[문서 번호: SEC-2025-001]

[시행 일자: 2025. 01. 01]

보안 및 IT 운영 통합 규정

---

1. 개인정보 내부 관리 계획

(본 계획은 '개인정보 보호법' 제29조에 의거하여 개인정보의 안전성 확보를 위해 수립된 법적 필수 규정입니다.)

제1장 총칙

제1조 (목적)

본 계획은 회사가 처리하는 고객 및 임직원의 개인정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적·관리적·물리적 보호 조치를 규정함을 목적으로 한다.

제2조 (개인정보 보호책임자, CPO)

회사는 개인정보 보호 업무를 총괄하거나 업무 처리를 지휘·감독하기 위하여 개인정보 보호책임자(CPO)를 지정하며, CPO는 개인정보 보호 계획의 수립 및 시행, 실태 점검 등의 업무를 수행한다.

제2장 안전성 확보 조치

제3조 (접근 권한의 관리)

1. 개인정보처리시스템에 접근할 수 있는 권한은 업무 수행에 필요한 최소한의 범위로 차등 부여한다.
2. 전보, 퇴직 등 인사이동이 발생한 경우 지체 없이 접근 권한을 변경 또는 말소한다.

제4조 (암호화 조치)

1. 고유식별정보(주민등록번호, 여권번호 등), 비밀번호, 바이오 정보는 반드시 암호화하여 저장한다.
2. 업무용 컴퓨터 또는 모바일 기기에 개인정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 등을 사용하여야 한다.

제5조 (접속 기록의 보관)

개인정보취급자가 개인정보처리시스템에 접속한 기록은 최소 1년 이상(5만 명 이상의 정보 주체 또는 고유식별정보 처리 시 2년 이상) 보관 및 관리하며, 월 1회 이상 점검한다.

제6조 (교육)

개인정보취급자를 대상으로 연 1회 이상 개인정보 보호에 관한 정기 교육을 실시한다.

---

2. 정보보안 규정

제1장 정보의 분류 및 취급

제1조 (정보 등급 분류)

회사의 문서는 중요도에 따라 다음과 같이 분류하여 관리한다.

1. **극비(Top Secret):** 유출 시 회사에 치명적인 손해를 끼칠 수 있는 핵심 기밀 (경영 전략, 미공개 기술 등).
2. **대외비(Confidential):** 회사 내부에서만 공유되어야 하며 외부 공개가 제한된 정보 (인사 정보, 영업 실적 등).
3. **일반(Public):** 외부에 공개되어도 무방한 정보.

제2조 (정보의 반출)

1. 업무상 필요에 의해 중요 정보를 외부로 반출(이메일 발송, USB 저장, 출력 등)할 경우, 사전에 부서장 및 보안 담당자의 승인을 득해야 한다.
2. 퇴사 시 업무와 관련된 모든 자료는 반납 및 파기하여야 하며, 무단 반출 시 민형사상 책임을 진다.

제2장 계정 및 비밀번호 관리

제3조 (비밀번호 설정)

1. 비밀번호는 영문, 숫자, 특수문자를 포함하여 8자리 이상(또는 10자리 이상)으로 설정해야 한다.
2. 연속된 숫자, 생년월일, 전화번호 등 유추하기 쉬운 비밀번호 사용을 금지한다.
3. 비밀번호는 최소 3개월(분기)마다 1회 이상 변경해야 한다.

---

3. IT 자산 및 소프트웨어 사용 가이드

제1장 하드웨어 및 네트워크

제1조 (자산의 사용)

회사에서 지급된 IT 자산(PC, 노트북, 모니터 등)은 업무 목적으로만 사용하여야 하며, 임의로 부품을 분해, 교체, 반출해서는 안 된다.

제2조 (네트워크 사용)

1. 사내 네트워크를 통해 업무와 무관한 과도한 트래픽 유발 행위(P2P, 스트리밍, 대용량 파일 전송 등)를 금지한다.
2. 인가받지 않은 사설 공유기(AP)를 사내망에 무단 연결하여 사용하는 것을 엄격히 금지한다.

제2장 소프트웨어 라이선스

제3조 (정품 사용 의무)

1. 회사는 정품 소프트웨어 사용을 원칙으로 하며, 불법 복제 소프트웨어(Crack, Keygen 등)의 설치 및 사용을 엄격히 금지한다.
2. 회사가 승인하지 않은 소프트웨어(게임, 메신저, 주식 HTS 등)를 임의로 설치하여 발생하는 보안 사고 및 법적 책임은 사용자 본인에게 있다.

제4조 (점검 및 감사)

IT 관리 부서는 소프트웨어 라이선스 관리 및 보안 점검을 위해 불시에 임직원의 PC를 점검할 수 있으며, 사용자는 이에 협조하여야 한다.

---

4. 재택 및 원격 근무 보안 가이드

제1장 접속 및 환경 보안

제1조 (보안 접속)

1. 외부에서 사내 시스템에 접속할 때는 회사가 지정한 가상사설망(VPN) 또는 원격 접속 솔루션(VDI)을 통해서만 접속해야 한다.
2. 보안이 취약한 개방형 공용 Wi-Fi(카페, 공항 등 비밀번호가 없는 네트워크) 사용을 금지하며, 부득이한 경우 모바일 테더링을 권장한다.

제2장 단말기 보안

제2조 (보안 조치)

원격 근무에 사용하는 기기(개인 PC 포함)는 다음의 보안 조치를 적용해야 한다.

1. 운영체제(OS) 및 소프트웨어 최신 보안 패치 적용.
2. 백신 프로그램 설치 및 실시간 감시 기능 활성화.
3. 부팅 및 화면 보호기 암호 설정 (5분 이상 미사용 시 자동 잠금).

제3장 데이터 보호

제3조 (정보 유출 방지)

1. 업무 관련 파일은 사내 서버(클라우드, 그룹웨어 등)에서만 작업 및 저장해야 하며, 개인 PC의 로컬 디스크나 개인 USB에 저장하는 것을 금지한다.
2. 공공장소나 타인이 있는 공간에서 근무 시 화면 보안 필름을 부착하거나, 등 뒤에서 화면이 보이지 않도록 좌석 배치에 유의한다.
3. 화상 회의 시 화면 공유 기능을 사용할 때, 업무와 무관한 민감 정보나 배경이 노출되지 않도록 주의한다.