# 사고예방지침

**제1조 (목적)**

본 지침은 회사의 정보자산, 물리적 자산 및 인적 자원을 보호하고, 업무 수행 과정에서 발생할 수 있는 사고를 사전에 예방하기 위한 기준과 절차를 정함으로써 안전하고 신뢰성 있는 업무환경을 유지함을 목적으로 한다.

**제2조 (적용 범위)**

① 본 지침은 회사의 모든 임직원, 계약직, 파견직, 용역직, 인턴 및 업무상 회사 시스템·시설에 접근하는 외부 협력업체 직원에게 적용한다.

② 본 지침은 다음 각 호의 사항을 포함한다.

1. 정보보안 및 시스템 접근 통제
2. 물리적 보안 및 출입 통제
3. 퇴직·퇴사자 권한 처리
4. 사고 발생 시 보고 및 대응 절차
5. 미준수 시 제재 및 후속조치

**제3조 (정의)**

본 지침에서 사용하는 용어의 정의는 다음과 같다.

1. '정보자산'이라 함은 회사가 보유·관리하는 데이터, 소프트웨어, 하드웨어, 네트워크 인프라, 클라우드 자원 및 이에 준하는 일체의 IT 자산을 말한다.

2. '사고'라 함은 정보자산의 유출·훼손·파괴, 시스템 침해, 물리적 손상, 무단 접근 또는 이에 준하는 사건으로서 회사의 업무 연속성 또는 보안에 위협을 가하는 모든 상황을 말한다.

3. '접근 권한'이라 함은 회사의 내부 시스템, 데이터베이스, 클라우드 서비스, 협업 도구, 사내 네트워크 및 물리적 시설에 대한 접근·사용 권한을 말한다.

4. '퇴직·퇴사자'라 함은 사직, 해고, 계약 만료, 파견 종료, 용역 종료 등 사유를 불문하고 회사와의 고용 또는 위탁 관계가 종료된 자를 말한다.

5. '주관사업부'라 함은 본 지침의 운용을 담당하는 준법감사사업부를 말한다.

**제4조 (책임 및 역할)**

① 각 사업부장은 소속 사업부원이 본 지침을 준수하도록 관리·감독할 책임을 진다.

② 인사담당 사업부는 임직원의 입사·전보·퇴직 정보를 지체 없이 주관사업부 및 IT 담당 사업부에 통보하여야 한다.

③ IT 담당 사업부는 접근권한의 부여·변경·회수 업무를 실무적으로 수행하며, 권한 현황을 주기적으로 주관사업부에 보고하여야 한다.

④ 주관사업부는 본 지침의 이행 여부를 점검하고, 미준수 사항에 대하여 시정 요구 및

후속조치를 수행한다.

**제5조 (정보보안 일반 수칙)**

① 임직원은 업무 목적 외로 회사의 정보자산을 사용하거나 외부에 제공하여서는 아니 된다.

② 임직원은 업무용 계정의 비밀번호를 타인과 공유하거나 제3자가 추정하기 쉬운 형태로 설정하여서는 아니 된다. 비밀번호는 회사가 정한 주기에 따라 변경하여야 한다.

③ 임직원은 업무용 단말기를 장시간 자리를 비울 때 반드시 잠금 상태로 전환하여야 하며, 개인 소유 기기를 통한 사내 시스템 접근 시 회사가 정한 보안 정책을 준수하여야 한다.

④ 임직원은 검증되지 않은 외부 소프트웨어, 파일 또는 링크를 업무용 단말기에 설치하거나 실행하여서는 아니 된다.

⑤ 클라우드 서비스, 외부 메신저 등 비인가 채널을 통한 사내 자료 전송은 원칙적으로 금지하며, 불가피한 경우 사전에 소속 사업부장의 승인을 받아야 한다.

⑥ 소스코드, 고객 데이터, 계약 정보 등 민감 정보는 회사가 지정한 저장소 이외의 장소에 보관하여서는 아니 된다.

**제6조 (시스템 접근 통제)**

① 시스템 접근권한은 업무 수행에 필요한 최소 범위 내에서 부여함을 원칙으로 하며, 업무 변경 시 즉시 재검토하여야 한다.

② 관리자 권한은 해당 업무의 직접 담당자에 한하여 부여하며, 주관사업부의 승인을 거쳐야 한다.

