POLICY

Incident Response Plan

How to detect, contain, recover from and learn from security incidents

Document owner	[Owner name and role]
Approved by	[Approver name and role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, at least yearly]
Classification	[Internal]

Purpose

This plan sets how [Company Name] detects, assesses, contains, recovers from and learns from information security incidents, so that damage is limited, service is restored quickly, notification duties are met and incidents do not repeat.

Scope

This plan applies to:

- All information security events and incidents that affect [Company Name] systems, data, staff or customers, including those at suppliers that process company data.
- All employees and contractors, the incident response team and the people in the contact list.

An event is something that might affect security, such as a suspicious login alert. An incident is an event that is confirmed or likely to harm confidentiality, integrity or availability, such as an account takeover or data exposure.

Roles and responsibilities

Role	Responsibilities
Incident Commander ([Security Lead] or on-call delegate)	Leads the response. Sets severity. Assigns tasks. Decides on escalation. Owns the incident record until closure.
Technical Lead ([Engineering Lead] or on-call engineer)	Investigates, contains and fixes the technical cause. Preserves technical evidence.
Communications Lead ([Head of Customer Success / Marketing])	Prepares internal updates, customer messages and status page updates, approved by the Incident Commander.
Legal and privacy ([Legal Counsel / DPO])	Assesses legal, contractual and regulatory notification duties. Advises on external communication.
Executive sponsor ([CEO / CTO])	Approves external notifications and major decisions for High and Critical incidents. Names a scribe to keep the timeline.
All staff	Report suspected incidents immediately and follow instructions.

One person may hold more than one role in a small company, but the Incident Commander must not also be the only person fixing the issue in a High or Critical incident.

Severity levels

Severity	Description and examples	Start	Escalate to
SEV1 Critical	Confirmed customer data breach or full production outage. Examples: data exfiltration, ransomware, compromised cloud admin.	[30 min], 24/7	Sponsor, Legal, Comms
SEV2 High	Likely data exposure or major control failure. Examples: compromised account with confidential access, public bucket with customer data.	[2 hours], 24/7	Sponsor, Legal
SEV3 Medium	Limited to one user or system, no sign of exposure. Examples: malware blocked on a laptop, phishing link clicked without entering credentials.	[1 business day]	[Security Lead]
SEV4 Low	No real impact. Examples: encrypted laptop lost and wiped, failed brute force attempts.	[3 business days]	[IT Manager]

The Incident Commander must raise the severity as soon as new facts show a higher impact. Severity may be lowered only with a recorded reason.

Policy statements

1. All staff must report suspected incidents immediately through [#security-incidents channel / security@company email / phone number]. Outside business hours, Critical and High incidents must be reported to the on-call number [phone or paging tool].
2. Every reported event must be logged in [ticketing tool / incident tool] with a unique ID, and the Incident Commander must set its severity within the start time in the table above.
3. Critical and High incidents must have a dedicated channel, such as a private Slack channel, and a running timeline.
4. Notification decisions must be made and recorded within the deadlines set by law and contracts (see Communication and notification).
5. Critical and High incidents must have a lessons learned review within [10] business days of closure.
6. This plan must be tested at least once every [12 months] through a tabletop exercise or a real incident review.

Response phases

1. Detection and reporting

- Sources include staff reports, alerts from [SIEM / EDR / cloud security tool], customers, suppliers and external researchers.
- The person who detects the event must report it and must not investigate alone, delete files or contact the attacker.
- The on-call person must acknowledge the report and open an incident record.

2. Triage and assessment

- Confirm whether the event is a real incident and identify affected systems, data, customers and users.
- Assign severity and an Incident Commander, and decide who joins the response.

3. Containment

- Short term containment stops the damage quickly, for example: disable the compromised account in the [identity provider], revoke sessions and tokens, isolate a laptop through the [MDM / EDR], block an IP address, or make a public storage bucket private.
- Preserve evidence before making changes when possible (see Evidence handling).
- Record every containment action with time and owner.

4. Eradication

- Remove the root cause, such as malware, a vulnerable dependency, a leaked key or a misconfiguration, and rotate any exposed credentials.
- Check for persistence, such as new admin accounts, OAuth app grants, access keys or forwarding rules.

