(주)아이디에이 정보보안 관리규정

문서번호: IDA-ESG-S-031 (P3)
제정일: 2026. 08. 12.
개정번호: 00
주관부서: 경영지원팀 정보보안 담당
승인: 대표이사 최성규

제 1 장 총칙

제 1 조 목적

본 규정은 주식회사 아이디에이(이하 “회사”라 한다)가 보유·관리하는 정보 및 정보자산을 안전하게 보호하고 정보의 유출, 훼손, 변조, 분실 및 무단 접근을 예방함으로써 회사의 경영활동과 생산활동을 안정적으로 유지하고 고객 및 이해관계자의 신뢰를 확보하는 것을 목적으로 한다.

제 2 조 적용범위

본 규정은 회사의 임직원, 계약직, 파견근로자, 협력업체 및 회사의 정보자산을 취급하거나 접근하는 모든 자에게 적용한다.

회사의 다음 정보자산을 포함한다.

1. 회사의 전산시스템 및 네트워크
2. 컴퓨터, 노트북, 서버 및 업무용 모바일기기
3. 고객사 자료 및 기술자료
4. 제품 도면 및 사양서
5. 생산·품질 관련 자료
6. 영업·구매·원가 관련 자료

7. 인사·급여·개인정보
8. 이메일 및 전자문서
9. USB 및 외장 저장장치
10. 클라우드 및 외부 정보서비스
11. 기타 회사가 보호할 필요가 있다고 판단하는 정보

제 3 조 정보보안의 기본원칙

회사는 정보보안 관리에 있어 다음 원칙을 준수한다.

1. **기밀성(Confidentiality):** 승인되지 않은 자에게 정보가 공개되지 않도록 한다.
2. **무결성(Integrity):** 정보가 무단으로 변경 또는 훼손되지 않도록 한다.
3. **가용성(Availability):** 정당한 권한을 가진 사용자가 필요한 정보를 이용할 수 있도록 한다.
4. **최소권한 원칙:** 업무수행에 필요한 최소한의 정보만 접근할 수 있도록 한다.
5. **업무상 필요한 정보만 수집·이용한다.**
6. 고객 및 제 3 자의 정보를 계약 및 관련 법령에 따라 보호한다.

제 2 장 정보자산 관리

제 4 조 정보자산의 분류

회사의 정보는 중요도 및 기밀성에 따라 다음과 같이 분류한다.

등급	분류	주요 정보
1 등급	극비	고객사 핵심기술, 영업비밀, 중요 도면
2 등급	대외비	구매가격, 원가자료, 협력사 정보, 내부경영자료
3 등급	내부정보	내부 업무자료, 교육자료, 일반 업무문서
4 등급	공개정보	홈페이지 게시자료 등 공개 가능한 정보

제 5 조 중요정보 관리

다음 정보는 중요정보로 관리한다.

1. 고객사의 기술자료 및 도면
2. 고객사로부터 제공받은 영업·품질자료
3. 제품 개발 및 생산기술 자료
4. 금형 및 공정 관련 기술자료
5. 원가 및 가격정보
6. 협력사 정보
7. 개인정보
8. ESG 및 고객사 평가자료
9. 계약서 및 비공개 문서
10. 기타 회사가 중요하다고 지정한 자료

중요정보는 회사의 승인 없이 외부로 복사, 전송, 공개 또는 반출하여서는 안 된다.

제 3 장 정보 접근 및 계정관리

제 6 조 사용자 계정

1. 정보시스템의 사용자 계정은 개인별로 부여한다.
2. 타인의 계정을 공유하거나 사용하는 것을 금지한다.
3. 계정 및 비밀번호를 타인에게 알려주어서는 안 된다.
4. 업무상 필요하지 않은 시스템에 접근하여서는 안 된다.

제 7 조 비밀번호 관리

1. 비밀번호는 타인이 쉽게 추측할 수 없는 것으로 설정한다.
2. 이름, 생년월일, 전화번호 등 개인정보를 비밀번호로 사용하는 것을 지양한다.
3. 비밀번호는 타인에게 알려주지 않는다.

4. 비밀번호가 노출되었다고 판단되는 경우 즉시 변경한다.

