(주)아이디에이 정보보안 사고 대응 절차서(IRP) Incident Response Plan

문서번호: IDA-ESG-S-032 (P3)
제정일: 2026. 08. 12.
개정번호: 00
주관부서: 경영지원팀 정보보안 담당
승인: 대표이사 최성규

제 1 조 목적

본 절차서는 (주)아이디에이에서 발생할 수 있는 정보보안 사고를 신속하게 탐지·보고·분석하고, 피해를 최소화하며, 정보자산을 보호하고 업무를 정상적으로 복구하기 위한 사고 대응체계를 수립하는 것을 목적으로 한다.

또한 정보보안 사고 발생 시 임직원의 역할과 책임, 대응방법 및 보고체계를 명확히 하여 기밀정보의 유출, 훼손, 변조 및 무단접근으로 인한 회사의 피해를 예방하고 재발을 방지한다.

제 2 조 적용범위

본 절차서는 (주)아이디에이가 보유하거나 관리하는 다음 정보자산 및 정보에 적용한다.

1. 회사의 전산시스템 및 네트워크
2. PC, 노트북, 서버, 저장장치 및 업무용 모바일기기
3. 이메일 및 파일공유 시스템
4. ERP, MES, 품질관리시스템 등 업무시스템
5. 고객사 및 협력사의 기술자료
6. 도면, 사양서, 견적서, 원가자료 등 기술·영업정보

7. 인사·급여 등 개인정보
8. 비밀번호 및 계정정보
9. USB 등 이동식 저장매체
10. 기타 회사가 기밀정보로 지정한 정보

제 3 조 용어의 정의

1. 정보보안 사고

정보자산의 기밀성, 무결성 또는 가용성을 침해하거나 침해할 우려가 있는 사건을 말한다.

2. 기밀정보

업무상 외부에 공개될 경우 회사 또는 고객사에 손해를 발생시킬 수 있는 정보로서 회사가 기밀 또는 대외비로 지정한 정보를 말한다.

3. 정보유출

기밀정보 또는 개인정보가 승인되지 않은 자에게 열람·복사·전송·제공되는 것을 말한다.

4. 사고 대응

정보보안 사고의 탐지부터 신고, 분석, 억제, 제거, 복구 및 사후 개선까지 수행하는 일련의 활동을 말한다.

5. 사고 대응 책임자

정보보안 사고 발생 시 대응을 총괄하고 필요한 조치를 지휘하는 담당자를 말한다.

제 4 조 정보보안 사고의 유형

정보보안 사고는 다음과 같이 구분한다.

구분	주요 사례
기밀정보 유출	고객사 도면, 기술자료, 원가자료 등의 외부 유출
개인정보 유출	임직원 개인정보의 무단 열람·전송
계정 침해	ID/PW 도용, 비인가 계정 사용
악성코드	바이러스, 트로이목마, 랜섬웨어 등
이메일 사고	피싱메일, 악성 첨부파일, 오발송
해킹	외부 침입, 비인가 접속
자료 훼손	파일 삭제, 변조 또는 데이터 손상
정보자산 분실	노트북, USB, 저장매체 등의 분실
내부자 사고	임직원의 고의 또는 부주의에 의한 정보 유출
협력사 사고	협력업체를 통한 정보 유출 또는 시스템 침해
기타	위 유형에 해당하지 않는 보안사고

제 5 조 사고 대응 조직

정보보안 사고 발생 시 다음과 같이 대응한다.

1. 사고 대응 책임자

정보보안 담당자를 사고 대응 책임자로 지정하며 다음 업무를 수행한다.

- 사고 접수 및 초기 상황 파악
- 사고 등급 결정
- 대응조직 소집
- 사고 확산 방지
- 기술적 조치 지휘
- 대표이사 및 관련 부서 보고
- 외부기관 또는 고객사 대응 필요성 검토

- 사고 종결 승인 요청
- 재발방지 대책 수립

2. IT 담당자

- 시스템 및 네트워크 상태 확인
- 계정 잠금 및 접근 차단
- 감염 시스템 격리
- 로그 및 접속기록 확보
- 악성코드 제거
- 시스템 복구
- 백업자료 확인

3. 해당 부서 책임자

- 사고 발생 사실 및 업무 영향 확인
- 해당 정보의 중요도 판단
- 관련 자료 및 사용자 확인
- 업무 연속성 확보

4. 인사·총무 관련 부서

내부자에 의한 사고 또는 개인정보 관련 사고 발생 시 필요한 인사·법무 조치를 지원한다.

