2025 년 12 월 19 일

동아특수화학(주)

정보보안 표준운영 절차서

승인자	서무 이한경 차장
제정	2025년 12월 19일
개정	최초 제정
문서 관리 번호	DGP-0212
문서 관리자	서무 이한경 차장

I. 당사 내부용 정보보안 표준운영 절차서

제 1장 [총칙]

가. 목적

본 절차서는 회사의 정보 자산을 보호하고, 정보보안 위험을 효과적으로 관리하며, 관련 법규 및 국제 표준(ISO 27001) 요구사항을 준수하기 위한 정보보안 관리 체계 및 운영 절차를 정의함을 목적으로 한다. 이를 통해 정보의 기밀성, 무결성, 가용성을 확보하고, 지속적인 정보보안 개선 활동을 수행한다.

나. 적용범위

본 절차서는 회사의 모든 정보 자산(정보 시스템, 데이터, 네트워크, 물리적 시설 등), 정보보안 활동에 관련된 모든 임직원 및 외부 이해관계자(협력업체, 파견 직원 등)에게 적용된다.

다. 용어 정의

1. 정보보안
   정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 유지하는 것.
2. 정보 자산
   회사 업무 수행에 필요한 모든 정보 및 정보를 처리, 저장, 전송하는 수단.
3. 정보보안 위험
   정보 자산의 손실을 초래할 수 있는 위협과 취약점의 조합.
4. ISMS (Information Security Management System)
   정보보안을 수립, 구현, 운영, 모니터링, 검토, 유지 및 개선하는 데 사용되는 경영 시스템.

제 2장 [정보보안 정책 및 조직]

가. 정보보안 정책

회사의 정보보안 최고 책임자는 정보보안에 대한 의지를 표명하고, 정보보안 목표, 원칙 및 책임을 명시한 정보보안 정책을 수립하고 공표한다. 모든 임직원은 정보보안 정책을 숙지하고 준수해야 한다.

나. 정보보안 조직 및 책임

1. 정보보안위원회
   정보보안 정책 및 전략 수립, 주요 정보보안 투자 결정, 정보보안 관련 중요 사안 심의 및 의결을 담당한다.
2. 정보보안담당관
   정보보안 활동의 총괄 책임자로서, 정보보안 정책 및 절차의 수립, 이행 감독, 정보보안 교육 및 인식 제고 활동을 주관한다.
3. 정보보안팀
   정보보안 정책 및 절차의 실질적인 이행, 정보보안 시스템 운영 및 관리, 취약점 점검, 침해사고 대응 등 실무를 담당한다.
4. 각 부서장
   소관 부서의 정보 자산 보호 책임, 정보보안 정책 및 절차 준수 감독, 부서원 교육 및 인식 제고를 담당한다.
5. 모든 임직원
   정보보안 정책 및 절차 준수, 정보보안 사고 징후 발견 시 즉시 보고 의무를 가진다.

제 3장 [정보보안 위험 관리]

가. 위험 식별

정보 자산의 중요도, 위협 및 취약점을 식별하여 정보보안 위험을 파악한다.

1. 정보 자산 식별
   모든 정보 자산(하드웨어, 소프트웨어, 데이터, 문서, 서비스 등)을 식별하고 목록화한다.
2. 위협 식별
   정보 자산에 대한 잠재적 위협(자연 재해, 시스템 장애, 해킹, 내부자 위협 등)을 식별한다.
3. 취약점 식별
   정보 시스템, 프로세스, 인력 등의 보안 취약점을 식별한다.

나. 위험 평가

식별된 위험에 대해 발생 가능성과 비즈니스에 미치는 영향을 평가하여 위험 수준을

결정합니다. 정량적 또는 정성적 방법을 사용하여 위험도를 산정한다.

다. 위험 처리
평가된 위험 수준에 따라 적절한 위험 처리 방안을 수립하고 이행한다.
1. 위험 회피
위험 발생 가능성이 높은 활동을 중단한다.
2. 위험 감소
보안 통제 수단을 적용하여 위험 수준을 허용 가능한 수준으로 낮춘다.
3. 위험 전이
보험 가입 등을 통해 위험을 제3자에게 전가한다.
4. 위험 수용
잔여 위험이 허용 가능한 수준일 경우 위험을 수용한다.

라. 위험 모니터링 및 검토
정보보안 위험은 주기적으로 재평가하고, 새로운 위협 및 취약점에 대한 정보를 지속적으로 모니터링하여 위험 관리 계획을 업데이트한다.

제 4장 [정보보안 통제 영역별 운영 절차]

가. 인적 보안
1. 채용 시 보안
신규 입사자에 대한 배경 확인 및 보안 서약서 징구, 정보보안 교육 실시.
2. 재직 중 보안
정기적인 정보보안 교육 및 인식 제고 활동, 직무 변경 시 접근 권한 재조정, 보안 위반 시 징계 절차 적용.
3. 퇴직 시 보안
정보 자산 반납 확인, 시스템 접근 권한 즉시 회수, 비밀유지 의무 고지.

나. 자산 관리
1. 자신 식별 및 분류
모든 정보 자산에 대해 소유자, 중요도, 기밀성, 무결성, 가용성 기준에 따라 분류하고 라벨링한다.
2. 자산 소유권 지정
모든 정보 자산에 대해 명확한 소유자를 지정하고, 소유자는 해당 자산의 보호에 대한 책임을 가진다.
3. 자산 사용 정책
정보 자산의 올바른 사용 및 처리 방법에 대한 정책을 수립하고 준수한다.

