RESOURCES BY BUI

Incident Response Plan Checklist

Use our summarised checklist to guide you in creating your Incident Response Plan (IRP).

OBJECTIVES AND SCOPE

- [ ] Define your main goals for incident response.
- [ ] Outline the scope of incidents the IRP will cover.
- [ ] Align objectives with overall business and compliance requirements.

ROLES AND RESPONSIBILITIES

- [ ] Designate a primary point of contact for incident response.
- [ ] Identify incident response team members.
- [ ] Designate roles and responsibilities for team members.

INCIDENT CATEGORISATION

- [ ] Define categories of incidents (e.g., phishing, malware, data breach).
- [ ] Assign impact levels (e.g., low, medium, high) to guide response urgency.
- [ ] Establish clear criteria for escalation.

DETECTION AND NOTIFICATION

- [ ] Set up monitoring tools (e.g., intrusion detection systems, endpoint protection).
- [ ] Outline a process for reporting suspicious activity.
- [ ] Develop an incident notification process for internal and external stakeholders.

CONTAINMENT AND ERADICATION

- [ ] Document containment steps for different incident types.
- [ ] Define procedures for short-term and long-term containment.
- [ ] Outline eradication techniques specific to each incident type.

RECOVERY AND REMEDIATION

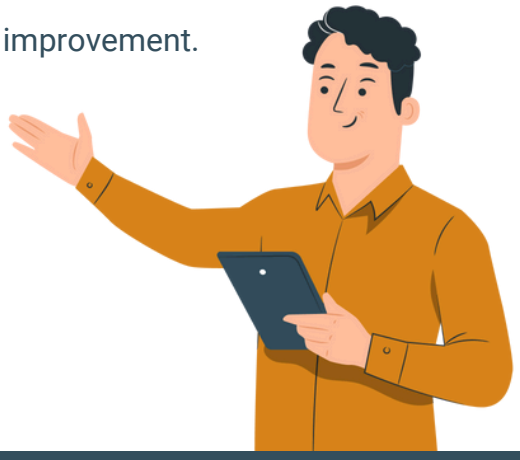
- [ ] Document recovery steps, including system checks and data restoration.
- [ ] Set criteria for safely resuming regular operations.
- [ ] Develop ongoing monitoring for potential threat resurgence.

COMMUNICATION PLAN

- [ ] Identify key audiences (e.g., employees, customers, regulatory bodies).
- [ ] Prepare draft statements and notifications to adapt during incidents.
- [ ] Designate spokespersons and establish approval workflows.

POST-INCIDENT REVIEW

- [ ] Schedule a post-incident review meeting.
- [ ] Document key takeaways, successes, and areas for improvement.
- [ ] Update the IRP to incorporate lessons learned.



By following these steps, you'll have a robust and actionable Incident Response Plan tailored to your organisation's needs.