Incident response policy and operational plan

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

Template version: 3.0. Type: organizational policy and execution plan. Proposed adoption profile: a business of approximately 80 people, with IT operations and monitoring potentially outsourced. This profile is an adaptation assumption, not a description of your organization. Business decisions, risk acceptance and external communications remain assigned to named internal people.

After adaptation and adoption, “must” and operational instructions express internal requirements within approved scope. Before adoption they remain proposals. The policy owner must complete parameters, verify capabilities and contracts, obtain signatures and distribute a controlled version. This template grants no additional authority and guarantees neither compliance, absence of incidents nor recovery within a specified time.

1. Scope and adoption decisions

The policy covers reports involving identities, endpoints, networks, applications, data, hosted services and suppliers supporting selected activities. The owner must reconcile inventory, contracts and business ownership. Personal devices, external accounts, unmanaged services and industrial systems require an explicit rule covering investigation authority, contact and limits. An exclusion must not silently remove an asset from inventory.

Parameter	Local decision	Approver	Required evidence
Entity and priority activities	[TO COMPLETE: services, sites, data, exclusions]	Management	Dated scope and owners
Lead and deputies	[TO COMPLETE: people, delegation, contacts]	Management	Accepted responsibilities
Coverage and suppliers	[TO COMPLETE: staffed hours, contracts, fallback]	Internal owner	Confirmation and contact test
Response parameters	[TO COMPLETE: targets by severity, updates, retention]	Relevant authorities	Local justification; no universal deadline
Document control	[TO COMPLETE: local version, effective date, review, signatures]	Owner and management	Accessible approved version

Before the effective date, the owner must verify that participants understand their powers, planned collection is possible and urgent changes can be authorized. Missing capability requires reduced scope or an explicit exception. A monitoring contract does not demonstrate a containment or reconstruction capability. Promised services must be checked against the actual engagement and available access.

Business owners must describe minimum acceptable service and interruption effects, including identity, network, supplier, application and data dependencies. The lead must be able to retrieve this information outside an incident. Undecided parameters must remain visible in a gap register with an owner and the decision required. Adoption must not treat an unfinished field as an approved commitment.

2. Responsibilities, decisions and absence

The internal lead directs each incident. The MSSP may assess and investigate; the IT provider may execute changes. Suppliers require a precise assignment. They must not independently stop business activity, communicate externally or accept business risk. One person may perform compatible roles, but each sensitive decision must retain an identifiable accountable person.

Function	Power or task	Boundary	Absence arrangements
Management or delegate	Activate crisis arrangements, arbitrate interruptions, accept risk	No unsupported technical conclusion	Named deputy

Function	Power or task	Boundary	Absence arrangements
Internal lead	Prioritize, assign, record decisions and request resources	Delegation and safety limits	Recorded handover to deputy
Business owner	Explain impact and validate recovered service	Cannot alone declare compromise eliminated	Designated business deputy
MSSP or analyst	Provide facts, hypotheses, scope and checks	No measure outside mandate	Contract escalation and internal fallback
IT provider or operator	Execute and verify authorized changes	No improvised evidence deletion	Authorized alternate or approved specialist
Legal, privacy and communications	Assess obligations and messages	No legal deadline inferred from template	Recorded use of approved alternate advice

The directory must distinguish operational contact, supplier escalation and internal decision-maker. It must remain available when ordinary email, directory or workstation is unavailable. The lead must verify an external responder's identity independently before granting access. An absent person must not retain a critical task without an accepted transfer of responsibility.

Before adoption, the owner must test substitution: the deputy locates delegation, receives a report and assigns a task without using the primary person's account. Identified gaps require correction or a risk decision. Replacement authority must not be improvised from an unverified message. Acceptance of the role, its limits and escalation contact must be recorded.

3. Reporting, assessment and severity

People must be able to report suspicious activity through [TO COMPLETE: normal and fallback channels]. The recipient must open a case and record time and zone, reporter, service, symptom and actions already taken. Do not request passwords, MFA codes, usable cookies or tokens. Preserve suspicious messages through the designated collection channel rather than ordinary distribution.