③ 외부 협력업체 직원에 대한 접근권한은 계약 기간 내로 한정하며, 계약 만료 즉시 회수하여야 한다.

④ IT 담당 사업부는 접근권한 부여·변경·회수 내역을 기록·보관하며, 주관사업부의 요청 시 즉시 제출하여야 한다.

⑤ 접근권한 현황에 대한 정기 검토는 반기 1회 이상 실시하며, 그 결과를 주관사업부에 보고하여야 한다.

**제7조 (퇴직·퇴사자 권한 처리)**

① 인사담당 사업부는 임직원의 퇴직·퇴사가 확정된 즉시(늦어도 퇴직일 전일까지) IT 담당 사업부 및 주관사업부에 해당 사실을 통보하여야 한다.

② IT 담당 사업부는 퇴직·퇴사자의 접근권한을 퇴직일 당일 업무 종료 시각을 기준으로 즉시 회수하여야 하며, 다음 각 호의 조치를 이행하여야 한다.

1. 사내 시스템(ERP, 그룹웨어, 인사시스템 등) 계정 비활성화 및 삭제
2. 클라우드 서비스(이메일, 협업 도구, 저장소 등) 계정 접근 차단
3. VPN 및 원격접속 권한 즉시 회수
4. 출입증, 보안카드, 물리적 열쇠 등 물리적 접근 수단 반납 확인
5. 개인 소유 기기에 설치된 업무용 앱·데이터의 원격 삭제 또는 반납 처리
6. 공유 계정·비밀번호 등 해당 직원이 알고 있는 인증정보의 즉시 변경

③ 퇴직·퇴사자는 재직 중 취득한 회사의 정보자산, 소스코드, 고객 정보, 영업 비밀 등 일체의 자료를 퇴직일 이전에 반납하여야 하며, 퇴직 후 이를 보유·사용·유출하여서는 아니 된다.

④ 인사담당 사업부는 퇴직·퇴사자로부터 정보보안 서약서를 징구하여야 하며, 주관사업부는 이의 이행 여부를 확인한다.

⑤ IT 담당 사업부는 퇴직·퇴사자의 권한 회수 완료 사실을 주관사업부에 서면으로 보고하여야 한다. 권한 회수가 퇴직일로부터 3영업일을 초과하는 경우 그 사유를 명시하여야 한다.

**제8조 (물리적 보안 및 출입 통제)**

① 회사 시설에 대한 출입은 인가된 임직원 및 방문자에 한하며, 미인가자의 출입을 허용하여서는 아니 된다.

② 외부 방문자는 방문 목적, 방문 사업부 및 담당자를 확인한 후 방문증을 패용한 상태에서 담당자의 안내 하에 출입하여야 한다.

③ 서버실, 전산실 등 주요 시설에 대한 출입은 해당 업무 권한을 가진 자에 한하며, 출입 기록을 유지하여야 한다.

④ 임직원은 퇴근 시 보안 구역의 잠금 여부를 확인하여야 하며, 미확인으로 인한 사고 발생 시 귀책 사유가 인정될 수 있다.

⑤ 출입증 분실 시 지체 없이 인사담당 사업부 및 주관사업부에 신고하여야 하며, 분실 출입증은 즉시 무효 처리한다.

**제9조 (사고 예방 교육)**

① 주관사업부는 임직원을 대상으로 연 1회 이상 사고예방 교육을 실시하여야 한다.

② 신규 입사자는 입사 후 1개월 이내에 사고예방 교육을 이수하여야 한다. 단 신규 입사자가 인사담당 사업부에서 실시하는 자체 교육을 이수한 경우에는 본 조에 따른 사고예방교육을 이수한 것으로 본다.

③ 임직원은 회사가 실시하는 피싱 메일 모의훈련, 보안 점검 등 사고 예방 관련 훈련에 성실히 참여하여야 한다.

④ 교육 미이수자 명단은 주관사업부가 관리하며, 반복적으로 교육을 기피하는 경우 소속 사업부장 및 인사담당 사업부에 통보할 수 있다.

**제10조 (사고 발생 시 보고 및 대응)**

① 임직원은 사고 또는 사고 징후를 인지한 즉시 소속 사업부장 및 주관사업부에 보고하여야 한다. 사고를 인지하고도 보고하지 아니하는 경우 은닉으로 간주될 수 있다.

