Security logging and monitoring policy

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

Template version: 3.0. Type: policy and procedures for acceptance, monitoring and handling gaps. Proposed adoption profile: an organization of approximately 80 people, potentially using an IT provider and MSSP. This does not assert that your tools collect the events described. An internal owner retains decisions about uses, permissions, accepted coverage and risks arising from missing sources.

After adaptation and adoption, “must” and operational instructions become internal requirements within approved scope. Before adoption they remain proposals. Confirm capabilities, contracts and people, then approve parameters and exceptions. This document guarantees neither exhaustive detection, compliance nor automatic evidential status. Hours, frequencies, thresholds and retention require local decisions; no universal values are prescribed.

1. Purpose, scope and approval

Logging must support defined security questions: access, sensitive changes, operations and protection status. Monitoring must connect observations to a person responsible for assessment and action. Accumulating logs without an intended use, controlled access or alert recipient is not demonstrated capability. Distinguish collection, search, detection and response actually available rather than describe them as one interchangeable function.

Scope must cover priority services and dependencies: identity, endpoints, remote access, network, applications, hosting and the collection pipeline. Outsourced services must identify accessible categories, export, licensing, location, responsibilities and contractual limits. Personal or industrial devices need suitable authority and methods. Missing sources must remain visible, together with the investigation questions they prevent the team from answering.

Parameter	Local decision	Owner	Evidence before adoption
Uses and scope	[TO COMPLETE: services, scenarios, exclusions]	Internal owner and business	Questions and sources register
Monitoring	[TO COMPLETE: hours, staffed on-call, fallback]	Internal owner and MSSP	Contacts and receipt exercise
Protection and access	[TO COMPLETE: storage, roles, export, administration]	Operations and security	Access and separation tests
Retention and data	[TO COMPLETE: categories, justification, periods, deletion]	Competent functions	Decision by use and constraint
Document control	[TO COMPLETE: version, effect, approver, review]	Management	Approval and controlled distribution

Before the policy takes effect, demonstrate a source through handling of an authorized benign event. Test an outage and a refused access attempt as well. Results must identify missing capability. Adoption must not label an integration operational merely because an agent is installed or a dashboard shows volume. The internal owner must decide whether demonstrated scope is sufficient.

2. Responsibilities and supplier boundaries

Function	Responsibility	Decision boundary	Fallback
Internal owner	Decide uses, coverage, exceptions and resources	Internal risk acceptance	Deputy with register access

Function	Responsibility	Decision boundary	Fallback
Source owner	Authorize configuration, categories and changes	No promise of unverified export	Alternate service owner
IT provider	Configure, transport, store and monitor collectors	No silent collection reduction	Technical escalation and authorized operator
MSSP or analysts	Assess alerts and document scenarios and limits	No business action outside delegation	Handover and contractual contact
Security and access management	Define and test permissions	Justified access, not general availability	Named replacement
Legal and privacy functions	Assess uses, preservation and obligations	No universal legal rule inferred	Approved alternate advice

Specify who configures a source, checks rejections, receives outage alerts and verifies correction. Contracts must cover data access, return and service termination. Outsourcing monitoring must not remove the organization's ability to understand gaps or recover authorized evidence. Provider statements must be linked to the service and the capabilities actually purchased.

During absence, tasks must be transferred and accepted. If the MSSP does not cover a period, decide who receives urgent signals or explicitly accept that risk. Automation without a recipient must not be described as handling. Test the fallback and retain the result. An escalation number that nobody has tested must remain an unverified dependency in readiness assessment.

3. Build coverage from investigation questions

For each priority service, business and security owners must define questions: which account accessed it, which operation succeeded, which permission changed and which device observed a connection? Link each question to a category, required fields, owner and test event. A list of products does not replace this mapping or demonstrate that the needed data exists.