The lead must separate observed impact, plausible impact and unknowns. Analysts must identify searched sources and their time coverage. An observed event is not automatically an incident; classification depends on analysis. Missing logs or alerts do not prove that activity did not occur. Report details must remain available only to authorized participants.

Proposed level	Conditions to assess	Internal decision	Evidence and reassessment
Critical	Plausible spread, foundational privileges affected or essential activity threatened	Contact management; consider crisis coordination	Facts, unknowns, scope and next check
Major	Credible compromise with contained but significant impact	Lead mobilizes business, MSSP and operations	Measures and worsening criteria
Limited	Localized signal, low impact and plausible control	Assign proportionate assessment	Scope justification and outcome
Unqualified	Insufficient or conflicting evidence	Set protective provisional priority; name next collection	Missing information and reassessment point

This matrix is an organizational choice requiring approval. The lead must consider scope, data, privilege, dependencies and recoverability rather than an isolated score. Priority may change with justification. Safety impacts follow competent procedures. Mobilization targets and update points must reflect local severity, coverage and funded resources; this template introduces no universal numerical target.

The MSSP must provide a usable summary, not merely an alert: observation, source, target, period, evidence-based confidence, unknowns and proposed check. Missing identifiers or scope require clarification and a provisional priority. Lack of information must not be converted into dismissal. The internal lead remains responsible for obtaining enough information to make or escalate the decision.

4. Activation, independent channels and suppliers

On activation, name lead, deputy, teams, channel and next update. Confirm who may request isolation, suspend an account, interrupt a service or engage specialists. If the normal channel appears compromised, use the tested independent channel. Fallback coordination must not place new secrets on a suspect system or assume that the usual account still proves the sender's identity.

Each supplier request must specify reference, target, authorized action, exclusions, expected result and return channel. The lead must obtain operational acceptance, not merely an automatic acknowledgment. Check contracted hours, permissions, record preservation, subcontractors and escalation. Unavailable service is a response limitation, never a completed measure. Record who owns the unanswered request internally.

Blocker	Lead's action	Evidence	Escalation
Unresponsive supplier	Use escalation contact; seek authorized fallback	Attempts and missing capability	Management for resources and waiting risk
Absent decision-maker	Call deputy; use preauthorized measures only	Delegation and time	Defined internal fallback authority
Ambiguous permission	Restate objective, target and boundaries	Named agreement	No silent expansion
Safety conflict	Pause affected action; consult competent operator	Reason and alternative protection	Business and safety authority

Temporary specialist access must be named, limited and tracked. The lead must define withdrawal and request return of relevant materials. Exchange files through approved storage. Closing a supplier assignment must confirm completed work, gaps and record custody; it must not automatically close the incident. Provider execution and the organization's verification are distinct records.

5. Containment and result checks

Before a measure, identify threat, intended benefit, business effects, dependencies and evidence potentially lost. Operators require a verifiable target, stop conditions and a feasible fallback where available. The lead decides whether collection precedes action. Urgency may justify protection first, provided evidence made unavailable is recorded and the decision-maker understands that tradeoff.

Measure	Input and authority	Execution and evidence	Missing result
Endpoint isolation	Confirmed identifier; lead's delegation	Operator isolates and checks network scope	Keep containment unconfirmed; seek another check
Account restriction	Stable account, services and business impact	Identity team acts; application owners verify access	No conclusion about all access from one console
Service restriction	Dependencies and business decision	Operator applies and tests degraded service	Reassess impact and protection
Backup protection	Known repositories and administration identities	Backup team checks access and preserved copy	Escalate uncertain recovery capability

A completed command or closed ticket does not establish the intended effect. Seek independent checks where possible: actual state, authorized test or owner confirmation. Temporary measures require owner, locally decided duration and removal criteria. Assess rollback because restoring a configuration may reopen exposure. An inability to verify must remain visible in incident status.

