Risk Management and Crisis Communication Protocol

Purpose:

To ensure the smooth global operations of the SlavkaSk nonprofit organization, a unified and pre-defined risk management and crisis communication system is essential. The purpose of this protocol is to enable rapid response, ensure transparent information flow, and protect the safety of all stakeholders.

1. Risk Categories

Risks are classified into three main categories:

1.1 Technical Risks:

- Equipment failure, explosions, leaks
- Technological malfunctions, filtration errors
- Shutdowns of electrical or heating systems

1.2 Natural and External Risks:

- Floods, earthquakes, storms, extreme temperatures
- Political or governmental intervention, protests

1.3 Human and Organizational Risks:

- Human error, rule violations, negligence
- Internal data theft, communication breakdowns
- Reputational or trust-related crises

2. Risk Assessment and Prevention

2.1 Risk Matrix:

Each site must prepare a risk matrix quarterly, including:

- The endangered area
- The likelihood of occurrence
- The severity of the risk
- Recommended preventive measures

2.2 Preventive Inspections:

- Monthly technical audits
- Annual fire and accident drill (at least once a year)
- Annual emergency response training for all employees

3. Crisis Procedure

3.1 Crisis Team Appointment:
Each facility must have a designated crisis coordinator and deputy who maintain continuous contact with headquarters.

3.2 Immediate Actions:

- Securing the area and ensuring employee safety
- Shutting down mechanical and electrical systems
- Notifying local authorities and the central office within 1 hour

3.3 Documentation:

- Creating an official incident report
- Photo documentation and witness statements
- Sending a full report to SlavkaSk headquarters within 24 hours

4. Crisis Communication

4.1 Internal Communication:

- Employees are informed via official channels by the crisis team
- Communication must be calm, factual, and controlled to prevent panic

4.2 External Communication:

- Only the central office may issue public statements or communicate via social media
- Local sites are not authorized to release official information

4.3 Client and Partner Notification:

- Partners will be informed in writing within 48 hours, depending on the severity of the incident
- A dedicated communication plan will be developed to restore trust

5. Post-Crisis Risk Management

- After each crisis, a full analysis is conducted and lessons learned are integrated into future procedures
- The protocol is updated annually based on new experiences

Regulation Issued By:
Ignác Czakó, President of the SlavkaSk International Nonprofit Organization