2018

해상 사이버보안 관리 시스템 지침

GC-24-K

한 국 선 급

“해상 사이버보안 관리 시스템 지침”의 적용

1. 별도로 명시하지 않는 한, 이 지침은 2018년 3월 2일 이후 해상 사이버보안 관리 시스템에 대하여 인증을 받고자 검사 신청하는 회사 및 선박에 적용한다.

차 례

제 1 장 일반사항

제 1 절 일반사항

101. 적용

1. 이 지침은 정보기술(IT)이나 운영기술(OT)을 운용하며 사이버보안 관리 시스템을 갖춘 회사 또는 선박에 적용한다.
2. 이 지침은 사이버보안 관리 시스템의 수준 및 그 수준에 해당하는 요건을 규정하며 적용하고자 하는 범위는 선주의 요청에 의해 결정된다.
3. 이 지침에서 규정하지 아니하는 사항은 **선급 및 강선규칙**의 각 해당 요건에 따른다. 다만, 사이버보안 관리 시스템에 적용할 수 없는 요건은 제외한다.
4. 이 지침에 포함되지 않은 사항에 대하여는 우리 선급이 적절하다고 인정하는 바에 따라 ISO, IEC 또는 이와 동등 이상의 인정된 기준에 따를 수 있다.
5. 본 지침의 규정 이외에 IMO 등 국제 규정에 따른 별도 요건이 있거나 정보기술 및 운영기술의 발전에 따라 우리 선급이 필요하다고 인정되는 경우 추가적인 고려사항 및 요건이 요구될 수도 있다.
6. 이 지침은 회사나 선박의 사이버보안 관리 시스템에 대한 최소한의 요건을 명시하고 있으며, 모든 사이버보안 사고를 방지하는 것을 의미하는 것은 아니다.

102. 용어의 정의

용어의 정의는 여기에 별도로 정하는 경우를 제외하고는 **선급 및 강선규칙**에 따른다.

1. **"사이버보안(Cybersecurity)"**이라 함은 조직의 자산과 그에 포함된 정보의 기밀성, 무결성, 가용성을 보장하기 위한 활동 또는 프로세스, 역량 등을 말한다.
2. **"사이버보안 관리 시스템(Cybersecurity Management System)"**이라 함은 사이버보안 리스크 평가를 기반으로 조직의 자산에 대하여 조직에서 요구하는 수준의 사이버보안을 유지하기 위한 종합적 관리체계를 말한다.
3. **"정보 기술(Information Technology)"**이라 함은 데이터 또는 정보의 자동 수집, 저장, 조작, 관리, 이동, 제어, 디스플레이, 스위칭, 교환, 전송 또는 수신에 사용되는 장비, 상호 연결된 시스템 또는 장비의 하위 시스템을 말한다.
4. **"운영 기술(Operating Technology)"**이라 함은 내장된 시스템을 모니터링하고 제어하는 장치, 센서, 소프트웨어 및 관련 네트워킹을 말한다.
5. **"사이버보안 사고(Cybersecurity Incident)"**라 함은 외부 또는 내부의 악의적인 사용자에 의한 비인가된 시스템 사용, 사용자 계정 도용, 악성코드 유입 및 실행, 사이버보안 시스템 방해 등 회사나 선박 시스템의 서비스를 왜곡 또는 지연시키거나 시스템을 파괴, 데이터를 변조, 삭제하는 등의 행위를 말한다.
6. **"기밀성(Confidentiality)"**이라 함은 자산이 인가된 당사자에 의해서만 접근하는 것을 보장하는 것을 말한다.
7. **"무결성(Integrity)"**이라 함은 자산이 인가된 당사자에 의해서 인가된 방법으로만 변경 가능한 것을 말한다. 이는 자산의 완전성과 정확성을 보장하는 것을 의미한다.
8. **"가용성(Availability)"**이라 함은 자산이 적절한 시간에 인가된 당사자에게 접근 가능하여야 하는 것을 말한다.
9. **"역량(Capability)"**이라 함은 특정 행위를 수행할 수 있는 능력을 말한다.
10. **"정책(Policy)"**이라 함은 최고 경영층에서 공식적으로 언급하는 목표 및 방침과 관련한 회사의 전체적인 의도 및 방향을 말한다.
11. **"리스크(Risk)"**라 함은 예상되는 위협이 발생할 수 있는 가능성과 그러한 위협이 야기할 수 있는 손실의 기대치를 말한다.
12. **"선주(Ship Owner)"**라 함은 선박소유자, 선박임차인, 선박소유자의 대리인 또는 선박임차인의 대리인 및 선장을 말한다.
13. **"결함(Deficiency)"**이라 함은 사이버보안 관리 시스템 관련 요건을 충족하고 있지 못하다는 것이 객관적인 증거에 의하여 관찰된 사항을 말한다.
14. **"주요 변경 사항(Major Change)"**이라 함은 사이버보안 관리 시스템과 연관된 주요 문서와 자산의 변경 또는 중대한 사이버위협이 식별된 경우를 말한다.
15. **"변경 관리(Change Management)"**는 하드웨어와 소프트웨어의 신규 설치, 펌웨어 업데이트, 패치 등으로 인

한 형상이 변경된 것을 말한다.

103. 선급부호

1. 이 지침의 요건을 만족하는 사이버보안 관리 시스템을 갖춘 선박에는 추가 특기사항으로서 다음과 같이 선급부호를 부여할 수 있다.
   (1) **CSMS1(Cybersecurity Management System Level 1)**은 **3장 2절**의 요건을 만족하는 기본적인 사이버보안 관리 시스템을 갖춘 선박을 의미한다.
   (2) **CSMS2(Cybersecurity Management System Level 2)**는 CSMS1의 요건에 추가하여 **3장 3절**의 검사항목을 만족하는 강화된 사이버보안 관리 시스템을 갖춘 선박을 의미한다.
   (3) **CSMS3(Cybersecurity Management System Level 3)**은 CSMS2의 요건에 추가하여 **3장 4절**의 검사항목을 만족하는 고도의 사이버보안 관리 시스템을 갖춘 선박을 말한다.
2. 사이버보안 관리 시스템을 인증 받은 회사의 선박에 대하여 CSMS 부호에 추가 부호가 부여된다. 선급부호는 CSMS1(C), CSMS2(C) 또는 CSMS3(C)로 표시된다.

104. 동등효력

이 지침에 규정되어 있지 아니한 특수한 설비가 이 지침의 규정에 적합한 것과 동등 이상의 성능이 있다고 우리 선급이 인정하는 경우에는 이 지침의 규정에 적합한 것으로 본다.