제 8 조 인사이동 및 퇴직자 관리

1. 인사이동 시 변경된 업무에 따라 정보 접근권한을 조정한다.
2. 퇴직자의 정보시스템 계정 및 접근권한은 퇴직 즉시 회수 또는 차단한다.
3. 퇴직자에게 지급된 노트북, USB, 저장장치 및 기타 정보자산을 회수한다.
4. 퇴직자는 회사의 중요정보 및 고객정보를 외부로 반출하여서는 안 된다.
5. 필요한 경우 퇴직자의 정보반출 여부를 확인한다.

제 4 장 문서 및 정보의 외부 반출

제 9 조 정보 외부반출

다음 행위는 사전 승인 없이 금지한다.

1. 회사자료의 USB 복사
2. 개인 이메일로 회사자료 전송
3. 개인 클라우드에 회사자료 업로드
4. 메신저를 통한 중요자료 외부 전송
5. 회사자료의 개인 PC 저장
6. 고객사 자료의 무단 복제
7. 회사자료의 외부 출력 및 반출

제 10 조 USB 및 외부저장장치

1. USB 및 외부 저장장치의 사용은 업무상 필요한 경우에 한한다.
2. 중요자료를 USB 에 저장하여 외부로 반출하는 경우 사전 승인을 받아야 한다.
3. 외부 저장장치에 저장된 중요정보는 필요한 경우 암호화한다.
4. 승인 없이 개인 USB 를 회사 업무에 사용하지 않는다.

제 5 장 이메일 및 인터넷 사용

제 11 조 이메일 보안

1. 회사 이메일은 업무 목적으로 사용한다.
2. 고객사 및 회사의 중요자료를 개인 이메일로 전송하여서는 안 된다.
3. 출처가 불명확한 첨부파일 및 링크를 임의로 실행하지 않는다.
4. 의심스러운 이메일을 발견하면 정보보안 담당자에게 보고한다.
5. 대량의 중요자료를 이메일로 전송할 경우 수신자 및 첨부파일을 반드시 확인한다.

제 12 조 인터넷 및 클라우드 사용

1. 업무와 무관하거나 보안상 위험한 사이트의 이용을 금지한다.
2. 회사의 중요자료를 승인되지 않은 클라우드 서비스에 저장하지 않는다.
3. 회사자료를 개인용 AI 서비스, 파일공유 서비스 또는 온라인 저장공간에 무단 업로드하지 않는다.
4. 외부 온라인 서비스를 이용하여 고객사 자료를 처리할 경우 사전 승인을 받는다.

제 6 장 개인정보 보호

제 13 조 개인정보 보호

회사는 개인정보를 관련 법령 및 회사 내부기준에 따라 보호한다.

개인정보는 업무수행에 필요한 최소한의 범위에서 수집·이용하며, 승인되지 않은 자에게 제공하거나 공개하지 않는다.

제 14 조 개인정보 접근관리

1. 개인정보 접근권한은 업무상 필요한 자에게만 부여한다.
2. 개인정보를 개인 PC 또는 승인되지 않은 저장장치에 저장하지 않는다.
3. 개인정보가 포함된 문서를 외부로 전송하는 경우 보안조치를 적용한다.

4. 보유기간이 경과한 개인정보는 관련 절차에 따라 안전하게 파기한다.

첨부 샘플 역시 개인정보에 대해 접근권한 제한, 암호화, 보안프로그램 설치·갱신 등의 안전성 확보조치를 규정하고 있으므로 이를 아이디에이의 내부관리 기준에 반영한다.

제 7 장 고객사 및 협력사 정보보호

제 15 조 고객사 정보보호

1. 고객사로부터 제공받은 정보는 고객사의 요구사항 및 계약조건에 따라 보호한다.
2. 고객사 도면, 사양서, 품질자료 및 기술자료를 무단으로 복제하거나 외부에 공개하지 않는다.
3. 고객사 정보는 승인된 업무 담당자만 접근할 수 있도록 한다.
4. 고객사 자료를 개인 이메일 또는 개인 클라우드에 저장하지 않는다.
5. 고객사 정보의 외부 제공이 필요한 경우 고객사 및 회사의 승인절차를 준수한다.

제 16 조 협력사 정보보호

협력사로부터 제공받은 기술자료, 가격자료, 계약자료 및 개인정보 등은 업무상 필요한 범위에서만 사용하며 무단 공개 또는 제 3 자 제공을 금지한다.

제 8 장 정보보안 사고관리

제 17 조 정보보안 사고

다음 사항을 정보보안 사고로 정의한다.