5. 대표이사

중대 사고에 대한 대응방향을 승인하고 필요한 경영적 의사결정을 수행한다.

제 6 조 정보보안 사고의 보고체계

정보보안 사고를 발견하거나 의심한 임직원은 지체 없이 정보보안 담당자에게 신고하여야 한다.

신고 순서

사고 발견자 → 부서장 → 정보보안 담당자 → 사고 대응 책임자 → 대표이사

단, 긴급한 사고의 경우 발견자가 정보보안 담당자에게 직접 신고할 수 있다.

사고 신고방법

- 전화
- 이메일
- 사내 메신저
- 정보보안 사고 신고서

사고 신고 시 가능한 범위에서 다음 사항을 포함한다.

1. 사고 발생 일시
2. 사고 발견 일시
3. 사고 발생 시스템 또는 장비
4. 사고 유형
5. 사고 내용
6. 관련 파일 또는 정보
7. 외부 전송 여부
8. 피해가 예상되는 정보
9. 발견자가 실시한 조치
10. 기타 확인된 사항

제 7 조 정보보안 사고 등급

사고의 영향도에 따라 다음과 같이 등급을 분류한다.

등급	기준	예시	대응
1 급	경미	단순 비밀번호 오류,	담당자 확인

등급	기준	예시	대응
		의심 이메일	
2 급	보통	악성코드 감염, 중요자료 오발송	즉시 차단 및 조사
3 급	중대	기밀정보 외부 유출, 다수 PC 감염	비상 대응
4 급	심각	고객사 핵심기술 유출, 랜섬웨어 확산, 대규모 개인정보 유출	경영진 지휘 및 외부 대응 검토

※ 실제 사고 등급은 정보의 중요도, 유출 범위, 업무 영향, 고객사 영향 및 법적 위험 등을 종합하여 결정한다.

제 8 조 정보보안 사고 대응 절차

정보보안 사고는 다음의 7 단계로 대응한다.

① 준비 → ② 탐지 → ③ 신고 및 접수 → ④ 분석 및 등급분류 → ⑤ 억제·차단 → ⑥ 제거·복구 → ⑦ 사후조치

8.1 준비 단계

정보보안 담당자는 평상시 다음 사항을 준비한다.

- 정보자산 목록 관리
- 중요정보 분류
- 사용자 계정 관리
- 접근권한 관리

- 백업체계 유지
- 보안프로그램 운영
- 시스템 로그 관리
- 사고 연락망 유지
- 사고 대응 담당자 지정
- 임직원 정보보안 교육 실시
- 사고 대응 모의훈련 실시

8.2 탐지 단계

다음과 같은 이상징후가 발견될 경우 정보보안 사고 여부를 확인한다.

- 비정상적인 로그인
- 반복적인 로그인 실패
- 알 수 없는 프로그램 실행
- 파일의 비정상적인 변경 또는 삭제
- 외부로 대량의 파일 전송
- 랜섬웨어 의심 화면 발생
- 이메일 계정의 비정상 발송
- USB 등 저장매체의 무단 사용
- PC 또는 서버의 비정상적인 작동
- 고객사 또는 협력사의 보안사고 통보

8.3 신고 및 접수 단계

사고를 발견한 임직원은 즉시 정보보안 담당자에게 신고한다.

정보보안 담당자는 다음 사항을 기록한다.

- 사고번호

- 발생일시
- 신고자
- 발생부서
- 사고유형
- 관련 정보자산
- 사고내용
- 초기 피해범위
- 초기 대응조치

제 9 조 사고 분석 및 조사

정보보안 담당자는 사고의 원인과 범위를 확인한다.

조사 항목

1. 언제 발생했는가?
2. 어디에서 발생했는가?
3. 어떤 시스템이 영향을 받았는가?
4. 어떤 정보가 영향을 받았는가?
5. 누가 접근 또는 사용했는가?
6. 외부로 정보가 전송되었는가?
7. 추가 피해 가능성이 있는가?
8. 고객사 또는 협력사에 영향이 있는가?
9. 개인정보가 포함되어 있는가?
10. 법적 또는 계약상 신고의무가 발생하는가?

조사 과정에서 확보한 로그, 이메일, 파일, 화면자료 등은 임의로 삭제하거나 변경하지 않는다.

