Danish Crown

Information Security Policy

Governance	
Version	2
Application date of present version	01-05-2025
Approved by	Board of Directors, Danish Crown A/S
Accountable for implementation of policy	Group CFO, Danish Crown A/S
Scope	Danish Crown Group
Review frequency	Every year

Content

Introduction **4**
1.1 Purpose 4
1.2 Objectives 4
1.3 Scope 4
1.4 Risk Assessment 5
1.5 Documentation 5
1.5.1 Document structure and related documents 5
1.6 Management Review 5
1.7 Communication 5
1.8 Violations 5

Information Security Governance and Compliance **6**
2.1 Information Security Responsibility 6
2.2 Compliance 6
2.3 Exemptions 7

Requirements for Information Security **8**
3.1 Organizational Security 8
3.2 People Security 8
3.3 Physical Security 8
3.4 Technical Security 8

Definitions **10**

Introduction

1.1 Purpose

Information security is defined as the necessary protection of all resources involved in or contributing to the processing or communication of data in electronic or physical form. This includes technology as well as business processes.

The purpose of the Information Security Policy is to document and represent the decisions taken by Danish Crown Group executive management to define the security level, responsibility, and define the high-level requirements that are necessary to ensure the desired security level is achieved.

The purpose of the Information Security Policy is also to provide a document structure to communicate the detailed security requirements, responsibilities and controls that must be in place across the organization to implement an Information Security Management System.

1.2 Objectives

The level of information security implemented must support the Danish Crown Group business to meet the objectives defined in this policy. In achieving these objectives, the information security supports that Danish Crown Group continues to live up to expectations on credibility by the owners, customers, and consumers.

The objectives are determined based on 3 main criteria:

- Confidentiality – protection against unauthorized access to data
- Integrity – reliable data with protection against corruption
- Availability – stable access to relevant data at all levels of the organization.

The objectives for information security are:

- Anchoring of information security responsibility and awareness throughout the organization
- High operational availability and minimizing risk of major outage and data loss
- Ensure correct processing within IT systems and minimizing risk of data manipulation and errors in the IT systems
- Ensure that necessary facilities are in place for confidential processing, transmission, and storage of information/data
- Implement security measures against attempts to bypass the implemented physical and logical security measures
- Ensure effective business continuity and disaster recovery is in place to minimize downtime in the event of a contingency situation
- Securing compliance with relevant legislation, such as GDPR (EU General Data Protection Regulation 2016/679 - GDPR) and NIS2 (EU Directive 2022/2555 - NIS2).

The objectives are achieved by applying recognized standards to implement information security controls in Danish Crown Group. The implementation shall follow ISO27001 and may apply supplementary methods and controls from other recognized standards such as CIS Critical Security Controls, NIST Cyber Security Framework and IEC62443 (IT Security in Industrial Networks and Systems). Attaining a certification within any of these standards is not in the scope of objectives.

1.3 Scope

This policy applies to all systems and all data within Danish Crown Group's possession/control. It applies to all production and administrative parts of the business that has direct or indirect impact on the operation of Danish Crown Group IT systems and paper archives.

The policy applies to all employees at Danish Crown Group regardless of which form of employment applies and to suppliers and partners with physical or logical access to systems or data controlled by Danish Crown Group.

1.4 Risk Assessment

A consistent and documented method for performing risk assessment and follow-ups must be implemented, and it must include a defined set of security risk criteria.

The security level as set out in this policy must be defined based on a group-level risk assessment. This risk assessment must take into account the current threat landscape, vulnerability assessment and security posture of the organization.

The responsibility for risk treatment, decisions on which risks to accept, and which to mitigate must be based on the agreed and documented risk appetite, and is anchored within the Information Security Board. Security generally carries high-cost levels. To optimize spending and ensure an acceptable investment level, all prioritizations must be accomplished using a riskbased approach.

Risk assessment, risk analysis and agreed follow-up activities must be documented and stored in the appropriate location that is relevant to the subject of the risk analysis.

The risk assessment must be reviewed at least once every year. Also, the risk assessment must be updated if any major changes occur, such as changes to IT system architecture organizational changes, or changes to the threat landscape.

1.5 Documentation

An Information Security Management System (ISMS) must be maintained to document compliance with this policy. The ISMS must contain at a minimum:

- Risk analysis
- Risk acceptance
- Documented policies, standards, and guidelines
- Relevant processes and other documentation
- Controls and follow-up
- Incident learnings
- Improvement activities.

