Vulnerability and patch management policy

Policy | English · Template to adapt | v3.0 · 2026-10-16

Template version: 3.0. Type: policy and operational procedure. Proposed adoption profile: an organization of approximately 80 people, with user devices, hosted services and IT operations potentially managed by a supplier. This profile makes no statement about your business. An internal owner retains prioritization, interruption, exception and risk-acceptance decisions even when discovery and deployment are outsourced.

After adaptation and adoption, “must” and the instructions below apply within approved scope. The policy owner must complete fields, confirm capabilities and contracts and obtain named approval. This policy guarantees neither compliance nor absence of vulnerabilities. Schedules require local decisions; no universal remediation deadline is introduced. The document must not be presented as proof that the adopting organization already performs its controls.

1. Purpose, scope and adoption

This policy organizes discovery, assessment, treatment and verification of exposure. It covers systems, applications, libraries, network devices, firmware and services included in inventory. Distinguish what the organization administers, what the supplier patches and which settings remain the organization's responsibility. Describing a service as cloud-hosted is not a sufficient allocation of responsibility.

Scope must address remote devices, infrequently connected equipment, administrative workstations, backup infrastructure, exposed services and relevant development components. Industrial or sensitive systems follow methods approved by their safety owners. Exclusions retain asset, reason, owner and risk treatment. An asset must not disappear from inventory merely to improve an indicator.

Adoption decision	Local value	Authority	Evidence
Covered services and assets	[TO COMPLETE: inventories, exclusions, supplier boundaries]	Technical and business management	List reconciled with contracts
Owners and deputies	[TO COMPLETE: lead, operators, security, approvers]	Management	Delegation and acceptance
Priorities and commitments	[TO COMPLETE: levels, starting event, local targets]	Risk authority	Exposure and resource justification
Windows and emergencies	[TO COMPLETE: cycles, authorization, stop and fallback]	Business and operations	Tested procedure
Version and review	[TO COMPLETE: local version, effective date, review, signatures]	Policy owner	Approved distributed document

Before declaring the process operational, follow an advisory through closure on a representative service, including a failure and an exception. If the IT provider cannot show deployment state or inventory coverage, record and treat that limitation before promising a service level. A tool's output is an input to acceptance, not a substitute for the acceptance decision.

2. Roles and decision boundaries

Function	Responsibility	Reserved decision	Absence or failure
Internal owner	Maintain scope, commitments, exceptions and reporting	Accept process readiness	Named deputy with register access

Function	Responsibility	Reserved decision	Absence or failure
Security or MSSP	Assess advisories, plausible exploitation and priority	Recommend; cannot alone accept business risk	Security fallback and contract escalation
IT provider or operator	Check versions, test, deploy and supply evidence	Changes within approved mandate only	Authorized alternate
Business owner	Assess interruption and verify service	Accept window and functional outcome	Named business deputy
Risk authority	Decide deferral, compensation and retirement	Explicitly accept residual risk	Planned delegation, never silent approval
Supplier management	Reconcile support, contract and stated capability	External commitments within authority	Replacement contact

Each campaign must tell the supplier which assets, action, window, constraints, success criteria and escalation apply. Obtain acceptance of both task and evidence expectations. A general commercial agreement does not establish who may act on an application, device or dependency covered by a separate contract. Shared responsibilities must be resolved before the planned change.

If a decision is missing, contact the deputy and record the delay. Preauthorized measures may proceed within their limits; others require an explicit decision. Inform the business owner of continuing exposure and interruption risk. Urgency must not allow a supplier to accept either risk alone. Keep the authorization connected to the affected assets and the planned intervention.

3. Discover and reconcile assets

Reconcile available inventories: endpoint management, directory, network equipment, hosting, applications, licensing and contracts. Identify assets present in one source but absent from another. Record coverage, observation dates and categories not observable. A powered-off or unreachable device must not be considered patched or silently excluded from scope.

For each asset, retain stable identifier, service, owner, environment, observed version, exposure and maintenance method. Link software dependencies to the production application or image. Distinguish installed version, available package and running instance. Check tool-generated inventory against a risk-appropriate sample before treating it as the sole reference. Preserve contradictory observations for resolution rather than choosing the more favorable one.