제 10 조 사고 억제 및 차단

사고가 확인된 경우 추가 피해를 방지하기 위하여 필요한 조치를 즉시 실시한다.

주요 조치

- 사용자 계정 잠금
- 비밀번호 변경
- 침해 PC 네트워크 분리
- 악성 IP 차단
- 외부 접속 차단
- 의심 이메일 회수
- USB 등 이동식 저장매체 사용 제한
- 침해 시스템 접근권한 제한
- 중요 파일 공유 차단
- 필요 시 관련 시스템 일시 중지

단, 시스템 차단으로 인한 생산 및 업무 중단이 예상되는 경우 사고 대응 책임자의 판단에 따라 조치한다.

제 11 조 기밀정보 유출 사고 대응

기밀정보가 외부로 유출되었거나 유출이 의심되는 경우 다음 절차에 따른다.

① 유출정보 확인

- 유출된 파일명
- 도면번호
- 고객사
- 기술자료
- 원가자료

- 계약자료
- 개인정보 등 확인

② 유출경로 확인

- 이메일
- USB
- 메신저
- 클라우드
- 인터넷 업로드
- 개인 PC
- 외부 저장장치
- 협력사 시스템 등

③ 유출범위 확인

- 유출 파일 수
- 유출 대상자
- 유출 대상 업체
- 외부 공개 여부
- 추가 전파 여부

④ 즉시 차단

필요 시 계정 및 접근권한을 차단하고 파일 공유 및 전송을 중지한다.

⑤ 증거 보존

관련 이메일, 로그, 파일, 접속기록 및 기타 증거자료를 보존한다.

⑥ 경영진 보고

3 급 이상 사고로 판단되는 경우 사고 대응 책임자는 대표이사에게 즉시 보고한다.

⑦ 고객사 통보 검토

고객사 정보 또는 고객사 기밀자료가 포함된 경우 계약조건 및 고객사 요구사항에 따라 통보 여부를 검토한다.

제 12 조 악성코드 및 랜섬웨어 대응

랜섬웨어 또는 악성코드가 의심되는 경우 다음 조치를 우선한다.

1. 감염 의심 PC 의 네트워크 연결 차단
2. 추가 감염 방지를 위한 공유폴더 접근 제한
3. USB 등 외부 저장매체 연결 금지
4. 감염 PC 임의 조작 최소화
5. 보안 담당자에게 즉시 신고
6. 로그 및 증거자료 보존
7. 감염범위 확인
8. 악성코드 제거
9. 안전한 백업자료 확인
10. 시스템 복구
11. 복구 후 보안상태 확인
12. 재발방지 대책 수립

랜섬웨어 감염 시 사용자가 임의로 파일을 삭제하거나 포맷하지 않도록 한다.

제 13 조 계정 및 비밀번호 침해 대응

계정정보가 유출되었거나 부정사용이 의심되는 경우 다음 조치를 실시한다.

1. 해당 계정 잠금

2. 비밀번호 변경
3. 동일 비밀번호 사용 계정 확인
4. 최근 로그인 기록 확인
5. 비정상 접속 IP 확인
6. 계정 사용 이력 확인
7. 추가 침해 여부 확인
8. 필요 시 관련 계정 전체의 비밀번호 변경
9. 사고 원인 분석
10. 재발방지 조치

제 14 조 정보보안 사고 증거자료 관리

사고 조사에 필요한 증거자료는 임의로 변경하거나 삭제하지 않는다.

보존 대상

- 시스템 로그
- 접속기록
- 이메일
- 파일
- 파일 전송 기록
- CCTV 등 물리적 접근기록
- USB 사용기록
- 보안프로그램 탐지기록
- 사용자 인터뷰 기록
- 사고 화면 캡처
- 기타 관련 자료

증거자료는 접근권한을 제한하여 관리하며 사고 종결 후 회사의 정보보안 기록관리 기준에 따라 보관한다.

제 15 조 시스템 및 업무 복구

사고 원인을 제거한 후 시스템 복구를 실시한다.

복구 순서

1. 사고 원인 제거 확인
2. 시스템 보안상태 점검
3. 백업자료 무결성 확인
4. 시스템 복구
5. 계정 및 접근권한 재설정
6. 보안패치 적용
7. 백신 및 보안프로그램 점검
8. 정상작동 확인
9. 업무부서 확인
10. 정상 운영 전환

복구가 완료된 후 일정 기간 시스템 및 네트워크 상태를 집중 모니터링한다.

