Risk management policy

1. Purpose

The purpose of this Risk Management Policy is to establish a systematic and consistent approach to identifying, assessing, controlling, monitoring and reviewing risks that could affect the company's employees, operations, customers, products, assets, environment, financial performance and reputation.

The company recognises that effective risk management is an integral part of responsible business management and is essential to maintaining safe, reliable and sustainable manufacturing operations.

This policy applies to all activities associated with the manufacture, assembly, inspection, storage and delivery of steel products.

2. Scope

This policy applies to:

- All employees, contractors and temporary workers.
- Manufacturing and fabrication activities.
- Welding, cutting, grinding and other hot-work operations.
- Steel handling, lifting, storage and transportation.
- Machinery, tooling and production equipment.
- Product design, engineering and specification.
- Purchasing and supply-chain activities.
- Quality control and product inspection.
- Maintenance and facilities.
- Environmental management.
- Occupational health and safety.
- Information technology and cybersecurity.
- Financial and commercial activities.
- Legal and regulatory compliance.
- Business continuity and emergency response.
- Customer, supplier and contractor relationships.

3. Risk Management Principles

The company shall manage risk according to the following principles:

1. Risk management is everyone's responsibility.
2. Risks shall be identified proactively wherever reasonably practicable.
3. Risks shall be assessed using a consistent and documented methodology.
4. Significant risks shall have defined controls, responsible persons and review dates.
5. Risk controls shall follow the principle of eliminating or reducing risk at source wherever reasonably practicable.
6. Legal, regulatory, contractual and customer requirements shall be considered when assessing risk.

7. The company shall seek to prevent incidents rather than relying solely on corrective action after an incident occurs.
8. Risk assessments shall consider both the likelihood and potential consequence of an event.
9. Changes to processes, equipment, materials, personnel or suppliers shall be assessed for their potential impact on risk.
10. Risk information shall be communicated to relevant employees and other affected parties.
11. Risk management shall support continual improvement of the company's operations.

4. Risk Categories

The company shall consider, as applicable, the following categories of risk.

4.1 Health and Safety Risk

Examples include:

- Lifting and handling of heavy steel components.
- Cranes, lifting equipment and forklifts.
- Cutting, grinding and drilling.
- Welding and hot work.
- Fire and explosion.
- Electrical hazards.
- Machinery and moving equipment.
- Working at height.
- Noise and vibration.
- Radiation exposure.
- Exposure to welding fumes, dust and chemicals.
- Slips, trips and falls.
- Contractor activities.
- Emergency situations.

4.2 Manufacturing and Operational Risk

Examples include:

- Equipment breakdown.
- Production interruption.
- Incorrect production parameters.
- Material shortages.
- Capacity constraints.
- Manufacturing defects.
- Failure of critical machinery.
- Loss of utilities.
- Inadequate maintenance.
- Production scheduling failures.
- Damage to work-in-progress or finished products.

4.3 Quality Risk

Examples include:

- Incorrect material specification.
- Incorrect dimensions or tolerances.
- Welding defects.
- Inadequate inspection.
- Incorrect documentation.
- Non-conforming products.
- Customer complaints.
- Product failure in service.
- Failure to meet applicable standards or customer specifications.

Where applicable, welding and fabrication risks shall consider relevant standards and customer requirements, including requirements relating to qualified personnel, welding procedures, inspection and traceability.

4.4 Supply-Chain Risk

The company shall assess risks associated with:

- Steel and raw-material availability.
- Supplier financial stability.
- Supplier quality.
- Long lead times.
- Transportation disruption.
- Single-source suppliers.
- Geopolitical disruption.
- Energy and commodity price fluctuations.
- Supplier compliance.
- Subcontractors and external processors.

Critical suppliers shall be identified and monitored according to their importance to the company's operations.

4.5 Environmental Risk

Environmental risks may include:

- Steel and material waste.
- Welding and grinding emissions.
- Paint and coating emissions.
- VOC emissions.
- Hazardous substances.
- Waste disposal.
- Oil and chemical spills.
- Energy consumption.
- Water consumption.
- Noise.
- Air emissions.
- Contamination of soil or water.
- Environmental permit and regulatory requirements.

