Autonomous™

문서관리번호	2025-ENV-S001
최종 수정일	2025. 6. 30
문서 관리자	기획팀

㈜오토기기 정보보안 표준 운영절차(SOP)

2025. 06. 30

목차

1. 개요

1.1 목적

본 정보보안 표준운영절차(SOP)는 주식회사 오토기기(이하 '회사')의 정보자산을 보호하고, 정보보안 관련 위험을 효과적으로 관리하기 위한 표준 절차와 지침을 제공하는 데 그 목적이 있다. 본 문서는 회사의 정보보안 정책을 실행하기 위한 구체적인 방법과 절차를 정의하여, 정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보장하고자 한다.

본 SOP는 다음과 같은 세부 목적을 가진다:

회사의 정보자산에 대한 무단 접근, 유출, 변조, 파괴 등의 위협으로부터 보호

정보보안 관련 법적 요구사항 및 규제 준수

정보보안 사고 발생 시 신속하고 효과적인 대응 체계 구축

임직원의 정보보안 인식 제고 및 책임 의식 강화

지속적인 정보보안 관리체계 개선을 통한 보안 수준 향상

1.2 적용범위

본 SOP는 다음 대상에 적용된다:

인적 범위

회사의 모든 임직원(정규직, 계약직, 파견직)

인턴, 임시 근로자

외부 협력업체 직원(회사 정보자산에 접근하는 경우)

컨설턴트 및 외부 전문가

물리적 범위

본사 사무실(서울특별시 광진구 천호대로 690 5층)

공장(경기도 광주시 초월읍 경충대로 1284번길 70)

원격 근무지(재택근무 등)

정보시스템이 설치된 모든 장소

기술적 범위

회사 소유 또는 관리하는 모든 정보시스템

네트워크 장비 및 인프라

서버, 데스크톱, 노트북, 모바일 기기

소프트웨어 및 애플리케이션

저장매체 및 백업 장치

정보적 범위

회사가 생성, 취득, 보관, 처리하는 모든 정보

전자적 형태의 정보(파일, 데이터베이스 등)

비전자적 형태의 정보(종이 문서, 도면 등)

고객 정보, 기술 정보, 영업 정보 등

1.3 용어 정의

정보자산: 회사가 보유하고 있는 모든 형태의 정보와 이를 처리하는 시스템, 네트워크, 설비 등을 포함하는 자산

정보보안: 정보자산의 기밀성, 무결성, 가용성을 보장하기 위한 모든 활동

기밀성(Confidentiality): 인가되지 않은 개인, 단체, 프로세스에 정보가 노출되지 않도록 보장하는 특성

무결성(Integrity): 정보의 정확성과 완전성을 보호하는 특성

가용성(Availability): 인가된 개체가 요구할 때 접근 및 사용이 가능하도록 보장하는 특성

위험(Risk): 위협이 취약점을 이용하여 자산에 손실이나 손상을 초래할 가능성

위협(Threat): 자산에 손실을 초래할 수 있는 원하지 않는 사건의 잠재적 원인

취약점(Vulnerability): 하나 이상의 위협에 의해 악용될 수 있는 자산의 약점

보안사고: 정보자산의 기밀성, 무결성, 가용성을 침해하는 모든 사건

CERT(Computer Emergency Response Team): 보안사고 대응팀

접근통제: 인가된 사용자만 정보자산에 접근할 수 있도록 제한하는 것

인증: 사용자 또는 시스템의 신원을 확인하는 과정

암호화: 정보를 권한이 없는 사용자가 이해할 수 없는 형태로 변환하는 과정

1.4 참조 표준 및 법규

본 SOP는 다음의 표준 및 법규를 참조하여 작성되었다:

국내 법규

개인정보 보호법

정보통신망 이용촉진 및 정보보호 등에 관한 법률

산업기술의 유출방지 및 보호에 관한 법률

전자금융거래법

정보보호산업의 진흥에 관한 법률

국제 표준

ISO/IEC 27001:2013 (정보보안관리체계)

ISO/IEC 27002:2013 (정보보안 통제 실행 지침)

NIST Cybersecurity Framework

CIS Controls

산업 표준

자동차 산업 정보보안 가이드라인

제조업 사이버보안 프레임워크

2. 정보보안 조직 및 책임

2.1 정보보안 조직 구성

회사의 정보보안 조직은 다음과 같이 구성된다:

정보보안 최고책임자(CISO: Chief Information Security Officer)

