

**ISMS**policy

|  |  |  |
| --- | --- | --- |
| **This policy concerns:** | | |
| SKOV A/S | SKOV Thailand | SKOV China |
| SKOV North America Inc. | Secco International Inc. | XIO A/S |
| SKOV-SERCOM B.V. |  |  |
|  |  |  |
| Created by/Date:  LEO/2025-08-29 | Approved by/Date:  LEO/2025-08-29 | Version:  2.0 |

**Contents**

[1 Purpose 3](#_Toc190413040)

[2 Policy 3](#_Toc190413041)

[2.1 ISMS commits us to work on the below items actively 3](#_Toc190413042)

# Purpose

SKOV A/S's policy is to implement and maintain an Information Security Management System (ISMS) based on ISO 27001 and ISO 27002, aligned with the overarching principles and objectives set forth in the "*Guideline for Information Security*" of the Big Dutchman Group.

Our ISMS is a formalized, documented system comprising activities, processes, policies, procedures, and responsibilities, all designed to achieve our information security objectives.

# Policy

## ISMS commitments

Our ISMS commits us to actively work on the following items:

* Ensure that the information security policy and objectives are established and aligned with SKOV’s strategic direction.
* Integrate the information management system into SKOV’s business processes.
* Communicate our policy to stakeholders and interested parties — including external parties — who have a legitimate need to understand our security practices.
* Comply with all legal requirements and codes of practice relevant to our business.
* Fulfill applicable information security requirements and ensure continuous improvement of our ISMS.
* Provide the necessary resources – including equipment, competent staff, and investments - to achieve our objectives.
* Ensure that all employees and stakeholders are aware of their responsibilities regarding our ISMS.
* Maintain a management system that supports our objectives and promotes continuous improvement in information security.
* Reduce the risk of unauthorized access to our controllers and software products by incorporating data security into product design and advising customers to report any security vulnerability to SKOV.
* Ensure that senior management, SKOV MTS (Management Team SKOV), understands their responsibility to review the management system to keep it appropriate and effective for our business.
* Remain committed to keeping the ISMS compliant with the EN ISO/IEC 27001:2022 and EN ISO/IEC 27002:2022, and to observing all current legislation and regulatory requirements.
* Align with the "*Guideline for Information Security*" of the Big Dutchman Group and contribute to the group’s overall information security objectives.