제 16 조 외부기관 및 고객사 대응

다음과 같은 경우 대표이사의 승인 또는 회사가 정한 보고체계에 따라 관계기관, 고객사 또는 전문기관과 협의할 수 있다.

1. 개인정보 유출이 의심되는 경우
2. 고객사 기밀정보가 유출된 경우
3. 법적 신고 또는 통지가 필요한 경우
4. 해킹 또는 랜섬웨어 등 중대한 사고가 발생한 경우
5. 회사의 업무 연속성에 중대한 영향을 미친 경우

6. 계약상 고객사에 통보할 의무가 있는 경우

외부기관 또는 고객사에 제공하는 정보는 사고 대응에 필요한 최소 범위로 한다.

제 17 조 사고 종결

다음 조건을 충족하는 경우 사고를 종결할 수 있다.

1. 사고 원인이 확인되었을 것
2. 추가적인 정보유출 또는 침해 가능성이 차단되었을 것
3. 시스템이 정상적으로 복구되었을 것
4. 관련 계정 및 접근권한 조치가 완료되었을 것
5. 필요한 고객사·관계기관 대응이 완료되었을 것
6. 증거자료가 확보되었을 것
7. 재발방지 대책이 수립되었을 것
8. 사고 결과보고서가 작성되었을 것

사고 종결은 정보보안 담당자가 사고 대응 책임자에게 보고하고 승인받아 확정한다.

제 18 조 사고 사후분석 및 재발방지

사고 종결 후 다음 사항을 분석한다.

- 사고 발생 원인
- 대응 과정의 문제점
- 피해범위
- 대응시간
- 대응조치의 적절성
- 보안취약점

- 내부관리 문제
- 교육 필요사항
- 시스템 개선사항

분석 결과에 따라 다음 조치를 실시할 수 있다.

- 보안정책 개정
- 접근권한 개선
- 시스템 보안 강화
- 비밀번호 정책 개선
- 백업체계 개선
- 보안프로그램 강화
- 임직원 교육
- 협력사 보안관리 강화
- 고객사 정보관리 강화

제 19 조 정보보안 사고 대응 기록

정보보안 담당자는 발생한 사고에 대해 다음 기록을 유지한다.

관리항목	기록내용
사고번호	IR-2026-001
발생일시	YYYY-MM-DD HH:MM
신고일시	YYYY-MM-DD HH:MM
신고자	성명 / 부서
사고유형	정보유출/악성코드/계정침해 등
사고등급	1~4 급
발생시스템	PC/서버/ERP/MES 등
관련정보	도면/고객정보/개인정보 등

관리항목	기록내용
피해범위	건수 및 영향
초기조치	계정잠금/네트워크차단 등
원인	사고 원인
복구일시	YYYY-MM-DD HH:MM
고객사 통보	해당/비해당
관계기관 통보	해당/비해당
재발방지	개선조치
종결일	YYYY-MM-DD
승인자	사고 대응 책임자

제 20 조 정보보안 사고 대응 KPI

정보보안 사고 대응의 효과성을 다음과 같이 관리한다.

KPI	산정기준	목표
보안사고 발생건수	연간 사고건수	최소화
기밀정보 유출건수	연간 유출건수	0 건
사고 신고 준수율	적정시간 내 신고건수 / 전체 사고 ×100	100%
초동대응 준수율	절차에 따른 초동대응 건수 / 전체 사고 ×100	100%
사고 복구율	정상 복구 사고건수 / 전체 사고 ×100	100%
재발사고율	동일 원인 재발건수 / 전체 사고 ×100	0%
정보보안 교육 이수율	이수자 / 대상자 ×100	100%
사고 대응훈련 실시	연간 실시횟수	1 회 이상

제 21 조 정보보안 사고 대응 모의훈련

정보보안 담당자는 연 1 회 이상 정보보안 사고 대응 모의훈련을 실시할 수 있다.

훈련 유형은 다음과 같이 선정한다.

1. 기밀정보 오발송
2. 피싱메일
3. 악성코드 감염
4. 랜섬웨어
5. 계정정보 유출
6. USB 를 통한 정보유출
7. 고객사 기술자료 유출

훈련 종료 후 훈련 결과를 평가하고 미흡사항에 대해서는 개선조치를 실시한다.