5. Recovery

- Restore from known good backups or rebuild from infrastructure as code. Return systems to production only after the Technical Lead confirms they are clean.
- Monitor closely for [number] days after recovery.

6. Lessons learned

- Hold a blameless review and document the timeline, root cause, what worked, what did not, and actions with owners and due dates.
- Track actions in [ticketing tool] until done.
- Update the risk register, this plan and related controls when needed.
- Close the incident record only when the review is done for Critical and High incidents.

Communication and notification

1. During Critical and High incidents, the executive sponsor must get updates at least every [4 hours].
2. Only the Communications Lead may send external messages, with approval from the Incident Commander and, for Critical incidents, the executive sponsor.
3. Legal must assess notification duties for any incident involving personal or customer data, for example to regulators under privacy laws such as GDPR (72 hours to the supervisory authority in many cases) and to customers under contracts, which often require notice within [24 to 72 hours]. Record these duties in the [customer notification register].
4. The executive sponsor decides, with Legal advice, on notifying law enforcement, the cyber insurer and affected individuals.
5. Staff must not discuss incidents outside the response team.

> **Warning:** Notification deadlines depend on your jurisdictions, contracts and industry. Have them confirmed by your legal advisor and record the real deadlines in this section.

Evidence handling

1. Evidence must be collected before systems are changed or wiped, where this does not increase harm.

2. Typical evidence includes cloud audit logs ([CloudTrail / Cloud Audit Logs / Azure Activity Log]), identity provider logs, EDR telemetry, email headers, screenshots, disk or memory images and chat messages.
3. Evidence must be stored in a restricted location, [secure evidence folder or bucket], with access limited to the response team.
4. A chain of custody record must show who collected each item, when, from where, its hash where possible, and every person who handled it.
5. Security logs must be kept for at least [12 months]. Where legal action is possible, Legal decides whether an external forensic firm collects evidence.

Contact list

Keep this list current. Test it at least every [6 months].

Role	Name	Phone	Email	Backup contact
Incident Commander	[Name]	[Phone]	[Email]	[Backup name]
Technical Lead	[Name]	[Phone]	[Email]	[Backup name]
Communications Lead	[Name]	[Phone]	[Email]	[Backup name]
Legal and privacy	[Name]	[Phone]	[Email]	[Backup name]
Executive sponsor	[Name]	[Phone]	[Email]	[Backup name]
Cloud provider support	[AWS / GCP / Azure support plan]	[Phone]	[Support URL]	[Account manager]
Cyber insurance provider	[Insurer]	[Hotline]	[Email]	[Policy number]
External forensic firm	[Firm name]	[Phone]	[Email]	[Retainer reference]
Data protection authority	[Authority]	[Phone]	[Reporting portal]	

Exceptions

During an active incident, the Incident Commander may approve deviations from this plan to limit harm and must record them. Permanent exceptions follow the Information Security Policy.

Enforcement

Failing to report a known incident, hiding information or destroying evidence may lead to disciplinary action under [Company Name]'s HR procedures. Good faith reports never do.

Related documents

- Information Security Policy, Acceptable Use Policy and Access Control Policy
- [Business Continuity and Disaster Recovery Plan], [Customer notification register] and [Incident record template]

Annex A mapping

Annex A control	Section that covers it
5.5 Contact with authorities	Communication and notification, Contact list
5.24 Information security incident management planning and preparation	Roles and responsibilities, Policy statements
5.25 Assessment and decision on information security events	Severity levels, Triage and assessment
5.26 Response to information security incidents	Containment, Eradication, Recovery
5.27 Learning from information security incidents	Lessons learned
5.28 Collection of evidence	Evidence handling
5.29 Information security during disruption	Recovery
6.8 Information security event reporting	Detection and reporting, Policy statement 1
8.15 Logging	Evidence handling
8.16 Monitoring activities	Detection and reporting

Review and approval

The [Security Lead] must review this plan at least once every [12 months], after every Critical or High incident and after each test. Changes are approved by [Security Committee], recorded in the document control table and shared with everyone in the contact list.