ESG경영실장이 겸직

회사의 전반적인 정보보안 전략 및 정책 수립 책임

정보보안팀

정보보안 정책 및 절차 수립, 이행, 모니터링 담당

정보보안 교육 및 인식 제고 활동 수행

보안사고 대응 및 조사 주관

정보시스템팀

IT 인프라 및 시스템의 기술적 보안 통제 구현

네트워크, 서버, 애플리케이션 등의 보안 설정 관리

보안 업데이트 및 패치 관리

정보보안 담당자

각 부서별로 지정된 정보보안 담당자

부서 내 정보보안 활동 이행 및 모니터링

보안 이슈 발생 시 정보보안팀과 협력

정보보안 위원회

주요 정보보안 정책 및 사안에 대한 의사결정 기구

분기별 정기 회의 및 필요시 임시 회의 개최

2.2 역할 및 책임

2.2.1 정보보안 최고책임자(CISO)

회사의 정보보안 전략 수립 및 이행 총괄

정보보안 정책 및 지침 승인

정보보안 예산 및 자원 할당 검토

중대 보안사고 발생 시 대응 지휘

정보보안 위원회 의장 역할 수행

경영진에 정보보안 현황 및 이슈 보고

2.2.2 정보보안팀장

정보보안 정책, 지침, 절차 개발 및 유지관리

정보보안 위험 평가 및 관리 프로세스 운영

정보보안 교육 및 인식 제고 프로그램 운영

보안사고 대응 프로세스 관리

정보보안 준수 여부 모니터링 및 감사

정보보안 관련 법규 및 규제 준수 확인

2.2.3 정보시스템팀장

IT 인프라 및 시스템의 보안 설계 및 구현

보안 솔루션 도입 및 운영

시스템 취약점 관리 및 패치 적용

백업 및 복구 절차 수립 및 이행

기술적 보안 통제 구현 및 운영

2.2.4 부서장

부서 내 정보보안 정책 및 지침 준수 책임

부서 정보보안 담당자 지정

부서 내 정보자산 보호 및 관리 감독

부서원 대상 정보보안 인식 제고

2.2.5 임직원

정보보안 정책 및 지침 준수

정보보안 교육 이수

보안사고 및 취약점 발견 시 보고

회사 정보자산의 적절한 사용 및 보호

2.3 정보보안 위원회

2.3.1 구성

위원장: 정보보안 최고책임자(CISO)

위원: 정보보안팀장, 정보시스템팀장, 인사팀장, 법무팀장, 주요 사업부서장

간사: 정보보안팀 담당자

2.3.2 역할

정보보안 정책 및 주요 지침 검토 및 승인

정보보안 위험 평가 결과 검토 및 대응 방안 승인

중대 보안사고 대응 방안 검토 및 승인

정보보안 예산 및 투자 계획 검토

정보보안 관련 주요 의사결정

2.3.3 회의

정기회의: 분기별 1회

임시회의: 필요시(중대 보안사고 발생, 주요 정책 변경 등)

회의록 작성 및 보관: 간사 담당

의결 정족수: 재적 위원 과반수 출석 및 출석 위원 과반수 찬성

2.4 보안사고 대응팀(CERT)

2.4.1 구성

팀장: 정보보안팀장

팀원: 정보보안팀 담당자, 정보시스템팀 담당자, 법무팀 담당자, 홍보팀 담당자, 관련 부서 담당자

2.4.2 역할

보안사고 접수 및 초기 대응

보안사고 조사 및 분석

보안사고 복구 및 피해 최소화 조치

보안사고 재발 방지 대책 수립

보안사고 관련 외부 기관 대응

2.4.3 운영

상시 대기 체제 운영

보안사고 대응 절차에 따라 활동

정기적인 보안사고 대응 훈련 실시

보안사고 대응 결과 보고서 작성 및 보고

3. 정보자산 분류 및 관리

3.1 정보자산 분류 체계

3.1.1 정보자산 유형

회사의 정보자산은 다음과 같이 분류한다:

정보

전자문서: 워드, 엑셀, PDF 등의 전자적 형태의 문서

비전자문서: 종이 문서, 인쇄물 등

데이터베이스: 구조화된 데이터 집합

백업 데이터: 시스템 및 데이터 백업본

소프트웨어

응용 소프트웨어: 업무용 애플리케이션, ERP, CRM 등

시스템 소프트웨어: 운영체제, DBMS 등

개발 소프트웨어: 개발 도구, 테스트 도구 등

보안 소프트웨어: 백신, 방화벽, IDS/IPS 등

하드웨어

서버: 물리 서버, 가상 서버

네트워크 장비: 라우터, 스위치, 방화벽 등

저장장치: NAS, SAN, 외장 하드 등

사용자 단말: PC, 노트북, 태블릿, 스마트폰 등

주변기기: 프린터, 스캐너, 복합기 등

시설

전산실: 서버룸, 네트워크 장비실 등

통신설비: 회선, 배선, 통신장비 등

보안설비: 출입통제 시스템, CCTV 등

부대설비: UPS, 항온항습기, 소화설비 등

서비스

내부 서비스: 인트라넷, 그룹웨어 등

외부 서비스: 홈페이지, 고객 포털 등

클라우드 서비스: IaaS, PaaS, SaaS 등

통신 서비스: 인터넷, VPN, 전용회선 등

3.1.2 보안 등급 분류

정보자산의 중요도에 따라 다음과 같이 보안 등급을 분류한다:

