

GUIDE

Incident Response Plan Guide

A guide to preparing an incident response plan that defines in advance what to do when a security incident occurs.



GUIDE

ABOUT 6 MIN READ

INCIDENT RESPONSE

IN THIS GUIDE

1. Why you need a plan
2. Phases of incident response
3. Roles and responsibilities
4. Classifying incidents
5. First 60 minutes checklist
6. Playbooks and exercises

01 Why you need a plan

In an incident, time is the most expensive thing. If who decides, who acts and who is informed is debated in the moment, losses grow. A good plan lowers the thinking load in a crisis and keeps everyone on the same page.

02 Phases of incident response

1

Preparation

Plan, roles, tools, training

2

Detection and analysis

Notice, classify, understand scope

3

Containment

Stop the spread

4

Eradication and recovery

Remove the cause, restore safely

5

Post-incident

Root cause analysis and lessons

03 Roles and responsibilities**Incident manager**

Runs the process, decides and reports status.

Technical team

Carries out analysis, containment and recovery.

Legal / data protection

Assesses notification duties and evidence integrity.

Communications

Keeps internal and external messaging consistent.

Management

Decides on resources and priorities.

External support

Forensic or response specialists, if needed.

04 Classifying incidents

Not every incident is handled the same way. A predefined scale gets the right people involved at the right speed:

- Low: limited impact, solved with routine team capacity
- Medium: affects a business process or several users, management informed
- High: a critical system or personal data is affected, the crisis team convenes and notification duties are assessed

05 First 60 minutes checklist

- | | |
|--|--|
| ☐ Record the incident: when, who noticed, what was seen | ☐ Isolate affected systems from the network without destroying evidence (do not power off unless necessary) |
| ☐ Assemble the incident manager and crisis team | ☐ Preserve logs and related evidence |
| ☐ Communicate over a secure channel (e-mail may be compromised) | ☐ Inform legal / data protection |

- ☐ Classify the incident and brief management

06 Playbooks and exercises

Prepare step-by-step playbooks for common scenarios: ransomware, account takeover, data leak and denial of service. Test them with a tabletop exercise at least once a year; an exercise shows gaps in the plan before a real incident does.

Important: Do not write the plan and shelve it. Update contacts, roles and tools as they change.

Let's build your incident response readiness together We will create your plan, roles and exercises together.

// CONTACT

Get in touch

Share your needs and current situation and we will define the right scope and roadmap together. Fill in our information form or contact us directly.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul, Türkiye

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Scan the QR code for the
service page and information
form