Discovery gap	Required action	Evidence	Escalation
Ownerless asset	Identify service and accountable person; keep visible	Identifier, sources, attempts	Technical leadership
Conflicting versions	Check locally or with vendor	Method and effective version	Security if urgent
Missing remote device	Contact manager; arrange return or authorized check	Last observation and decided restriction	Internal owner
Unsupported component	Confirm support and treatment options	Supplier reference and plan	Risk authority and business

Active assessments require authorized scope, a window and stop conditions. Fragile systems require operator-approved methods. Results must state what was authenticated or actually checked. A scan with no findings cannot alone distinguish no vulnerability, insufficient access or incomplete coverage. The assessment owner must explain limits before a result supports a treatment or closure decision.

4. Assess advisories and set priority

Security must monitor vendor advisories, CERT-FR advisories and selected primary sources. Retain reference, advisory revision, consultation date and proposed applicability. Revised publications require reassessment of affected findings. An old screenshot must not replace current treatment instructions. The analyst must connect the advisory to the particular product and configuration rather than rely on a similar name.

The CISA Known Exploited Vulnerabilities catalog records known exploitation and can inform priority. Absence from it does not establish that a vulnerability is unexploited. Agency-specific deadlines do not automatically apply to the organization. Combine threat, exposure and consequences rather than copy a deadline without checking its scope.

Situation	Assessment	Proposed decision	Check
Observed or credible exploitation on exposed asset	Applicability, access, privileges, compromise indicators	Urgent treatment and incident assessment	Named protection and verification
Applicable vulnerability on critical service	Actual access path, protections and impact	High priority according to local risk	Explicit window or compensation
Less exposed asset with confirmed defect	Dependencies and movement opportunities	Justified planned campaign	Approved target, not neglect
Unknown applicability	Missing version, configuration or conditions	Bounded investigation with protective priority	Next information, owner and reassessment

The priority record must explain reachability, potential consequences and protections actually checked. Technical severity does not describe business impact alone. Distinguish assumed and tested protection. Missing information requires a protective measure or explicit acceptance of waiting by the competent authority. The reasoning must be understandable to a replacement analyst, not just an unexplained priority label.

Local targets must define their starting event: detection, confirmed applicability or treatment availability. Preserve these dates separately. An extension must not artificially reset the finding's age. Changes in threat or exposure may accelerate an already approved ordinary window. The lead must record both the revised decision and any business or resource constraint that remains unresolved.

5. Validate treatment and prepare change

Operators must confirm product, version, configuration, prerequisites and dependencies before selecting a package or mitigation. Read vendor instructions and verify provenance and integrity using available methods. Link download information, intended version and known restrictions to the ticket without attaching administrative secrets. Uncertain authenticity is a stop condition, not an acceptable shortcut justified by urgency.

Testing must represent the affected service, authentication, application access, scheduled work, backup and monitoring where relevant. Define stop criteria and a realistic fallback. A successful backup job does not itself demonstrate restoration. Rollback may be unavailable or restore vulnerability; decide that risk before intervention. The test report must identify which functions were exercised and which were not.

Preparation check	Owner and input	Required result	Failure and decision
Applicability	Operator; version and advisory	Confirmed defect or reasoned exclusion	Reassess priority; no empty closure
Treatment provenance	Operator; vendor channel	Identified package and validation	Stop suspect installation

Preparation check	Owner and input	Required result	Failure and decision
Technical test	Operator; environment and criteria	Recorded results, version, effects	Revise plan or compensate
Business validation	Owner; representative operation	Expected function demonstrated	Reject broad rollout or decide degraded service

Prepare a change record another operator can use: targets, sequence, justified duration estimate, stop conditions, contacts and completion check. Estimates are not guarantees. Missing skills require an authorized fallback or deferral under a risk decision, not permission to improvise. The lead must ensure that decision-makers understand limitations before authorizing the window.

6. Run an ordinary campaign

Group assets by technical characteristics, criticality and maintenance constraints. Validate group membership: laptops, business servers and network equipment do not necessarily share a method. Preserve the starting population so actual coverage can be measured. Assets discovered during the campaign require an explicit inclusion or follow-up decision rather than disappearing between successive reports.