극비(Top Secret)

무단 유출 시 회사의 존립을 위협할 수 있는 핵심 정보

예: 미공개 신기술 설계도, 인수합병 계획, 핵심 기술 소스코드 등

대외비(Confidential)

무단 유출 시 회사에 중대한 손실을 초래할 수 있는 정보

예: 고객 정보, 재무 정보, 인사 정보, 주요 계약 정보 등

일반(Internal)

회사 내부용 정보로 외부 유출은 제한되나, 유출 시 영향이 제한적인 정보

예: 내부 업무 지침, 일반 업무 문서, 내부 공지사항 등

공개(Public)

외부에 공개되어도 무방한 정보

예: 회사 소개 자료, 제품 카탈로그, 보도자료 등

3.2 정보자산 목록 관리

3.2.1 정보자산 식별

모든 정보자산은 고유 식별자(ID)를 부여하여 관리

식별자 체계: [자산유형]-[부서코드]-[일련번호]

예: HW-IT-001 (IT부서의 첫 번째 하드웨어 자산)

3.2.2 정보자산 목록 작성

정보자산 목록에는 다음 정보를 포함한다:

자산 식별자

자산명

자산 유형

보안 등급

소유자/관리자

위치/보관장소

취득일자

용도/설명

관련 시스템/서비스

최종 업데이트 일자

3.2.3 정보자산 목록 갱신

정보자산 목록은 분기별로 정기 갱신

신규 자산 도입, 폐기, 이전 등 변경 사항 발생 시 즉시 갱신

자산 관리자는 변경 사항을 정보보안팀에 보고

정보보안팀은 정보자산 목록의 정확성 검토 및 승인

3.3 정보자산 중요도 평가

3.3.1 평가 기준

정보자산의 중요도는 다음 기준에 따라 평가한다:

기밀성 영향도

상(3점): 유출 시 심각한 법적, 재정적, 평판 손실 초래

중(2점): 유출 시 중대한 영향이 있으나 제한적 손실 초래

하(1점): 유출 시 경미한 영향

무결성 영향도

상(3점): 변조 시 심각한 업무 장애 및 의사결정 오류 초래

중(2점): 변조 시 중대한 영향이 있으나 제한적 장애 초래

하(1점): 변조 시 경미한 영향

가용성 영향도

상(3점): 이용 불가 시 핵심 업무 중단 및 심각한 손실 초래

중(2점): 이용 불가 시 중대한 영향이 있으나 대체 수단 존재

하(1점): 이용 불가 시 경미한 영향

3.3.2 중요도 산정

총점 = 기밀성 점수 + 무결성 점수 + 가용성 점수

중요도 등급:

8-9점: 극비(Top Secret)

5-7점: 대외비(Confidential)

3-4점: 일반(Internal)

3점 미만: 공개(Public)

3.3.3 평가 주기

신규 자산 도입 시 초기 평가 실시

기존 자산은 연 1회 정기 평가

자산의 용도, 환경 등 중대한 변화 발생 시 재평가

3.4 정보자산 라벨링 및 취급

3.4.1 라벨링 원칙

모든 정보자산은 보안 등급에 따라 적절히 라벨링

전자문서: 문서 상단 또는 하단에 보안 등급 표시

비전자문서: 표지 또는 각 페이지에 보안 등급 스탬프 날인

저장매체: 외부에 보안 등급 라벨 부착

하드웨어: 자산 태그 및 보안 등급 라벨 부착

3.4.2 등급별 취급 지침

극비(Top Secret)

지정된 책임자만 접근 가능

암호화 저장 및 전송 필수

사본 생성 시 책임자 승인 필요

업무 외 장소 반출 금지

폐기 시 완전 파기 후 증빙 기록 보관

대외비(Confidential)

업무상 필요한 인가자만 접근 가능

암호화 저장 및 전송 권장

사본 생성 시 관리대장 기록

업무 외 장소 반출 시 승인 필요

안전한 방법으로 폐기

일반(Internal)

회사 임직원만 접근 가능

민감 정보 포함 시 암호화 권장

업무 목적 외 사용 금지

외부 반출 시 주의 필요

일반 폐기 가능

공개(Public)

