GINRŌ GUARD

CapsuleCorp

Vulnerability Management Policy Example

Date: September 28, 2025
Project: CCorp-VMP-2025-09-A
Policy Author: Baptiste Bellecour
Version: 1.0

Confidentiality Notice

This policy document contains confidential and proprietary information. It has been prepared exclusively for the internal use of CapsuelCorp. Unauthorized distribution, disclosure, or reproduction of this document is strictly prohibited. The content is intended to support CapsuleCorp's governance, risk, and compliance framework and should be safeguarded in accordance with the organization's information classification standards.

Disclaimer

This policy document is provided by GINRŌ GUARD for advisory purposes. While it is based on industry standards and best practices, it must be reviewed, adapted, and formally approved by CapsuleCorp's management before adoption. GINRŌ GUARD makes no warranties, express or implied, and shall not be held liable for any damages arising from the use or implementation of this policy without proper review, customization, and oversight by CapsuleCorp.

TABLE OF CONTENTS

Vulnerability Management Policy

Organization	CapsuleCorp
Owner	Dev BOB - CISO - CapsuleCorp
Author	Baptiste BELLECOUR - GINRŌ GUARD
Approved by	CEO, CRO, CISO
Effective data	2025-10-14
Review cadence	Annual, or after significant change

1 - Purpose

The purpose of this policy is to establish a structured and consistent approach for identifying, assessing, prioritizing, and remediating vulnerabilities across CapsuleCorp's technology environment. By defining clear responsibilities, remediation timelines, and verification requirements, this policy supports CapsuleCorp's governance, risk, and compliance framework. Effective vulnerability management reduces the likelihood of security incidents, ensures alignment with regulatory and contractual obligations, and helps maintain business continuity and stakeholder trust.

2 - Scope

In scope	Corporate laptops, servers, networks, cloud accounts, containers, CI/CD, source code repos, third-party SaaS.
Out of scope	Personal devices not enrolled in MDM, client-owned assets unless contractually managed.
Environment	• Production • Staging • Dev • Sandboxes

3 - Policy Statements

- All in-scope assets must be scanned on a defined cadence.
- Critical and High findings are tracked to closure with service-level targets.
- Emergency patching can bypass normal change windows with post-review.
- Exceptions are time-bound, risk-accepted by the Security Lead.
- Remediation is verified by rescans or targeted tests before closure.
- Metrics are reported monthly to leadership.

4 - Roles and Responsibilities

Security Lead	Sets strategy, approves exceptions, reports metrics.
Vulnerability Analyst	Triage, correlate, de-duplicate, propose priority, assess.
Cloud Ops	Patch OS, platforms, and infrastructure, maintain inventory.
DevSecOps	Integrate SCA, SAST, DAST, container and IaC scans in CI/CD.
Asset Owners	Validate fixes, schedule maintenance windows.
Vendors/Suppliers	Meet or exceed our SLAs per contract, provide evidence.

5 - Asset Inventory and Classification

Maintain a single authoritative inventory including: owner, environment, internet exposure, data class, business criticality, OS/version, tags. Inventory drives scan scope and SLA tiering.

6 - Discovery and Assessment

Network and host scanning

- Internet-facing prod: weekly
- Internal prod and cloud workloads: monthly
- Staging/dev: monthly, plus pre-release scans

Application security

- SCA/SAST - every PR or commit.
- DAST - before each major release and quarterly for key apps.

Containers and images

- Scan on build and before deploy.
- Prefer credentialed scans where feasible to reduce false negatives.

7 - Prioritization Model

Risk = Severity x Exploitability x Exposure x Business Criticality.

Key inputs include the CVSS base score, inclusion on known exploited vulnerability lists, public exploit availability, level of internet exposure, data classification, and service tier. This model ensures that both technical severity and business context are considered.

When two or more findings result in the same calculated risk score, prioritization is applied in the following order: (1) vulnerabilities on internet-exposed assets, and (2) vulnerabilities affecting systems with the highest business criticality.

8 - Remediation Targets (SLAs)

SEVERITY	RISK SCORE	TARGET	DESCRIPTION
CRIT	9-10	7 Days	RCE on internet-facing
HIGH	7-10	14 Days	Priv-esc on prod host
MEDIUM	4-6	30 Days	Lib with limited exposure
LOW	2-3	90 Days	Minor info leak, no exposure

Emergency fixes may be applied sooner. If patch is not available, use mitigations and raise an exception.

9 - Change and Release Control

Normal patches must follow the organization's established change control process and, whenever practical, should be tested in non-production environments prior to deployment. In situations where a Critical-risk vulnerability requires immediate action, emergency patches may be applied outside of the normal change window. In such cases, a post-implementation review must be completed within 48 hours, and a documented rollback plan must be in place to mitigate any unintended impact.

10 - Validation and Closure

All remediation efforts must be verified through a targeted re-test or re-scan to ensure that the vulnerability has been effectively addressed. Closure of a finding requires documented evidence, which may include the associated ticket, change record, commit or build link, and a scan report confirming that the issue does not recur. A vulnerability is not considered resolved until verification is complete and evidence is formally recorded in the tracking system.

11 - Exceptions and Compensating Controls

If a vulnerability cannot be remediated within the defined timeframe, an exception may be requested. All exceptions must be formally documented, time-bound, and include a clear end date, the designated risk owner, the rationale for the exception, and the compensating controls implemented to mitigate residual risk. Examples of compensating controls may include web application firewall rules, network access controls, policy hardening, rate limiting, or the use of feature flags. Exceptions must be reviewed and approved by the Security Lead, and they are tracked within the same workflow and ticketing system as standard vulnerability findings to ensure visibility and accountability.

