Standard Operating Procedure (SOP) for Corporates to Secure Assets in the Event of War with Pakistan

Document Title: SOP for Asset Security in Times of Conflict

Effective Date: Thursday, 1st May 2025

Prepared by: Central Association of Private Security Industry (CAPSI)

1. Purpose

The purpose of this SOP is to outline the steps and measures corporates should undertake to secure assets and ensure business continuity during a potential conflict situation, particularly in the event of war with Pakistan. The safety of employees, facilities, and corporate assets is paramount.

2. Scope

This SOP applies to all employees, contractors, and stakeholders within your Organisation, and is relevant for all corporate facilities and assets located in regions that may be affected by such a conflict.

3. Responsibilities

- **Crisis Management Team:**
  Responsible for oversight and implementation of this SOP, ensuring proper communication and resource allocation.
- **Facility Security Team:**
  Ensures physical security measures are in place and operational.
- **Human Resources:**
  Communicates safety protocols to employees and manages evacuation plans.
- **IT Department:**
  Secures digital assets and ensures data backup and integrity.
- **Public Relations:** Handles external communication and maintains the company's reputation during crises.

4. Pre-War Preparations

a. **Risk Assessment:**
- Conduct a comprehensive risk assessment to identify vulnerabilities in all corporate assets.

b. **Emergency Response Plan:**
- Develop and maintain an emergency response plan tailored to potential war scenarios, including evacuation routes, shelter locations, and communication protocols.

c. **Asset Inventory:**
- Create and regularly update a complete inventory of all critical assets, including physical documents, equipment, and digital data.

d. **Security Measures:**
- Enhance physical security through barriers, surveillance systems, and access control measures.
- Engage with local law enforcement and security agencies for collaborative strategies.

e. Employee Training:
- Regularly conduct training sessions for employees on emergency protocols, including evacuation procedures and personal safety measures.

5. During Conflict

a. Situation Monitoring:
- Continuously monitor news and government advisories for updates on the conflict situation.

b. Communication Protocol:
- Maintain open lines of communication with employees, providing timely updates and instructions.
- Use multiple channels (e.g., emails, messaging apps) to ensure messages reach all employees.

c. Asset Protection:
- Implement heightened security measures based on the severity of conflict.
- Relocate critical assets if deemed necessary and feasible.

d. Employee Safety:
- Activate the emergency response plan, ensuring employee safety is the top priority.
- Facilitate immediate evacuation if necessary and provide necessary support for employees and their families.

6. Post-Conflict Review

a. Damage Assessment:
- Conduct a thorough assessment of any damages to corporate assets and facilities.

b. Crisis Evaluation:
- After the conflict has subsided, hold a debriefing session with the Crisis Management Team to evaluate the effectiveness of the implemented SOP.
- Identify lessons learned and areas for improvement.

c. Recovery Plan:
- Develop and implement a recovery plan to restore operations and assets to pre-conflict status.

7. Documentation and Reporting

All actions taken during a conflict must be documented, including communication records, asset assessments, and recovery efforts. This data will be crucial for future planning and compliance.

8. Conclusion

Effective asset security during a potential war requires proactive planning, ongoing communication, and strategic responsiveness. This SOP serves as a foundational guide to help your organization to protect its interests and ensure the safety of its employees.

Kunwar Vikram Singh
Chairman
Central Association of Private Security Industry
www.capsi.in