

Vulnerability Management Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy sets how [Company name] (the "Company") finds, tracks and fixes vulnerabilities and protects its network. It supports the SOC 2 common criteria CC6.6 and CC7.1 by establishing controls to protect the network and manage vulnerabilities.

This policy applies to all production networks and [In-scope systems].

2. Finding vulnerabilities

- Dependencies, container images and infrastructure code are scanned automatically with [Vulnerability scanner], and the results are reviewed at least monthly.
- External and internal scans of the production environment run at least monthly.
- An independent penetration test of the production application runs at least once a year.
- Reports from customers, researchers and vendor advisories are treated as findings.

3. Fix deadlines

Every confirmed finding is recorded with its severity, an owner and a due date set by the table below. Adjust the days to deadlines the Company can meet, because the policy is tested against what it says.

Severity	Fix within	Example
Critical	7 days	Remotely exploitable flaw in a production system, or one already being exploited.
High	30 days	Serious flaw that needs some access or user action to exploit, such as an outdated library with a known exploit.
Medium	90 days	Flaw with limited impact or hard to exploit, such as a missing security header.

Severity	Fix within	Example
Low	180 days	Minor hardening item or informational finding.

A vulnerability known to be exploited in the wild is treated as Critical, whatever its score.

4. Patching and tracking

- Patching: Security patches for operating systems, images and dependencies are tested and deployed within the fix deadlines in section 3. Company devices install updates automatically.
- Tracking: Each finding is closed only with the date it was fixed and a link to the evidence, such as the pull request or the clean rescan.

5. Accepted vulnerabilities

A finding that will not be fixed by its due date is accepted only in writing by the [Policy approver role], with the reason, any compensating control and a date to look again. Accepted findings are reviewed every quarter.

6. Network security

- Firewalls and security groups: Network rules deny by default and allow only the traffic the service needs. Rules are reviewed every quarter.
- Application filtering: Public traffic to the application passes through [Web application firewall] where one is in use, to block common application attacks.
- Segmentation: Production and non-production environments are logically separated.

7. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
Finding owners	[Engineering owner role]	Fix assigned findings by their due date and record the evidence.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

8. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Firewall rules	Screenshot of current rule set.	[Cloud provider]
Vulnerability scan results	Reports from the scanning tool.	[Vulnerability scanner]
Patch status report	Report showing current patch compliance.	[Device management tool]
Vulnerability tracker	Every finding with its severity, owner, due date and fix date.	[Evidence storage location]
Penetration test report	The annual test and the fixes it led to.	[Evidence storage location]

9. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

10. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

11. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[In-scope systems]	The product, cloud accounts and tools inside the audit boundary.
[Cloud provider]	Where production runs, for example AWS, Google Cloud or Azure.
[Web application firewall]	The service that filters traffic to the application, if you use one.

Field	What to enter
[Vulnerability scanner]	The tools that scan code, containers and hosts.
[Device management tool]	The tool that enforces settings on company devices.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[Engineering owner role]	The role that owns production systems, for example engineering lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/vulnerability-management-policy (CC BY 4.0).