VERKKOKAUPPA.COM OYJ

RISK MANAGEMENT POLICY

The Board of Directors (the "**Board** ") of Verkkokauppa.com Oyj (the **"Company"**) has approved this Risk Management Policy (the "**Policy**") on 17 June 2025.

1 Introduction and purpose

Due to its business environment, it is very important for the Company to identify the risks and uncertainties related to its operations and to react to them at the appropriate level and with the necessary actions. The risks and uncertainties are related, but not limited to the Company's operating environment and general economic development, such as demand in the home appliance sector, the nature of the industry and the competitive situation. In addition, the Company's business operations involve risks and uncertainties, such as risks related to business strategy and investment execution, risks related to procurement and logistics, as well as risks related to information systems and other operational factors of the Company's business. Quality risks, such as information security, data protection and compliance, are comprehensively taken into account in the Company's risk management. The risks and uncertainties described above may have a negative or positive impact on the Company's business, financial position or result.

Applicable legislation and other requirements for the Company require consistent and defined risk management from us. The Company's risk management is based on the ISO 31000 standard and other well-known good practices.

The purpose of this Policy is to describe the risk management framework and process for the Company's risk management.

2 Extent

This Policy applies to the Company, all subsidiaries, and their employees.

3 Definitions

"**Risk management**" is an organization-wide, systematic process in which all types of risks are identified, evaluated, and managed in a uniform manner as part of strategic decision-making, with the goal of optimizing risk-taking in relation to business objectives and value creation.

"Risk" is the uncertainty of an event or circumstance that, if realized, will have either a positive or negative impact on the organization's goals, and is measured as a combination of its probability and consequences.

- **Strategic,** which refers to risks that lead to wrong choices or loss of opportunities.
- **Operational,** which refers to risks caused by e.g. processes not working or people failing.
- **Financial,** which refers to risks that lead to failures in capital, market or financial processes, among other things.
- **Damage, liability and safety risks**, which refer to, among other things, risks arising from the possibility of danger or damage.

The "**Risk Officer**" is the role responsible for the overall risk management of the Company. The role is held by the CIO.

A "**risk owner**" is a designated person or entity within the Company that has the authority, responsibility and resources to manage a particular risk, including its assessment, determination of actions, monitoring implementation and regular reporting as part of the risk management process.

4 Risk management process

4.1 General

Risk management is part of the Company's management system and is managed in accordance with the annual cycle. The risk management system has been built in accordance with the ISO 31000 standard. Operations in accordance with the standard drive risk management towards annual assessment and its development.

The Company's risk assessment process consists of five different stages. In the first step, before the risk assessment is carried out, the subject of the risk assessment is defined. The second, third and fourth phases include the identification, analysis and management of risks, after which the risks are reported further in accordance with the reporting principles.

4.2 Defining the operating environment

The subject of the risk assessment determines where the risk assessment is targeted, such as the entire Company, an individual department, or a departmental process.

4.3 Identifying risks

When identifying risks, the risks that may be realized or have already materialized are listed in the risk register for the target. Risks are identified by category (strategic, operational, financial, damage, safety and responsibility) and through the risk themes they contain.

4.4 Risk analysis

The identified risk is analyzed on the basis of the probability and impact of its realization. Probability and impact are assessed separately, first the probability and then the impact of the actual event. The assessment is done on a 5x5 basis.

4.5 Assessing the significance of risks

The significance of risks is assessed as the product of probability and impact. The significance of the risk determines the proposed measures related to the management of the risk.

4.6 Risk treatment

In risk treatment, a measure for risk mitigation/treatment must first be defined. Based on the results of the risk assessment, measures for the risk may include:

- No acute measures required

- Monitor the development of risk
- Create a plan to reduce risk
- Requires immediate action

If the identified risk requires action, a free-form description of the risk measures must be drawn up, a responsible person must be selected and a target schedule for possible corrective actions must be defined.

5 Roles and responsibilities

5.1 The Company's entire personnel is responsible for risk management. Risk management is part of the Company's quality, and its roles and responsibilities form a risk management organization. The roles and responsibilities of the risk management organization are divided as follows:

The Management Team / CIO is responsible for overseeing risk management and must report on its effectiveness and any identified risks to the Board.

The Risk Officer (CIO) is responsible for the operational management of risk management, the operations of the risk management and the development and supervision of risk management.

The Risk Management Steering Group is responsible for the coordination and development of risk management. The Risk Management Steering Group meets regularly to report on the state of risk management.

Directors are responsible for coordinating the risk management of their own department and for reporting risks within their department.

Managers are responsible for organizing a risk assessment workshop for their department.

The owner of a process, information or system is responsible for the risk management and reporting of the object they own.

Supervisors are responsible for informing their subordinates about the principles of risk management and guiding their subordinates' risk management work. The supervisor is obligated to report the risks identified by their subordinates.

Every employee is responsible for participating in possible risk workshops and for reporting any risks they have observed to their supervisor.

6 Additional information

Any questions regarding this Policy should be directed to the CIO.

7 Validity

This Policy has been approved by the Board on 17 June 2025 and it will enter into force on the same day.

This Policy replaces the Risk Management Policy approved by the Board on 31 March 2020.