1. 회사 정보의 외부 유출
2. 고객사 정보의 무단 유출
3. 개인정보 유출

4. 악성코드 또는 랜섬웨어 감염
5. 해킹 및 무단 침입
6. 계정 또는 비밀번호 도용
7. 노트북·USB 등 정보자산 분실
8. 중요정보의 무단 복사
9. 이메일 오발송
10. 기타 정보보안에 영향을 미치는 사고

제 18 조 정보보안 사고 신고

정보보안 사고 또는 의심되는 상황을 발견한 임직원은 지체 없이 정보보안 담당자 또는 소속 부서장에게 보고한다.

사고 발생 시 다음 사항을 우선적으로 실시한다.

① 사고 발견 → ② 즉시 보고 → ③ 확산 차단 → ④ 원인 조사 → ⑤ 복구 → ⑥ 재발방지

첨부된 기존 샘플에서도 사고 대응을 '감지 및 보고 → 사고 등급 분류 및 확산 차단 → 조치계획 수립 및 실행 → 후속보고 및 재발방지' 순으로 제시하고 있으므로 이를 아이디에이의 사고대응 절차에 반영한다.

제 9 장 물리적 정보보안

제 19 조 문서 보안

1. 중요문서는 승인되지 않은 장소에 방치하지 않는다.
2. 회의실 및 프린터 등에 중요문서를 방치하지 않는다.
3. 중요문서 폐기 시 분쇄 등 적절한 방법으로 폐기한다.
4. 고객사 도면 및 기술자료는 업무 종료 후 적절하게 보관한다.

제 20 조 전산장비 관리

1. 업무용 PC 및 노트북은 임의로 다른 사람에게 양도하지 않는다.
2. 사용하지 않을 때는 화면 잠금 기능을 사용한다.
3. 승인되지 않은 프로그램을 설치하지 않는다.
4. 보안프로그램 및 운영체제 업데이트를 유지한다.
5. 노트북 및 이동식 정보자산의 분실을 예방한다.

제 10 장 정보보안 교육

제 21 조 교육 실시

회사는 임직원의 정보보안 인식 향상을 위해 정기적으로 정보보안 교육을 실시한다.

교육내용에는 다음 사항을 포함한다.

1. 정보보안 기본원칙
2. 개인정보 보호
3. 고객사 정보보호
4. 비밀번호 관리
5. 이메일 보안
6. USB 및 외부저장장치 관리
7. 악성코드 및 랜섬웨어 예방
8. 정보유출 방지
9. 정보보안 사고 신고방법
10. 퇴직 및 인사이동 시 정보보안
11. 외부 클라우드 및 AI 서비스 사용 시 보안수칙

교육 실시 결과는 교육일지 또는 교육결과보고서로 기록·관리한다.

제 11 장 정보보안 점검 및 관리

제 22 조 정기점검

정보보안 담당자는 다음 사항을 정기적으로 점검한다.

1. 사용자 계정 및 접근권한
2. 퇴직자 계정 삭제 여부
3. 중요정보 접근권한
4. USB 및 외부저장장치 사용
5. 보안프로그램 및 업데이트 상태
6. 백업상태
7. 중요자료 보관상태
8. 개인정보 보호상태
9. 고객사 자료 관리상태
10. 정보보안 사고 발생 여부

제 23 조 백업 및 복구

중요한 업무자료는 데이터 손실에 대비하여 정기적으로 백업한다.

백업자료는 원본과 동일한 사고로 동시에 손실되지 않도록 적절한 장소 또는 시스템에 보관한다.

중요 데이터의 복구 가능 여부는 정기적으로 확인한다.

제 12 장 정보보안 위반 및 신고

제 24 조 정보보안 위반 신고

임직원 및 이해관계자는 정보보안 위반 또는 의심되는 상황을 발견한 경우 정보보안 담당자 또는 회사가 지정한 신고채널을 통해 신고할 수 있다.

회사는 신고자의 신원을 보호하고 신고를 이유로 불이익을 주지 않도록 한다.

첨부된 샘플 역시 임직원 및 이해관계자의 보안위협 신고를 허용하고 신고자의 신원을 보호하도록 규정하고 있다.

제 25 조 위반에 대한 조치

본 규정을 위반한 경우 회사는 위반행위의 내용 및 중대성에 따라 다음과 같은 조치를 할 수 있다.

