10. Check list for the termination of cooperation

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - When terminating a partnership or a service agreement, it is important to take into account a number of cybersecurity measures to protect data, systems, and business-critical information.
- **Participants**
  - Management, IT, legal.
- **Application**
  - In connection with the termination of collaboration with partners (e.g., suppliers).

Procedure / check list 1/6

1. Preparation phase

Purpose: Ensure planning and overview before termination.

- ❑ Identify all systems, data, and services that the partner has had access to.
- ❑ Review the contract for requirements regarding data deletion, confidentiality, and handover.
- ❑ Appoint responsible persons for the termination process (IT, legal, management).
- ❑ Prepare a detailed termination plan with timeline and milestones.
- ❑ Inform relevant internal stakeholders

Procedure / check list 2/6

2. Access control

Purpose: Prevent unauthorized access after termination.

- ❑ Disable or remove all user accounts belonging to the partner.
- ❑ Change passwords for shared accounts and systems and update multi-factor authentication.
- ❑ Close VPN, API (Application Programming Interface), and remote access.
- ❑ Remove the partner’s devices from the network and any mobile solutions (mobile, PC).

Procedure / check list 3/6

3. Data Management

Purpose: Protect and control data in accordance with GDPR and the contract.

- ❑ Identify all data that the partner has processed or stored.
- ❑ Agree on and document how data should be returned, transferred, or deleted.
- ❑ Document the deletion and obtain written confirmation of data deletion from the partner.
- ❑ Conduct internal checks to ensure that no data has been copied or exfiltrated.
- ❑ Prepare a detailed termination plan describing:
  - ❑ Which systems and data must be transferred or deleted.
  - ❑ Timeline for termination.
  - ❑ Allocation of responsibilities.

Procedure / check list 4/6

4. Documentation and Handover

Purpose: Ensure continuity and knowledge transfer.

- ❑ Receive all relevant documentation (system configuration, source code, licenses, etc.).
- ❑ Carry out a technical handover if the partner has been responsible for operations or development.
- ❑ Archive all communication and documentation related to the termination.

Procedure / check list 5/6

5. Monitoring and Incident Handling

Purpose: Prevent and detect security breaches.

- ❑Increase monitoring of systems during the transition period.
- ❑Conduct a security review after termination.
- ❑Be alert to potential threats, including insider threats and attempts at data theft.
- ❑Update the incident response plan with scenarios related to termination.
- ❑Have a contingency plan ready in case of a security breach.

Procedure / check list 6/6

6. Evaluation and Learning

Purpose: Improve future processes.

- ❑ Evaluate the entire termination process with relevant teams.
- ❑ Update internal policies and procedures based on lessons learned.
- ❑ Document improvement proposals for future collaborations.
  - ❑ For example, include clear clauses on cybersecurity in the contract, such as:
    - ❑ Requirements for data deletion.
    - ❑ Confidentiality obligations continuing after termination.
    - ❑ Right to audit and inspection.
  - ❑ Inform relevant internal parties (IT, Legal, Management) about the termination.
  - ❑ Train employees on how to handle inquiries from former partners.