CORPORATE SECURITY AND CONTINGENCY POLICY

Version 2

It is the policy of the company to provide a secure working environment by addressing security threats, establishing and maintaining the relevant security measures to protect personnel and assets. The company is prepared with contingency plans to cope effectively with whatever major incident or disaster occurs.

In the event of an attack on a ship, terminal, office or a highjack attempt, the preservation of the lives of personnel, subcontractors or visitors is to be placed above all other considerations.

The company is committed to

- Risk assessment shall be conducted annually to identify potential threats and the necessary preventive measures to be implemented.
- Security & Contingency plans for each ship, terminal and shore-based office including procedures and practices are established, classified in accordance to sensitivity of content and maintained.
- At all shore-based office locations Manager Overseas Office or the General Manager are appointed as responsible persons for security & contingency issues.
- Company Security Officer (CSO) is appointed, trained and informed to personnel.
- Ship Security Officer (SSO) for each ship and Port Facility Security Officer (PFSO) at each terminal are appointed, trained and informed to personnel.
- Regular security & contingency training, drills and exercises are conducted.
- Corporate Travel policy is in place to minimize security threats to personnel.
- Corporate IT Security Policy defines security standards and practices for the protection of IT systems and information stored within them, against accidental or malicious modification, destruction, disclosure or unauthorized access.
- Odfjell has a 3-level emergency response organization with Emergency Response Teams on 1st operational level, Emergency Response Management Teams on the 2nd tactical level and a Corporate Contingency Council on the 3rd strategic level.
- Emergency Response Management Team's (ERMT's) and a Corporate Contingency Council (CCC) to support the ERMT's are established and maintained.

This policy will be reviewed and improved if needed based on the annual risk assessment.

We comply with international standards like the "International Ship & Port Facility Security Code" (ISPS) to reduce exposure to terrorism, piracy, cybercrime and other criminal acts.

The company expects its employees to take a leading role in the protection of lives and property from any unlawful acts, however employees should not act as law enforcement entities, nor are they asked to exercise police powers.

Harald Fotland, CEO