Standard Operating Procedure (SOP): Threat Assessment and Risk Mitigation Procedures

This SOP details **threat assessment and risk mitigation procedures**, encompassing the identification, evaluation, and prioritization of potential threats, the implementation of strategies to reduce risks, continuous monitoring and review of risk factors, and response planning to enhance organizational security and resilience. The goal is to proactively protect assets, personnel, and operations by effectively managing and mitigating risks.

1. Purpose

To establish systematic procedures for identifying, assessing, mitigating, and monitoring threats to organizational assets, personnel, and operations.

2. Scope

This SOP applies to all departments, employees, and contractors involved in security, risk management, and operational continuity.

3. Definitions

Term	Definition
Threat	A potential event or action that could cause harm or loss to the organization.
Risk	The combination of the likelihood of a threat occurring and the potential impact.
Mitigation	Strategies or actions taken to reduce the probability or impact of risks.
Asset	Anything of value to the organization, including people, information, infrastructure, and reputation.

4. Procedures

4.1 Threat Identification

- Collect information on potential internal and external threats (e.g., natural disasters, cybersecurity, physical intrusions).
- Consult incident reports, risk registers, and conduct interviews with stakeholders.
- Maintain a current list of identified threats.

4.2 Threat Assessment & Risk Analysis

- Evaluate identified threats based on likelihood and potential impact.
- Use risk matrices or qualitative/quantitative methods to rate threats.
- Document findings and assign risk levels (e.g., Low, Medium, High).

4.3 Risk Prioritization

- Rank risks according to their assessed levels.
- Focus mitigation efforts on the highest priority risks.
- Allocate resources proportionally to risk severity.

4.4 Risk Mitigation Strategies

- Develop and implement controls to address prioritized risks (e.g., training, technical safeguards, physical security measures).
- Assign ownership of mitigation actions to relevant team members.
- Document all mitigation actions in the risk register.

4.5 Continuous Monitoring and Review

- Regularly review and update the risk register and threat profile.
- Monitor the effectiveness of implemented controls and update as needed.
- Conduct periodic audits and drills to ensure preparedness.

4.6 Response Planning

- Develop response plans for prioritized threats, including communication protocols and escalation procedures.
- Ensure contingency plans are tested and updated regularly.
- Assign roles and responsibilities for crisis response.

5. Roles and Responsibilities

Role	Responsibility
Risk Manager	Coordinate risk assessment and mitigation activities; maintain risk documentation.
Department Heads	Identify departmental risks and implement mitigation measures.
Employees	Report observed threats; participate in training and mitigation procedures.
Security Team	Monitor security controls and respond to incidents.

6. Documentation and Recordkeeping

- Maintain records of risk assessments, mitigation actions, and incident responses.
- Ensure documentation is reviewed and updated at least annually or after significant incidents.

7. Review and Continuous Improvement

- Review this SOP annually or as needed based on organizational changes or after major incidents.
- Solicit feedback and incorporate lessons learned to improve procedures.