The company shall seek to prevent pollution and minimise environmental impacts arising from its activities.

4.6 Financial and Commercial Risk

Financial and commercial risks may include:

- Customer credit risk.
- Cash-flow problems.
- Currency fluctuations.
- Steel price fluctuations.
- Energy price increases.
- Unexpected production costs.
- Contractual penalties.
- Warranty claims.
- Major customer dependency.
- Insurance limitations.
- Fraud and financial misconduct.

4.7 Legal and Compliance Risk

The company shall identify and manage risks associated with:

- Applicable laws and regulations.
- Occupational health and safety requirements.
- Environmental legislation.
- Product requirements.
- Employment legislation.
- Export and import controls.
- Customs requirements.
- Tax requirements.
- Anti-bribery and anti-corruption requirements.
- Contractual obligations.
- Customer-specific requirements.

4.8 Information Security and Cybersecurity Risk

The company shall consider risks relating to:

- Loss of company data.
- Cyberattacks.
- Ransomware.
- Unauthorised access.
- Loss of production systems.
- Compromise of customer information.
- Intellectual property theft.
- Email fraud and phishing.
- Loss of backups.
- IT system failure.

Appropriate technical, organisational and physical controls shall be implemented according to the level of risk.

4.9 Business Continuity Risk

The company shall identify events that could significantly interrupt operations, including:

- Fire.
- Flood.
- Major equipment failure.
- Loss of electricity or utilities.
- Cyberattack.
- Major supplier failure.
- Loss of critical personnel.
- Serious workplace incident.
- Natural disaster.
- Transportation disruption.
- Significant quality incident.

Business continuity and emergency arrangements shall be established for significant risks where appropriate.

5. Risk Assessment Methodology

Risks shall be assessed using a **5 × 5 risk matrix** based on:

- Likelihood and of occurrence;
- Severity of consequence.

Score	Likelihood	Description
1	Rare	Very unlikely to occur
2	Unlikely	Could occur but not expected
3	Possible	Could occur occasionally
4	Likely	Expected to occur periodically
5	Almost Certain	Expected to occur frequently

Score	Severity	Description
1	Insignificant	Minimal impact; no significant injury, loss or disruption
2	Minor	Minor injury, loss, quality issue or disruption
3	Moderate	Significant injury, financial loss, environmental impact or operational disruption
4	Major	Serious injury, major financial loss, significant environmental or operational impact
5	Catastrophic	Fatality, major environmental incident, substantial financial loss or prolonged business interruption

Score	Risk Level	Required Action
1–4	Low	Manage through normal procedures and monitor
15–9	Medium	Additional controls should be considered
10–16	High	Action required; management oversight
17-25	Critical	Immediate action required; activity may need to stop until adequately controlled

The company's risk register shall record both the **initial risk** and the **residual risk** remaining after controls have been implemented.

6. Risk Controls

Risk controls shall be selected according to the following general hierarchy:

1. Eliminate the hazard or risk.
2. Substitute with a lower-risk alternative.
3. Apply engineering controls.
4. Apply administrative controls and procedures.
5. Provide appropriate personal protective equipment.

The company shall not rely solely on personal protective equipment where higher-level controls are reasonably practicable.

Examples of controls within steel manufacturing may include:

- Machine guarding.
- Interlocks and emergency stops.
- Crane and lifting inspections.
- Certified lifting accessories.
- Preventive maintenance.
- Welding fume extraction.
- Local exhaust ventilation.
- Fire prevention systems.
- Material handling procedures.
- Safe storage of steel.
- Operator training.
- Permit-to-work systems.
- Welding procedures and qualifications.
- Inspection and testing.
- Supplier approval.
- Product traceability.
- Emergency response procedures.

7. Risk Register

Significant risks shall be recorded in a controlled **Risk Register.**

- Risk identification number.
- Department/process.
- Risk description.
- Potential cause.
- Potential consequence.
- Existing controls.
- Likelihood.
- Severity.
- Initial risk rating.
- Additional controls/actions.
- Responsible person.
- Target completion date.
- Residual likelihood.
- Residual severity.
- Residual risk rating.
- Evidence/records.
- Review date.
- Status.