105. 제외사항

1. 우리 선급은 사이버보안 관리 시스템에 대하여 이 지침에 명시되지 않은 기타 기술적인 특성에 대하여는 책임을 지지 아니한다. 다만, 위의 사항에 대하여 문의가 있을 때는 자문에 응할 수 있다. ⚓

제 2 장 선급검사

제 1 절 일반사항

101. 일반사항

1. 적용

사이버보안 관리 시스템에 대한 선급검사는 특별히 이 장에서 규정한 것 외에는 **선급 및 강선규칙 1편**의 규정에 따른다. 또한, ISM Code 및 ISPS Code의 관련 요건의 관련 요건을 만족하여야 한다.

2. 검사의 종류

검사의 종류는 다음과 같다.

(1) 최초 인증을 위한 검사(이하, 최초검사라 한다.)

(2) 인증을 유지하기 위한 검사의 종류는 다음과 같다.

(가) 연차검사

(나) 정기검사

(다) 임시검사

3. 검사의 시기

검사의 시기는 다음의 규정에 따른다.

(1) 회사 및 선박에 대한 최초검사는 최초 인증 신청이 있을 때 시행한다.

(2) 인증을 유지하기 위한 검사는 다음의 시기에 시행한다.

(가) 연차검사는 **선급 및 강선규칙 1편 2장 201.**에서 규정하는 시기에 시행한다.

(나) 정기검사는 **선급 및 강선규칙 1편 2장 401.**에서 규정하는 시기에 시행한다.

(다) 임시검사는 **401. 3**항에서 규정하는 시기에 시행한다.

4. 선주의 의무

(1) 우리 선급으로부터 인증을 받은 회사 및 선박에 대하여 인증된 사이버보안 관리 시스템에 영향을 미치는 변경 사항이 발생한 경우에는 지체 없이 우리 선급에 통보하여야 한다.

(2) 사이버보안 관리 시스템 관련 문서는 항상 최신화 되어야 하며, 선급검사 시 이를 확인할 수 있어야 한다.

제 2 절 회사 최초검사

201. 일반사항

1. 우리 선급으로부터 회사의 사이버보안 관리 시스템에 대하여 최초검사를 받고자 하는 회사의 경우 사이버보안 관리시스템을 3개월 이상 이행한 후 직접 우리 선급에 검사신청을 하여야 한다.
2. 회사 내 사이버보안 관리 시스템 검사 대상 설비 또는 장비는 이 지침의 검사 요건에 따라서 검사하여야 한다.

202. 문서검토

1. CSMS1에 해당하는 인증을 받고자 하는 회사는 우리 선급에 검토용으로 아래의 자료 각 2부를 제출하여야 한다.

(1) 외부 협력조직 명단 및 연락망

(2) 회사 사이버보안 정책

(3) 사이버보안 조직도 및 보안인력 직무기술서

(4) 사이버보안 교육 결과 보고서

(5) 사이버보안 위협 목록

(6) 사이버보안 리스크 관리 계획서

(7) 사이버보안 관련 자산 취약성 진단 결과

(8) 사이버보안 리스크 평가 보고서

(9) 개선조치 계획 및 결과

(10) 자산 및 장비 목록과 각 자산에 대한 담당자 현황
(11) 데이터 중요도 분류표
(12) 접근권한 관리 정책
(13) 물리보안 정책
(14) 사고대응 및 복구 정책
(15) 사고대응 팀 조직도 및 비상연락망
(16) 침해사고 조사 분석 절차서
(17) 외부자 보안 정책 / 외부자 사업 계약서
(18) 소프트웨어 도입 절차
(19) 패치 작업/승인 내역서
(20) 원격접속 보안 정책
(21) 암호화 기준
(22) 네트워크 구축 계약서 / 구축 수행계획서 / 네트워크 구성도
(23) 변경관리 절차 및 변경신청서
(24) 사이버보안 관리 시스템 수준별 적용성 검토서
(25) 정보기술 시스템에 대한 사이버보안 기능에 대한 시험 보고서
(26) 데이터 백업 및 복구 기준
(27) 기능 요구사항 / 명세서

2. CSMS2에 해당하는 인증을 받고자 하는 회사는 202. 1항에 추가하여 우리 선급에 검토용으로 아래의 자료 각 2부를 제출하여야 한다.
(1) 정책 제개정 승인 내역서
(2) 회사 사이버보안 지침 및 매뉴얼
(3) 사이버보안 교육 계획서
(4) 사고 기준 분류표
(5) 침해사고 조사 분석 인력조직도
(6) 재해복구 계획서 / 범위정의서
(7) 개발보안 요구사항
(8) 침투테스트 결과 보고 내역
(9) 이상 징후 모니터링 절차 및 결과

3. CSMS3에 해당하는 인증을 받고자 하는 회사는 202. 2항에 추가하여 우리 선급에 검토용으로 아래의 자료 각 2부를 제출하여야 한다.
(1) 사이버보안 심사 정책 및 계획
(2) 사이버보안 협의체 구성도
(3) 재해복구 모의 훈련 결과
(4) 암호키 관리 절차
(5) 개발 소프트웨어 소스 코드에 대한 보안 요구사항

4. 문서검토 시 발견된 결함에 대하여 회사는 조치 결과가 반영된 문서를 우리 선급에 제출하여 적절성을 검토 받아야 한다.

203. 현장검사

1. 현장검사는 수집된 회사의 사이버보안 관련 자료를 기반으로 회사 내 사이버보안 관리 시스템 및 관련 자산의 기밀성, 무결성 및 가용성을 계속 유지할 수 있는지에 대하여 검사하는 것이다.
2. 문서 검토가 완료된 이후 현장검사가 실시되어야 한다.
3. 회사는 현장검사를 위한 자료를 검사원이 현장에서 확인할 수 있도록 비치하여야 하며 검사원은 이에 대하여 현장검사를 진행하여야 한다.
4. CSMS1에 해당하는 인증을 위한 현장 검사 시 아래 사항을 검사하여야 한다.
(1) 사이버보안 이슈 공지내역
(2) 사이버보안 교육 결과
(3) 부재자/전문 사이버보안 교육 결과
(4) 사이버보안 리스크 관리 결과