접근 제한 없음

암호화 불필요

자유로운 배포 가능

일반 폐기 가능

4. 인적 보안

4.1 채용 전 보안

4.1.1 보안 요구사항 명시

채용 공고 및 직무 기술서에 보안 책임 명시

면접 과정에서 보안 인식 및 태도 평가

채용 예정자에게 정보보안 정책 사전 안내

4.1.2 신원 확인 및 검증

입사 지원자의 신원 및 이력 확인

주요 직위 지원자의 경우 추가 배경 조사

보안 민감 직무의 경우 보안 적합성 평가

법적 허용 범위 내에서 신용 및 범죄 이력 확인

4.1.3 비밀유지 서약

입사 지원자 면접 시 비밀유지서약서 작성

채용 결정 후 정식 비밀유지서약서 서명

비밀유지 의무 범위 및 위반 시 책임 명시

4.2 채용 시 보안

4.2.1 고용 계약 보안 조항

고용 계약서에 정보보안 관련 조항 포함

회사 정보자산 보호 의무

지적재산권 및 비밀정보 보호 의무

보안 정책 및 지침 준수 의무

위반 시 제재 조치

4.2.2 보안 서약서

모든 신규 입사자는 정보보안 서약서 서명

서약 내용:

정보보안 정책 및 지침 준수

회사 기밀정보 보호

정보자산의 적절한 사용

보안사고 발생 시 보고 의무

퇴사 후에도 지속되는 비밀유지 의무

4.2.3 신규 입사자 보안 교육

입사 첫 주 내 기본 정보보안 교육 실시

교육 내용:

정보보안 정책 및 지침 개요

계정 및 패스워드 관리

이메일 및 인터넷 사용 보안

악성코드 예방

보안사고 대응 및 보고 절차

4.3 재직 중 보안

4.3.1 정기 보안 교육

전 임직원 대상 연간 정보보안 교육 계획 수립

기본 교육: 전 직원 대상 연 2회

직무별 특화 교육: 직무 특성에 맞는 교육 연 1회

관리자 교육: 부서장 이상 관리자 대상 연 1회

교육 이수 여부 인사평가 반영

4.3.2 보안 인식 제고 활동

월간 보안 뉴스레터 발행

보안 포스터 및 안내문 게시

보안 캠페인 및 이벤트 실시

모의 피싱 훈련 분기별 실시

보안 우수 직원 포상

4.3.3 직무 분리

중요 업무의 직무 분리 원칙 적용

개발, 테스트, 운영 환경 분리

권한 부여 시 직무 충돌 검토

불가피한 경우 상호 검토 및 모니터링 강화

4.3.4 인사 변동 시 보안 관리

부서 이동, 직무 변경 시 접근 권한 재검토

휴직 시 계정 및 접근 권한 일시 중지

장기 부재 시 업무 인계 과정에서의 보안 관리

복직 시 보안 교육 재실시 및 권한 재부여

4.4 퇴직 시 보안

4.4.1 퇴직 절차

퇴직 예정자 대상 보안 점검표 작성

회사 소유 정보자산 반납 확인

계정 및 접근 권한 회수

보안서약서 재확인 및 퇴직 후 의무 고지

정보 유출 방지를 위한 최종 점검

4.4.2 자산 반납 및 계정 처리

노트북, 모바일 기기 등 회사 자산 반납

출입카드, 사원증 등 물리적 접근 수단 회수

사내 시스템 계정 비활성화

공유 계정 패스워드 변경

이메일 전달 설정 및 자동 응답 메시지 설정

4.4.3 퇴직자 보안 서약

퇴직 시 비밀유지서약서 재서명

퇴직 후에도 지속되는 비밀유지 의무 고지

회사 정보 보유 금지 및 삭제 확인

경쟁업체 취업 제한 조항 확인(해당 시)

5. 물리적 보안

5.1 보안구역 지정 및 관리

5.1.1 보안구역 분류

회사의 물리적 공간은 다음과 같이 보안구역으로 분류한다:

제한구역(Restricted Area)

정의: 핵심 정보자산이 위치하며 가장 높은 수준의 보안이 요구되는 구역

예: 전산실, 통신실, 보안관제실, 중요 문서 보관소

통제구역(Controlled Area)

정의: 중요 업무가 수행되며 인가된 인원만 출입 가능한 구역

예: 연구개발실, 임원실, 인사팀, 재무팀 등 주요 부서 공간

일반구역(General Area)

정의: 일반 업무가 수행되며 기본적인 출입 통제가 적용되는 구역

예: 일반 사무공간, 회의실, 휴게실

공개구역(Public Area)