Critical and high risks shall receive priority for corrective or preventive action.

8. Responsibilities

Managing Director

The Managing Director shall:

- Approve this policy.
- Ensure appropriate resources are available for risk management.
- Review significant organisational risks.
- Ensure that critical risks receive appropriate management attention.

Management Team

Managers shall:

- Identify risks within their areas of responsibility.
- Ensure appropriate risk assessments are completed.
- Implement and maintain controls.
- Allocate responsible persons and target dates.
- Monitor risk-reduction actions.
- Escalate significant risks to senior management.

Health, Safety and Environmental / Quality Personnel

Where applicable, designated personnel shall:

- Coordinate risk assessments.
- Maintain the risk register.
- Provide guidance on risk assessment methodology.
- Monitor regulatory and operational requirements.
- Review incidents and near misses.
- Report significant risks to management.

Employees

Employees shall:

- Follow established procedures and controls.
- Use machinery and equipment correctly.
- Wear required PPE.
- Report hazards, incidents, near misses and unsafe conditions.
- Participate in risk assessments where appropriate.
- Not deliberately bypass safety or risk controls.

Contractors

Contractors shall comply with applicable company requirements and shall provide relevant risk assessments and method statements where required.

9. Change Management

Risk assessments shall be reviewed before significant changes are introduced, including:

- New machinery.
- New production processes.
- New materials or chemicals.
- Changes to product design.
- Changes to factory layout.
- Significant changes in staffing.
- New suppliers or subcontractors.
- Changes in legislation.
- Major IT or production-system changes.

Changes shall not be implemented without appropriate consideration of their potential risks.

10. Incident and Near-Miss Management

The company shall investigate significant:

- Accidents.
- Injuries.
- Near misses.
- Environmental incidents.
- Product failures.
- Quality non-conformities.
- Equipment failures.
- Security incidents.
- Customer complaints.

Investigations shall seek to identify underlying causes and opportunities for improvement rather than simply assigning blame.

Corrective and preventive actions shall be documented and monitored to completion.

11. Risk Monitoring and Review

Risk assessments shall be reviewed:

- At planned intervals.
- Following significant incidents or near misses.
- Following significant changes.
- When new hazards or risks are identified.
- When legal or regulatory requirements change.
- When existing controls are found to be ineffective.
- When significant changes occur within the business.

Critical and high risks shall be reviewed more frequently than lower-level risks.

12. Training and Awareness

Employees shall receive appropriate information and training concerning risks relevant to their work.

Training may include:

- Safe operation of machinery.
- Crane and lifting operations.
- Welding and hot work.
- Chemical handling.
- Fire prevention.
- Emergency response.
- PPE.
- Manual handling.
- Environmental responsibilities.
- Quality requirements.
- Cybersecurity awareness.
- Reporting of hazards and incidents.

Training records shall be maintained.

13. Risk Acceptance and Escalation

Risks shall only be accepted at a level appropriate to the company's circumstances and applicable legal requirements.

Critical risks shall not be accepted without explicit management review and documented justification.

Where a risk cannot be adequately controlled, the company shall consider stopping, modifying or postponing the affected activity until suitable controls are implemented.

14. Records

The company shall retain appropriate records relating to risk management, including:

- Risk assessments.
- Risk registers.
- Action plans.
- Inspection records.
- Maintenance records.
- Training records.
- Incident and near-miss reports.
- Audit reports.
- Emergency exercises.
- Supplier assessments.
- Compliance assessments.
- Management review records.

Records shall be maintained in accordance with the company's document-control and record-retention requirements.

15. Continual Improvement

The company is committed to continually improving its approach to risk management.

Information from incidents, near misses, audits, inspections, customer feedback, changes in legislation, management reviews and operational experience shall be used to improve risk controls and business performance.

16. Policy Approval

This policy has been approved by senior management and shall be communicated to all relevant employees and other interested parties.

Frantisek Plachy
Managing Director
SEA Enterprises a.s.

1 October 2026

1026-01