(5) 퇴직자 보안 서약서
(6) 외부자 자산 반납 문서
(7) 접근권한 변경 기록
(8) 특수권한 분류표
(9) 로그 모니터링 절차 및 결과
(10) 물리적 통제 방안
(11) 침입차단 시스템 정책 운영 현황
(12) 백신 운영 현황
(13) 데이터 및 통신 암호화 현황
(14) 원격접속 통제 현황
(15) 로그 보관과 모니터링 절차 및 결과
(16) 데이터 백업 관리대장
(17) 저장매체 폐기 관리대장
(18) 신규 소프트웨어 테스트 보고서 (해당할 경우)
(19) 신규 소프트웨어 이관 승인결과 (해당할 경우)
(20) 시험 및 이관 보고 결과
(21) 데이터 오남용 방지 결과

5. CSMS2에 해당하는 인증을 위한 현장 검사 시 203. 4항에 추가하여 아래 사항을 검사하여야 한다.
(1) 소프트웨어 테스트 결과
(2) 변경관리 기록
(3) 원격 사용자 관리대장
(4) 사이버보안 지침 및 매뉴얼 개정이력
(5) 외부자 교육, 점검 결과
(6) 외부자 계정발급 승인내역
(7) 취약성 조치 계획 및 결과

6. CSMS3에 해당하는 인증을 위한 현장 검사 시 203. 5항에 추가하여 아래 사항을 검사하여야 한다.
(1) 전문 사이버보안 교육 결과
(2) 재해복구 계획 운영 내역
(3) 네트워크 접근제어 모니터링 내역
(4) 암호키 변경 내역

7. 결함 조치 및 확인
(1) 현장검사 시 본 지침의 요건에 대한 검사를 통해 발견되는 결함에 대하여 조치 결과를 현장 검사 후 3개월 이내 우리 선급에 제출하여 적절성을 검토 받아야 한다.
(2) 결함 조치 및 보안 시스템이 제대로 이행되었는지에 대하여 결함 조치 통보 후 3개월 이내에 현장 재검사를 통하여 최종 확인되어야 하며 조치된 최종 결과가 검사보고서에 포함되어야 한다.

204. 검사보고서 및 인증서 발급

1. 본 지침에서 요구되는 모든 현장검사 항목을 통과한 경우, 선급은 사이버보안 관리시스템에 대한 검사보고서를 작성하여 인증서와 함께 회사에 제공한다.
2. 사이버보안 검사보고서에는 최소한 다음을 포함하여야 한다.
(1) 회사의 사이버보안 대상 시스템 및 자산 목록
(2) 회사 사이버보안 관리 시스템에 대한 문서 목록
(3) 회사 사이버보안 관리 시스템 적용성 검사 결과
(4) 결함 조치 결과
(5) 사이버보안 관리 시스템 유지에 필요한 검사의 종류 및 시기, 확인 사항

제 3 절 선박 최초검사

301. 검사신청

1. 우리 선급으로부터 사이버보안 관리 시스템에 대하여 최초 검사를 받고자 하는 선박의 경우 사이버보안 관리시스템을 3개월 이상 이행한 후 선주가 우리 선급에 검사신청을 하여야 한다. 다만, 제조중 등록 검사 선박인 경우 조선소에서 우리 선급에 검사신청을 할 수 있다.
2. 우리 선급은 검사신청서가 제출된 후 신청된 검사가 계속하여 진행되지 않는 등 수검의사가 불명확한 경우, 검사수수료가 지불되지 아니한 경우, 본선이 우리 선급의 요건에 맞지 아니한 경우 등 우리 선급이 필요하다고 인정하는 경우에는 검사신청을 거절할 수 있는 권리를 지닌다.

302. 문서검토

1. CSMS1 인증을 받고자 하는 선박에 대하여 선주는 우리 선급에 검토용으로 아래의 자료 각 2부를 제출하여야 한다.
   (1) 사이버보안 조직도 및 보안인력 직무기술서
   (2) 사이버보안 교육 결과 보고서
   (3) 데이터 백업 및 복구 기준
   (4) 기능 요구사항 / 명세서
   (5) 모바일 보안 정책
   (6) 선박에 대한 기본 사항
   (7) 사이버보안 관련 자산 및 장비 목록과 각 자산에 대한 담당자 현황
   (8) 사이버보안 리스크 평가 보고서
   (9) 네트워크 구축 계약서 / 구축 수행계획서 / 네트워크 구성도
   (10) 선박 사이버보안 관리 시스템 적용성 검토서
   (11) 사이버보안 관리 시스템에 대한 정책서, 절차서 및 지침서
   (12) 외부자 보안 정책 / 외부자 사업 계약서
   (13) 물리보안 정책
   (14) 사고대응 및 복구 정책
   (15) 사이버보안 위협 목록
   (16) 리스크 관리 계획서
   (17) 자산 취약성 진단 결과
   (18) 개선조치 계획 및 결과
   (19) 데이터 중요도 분류표
   (20) 접근권한 관리 정책
   (21) 소프트웨어 도입 절차
   (22) 패치 작업/승인내역서
   (23) 암호화 기준
   (24) 변경관리 절차 및 변경신청서
2. CSMS2 인증을 받고자 하는 선박에 대하여 선주는 302. 1항에 추가하여 우리 선급에 검토용으로 아래의 자료 각 2부를 제출하여야 한다.
   (1) 정책 제개정 승인 내역서
   (2) 사이버보안 지침 및 매뉴얼
   (3) 사이버보안 교육 계획서
   (4) 사고 기준 분류표
   (5) 재해복구 계획서 / 범위정의서
   (6) 침투테스트 결과 보고 내역
   (7) 이상 징후 모니터링 절차 및 결과
3. CSMS3 인증을 받고자 하는 선박에 대하여 선주는 302. 2항에 추가하여 우리 선급에 검토용으로 아래의 자료 각 2부를 제출하여야 한다.
   (1) 사이버보안 심사 정책 및 계획

(2) 재해복구 모의 훈련 결과
(3) 암호키 관리 절차

4. 문서검토 시 발견된 결함에 대하여 선주는 조치 결과가 반영된 문서를 우리 선급에 제출하여 적절성을 검토 받아야 한다.