12 - Third-Party and SaaS

Third-party providers and SaaS vendors that process or store CapsuleCorp's data are required to adhere to security clauses that mandate timely vulnerability management, defined patching timelines, and evidence sharing upon request. For vendors deemed high-risk, CapsuleCorp requires an annual penetration test or independent security assessment, accompanied by formal attestation of remediation for any identified vulnerabilities.

13 - Metrics and Reporting

Vulnerability management metrics must be compiled and reported to leadership on a monthly basis to ensure transparency and accountability. Reports will include the number of open findings by severity and age, adherence to defined service-level targets, and the median time to remediate vulnerabilities across different environments. Additional metrics include scan coverage rates, the number of known exploited vulnerabilities that remain outstanding, and recurring root causes with corresponding prevention actions. These metrics provide management with a clear view of risk trends and the effectiveness of the organization's vulnerability management program.

14 - Incident Linkage

If exploitation of a vulnerability is suspected or confirmed, the issue must immediately be escalated and treated as a security incident. An incident record must be opened, and the security team will coordinate containment, eradication, and recovery activities in line with the organization's incident response procedures. Lessons learned from the incident must be documented and integrated into future hardening measures, patch management processes, and vulnerability remediation plans to reduce the likelihood of recurrence.

15 - Training and Awareness

All personnel involved in vulnerability management, including engineers, IT staff, and developers, must receive annual training on patch coordination, safe rollback procedures, and emergency change handling. This training ensures that staff are equipped to respond effectively to both routine and urgent remediation activities. In addition, all new employees whose roles involve system administration or development are required to complete onboarding guidance on vulnerability management practices as part of their initial training. Regular refreshers and updates are provided when significant changes are made to the organization's processes or supporting technologies.

16 - Review and Maintenance

This policy must be reviewed at least annually by the Security Lead, or more frequently if significant incidents, audits, regulatory updates, or architectural changes occur. Each review will assess the policy's continued relevance, alignment with industry standards, and effectiveness in supporting CapsuleCorp's governance, risk, and compliance framework. Any updates or revisions must be versioned, formally approved by management, and communicated to all affected stakeholders to ensure consistent application across the organization.

Annexes

Annex A - Scan Cadence Matrix

Asset group	Environment	Cadence	Method	Credentialed
Public web apps	All	Monthly	DAST	yes
Internet-facing hosts	Production	Weekly	Host scanner	no
Internal workloads	Production	Monthly	Host agent	yes
Cloud assets	Pipeline	Every build	Images scanner	yes
Source repos	All	Each commit	SAST	yes
Internal apps	Staging	Pre-Release	DAST	yes

Annex B - RACI Table

Activity	Leads	Analyst	Cloud Ops	DevSecOps	Owner	Vendor
Maintain inventory	A	C	R	C	C	C
Run scans	C	R	R	R	C	C
Triage findings	A	R	C	C	C	C
Remediate infra	C	C	R	C	C	C
Remediate code	C	C	C	R	C	C
Verify fix	A	R	R	R	C	C
Exceptions	A	C	C	C	C	C

A = Accountable, **R** = Responsible, **C** = Consulted

Annex C - Ticket Workflow

When a vulnerability is identified, the scanner or CI tool automatically generates a ticket containing key details such as the asset tag, severity, exploitability, exposure level, and assigned owner. The Vulnerability Analyst is required to triage the ticket within two business days, confirming the accuracy of the severity rating and establishing the appropriate priority. Once triage is complete, the ticket is assigned to the designated remediator, and a target remediation date is set in accordance with the defined SLA. The assigned team implements the fix and ensures it is properly verified. The ticket is then closed with supporting evidence, such as a scan report or change record, or escalated through the exception process if remediation is not feasible within the required timeframe.

Annex D - Exception Request Template

When a vulnerability cannot be remediated within the defined SLA, an exception request must be submitted and formally documented. The request must clearly identify the vulnerability by ID and asset, include the severity level, and provide a detailed explanation of why remediation is not feasible within the required timeframe. The request must also specify the compensating controls in place, along with evidence of their effectiveness in mitigating the associated risk. A proposed end date must be included to ensure the exception remains time-bound. Final approval requires confirmation from the designated risk owner as well as formal sign-off from the Security Lead.

Annex E - Metrics Definitions

To ensure consistent measurement and reporting, vulnerability management metrics must be defined in clear and standardized terms. Coverage is measured as the ratio of assets scanned during the reporting period compared to the total number of in-scope assets, providing visibility into the effectiveness of the scanning program. Mean Time to Remediate (MTTR) is calculated as the median number of calendar days between ticket creation and verified closure, reflecting the speed of remediation efforts. SLA adherence is measured as the percentage of vulnerabilities closed within the defined service-level window for each severity tier. In addition, the Known Exploited Vulnerability (KEV) backlog represents the number of open findings that have confirmed active exploitation in the wild. These definitions provide a common framework for tracking program performance and communicating results to leadership and auditors.

Annex F - Optional Local Notes

This section is reserved for documenting any organization-specific requirements or contextual information that may influence vulnerability management activities. Local notes may include coordinated vulnerability disclosure contacts and escalation procedures, regulatory or contractual obligations that define stricter patch windows, or customer requirements that affect remediation timelines. Organizations may also include platform-specific playbooks, operational maintenance windows, or other practical guidance tailored to their technology environment. These local notes serve as a supplement to the core policy, ensuring that CapsuleCorp's vulnerability management practices remain aligned with both external obligations and internal operational realities.

Operational Handoff

This checklist provides a practical reference for teams to confirm that all foundational elements of the vulnerability management program are in place and ready for execution.

- Inventory complete with owners and tags
- Scan jobs scheduled per Annex A
- CI checks for SCA/SAST enabled
- Ticket templates and fields live
- Exception workflow enabled
- Monthly metrics dashboard configured