made aware of [SecureCyberGates] remediation schedule and remediate vulnerabilities accordingly.

6) Vulnerability Analysis Process

Vulnerability analysis, in relation to patch management, is the process of determining when and if a patch should be applied to a system.

It is necessary that security personnel analyze and determine whether the system is vulnerable to identified attacks. A method used to determine if a system is vulnerable to an identified attack is the "vulnerability footprint," also known as the attack surface. The vulnerability footprint consists of four (4) key elements.

- Deployment
- Exposure
- Impact
- Simplicity

The assessment of risk should be in accordance with [SecureCyberGates]'s Risk Management Program **Document ID** "SCG/RMF/015/1.0".

6.1) Vulnerability Footprint

The following elements define the vulnerability footprint and can be used by vulnerability management personnel in determining the criticality of patching systems and applications:

Deployment: The deployment component relates to the asset's location in the network.

- A higher deployment rating would be assigned to an asset that is exposed to the Internet (e.g., DMZ).
- A lower deployment rating would be assigned to an asset that is in an internal segment with limited Internet access [VPN].

Exposure: The exposure component relates to the available layers of defence and existing controls.

- A higher exposure rating indicates that an attacker could gain unauthenticated access to the asset from another less-secure network (e.g., the Internet).
- A lower exposure rating indicates that an attacker could gain limited physical access.

Impact: The impact component relates to assessing the risk associated with the successful exploitation of a vulnerability.

- A higher impact rating indicates that an attacker could successfully exploit a vulnerability and gain full system control.
- A lower impact rating indicates that an attacker could gain enough information for a preliminary reconnaissance effort on [SecureCyberGates] network architecture.

Simplicity: This simplicity rating applies to the relative ease of the technical exploit.

- A higher simplicity rating indicates an exploit that is readily available and only requires basic hacking skills to use (e.g., script kiddie exploits).
- A lower simplicity rating indicates that the exploit requires a high level of computer skill and related knowledge.

6.2) Assessing Impact

When scanning for vulnerabilities, findings can be easily rated on a 1-5 severity scale, with 1 being "False positive / Informational" and 5 "Critical risk." Asset/Application owners and asset custodians must prioritize the remediation of severity 4[High] and 5[Critical] vulnerabilities before addressing lower severity vulnerabilities.

One important concept to understand is that risk is variable - it can be changed and is not static. This is important to keep in mind since the "risk rating" is subject to change as the risk environment changes.

What is crucial to understand is that risk represents exposure to harm or loss. This is commonly
Quantified as a combination of potential impact, likelihood, and control effectiveness.

Impact Level	Vulnerability Impact Severity Description
[5] Critical	Widely available tools exist that can allow threats to gain control of the host. Note: Exposure includes read/write access to data and privileged access to the host and its applications.
[4] High	It is reasonable to assume a dedicated and competent threat can gain control of the host. Note: Exposure includes read/write access to data and privileged access to the host and its applications.
[3] Medium	Service / application / host is susceptible to a denial-of-service attack.
[2] Low	Exposure to include information about the host (e.g., open ports, services, etc.) that may be useful to find other vulnerabilities. This can include software versions, directory browsing, and security mechanisms being used.
[1] Informational	Threat is a false positive / Informational and is not applicable to the environment.

6.3) Vulnerability Impact Assessment Methods

Methods used in analysing impact can be:

- Qualitative
- Semi-Quantitative
- Quantitative.

The degree of detail required to assess impact will depend upon the application, the availability of reliable data and [SecureCyberGates]'s decision-making needs.

Assess Risks Qualitative

Qualitative assessment defines consequence, probability, and level of impact by significance levels such as "HIGH," "MEDIUM" and "LOW," may combine consequence and

probability, and evaluates the resultant level of risk against qualitative criteria.

Assess Risks Semi-Quantitative

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic or have some other relationship.

Assess Risks Quantitative

Quantitative analysis estimates practical values for consequences and their probabilities and produces values of the level of risk in specific units defined when developing the context.

Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, influence of human factors, or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

7) System & Application Patching

Vulnerability management includes patch management as a core component. Key concepts to be aware of include:

- While a missing patch is always associated with a vulnerability, a vulnerability may not always have a patch associated with it.
- A vulnerability may simply be associated with a configuration and have nothing to do with a software patch.

7.1) Information Security Considerations for Patching Systems

Managing vulnerabilities in operating systems and applications rely, in great part, on to the software vendor. Since all vendors differ in their approach to publishing software patches or when software fixes are not currently available, there are situations where alternate remediation steps may be required to minimize the risk associated with the organization. The goal is to minimize the window of exposure in managing software patching operations.

7.2) Recommended Timelines for Patching

Remediation is prioritized on systems that are directly exposed to the Internet and are susceptible to published vulnerabilities.

Risk	Priority	Time for delivery a remediation plan (after information given)	Time to implement protection (after information given)
Critical	P1	Same day as notification	3* Days
High	P2	2 Days	5* Days
Medium	P3	5 Days	5* Days
Low	P4	10 Days.	10* Days.
Information	P5	NA	NA

Note: *: Actual SLA would depend on project Contract, for Emergency patching, please refer to Change Management Process **DOCUMENT ID:** SCG/CMP/028/1.0

For cloud services, the Vulnerability Scanning Service gives development teams the confidence to develop their code on instances with the latest security patches and helps ensure a smooth transition to building production code. It allows the operations teams to gain a unified view of all instances to quickly remediate any open ports or patch unsafe packages discovered by the Vulnerability Scanning Service.

