CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

Cyber Incident Response Plan

The tool have been provided in connection with the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), funded by the Danish Industry Foundation. Publication date: 29.12.2025

Cyber Incident Response Plan

→A cyber incident response plan is a document that describes how a company **prevents**, **detects**, **manages**, and **recovers** from cyber incidents such as hacking attacks, ransomware, data breaches, or system outages.

→The plan functions as an operational playbook designed to ensure rapid, coordinated, and correct action when something goes wrong.

→**Purpose and Scope**

- →Purpose:
  - → Prevent and manage cyberattacks.
  - → Minimize the impact on production, data, and customers.
  - → Ensure rapid response, communication, and recovery.
- →Scope:
  - → All IT systems, production management systems, ERP, CRM, networks, servers, and cloud services.
  - → All employees, contractual partners, and external suppliers with access to systems.

Roles and Responsibilities (examples)

Roles	Responsibilities	Contact information	Backup
Crisis Management Team Leader	Overall decision-making during a cyber crisis	Name Telephone E-mail	CEO
IT-Manager	Technical handling of attacks, isolation, and recovery	Name Telephone E-mail	IT-support
Responsible for communication	Internal and external communication	Name Telephone E-mail	Communications staff member / CEO
HR-Manager	Handling of personnel and security procedures	Name Telephone E-mail	HR-staff member
Responsible for Compliance / GDPR	Reporting to authorities and customers	Name Telephone E-mail	Legal advisor (internal/external)

Action Plan (Checklist) in Case of Suspected Cyberattack

→Isolate affected systems (disconnect from the network).
→Inform the IT manager and the crisis management team.
→Stop the spread (disable accounts, change passwords).
→Assess the impact (IT, production, data).
→Restore systems from backup.
→Communicate internally/externally according to the plan.
→Document the incident.

Incident Response Plan – if the Worst Happens

Incident	Classification	What do we do? (reactive action)	Responsible (examples)
Phishing attempt / suspicious e-mail	Low	Warn the recipient and other employees. Report the incident to IT. Delete the email and any links.	IT-Manager
Malware/virus on a workstation	Medium	Isolate the infected machine from the network. Run antivirus/malware scanning. Identify and remove malicious files. Evaluate whether other systems are affected.	IT-Manager
Ransomware attack on production systems	High	Immediately isolate all affected systems. Activate the incident response plan. Inform the crisis management team and management. Restore systems from secure backups. Notify authorities, if relevant.	IT-Manager/Crisis Management Team Leader
Data breach / compromise of customer data	High	Identify which data is affected. Inform management and the data protection officer (GDPR). Notify affected customers and authorities within legally required timeframes. Implement security measures to prevent further access.	IT-Manager/Crisis Management Team Leader

Communication Plan (examples)

Target group	Channel	Responsible	Message	Timing
Employees	E-mail, telephone, intranet	HR / Responsible for Communication	Instructions, updates	Immediately after the incident
Customers	E-mail, telephone, website	Responsible for Communication	Inform about delays and data incidents	Within 4 hours of the incident
Suppliers	E-mail, telephone	Purchasing	Status of deliveries / system access	Immediately after the incident
Authorities	E-mail, telephone	Crisis Management Team Leader / Compliance / CEO	Statutory reporting	As soon as necessary

Preventive (Proactive) Actions (Examples)

1. Antivirus and firewall on all devices.
2. Network monitoring.
3. MFA (Multi-Factor Authentication) on critical systems. Identity must be verified using two or more different types of evidence (factors) to gain access to data/systems.
4. Patch and update policy (a patch is an update to software).
5. Security testing / penetration testing.
6. Backup of critical systems and data: daily, tested, offline + cloud.
7. Awareness training for employees in phishing and social engineering.

Reactive Strategies

→Incident response plan with roles and step-by-step actions.
→Isolation of infected systems.
→Restoration from backup.
→Communication to employees, customers, and authorities.
→Evaluation and updating of security policies.

Training and Test (examples)

→Simulation of cyber attacks (phishing, malware, ransomware) 1-2 times a year.
→Training of crisis staff and IT personnel.
→Documentation of exercises and evaluation of improvement points.

Maintenance (examples)

→Update contact information and roles every 6 months.
→Revise risk classification and strategies annually.
→Evaluate and update the plan after each exercise or real-life incident.
→Ensure all employees have access to the latest version.