제 22 조 임직원의 준수사항

모든 임직원은 다음 사항을 준수하여야 한다.

1. 정보보안 사고를 발견한 경우 즉시 신고한다.
2. 사고를 발견하고도 임의로 은폐하거나 지연하지 않는다.
3. 사고 관련 자료를 임의로 삭제하지 않는다.
4. 기밀정보를 개인 이메일로 전송하지 않는다.
5. 승인되지 않은 USB 및 저장매체를 사용하지 않는다.
6. 비밀번호를 타인에게 제공하지 않는다.
7. 의심스러운 이메일의 첨부파일 또는 링크를 실행하지 않는다.
8. 회사의 정보보안 정책 및 절차를 준수한다.

제 23 조 사고 대응 금지사항

사고 발생 시 다음 행위를 금지한다.

- 사고 사실의 임의적인 외부 공개
- 사고자료 임의 삭제
- 증거자료 임의 변경
- 승인 없는 시스템 포맷
- 개인적인 판단에 의한 고객사 통보
- 사고 관련 자료의 외부 전달
- 사고 사실의 은폐
- 사고 원인에 대한 근거 없는 추측 유포

제 24 조 문서 및 기록 보존

정보보안 사고 관련 기록은 회사의 문서관리 및 정보보안 기록관리 기준에 따라 보존한다.

사고 관련 개인정보 및 기밀정보가 포함된 기록은 접근권한을 제한하여 관리한다.

제 25 조 절차의 검토 및 개선

정보보안 담당자는 본 절차서를 연 1 회 이상 검토하고 다음 사항을 반영하여 개정한다.

1. 실제 발생한 정보보안 사고
2. 모의훈련 결과
3. 정보보안 위험평가 결과
4. 고객사 보안 요구사항
5. 법령 및 규정 변경
6. 정보보안 기술 변화

7. 조직 및 시스템 변경사항

[별표 1] 정보보안 사고 대응 흐름

1. 사고 발견

↓

2. 즉시 신고

↓

3. 사고 접수 및 기록

↓

4. 초기 분석

↓

5. 사고 등급 결정

↓

6. 1~2 급 : 담당자 중심 대응

3~4 급 : 사고 대응 책임자 및 경영진 대응

↓

7. 확산 방지 및 시스템 격리

↓

8. 원인 및 피해범위 조사

↓

9. 기밀정보 유출 여부 확인

↓

10. 제거 및 복구

↓

11. 고객사·관계기관 대응 검토

↓

12. 정상 운영 확인

↓

13. 사고 결과보고

↓

14. 재발방지 대책

↓

15. 사고 종결

↓

16. 사후 모니터링

[별표 2] 중대 정보보안 사고 즉시 대응 체크리스트

- ☐ 사고 발생 사실 확인
- ☐ 사고 신고 및 접수
- ☐ 사고 대응 책임자 통보
- ☐ 사고 등급 결정
- ☐ 감염 또는 침해 시스템 격리
- ☐ 관련 계정 잠금
- ☐ 비밀번호 변경
- ☐ 외부 접속 차단
- ☐ 로그 및 증거자료 보존

- ☐ 기밀정보 유출 여부 확인
- ☐ 개인정보 포함 여부 확인
- ☐ 고객사 정보 포함 여부 확인
- ☐ 피해범위 확인
- ☐ 대표이사 보고
- ☐ 고객사 통보 필요성 검토
- ☐ 관계기관 신고 필요성 검토
- ☐ 시스템 복구
- ☐ 정상작동 확인
- ☐ 사고 결과보고서 작성
- ☐ 재발방지 대책 수립
- ☐ 사고 종결 승인
- ☐ 사후 모니터링 실시

[별표 3] 정보보안 사고 결과보고서 필수항목

1. 사고번호
2. 사고 발생일시
3. 사고 발견일시
4. 사고 신고자
5. 발생부서
6. 사고 유형
7. 사고 등급
8. 관련 시스템
9. 관련 정보
10. 사고 원인
11. 피해범위

12. 초기 대응조치
13. 조사 결과
14. 기밀정보 유출 여부
15. 개인정보 유출 여부
16. 고객사 영향 여부
17. 복구조치
18. 외부기관·고객사 대응
19. 재발방지 대책
20. 사고 종결일
21. 담당자
22. 승인자

부칙

본 절차서는 2026 년 08 월 13 일부터 시행한다.