

BASESECURE

SECURITY · POLICY · COMPLIANCE

Incident Response Plan

Prepared for [COMPANY NAME]

Document Owner	[NAME / ROLE]
Approved By	[NAME / ROLE]
Effective Date	[DATE]
Next Review	[DATE]
Version	1.0
Classification	Internal Use Only

Document Control

Version	Date	Author	Approved By	Summary of Changes
1.0	[DATE]	[NAME]	[NAME]	Initial release

1. Purpose

This plan defines how [COMPANY NAME] detects, reports, assesses, contains, eradicates, recovers from, and learns from information security incidents.

Its objective is to limit damage and recovery time by ensuring that everyone knows what to do, who decides, and who to call — before an incident happens rather than during one.

2. Scope

This plan applies to any actual or suspected event that compromises, or may compromise, the confidentiality, integrity, or availability of [COMPANY NAME] information or systems — including those operated on its behalf by a third party.

3. Incident Response Team

Role	Responsibility
Incident Lead — [NAME / ROLE]	Declares an incident, sets severity, directs the response, and decides on containment actions.
Technical Lead — [NAME / ROLE]	Performs investigation, containment, eradication, and recovery. Preserves evidence.
Communications Lead — [NAME / ROLE]	Handles internal updates, customer communication, and any public statement.
Legal / Compliance — [NAME / ROLE]	Advises on notification obligations, evidence handling, and regulatory exposure.
Executive Sponsor — [NAME / ROLE]	Authorizes major decisions including service shutdown, external assistance, and ransom-related decisions.
External Support	[MSP / IR FIRM / INSURER] — engaged per the contact list in section 9.

[In a small business one person may hold several of these roles. Name a deputy for each, because incidents do not wait for people to be available.]

4. Severity Levels

Level	Description	Response Time	Escalation
SEV 1 — Critical	Confirmed breach of regulated or customer data, ransomware, or total loss of a critical service.	Immediate, 24/7	Executive Sponsor and Legal immediately. External IR support engaged.
SEV 2 — High	Suspected breach, compromise of a privileged account, or significant service degradation.	Within [NUMBER] hour(s)	Incident Lead and Executive Sponsor.
SEV 3 — Moderate	Isolated malware, single compromised standard account, or limited data exposure.	Within [NUMBER] hours	Incident Lead.
SEV 4 — Low	Policy violation, blocked phishing attempt, or minor issue with no confirmed impact.	Within [NUMBER] business days	Handled by [IT MANAGER / MSP]; logged and reviewed.

5. Reporting an Incident

- Anyone who suspects an incident reports it immediately to [REPORTING CONTACT] by [PHONE / EMAIL / CHANNEL] — speed matters more than certainty.
- Report first, investigate second. Users must not attempt to fix, delete, or "clean up" anything before reporting.
- Reports made in good faith carry no blame, including from the person who caused the incident.
- If the reporting channel itself may be compromised, use the out-of-band contact method in section 9.

The report should state what was observed, when, on which system or account, and what action has already been taken.

6. Response Phases

6.1 Detect and Record

- Log the incident in the incident register with a unique reference, the time of detection, and the reporter.
- Start a timeline immediately and record every action with its timestamp and the person who took it. This record drives both the recovery and any later regulatory or insurance claim.
- Assign an initial severity; severity may be revised at any point as facts emerge.

6.2 Assess

- Determine what systems, accounts, and data are affected, and whether personal or regulated data is involved.
- Determine whether the incident is ongoing or historic.
- Notify [INSURER] as soon as a SEV 1 or SEV 2 is declared — many cyber policies require prompt notice and pre-approval of external responders.
- Where personal or regulated data may be affected, notify Legal immediately: statutory notification clocks may already be running.

6.3 Contain

- Take the minimum action needed to stop the damage spreading — isolate affected systems from the network, disable compromised accounts, revoke sessions and tokens, block malicious indicators.
- Preserve evidence before making changes: capture memory and disk images where feasible, and export relevant logs before retention expires.
- Do not power off a system unless directed by the Technical Lead — shutting down destroys volatile evidence.
- Reset credentials for affected accounts, and for any account that shared those credentials.