② 주관사업부는 사고 보고를 접수한 즉시 사실관계 확인에 착수하고, 피해 확산 방지를 위한 긴급 대응 조치를 지시할 수 있다.

③ 긴급 대응 조치에는 다음 각 호의 사항이 포함될 수 있다.

1. 관련 시스템의 일시 접속 차단 또는 격리
2. 관련 계정의 즉시 비활성화
3. 관련 자료 및 로그의 보전 조치
4. 관련 임직원에 대한 출입 제한 또는 업무 배제

④ 주관사업부는 사고 대응 결과를 대표이사에게 보고하여야 하며, 재발 방지 대책을 수립 · 시행하여야 한다.

**제11조 (점검 및 감사)**

① 주관사업부는 본 지침의 이행 여부를 확인하기 위하여 정기 또는 수시 점검을 실시할 수 있다.

② 점검 대상 사업부는 주관사업부가 요구하는 자료를 지체 없이 제출하여야 하며, 정당한 사유 없이 제출을 거부하거나 점검을 방해하여서는 아니 된다.

③ 정당한 사유 없이 자료 제출을 거부하거나 점검에 불응하는 경우, 주관사업부는 확보된 자료를 기초로 해당 사업부에 불리하게 사실관계를 추정하여 점검 결론을 도출할 수 있다.

④ 주관사업부는 점검 결과를 기록 · 보관하며, 중대한 미준수 사항이 발견된 경우 대표이사에게 보고하여야 한다.

**제12조 (미준수 시 제재)**

① 본 지침을 위반한 임직원에 대하여 주관사업부장은 다음 각 호의 조치를 건의할 수 있다.

1. 시정 명령 및 경위서 제출 요구
2. 인사위원회 또는 징계위원회 회부
3. 접근권한의 일시 제한 또는 회수
4. 사업부 평가에의 반영 요청
5. 대표이사 직접 보고

② 위반 행위가 중대하거나 반복되는 경우, 관련 법령에 따른 민 · 형사상 책임이 별도로 부과될 수 있다.

③ 소속 사업부장이 소속 사업부원의 위반 사실을 인지하고도 주관사업부에 보고하지 아니한 경우, 해당 사업부장에 대하여도 제1항의 조치를 취할 수 있다.

④ 퇴직 · 퇴사자가 제7조를 위반하여 회사 정보를 보유 · 사용 · 유출한 경우, 주관사업부는 법적 조치를 취할 것을 건의할 수 있다.

**제13조 (이의신청)**

① 주관사업부의 시정 요구 또는 조치 건의에 이의가 있는 임직원 또는 사업부장은 통보일로부터 10일 이내에 구체적인 사유 및 입증자료를 갖추어 서면으로 이의신청을 청구할 수 있다. 이의신청은 1회에 한한다.

② 주관사업부장은 이의신청이 소정 요건을 갖추지 못한 경우 접수하지 아니하거나 각하할 수 있으며, 신규 사실 또는 중대한 오류가 없다고 인정되는 경우 이를 기각한다. 기각 결과에 대하여 재이의를 제기할 수 없다.

③ 이의신청이 이유 있다고 인정되는 때에는 당초 조치 요구를 취소하거나 변경할 수 있다.

**제14조 (준거 기준)**

주관사업부 또는 점검 담당자는 본 지침과 회사의 관계 규정 및 내부절차에 준거하여 업무를 수행한다. 준거해야 할 명백한 규정이 없거나 해석이 모호한 경우에는 관련 법령, 정보보안 국제표준(ISO/IEC 27001 등) 및 합리적인 경영 목적에 입각하여 공정 타당하게 처리한다.

## 부 칙

### 제1조 (시행일)

본 지침은 공표한 날로부터 시행한다. 단 결재권자의 승인이 지연될 경우, 이메일·메신저 등을 통한 업무상 지시 또는 회람이 완료된 시점을 시행일로 간주한다.

### 제2조 (경과조치)

본 지침 시행 전 이미 부여된 접근권한에 대해서는 시행일로부터 1개월 이내에 본 지침의 기준에 따라 재검토하여야 하며, 기준에 부합하지 아니하는 권한은 즉시 조정한다.

### 제3조 (협조 의무)

본 지침의 안정적인 정착을 위하여 시행일로부터 1개월 간을 적응 기간으로 두며, 이 기간 중 발생하는 해석상 이견은 관련 법령 및 정보보안 국제표준에 비추어 주관사업부가 결정한다.