TMSA 3 (개정일자:2017.04.10 / 시행일자:2018.01.01.)

□ Element 13 Maritime Security(해상보안)

1. 목적

1) 보안 관리를 위한 적극적인 대응을 통한 안전한 작업 환경 제공

2) 보안 위험의 최소화 및 보안 위험의 결과로 나타날 수 있는 회사, 직원, 자산 손실 최소화

2. 보안 관리

회사는 유동적인 해상 보안 상황에 대응하기 위해 모니터링, 변화관리 등에 대한 시스템을 보유하여야 함

1) 회사 모든 업무를 커버하는 보안 계획

2) 회사 모든 업무의 보안 위협을 식별할 수 있는 절차

3) 식별된 위협을 완화, 대응하기 위한 대책 보유

4) 보안 관련 정보에 대한 관리 및 검토

5) 실제 사고 및 잠재적 위협에 대한 보고 절차

6) 업무 담당자의 적절한 교육 이수

7) 사이버 보안 관련 위험 식별을 포함한 절차 보유

- 적절한 지침, 완화 조치, 절차 인지(이해)를 위한 회사의 적극적 증진 활동

8) 직원의 업무 출장 등에 대한 traveling 보안 위협 최소화 방침 보유

9) 회사 보안 절차는 산업계 최신 지침에 따라 정기적으로 최신화 되어야 함

10) 내부심사시 보안관리 항목 포함

11) 보안 대응의 상태 점검을 위한 평가 및 훈련 시행

12) 식별된 위협의 적절한 대응을 위한 독립적인 전문가 제공 요구

13) 선박에 강화된 보안 및 모니터링 장비 제공

14) 선박 수리 및 신조시 선박 보안 강화를 위한 사항 고려

15) 혁신적인 보안 기술에 대한 적절한 점검 및 사용

3. 사이버 보안 관련 요구사항(Element 13 Maritime Security 내용 중)

No.	KPI	BP
13.1.2	회사는 선박이 항행하는 구역 및 회사 사무실에 적용되는 보안 위협을 식별하는 절차가 있다.	①보안 위협은 아래 사항을 포함한다. -좀도둑질(Petty theft) -기물파손(vandalism) -밀항자 -화물 절도 -사이버 위협 -불충분한 항만 보안 -인신매매, 무기 또는 마약 밀매 -밀수 -해적질 -파괴행위 및 방화(Sabotage and arson) -테러 및 그 테러의 후속영향 ②식별된 위협은 환경 변화에 따라 필요시, 검토된다

13.2.3	사이버 보안을 포함하고 있는 방침 및 절차를 통해 적절한 지침 및 경감 조치가 제공된다.	①IT 시스템에 대한 보안 위험을 아래를 포함한다. -의도적이고 승인되지 않은 위반 -의도되지 않고 돌발적인 위반 -불충분한 시스템의 완전성, (예, firewalls and/or virus protection.) ②시스템의 직간접적 커뮤니케이션 링크들 중 외부 위협이나 부적절한 사용에 취약한 부분을 식별한다. ③이것은 항해, 엔지니어링, 콘트롤 및 커뮤니케이션 시스템을 포함한다. ④회사가 절차서를 개발할 때는 현 업계의 관련 지침을 참조한다.
13.2.4	회사는 적극적으로 사이버 보안 인식을 증진시킨다.	①효과적인 수단을 통해 육상, 선박 및 계약자들의 책임감 있는 행동이 장려된다. ②그러한 행동은 아래 사항을 포함한다. -사람이 없는 작업 장소는 자물쇠로 잠금 -암호 보호 -승인받지 않은 소프트웨어 사용 금지 -소셜미디어의 책임감 있는 사용 -이동식 하드웨어 및 메모리스틱의 잘못된 사용을 관리 및 예방
13.3.2	보안 절차는 현행 지침을 고려하여 업데이트 된다.	업계 지침은 아래를 포함한다. ▸Guidelines on cyber security from industry and Class.
13.4.5	회사는 혁신적인 보안 기술 및 시스템을 테스트하고 회사에 시행하는데 참여하고 있다.	①이것은 아래 사항을 포함한다. -보안 개선을 위한 물리적인 조치 -IT 시스템에 대한 소프트웨어 강화

RIGHTSHIP 검사 점검표(개정/시행일자:2017.05.11.)

□ 4.7 사이버보안

No.	점검 항목
4.7.1.	선박 및/또는 회사는 문서화된 소프트웨어/펌웨이 및 하드웨어 유지 관리 절차를 가지고 있는가?
4.7.1.1	관련 서비스 레포트를 보유하고 있는가?
4.7.2	선박 및/또는 회사는 사이버 보안 절차가 있는가?
4.7.2.1	사이버 공격에 대한 위험성 평가가 완료되었는가?
4.7.2.2	사이버 공격 대응 계획이 준비되어 있는가?
4.7.3	선박 및/또는 회사가 사이버 보안 교육을 제공하는가?