303. 현장검사

1. 현장검사는 수집된 선박의 사이버보안 관련 정보를 바탕으로 선박 내 정보기술 또는 운영기술 시스템과 자산들에 대하여 본 지침의 요건을 만족 하는지를 검사하는 것이다.
2. 문서 검토가 완료된 이후 현장검사가 실시되어야 한다.
3. CSMS1 인증을 받고자 하는 선박에 대하여 현장 검사 시 아래 사항을 검사하여야 한다.
(1) 사이버보안 이슈 공지내역
(2) 사이버보안 교육 결과
(3) 부재자/전문 사이버보안 교육 결과
(4) 리스크 관리 결과
(5) 퇴직자 보안 서약서
(6) 외부자 자산 반납 문서
(7) 접근권한 변경 기록
(8) 특수권한 분류표
(9) 로그 모니터링 절차 및 결과
(10) 물리적 통제 방안
(11) 침입차단 시스템 정책 운영 현황
(12) 백신 운영 현황
(13) 데이터 및 통신 암호화 현황
(14) 원격접속 통제 현황
(15) 로그 보관과 모니터링 절차 및 결과
(16) 데이터 백업 관리대장
(17) 저장매체 폐기 관리대장
(18) 신규 소프트웨어 테스트 보고서(해당할 경우)
(19) 신규 소프트웨어 이관 승인결과(해당할 경우)
(20) 시험 및 이관 보고 결과
(21) 데이터 오남용 방지 결과
(22) 시스템별 운영매뉴얼
4. CSMS2 인증을 받고자 하는 선박에 대하여 현장 검사 시 **303. 3**항에 추가하여 아래 사항을 검사하여야 한다.
(1) 변경관리 기록
(2) 원격 사용자 관리대장
(3) 사이버보안 지침 및 매뉴얼 개정이력
(4) 외부자 사이버보안 교육, 점검 결과
(5) 외부자 계정발급 승인내역
(6) 취약성 조치 계획 및 결과
5. CSMS3 인증을 받고자 하는 선박에 대하여 현장 검사 시 **303. 4**항에 추가하여 아래 사항을 검사하여야 한다.
(1) 전문 사이버보안 교육 결과
(2) 재해복구 계획 운영 내역
(3) 네트워크 접근제어 모니터링 내역
(4) 암호키 변경 내역
6. 선박의 사이버보안 관리시스템 관련 설비의 설치 상태는 **선급 및 강선규칙**에서 적용되는 규정에서 요구되는 수준을 만족하는 여부가 현장검사 시 확인되어야 한다.
7. 결함 조치 및 확인
(1) 현장검사 시 본 지침의 요건에 대한 검사를 통해 발견되는 결함에 대하여 조치 결과를 현장 검사 후

3개월 이내 우리 선급에 제출하여 적절성을 검토 받아야 한다.

(2) 결함 조치 결과는 필요한 경우 시정조치 후 3개월 이내에 현장 재검사를 통해 확인되어야 한다. 다만, 결함이 경미하거나, 문서검토로 대체 가능한 경우 이를 인정할 수 있다.

304. 검사보고서 작성 및 인증서 발급

1. 본 지침에서 요구되는 모든 현장검사 항목에 통과한 경우, 선급은 사이버보안 관리시스템에 대한 검사보고서를 작성하여 인증서와 함께 선박에 제공하며, 선박에 선급 부기부호를 부여한다.
2. 사이버보안 검사보고서에는 최소한 다음을 포함하여야 한다.
   (1) 선박의 사이버보안 대상 시스템 및 자산 목록
   (2) 선박 사이버보안 관리 시스템에 대한 문서 목록
   (3) 선박 사이버보안 관리 시스템 적용성 검사 결과
   (4) 결함 조치 결과
   (5) 사이버보안 관리 시스템 유지에 필요한 검사의 종류 및 시기, 확인 사항

제 4 절 인증을 유지하기 위한 검사

401. 일반사항

1. 연차검사

(1) 연차검사는 사이버보안 관리 시스템 및 관련 설비가 본 지침의 관련 요건을 준수하여 만족한 상태로 이행되거나 유지되고 있음을 보증하기 위하여 시행하여야 한다.

(2) 검사 이후 사이버보안 관리 시스템에 대하여 승인되지 않은 변경사항이 있었는지의 여부를 확인하여야 한다.

(3) 사이버보안 관련 운영지침서가 선박에 비치되어 있고 모든 변경 사항이 반영되어 있어야 한다. 검사원은 검사를 위한 기초로서 점검기록 및 그 내용에 대하여 특별히 주의하여 운영지침서를 확인하여야 한다.

2. 정기검사

(1) 정기적 검사를 정해진 기간 내에 받는 조건으로 지정되는 5년의 새로운 인증 기간 동안 사이버보안 관리 시스템을 만족한 상태로 이행하고 있으며, 관련 보안설비가 정상적으로 작동되고 있는지를 확인하기에 충분한 범위에 대하여 최초검사에 준하여 검사하여야 한다.

(2) CSMS2 이상의 경우 사이버보안 관리 시스템에 포함된 주요 자산의 존재할 수 있는 침투, 탈취, 변형, 파괴, 손상 또는 기타 통신 결함을 식별하기 위한 모의침투시험을 수행하여야 하며, 모의시험결과가 검사원에 제출되어 확인되어야 한다.

3. 임시검사

(1) 임시검사는 선급의 인증을 받은 회사나 선박이 연차 또는 정기검사를 받을 시기 이외에 다음에 해당하는 경우에 한다.
   (가) 사이버보안 관리 시스템 관련 설비에 손상이 발생하거나 손상 가능성이 발견된 경우
   (나) 중요한 사이버보안 관리 시스템 관련 설비에 대한 수리 또는 교체가 발생한 경우
   (다) 사이버보안 관리 시스템의 주요 변경 사항이 발생한 경우

(2) 임시검사에서는 (1)호의 규정에 따라 필요한 사항을 시험 및 검사를 한다.

402. 회사 인증 유지 검사

1. 사이버보안 관리 시스템을 갖춘 회사가 계속 인증을 유지하기 위하여 매년 정기적으로 다음에 대한 연차검사를 받아야 한다.

(1) CSMS1에 해당하는 인증을 유지하기 위한 현장 검사 시 아래 사항을 검사하여야 한다.
   (가) 시스템별 사용자 접근기록
   (나) 사이버보안 사고조치 보고서
   (다) 사이버보안 사고대응 및 복구정책
   (라) 로그 모니터링 절차 및 결과
   (마) 시스템 패치 관리 기록

(바) 변경된 자산목록 및 변경관리 기록
(사) 물리적 보안 이행 상태
(아) 접근통제 이행 상태
(자) 사이버보안 리스크 평가 보고서 및 리스크 관리 계획서의 이행 상태
(차) 직원의 사이버보안 교육훈련 기록
(카) 사이버보안 관련 설비 작동 상태

(2) CSMS2에 해당하는 인증을 유지하기 위한 현장 검사 시 **402. 1** (1)호에 추가하여 아래 사항을 검사하여야 한다.
(가) 이상 징후 모니터링 결과
(나) 사이버보안 정책, 절차서, 지침서 제/개정 이력
(다) 사이버보안 보안지침 및 매뉴얼 개정이력
(라) 침투테스트 계획 및 결과

(3) CSMS3에 해당하는 인증을 유지하기 위한 현장 검사 시 **402. 1** (2)호에 추가하여 사이버보안 심사 결과를 검사하여야 한다.