다. 접근 통제
1. 사용자 등록 및 해지
모든 시스템 사용자는 고유 ID를 부여받고, 퇴사 또는 전배 시 즉시 계정을 해지한다.
2. 권한 관리
최소 권한 원칙에 따라 업무상 필요한 최소한의 접근 권한만 부여하고, 주기적으로 권한의 적정성을 검토한다.
3. 패스워드 정책
강력한 패스워드 설정 규칙(길이, 복잡성, 변경 주기 등)을 수립하고 강제 적용한다.
4. 네트워크 접근 통제
방화벽, 침입탐지/방지 시스템 등을 통해 네트워크 접근을 통제하고, 외부 네트워크 접근 시 VPN 등 보안 채널을 사용한다.

라. 암호화
기밀 정보 저장 및 전송 시 암호화 기술을 적용하며, 암호화 키 관리 정책을 수립하여 키의 생성, 저장, 사용, 파기 등 라이프사이클을 안전하게 관리한다.

마. 물리적 및 환경적 보안
1. 보안 구역 설정
서버실, 데이터센터 등 중요 정보 자산이 보관된 구역은 출입 통제 시스템을 설치하고, 인가된 인원만 접근을 허용한다.

2. 설비 보안
   정보 시스템 및 저장 매체는 물리적 손상, 도난, 무단 접근으로부터 보호되도록 안전하게 관리한다.
3. 환경 보안
   화재, 침수, 정전 등 재해로부터 정보 자산을 보호하기 위한 비상 전원, 소화 설비, 항온항습 장치 등을 운영한다.

바. 운영 보안

1. 운영 절차
   시스템 운영 및 관리 작업(패치, 설정 변경 등)은 문서화된 절차에 따라 수행한다.
2. 악성코드 방지
   백신 소프트웨어 설치 및 최신 업데이트 유지, 의심스러운 파일 및 웹사이트 접근 제한 등 악성코드 감염을 예방한다.
3. 백업 및 복구
   중요 데이터 및 시스템 구성 정보는 정기적으로 백업하고, 백업 데이터의 무결성을 확인하며, 복구 절차를 수립하고 주기적으로 테스트한다.
4. 로깅 및 모니터링
   모든 정보 시스템의 접근 및 활동 로그를 기록하고, 비정상적인 활동에 대해 실시간 모니터링 및 분석을 수행한다.
5. 취약점 관리
   정보 시스템 및 애플리케이션의 보안 취약점을 주기적으로 점검하고, 발견된 취약점에 대해 신속하게 패치 또는 보안 조치를 적용한다.

사. 통신 보안

1. 네트워크 보안
   네트워크 장비의 보안 설정 강화, 불필요한 포트 차단, 네트워크 분리 등을 통해 안전한 통신 환경을 구축한다.
2. 정보 전송 보안
   이메일, 파일 전송 등 정보 전송 시 기밀 정보는 암호화하거나 보안 채널을 통해 전송한다.

아. 시스템 개발 및 유지 보수 보안

1. 보안 개발 수명 주기
   시스템 개발 초기 단계부터 보안을 고려하고, 설계, 구현, 테스트, 배포 등 모든 단계에서 보안 취약점을 점검한다.
2. 테스트 및 승인
   개발된 시스템은 배포 전 충분한 보안 테스트를 거치고, 정보보안팀의 승인을 받아야 한다.
3. 변경 관리
   시스템 및 소프트웨어 변경 시 보안 영향을 평가하고, 변경 사항은 문서화된 절차에 따라 통제된다.

자. 공급업체 관계 보안

1. 보안 요구사항 명시
   외부 공급업체와 계약 체결 시 정보보안 요구사항을 명확히 명시하고, 비밀유지협약(NDA)을 체결한다.
2. 보안 점검 및 모니터링
   공급업체가 회사의 정보를 처리하는 경우, 주기적으로 보안 준수 여부를 점검하고 모니터링한다.

차. 정보보안 사고 관리

정보보안 사고의 예방, 탐지, 대응, 복구 및 사후 처리에 대한 절차를 수립하고 이행한다. (자세한 내용은 별도의 "정보보안 사고 대응 절차서"에 따른다.)

카. 사업 연속성 관리

정보보안 사고 또는 재해 발생 시 핵심 비즈니스 기능의 연속성을 보장하기 위한 사업 연속성 계획(BCP) 및 재해 복구 계획(DRP)을 수립하고, 주기적으로 테스트한다.

타. 법규 준수
정보보안 관련 국내외 법규 및 규제(예: 개인정보보호법, 정보통신망법, GDPR 등)를 식별하고, 이에 대한 준수 여부를 지속적으로 확인한다.

제 5장 [검토]

가. 경영진 검토
정보보안 최고 책임자는 정보보안 관리 체계의 지속적인 적합성, 충분성 및 효과성을 보장하기 위해 주기적으로 경영진 검토를 수행한다.

제 6장 [문서 관리]

가. 문서화
정보보안 정책, 절차서, 지침 등 모든 정보보안 관련 문서는 명확하고 이해하기 쉽게 문서화한다.

나. 문서 통제
정보보안 문서는 승인, 배포, 개정, 보관, 폐기 등 문서 통제 절차에 따라 관리하며, 최신 버전이 유지되도록 한다.

2025. 12. 19

동아특수화학주식회사 대표이사 전병철