

SME Incident Response Plan (IRP) — Template

SecureBusinessHub — Educational Resource for SMBs

1. Objective

Provide a clear, repeatable process for detecting, containing, eradicating and recovering from cyber security incidents while preserving evidence and meeting regulatory obligations.

2. Roles & Responsibilities

- Incident Commander — coordinates the response and owns decisions.
- Technical Lead — performs containment and forensic capture.
- Communications Lead — manages internal and external messaging.
- Legal/Compliance Lead — handles GDPR notifications and regulator contact.
- Executive Sponsor — authorises spend and external assistance.

3. Severity Classification

- SEV-1: Active data exfiltration, ransomware, or service-down impacting customers.
- SEV-2: Confirmed compromise of a single account or endpoint, contained.
- SEV-3: Suspicious activity under investigation, no confirmed impact.

4. Detection & Triage

Sources include EDR alerts, SIEM correlations, user reports and third-party notifications. Within 30 minutes of triage, classify severity, open an incident ticket, and notify the Incident Commander.

5. Containment

- Isolate affected hosts from the network (do not power off — preserve memory).
- Revoke compromised credentials and rotate API keys and service tokens.
- Block known indicators of compromise at the firewall and email gateway.

6. Eradication & Recovery

Rebuild affected systems from known-good images. Restore data from immutable backups verified against pre-incident hashes. Re-enable services in stages with heightened monitoring for at least 14 days.

7. GDPR & Regulatory Notification

Where personal data is involved and risk to data subjects is likely, notify the supervisory authority (AEPD in Spain) within 72 hours of becoming aware of the breach. Document the decision in any

case.

8. Communications

Use pre-approved templates. Acknowledge facts, avoid speculation, and route media enquiries to the Communications Lead. Internal updates at minimum every 4 hours during a SEV-1.

9. Post-Incident Review

Within 10 business days conduct a blameless retrospective. Capture root cause, timeline, what worked, what failed and concrete remediation actions with owners and deadlines.

10. Contact List

Maintain an out-of-band contact list (printed or stored offline) including IT staff, executives, legal counsel, cyber insurance and external incident response retainer.

This template is provided for educational purposes. Adapt to your organisation's context and seek professional advice where appropriate.