2. 보안 정책

목적 및 적용 범위

- 본 보안 정책은 우리 회사의 정보 자산과 고객 데이터를 보호하고, 관련 법규를 준수하기 위한 최소한의 행동 수칙을 정하는 것을 목적으로 합니다. 임직원 모두가 알아야 할 보안 지침을 명문화함으로써 기준을 제시하고 보안을 회사 문화의 일부로 정착시키고자 합니다.
- 이 정책은 회사의 모든 임직원, 계약직, 인턴 및 당사와 기밀정보를 취급하는 외부 협력업체 직원까지 포함하여 적용됩니다. 회사가 보유하거나 관리하는 모든 정보시스템(서버, PC, 클라우드 계정 등), 네트워크, 데이터에 본 정책이 미치며, 업무상 사용되는 개인 기기도 일정 범위 내에서 준수 요구사항이 적용됩니다.

법령 및 규제 준수

- 우리 회사는 **개인정보보호법 제29조**에 따른 내부 관리계획을 수립·운영하여 개인정보를 보호합니다. 고객의 개인정보를 취급하는 부서나 직무는 해당 내부관리계획(본 보안 정책 및 세부지침)을 반드시 숙지해야 합니다.
- 정보통신망법, 전자금융거래법 등 업종별 보안 관련 법규를 준수합니다.
- 회사는 정기적으로 법 규제 동향을 모니터링하고 정책을 업데이트하여 기업이 사업 추진 과정에서 자발적으로 관련 법규를 준수하도록 하기 위한 일련의 시스템인 컴플라이언스를 유지합니다.

역할과 책임

- **경영진(CISO/보안담당 임원):** 회사의 최고정보보호책임자로서 전사 보안정책 수립을 승인하고 자원 배분을 책임집니다. 연 1회 이상 보안 리스크를 검토하고 필요한 조치를 지시합니다.
- **보안 담당자/팀:** 일상적인 보안 운영을 관장하며, 정책 준수 여부 모니터링, 보안 교육 실시, 사고 대응 계획 수립 등의 업무를 맡습니다. 신규 입사자 보안교육 및 연례 보안 점검을 주관합니다.
- **IT 관리자:** 사내 시스템 계정 발급/폐기, 권한 관리, 패치 적용, 백업 등 기술적 보안 통제를 실무 수행합니다. 보안 이벤트 발생 시 신속히 대응하고 보안팀에 보고합니다.
- **일반 임직원:** 보안 정책을 준수하고, 의심스러운 상황이나 사고 발견 시 지체 없이 보안 담당자에게 보고할 책임이 있습니다. 모든 직원은 보안 담당자가 아니라도 자신의 역할 범위 내에서 보안을 실천해야 합니다.

접근 통제 및 계정 관리

- **인증 정보 관리:** 모든 사내 시스템은 각 사용자별 개인 계정을 사용하며, 공유 ID를 사용하지 않습니다. 신규 입사자에게 필요한 시스템 계정을 발급하고, 퇴사자의 계정은 즉시 권한 회수 및 비활성화합니다.
- **비밀번호 규칙:** 안전한 패스워드 정책을 시행합니다. 비밀번호는 최소 12자 이상이어야 하며 대문자, 소문자, 숫자, 특수문자를 각각 1자 이상 포함해야 합니다. 비밀번호는 90일마다 주기적 변경을 권고하고 동일 비밀번호를 재사용하지 않습니다. 중요한 시스템의 경우 최근 5개 이전 비밀번호와 다른 값으로 변경해야 합니다.
- **다중인증(MFA):** 관리콘솔, 개발서버 등 중요 시스템의 관리자 권한에는 원칙적으로 2단계 인증(MFA)을 적용합니다. 이메일, Slack 등 업무용 도구도 MFA 사용을 강력히 권장하며, 특히 외부에서 접속할 수 있는 서비스는 반드시 MFA를 활성화합니다.
- 접근 권한 원칙: 최소 권한의 원칙을 준수하여 업무에 필요한 최소한의 접근권한만 부여합니다. 부서 이동이나 역할 변경 시 권한을 신속히 변경하며, 사용하지 않는 권한은 즉시 회수합니다. 분기 1회 이상 모든 계정의 권한을 리뷰하여 과도한 권한이 부여된 계정이 없는지 점검합니다.