2. 회사 내 사이버보안 관리 시스템의 인증을 갱신하기 위해서 매 5년마다 정기 검사를 받아야 한다. 자세한 검사항목은 **2장 202.**와 **203.**의 규정에 따른다.

403. 선박 인증 유지 검사

1. 사이버보안 관리 시스템을 갖춘 선박이 계속 인증을 유지하기 위하여 정기적으로 연차검사를 받아야 한다.

(1) CSMS1 인증을 유지하고자 하는 선박에 대하여 연차검사 시 아래 사항을 검사하여야 한다.
(가) 시스템별 사용자 접근기록
(나) 사이버보안 사고조치 보고서
(다) 사이버보안 사고대응 및 복구정책
(라) 로그 모니터링 절차 및 결과
(마) 시스템 패치 관리 기록
(바) 변경된 자산목록 및 변경관리 기록
(사) 물리적 보안 이행 상태
(아) 접근권한 변경(생성, 삭제 등) 기록
(자) 접근권한 검토 결과서
(차) 성능 모니터링 결과
(카) 사이버보안 리스크 평가 보고서 및 리스크 관리 계획서의 이행 상태
(타) 선원의 사이버보안 교육훈련 기록
(파) 사이버보안 관련 설비 작동 상태
(하) 접근통제 이행 상태

(2) CSMS2 인증을 유지하고자 하는 선박에 대하여 연차검사 시 **403. 1** (1)호에 추가하여 아래 사항을 검사하여야 한다.
(가) 이상 징후 모니터링 결과
(나) 사이버보안 정책, 절차서, 지침서 제/개정 이력
(다) 사이버보안 보안지침 및 매뉴얼 개정이력
(라) 침투테스트 계획 및 결과
(마) 사이버보안 침해사고 보고서 또는 침해사고 조사 분석 절차서

(3) CSMS3 인증을 유지하고자 하는 선박에 대하여 연차검사 시 **403. 1** (2)호에 추가하여 아래 사항을 검사하여야 한다.
(가) 사이버보안 심사 결과
(나) 재해복구 모의훈련 결과

2. 선박 사이버보안 관리 시스템의 인증을 갱신하기 위해서 선박 정기적 검사 주기에 따른 정기 검사를 받아야 한다. 자세한 검사항목은 **2장 302.**와 **303.**의 규정에 따른다. ⚓

제 3 장 해상 사이버보안 관리 시스템에 대한 요건

제 1 절 일반사항

101. 일반사항

1. 이 장은 회사 및 선박의 사이버보안 관리 시스템에 적용하여야 하는 정보기술 및 운영기술에 대한 요구 및 조직 절차를 규정한다.
2. 이 장은 사이버보안 관리 시스템의 준수를 위한 조직 내 정보기술 및 운영기술 영역 내에서 사이버보안과 관련한 필수 요건을 설명하고 있으며 조직 내 구성원의 역량을 구성한다.

제 2 절 CSMS1 (CSMS1(C))

201. 사례 검토

1. 회사는 사이버보안 위협, 사례 등 외부 환경요인 변화의 최신 정보를 공유하기 위해 정부기관, 보안전문업체 등과 협력하여야 한다.
2. 회사는 사이버보안 위협, 사례 등 외부 환경요인의 변화에 대한 정보가 입수된 경우 지체 없이 임직원 및 관계자들에게 공유하여야 한다.

202. 보안 정책

1. 회사는 보안운영을 위한 운영방법, 절차 등의 책임자를 명시하여 정책으로 수립하고, 지속적으로 검토 및 관리되어야 한다.
2. 보안조직은 보안활동 관련 역량을 보유한 인력을 지정하고 책임과 권한을 부여하여야 한다.

203. 보안 교육

1. 보안활동 관련자는 보안교육 계획에 따라 연 1회 이상 보안교육을 실시하여야 한다.
2. 신규 입사자(협력업체, 임시직 포함) 및 퇴사자에 대한 보안교육을 실시하여야 하며, 특히 국내외 출장 및 부재자에게 필요한 교육도 실시하여야 한다.
3. 회사는 정보기술 및 운영기술의 운영 인력에게 실무 시 적용되는 보안기술 관련 전문교육을 실시하여야 한다.

204. 위험 관리

1. 내부 정보기술 및 운영기술 환경에 영향을 미치는 외부 환경요인을 위협으로 식별하고 목록화하여야 한다.
2. 사이버 보안위험을 관리할 수 있도록 위험평가 방법 및 절차 등을 포함한 위험관리 계획을 수립하여야 한다.
3. 회사는 주기적으로 자산에 대한 취약성 진단을 실시하여야 한다.
4. 모든 자산에 대해 위협식별, 취약성 진단 결과를 연계하여 정기적으로 위험평가를 실시하여야 한다.
5. 위험평가 결과에 따라 위험수준별 우선순위를 선정하고 개선조치를 실시하여야 한다.
6. 위험평가 결과는 모든 관련자에게 공유하고 개선조치를 지원할 수 있도록 하여야 한다.

205. 자산 관리

1. 시스템, 설비, 데이터 등 보호되어야 하는 모든 자산은 평가 기준을 수립하여 분류하여야 한다.
2. 회사는 보안이 요구되는 장비, 설비 등 자산별 책임자를 지정하고 역할을 정의하여야 한다.
3. 유출 및 손상 시 영향도 등 기준을 고려하여 데이터 중요도를 분류하고 문서화하여야 한다.
4. 정보자산은 중요도에 따라 분리된 보관 장소에 보호조치를 적용하여야 한다.
5. 선원을 포함한 모든 임직원 또는 외부자의 고용 또는 계약 및 작업 종료 시 해당 내외부 직원이 소유

한 자산은 반납되어야 한다.

206. 접근통제

1. 운영시스템 접근권한에 대한 기준, 원칙, 절차 등을 포함한 접근통제 정책을 수립하여야 한다.
2. 시스템에 접속 가능한 사용자는 최소한으로 권한을 부여하고 목록화하여 관리하여야 한다.
3. 일반 사용자와 관리자의 권한을 차등 부여하고 업무별 권한 기준을 정의하여야 한다.
4. 사용자의 접근권한은 접근통제 정책에 따라 공식적인 절차로 관리하여야 한다.
5. 특수 목적을 위해 부여한 권한을 분류하고 식별하여 별도 통제하여야 한다.
6. 사용자 계정(ID)별 책임을 명확히 하고 기밀성을 유지하기 위한 보안기능을 설정하여야 한다.
7. 시스템에 대한 사용자의 접근기록을 일정 기간 이상 보유하고 주기적으로 검토하여야 한다.