Proposed question	Required observation	Local verification	Limitation
Who obtained access?	Stable identifier, service, result, period	Locate a known test sign-in	Shared account, missing category, absent context
Which permission changed?	Before/after if available, technical actor, target	Authorized benign change	Incomplete history or unknown human attribution
Which application operation?	Type, target, outcome, reference	Search a known action	Partial collection or missing session association
Does collection work?	Agent, transport, parsing and storage state	Simulated interruption or delay	Monitoring depends on failed component

Distinguish planned source, verified emission, receipt, interpretation and tested detection use. A source that emits while a parser rejects a critical field is not fully operational. The internal owner must approve actual status. Analysts must see the limitation while assessing alerts, rather than only in an administrative document disconnected from their working process.

Priorities must reflect selected risks and resources. Each integration must state enabled and disabled categories, license or cost limits, available history and lost periods. Enabling a category today does not create historical events retroactively. The supplier must confirm export limitations; the organization must decide their effect on planned investigations. Coverage changes require an updated acceptance record.

4. Configure and accept a source

The source owner must provide identifier, version, configuration, technical identity, protocol, destination and maintenance responsibility. Operators must use authorized change, restrict permissions and plan fallback if logging disrupts service. Sensitive systems require testing with their operator; indiscriminately enabling detail incompatible with operation is not an acceptable implementation of this policy.

Generate an identifiable benign event and locate it at available stages: source, collector, storage and search. Compare fields, time, result and origin. Transformations must preserve meaning and a link to original format where needed. Filters and exclusions must be known. Silent rejection must not be presented as nonexistence of the underlying activity.

Acceptance check	Input and operator	Required evidence	Failure and decision
Emission	Owner; authorized event	Source record and configuration	Correct or record missing capability
Transport	Operator; route and technical identity	Receipt linked to origin	Identify failure, permission or format
Interpretation	Analyst; expected fields	Source/search comparison	Fix parser; limit affected scenarios
Use and handling	MSSP; rule or test search	Result and identified recipient	Do not announce operational detection

The acceptance record must identify reviewer, date, scope and reservations. The internal owner explicitly accepts or rejects operation. Rejection must not erase already useful records; state the restricted use permitted. Retest corrections and preserve the previous result. A supplier's declaration must be distinguishable from the organization's reviewed acceptance and any conditions attached to it.

5. Control time and identifiers

Operators must verify coherent clocks and selected time references. Retain event time, time zone or reference, receipt time and known offsets. Configuration must support explanation of conversions and seasonal changes. A clock correction must not silently rewrite the history used in an investigation. Keep source-time uncertainty separate from transport delay.

Compare a known event on the source with its searchable representation. Justify acceptable tolerance by intended use: [TO COMPLETE: reference, tolerance, method]. If exceeded, limit temporal conclusions, inform analysts and correct the cause. A late arrival and an incorrect source clock require different explanations; one must not be used to conceal the other.

Identifiers must remain stable or interpretable: account, endpoint, service, tenant or network context as appropriate. A reused address alone cannot establish a historical endpoint; an account display name does not prove a person. Normalization must preserve unknowns and avoid replacing missing values with assumed identities. Source owners must explain relevant changes to identifiers and their historical interpretation.

6. Protect transport, storage and confidentiality

Select transfer and storage according to sensitivity, possible loss and constraints. Document paths, permissions, technical identities and transport protections. Check whether outage or saturation destroys events, retains them locally or allows retransmission. Claimed capacity must be compared with the chosen operating conditions. Record what happens outside those conditions so analysts understand possible missing periods.

Separate search, export, configuration, administration and deletion permissions. Investigators do not automatically require collector administration. Exceptional access must be named, authorized and withdrawn at completion. Technical accounts must be limited and tracked; a shared administrative account does not provide the same individual attribution as a personal identity. Explain unavoidable limitations rather than claim equivalent traceability.

