2025 년 12 월 19 일

동아특수화학㈜

정보보안 사고 대응 절차서

승인자	총무 이한경 차장
제정	2025년 12월 19일
개정	최초 제정
문서 관리 번호	DGP-0211
문서 관리자	총무 이한경 차장
정보보안담당자	총무 이한경 차장

2025 년 12 월 19 일

Ⅰ. 내부용 정보보안 사고 대응 절차서

제 1 장 [개요]

가. 목적

본 절차서는 정보보안 사고 발생 시 신속하고 효율적인 대응을 통해 정보 자산의 피해를 최소화하고, 재발을 방지하여 회사의 정보보안 안정성을 확보하는 것을 목적으로 한다.

나. 적용 범위

본 절차서는 회사의 모든 정보 시스템, 네트워크, 정보 자산 및 이를 이용하는 모든 임직원과 협력업체 직원에 적용된다.

다. 용어 정의

1. 정보보안 사고(Incident)
   정보 자산의 기밀성, 무결성, 가용성을 침해하는 모든 행위 또는 상황을 의미하며, 정보 유출, 시스템 마비, 악성코드 감염 등을 포함한다.
2. 침해사고 긴급 대응반(IR Team)
   정보보안 사고 발생 시 사고 인지 및 접수, 대응, 조치, 사후관리까지 일련의 과정을 수행하는 전담 조직이다.
3. 개인정보
   살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)를 말합니다.

제 2 장 [정보보안 사고 관리 체계]

가. 조직 및 역할

역할	책임 및 권한
정보보안담당관	정보보안 사고 대응 총괄, 최종 의사결정, 대외 협력 및 보고
침해사고 긴급 대응반	사고 인지 및 접수, 분석, 통제, 복구, 사후 처리 등 실무 총괄
각 부서장	소속 부서 내 사고 인지 및 초기 보고, 사고 대응 협조
모든 임직원	정보보안 사고 인지 시 즉시 보고, 보안 지침 준수

나. 침해사고 긴급 대응반 구성

침해사고 긴급 대응반은 다음과 같이 구성되며, 사고 발생 신속하게 소집된다.

1. 반장: 정보보안담당관
2. 팀원: 정보기획보안팀장, 시스템 담당자, 네트워크 담당자, 데이터베이스 담당자 등 관련 부서 실무자

다. 협력 체계

1. 내부 협력
   사고 발생시 관련 부서(총무팀)와 긴밀히 협력하여 법적 대응, 대외 공지, 직원 교육 등을 수행한다.
2. 외부 협력
   필요한 경우 외부 보안 전문 업체, 한국인터넷진흥원(KISA), 개인정보보호위원회 등 유관기관에 자문을 요청하거나 협조를 구한다.

제 3 장 [사고 대응 절차]

정보보안 사고 대응은 크게 인지 및 신고, 접수 및 초기 대응, 분석 및 진단, 통제 및 격리, 복구 및 재가동, 사후 처리 및 재발 방지 단계로 진행된다.

가. 사고 인지 및 신고

1. 사고 인지
   임직원은 정보보안 사고 징후(예: 시스템 이상 작동, 악성코드 감염 의심, 비정상적인 정보 접근 시도 등)를 인지하는 즉시 정보보안담당관 또는 침해사고 긴급 대응반에 신고해야 한다.
2. 신고 채널
   유선, 이메일, 내부 신고 시스템 등 지정된 채널을 통해 신고한다.
3. 초기 정보 수집
   신고자는 사고 발생 시간, 내용, 영향 범위 등 가능한 한 상세한 정보를 제공해야 한다.

나. 사고 접수 및 초기 대응

1. 사고 접수
   침해사고 긴급 대응반은 신고된 내용을 접수하고, 사고 유형과 심각도를 초기 평가한다.
2. 긴급 대응반 소집
   심각한 사고로 판단될 경우 즉시 긴급 대응반을 소집한다.
3. 상황 전파
   정보보안담당관은 사고 발생 사실을 경영진에게 보고하고, 필요시 관련 부서에 전파한다.

다. 사고 분석 및 진단

1. 사고 유형 및 범위 파악
   사고의 원인, 공격 경로, 피해 시스템, 유출된 정보의 종류 및 규모 등을 상세히 분석한다.
2. 증거 보전
   사고 관련 로그, 시스템 이미지, 네트워크 패킷 등 모든 증거를 훼손되지 않도록 확보하고 보전한다.
3. 영향도 평가
   사고가 회사 업무, 재정, 대외 이미지 등에 미치는 영향을 평가한다.

라. 사고 통제 및 격리

1. 확산 방지
   추가적인 피해 확산을 막기 위해 감염 시스템의 네트워크 차단, 서비스 일시 중단, 계정 잠금 등 필요한 조치를 수행한다.
2. 악성코드 제거
   악성코드 감염의 경우, 해당 악성코드를 즉시 삭제하고 확산 경로를 차단한다.

마. 사고 복구 및 시스템 재가동

1. 복구 계획 수립
   분석 결과를 바탕으로 시스템 및 데이터 복구 계획을 수립한다.
2. 시스템 복구
   백업된 데이터를 활용하거나 시스템 재설치 등을 통해 정상 상태로 복구한다.
3. 취약점 제거
   사고 원인이 된 보안 취약점을 제거하고, 필요한 보안 패치를 적용한다.
4. 시스템 재가동
   복구 및 보안 강화 조치가 완료된 후, 시스템의 정상 작동 여부를 확인하고 재가동한다.

바. 사고 사후 처리 및 재발 방지

1. 사고 당사자 진술서 작성
   필요한 경우 사고 관련 당사자의 진술서를 확보한다.
2. 재발 방지 대책 수립
   사고 원인 분석을 통해 도출된 문제점을 바탕으로 재발 방지를 위한 기술적, 관리적 대책을 수립한다.
3. 보안 시스템 강화
   사고 발생으로 드러난 보안 취약점을 보완하기 위해 보안 시스템을 강화한다.

제 4 장 [사후 관리 및 개선]

가. 사고 보고 및 기록

1. 사고 결
2. 과 보고서 작성
   사고 처리 과정, 결과, 조치 사항, 재발 방지 대책 등을 포함하는 최종 보고서를 작성한다.
3. 사고 기록 유지
   모든 정보보안 사고 관련 문서를 체계적으로 기록하고 보관한다.

나. 지속적인 개선 활동

1. 절차서 검토 및 업데이트
   사고 대응 절차서의 실효성을 주기적으로 검토하고, 변화하는 보안 위협 및 기술 동향에 맞춰 지속적으로 업데이트한다.
2. 보안 정책 개선
   사고 사례를 바탕으로 회사의 정보보안 정책 및 지침을 개선한다.

다. 교육 및 훈련

1. 정기 교육
   모든 임직원을 대상으로 정보보안 의식 제고 및 사고 대응 절차에 대한 정기적인 교육을 실시한다.
2. 모의 훈련
   침해사고 긴급 대응반을 중심으로 실제 상황과 유사한 모의 훈련을 정기적으로 실시하여 대응 능력을 강화한다.

제 5 장 [관련 법규 및 지침]

가. 관련 법규

1. 개인정보보호법
   개인정보 유출 등 사고 발생 시 법적 고지 의무 및 관련 조치 사항을 준수한다.
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률
   정보보호 관련 법적 요구사항을 준수한다.

나. 내부 규정 및 지침

본 절차서는 회사의 정보보안 규정 및 기타 관련 지침과 연계하여 적용된다.

2025 년 12 월 19 일

2025. 12. 19

동아특수화학주식회사 대표이사 전병설