[Ransomware: do not attempt to negotiate, pay, or contact the attacker without Executive Sponsor and Legal authorization. Payment may carry sanctions exposure in several jurisdictions.]

6.4 Eradicate

- Identify and remove the root cause — malware, unauthorized access, misconfiguration, or vulnerability.
- Patch or reconfigure the exploited weakness before restoring service.
- Verify that persistence mechanisms, added accounts, forwarding rules, and unauthorized access paths have been removed.

6.5 Recover

- Restore systems from known-good backups, verified clean before reconnection.

- Return services to production in a controlled sequence, monitoring closely for recurrence for at least [NUMBER] days.
- Confirm data integrity with the relevant business owner before declaring recovery complete.
- The Incident Lead formally declares the incident closed and records the closure time.

6.6 Review

- A post-incident review is held within [NUMBER] business days of closure for all SEV 1 and SEV 2 incidents.
- The review covers what happened, how it was detected, what worked, what did not, and what will change.
- The review is blameless in tone and focused on system and process improvement.
- Resulting actions are assigned an owner and a due date, and tracked to completion.

7. Evidence Handling

- Evidence is collected and stored so that it remains admissible: record who collected what, when, from where, and who has held it since.
- Original media is preserved and work is performed on copies wherever possible.
- Evidence is retained for at least [DURATION], or longer if litigation, insurance, or regulatory action is anticipated.

8. Communication

- Only the Communications Lead or Executive Sponsor communicates externally about an incident.
- Personnel must not discuss incidents on social media, with customers, or with press.
- Internal updates are issued at a defined cadence during SEV 1 and SEV 2 incidents so that people are not left guessing.
- Customer and regulatory notification follows the Breach Notification Procedure.
- Where email or chat may be compromised, communications move to the out-of-band channel in section 9.

9. Contact List

Contact	Detail
Incident reporting	[PHONE / EMAIL / CHANNEL]
Out-of-band channel	[ALTERNATIVE METHOD — must not depend on company email or network]
Incident Lead	[NAME] — [PHONE] — deputy: [NAME]
IT provider / MSP	[COMPANY] — [24/7 NUMBER] — contract ref [REF]
Cyber insurance	[INSURER] — [CLAIMS NUMBER] — policy [NUMBER]
External IR firm	[FIRM] — [NUMBER] — retainer [YES / NO]
Legal counsel	[FIRM] — [NUMBER]
Regulator(s)	[NAME AND REPORTING ROUTE]
Law enforcement	[LOCAL / NATIONAL CYBERCRIME REPORTING ROUTE]
Key customers requiring notice	[LIST OR REFERENCE TO CONTRACT SCHEDULE]

[Print this page and keep a copy offline. In a ransomware event you may have no access to the systems holding this document.]

10. Testing and Maintenance

- This plan is tested at least [FREQUENCY] through a tabletop exercise involving the response team.
- Contact details are verified at least [FREQUENCY] and after any personnel change.
- The plan is updated after every test and after every SEV 1 or SEV 2 incident.

11. Review

This plan is reviewed by [SECURITY LEAD] at least annually, and whenever the organization materially changes its systems, its suppliers, or its regulatory obligations.

Important Notice

This document is a template. It must be reviewed and customized to reflect the actual operations, jurisdiction, contractual obligations, and risk profile of the organization using it.

It does not constitute legal, regulatory, or compliance advice. It does not guarantee compliance with any framework, standard, regulation, or audit, and it does not guarantee certification of any kind.

Incident notification duties, evidence handling, and sanctions exposure around ransom payments are governed by law that varies by jurisdiction and industry. Engage qualified counsel at the point an incident is declared, not afterwards.

Licensed to a single organization unless a reseller or MSP license has been purchased. Redistribution or resale of this template is not permitted.