Use	Authority and action	Evidence	Negative check
Investigation reading	Authorize defined scope	Identity, case and access	Out-of-role user refused
Export	Authorize content and destination	Reference, recipient, retention	No public or unapproved repository
Administration	Authorized operator implements change	Approval, configuration and check	Analyst without rights cannot modify
Deletion or retention	Designated authority approves rule	Justification and tested execution	Unauthorized deletion refused and reported

Do not deliberately collect passwords, private keys, usable cookies or tokens for ordinary investigation context. Minimize unnecessary personal data. Indispensable exceptions must define access, storage and retention with competent functions. Exports, case attachments, backups and local copies require their own restrictions; protection at the source does not automatically protect subsequent copies or recipients.

7. Detect outage, delay and alteration

Monitor the pipeline itself: silent sources, stopped agents, queues, parsing rejections, saturation, space and access errors. Set thresholds per source and purpose rather than import universal values. Normally quiet sources require suitable checks. Missing volume does not always mean failure, and high volume does not establish quality. Operators must explain the expected activity against which they assess health.

Symptom	Initial verification	Action and evidence	Escalation
Silent source	Expected activity, source state, known emission	Locate break; record affected period	Service owner and MSSP
Delay	Source/receipt time and queues	Establish freshness; track catch-up	Internal owner if investigation affected
Lost critical field	Compare original format	Limit rule; correct and rerun test	Analyst and operator
Suspect deletion/change	Authorization and independent records available	Preserve, restrict under authority, assess incident	Response lead

Test receipt of outage alerts through a channel not wholly dependent on the failed component. If independence is unavailable, document and compensate for or accept the limitation. Supplier requests must identify possibly lost periods, expected restoration and necessary verification. Restarting a service does not prove that every missing event was recovered.

When alteration is suspected, preserve useful evidence and avoid masking traces through unrecorded repair. An integrity alert alone does not prove malicious intent; authorized changes and errors must also be considered. Separate collection restoration from investigation of its cause. The lead must decide whether the situation requires incident response and record what remains uncertain.

8. Retention, privacy and exceptional preservation

Define retention by category and use with competent functions: investigation needs, current access, any archive, contract and applicable obligations. Justify detail and permissions. This policy sets no universal retention duration. A period offered by a tool does not alone justify retaining every data category for that period. Record the decision and its supporting local assessment.

The lifecycle must include deletion and copies. Test that expired data disappears from relevant locations through available mechanisms without affecting authorized preservation. If a backup cannot support

individual deletion, assess that constraint and its treatment. Do not promise immediate erasure that the organization cannot perform. Retain implementation limitations and the authority that accepted their handling.

Decision	Information to retain	Check	Reassessment
Ordinary period	Category, use, reason, authority	Tested search and deletion	Changed obligation or purpose
Restricted access	Role, purpose, authorized population	Access tests and review	Role or assignment change
Case preservation	Scope, reason, authority, review point	Identified copies and access	End of need or competent decision
Supplier export	Terms, destination, return	Recoverable readable example	Contract end or changed capability

Exceptional preservation must remain limited to a case and subject to review; it must not become unlimited archiving of all sources. Competent functions decide specific legal constraints. Analysts should reference authorization rather than distribute legal analysis or unnecessary personal details across every ticket. A preservation decision must say who can lift it and how that decision is recorded.

9. Assess and handle alerts

Each scenario must define objective, sources, known conditions, owner, expected evidence and assessment procedure. Analysts must check original events, target, period and coverage before concluding. Seek an authorized explanation and an independent observation. An alert is neither complete proof of an incident nor evidence that containment was executed. The assessment must state which interpretation is supported.

Stage	Analyst action	Useful evidence	Failure requiring escalation
Accept	Take ownership and verify scope	Owner and next decision	Missing recipient or rights
Assess	Compare source, context and hypotheses	Query, events and unknowns	Missing source or contradiction
Decide	Classify with reason or activate response	Conclusion and authority	Plausible uncontrolled compromise
Tune	Obtain authorization and test change	Version, test and scope	Silent coverage reduction

Tuning must explain unnecessary alerts without hiding service coverage. Exclusions require owner, reason, expiry if temporary and regression testing. Falling alert counts may result from failure; they must not be reported as improvement without coverage checks. The internal owner must accept reservations when a scenario is paused, and the working view must show that pause.

