# Protection of intellectual property rights

www.cyber-smv.dk

The tool has been developed as part of the project Cybersecurity and Business Continuity (www.cyber-smv.dk), supported by the Danish Industry Foundation.
Published on May 12, 2026.

# Purpose, participants and application

- **Purpose**
  - To support the establishment and coordination of cybersecurity measures for the protection of intellectual property (IP).
- **Participants**
  - Data and IT managers, suppliers, and other relevant external partners.
- **Application**
  - Should be carried out at appropriate intervals.

# Approach

1. Classification of existing intellectual property rights (IP).
2. Mapping of knowledge among employees.
3. Implementation of appropriate cybersecurity measures.
4. Preparation of recovery and business continuity plans.

*Special SME characteristics are taken into consideration:*

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

# Classification of existing intellectual property (IP)

## Methods

- **Different levels of confidentiality, at a minimum:** Public, internal, confidential (restricted).
- **Awareness of IP and confidentiality:** Not only for employees, but also for consultants/contractors.
- **Crown jewels:** IP that is essential to the company's existence and constitutes high-value targets.

## Policy

- **Target group:** Employees, consultants/contractors, and suppliers.
- A policy that defines data classification levels, including criteria for each level.
- The policy should include examples illustrating the application of the criteria and classification levels.

# Mapping of knowledge among employees

## Considerations

- Individuals require different levels of access to confidential information.
- **Mapping of high-risk roles:** Balancing dependence on key/expert employees and the associated risk.
- **Non-disclosure agreements (NDAs):** For employees and consultants/contractors, but should not stand alone.
- **Compliance monitoring:** Active control of adherence to policies and agreements to prevent breaches.
- **Ethics policy:** Data classification and responsibility for compliance among employees and consultants/contractors.
- **Legal action:** Be prepared to initiate legal measures in the event of disclosure.

## Threats

- Intentional or accidental disclosure.
- **Insider threats:** Dissatisfied employees, former employees, or consultants/contractors.
- **External threats:** Malicious actors.

# Implement appropriate cybersecurity measures

## Considerations

- **Scope of risk:** All infrastructure (ERP, email, collaboration tools, etc.) may contain confidential IP.
- **Data protection:** Protect data at rest, in transit, and in use with controls adapted to each specific state.
- **Use of AI/LLMs (Large Language Models):** Treat (public and private) LLMs as high-risk data processors; define permitted data types, licensing restrictions, and classification rules before use.
- **Supplier intelligence:** Supplier assessments and content in ERP systems are valuable targets and should be protected to avoid enabling compromise further down the supply chain.

## Threats

- **Data exfiltration via collaboration tools** – leakage through email, Slack, Teams, or file-sharing solutions.
- **Human targets** – social engineering, theft of login credentials, phishing, and accidental disclosure.
- **Technological weaknesses** – misconfigurations (e.g., insufficient encryption) and outdated systems.

# Develop recovery and business continuity plans

## Considerations

- **Visibility and telemetry (remote measurement/transmission of measurement data via telecommunications):** Effective data loss prevention and monitoring require full visibility.
- **Supply chain dependencies:** Map third-party suppliers, their security level, and alternative suppliers or mitigating measures in the event of supplier compromise.
- **Testing and tabletop exercises:** Plan regular exercises for scenarios involving IP leakage/loss and supplier takeover.
- **Backup integrity and access:** Establish and validate effective backups of IP and ensure that procedures are tested and exercised.

## Threats

- **Supply chain attacks** – attackers exploit leaked supplier assessments or impersonate suppliers.
- **Incomplete collection of forensic data** – recovery actions that overwrite evidence needed to determine the cause of the breach, thereby hindering legal action or remediation.