1. 주의
2. 경고
3. 재교육
4. 직무상 조치
5. 징계위원회 회부
6. 민·형사상 조치

고의 또는 중대한 과실로 고객정보, 개인정보 또는 회사의 중요정보를 유출한 경우에는 회사의 관련 규정에 따라 엄중하게 조치할 수 있다.

첨부 샘플에서도 정보보안 위반에 대해 주의·경고·직무정지·징계위원회 회부·민형사상 고발 등의 조치를 규정하고 있다.

제 13 장 책임과 역할

제 26 조 대표이사

대표이사는 회사의 정보보안 관리체계를 승인하고 정보보안 활동에 필요한 자원을 지원한다.

제 27 조 정보보안 담당자

정보보안 담당자는 다음 업무를 수행한다.

1. 정보보안 규정 관리
2. 정보보안 교육
3. 정보자산 관리
4. 접근권한 관리
5. 정보보안 점검
6. 보안사고 대응
7. 보안사고 기록관리
8. 개선조치 관리
9. 고객사의 정보보안 요구사항 대응

제 28 조 부서장

부서장은 소속 직원의 정보보안 준수 여부를 관리하고 업무상 필요한 정보 접근권한을 요청·관리한다.

제 29 조 임직원

모든 임직원은 본 규정을 준수하고 정보보안 사고 또는 의심사항을 발견한 경우 즉시 보고하여야 한다.

제 14 장 기록관리

제 30 조 정보보안 관련 기록

다음 자료를 정보보안 관련 기록으로 관리한다.

1. 정보보안 교육일지
2. 정보보안 교육결과보고서
3. 정보보안 점검표
4. 사용자 계정 및 접근권한 관리대장
5. 정보자산 관리대장
6. 정보보안 사고보고서
7. 사고조치 및 재발방지 보고서
8. 중요정보 외부반출 승인기록
9. USB 및 외부저장장치 사용기록
10. 개인정보 관련 관리기록

기록의 보존기간은 관련 법령, 고객사 요구사항 및 회사의 문서관리 기준에 따른다.

제 15 장 부칙

제 31 조 시행

본 규정은 대표이사의 승인을 받은 날부터 시행한다.

제 32 조 개정

법령, 고객사 요구사항, 정보보안 환경 또는 회사의 업무환경 변경에 따라 필요한 경우 본 규정을 개정할 수 있다.

[별표 1] 정보보안 사고 신고 기준

사고유형	예시	조치
정보유출	고객사 도면 외부 전송	즉시 보고
개인정보	개인정보 오발송	즉시 보고
계정	계정·비밀번호 도용	계정 차단 및 보고
악성코드	랜섬웨어 감염	네트워크 차단 및 보고
장비분실	노트북·USB 분실	즉시 보고
해킹	비정상 로그인	접근 차단 및 조사
기타	중요정보 무단복사 등	담당자 보고

[별표 2] 정보보안 임직원 준수사항

- ☐ 회사 계정 및 비밀번호를 타인과 공유하지 않는다.
- ☐ 고객사 자료를 개인 이메일로 전송하지 않는다.
- ☐ 회사자료를 개인 클라우드에 저장하지 않는다.
- ☐ 승인 없이 USB 로 자료를 반출하지 않는다.
- ☐ 출처가 불명확한 이메일 첨부파일을 실행하지 않는다.
- ☐ 의심스러운 링크를 클릭하지 않는다.
- ☐ 중요문서를 방치하지 않는다.
- ☐ 퇴근 시 PC 화면을 잠근다.
- ☐ 중요정보 유출사고 발생 시 즉시 보고한다.
- ☐ 퇴직 또는 인사이동 시 회사 정보자산을 반납한다.

[별표 3] 정보보안 관리 KPI

KPI	목표
정보보안 교육 실시율	100%

KPI	목표
정보보안 교육 이수율	100%
정보보안 정기점검 실시율	100%
퇴직자 계정 회수율	100%
중요정보 접근권한 점검율	100%
정보보안 사고 재발방지 조치율	100%
고객사 정보보안 요구사항 대응률	100%

문서관리: 본 규정은 회사의 정보보안 관련 내부관리 문서로 관리하며 개정 시 개정이력을 기록한다.

주식회사 아이디에이

대표이사 최성규