Incident Response Plan

Organization:

Version:

Date:

Approved by:

CYLOQ

1

Purpose and scope

This plan describes how *organization name:* identifies, manages, and recovers from cybersecurity incidents. The goal is to minimize damage, meet reporting obligations, and ensure the organization can return to normal operations as quickly as possible.

What counts as an incident?

An incident is any event that affects or risks affecting the confidentiality, integrity, or availability of the organization's systems or data.

Severity levels:

Level	Description	Examples
Critical	Active breach, data being exfiltrated, business-critical systems down	Ransomware, active intrusion
High	Suspected compromise, sensitive data exposed	Account compromise, data breach
Medium	Limited impact, no evidence of exfiltration	Isolated malware, phishing attempt
Low	Security alert with no confirmed impact	Failed login attempts

2 Roles and contact information

Incident team

Role	Name	Phone	Email	Backup
Incident Manager				
Technical Lead				
CISO / Security Officer				
Legal Counsel				
Communications Lead				
CEO / Leadership				

External contacts

Organization	Kontakt	Telefon	When to contact
External security provider			All critical and high incidents
Cyloq (incident support)		010-333 10 33	When external forensics or support is needed
Insurance company			Within 24 hours of incident
Supervisory authority (NIS2)			Within 24 hours (NIS2)
Data protection authority (GDPR)			Within 72 hours (GDPR)
Police			In case of extortion or significant damage

3

Communication plan

Internal communication

- The Incident Manager is responsible for daily situation updates to leadership for the duration of the incident.
- Other employees are informed once an accurate and complete message can be given.
- Primary communication channel during incident: _____

External communication

- Authorized to speak externally: _____
- Approval process for external statements: _____
- Customers are informed if their data is affected, after scope has been confirmed.
- Media enquiries handled by: _____

Communication templates

Prepare ready-made communication templates for the scenarios most relevant to your organization. Examples: data breach, ransomware, service disruption. Each template should cover: who the communication is addressed to, what has happened (in general terms), what you are doing about it, and what the recipient needs to do.

4

Technical runbooks

4.1 Ransomware

1. Isolate affected systems – disconnect from the network but do not shut down the machines.
2. Identify which systems are encrypted and how far the breach has spread.
3. Secure logs from firewall, Active Directory, and endpoints immediately.
4. Contact external security expert.
5. Contact insurer within 24 hours.
6. Report to supervisory authority within 24 hours (NIS2) and data protection authority within 72 hours if personal data is involved (GDPR).
7. Begin restoration from verified, clean backups – do not reconnect systems until they have been reviewed.
8. Do not pay the ransom without legal counsel.

4.2 Data breach / unauthorized access

1. Identify which account or system has been compromised.
2. Disable affected accounts and revoke access.
3. Secure logs for forensic analysis.
4. Assess what data may have been exposed.
5. Engage external expert if needed.
6. Report to data protection authority within 72 hours if personal data is involved.
7. Notify affected customers once scope has been confirmed.

4.3 DDoS

1. Contact internet service provider and activate DDoS protection if available.
2. Document attack patterns and timing.
3. Assess whether the attack is a smokescreen for another intrusion – check other systems in parallel.
4. Communicate service disruption internally and externally as needed.

4.4 Account compromise

1. Disable the compromised account immediately.
2. Revoke active sessions and tokens.
3. Review logs to assess what the account had access to.
4. Reset credentials and enforce MFA if not already in place.
5. Assess whether the attacker has moved to other systems or accounts.

5

Reporting obligations and deadlines

Authority / Party	Deadline	Condition	Responsible
Supervisory authority – initial report (NIS2)	24 hours	Essential and important entities	
Supervisory authority – full report (NIS2)	72 hours	Essential and important entities	
Data protection authority (GDPR)	72 hours	If personal data is involved	
Insurance company	24 hours	Check policy terms	
Police	As soon as possible	In case of extortion or significant damage	

6

Recovery procedures

Recovery priority order

(List your business-critical systems in order of priority)

Priority	System	Responsible	Dependencies
1			
2			
3			

Recovery principles

- Restoration is always carried out from verified, clean backups.
- Systems are not reconnected to the network until they have been forensically reviewed and hardened.
- Sign-off for system restart given by: _____
- Backups are stored at: _____
- Most recent verified backup test: _____

7

Lessons learned process

Following every incident, the steps below should be completed within two weeks:

1. **Debrief with the incident team –** what happened, in what order, and why?
2. **Root cause analysis –** how did the attacker get in and what made it possible?
3. **Document lessons learned –** what worked, what did not?
4. **Update the plan –** revise procedures, contact details, and runbooks based on the incident.
5. **Action plan –** concrete improvement measures with assigned owner and deadline.

Lessons learned report template:

- Incident date: _____
- Incident type and severity level: _____
- Timeline: _____
- Root cause: _____
- Actions taken: _____
- Improvement measures: _____
- Responsible for follow-up: _____

8

Maintenance and version control

Activity	Frequency	Responsible
Full review and update of the plan	At least annually	
Verification of contact details	Quarterly	
Tabletop exercise	At least annually	
Update following an incident	After every incident	
Leadership sign-off	At least annually	

This template was developed by **Cyloq** and is designed for organizations subject to NIS2 and GDPR requirements. For help implementing the plan or running security tests, contact us at **+46 10-333 10 33** or **cyloq.se**.