207. 물리적 보안

1. 회사는 시스템 장비, 설비, 시설 등에 대한 물리적 보안 기준을 정의한 정책을 수립하여야 한다.
2. 회사는 자산이 포함된 보호구역에 대해 인가된 자만 접근할 수 있도록 물리적 통제방안을 마련하여야 한다.
3. 회사는 보호구역 내 주요 자산에 대한 작업 시 불법적 침입을 감시 및 추적하여야 한다.
4. 보호구역을 감시하기 위해 설치된 CCTV 등과 같은 장치가 설치되는 경우 인증수단 등을 통해 사용자를 분리하여 비인가자의 접속을 차단하여야 한다.
5. 주요 시스템은 물리적, 논리적 접근이 가능한 자의 권한을 분리하여 관리하고 비인가된 자의 접근을 통제하여야 한다.
6. 회사는 신규 시스템 설치 시 기존 시스템과 최소한 동일한 물리적 보안이 적용되었는지 확인하여야 한다.
7. 통신회선 등 주요 시스템 운용에 필수적인 설비들이 물리적 공격에 노출되지 않도록 보호하고 주기적 점검을 실시하여야 한다.
8. 회사는 USB 등 휴대용 저장매체를 통한 내부 자산 및 네트워크 연결을 통제하여야 한다.
9. 회사는 노트북 등 휴대용 장비가 도난 또는 분실에 의해 정보가 유출되지 않도록 보호대책을 마련하여야 한다.
10. 모든 하드웨어 자산의 재사용 여부에 대한 기준을 마련하고 재사용하지 않는 경우 안전한 파기가 이뤄질 수 있도록 대책을 마련하여야 한다.
11. 서류 및 휴대용 저장 매체가 보관된 공간의 클린 데스크 운영 및 단말기 화면보호 정책이 마련되어 적용되어야 한다.

208. 사고대응 및 복구

1. 회사는 사고 발생 시 사고 유형과 그에 따른 대응방법 및 절차 등을 포함한 사고대응 및 복구 정책을 수립하여야 한다.
2. 회사는 시스템 운영 및 보안이슈에 즉각적으로 대응 및 복구 업무를 수행할 조직 또는 담당자를 구성하여 역할 및 책임을 정의하여야 한다. 또한 내외부 관련자들과 신속한 연락이 가능하도록 비상연락 체계를 구축하고 비상 연락망을 최신화하여 관리하여야 한다.
3. 선박 내 운영시스템은 비상 상황 발생 시에도 운영될 수 있도록 비상 운영 기능을 확보하여야 한다.
4. 사고발생 시 시스템의 안전하고 지속적인 운영이 가능하도록 관련 기능을 제공하고 매뉴얼을 문서화하여야 한다.
5. 시스템 설계 시 운영 장애에 대비한 보안요구사항을 반영하여야 한다.

209. 외부자 보안

1. 회사는 외부자에 의한 보안 사고를 대비하기 위한 외부자의 정보기술 장비, 데이터 등에 대한 보안정책을 수립하여야 한다.
2. 회사는 외부자와 계약 시 보안요구사항을 명시하고 사업기간 중 관리·감독에 관한 사항을 명시하여야 한다.
3. 회사는 외부자에게 시스템 접속권한을 부여하여야 하는 경우 책임자에 의한 승인절차를 따라야 한다.
4. 외부자는 회사 보안요구사항을 준수하여 시스템을 사용하여야 하며 외부자 소유의 장비를 시스템에 연

결하는 경우 보안기능 검사를 사전에 실시하여야 한다.

210. 데이터 보안

1. 중요 데이터는 별도의 공간에 백업하여 안전하게 보관하여야 한다.
2. 데이터는 중요도에 따라 사용자 접근을 제한하고 물리적, 논리적 접근통제를 실시하여야 한다.
3. 개인 이메일 사용이나 불법사이트 접근을 통해 비인가자 공격 및 데이터 접근을 방지하기 위해 사적인 인터넷 사용을 제한적으로 금지하여야 한다.
4. 데이터가 저장된 장비의 폐기 시 저장된 데이터를 재생 불가능한 방법으로 삭제하여야 한다.

211. 로그 관리

1. 시스템별 로그는 유형을 분류하여 필수적인 로그를 일정 기간 동안 안전하게 보관하여야 한다.
2. 로그 저장 시 로그 데이터 무결성의 유지 여부를 확인하여야 한다.
3. 로그가 저장된 시스템은 비인가자의 침입을 막기 위해 물리적, 논리적 접근통제를 실시하여야 한다.
4. 회사가 운영하는 소프트웨어와 하드웨어는 동일한 시간대로 동기화되어야 한다.
5. 시스템 성능 및 용량의 초과가 발생하지 않도록 모니터링을 실시하고 장애발생 시 신속히 대응하여야 한다.

212. 소프트웨어 개발 및 테스트

1. 소프트웨어 및 응용프로그램의 도입 전 보안 테스트를 실시하기 위한 절차를 수립하여야 한다.
2. 소프트웨어 테스트를 통해 결함을 확인하고 테스트를 통과하지 못한 경우 실제 운영시스템에 적용을 금지하여야 한다.
3. 테스트 수행을 위한 테스트환경을 구축하고 절차에 따라 테스트를 실시하여야 한다.
4. 테스트를 통과한 소프트웨어는 적용 전 책임자의 승인 획득 후 운영시스템에 적용하여야 한다.
5. 소프트웨어 개발 시 회사에서 지정한 저장소만을 사용하며 클라우드 서비스 등 외부 저장소 사용 필요 시 사전 승인을 받도록 하여야 한다.

213. 시스템 관리

1. 운영시스템 내 승인되지 않은 인터페이스, 포트 또는 서비스가 존재하는지 확인하도록 한다.
2. 운영시스템 내 파일 정보 전송 시 정보제공 규격이 정의되어 적용되어 있는지 확인하여야 한다.
3. 모든 정보자산 도입 시 최초의 기본 설정값은 회사의 보안 정책 또는 변경관리 기준에 따라 보안설정을 변경하여야 하며, 보안설정이 변경되기 전 사용을 금지하여야 한다.
4. 시스템의 변경 전 장애사항을 대비하여 필요 시 관련 데이터를 백업하여야 한다.
5. 운영시스템 소프트웨어 설치는 보안부서에 의해 제한되어야 하며, 승인되지 않은 소프트웨어 업데이트 또는 업데이트 방법이 적용되지 않도록 하여야 한다.
6. 정보자산에 접근하는 모든 소프트웨어는 자동 실행되지 않도록 구성하여야 한다.
7. 변경관리 시행 시 사전 테스트를 실시하고 변경관리 기록을 보관 및 관리하여야 한다.