정의: 외부인의 출입이 허용되는 구역

예: 로비, 접견실, 교육장

5.1.2 보안구역 표시

각 보안구역은 명확한 경계 설정 및 표지판 부착

제한구역, 통제구역은 "관계자 외 출입금지" 표시

출입문에 보안구역 등급 및 출입 요건 명시

CCTV 설치 구역 안내 표지 부착

5.1.3 보안구역 설계 및 구축

제한구역: 이중 출입통제, 방화벽, 항온항습 설비, 무정전 전원 공급 장치

통제구역: 출입통제 시스템, 방화설비

일반구역: 기본 잠금장치, 화재 감지기

공개구역: 안내데스크, CCTV

5.2 출입 통제

5.2.1 출입 권한 관리

보안구역별 출입 권한 정책 수립

직무 및 업무 필요성에 따른 최소 권한 부여

출입 권한 정기 검토 및 갱신(분기별)

퇴직, 휴직, 부서이동 시 즉시 권한 조정

5.2.2 출입 통제 시스템

사원증 기반 출입카드 시스템 운영

제한구역: 생체인식(지문, 얼굴) + 출입카드 이중 인증

통제구역: 출입카드 인증

일반구역: 출입카드 또는 기본 잠금장치

출입 이력 자동 기록 및 보관(최소 3개월)

5.2.3 방문자 관리

방문자 사전 등록 시스템 운영

방문자 신분 확인 및 방문증 발급

방문 목적, 방문 대상자, 방문 시간 기록

방문자 출입 가능 구역 제한

방문자 안내 및 에스코트 정책

5.2.4 출입 모니터링 및 위반 대응

출입 기록 정기 검토(주 1회)

비정상 출입 시도 실시간 경고

미승인 출입 시도 시 보안 담당자 즉시 대응

출입 위반 사례 기록 및 조치

5.3 사무환경 보안

5.3.1 클린 데스크 정책

자리 이석 시 중요 문서 및 저장매체 보관

퇴근 시 책상 위 문서 정리 및 서랍 잠금

공용 프린터 출력물 즉시 수거

화이트보드 회의 내용 퇴실 시 삭제

정기적인 클린 데스크 점검 실시(월 1회)

5.3.2 화면 보호 정책

자리 이석 시 화면 잠금 필수(단축키 교육)

무인 상태 10분 경과 시 자동 화면 잠금

화면 보호기 설정 의무화

모니터 보안 필름 설치(필요 시)

5.3.3 문서 관리

문서 보안 등급에 따른 취급 지침 준수

중요 문서 전용 보안 캐비닛 사용

문서 파쇄기 비치 및 사용 의무화

공용 프린터 보안 인쇄 기능 활용

5.4 장비 보안

5.4.1 장비 배치 및 보호

중요 장비는 접근 통제된 구역에 배치

수해, 화재, 전자기 간섭으로부터 보호

전원 및 통신 케이블 보호

장비 정기 점검 및 유지보수

5.4.2 장비 반출입 관리

장비 반출입 승인 절차 수립

반출입 장비 등록 및 기록

외부 반출 장비의 데이터 보호 조치

반입 장비의 보안 검사

5.4.3 저장매체 관리

저장매체 등록 및 관리 대장 유지

중요 데이터 저장 시 암호화 적용

불필요한 저장매체 안전 폐기

재사용 저장매체의 완전 삭제 확인

6. 접근 통제

6.1 접근통제 정책

6.1.1 기본 원칙

최소 권한의 원칙: 업무 수행에 필요한 최소한의 권한만 부여

알 필요성의 원칙: 업무상 알아야 할 필요가 있는 정보에만 접근 허용

직무 분리의 원칙: 중요 업무의 여러 부분을 한 사람이 담당하지 않도록 분리

기본 거부의 원칙: 명시적으로 허용되지 않은 접근은 모두 차단

6.1.2 접근통제 모델

역할 기반 접근 통제(RBAC) 적용

직무/직책에 따른 역할 정의

역할별 접근 권한 매트릭스 관리

예외적 권한 부여 시 별도 승인 및 기한 설정

6.1.3 접근통제 검토

분기별 사용자 계정 및 권한 검토

미사용 계정 및 과도한 권한 식별

직무 변경에 따른 권한 조정

검토 결과 문서화 및 조치

6.2 사용자 접근 관리

6.2.1 사용자 등록 및 권한 부여

공식적인 사용자 등록 및 해지 절차

고유 사용자 ID 부여 원칙

권한 부여 시 관리자 및 부서장 승인

특별 권한 계정의 별도 관리

6.2.2 권한 검토 및 변경

정기적 사용자 접근 권한 검토(분기별)

