CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

2. Cybersecurity roles and responsibilities

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - To support the establishment, communication, and coordination of cybersecurity roles and responsibilities for suppliers, customers, and partners.
- **Participants**
  - Data and IT managers, suppliers, possibly customers, and other relevant external partners.
- **Application**
  - Should be carried out with an appropriate frequency.

Approach

1. Define roles and responsibilities
2. Communicate roles and responsibilities
3. Coordinate and collaborate
4. Visualize and document

Special SME characteristics are taken into account

- Limited IT resources
- Dependence on external IT suppliers
- Need for cost-effective security solutions

Definition of roles and responsibilities (examples)

Role	Responsibility	Internal / External	Examples
CISO / IT-responsible	Overall cybersecurity strategy and policies	Internal	Development of policies, risk assessment
System administrator	Technical implementation and maintenance	Internal	Firewall, access control, updates
Data processor (supplier)	Ensuring data security in accordance with the contract	External	Hosting, cloud services
Customer	Compliance with secure use and reporting	External	Use of secure passwords, incident reporting
Trade partners	Compliance with common security protocols	External	Shared access to systems, data sharing

Communication of roles and responsibilities

Internal

- Policies and procedures: Document and share via intranet or employee handbook.
- Workshops and awareness training: Regular sessions on cybersecurity.
- Incident response plan: Clear contact points and escalation paths.

External

- Contractual agreements: SLAs (service level agreements) and data processing agreements with security requirements.
- Onboarding packages: Information material for new customers and partners.
- Security communication: Use of secure channels for sharing sensitive information

Coordination and collaboration

Internal

❑Cross-functional teams: IT, HR, management, and legal collaborate on security.

❑Regular meetings: Status updates on threats, incidents, and compliance.

External

❑Joint contingency plans: Coordinated response to security incidents.

❑Security audits: Mutual audits and controls.

❑Threat information sharing: e.g., via incident information centers or industry forums.

Visualization and documentation (example)

- It may be beneficial to prepare a **RACI** diagram (Responsible, Accountable, Consulted, Informed) for each important cybersecurity activity.
- See example below.

Activity	**IT-responsible**	**Supplier**	**Customer**	**Partner**
Access control	R	A	I	I
Data protection	A	R	I	C
Incident response	A	C	I	C
xx	xx	xx	xx	xx