데이터 보안

- **민감정보 및 개인 데이터:** 고객 개인정보나 회사의 기밀자료는 암호화하여 저장하고 전송합니다. 개인정보 파일은 지정된 암호화 폴더나 DB에만 보관하며, 이메일·메신저 등으로 공유 시 비밀번호 설정 등 보호조치를 취합니다.
- **파일 및 문서 관리:** 사내 문서는 중앙 관리되는 클라우드 스토리지에 저장하며, 인가되지 않은 외부 공유를 금지합니다. 중요 문서에는 열람 권한 설정을 통해 필요 인력만 접근하도록 합니다. 용도 외 목적으로 회사 데이터를 무단 반출하거나 개인 USB 등 외부 매체에 저장하는 것을 금지합니다.
- **소스코드 및 레포지토리:** 회사의 소스코드는 승인된 Git 리포지토리로 관리되고 접근 권한은 개발팀으로 제한됩니다. 코드 저장소에 데이터베이스 비밀번호, API 키 등 비밀정보를 하드코딩 금지하며, 이러한 정보는 별도 안전한 저장소에 보관합니다. 레포지토리에 변경이 발생하면 리뷰 프로세스를 통해 코드에 비밀정보가 포함되지 않았는지 검토합니다.
- **백업 및 복구:** 중요한 데이터베이스 및 파일 서버는 정기 백업을 시행합니다. 백업 파일은 본 서버와 분리된 별도 저장소에 저장하고, 백업 데이터에 대한 암호화 및 무결성 검증을 수행합니다. 정기적으로 복구 테스트를 실시하여, 실제 장애 시 데이터를 복원할 수 있음을 확인합니다.

업무 기기 및 환경

- **PC 보안:** 모든 직원의 업무용 PC에는 회사에서 승인한 안전한 OS와 소프트웨어만 설치해야 합니다. 운영체제 및 소프트웨어 업데이트를 항상 최신으로 유지하고, 백신/안티멀웨어 프로그램을 상시 실행합니다. PC에는 로그인 비밀번호를 설정하고 15분 이하의 비사용 시간 후 자동으로 화면이 잠기도록 합니다.
- **모바일 기기:** 회사 이메일 등 업무 용도로 휴대폰, 태블릿 등을 사용할 경우 화면잠금을 설정해야 합니다. 업무 관련 앱 사용 모바일 기기는 분실 시 지체 없이 보고하여 원격으로 데이터를 삭제하는 등 조치를 취합니다.
- **출입 및 물리적 보안:** 사무실 출입권한은 사원증으로 관리하며, 외부인은 출입통제구역에 임직원 동행 하에 방문해야 합니다. 퇴근 시 책상 위에 중요 문서를 두지 않고, 종이

문서는 파쇄기를 통해 폐기합니다. 회사 자산을 외부로 반출할 경우 사전 승인 및 기록을 남깁니다.

- **클라우드 및 외부 서비스:** 회사가 사용하는 클라우드 서비스의 접근 권한은 최소한으로 관리하고, IAM 정책을 통해 불필요한 서비스 접근을 막습니다. 클라우드 자산 설정 변경 시 Logging을 활성화하여 추적하며, S3 버킷 등은 퍼블릭 접근 차단을 기본으로 합니다. 외부 SaaS 도구도 가능하면 SSO로 통합해 관리하고, 사용 현황을 정기 점검합니다.

보안 교육

- 모든 임직원은 **연 1회 이상 보안 교육**을 이수해야 합니다. 교육 내용에는 개인정보보호법 준수, 사회공학적 해킹 사례, 회사 보안규정, 사고 시 대응 요령 등이 포함됩니다.
- 신규 입사자에 대해서는 입사 첫 주 **온보딩 보안 세션**을 통해 회사 보안정책의 핵심을 전달합니다. 특히 개발직군 신입의 경우 코드 보안, 데이터 접근, 인프라 키 관리 등에 대한 별도 세션을 추가로 진행합니다.

사이버 사고 대응

- **대응 팀 구성:** 심각한 보안 사고인 경우 사고대응 TF를 구성합니다. TF는 보안담당자, 관련 시스템 담당 엔지니어, 법무담당, 경영진 대표 등으로 이루어지며, 각자의 역할을 사전에 정의해 둡니다.
- **사고 조사 및 조치:** 사고 발생 시 시스템 로그, 계정 사용 내역 등을 확보하여 원인을 규명합니다. 추가 피해 확산을 막기 위해 침해 시스템 격리, 계정 차단 등의 긴급 대응조치를 취합니다. 원인 분석 후에는 재발 방지 대책을 수립하고 관련 부서에 교육합니다.
- **보고 및 통지:** 법령상 요구되는 경우 관계기관 및 정보주체 통지를 진행합니다. 예를 들어 개인정보 유출 사고 시 72시간 이내 KISA 등 관계기관에 신고하고 피해 고객에게 개별 통지합니다. 이러한 외부 보고는 법무담당과 협의하여 진행하며, 보고 내용에는 유출된 정보 항목, 대응 조치, 상담 창구 등을 포함합니다.

위반 시 제재

- 보안 정책을 고의 또는 중대한 과실로 위반하여 회사에 손해를 끼친 경우, 회사는 해당 직원에 대해 인사 조치(경고, 징계, 손해배상 청구 등)를 취할 수 있습니다. 예를 들어, 인가되지 않은 외부로 회사 데이터를 반출하거나 고객 정보를 유출한 경우 지체 없이 계정 접속을 차단하고 진상을 조사합니다. 중대한 위반자는 징계위원회 회부 및 민·형사상 책임까지 물을 수 있습니다.
- 경미한 위반의 경우 교육 기회를 부여하고 시정을 요구하되, 반복 발생 시 엄중 조치합니다. 모든 제재 조치는 사전에 명시된 절차에 따라 공정하게 이루어지며, 징계 대상자에게도 소명 기회가 제공됩니다.