RISK MANAGEMENT POLICY

1. Introduction

The purpose of INNA risk management is to identify the most significant risks to INNA Group of companies, which are INNA Finland, INNA Sweden and INNA Danmark (“INNA” or “INNA Group”), business operations and to manage them. Risk management is integral part of effective management practice. By appropriate risk management we aim to ensure the continuity of our operations and achievement of our business objectives.

Code of Conduct Policy is INNA´s top policy, which collects all other policies together. Different policies are described shortly in our Code of Conduct Police and made reference to each specific policy.

INNA´ s risk management policy describes the main principles of risk management at INNA. The CEO of INNA Group and each country-specific CEO of the INNA Group, together with their management team, have the overall responsibility for INNA´ s risk management. Business and support functions are responsible for the practices relating to identification, evaluation, review and management of risks in their field of business and mandate. They manage risks by defining and implementing controls. Appointed risk owners are responsible for specific identified risks within their range of responsibility.

INNA Group’s country-specific CEO’s follow the compliance of legislation and other regulatory requirements, generally acknowledged ethical principles, Code of Conduct and other Policies and internal instructions and procedures, including the risk management process in their relevant countries. Employees and stakeholders are encouraged to report any misconduct or suspected misconduct. Internal Audit performs annually audits according to audit plan and presents audit outcomes to the Audit Committee.

In addition to this Policy, INNA may have internal instructions for its employees about risk management. In case of any discrepancies between this Policy and other instructions, this Policy shall prevail.

2. Risk management process

INNA has identified key risks to its operations and maintains a risk register. Risk owners have been named in the risk register. Risk register is regularly reviewed, assessed and kept updated. INNA management team has annually separate risk review meeting. Risk management is also part of the Management system and reporting process. Between regular reviews, identified material changes are evaluated, reported and discussed separately.

Key risks have been categorized as strategic, operational, financial and damage risks in INNA´ s risk register. Strategic risks refer to such external or internal events that may have impact on company´s ability to achieve its objectives and strategic goals in short, medium or longer term, such as market conditions, organizational structure, company´s reputation and brand etc. Strategic risk may even endanger the existence of the company. Operational risks are risk of losses caused by failed processes, policies, systems or events that interrupt or disrupt business operations. Typical categories of operational risks are people risks, process risks, system risks, contract-related risks and legal & compliance risks. Financial risk is any risk associated with financing. Financial risks include market risk, credit risk, liquidity risk and operational risk. By damage risks are meant risks to people or property

Risk identification and evaluation process:

- Identification of possible risks
- Analysis of identified risks
- Evaluation and prioritization of risks (impact and likelihood)
- Key risks are listed in risk register
- Risk prevention and mitigation
- Risk register kept updated and reviewed regularly

3. Reporting concerns

If you become aware of or suspect a possible violation of law, rule, regulation or a violation of this Policy or any other of INNA's policies, you shall contact your INNA Group's country-specific CEO, Head of business unit or closest supervisor.

You can also raise concerns through INNA's whistleblowing system, available in country specific web pages. INNA will not tolerate any attempt to take adverse action against an employee for reporting a genuine concern regarding suspected wrongdoings. Retaliation against anyone who speaks up is a violation of the Code of Conduct and will not be tolerated.

INNA does not tolerate any illegal or unethical behaviour. Violations of this Policy is likely to damage INNA's brand and reputation. Failure to follow this Policy is taken seriously and may result in disciplinary action appropriate to the violation, including, but not limited to, termination of employment.

4. Review and follow-up

Compliance with this Risk Management Policy by all INNA entities and employees is monitored and reviewed on an ongoing basis, as appropriate. Any relevant matters identified are followed up internally.

Effective date	Version	Change description
October 2021	v1	original
20 December 2023	v2	updated
2026	v3	updated