Begin with the approved representative group, check outcomes and expand according to criteria. Include required restarts, reloads and redeployment. A library updated in a repository but not in running instances remains incomplete treatment. Stop expansion when unexpected results mean risk is no longer understood. The operator must keep the lead informed of affected service and current state.

☐ Confirm population, owners, dependencies and window.

☐ Check operator access, package and current instructions.

☐ Confirm fallback resources and stop conditions.

☐ Inform people affected by planned interruption.

☐ Execute the pilot and retain results and errors.

☐ Verify effective version and business operation before expansion.

☐ Record successful, failed, excluded and unobserved assets.

☐ Assign retry actions and report reservations to the lead.

Closing the window must produce explicit status. A powered-off or inaccessible asset receives follow-up, not presumed success. Unexpected changes require explanation and authorization under the applicable procedure. If rollback was used, verify resulting exposure and temporary protection separately. The report must state the service's actual operating state, not merely whether the installation tool finished.

7. Emergency, suspected exploitation and no-patch treatment

During an emergency, security, operations and business owners must choose available protection: accelerated patching, access restriction, disabling a function or retiring service. Record threat, measure impact and next check. Missing ordinary testing requires focused testing and an explicit decision; it must not be hidden. Supplier requests must specify exactly which emergency authority was invoked.

Suspected exploitation must initiate incident response. Coordinate patching and investigation to preserve useful evidence and address access already obtained. Fixing the defect does not establish that an attacker is absent. Identify who investigates, who protects service and who authorizes its return. A patch ticket must not silently replace the incident record and its remaining questions.

Emergency branch	Minimum action	Verification	Escalation
Available, testable patch	Test essential functions; expand progressively where possible	Actual version and service	Failure to business and security

Emergency branch	Minimum action	Verification	Escalation
No patch	Check proposed exposure reduction	Access or function actually restricted	Accepted risk, target and vendor follow-up
Service cannot stop	Define degraded operation or suitable protection	Observable compensation	Risk authority, not supplier alone
Compromise indication	Open incident; coordinate collection and containment	Known and unknown extent recorded	Incident lead

Temporary protection requires an owner and replacement condition. Once durable treatment is available, decide when to apply it and withdraw unnecessary compensation. Removing a restriction before confirming the patch may restore risk; keeping an emergency measure indefinitely may impair service. Record the transition so another operator can verify that neither step was assumed complete.

8. Legacy assets, exceptions and accepted risk

Unsupported or unpatchable assets require a specific record: essential use, owner, dependencies, replacement options and exposure. Operators must explain why patching is impossible and what was tested. Business owners must assess restricted use or replacement. “Critical application” alone does not justify an exception. A long-lived limitation requires an explicit plan, not repeated administrative renewal.

Exception field	Completed fictional example	Blank local value	Validation
Asset and constraint	Old test gateway; incompatible business software	[TO COMPLETE]	Owner and evidence
Compensation	Restricted approved-network access; logs checked	[TO COMPLETE]	Test and operator
Accepted risk	Restriction failure or use outside scope	[TO COMPLETE]	Named internal authority
Exit and expiry	Replacement linked to business project; review before locally set expiry	[TO COMPLETE]	Owner and next decision

Expiry must be a real local date completed before approval. The example does not waive that decision. Verify compensation at the approved frequency and after threat changes. At expiry provide correction, retirement or new justification. Silent renewal and acceptance by the operator alone are prohibited. Keep the original exposure and treatment history available throughout the exception.

9. Verify and close using evidence

Link each asset to its finding, change and performed check. Security must assess whether evidence addresses the defect: running version, configuration, restart or authorized reassessment. Closure must distinguish confirmed correction, temporary protection, accepted risk, demonstrated non-applicability and unknown state. These are not interchangeable successes and must remain separate in management reports.