Policies, Standards and Guidelines must be stored in Group Library and linked in the ISMS. Other documents can be stored inside the ISMS directly or outside where appropriate and linked. It is the responsibility of the Director of Information and Security to ensure that the ISMS is maintained in accordance with the improvement cycle of ISO27001.

1.5.1 Document structure and related documents

The Information Security Policy, the Information Security Governance and the specific control requirements in section "Requirements for Information Security" are supported by a set of underlying standards and guidelines that must be aligned.

1.6 Management Review

This policy must be reviewed annually or when major changes affecting the policy occur. The policy follows Danish Crown's approval process and thus, is subject to approval by the board to ensure anchoring and alignment with overall strategies.

1.7 Communication

Employees must be aware of the Information Security Policy in the form of the IT Security Guideline, and they must read and acknowledge compliance with the IT Security Guideline before getting access to systems or data.

External parties who as well must comply with the Information Security Policy must receive the policy in full or a subset thereof with relevant guidelines and acknowledge compliance before getting access to systems or data.

When the Information Security Policy is updated, all relevant stakeholders must be made aware of the changes to ensure that the underlying standards and guidelines can be equally updated.

1.8 Violations

A violation of the Information Security Policy and the IT Security Guideline can – depending on the circumstances – lead to disciplinary actions in accordance with HR procedures.

Information Security Governance and Compliance

2.1 Information Security Responsibility

The objective of the organizational governance is to ensure an efficient cooperation between the Business Units, Global IT, and other relevant parts of the organization. The key stakeholders for information security are:

- **The Audit and Risk Management Committee** represents the Board of Directors on information security and is responsible for setting the overall risk acceptance level in Danish Crown

- **The Information Security Board** has the overall responsibility to set the direction for information security. The Information Security Board decides on strategic information security projects and provides necessary funding

- **The Senior Vice President of Global IT** is delegated the management accountability for information security per appointment by Excecutive Management.

- **The Director of Information and Security** is responsible for managing the implementation of the direction set forth by the Information Security Board. This includes providing the Information Security Board with updated information on risk picture, threat analysis, and suggested road map for information security and supporting IT Operations

- **The IT Security Team** carries out the implementation of the projects approved by the Information Security Board and handles incidents and daily security operation in cooperation with IT Operations. Additionally, the security team must provide consultancy to the organization on IT security matters (or sourcing from external suppliers)

- **Employees** People managers are responsible for ensuring that their employees are aware of the IT Security Guideline and that they participate in the necessary training programs. All employees are responsible for complying with the requirements of the IT Security Guideline

- **Suppliers, and partners** are non-Danish Crown employees with access to systems or data, and they are responsible for complying with information security requirements as stated by Danish Crown Group

- **Business process owners/assets owners** are responsible for implementing security requirements in their processes and for implementing appropriate security measures on assets.

The organization of information security is documented in the Information Security Governance document.

2.2 Compliance

Cyber security is increasingly becoming a critical part of contracts with customers and suppliers.
Also, legislation is in effect in many of the countries in which we operate that affect our security requirements. Compliance with relevant laws (such as EU General Data Protection Regulation 2016/679 - GDPR and EU Directive 2022/2555 - NIS2) as well as upholding the requirements set forth in contracts is critical.

The IT Security Team must define and implement a method to continuously monitor and measure the level of compliance with this policy in the organization, including ways of protecting information systems during audit testing. Measurements or tests must cover both Global IT as well as the individual factories and must be integrated with risk analysis and implementation of improvements.

As a minimum once every three years an external assessment of the organizations compliance to this policy as well as the related standards must be performed. The assessment must be performed by an independent third party with accreditation to perform such assessments.

2.3 Exemptions

Exemptions from this policy may be granted only by the Senior Director of IT Operations, the Director of Information and Security, or the Senior Vice President of Global IT. It is a requirement to document exemptions in the ISMS and to maintain a current catalog of exemptions that may be granted to this policy as well as the related standards. An exemption must always be accompanied by a documented risk assessment.

An exemption request must use the exemption request form and as a minimum document:

- Which system/process requires exemption
- Which (part of) policy or standard is the system/ process exempted from
- Reason for exemption
- Expected duration of exemption and exemption expiration date
- Documented Risk Analysis
- Responsible Manager
- Approver.

Requirements for Information Security

3.1 Organizational Security

Organizational Security covers managing the risk associated with organizational processes and governance, e.g. by developing written operating procedures and implementing these to ensure that access to a system is given on basis of a work-related need and with prior documented approval.