인사 변동(승진, 부서이동, 퇴직 등)에 따른 권한 조정

휴직자 계정 일시 중지

퇴직자 계정 즉시 비활성화

6.2.3 특별 권한 관리

관리자 권한 최소화 및 제한적 부여

관리자 계정 사용 내역 상세 기록

관리자 권한 작업 시 이중 승인 적용

응급 상황용 계정의 안전한 보관 및 사용 기록

6.3 패스워드 관리

6.3.1 패스워드 정책

최소 길이: 10자 이상

복잡성: 대문자, 소문자, 숫자, 특수문자 중 3종류 이상 조합

유효기간: 90일

이력 관리: 최근 5개 패스워드 재사용 금지

잠금 정책: 5회 연속 실패 시 30분 계정 잠금

6.3.2 패스워드 생성 및 변경

초기 패스워드 임시 발급 및 최초 로그인 시 변경 강제

패스워드 변경 시 기존 패스워드 확인

패스워드 만료 전 알림 제공(14일, 7일, 3일 전)

패스워드 변경 이력 기록

6.3.3 패스워드 보호

패스워드 암호화 저장

화면에 패스워드 마스킹 처리

전송 중 패스워드 암호화

패스워드 공유 금지 정책

6.4 네트워크 접근 통제

6.4.1 네트워크 분리

업무망과 인터넷망 분리

중요 시스템 네트워크 별도 분리

DMZ 구성 및 관리

무선 네트워크 분리

6.4.2 네트워크 접근 제어

IP 기반 접근 통제

MAC 주소 기반 접근 통제

NAC(Network Access Control) 시스템 운영

비인가 장치 접속 차단

6.4.3 원격 네트워크 접근

VPN을 통한 암호화된 접속만 허용

원격 접속 사용자 인증 강화

원격 접속 세션 타임아웃 설정(30분)

원격 접속 로그 기록 및 모니터링

6.5 운영체제 접근 통제

6.5.1 안전한 로그온 절차

로그온 정보 최소 표시

로그온 실패 시 구체적 오류 메시지 제한

로그온 시도 제한 및 지연

마지막 로그온 정보 표시

6.5.2 시스템 유틸리티 통제

시스템 유틸리티 사용 제한

관리자 권한 필요 유틸리티 통제

유틸리티 사용 로그 기록

불필요한 유틸리티 제거

6.5.3 세션 관리

비활성 세션 자동 종료(15분)

동시 로그온 제한

중요 작업 수행 시 재인증

세션 하이재킹 방지 조치

7. 시스템 개발 및 유지보수 보안

7.1 보안 요구사항 정의

7.1.1 보안 요구사항 식별

시스템 개발 초기 단계에서 보안 요구사항 정의

법적, 규제적 요구사항 반영

비즈니스 보안 요구사항 식별

위험 평가 결과 기반 보안 요구사항 도출

7.1.2 보안 요구사항 명세

기능적 보안 요구사항 명세

비기능적 보안 요구사항 명세

보안 통제 요구사항 문서화

요구사항 추적성 확보

7.1.3 보안 요구사항 검토

보안 요구사항 적정성 검토

이해관계자 검토 및 승인

보안 요구사항 변경 관리

요구사항 구현 가능성 평가

7.2 안전한 개발 환경

7.2.1 개발 환경 보호

개발 환경과 운영 환경 분리

개발 환경 접근 통제

개발 서버 보안 강화

개발 데이터 보호

7.2.2 소스 코드 관리

소스 코드 버전 관리 시스템 사용

코드 변경 이력 추적

코드 접근 권한 관리

코드 백업 및 복구 절차

7.2.3 개발자 보안

개발자 보안 교육

안전한 코딩 가이드라인 제공

개발자 계정 관리

개발 도구 보안 설정

7.3 시스템 개발 생명주기 보안

7.3.1 설계 단계 보안

보안 아키텍처 설계

위협 모델링 수행

보안 설계 검토

설계 문서 보안 관리

7.3.2 구현 단계 보안

시큐어 코딩 적용

코드 품질 및 보안 점검

코드 리뷰 수행

알려진 취약점 예방

7.3.3 테스트 단계 보안

보안 기능 테스트

침투 테스트

취약점 스캔

부하 테스트

7.3.4 배포 단계 보안

안전한 배포 절차

운영 환경 이관 통제

배포 전 최종 보안 점검

배포 후 모니터링

7.4 시스템 변경 관리

7.4.1 변경 요청 및 승인

공식적인 변경 요청 절차

변경 영향 분석

보안 영향 평가

변경 승인 권한 체계

7.4.2 변경 구현 및 테스트

변경 사항 구현

변경 전 백업

변경 후 테스트

보안 영향 확인

7.4.3 변경 문서화 및 추적

변경 내용 상세 기록

변경 이력 관리

변경 관련 문서 업데이트

변경 결과 보고

8. 운영 보안

8.1 운영 절차 및 책임

8.1.1 운영 절차 문서화

주요 시스템 운영 절차 문서화

정기 점검 및 유지보수 절차

장애 대응 절차

백업 및 복구 절차

8.1.2 운영 책임 할당

시스템별 운영 책임자 지정

책임과 권한 명확화

업무 인수인계 절차

비상 연락망 유지

8.1.3 변경 관리

변경 관리 절차 수립

변경 요청 및 승인 프로세스

변경 영향 평가

변경 후 검증

8.1.4 용량 관리

시스템 자원 모니터링

용량 계획 수립

성능 병목 현상 예방

용량 한계 도달 시 대응 계획

8.2 백업 관리

8.2.1 백업 정책

백업 대상 및 주기 정의

백업 유형(전체, 증분, 차등)