214. 패치 (Patch) 관리

1. 회사는 시스템 패치 시 패치 우선순위를 선정하여 승인된 절차를 통해 패치를 수행하도록 하며, 패치 전 사전에 알려진 취약성, 장애요인 등을 목록화하여 패치를 수행하여야 한다.
2. 자동 패치도구의 사용이 불가능 하거나 비호환 시스템의 경우 별도 타 시스템과 동일한 기준으로 별도 관리하여야 한다.
3. 누락된 시스템 없이 패치를 수행하고 패치별 버전관리를 위해 시스템별 버전을 기록하고 관리하여야 한다.

215. 모바일 보안

1. 회사는 회사 모바일 기기 및 직원 소유의 모바일 기기 사용을 통제하기 위한 보안정책을 수립하여야 한다.

2. 회사는 회사에서 이용 가능한 모바일 기기와 기능을 정의하고 사용 중인 기기를 식별하여야 한다.
3. 모바일 기기는 네트워크 및 시스템 연결을 제한하고 사진촬영 등 통화 외 기능 사용을 통제하여야 한다.
4. 회사는 임직원이 사용하는 모바일 기기가 악성코드 감염 또는 해킹에 악용되는 비인증 엑세스 포인트(Rogue Access Point)에 접속하는 것을 예방하여야 한다.

216. 암호화

1. 데이터 전송 시 암호화된 방식으로 통신할 수 있는 환경을 구축하여야 한다.
2. 데이터 보호를 위한 암호화 적용 기준을 마련하고 계획하여야 한다.
3. 중요 등급으로 분류된 데이터는 암호화하여 저장하여야 한다.

217. 악성코드 대응

악성코드로부터 네트워크, 정보시스템 및 운영시스템, 단말기를 보호하기 위한 통제장치가 마련되어야 한다.

218. 네트워크 관리

1. 통신 채널의 결함으로 타 네트워크에 영향을 미치지 않도록 네트워크 장비의 취약성을 주기적으로 확인하여야 한다.
2. 내부 네트워크의 보호를 위하여 외부 비인가된 접근을 차단하는 침입차단 시스템의 설치 및 운영이 이뤄져야 하며 지속적 관리를 적용하여야 한다.
3. 무선 네트워크 환경 구축 시 외부인이 접속 가능한 무선 네트워크와 분리되어 구성되어야 한다.
4. 운영시스템이 무선 네트워크를 통하여 접근되지 않도록 제한하여야 한다.
5. 정보시스템 또는 운영시스템의 내외부 통신 인터페이스는 통제되어 연결이 제한되어야 한다.
6. 정보시스템과 운영시스템의 네트워크는 상호 분리 운영되어야 한다.
7. 외부 네트워크를 통해 시스템에 접속하는 경우 강화된 인증기술 등을 통한 안전한 접속방법을 적용하여야 한다.
8. 네트워크 경로를 파악할 수 있는 도식화된 네트워크 흐름을 보유하여야 한다.
9. 네트워크 관련 장비 구축 시 기본 설정값(default)을 제거하고 보안 관련 기능을 활성화 하도록 하여야 하며, 필요 시 공급자에게 요구하여 적용하여야 한다.
10. 통신회선을 구축하는 경우 통신경로, 연결우선 순위, 프로토콜을 사전에 정의하여 결함을 최소화 하고 서비스 수준 협약 등을 공급자 계약에 포함하여야 한다.

제 3 절 CSMS2 (CSMS2(C))

301. 위협정보 수집체계 구축

회사는 사이버 보안 위협, 사례 등 외부 환경요인의 변화를 검토하여 회사 정책에 반영하여야 한다.

302. 보안 정책 및 매뉴얼의 지속적 관리

1. 회사의 지침 및 매뉴얼은 주기적으로 검토하여 회사 정책 및 기국 또는 IMO와 같은 국제기구의 요구사항을 만족하여야 하며 개정사항은 기록 관리하여야 한다.
2. 회사는 정책 및 지침을 수행하기 위해 참고하여야 할 절차 및 표준을 고려하여 문서화하여야 한다.

303. 강화된 보안 조직

1. 회사는 회사 및 선박의 사이버보안을 총괄 관리할 수 있는 최고책임자를 임원급 이상에서 지정하여야 한다.
2. 자산의 규모, 회사의 특성 등을 고려하여 회사와 선박에서 보안활동 실무를 수행할 보안조직을 구성하여야 한다.

304. 전문 보안 교육

1. 내외부 환경요인, 자산의 변화 등을 고려하여 강화된 회사 보안교육 계획 및 선박 보안교육 계획을 수립하여야 한다.
2. 회사는 소프트웨어 적용 테스트를 실시하는 인력에게 테스트 절차 및 표준에 대한 교육을 실시하여야 한다.

305. 이상 징후 탐지

1. 회사는 사용자 직무변화에 따라 권한의 변동이 적절히 이루어졌는지 주기적으로 검토하여야 한다.
2. 정보시스템에 대한 비인가자의 접속 또는 이상 징후를 탐지하기 위하여 침입탐지 기능을 보유하여야 한다.
3. 회사는 시스템 사용자 행동 파악을 통해 로그 우선순위를 분류한 기준을 수립하여야 한다.
4. 회사는 로그의 분석 시 기준을 수립하고 목표치를 수립하여 달성여부를 측정하여야 된다.
5. 원격접근이 허용된 시스템의 경우 안전한 기능요구사항을 반영하고 주기적으로 기능의 안전성 여부를 점검하여야 한다.
6. 네트워크 액세스 제어 기술을 기존 네트워크, 원격 및 무선 네트워크를 포함한 모든 통신방법에 적용하여야 한다.
7. 데이터가 저장된 장비의 폐기 시 저장된 데이터를 재생 불가능한 방법으로 삭제하여야 한다.

306. 선박 내 물리적 통제 개선

1. 선박 보호구역내 CCTV를 설치한 경우 주기적으로 장비기능을 검사하여야 한다.
2. 선박 보호구역내 CCTV를 설치한 경우 주요 시스템의 통신망과 분리하여야 한다.

