COPENHAGEN OFFSHORE PARTNERS

Information Security Policy

COPENHAGEN OFFSHORE PARTNERS

Table of Contents

1. Purpose and Scope

Copenhagen Offshore Partners (COP) is committed to conduct its business responsibly and with integrity towards all stakeholders across our value chain. As an **ISO 27001:2022–certified organization**, COP maintains an Information Security Management System (ISMS) that ensures our information assets are systematically identified, recorded, and protected through risk-based and continuously improving security controls.

This document sets forth certain principles regarding the responsible use of information by Copenhagen Offshore Partners and outlines the roles and responsibilities of personnel to protect the confidentiality, integrity, and availability of Copenhagen Offshore Partners' resources and data.

This policy covers Copenhagen Offshore Partners' information and information systems, including information and information systems used, managed, or operated by a contractor or other vendors and applicable to all Copenhagen Offshore Partners employees, contractors, and other users of Copenhagen Offshore Partners' information and information systems.

The scope of the information security policy includes protecting the confidentiality, integrity, and availability of information and applies to all data, material, information, Personally Identifiable Information (PII) and other categories of protected information in any form (physical, electronic, verbal, etc.) owned or controlled by the Company.

2. Policy Statements

- Implement and maintain the Information Security Program at Copenhagen Offshore Partners.
- Continuously improve and align information security practices to global best practices and standards.
- Information security policies shall be reviewed regularly by management. Copenhagen Offshore Partners employees shall acknowledge their adherence to these information security policies and practices annually.
- Security awareness training shall be provided regularly.
- Internal assessments or audits of Copenhagen Offshore Partners' Information Security Program shall be performed periodically, and any gaps or findings shall be remediated promptly.
- A risk assessment process for Copenhagen Offshore Partners' information assets shall be defined and followed. Risk reduction shall be carried out through the process of continuous improvement.
- Copenhagen Offshore Partners' information asset inventories shall be reviewed and updated when a new asset is added and/or an existing asset is upgraded.
- Business continuity plans (BCPs) and backup plans shall be reviewed and tested at least annually.

- Roles and responsibilities of senior officials and staff shall be clearly defined and communicated to relevant individuals.
- Information shall be classified and handled according to its criticality and sensitivity as mandated by relevant legislative, regulatory and contractual requirements.
- Appropriate contacts shall be maintained with relevant authorities, special interest groups or other specialist security forums.
- As needed, the security incidents shall be reported outside of Copenhagen Offshore Partners by a designated person nominated by executive management.
- Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
- Any information shared by Copenhagen Offshore Partners (i.e., independent review of ISMS, audit report, certifications) with prospects, prior to entering, and for the duration of, a contract, shall be done in accordance with the established confidentiality or non-disclosure agreements.
- COP shall commit to upholding intellectual property rights, including software and information products. Employees shall adhere to legal requirements, acquire software from reputable sources, and partake in appropriate user awareness for the proper use of intellectual property.
- Anti-virus and anti-malware solutions shall be deployed on system components.
- Prevention, detection, and recovery controls to protect against malware and phishing attacks shall be implemented by Copenhagen Offshore Partners, and these will be combined with appropriate user awareness.
- An incident management process shall be established to correctly identify, contain, investigate, and remediate incidents that threaten the security or confidentiality of Copenhagen Offshore Partners' information assets.
- Copenhagen Offshore Partners shall develop and maintain a vendor management process for third-party vendor engagement and assessment.
- Change and vulnerability management controls shall be established and implemented.
- COP maintains a structured compliance approach by identifying, recording, and monitoring all applicable legislative, regulatory, and contractual requirements, including but not limited to the General Data Protection Regulation (GDPR) and relevant Danish laws. These obligations are documented, reviewed annually, and communicated to responsible stakeholders.
- Compliance activities are centrally managed through COP's internal Governance and Compliance Platform ("Global Compliance App"), which ensures that applicable requirements are linked to relevant processes, controls, and owners. The platform facilitates timely updates, periodic reviews, and evidence collection to demonstrate alignment with legal, regulatory, and contractual obligations.

- Senior management is responsible for overseeing compliance, while department owners ensure that day-to-day operations adhere to these obligations. Where applicable, documented procedures and audit trails support internal reviews and external audits.