백업 보관 기간

백업 매체 관리

8.2.2 백업 절차

자동화된 백업 시스템 구축

백업 일정 및 방법

백업 로그 기록

백업 완료 확인

8.2.3 백업 테스트 및 복구

정기적 복구 테스트(분기 1회)

복구 절차 문서화

복구 소요시간 측정

복구 결과 검증

8.2.4 오프사이트 백업

중요 데이터 오프사이트 백업

오프사이트 보관 장소 보안

오프사이트 백업 이송 보안

재해 시 오프사이트 백업 접근 절차

8.3 로그 관리 및 모니터링

8.3.1 로그 기록

로그 기록 대상 및 항목

로그 형식 및 내용

로그 시간 동기화(NTP 서버 활용)

로그 저장 공간 관리

8.3.2 로그 보호

로그 접근 통제

로그 무결성 보장

로그 백업 및 보관

로그 위변조 방지 대책

8.3.3 로그 모니터링

실시간 모니터링 체계

이상 징후 탐지 규칙

경보 발생 및 대응 절차

정기 로그 검토(주 1회)

8.3.4 로그 분석 및 보고

로그 분석 도구 활용

주기적 분석 보고서 작성

보안 이벤트 상관관계 분석

분석 결과 기반 보안 개선

8.4 악성코드 통제

8.4.1 악성코드 예방

바이러스 백신 설치 및 실시간 감시

정기적인 전체 시스템 검사(주 1회)