When a check shows unexpected scope, the operator must stop expansion and inform the lead. Distinguish technical failure, incorrect target and visibility limitation. Inform the business owner of confirmed impact. Alternative protection must remain authorized and verifiable; teams must not accumulate measures whose effects are no longer understood. Update the decision record rather than overwriting the failed action.

6. Investigation, evidence and handover

Analysts must define useful questions: plausible initial access, observed operations, affected privileges, exposed systems and unknown extent. Separate event, receipt and observation times and record clock corrections. Timing correlation or a shared address alone cannot attribute an action to a person. Conclusions must link to evidence and explain limitations, rather than presenting assumptions as confirmed findings.

The custodian must reference each item, record origin, collection, operator, access and transfers, and apply suitable integrity checks. Protect originals and analyze copies where possible. Exports and screenshots may contain sensitive data. Collection must remain authorized and proportionate, with justified storage and retention. Specialist acquisition requires appropriate skills and a documented method.

Check	Owner and input	Usable output	Failure to report
Log search	Analyst; question, source, period	Saved query, result and coverage	Missing category, expiration, insufficient rights
Specialist acquisition	Authorized expert; purpose and authority	Method, media, integrity and limitations	Impossible collection or known alteration
Technical attribution	Analyst and source owner	Matching identifiers and historical context	Association remains assumed
Handover	Outgoing and incoming leads	Restated priorities and accepted actions	Inaccessible evidence or unaccepted ownership

Revise contradicted hypotheses without erasing earlier conclusions; preserve the reason for change. Distinguish “not found in searched sources,” “source unavailable” and “activity excluded by a specific check.” Routine tickets or assistants must not receive raw secrets or information whose sharing is unauthorized. A useful case must expose the uncertainty another analyst needs to challenge it.

Handover must cover active measures, pending decisions, urgency and the next check. Incoming staff must verify access to relevant evidence and restate their actions. If transfer fails, the outgoing responder must identify the blocker to the lead. A meeting invitation or transmitted link is not acceptance of responsibility for an action.

7. Obligations, communications and external decisions

Consult the competent function when an incident may involve personal data, contractual commitments, regulated activities or third parties. Provide facts, territories, entities, data categories, services, dates and unknowns. The adviser must document applicability, recipients, selected deadlines and the relevant starting event. This model imposes no universal notification deadline and does not substitute for a jurisdiction-specific assessment.

Communications must distinguish observation, action and uncertainty. The internal spokesperson validates audience and channel with competent functions. Avoid premature attribution, guarantees of data deletion or unverified recovery claims. Retain approved text, recipients and dispatch time. Verify external requests before releasing sensitive materials; the requester's apparent authority must not replace the approved sharing process.

Record a decision to notify or not notify, the consulted person and reassessment when facts change. No decision must not be represented as a negative decision. Exchanges with insurers, authorities and partners follow applicable authority and contracts. A technical provider must not improvise a legal position on the organization's behalf.

8. Recovery and conditional closure

The lead, business and operations teams prepare a recovery proposal: minimum service, dependency order, environment, addressed access, controls, tests and stop conditions. Initial access may remain partly uncertain; document and explicitly decide that limitation. Fixing one defect does not establish removal of every persistence mechanism or hostile access path.

Gate	Required evidence	Decision-maker	Reserve or rejection
Reconstruction	Verified administration, dependencies and restoration assets	Lead and operator	Do not reuse suspect resources without decision
Pilot recovery	Data and business operation tested; monitoring available	Business owner and lead	Restricted scope or degraded operation
Expansion	Pilot results, gaps and remaining risk	Recovery authority	Pause if suspicious indications appear
Recovery end	Approved criteria met; remaining tasks assigned	Management or delegate	Defer closure or explicitly accept risk

Check restoration assets before use and services after restoration. Business owners must test a representative operation, not simply open a page. Define enhanced monitoring and exit criteria. If suspicious indications recur, pause expansion and reassess; a new alert alone does not prove recurrence. Recovery evidence must show both technical state and agreed business function.

Closure must state explained activity, remaining uncertainty and assigned corrections. Remove temporary measures and expert access or transfer them to durable ownership. Decide preservation of evidence. Lessons learned must examine arrangements, contracts and coordination rather than reduce analysis to an assumed individual mistake. Outstanding work remains tracked after the incident record is administratively closed.

9. Complete fictional example

Fictional business Atelier Rivage has approximately 80 people and outsourced operations. Its MSSP reports an unknown forwarding rule and a disputed sign-in on a finance account. An internal administration manager leads; a named deputy takes over if absent. This illustrates adaptation, not customer experience or a required organizational model.

Logical stage	Fictional fact or decision	Owner	Evidence or result
Report	Unknown rule confirmed; session association unknown	MSSP analyst	E-01 export with stated scope
Activation	Provisional major level; user reached through verified number	Internal lead	D-01, independent channel
Containment	Identity and application restrictions authorized	Assigned operators	D-02, two checks; another application unknown
Investigation	Authorized rule removal; MFA history requested	IT provider: rule; MSSP: analysis	E-02, missing category recorded
Recovery	Necessary access on checked endpoint; bounded monitoring	Business and lead	D-03, residual risk accepted; supplier action open

Acceptance requires a second responder to locate E-01, distinguish the recognized sign-in from the disputed operation and explain the reserve for the unchecked application. They must identify recovery authority and the next check. “MFA present, close case” and “password changed, every access terminated” are rejected conclusions in this exercise.

10. Adaptable annexes and adoption test

Blank activation register	Local value	Check	Owner
Case and scope	[TO COMPLETE: reference, services, period]	Identifiers confirmed	[TO COMPLETE]

Blank activation register	Local value	Check	Owner
Severity and unknowns	[TO COMPLETE: facts, hypotheses, level]	Reassessment planned	[TO COMPLETE]
Coordination	[TO COMPLETE: lead, deputy, channel, update]	Contacts tested	[TO COMPLETE]
Action and authority	[TO COMPLETE: target, approval, result]	Effect checked or reserve	[TO COMPLETE]
Recovery and closure	[TO COMPLETE: criteria, remaining risk]	Named acceptance	[TO COMPLETE]

☐ A report outside normal tools reaches an accountable person.

☐ The deputy finds delegation and obtains supplier acceptance.

☐ Fictional isolation has a target, authorization, expected effect and check.

☐ Evidence is located, a hypothesis challenged and handover accepted.

☐ Obligations are examined without importing another jurisdiction's deadline.

☐ Business owners can reject recovery with unverified dependencies.

11. Exceptions, assurance and revision

Exceptions must identify requirement, scope, risk, compensation, decision-maker, owner, expiry and next check. Requesters explain why the rule cannot be applied. The authority explicitly approves or rejects; a supplier must not accept business risk without delegation. An expired exception requires correction or reassessment, never silent renewal. Emergency authority must be defined before use and recorded when invoked.

At [TO COMPLETE: oversight body and cadence], review unassigned incidents, overdue actions, unverified measures, contractual gaps and exercises. Each gap requires an owner and resolution evidence. Distinguish apparent speed, assessment quality and recoverability; closed-case counts alone do not demonstrate effectiveness. Report the observation period and scope so management can understand what was actually assessed.

Each revision records author, reason, approver and changes. Preserve decisions and control evidence according to [TO COMPLETE: repository, access, justified retention]. Distribute approved copies and withdraw superseded versions. Repeat exercises after material changes or significant failure. Ordinary frequency, preservation rules and mobilization targets remain approved local parameters.

Primary references and limitations

NIST SP 800-61 revision 3, April 2025 addresses roles, suppliers, assessment, evidence and recovery, including §2.2 and RS.MA, RS.AN, RS.CO and RC.RP. ANSSI crisis guidance distinguishes strategic leadership from technical response.

The matrices, delegations, examples and detailed criteria are proposed operational choices, not universal prescriptions of those sources. Validate them with business owners, suppliers and competent advisers. This plan replaces neither safety and continuity arrangements nor specialist expertise or incident-specific legal analysis.