

MSP Incident Response Runbook SOP

Document no.	SOP-MSP-004
Revision	1.0
Owner	Security Lead
Effective date	October 15, 2026
Review cycle	Every 6 months

1. Purpose

To respond to security incidents at managed clients quickly and consistently, limit damage, keep the client informed and stop a threat in one client from spreading through the MSP's shared tools to others.

2. Scope

Applies to suspected or confirmed security incidents in any managed client environment or in the MSP's own tools, such as ransomware, compromised accounts, malware and data exposure. Routine service outages follow the incident management process instead.

Definitions

Security incident	An event that threatens the confidentiality, integrity or availability of client systems or data and needs a coordinated response.
Incident Commander	The person who leads the response, assigns tasks, makes decisions and owns communication until the incident is closed.
Indicator of compromise	Evidence such as a file hash, IP address, domain or account activity that points to malicious activity.
Containment	Actions that stop an incident from spreading, such as isolating devices or disabling accounts, before the cause is removed.

3. Responsibilities

Service Desk Technician	Receives the first report or alert, gathers the initial facts and escalates to security without delay.
Security Engineer	Classifies the incident, contains and investigates it, preserves evidence and removes the cause.
Incident Commander	Leads the response, coordinates engineers, keeps the timeline and runs the post-incident review.
Technical Account Manager	Notifies the client, gives regular updates and records the client's decisions.
Client Point of Contact	Makes business decisions, approves disruptive actions and handles the client's legal, insurance and regulatory notifications.

RACI matrix

Activity	Service Desk Technician	Security Engineer	Incident Commander	Technical Account Manager	Client Point of Contact
Triage and classify the incident	R	R/A	I	I	-
Lead and coordinate the response	I	C	R/A	C	I
Contain, eradicate and recover	C	R	A	I	C
Communicate with the client	-	C	A	R	C
Decide on external notifications	-	C	C	C	R/A

R = Responsible, A = Accountable, C = Consulted, I = Informed

4. Materials and PPE

Materials, tools and systems

- EDR and security monitoring consoles
- RMM tool with remote isolation
- PSA ticketing system
- Dedicated incident chat channel or bridge line
- Client contact and escalation matrix
- Incident timeline template
- Verified backups for recovery

5. Procedure

Step	Task	Owner	Done
5.1	Receive and triage the alert The Service Desk Technician logs the alert or report in the PSA, records what was seen, when and on which devices, and escalates to the Security Engineer immediately.	Service Desk Technician	☐
5.2	Classify the incident severity The Security Engineer confirms whether it is a real incident and classifies severity by the systems, data and number of users affected. Checkpoint: Severity is recorded in the ticket within 30 minutes of the alert being escalated.	Security Engineer	☐
5.3	Assign an Incident Commander For high and critical incidents, the Incident Commander takes the lead, opens a dedicated incident channel and assigns tasks to engineers.	Incident Commander	☐
5.4	Notify the client The Technical Account Manager notifies the Client Point of Contact using the escalation matrix, explains what is known and agrees the update schedule.	Technical Account Manager	☐
5.5	Contain the threat The Security Engineer isolates affected devices, disables compromised accounts, revokes active sessions and blocks known malicious addresses and files. Warning: Do not wipe or rebuild affected systems before evidence has been preserved, unless the Incident Commander decides it is needed to stop the spread.	Security Engineer	☐

Step	Task	Owner	Done
5.6	Preserve evidence The Security Engineer exports relevant logs, captures alerts and screenshots and keeps affected disks or images, recording who collected what and when.	Security Engineer	☐
5.7	Check other clients for the same threat The Security Engineer searches every other managed client and the MSP's own RMM, remote access and vault for the same indicators of compromise.	Security Engineer	☐
5.8	Remove the cause The Security Engineer removes malware and persistence, closes the exploited weakness and resets credentials that may have been exposed.	Security Engineer	☐
5.9	Recover affected systems The Security Engineer restores systems from known-good backups or rebuilds them, then monitors them closely for signs of reinfection. Checkpoint: Restored systems are scanned clean and monitored for at least 72 hours before the incident is closed.	Security Engineer	☐
5.10	Keep the timeline and send updates The Incident Commander keeps a timestamped timeline of actions and decisions and makes sure the client receives updates at the agreed interval.	Incident Commander	☐
5.11	Decide on external notifications The Client Point of Contact decides whether to notify insurers, regulators, customers or law enforcement, using the facts and timeline supplied by the MSP.	Client Point of Contact	☐
5.12	Close the incident The Incident Commander closes the incident once the threat is removed, systems are recovered and the client agrees, and records the final status in the ticket.	Incident Commander	☐
5.13	Run the post-incident review The Incident Commander runs a blameless review within five business days and assigns actions to update runbooks, client documentation and security controls.	Incident Commander	☐

6. Quality checks

- Every security alert was escalated and classified within the target time.
- Containment happened before any evidence-destroying recovery work.
- Other managed clients were checked for the same indicators of compromise.
- The client received updates at the agreed interval throughout the incident.
- A post-incident review was held and its actions have owners and due dates.

7. Records

- Incident ticket with severity and final status
- Timestamped incident timeline
- Evidence collection log
- Client communication log
- Post-incident review report and actions

8. KPIs

- Mean time from alert to containment
- Mean time to recover affected systems
- Percentage of incidents with a completed post-incident review
- Number of incidents that spread beyond the first device or client

9. Common mistakes

- Rebuilding infected machines before collecting evidence.
- Fixing the affected client without checking every other client for the same threat.
- Going quiet with the client while engineers work the problem.
- Making legal or regulatory notification decisions on the client's behalf.

10. Revision history

Revision	Date	Description	Reviewed by
1.0	October 15, 2026	Initial release	Iliia Pirozhenko

Approval

Prepared by	Approved by	Date

This is a template. Adapt it to your organization, equipment and local regulations before use.



Scan for the latest version

Opens this template online, where you can download it again in Word, PDF, Excel or CSV — free, no sign-up.

Or [add it to Perfect Wiki](#) so your team can find it and ask questions about it in Microsoft Teams, Slack, kChat or Mattermost.