307. 침해사고 대응 역량 강화

1. 회사는 업무 또는 임무 중요도와 위협 종류에 따라 사고의 유형을 분류하고 유형별 사고 대응 절차서를 수립하여 보관하여야 한다.
2. 회사는 외부 공격에 의한 사고를 예방하기 위해 알려진 주요 시스템 취약성을 확인하고 조치하여야 한다.
3. 회사는 사고와 관련된 징후를 모니터링하고 내부 영향도를 고려하여 사전에 조치하여야 한다.
4. 회사는 사고의 조사 및 대응 시 생성된 정보를 기록하고 영향도 및 조치계획을 포함하여 경영진에게 보고하여야 한다.
5. 회사는 사고 대응 및 분석을 위한 인력, 장비 또는 기술을 보유하여야 한다.
6. 회사는 침해사고 조사 분석을 수행할 인력을 지정하고 관련 내용을 숙지시켜야 한다.
7. 회사는 침해사고의 심각도를 사전에 정의하여 심각도에 따른 대응 조치를 실시하여야 한다.
8. 회사는 침해사고 조사 분석 시 피해 정도에 따라 유관 자산을 파악하여 조사 분석 범위를 정의하여야 한다.
9. 침해사고 분석 시 범위 내 모든 로그 데이터를 조사하여야 한다.
10. 회사는 효과적인 보안을 점검하기 위한 모의훈련 또는 침투테스트를 주기적으로 실시하고 관련 계획을 수립하여야 한다.
11. 모의훈련 또는 침투테스트의 범위는 운영 중인 시스템 업무 연속성에 영향을 주지 않지 않도록 정의되어야 한다.
12. 침투테스트는 사전 계획에 따라 수행하며 가능한 모든 자원을 동원하여 테스트를 실시하여야 한다.

308. 사이버보안 내부심사

1. 정책 위반사항이 사이버보안 내부 심사 계획에 따라 보고되어야 한다.
2. 회사는 외부자가 사업을 수행하는 중 주기적으로 보안 실태점검 및 교육을 실시하여야 한다.

309. 변경관리

1. 시스템별 변경관리 이력을 기록하고 특이사항을 관리하여 문제점이 반복되지 않도록 관리하여야 한다.
2. 시스템 패치 전 업무 영향도, 예상 장애 등을 고려한 사전 테스트를 수행하여야 한다.
3. 시스템 패치 시 신뢰할 수 있는 네트워크 연결만을 허용하며 원격으로 작업이 진행되는 경우 상황을

모니터링하여야 한다.

4. 회사는 안전한 소프트웨어 개발을 위한 개발 시 강화된 보안요구사항을 정의하여야 한다.
5. 회사는 외부 개발자를 포함하여 소프트웨어 개발자가 접근하는 데이터를 제한하고 모니터링 할 수 있도록 하여야 한다.

310. 비즈니스 연속성 강화

1. 시스템 운영매뉴얼은 내부 정책과 연계성을 주기적으로 검토하고 위험관리 프로세스와 연계되어야 한다.
2. 회사는 비즈니스 연속성을 유지하기 위한 비상상황 발생 시 재해복구 계획을 수립하여야 한다.

311. 모바일 보안관리

모바일 기기 사용통제를 위해 자동화된 통제 도구, 모바일 백신을 통해 기술적 보안을 적용하여야 한다.

312. 보안투자

1. 시스템 수명주기와 보안기술 요구사항을 고려하여 예산을 책정하여야 한다.
2. 기술인수가 필요한 예산의 경우 시스템별 요구사항, 업계 표준 등을 만족하는 기술인수 예산을 책정하여야 한다.
3. 위험평가 결과와 위험관리 계획을 고려하여 예산을 책정하여야 한다.

제 4 절 CSMS3 (CSMS3(C))

401. 보안체계의 일원화

1. 회사는 유관된 법률, 표준, 기술 가이드 등의 변화를 모니터링하여 회사 정책에 반영하여야 한다.
2. 회사는 보안조직, 정보기술 및 운영기술 인력 간 보안이슈를 공유 및 협의할 수 있는 보안협의체를 구성하여야 한다.

402. 보안엔지니어링

1. 교육을 통해 습득한 보안 관련 이슈사항을 주기적으로 테스트하는 훈련을 실시한다.
2. 개발 시 코드의 보안성을 검토하여야 하며, 개발된 애플리케이션을 통해 저장 및 전송 되는 데이터의 보안요구사항을 점검하여야 한다.

403. 비즈니스 연속성 보장

1. 회사는 사고대응을 지원하는 시스템을 주기적으로 점검하고, 필요 시 업데이트를 실시하여야 한다.
2. 회사는 내외부 환경요인과 자산의 변화 및 변경 등을 고려하여 사고대응 계획서를 지속적으로 검토하고 개선하여야 한다.
3. 재해복구를 위한 시스템 보안요구사항을 적용하고 정기적으로 점검하고 조치하여야 한다.
4. 재해복구능력을 테스트하고 계획의 검증을 위해 주기적으로 가상 모의훈련을 실시하여야 한다.
5. 침투테스트 전 사전평가를 통해 취약성을 제거하여야 한다.
6. 침투테스트 완료 시 결과를 검토하고 회사 보안의 효과성을 측정하여 보고하여야 한다.
7. 회사는 침해사고 조사 분석 시 관련 정책, 조사실, 기술도구를 제공하여야 한다.

404. 실시간 모니터링 역량 강화

1. 네트워크 액세스 제어 기술을 사용하여 비정상적인 통신을 감시하고 제한조치를 실행하여야 한다.
2. 회사와 선박은 네트워크에 접속하는 다양한 트래픽을 실시간으로 모니터링하여 비정상 행위를 사전에 인지하고 대응하여야 한다.
3. 신규 취약점을 악용하는 악성코드에 의한 감염 및 확산을 방지하기 위하여 실시간 모니터링 및 대응체계를 구축하여 운영하여야 한다.

405. 사이버보안 심사

1. 회사는 회사 및 사이버보안 전문기관에 의한 사이버보안 심사를 수행하기 위한 정책을 수립하여야 한다.
2. 회사는 주기적으로 회사 및 사이버보안 전문기관에 의한 사이버보안 심사 계획을 수립하고 실시하여야 한다.

406. 암호키 관리

암호키는 절차를 수립하여 관리하여야 하며, 접근통제 정책에 따라 분리하여 보관하여야 한다. ⚓

인 쇄 2018년 3월 24일
발 행 2018년 4월 1일

해상 사이버보안관리 시스템 지침

발행인 이 정 기
발행처 **한 국 선 급**
부산광역시 강서구 명지오션시티 9로 36
전화 : 070-8799-7114
FAX : 070-8799-8999
Website : http://www.krs.co.kr

신고번호 : 제 2014-000001호 (93. 12. 01)