7.3) Tool Selection

[SecureCyberGates] conducts vulnerability scanning using SonarQube code scanner, Burp Suite Professional, OWASP ZAP, GITLAB Dependency Scan, GITLAB SAST/DAST. These scans are done before any source code is released to production or if there is any new infrastructure added. There are also periodic audits from clients or other external parties. Security team along with other teams would analyze vulnerability severity, priority, Impact and Remediation plans.

Note: Depending on need, [SecureCyberGates] may use any relevant tool for vulnerability scanning

7.4) Patch Management Lifecycle

[SecureCyberGates] Application Framework has internal deployment and patch manager. This manager automatically generates deployment packages by extracting changes from source code between different commit points on release branches. It eases rolling out upgrades and fixes.

Patch Management controls that [SecureCyberGates] adheres to are as follows:

For any vulnerabilities that needs to update / patch to higher versions [e.g., Update Development Libraries, O.S Security update, DB version update etc.] then a stable version that does not have Critical/High CVE should be selected and it should be first applied to development environment.

Patch Testing: All patches and updates will be thoroughly tested in a non-production environment before deployment to minimize the risk of system disruptions or compatibility issues.

Patch Deployment Schedule: A regular patch deployment schedule will be maintained to ensure that critical patches are applied in a timely manner, with minimal disruption to business operations

Regardless of the type of patch to be installed, the patch management process consists of four (4) distinct steps that must be followed:

- Assess
- Identify
- Evaluate & Plan
- Deploy

Assess

Processes:

- Create and maintain a baseline of systems;
- Assess patch management architecture;
- Review infrastructure / configuration;
- Discover assets; and
- Inventory clients.

Questions to Answer:

- Are there any threats or vulnerabilities in the environment?
- Has anything changed in production?

Identify

Processes:

- Identify new patches;
- Determine patch relevance and
- Verify patch authenticity & integrity.

Questions to Answer:

- Is the patch relevant to the organization?
- Does this Patch applicable for Core application Framework?
- Which systems [Web Application, Server OS etc.] need to be patched?
- Do all systems need to be patched with the same level of priority?
- Which systems are most vulnerable?
- Has the patch been downloaded and checked to be virus free?
- Does the patch install successfully on a trial system?
- Has a Request for Change (RFC) been submitted for this patch?

Evaluate & Plan

Processes:

- Test the patch, if possible;
- Perform a risk assessment for possible repercussions from patching or not patching;
- Obtain approval from the Management to deploy the patch; and
- Plan the patch release process and notify affected parties.

Questions to Answer:

- Can the patch be combined with other changes to minimize downtime?
- Do business-critical functions still work after the patch is installed?
- How and when is best to install the patch?
- What are considerations for mobile clients and connections across slow or unreliable networks?

Deploy

Processes:

- Distribute and install the patch(es);
- Report on progress to the Management;
- Handle exceptions with a coordinated mitigation plan; and
- Review deployment for future process improvement.

Questions to Answer:

- Does the production environment need to be prepared for new patches?
- Are users fully informed of possible downtime or issues?
- Have “lessons learned” from previous deployments been successfully implemented?

7.5) Patch Process overview

- When a vulnerability is identified, the Security team, in conjunction with the asset owner and IT staff, should determine if it affects any assets.
- If a patch does not exist, then a workaround should be analyzed to determine if compensating controls should be implemented.

7.6) Patch Review Process

A patch must be reviewed by all applicable stakeholders (e.g., Clients, IT, information security, process engineering, operations, and the asset owner) to determine if there is an immediate need to patch the asset (e.g., “out of band” patching) or if the patch should follow the standard patching cycle.

7.7) Issues to Consider

The following issues should be considered when creating the patch management plan and the processes and policies related to it:

- Testing [in Lower environments]
- Archiving/ Data Backups

- Contingency
- Regulatory Requirements
- Implementing Patches

7.8) Implementing Patches

It is always recommended to deploy patches in order of less critical to more critical. This can be accomplished by first deploying patches to test environments, followed by staging environments, and finally to production environments.

7.9) Remediation Operation & Enforcement

Systems and applications not remediated within the required remediation schedule or timeframe will be classified as non-compliant and will be quarantined. Under normal circumstances, non-compliant system and application owners will be provided a warning seven (7) days prior to removal from the network and quarantined. If quarantining is not technically feasible, compensating controls will need to be implemented to mitigate the risk.

The assessment of risk should be in accordance with [SecureCyberGates]'s Risk Management Program **Document ID** "SCG/RMF/015/1.0"

8) Employee Training and Awareness

8.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

8.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

9) Compliance and Monitoring

9.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

9.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

9.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this policy. These audits may include, but are not limited to:

- Reviewing Access Controls for System / Applications.
- Review Access Management Policy.

10) Escalation Matrix

10.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

10.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

10.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

11) Policy Exceptions

11.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

12) Policy Review and Updates

12.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

12.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

12.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

12.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for

familiarizing themselves with the latest version of the policy and adhering to its requirements.

13) Conclusion

By implementing and adhering to this comprehensive VPMP policy, [SecureCyberGates]aims to protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for password construction, protection, management, and system development standards.

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SecureCyberGates
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES