Information Security Policy

Prepared by:	CTO
Controlled by:	CEO
Approved by:	The Board
Version and date:	1.0 / 29.10.20
Regulations and internal rules:	-
Change log:	NA. First version.

1. Background and purpose

To achieve our overall goals, the Mercell Group ("the Group" or "Mercell"), which includes Mercell Holding AS and majority owned subsidiaries ("subsidiaries"), depends on trust from our customers, owners, authorities and other stakeholders. To maintain and strengthen this trust, we must manage our assets with due care.

One of the most important assets of the Group, is the information that we process in our daily operations. Processing of information includes collection, storing, sharing, archiving, printing, copying and deleting information. Inadequate information processing may cause serious impacts for Mercell, such as direct costs, loss of trust, sanctions or even legal prosecution.

Some information represents a greater risk than other. A breach involving personal information may induce severe financial punishment and exposure of confidential customer information may cause severe harm to the Group's reputation.

To ensure secure processing of information, Mercell has adopted this Information Security Policy. Information security requires a set of strategies for managing the processes, tools and policies / standards / guidelines necessary to prevent, detect, document and counter threats to digital and non-digital information. This policy defines the information security objectives and outlines the

principles for secure information processing for all companies in the Mercell Group, including how the work is organized and shall be done in the Group to reach the information security objectives and support the achievement of Mercell's overall goals.

The Information Security Policy is part of the Group's Information Security Management System ("ISMS"), which is based on the ISO/IEC 27001 standard. The policy is operationalized by a set of guidelines.

2. Applicability

This policy applies to:

- All services provided and/or produced by any of the Companies in the Mercell Group
- All employees in the Group
- All temporary/hired personnel and third parties engaged by the Group

Any Company-specific principles and guidelines for information security must be within the principles set out in this policy.

3. Definitions

Group: The Mercell Group comprising Mercell Holding AS and majority owned subsidiaries.

Company: Any legal entity for which this policy applies.

Incident: Any unplanned and unwanted event causing potential or actual harm to the Confidentiality, Integrity or Availability of the information.

4. Information security objectives

This policy shall support and enable the following objectives:

- Protection of the customers', employees' and Group's values, information and reputation.
- Maintaining authorities', customers', employees' and partners' trust in the Group's secure processing of information.
- Fulfilment of the Group strategy at all times, including the compliant and secure Group-wide sharing of information over the Data Highway and otherwise.
- Prevention of written, digital and verbal information from unauthorized disclosure.
- Compliance with all regulatory and contractual information security requirements, including customers' and employees' personal data protection.
- Secure and stable IT operations.

5. Key Principles for Information Security

5.1. Availability, Integrity and Confidentiality

Availability, Integrity and Confidentiality are key factors in caring for the information security. These factors should be considered in regard to the Group's business requirements and overall risk management.

Availability

Relevant information and purposeful IT solutions shall be available in an effective manner to employees, customers and providers with relevant authorization and professional purpose.

Downtime shall be kept to a minimum and relevant efforts shall be put into place to ensure that unwanted/unplanned downtime meets Mercell's and customers' requirements.

Integrity

Information, for which the Group is responsible, shall only be created and altered by employees or hired resources with the relevant authorization, professional purpose and training. Systems, processes and functions shall regularly be evaluated to identify potential need for improvement in order to limit the risk of unintentional information alterations.

Confidentiality

Information shall be protected from any unauthorized access or provision. Information shall only be accessed by authorized resources and employees with relevant professional purpose and training, and only after a signed agreement of confidentiality is in place. Information shall only be made available to employees with explicit authorization in accordance with the relevant process for access management.

5.2. Data classification

All data processed shall be classified as a mean to ensure adequate basis for assessing the involved risk. Specific, targeted and differentiated measures shall be implemented on the information according to its classification and the associated risk, ref. Standard Data Classes.

5.3. Risk assessment

The information security measures put into place shall take into consideration the level of risk involved given the nature of the information processed, the processing itself, and the circumstances under which the processing takes place.

The Group shall assess the information security risk at least once a year and provide relevant means to manage the risk within acceptable levels, whether technological, organizational or both.

A risk assessment shall be performed before any new processing, tool, system, service and vendor is taken in use or when there is a significant change in the risk involved in the processing of information, e.g. a change in regulatory or customer requirements, business processes, systems, platforms, infrastructure, company structure (e.g. mergers and acquisitions). Whenever such processing includes personal data, a Data Protection Impact Analysis ("DPIA") shall be considered, and, if required, carried out. The consideration shall be based on the Mercell Group standard DPIA checklist.

Risk assessments shall be performed using the relevant methods and criteria for acceptable risk and managing identified risks. Relevant technical and organizational measures shall be implemented in order to maintain the risks at an acceptable level.

5.4. Assets inventory and disposal/handover

The Company shall keep an inventory of equipment and systems, tools and services being used for the processing of information. System owners shall keep an inventory of the information processed by the relevant systems.

Disposal or handover of any equipment shall follow the procedures laid out in the "Guidelines for equipment disposal and handover".

5.5. Business continuity

Business critical functions, systems and processes shall be implemented in a manner that ensures the ongoing operation in the event of a critical error or a disaster. Plans shall be in place to secure information, personnel and company values and ensure the continuity of such functions and processes in such events.

System owners shall ensure that the business continuity and readiness requirements for business-critical functions are met by the relevant system-/service provider.

The plans shall be tested in practice at least once a year.

5.6. Internal review

The various roles and responsibilities related to information security are:

- The Board of Mercell Holding AS
    - shall oversee that this information security policy is adopted throughout the Grou
    - approves the Information Security Policy and decides the overall level of acceptable information security risk
- The Board of the respective legal entities shall oversee the legal entities' information security work and its alignment with the business strategy and the overall level of acceptable information security risk
- The Group CEO (Chief Executive Officer) is accountable for the Information Security Policy and the sufficient and adequate allocation of resources to meet the information security goals
- The Group CTO (Chief Technology Officer) is responsible for the implementation and the adherence to this policy, including:
    - developing awareness and guidance in the area of information security to the employees, temporary/hired personnel and third parties classifying the data and assessing the risk involved
    - establishing and maintaining continuity plans which secures the readiness and ongoing operation in the event of a critical error or a disaster
    - approval of any planned deviation from this Policy
- The GCM (Group Compliance Manager) is responsible for monitoring the effective implementation of this Policy, hereunder regular sample testing, vendor audits as well as investigating reports of violation of this Policy
- All Company Leaders are responsible for

- establishing a signed agreement of confidentiality with the employees and temporary/hired personnel before granting access to any Mercell systems / information
- informing the employees and temporary/hired personnel about the rules for information protection and how to find this information
- All employees and temporary/hired personnel and third parties have a responsibility to know, understand and follow this Policy and related guidelines

The roles and responsibilities are operationalized in a separate Security guideline.

6. Exceptions

Any planned, potential deviation from this policy, must be subject to a risk assessment and approval by the Group CTO.

Any incidents which constitute a breach of this Policy or may have negative consequences for the Company's information security, shall be reported without any undue delay using the "Guidelines for incident handling and reporting". The process shall enable the external reporting of any breach of personal privacy to the applicable Data Protection Authorities within 72 hours, as prescribed by the GDPR, Article 33.