Outcome	Required evidence	Next action	Closure authority
Corrected	Effective treatment on actual target	Monitor side effects	Process owner
Failed	Error and current state preserved	Decide retry or compensation	Lead, with business if affected

Outcome	Required evidence	Next action	Closure authority
Not applicable	Verified version/configuration and reason	Reassess on change	Security and owner
Unknown	Missing verification explicit	Obtain access or other evidence	Never close as corrected
Temporarily protected	Verified measure and limits	Plan patch or retirement	Risk authority

Reconcile supplier “installed” reports with the intended population. Identify absent rows, duplicates and conflicting versions. Errors must not vanish on retry. History must explain the exposure period without inventing a protection date. If the supplier cannot provide evidence, the internal owner must arrange another check or preserve unknown status with a decision on continued operation.

10. End-to-end fictional scenario

Fictional Atelier Rivage uses a remote portal managed by an IT supplier. A primary advisory may affect its version. The MSSP identifies plausible exposure; the supplier's inventory is old. The internal lead rejects the stale list as proof and requests a current observation. This is an exercise, not a customer result or a claim about a particular product.

Stage	Fictional decision	Expected evidence	Acceptance criterion
Discovery	Confirm asset and effective version	Observation linked to portal identifier	Applicable advisory or reasoned exclusion
Priority	Exposure justifies urgency	Access path and limits stated	Authority and next check named
Treatment	Temporary restriction, then tested patch	Restriction test and pilot result	No protection claim without verification
Deployment	One node succeeds; another remains unreachable	Two distinct states	No claim of complete campaign success
Closure	Remaining node checked after authorized retry	Running version and business test	History retained; compensation removed by decision

Acceptance requires a deputy to explain why the second node was not corrected, locate the accepted risk during the delay and demonstrate final verification. They must reject a favorable percentage obtained by excluding the unreachable node. They must also distinguish vulnerability treatment from investigation of possible exploitation. The exercise fails if either decision is replaced by a tool's success label.

11. Working registers and adoption test

Finding record	Required information	Owner	Completion check
Identification	[TO COMPLETE: advisory, revision, asset, version, service]	[TO COMPLETE]	Applicability and coverage
Decision	[TO COMPLETE: exposure, impact, priority, target]	[TO COMPLETE]	Approved reasoning
Change	[TO COMPLETE: test, window, sequence, stop, fallback]	[TO COMPLETE]	Approval and outcomes

Finding record	Required information	Owner	Completion check
Verification	[TO COMPLETE: method, date, effect, reservations]	[TO COMPLETE]	Explicitly qualified status
Exception	[TO COMPLETE: compensation, risk, decision-maker, expiry]	[TO COMPLETE]	Review and exit

Before adoption, test an applicable advisory, a version false positive, a remote asset, a failed deployment and a legacy asset. A replacement owner must locate decisions and reactivate the supplier task. Document unavailable capabilities. Another tool does not replace allocation of responsibility and verification of changes. Store a completed test example alongside the blank register for future operators.

12. Assurance, enforcement and revision

At [TO COMPLETE: body and cadence], report coverage, overdue findings, unobserved assets, expiring exceptions and unverified treatment. Every indicator must identify period, population and source. Gaps require assigned correction or accepted risk. Unknowns must remain visible even when they make results look worse. Reports must allow management to identify the decision needed, not merely present counts.

Unauthorized intervention, unsupported closure and expired exceptions must be examined by the owner. Decide immediate protection, operational consequences and follow-up with competent functions. This policy creates no automatic sanction; consequences follow internal rules and applicable obligations. Suppliers must participate in correcting their own process gaps, with internal acceptance of the corrective evidence.

Review after incidents, significant failure or changes in technology, supplier or responsibility. Preserve author, reason, approval and superseded version in [TO COMPLETE: repository, access and retention]. Inform operators of new rules. Reconfirm targets and frequencies against actual risk rather than simply carrying them forward from an old document.

Primary sources and limitations

NIST SP 800-40 revision 4, April 2022, particularly §2.2–2.3 and §3.2–3.6, addresses inventory, risk response, deployment, verification, maintenance groups and exceptions. NIST SP 800-61 revision 3 provides incident-response context when exploitation is suspected.

The matrices, roles, examples and local requirements are a Seculogik proposal, not universal normative reproduction of these sources. Check current vendor instructions and safety constraints before acting. No tool, provider or percentage guarantees absence of defects or removal of hostile access established before treatment.