3. Information security objectives (Key Performance Indicators)

We record the following objectives:

- **Governance & Compliance**
  To ensure that information security management complies with business requirements, organizational policies, and applicable legal, regulatory, and contractual obligations.
- **Framework & Processes**
  To maintain an effective administrative framework that governs the implementation, operation, and continuous improvement of information security within the organization.
- **People & Awareness**
  To ensure that employees and contractors understand their information security responsibilities, are suitable for their roles, and consistently fulfill these responsibilities.
- **Assets & Protection**
  To identify and protect the organization's information assets, ensuring appropriate classification, proportionate protection, secure handling in processing facilities and networks, and adequate safeguards when accessed by suppliers.
- **Continuity & Availability**
  To integrate information security into the organization's business continuity framework, ensuring the availability and resilience of critical information processing facilities and systems.
- **ISMS Effectiveness**
  To ensure that information security is effectively implemented, monitored, and operated in accordance with the organization's ISMS policies, procedures, and continuous improvement activities.

4. Information Security Policies

This document, along with the rest of Copenhagen Offshore Partners' information security policies, define the principles and terms of Copenhagen Offshore Partners' Information Security Program, as well as the responsibilities of the users and employees in carrying out and adhering to the respective program requirements.

The Company has also instructed the Cyber Security Lead in accordance with the Risk Assessment and to the extent required to create and revise the following (non-exclusive) information security policies:

- Access Control
- Clean Desk and Clean Screen
- Backup and restoration
- Key Management and Cryptography
- IT Vendor and Partner Governance
- Acceptable Use
- Workstation and Mobile Device
- Working out of Office
- System Development
- Risk Assessment
- Information Classification
- Change Management
- Incident Management
- Internal Assessment
- IT Asset Management
- Logging and Monitoring
- Network Security
- Personnel Security
- Privacy Policy
- Technology Equipment Handling and Disposal
- Vulnerability and Penetration Testing Management
- Data Retention and Disposal
- Business Continuity and Disaster Recovery
- Information Security Disciplinary Policy
- Generative AI Policy
- Physical and Environmental Security

Violations of Copenhagen Offshore Partners' information security policies may result in corrective actions and the start of a disciplinary process.

5. Obligations

The Company's senior management is responsible and committed with respect to information security within the organization to:

- Formulate and review this information security policy,

- Approve and review all procedures, actions and policies resulting from this policy,
- Provide all resources necessary to meet all information security requirements of the organization,
- Continuously improve the information security management system; and
- Make appropriate decisions with respect to information security

6. Information security definitions

Availability: Ensuring timely and reliable access to and use of information.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including text, numerical, graphic, cartographic, narrative, or audiovisual media.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide unimpeded confidentiality, integrity, and availability.

Information system: A discrete set of information sources organized for the collection, processing, maintenance, use, distribution, dissemination, or disposal of information.

Information Security Risk (Cyber Risk): The risk to organizational processes (including the mission, functions, image and reputation of the organization), organizational assets (tangible or intangible), individuals, other organizations as well as the State due to the potential unauthorized access, use, disclosure, dissemination, modification or destruction of information and/or information systems. (See ***Risk***).

Integrity: Protection against unauthorized modification or destruction of information including ensuring the non-waiver of liability and the authenticity of information.

Risk: A measure of the degree to which an entity is threatened by a potential circumstance or event, and typically a function in which:

- the adverse effects that would result if the circumstance or event occurred; and
- the probability of occurrence

7. Policy Awareness and Communication

Copenhagen Offshore Partners (COP) will communicate this policy internally via the company intranet, ensuring that it is accessible, visible, and understandable by all employees and contractors. All staff will be

required to acknowledge their awareness of and adherence to this policy through the designated compliance platform.

In addition, COP will make this policy publicly available on its corporate website to demonstrate transparency and commitment to information security towards clients, partners, regulators, and other external stakeholders.

COP maintains dedicated communication channels (e.g., Speak Up! Platform) to ensure that incidents or concerns related to information security or potential breaches of policy can be reported, evaluated, and addressed in a timely manner.

Examples of reportable information security incidents include, but are not limited to:

- Breaches of information security policies
- Unauthorized access to systems, applications, or data
- Suspected or actual phishing, malware, or ransomware attacks
- Loss, theft, or improper disclosure of confidential information,

All reports are handled in accordance with the Cyber Security Incident Communication Procedure, ensuring proper escalation, investigation, and resolution.

8. Policy Exceptions, Local Requirements and Enforcement

There are no exceptions to this policy and any request for exception will be addressed through **ISMSD-02 Exception Procedure.**

9. Policy Contact Email

Should you have any questions, feedback or complaints about COP's Information Security Policy, please email to CyberSecurity@cop.dk .

10. Policy Review, Monitoring and Approval

COP reserves the right to amend and revise the content of this policy when necessary (e.g., legislative changes, COP business changes). At a minimum, COP will initiate a review of this Policy every two (2) years. This policy is approved by the Chief Financial Officer of COP A/S.

11. Policy Versions

The following table illustrates version logs and respective changes to Policy.

Version No	Effective from	Changes	Approved by
1	01/01/25	New policy initiation	Chief Financial Officer