10. Fictional coverage and outage scenario

Fictional Atelier Rivage has approximately 80 staff and an outsourced application. Its MSSP receives sign-ins but not permission changes. The register marks partial emission and forbids describing the change scenario as tested. The IT provider enables an authorized category and performs a benign change. This is an exercise, not customer experience or a product capability claim.

Fictional event	Observation	Decision	Expected result
Initial acceptance	Sign-in present; change missing	Accept partial coverage with reservation	No complete scenario claimed
Configuration change	Category added; test found	Accept the permission-change question	Identifier, target and result checked
Format evolution	Actor becomes empty in search	Pause attribution conclusion	Original source and affected period retained
Repair	Parser fixed; test repeated	Reopen scenario	Possible loss and remaining limits visible

Acceptance requires another analyst to explain conclusions possible during partial coverage, locate the reservation and identify who authorizes resumption. They must distinguish wrong source time from delayed arrival. The exercise fails if volume is used to claim every question is covered. Correctly recognizing an unanswerable question is a valid result requiring treatment, not a defect to hide.

11. Usable annexes and adoption test

Blank source record	Local value	Owner	Acceptance evidence
Identity and purpose	[TO COMPLETE: service, identifier, question]	[TO COMPLETE]	Authorized event located
Categories and fields	[TO COMPLETE: enabled, missing, formats]	[TO COMPLETE]	Comparison with origin
Time and transport	[TO COMPLETE: reference, expected delay, loss]	[TO COMPLETE]	Clock and outage tests
Protection and lifecycle	[TO COMPLETE: access, export, retention, deletion]	[TO COMPLETE]	Positive and refused tests
Monitoring	[TO COMPLETE: hours, contact, action, fallback]	[TO COMPLETE]	Receipt and acceptance

☐ Locate a known sign-in and sensitive operation.

☐ Explain missing fields and uncovered periods.

☐ Verify source time, zone, receipt and delay.

☐ Trigger a benign interruption and obtain ownership.

☐ Refuse unauthorized access and check export.

☐ Test deletion and authorized preservation without conflating them.

☐ Confirm handover and escalation outside genuinely staffed hours.

12. Exceptions, oversight and revision

Exceptions must identify affected purpose, sources, cause, unanswered questions, compensation, owner, decision-maker and expiry. Short retention, missing fields or unexportable sources require explicit assessment. Suppliers must not accept risk alone. At expiry, obtain verified correction or a new decision; silent renewal is prohibited. A waiver records a coverage gap rather than demonstrating that the missing capability exists.

At [TO COMPLETE: body and cadence], report partial sources, lost periods, untested scenarios, exceptional access and expiring waivers. Indicators must state period, population and method. Gaps

require assigned tasks and checks. Unknown state must never count as operational to improve the report. The reviewer must be able to identify the next decision from the evidence supplied.

Format, supplier, purpose and responsibility changes require proportionate review and affected acceptance tests. Record author, reason, approver and previous references. Preserve evidence in [TO COMPLETE: repository, access and retention]. The organization must be able to recover approved records and source documentation at contract termination. A replacement provider must receive limitations as well as the list of nominal integrations.

Primary sources and limitations

The ANSSI logging architecture guide, version 2.0, January 2022 addresses time, coverage, transport, permissions and retention, including R3–R6, R9–R17 and R24–R27. NIST SP 800-61 revision 3 provides context for assessment and protection of investigation records.

The proposed matrices, uses, coverage states, roles and scenarios are local choices to approve and test, not product-capability promises. Adapt official recommendations to actual systems and obligations. This document does not replace privacy assessment or the technical expertise required for reliable collection and defensible interpretation.