백신 엔진 및 패턴 자동 업데이트

이동식 저장매체 자동 검사

8.4.2 사용자 인식 제고

악성코드 위험 및 예방법 교육

의심스러운 이메일 첨부파일 처리 지침

불명확한 출처의 소프트웨어 설치 금지

악성코드 감염 징후 인지 및 보고 방법

8.4.3 악성코드 대응

악성코드 감염 의심 시 대응 절차

감염 시스템 격리

악성코드 제거 및 시스템 복구

감염 원인 분석 및 재발 방지

9. 보안사고 관리

9.1 보안사고 대응 계획

9.1.1 보안사고 정의

보안사고 유형 및 심각도 분류

보안사고 판단 기준

보안 이벤트와 보안사고 구분

보안사고 예시

9.1.2 대응 체계

보안사고 대응팀(CERT) 구성

역할 및 책임 정의

비상 연락망 구축

외부 기관 협조 체계

9.1.3 대응 절차

탐지 및 보고

평가 및 결정

대응 및 복구

사후 관리

9.2 보안사고 보고

9.2.1 내부 보고

보안사고 발견 시 보고 절차

보고 내용 및 양식

보고 경로 및 시간

긴급 보고 체계

9.2.2 외부 보고

외부 보고 대상 사고 기준

관련 기관 보고 절차

고객 및 파트너사 통지 기준

언론 대응 절차

9.2.3 보고서 작성

초기 보고서 작성

중간 경과 보고서

최종 분석 보고서

보고서 승인 및 배포

9.3 보안사고 대응 및 복구

9.3.1 초기 대응

사고 현장 보존

증거 수집

피해 확산 방지

초기 분석

9.3.2 사고 분석

사고 원인 및 경로 분석

영향 범위 파악

피해 규모 평가

추가 위험 요소 식별

9.3.3 복구 활동

시스템 복구 우선순위 결정

정상 운영 복구 절차

데이터 복원

복구 결과 검증

9.3.4 피해 최소화

추가 피해 방지 조치

임시 대체 시스템 운영

업무 연속성 확보

이해관계자 커뮤니케이션

9.4 보안사고 사후 분석

9.4.1 사고 검토

사고 전체 과정 검토

대응 활동 평가

문제점 및 개선사항 도출

재발 방지 대책 수립

9.4.2 교훈 도출

사고 원인 및 배경 분석

유사 사고 예방을 위한 교훈

보안 정책 및 절차 개선점

교육 및 인식 제고 방안

9.4.3 개선 활동

보안 통제 강화

정책 및 절차 업데이트

보안 인식 교육 강화

모니터링 체계 개선

10. 업무 연속성 관리

10.1 업무 연속성 계획

10.1.1 업무영향분석

핵심 업무 프로세스 식별

업무 중단 시 영향 평가

복구 우선순위 설정

목표 복구 시간(RTO) 및 목표 복구 시점(RPO) 정의

10.1.2 연속성 전략

예방 전략

대응 전략

복구 전략

검증 전략

10.1.3 연속성 계획 수립

역할 및 책임 정의

비상 연락망 구축

대체 사업장 준비

필수 자원 확보 계획

10.2 재해복구 계획

10.2.1 재해복구 전략

시스템 및 데이터 백업 전략

대체 시스템 구축 방안

복구 우선순위 및 절차

복구 담당자 지정 및 교육

10.2.2 복구 시설 및 장비

대체 사업장 선정 및 준비

필수 IT 장비 및 소프트웨어 확보

통신 및 네트워크 대체 방안

복구에 필요한 문서 및 자료 준비

10.2.3 복구 절차

재해 선언 기준 및 절차

복구팀 소집 및 역할 분담

단계별 복구 활동

정상 운영 복귀 판단 기준 및 절차

10.2.4 외부 의존성 관리

주요 협력업체 및 서비스 제공자 식별

외부 서비스 중단 시 대응 방안

협력업체 재해복구 계획 검토

대체 공급자 확보 방안

10.3 업무 연속성 테스트

10.3.1 테스트 계획

테스트 유형 및 범위 정의

테스트 시나리오 개발

테스트 일정 및 참여자 선정

테스트 목표 및 성공 기준 설정

10.3.2 테스트 실행

문서 검토(Desk Check)

모의 훈련(Walkthrough)

시뮬레이션 테스트

전체 복구 테스트

10.3.3 테스트 결과 평가

목표 달성 여부 평가

문제점 및 개선사항 식별

계획 및 절차 업데이트

테스트 결과 보고 및 공유

10.3.4 정기적 검토 및 갱신

연 1회 이상 정기 테스트 실시

조직 변경 시 계획 검토 및 갱신

IT 환경 변화에 따른 계획 조정

테스트 결과 반영한 지속적 개선

11. 준거성

11.1 법적 요구사항 식별

11.1.1 관련 법규 식별

개인정보 보호법

정보통신망 이용촉진 및 정보보호 등에 관한 법률

산업기술의 유출방지 및 보호에 관한 법률

전자금융거래법

기타 관련 법규 및 규제

11.1.2 법적 요구사항 분석

법규별 주요 요구사항 분석

회사 업무와의 관련성 검토

법규 준수를 위한 필요 조치 식별

법규 미준수 시 위험 평가

11.1.3 법규 변화 모니터링

법규 개정 동향 정기 모니터링

유관 기관 공지사항 확인

법률 자문 활용

법규 변경 시 대응 계획 수립

11.1.4 준거성 평가

정기적 준거성 평가 실시(연 1회)

법적 요구사항 준수 여부 점검

미비점 식별 및 개선 조치

준거성 평가 결과 보고

11.2 개인정보 보호

11.2.1 개인정보 처리 원칙

개인정보 수집 제한 및 동의 획득

목적 외 이용 금지

안전한 관리 및 보호

정보주체 권리 보장

11.2.2 개인정보 처리방침

개인정보 처리방침 수립 및 공개

법적 필수 항목 포함

정기적 검토 및 갱신

변경 시 고지 절차

11.2.3 개인정보 안전성 확보 조치

관리적 보호조치

기술적 보호조치

물리적 보호조치

개인정보 유출 대응 체계

11.2.4 개인정보 처리 위탁 관리

수탁자 선정 시 보안 평가

위탁 계약 시 보안 조항 포함

수탁자 보안 관리 감독

위탁 현황 관리 및 공개

11.3 정보보안 검토 및 감사

11.3.1 내부 보안 점검

정기 보안 점검 계획 수립

점검 항목 및 체크리스트 개발

점검 실시 및 결과 기록

발견 사항 조치 및 후속 점검

11.3.2 정보보안 감사

연간 감사 계획 수립

감사 범위 및 방법론 정의

감사 수행 및 증거 수집

감사 결과 보고 및 개선 조치

11.3.3 취약점 진단

정기적 취약점 진단 실시

주요 시스템 대상 침투 테스트

발견된 취약점 위험도 평가

취약점 조치 및 검증

11.3.4 제3자 보안 평가

필요시 외부 전문기관 평가 의뢰

평가 범위 및 방법 합의

평가 결과 검토 및 수용

개선 권고사항 이행 계획 수립

12. 부록

12.1 정보보안 관련 서식

12.1.1 정보보안 서약서

임직원 정보보안 서약서

외부인력 비밀유지서약서

퇴직자 보안서약서

정보시스템 접근 신청서