Following ISO27001 clause 5, further governance and controls must be implemented to secure **Organizational Security**, within the following function areas:

- **Asset Management** to identify information assets, asset owners and to appropriately protect these assets according to a classification scheme to prevent unauthorized disclosure, modification, or loss of information

- **Access Control** to protect systems and information against loss of confidentiality, to ensure a process for authorized access and safeguarding credentials for authentication is implemented to prevent unauthorized access to systems and data

- **Documented Procedures** to define security responsibilities within operating procedures and to ensure consistency on process level
  - Detailed requirements shall be documented separately in dedicated operating procedures

- **Supplier Relations** to ensure that agreements that include information security requirements with suppliers are in place and that controls and technology must be in place to protect internal and external information assets to which suppliers have access

- **Incident Management** to ensure that security events are detected, handled, and learned from consistently according to procedures and relative to legislation

- **Service Continuity** to define responsibilities and ensure ongoing availability in cases of disruption.

3.2 People Security

People Security covers managing the risk associated with actions performed by employees and other stakeholders, such as implementing an information security awareness training program to ensure that employees can identify and avoid security threats.

Following ISO27001 clause 6, **People Security** controls must be implemented to ensure that management, employees, suppliers and external partners understand their responsibilities in relation to information security and apply appropriate security behavior throughout their employment cycle.

3.3 Physical Security

Physical Security covers managing the risk associated with outages or damage to physical equipment, such as implementing a secondary power supply to ensure that servers can run for a period of time if the power is out.

Following ISO27001 clause 7, **Physical Security** controls must be implemented to ensure that access to all physical locations of Danish Crown Group is secured against unauthorized access, damage and interference. Threats against Danish Crown Group property must be evaluated, and risk levels and necessary protection must be considered.

3.4 Technical Security

Technical Security covers managing the risk associated with information or systems from an IT operations/administrative point of view, such as ensuring that only persons with a work-related need have privileged access and ensuring that systems have sufficient backups to be recoverable in case of a cyber attack.

Following ISO27001 clause 8, further governance and controls must be implemented to secure **Technical Security**, within the following function areas:

- **Privileged Access Governance** to protect systems and information against unauthorized changes on configuration and ensure that only authorized users gain privileged access to prevent loss of confidentiality and integrity

- **Encryption** to effectively apply encryption according to an information classification scheme to protect information assets from unauthorized disclosure and/or unauthorized modification

- **Security in Network, Network Services and Devices** to protect information in systems and applications, and internally and externally transmitted data

- **IT Operations** to secure high availability of operational systems, to ensure correct data information processing and to protect against loss of data, including establishing appropriate backup procedures and malware/cyberattack protection

- **Log Management** to establish appropriate monitoring of logs, timely reaction on critical events and to prevent unauthorized modification of logs, thus protecting the integrity of logs on critical services for the purpose of performing forensics

- **User Endpoint Devices** to establish a security baseline (hardening) for end-point devices, such as computers, phones and tablets to secure confidentiality and integrity of information processed on the devices

- **Change Management and Secure Development Lifecycle** to ensure that information security is integrated in changes performed on operational systems and throughout the System Development Lifecycle.

Definitions

Information Security Board: Overall responsible for Information Security and owner of the Group IT Risk Analysis. Members are CFO, CIO, Director of Information Security, Senior Director of IT Operations, as well as a member from the business appointed by the CFO.

Information Security Management System: The management system that documents the information security level decided by the Information Security Board. This includes but is not limited to policies, standards, guidelines, exemptions, audit reports, improvement activities.

ISO27000: An international standard series for information security. The standard is divided into several sub-standards where ISO27001 provides the overall guidelines for steering of information security. It is the standard that companies normally are certified to.

GDPR: Refers directly to the EU General Data Protection Regulation 2016/679 of 2018. However, local legislation implementing the EU GDPR must also be considered each time GDPR is referenced.

NIS2: EU directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

ICT Security: Industrial Control Technology security generally refers to the security of systems that are used in the production/manufacturing area. There is a high requirement for availability to maintain our production ability.

Critical Services: Assets or systems with an essential role in the IT architecture or that plays an important part in system flow or processes and will be greatly impacted of a disruption.

Operational Systems: Active, productive systems.

Information Security: to protect against the unauthorized access, use, disclosure, disruption, modification, and destruction of information to provide confidentiality, integrity, and availability. The term is used regardless of the form the data may take (e.g., electronic, physical, or verbal).

IT Security or Information Technology Security: to protect against unauthorized access to computers, networks, and data. IT Security is a subset of information security referring to the technological aspects of information security.

System Development Lifecycle: is defined by the scope of activities associated with a system, including software on the system. The activities of within the life cycle of the system is its initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation.