정보보호규정

R-60-GG-01
Ver 2.2
2023.11.3.

주관부서: 정보보호실

개정 이력

Version	일자	개정 내용*	작성자	비고
		-중략-		
V 2.2	2023-11-03	용어변경 (정보보호 최고 책임자 → 정보보호 최고책임자, 영업비밀 → 영업비밀정보) (제 2 조) 적용범위 문구 수정 (제 3 조) 정보보호, 영업비밀정보 추가 (제 4 조) 임직원, 정보보호 주관부서, 회사 역할 분리 (제 8 조) 위치정보관리책임자 신설, 정보보호 조직 → 정보보호전담조직 (제 10 조) 인사사교육팀 → 인사팀 (제 17 조) 문구 수정 (제 32 조) 모바일 출입증 내용 신설 (제 50 조) 문구 수정 (전적인 책임 → 책임) (제 51 조) 업무용 정보통신 수단 내 인공형 인공지능 서비스 사용 시 준수사항 신설 (제 59 조) 사전 보안성 검토 (그룹정보보호위원회 → 정보보호 주관부서) (제 61 조) 파트너사 보안교육 신설 (제 71 조) 프로젝트 자체점검 신설		

*개정 내용: 변경이 발생되는 위치와 변경 내용을 자세히 기록함

목 차

제 1 장 총칙

제 1 조 [목적]

본 정보보호규정(이하 "규정")은 롯데정보통신(이하 "회사")의 정보보호를 위한 최상위 규정으로서, 회사의 정보자산을 안전하고 체계적으로 관리하기 위한 기본방침을 정립하여, 회사의 발전과 대외 신뢰도 향상에 이바지함을 목적으로 한다.

제 2 조 [적용범위]

본 규정은 회사에 소속된 임직원, 자회사 직원, 계약 관계에 있는 파트너사 직원, 회사를 방문하는 모든 외부인뿐만 아니라 회사가 소유, 보유하거나 회사에서 생성된 모든 유무형 자산에 대하여 적용하여야 한다.

제 3 조 [용어의 정의]

본 규정에서 사용하는 용어의 정의는 다음과 같다.

① 정보보호 : 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송수신 되는 정보의 유출, 위•변조, 훼손 등을 방지하기 위하여 관리적, 물리적, 기술적 수단을 강구하는 일체의 행위를 말한다.

② DMZ(Demilitarized Zone) : 기업의 내·외부 네트워크 사이에 일종의 중립 지역이 설치되는 호스트 또는 네트워크를 말한다.

③ 로그 : 정보화 장비 및 네트워크 운영 과정에서 발생하는 모든 내용들이 발생시간 등과 함께 기록된 자료를 말하며, 시스템 운영 내용이 기록된 시스템 로그와 사용자의 활동 내용이 선택적으로 기록되는 사용자 로그로 구별된다.

④ 블루투스 : 휴대폰, 노트북, 이어폰·헤드폰 등의 휴대기기를 서로 연결해 정보를 교환하는 근거리 무선 통신 기술 표준을 말한다.

⑤ 적외선 장치 : 적외선 포트가 내장되어 있어 각종 데이터를 적외선을 통해 무선으로 주고받을 수 있는 장치를 말한다.

⑥ 시리얼 넘버 : 대량으로 생산된 하드웨어나 컴퓨터 소프트웨어에 붙은 일련의 번호를 말한다.

⑦ 쉐어웨어 : 일정 기간 동안 자유롭게 사용하거나 복사할 수 있도록 시장에 공개하고 있는 소프트웨어를 말한다.

⑧ 소스프로그램 : 프로그래밍 언어로 작성한 프로그램을 말한다.

⑨ 파트너사 : IT 운영, 프로젝트(개발, 컨설팅 등), 콜센터, 개인정보 처리 업무 등을 위탁한 업무 수탁자 등을 말한다.

⑩ 모바일 단말 : 회사의 업무 목적으로 사용하는 스마트폰이나 태블릿 PC 등을 말하며 회사에서 업무 목적으로 지급한 법인 명의 또는 소유의 모바일 기기뿐만 아니라 업무 목적으로 사용되는 개인소유의 모바일 기기를 포함한다.

⑪ 개인정보 : 생존하는 개인에 관한 정보로서 성명•주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호•문자•음성•음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다.)를 말한다.

⑫ 영업비밀정보 : 회사가 보유 또는 사실상 보유한 정보로서 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로, 비밀로 관리된 생산 방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보

제 4 조 [역할과 책임]

① 임직원

가. 미션 및 경영 목표를 달성하는데 있어서 정보보호를 반드시 고려해야 한다.

나. 규정 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 유지할 책임이 있다.

다. 회사의 정보자산을 사용함에 있어, 업무 목적상 필요한 범위에서 적합하게 활용·처리해야 하며, 목적 외 용도로 활용해서는 안 된다.

② 정보보호 주관부서

가. 업무상 필요한 최소한의 사람만 정보에 접근할 수 있도록 관리해야 하며, 접근 승인을 받은 자는 해당 정보자산을 사용함과 동시에 보호할 책임을 갖는다.

나. 규정에 정의된 바에 따라 정보보호 책임 및 역할을 정의해야 한다.

다. 임직원의 업무상 필요한 보호 대책을 전사적이고 포괄적인 방식으로 수립·적용해야 하며 정기적으로 재평가해야 한다.

③ 회사

가. 규정에 따른 임직원의 업무 활동에 필요한 적절한 대책과 교육을 수행해야 한다.

제 2 장 정보보호 규정 및 지침 운영

제 5 조 [규정 및 지침 수립]

① 정보보호 규정 수립 시, 그룹의 정보보호규정 및 국내외 유관법령, 규제 등을 반영하여 수립해야 한다.

② 규정의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 명시한 정보보호 지침을 수립할 수 있다.

제 6 조 [승인 및 공표]

① 회사는 제·개정한 정보보호 규정을 최고 경영진의 승인을 득한 후 공표하며, 공표한 날로부터 시행해야 한다.

② 회사는 제·개정한 정보보호 지침을 정보보호 최고책임자의 승인을 득한 후 공표하며, 공표한 날로부터 시행해야 한다.

③ 정보보호 주관부서는 정보보호 규정 및 지침을 전 임직원이 상시 열람할 수 있도록 인쇄물 또는 전자문서 형태로 공표, 게시해야 한다.

제 7 조 [유지 관리]

정보보호 주관부서는 정보보호 규정 및 지침의 타당성과 적합성을 매년 검토하고, 그 결과를 반영해야 한다.

제 3 장 정보보호 조직

제 8 조 [정보보호 조직체계]

① 회사는 정보보호와 관련하여 명확한 방향 제시, 임직원의 참여, 책임의 부여 및 주기적인 검토 등을 통하여 적극적인 지원을 제공해야 한다.

② 회사는 다음의 역할을 원활히 수행할 수 있도록 정보보호 지식과 경험을 갖춘 임직원을 지정하여야 한다.

1. 정보보호 최고책임자 (CISO)
2. 개인정보 보호책임자 (CPO)
3. 위치정보관리책임자
4. 정보보호 관리자
5. 개인정보보호 관리자
6. 관리, 물리, 기술 영역 정보보호 담당자

③ 회사는 정보보호 최고책임자 및 개인정보보호 책임자의 역할을 지원하고 정보보호 활동을 체계적으로 이행하기 위한 정보보호 전담조직을 구성하여 운영해야 한다.

④ 회사는 각 부서별 정보보호 담당자를 지정하여 정보보호 관련 실무 활동을 체계적으로 이행하도록 한다.

⑤ 정보보호 최고책임자는 회사의 정보보호 관련 중요 사항에 대한 검토 및 의사 결정, 정보보호 활동 관련 부서별 이견 조정 등을 위하여 정보보호위원회, 정보보호 실무위원회를 운영해야 한다.

제 9 조 [정보보호 조직의 책임과 역할]

회사는 정보보호 조직의 각 구성원들의 역할과 책임을 구체화하여 정보보호 조직의 운영 및 관리를 원활히 할 수 있도록 한다.

제 4 장 인적 보안

제 10 조 [비밀 유지]

① 인사팀은 직원의 입사 시 정보보호 규정 및 지침을 이해하고 이를 준수하겠다는 내용의 보안서약서를 징구해야 한다.

② 정보보호 서약서는 다음 각 호의 내용을 포함해야 한다.

1. 회사의 정보보호 정책 준수
2. 회사의 지식 재산권에 대한 동의
3. 업무상 취득한 정보 및 개인정보의 보호
4. 불법소프트웨어 사용 금지
5. 필수 보안 솔루션 사용 준수
6. 회사와 관련된 법규 및 요건에 대한 준수
7. 재직기간 중 알게 된 회사의 영업비밀정보의 보호
8. 회사의 업무와 관련하여 생성한 영업비밀정보의 회사의 귀속에 대한 동의
9. 상기 사항을 위반하였을 경우 민·형사상 책임과 관계 법령에 의한 조치를 따를 것에 대한 동의

제 11 조 [퇴직 및 계약 해지]

① 임직원은 퇴사 및 계약 해지 시 회사 소유의 모든 정보자산을 반납하고, 근무 기간 중 습득한 정보에 대한 비밀을 준수할 것을 서약하는 비밀유지 서약서를 제출해야 한다.

② 정보보호 주관부서 및 관련 부서는 직원의 퇴사, 계약 해지 시 회사 소유의 정보자산 및 접근 권한을 즉시 회수해야 한다.

③ 정보보호 주관부서 및 관련 부서는 퇴사자에게 근무 기간 중 습득한 관련 비밀을 준수할 의무가 있음을 주지시키고 비밀유지 서약서를 징구하며, 재직 중 취득한 회사의 정보자산 및 기술을 유출할 수 없도록 조치해야 한다.

제 12 조 [주요직무자 구성]

정보보호 관리자는 회사의 중요 정보자산을 취급하는 직무를 확인하고 해당 직무를 수행하는 임직원을 주요직무자로 지정해야 한다.

제 13 조 [인사 이동 시]

① 정보보호 주관부서는 임직원의 인사이동 및 직무변경 시 기 부여한 접근 권한의 적정성을 확인하여, 불필요한 권한을 즉시 회수해야 한다.

② 부서별 정보보호담당자는 인사이동 및 직무변경 시 부서 내 공용으로 사용하는 계정의 비밀번호를 즉시 변경해야 한다.

③ 인사 이동 및 직무 변경자는 업무 관련 정보를 모두 인수자에게 인계해야 하며, 담당 부서장에게 이를 확인 받아야 한다.

제 14 조 [정보보호 교육]

① 정보보호 관리자는 연간 정보보호 교육 및 훈련 계획을 수립해야 한다.

② 정보보호 교육 및 훈련은 전 임직원을 대상으로 정기적으로 실시해야 한다.

③ 정보보호 교육은 직무 및 전문성을 고려하여 교육 대상에 따라 차별화해야 한다.

④ 사업 주관부서는 파트너사 직원 등 외부인력을 대상으로 정보보호 규정, 지침 및 업무 수행에 필요한 정보보호 준수사항에 대해 교육을 수행해야 한다.

⑤ 정보보호 교육 및 훈련 실시 후 결과를 문서화해야 하며 이에 대해 검토 후 차기 교육에 반영해야 한다.

제 15 조 [정보보호의 날]

① 정보보호 주관부서는 월 1 회 '정보보호의 날'을 지정하여 운영해야 한다.

② 정보보호 주관부서는 매월 '정보보호의 날'에 임직원 및 파트너사 직원의 정보보호 인식 개선을 위한 교육과 홍보 등을 포함한 개선 활동을 수행해야 한다.

제 16 조 [정보보호 상벌 제도]

① 임직원의 정보보호 인식 제고 및 규정의 준수를 위하여 상벌 제도를 운영할 수 있다.

② 포상 및 징계 수준은 사건의 경중을 고려하여 유관부서와 협의를 통하여 결정해야 한다.

제 5 장 정보자산 관리

제 17 조 [정보자산의 책임과 권한]

① 회사는 소유하고 있는 정보 및 정보시스템 등 정보자산을 식별하고 통제, 관리, 감독해야 한다.

② 각 정보자산에 대해 책임자 및 담당자를 지정함으로써 정보자산 보호에 대한 책임성을 확보해야 한다.

③ 정보자산 책임자는 정보자산에 대한 취득, 사용허가, 처분 또는 폐기 등의 권한을 가지며 해당 권한은 정보자산의 효율적 관리 운영을 위해 해당 역할 중 일부를 지시하거나 위임할 수 있다.

④ 정보자산 담당자는 정보자산 책임자의 지시 또는 위임을 받아 정보자산을 실질적으로 관리하는 자로서 정보자산 목록관리 및 업데이트 등 자산관리 현행화를 주기적으로 실시해야 한다.

제 18 조 [정보자산의 분류]

① 정보자산은 회사가 소유, 보유하거나 회사로부터 생성된 출력문서, 전자문서 등을 포함한 모든 유무형의 정보 및 기술, 자료, 시설 등을 포함한다.

② 정보자산은 유형에 따라 다음 각 호와 같이 분류하여 관리해야 한다.

1. 전자정보 : 데이터베이스, 데이터 파일 등 전자적 형태로 저장되는 정보를 말한다.
2. 문서정보 : 출력 또는 수기로 작성한 문서 형태의 자료(설계도, 계약서, 제안서 및 수행 산출물 등)를 말한다.
3. 정보시스템 자산 : 전자정보 및 문서정보의 전자적 업무 활용을 위한 서버, 네트워크, 보안시스템, 어플리케이션 등을 말한다.
4. 시설·설비 자산 : 전력, 항온·항습, 소화설비 등의 시설 인프라 및 물리적 출입 통제 장치, 영상처리기기 등 설비를 포함한다.

제 19 조 [정보자산의 보안등급]

① 전자자산의 보안등급 산정은 다음과 같이 수행한다.

1. 전자, 문서정보 : 최초 정보의 작성(기안)자가 수행
2. 정보시스템, 시설설비 자산 : 정보자산 담당자가 수행

② 보안등급의 조정권한은 결재권을 가진 부서장, 정보자산 책임자 또는 정보보호 관리자

에게 있다.

③ 동일 정보자산 내 기밀 정보와 대외비 정보가 있을 경우 해당 문서의 등급은 상위등급으로 지정해야 한다.

④ 정보자산은 다음 각 호와 같이 등급을 분류하여 관리해야 한다.

1. 기밀
2. 대외비
3. 일반

제 20 조 [정보자산의 평가]

① 정보보호 최고책임자는 회사 정보자산에 대하여 연 1 회 이상 평가하고 그 결과를 보안등급에 반영해야 한다.

② 정보보호 주관부서는 각 자산의 담당자로 하여금 해당 정보자산의 분류, 중요도의 평가 또는 검토를 요구할 수 있다.

③ 정보자산 신규 도입 시 정보자산의 식별, 분류, 중요도 평가, 보안등급 분류 업무를 즉시 시행해야 한다.

④ 정보자산 관리자는 국내외 관련 법령 및 규제 등을 반영하여 정보자산의 보존 기간, 파기 기준을 수립해야 한다.

제 21 조 [정보자산의 파기]

① 정보자산 관리자는 정보자산의 보존이 불필요할 경우 지체 없이 파기해야 한다.

② 대외비 이상의 정보자산은 복구 또는 재생할 수 없는 방법을 이용하여 파기해야 한다.

③ 정보자산의 파기를 파트너사에 위탁하는 경우, 관리·감독 등 보호 조치를 취해야 한다.

④ 모바일 단말 및 이메일에 저장된 중요 정보자산의 유출을 방지하기 위하여 해당 정보자산을 주기적으로 관리 및 점검해야 한다.

제 6 장 접근통제

제 22 조 [사용자 접근통제]

① 시스템 관리자는 사용자 및 업무의 중요도, 접근 과정에 따른 위험 등을 고려하여 1 개 이상의 인증 방식을 시스템에 적용해야 한다.

② 시스템 관리자는 중요정보 또는 외부 인터넷 망을 통해 내부시스템, 관리자 페이지, 중요정보에 접근하는 경우, 추가적인 인증을 수행하도록 시스템을 구현해야 한다.

제 23 조 [계정 관리]

① 계정의 신규 등록, 삭제 또는 변경 사유가 발생한 경우, 시스템 관리자의 승인을 득해야 한다.

② 모든 계정은 사용자 별로 개별 부여해야 한다.

③ 시스템 특성 상 공용 계정 사용이 불가피한 경우, 정보보호 주관부서의 승인을 득해야 한다.

④ 관리자 계정 명은 관리자 수준의 계정임을 나타내거나 암시해서는 안 된다.

⑤ 임시 계정 발급 시 계정의 유효기간을 설정하여 유효기간이 지나면 자동적으로 사용정지 되도록 설정해야 한다.

⑥ 시스템 관리자는 정기적으로 계정 현황을 확인하여, 불필요한 계정을 삭제 또는 비활성화 해야 한다.

제 24 조 [비밀번호 관리]

① 정보시스템 접속 비밀번호는 안전한 비밀번호를 생성, 관리해야 한다.

② 타인과 비밀번호를 공유하는 행위를 금지한다.

③ 비밀번호는 사용자가 직접 주기적으로 변경해야 한다.

④ 정보시스템 관리자는 비밀번호 입력, 변경, 저장 및 전송 시 노출되지 않도록 시스템을 구현해야 한다.

제 25 조 [권한 관리]

① 업무 목적상 필요한 최소한의 권한만 부여해야 한다.

② 권한 부여, 변경, 삭제 등 변경 사유 발생 시 사전에 승인을 득해야 한다.

1. 관리자 권한 부여, 변경, 삭제 시 시스템 관리 부서의 장에게 승인을 받아야 한다.

2. 중요 정보에 대한 접근 권한 부여, 변경, 삭제 시 정보자산 책임자의 승인을 득해야 한다.

③ 권한 부여, 변경, 삭제 등의 이력을 기록, 보관해야 한다.

④ 시스템 관리자는 부여한 권한의 적정성을 정기적으로 검토 및 평가를 시행, 조정해야 한다.

제 26 조 [정보시스템 접근통제]

① 정보시스템 관리자는 다음 각 호를 고려하여 시스템을 구현·운영해야 한다.

1. 접속 실패 시 최소한의 정보만 표기하고, 관련 기록을 남기도록 시스템을 설정해야 한다.
2. 접속오류 횟수가 비정상적일 경우에는 접속을 차단하고 해당 계정의 사용을 중지하도록 설정해야 한다.
3. 접속 후 일정 시간 동안 사용하지 않는 경우, 자동 로그오프 또는 세션을 종료하도록 설정해야 한다.
4. 하나의 계정으로 여러 단말기에서의 동시접속을 제한해야 한다.

② 정보시스템에 대한 외부 원격 유지보수 작업이 필요한 경우 보호대책을 수립한 후 정보보호 주관부서의 승인을 득해야 한다.

제 27 조 [네트워크 접근통제]

① 정보보호 주관부서는 필요한 최소한의 범위 내에서 접근을 허용해야 하며, 변경 내역을 기록·관리해야 한다.

② 내부 네트워크와 외부 네트워크의 연결(대외 기관, 외부 통신망, 인터넷 등) 또는 변경 시에는 필요한 보호대책을 수립하여, 정보보호 주관부서의 승인을 득해야 한다.

③ 그룹망 이외 내부 업무용 네트워크 운영 시 침해 위험, 서비스 안전성을 고려하여 그룹망 수준의 보호대책을 적용해야 한다.

④ 정보보호 주관부서는 정보보호 관련 법규를 고려하여 필요 시 사용자 단말, 정보시스템 등을 대상으로 인터넷망과 업무망을 분리해야 한다.

제 28 조 [인터넷 접근통제]

① 정보보호 주관부서는 비 업무용 사이트 및 불법 파일 전송이 가능한 사이트의 접속을 제한해야 한다.

② 정보보호 주관부서는 인터넷을 통한 악성코드의 사내 유입 및 확산을 탐지·모니터링해야 한다.

제 29 조 [무선 접근통제]

① 정보보호 주관부서는 비 인가자의 무선 네트워크 접속을 방지하기 위해 사용자 인증, 무선구간 통신데이터의 암호화 및 네트워크 접근통제 등 보호 대책을 수립, 적용해야 한다.

② 정보보호 주관부서는 비인가 무선접속장비의 설치·운용 여부를 보안점검 시 확인해야 한다.

제 30 조 [원격 업무 접근통제]

① 정보보호 주관부서는 재택·파견·이동근무 등 원격 업무 시 정보자산 유출 등의 보안사고 방지를 위해 원격 단말기, 내·외부 네트워크, 원격 접속 수단 등에 대한 보호 대책을 수립 및 이행해야 한다.

제 7 장 물리 보안

제 31 조 [보호구역의 설정]

물리적 정보보호 담당자는 회사의 관리하에 있는 물리적인 공간 중 보호해야 할 필요가 있는 구역을 보호구역으로 지정하고, 관리해야 한다.

제 32 조 [보호구역의 접근통제]

① 물리적 정보보호 담당자는 보호구역에 대한 출입통제를 위해 별도의 출입통제장치 및 감시시스템 등을 설치·운영해야 한다.

② 외부인이 보호구역에 출입할 때에는 항상 인가된 출입증을 패용하고 임직원이 동행해야 한다.

③ 물리적 정보보호 담당자는 통제구역의 출입 이력을 확인할 수 있는 수단을 마련해야 하며, 주기적으로 출입 내역을 검토해야 한다.

④ 노트북, 이동식 저장 매체 등을 소지하고 통제구역에 출입할 때에는, 사전에 승인을 득해야 하며, 사전 승인된 물품 이외에는 반출·입 할 수 없다.

⑤ 임직원 퇴사 시 출입증은 즉시 반납하여야 하며, 반납된 출입증은 폐기 및 관리하여야 한다.

⑥ 출입증 분실 시, 물리적 정보보호 담당자에게 신속히 알려야 한다.

⑦ 모바일 출입증은 퇴사와 함께 자동으로 권한이 삭제되어야 한다.

제 33 조 [정보자산 반출·입]

① 정보자산을 반출·입할 때에는 해당 부서장의 승인을 득해야 하며, 개인적 용도로 회사 정보자산을 반출하는 것을 금지한다.

② 정보자산의 반출 이력을 기록, 관리해야 한다.

제 34 조 [전산 시설 보호 대책]

물리적 정보보호 담당 부서는 환경적 위해 요소 및 불필요한 접근 등으로부터 전산 시설을 보호하기 위한 관련 전산 설비 구축 등의 보호대책을 이행해야 한다.

제 35 조 [사무실 보호대책]

① 물리적 정보보호 담당 부서는 문서 파기 장치를 임직원이 적절히 사용할 수 있도록 설치, 운영해야 한다.

② 중요 정보는 반드시 잠금 장치가 설치된 장소에 보관해야 한다.

③ 노트북은 반드시 잠금 장치를 통해 보호해야 하며 도난, 분실에 유의해야 한다.

④ 프린터, 팩스, 복사기 사용 시 산출되는 문서는 즉시 회수해야 한다.

⑤ 공용 PC 사용을 금지한다. 단, 필요할 경우 공용 PC 의 관리자를 지정하여 방치되거나 부당한 목적으로 사용되지 않도록 해야 한다.

⑥ 공용 캐비닛에는 관리자를 지정하고, 퇴실 시 항상 잠그며 열쇠는 안전한 곳에 보관해야 한다.

⑦ 개인서랍은 잠금 장치를 설치하고 퇴근 및 장시간 이석 시 항상 잠그며 열쇠는 안전한 곳에 보관해야 한다.

⑧ 관리적 정보보호 담당 부서는 사무실 보안 관리 현황을 분기별 1 회 이상 점검하며, 결과를 정보보호 최고책임자에게 보고해야 한다.

제 8 장 운영 보안

제 36 조 [운영 절차 수립]

① 정보 시스템 운영자는 다음 각 호와 같은 정보시스템 운영에 관한 절차를 문서화하여 관리해야 한다.

1. 정보시스템의 동작
2. 문제 발생 시 대처
3. 오류 및 예외 사항 처리 등

제 37 조 [권한 분리]

권한 오남용을 예방하기 위해 정보시스템 운영 담당자, 개발자 직무 분리 및 직무 구분에 따른 권한을 분리 운영해야 한다.

제 38 조 [정보보호 시스템 운영]

정보보호 시스템 운영자는 최신 정책 업데이트 및 이벤트 모니터링을 시행해야 하며, 정책의 등록·변경·삭제 시 정보보호 주관부서의 승인을 받아야 한다.

제 39 조 [암호 통제]

① 개인정보, 기밀정보 등 중요정보의 저장·전송 시 안전한 보호를 위하여 암호화해야 한다.

② 서버, 데이터베이스, 어플리케이션의 암호 키 생성·변경·폐기 시 정보보호 관리자의 승인을 포함한 키 관리 절차를 수립·운영해야 한다.

③ 암호키의 사용, 보관, 배포, 복구 시에는 시스템 관리 부서장의 사전 승인을 득한 권한이 있는 사용자만 사용가능 하도록 관리절차를 수립, 운영하여야 한다.

제 40 조 [장애 관리]

① 정보시스템 운영자는 정보시스템을 지속적으로 모니터링 해야 하며, 이상 징후가 감지될 경우 장애 여부를 판단하여 사안에 따라 대응해야 한다.

② 정보시스템 운영자는 장애 이력을 기록·관리해야 한다.

제 41 조 [취약점 점검]

① 정보시스템 관리자는 주기적으로 시스템 취약점 점검을 수행해야 한다.

② 취약점 점검 결과 도출된 문제점에 대해 반드시 보호 조치를 적용해야 하며, 그 결과에 대해 이행 점검을 시행해야 한다.

③ 시스템 관리자는 취약점 점검 결과 및 개선조치 사항에 대하여 정보보호 최고책임자에게 보고해야 한다.

제 42 조 [공개서버 보안]

① 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치해야 한다.

② 공개서버의 관리자는 정기적으로 게시 정보의 적정성을 검토하여 개인정보 등 주요 정보가 노출되지 않도록 관리해야 한다.

제 43 조 [정보시스템 저장매체 관리]

① 정보시스템 폐기 또는 재사용 시 해당 시스템에 저장된 정보는 복구할 수 없는 방법으로 삭제해야 한다.

② 정보시스템의 외부 수리 등 파트너사를 통해 업무를 처리하는 경우, 보안서약서 징구 등 필요한 조치를 취해야 한다.

제 44 조 [악성코드 통제]

① 정보시스템 운영자는 시스템에 백신 프로그램을 설치해야 하며, 정기적으로 정밀검사를 수행해야 한다.

② 백신 프로그램은 항상 최신의 정보를 유지할 수 있도록 정기적으로 업데이트를 수행해야 한다.

제 45 조 [패치 관리]

① 정보시스템 운영자는 정기적으로 패치 업데이트를 수행해야 하며, 적용 내역을 기록·관리해야 한다.

② 정보시스템 운영자는 패치 적용 전 안정성 테스트를 수행해야 한다.

③ 서비스 문제 등으로 인해 보안 패치를 적용하지 못하는 경우, 그에 따른 대응 방안을 마련해야 한다.

제 46 조 [로그관리 및 모니터링]

① 정보시스템 관리자는 정보보호 사고 발생 시 추적이 가능하도록 시스템 접근 및 사용 내역을 기록, 보관해야 한다.

② 로그 기록은 별도 저장매체에 백업해야 하며, 접근권한을 최소화해야 한다.

③ 모든 시스템은 로그에 대한 정확한 기록을 보증하기 위해 시간을 동기화해야 한다.

④ 정보시스템 관리자는 로그 기록을 정기적으로 검토해야 한다.

⑤ 주요 정보시스템은 침해 시도를 인지할 수 있도록 모니터링을 시행해야 하며, 이상 징후 발견 시 지체 없이 정보보호 주관부서에 보고해야 한다.

⑥ 정보시스템 관리자 계정, 주요 직무자 계정의 접근 및 이용 로그 기록은 별도의 강화된 기준을 적용하여 점검해야 한다.

⑦ 개인정보취급자가 개인정보처리시스템에 접속한 기록은 최소 1 년 이상 보존, 관리해야 한다. (단, 5 만 명 이상의 개인정보를 처리하거나, 고유식별정보, 민감정보를 처리하는 경우 2 년 이상 보관)

제 9 장 사용자 보안 관리

제 47 조 [PC 보안]

① 임직원은 PC 에 회사에서 운영하고 있는 보안 솔루션을 설치해야 하며 임의로 삭제할 수 없다.

② 사용자 임의로 하드웨어를 추가, 변경, 제거할 수 없다.

③ 임직원은 PC 에 그룹 화면보호기를 설정하고 대기시간을 10 분 이내로 하여 비밀번호를 설정해야 한다.

④ 업무 목적상 반드시 공유 폴더가 필요한 경우에는 접근 가능한 사용자 제한 등 보호 대책을 수립·적용해야 한다.

⑤ PC 에 정보를 보관하는 경우 문서 암호화를 적용해야 한다.

⑥ 업무 목적상 암호화 해제가 필요한 경우 사유 및 목적을 명확히 작성하여 승인을 득해야 하며, 목적을 달성한 즉시 삭제 또는 재 암호화해야 한다.

⑦ 업무 목적상 휴대용 저장 장치 등의 매체 사용이 필요한 경우 정보보호 주관부서의 승인을 득해야 한다.

⑧ 임직원은 PC 에 설치한 운영체제, 어플리케이션 등의 최신 보안패치를 유지해야 한다.

⑨ 임직원은 본인이 지급받은 PC 에 대한 보안 및 관리에 책임을 다해야 한다.

제 48 조 [모바일 보안]

① 모바일 업무 어플리케이션을 운영할 경우 다음 각 호의 보안 대책을 마련해야 한다.

1. 기밀, 대외비 자료가 모바일 단말에 저장되지 않도록 서버에서 편집 불가능한 형태로 변환하여 전송해야 한다.
2. 운영 체제, 플랫폼, 어플리케이션 위·변조 여부를 체크해야 한다.
3. 사전 허가된 단말에 한해 서비스 사용 가능하도록 설정해야 한다.
4. 중요 정보는 암호화 전송해야 한다.
5. 국내외 관련 법령 및 규제 등을 반영해야 하며 법령 및 규제 변경 시 업데이트 하여야 한다.

② 사용자는 모바일 단말기의 잠금 기능을 적용해야 하며, 비밀번호 입력 오류 반복 시 사용이 불가능하도록 설정해야 한다.

③ 모바일 단말 운영시스템 설정을 임의로 개조하거나 플랫폼 구조의 임의 변경을 금지한

다.

④ 회사의 주요 정보를 모바일 단말기에 저장할 때에는 암호화를 적용해야 한다.

⑤ 신뢰할 수 없는 무선 네트워크를 통한 결재, 중요 자료 열람 등을 금지한다.

⑥ 블루투스, 적외선 장치 기능 등은 필요한 경우에만 한정적으로 사용해야 한다.

제 49 조 [악성코드 예방]

① 임직원은 단말기 보호를 위해 악성코드 탐지 및 대응 솔루션을 설치해야 하며, 정기적으로 업데이트 및 실시간검사를 수행해야 한다.

② 특별한 이유 없이 시스템 혹은 프로그램이 동작하지 않는 등 악성코드 감염이 의심되는 경우 정보보호 주관부서에 신고해야 한다.

③ 전자우편, 메신저, SMS 등을 통해 출처가 불분명한 상대에게 의심스러운 메일, 링크, 첨부파일을 수신한 경우, 임직원은 수신한 자료를 클릭하지 않고 정보보호 주관부서에 신고해야 한다. 단, 업무 목적으로 불가피하게 첨부파일을 다운로드 및 실행해야 할 경우, 악성코드 검사 후 실행한다.

제 50 조 [불법 소프트웨어 사용 금지]

① 임직원은 회사에서 허가한 소프트웨어만을 사용해야 한다.

② 다음 각 호와 같은 불법 소프트웨어 사용을 금지하며, 사용으로 인한 피해 발생 시 사용자가 책임을 져야 한다.

1. 유료 소프트웨어를 별도의 라이선스 없이 무단 이용
2. 온라인 통신망 및 인터넷을 통한 불법 복제
3. 시리얼 넘버의 공유·도용·배포·전송 등의 행위
4. 기한이 지나거나 상업적 목적의 이용을 금지한 쉐어웨어 사용

제 10 장 업무용 정보통신 수단의 이용 및 관리

제 51 조 [업무용 정보통신 수단]

① 정보보호 주관부서는 사용자의 송·수신 기록을 확보할 수 있는 전자우편, 메신저 등을 임직원 업무용 정보통신 수단으로 지정해야 한다.

② 정보보호 주관부서는 업무용 정보통신 수단 외의 전자 우편, 메신저 등의 사용을 제한해야 한다.

③ 임직원은 업무용 정보통신 수단 외의 전자우편, 메신저를 사용해서는 안 된다.

④ 전자우편 및 메신저를 통해 중요 정보를 전송하는 경우, 암호화 등 보호 조치를 적용해야 한다.

⑤ 임직원은 업무용 정보통신 수단을 이용하여 다음 각 호의 행위를 해서는 안 된다.

1. 영업비밀정보에 속하는 사항을 업무 이외의 목적으로 발송하는 행위
2. 범죄를 목적으로 하거나 교사 또는 방조하는 내용을 발송하는 행위
3. 회사가 승인하지 않은 광고 문구를 이용하여 투자·광고하거나 회사가 승인하지 않은 대량의 메시지를 발송하는 행위
4. 업무상 알게 된 공개되지 않는 정보를 제공하는 등 관련 법규에서 금지하는 행위
5. 임직원 및 고객의 개인정보를 유출하는 행위

⑥ 임직원은 회사 전자우편으로 송수신한 자료를 업무용 정보통신 수단으로 지정되지 않은 외부 전자우편으로 자동포워딩 해서는 안 된다.

⑦ 임직원은 ChatGPT 등과 같은 생성형 인공지능 서비스를 업무에 활용하는 경우 다음 각 호의 내용을 준수하여야 한다.

1. 서비스가 생성한 결과물을 주의 깊게 검토하고, 부적절한 내용이나 유해한 요소가 포함되어 있는지 확인하여야 한다.
2. 기밀정보, 민감정보, 개인정보를 제공하지 않아야 하며 저작권에 위배되지 않는 용도로 사용되어야 한다.
3. 부정확한 정보 제공을 하는 서비스의 특성을 고려하여 정확성을 검증하여야 한다.
4. 서비스 공격 코드, 피싱 메일 제작 등의 유해한 결과물을 생성하지 않아야 하며 업무 목적에 맞게 사용하여야 한다.
5. 접속 PC 의 보안 패치는 최신으로 유지하고 보안 프로그램을 설치하여 사용하여야 한다.

제 52 조 [업무용 정보통신 수단 로그 기록 및 관리]

① 전자우편, 메신저 시스템 관리자는 정보통신수단의 사용기록 및 송·수신 정보를 기록, 보관해야 한다.

② 정보보호 주관부서는 업무용 정보통신 수단의 로그 보관 상태를 주기적으로 점검해야 하며, 점검 결과를 기록, 관리해야 한다.

③ 정보보호 주관부서는 업무용 정보통신 수단을 통한 회사의 중요정보 유출방지를 위해 모니터링을 수행할 수 있으며, 사전에 임직원 등에게 모니터링 사실을 공지하고 동의를 받아야 한다.

제 11 장 정보시스템 도입, 개발 및 유지보수

제 53 조 [정보시스템 개발과 운영 환경의 분리]

① 개발 및 테스트 시스템은 운영 시스템과 분리하여 설치, 운영해야 한다.

② 컴파일러, 편집기 등과 같이 개발에 필요한 도구를 운영환경에 설치하는 것을 금지한다.

제 54 조 [요구사항의 정의]

① 정보시스템 도입, 개발 및 유지보수 담당부서는 정보시스템 도입, 개발 및 유지보수 시 다음 각 호의 보안 요구사항을 명확히 정의하여 관리해야 한다.

1. 사용자 인증 방법
2. 접근통제 방법
3. 입력 데이터 검증, 내부처리, 출력 데이터 검증
4. 로그 관리
5. 암호화
6. 개인정보의 화면 출력 시 마스킹 표시
7. 기타 개발·운영 시 정보보호 통제

제 55 조 [개발 시 보안]

① 개발자는 어플리케이션 개발 및 유지보수 시 보안 요구사항을 고려하여 어플리케이션을 개발해야 한다.

② 소스코드 내에 비밀번호 및 중요 개인정보의 기록을 금지한다.

③ 소스코드에 대한 변경이력을 관리해야 한다.

④ 신규 프로그램 구축을 위해서 사업 준비 단계에서부터 보안 요소를 반영한 소스코드 점검을 개발일정에 반드시 포함해야 한다.

제 56 조 [소스코드 접근통제]

① 소스코드를 운영환경에 보관하는 것을 금지한다.

② 인가자만 소스코드에 접근할 수 있도록 보호 대책을 수립·적용해야 한다.

제 57 조 [테스트]

① 개발자는 어플리케이션 신규 개발 및 변경 시 테스트 환경에서 해당 어플리케이션을 충분히 테스트하고 그 결과를 문서화해야 한다.

② 운영 환경의 실 데이터를 변경 없이 테스트 데이터로 활용하는 것을 금지한다. 단, 반드시 실 데이터를 사용해야 할 경우에는 비 식별 처리하거나 부서장의 승인을 받고 사용해야 한다.

③ 테스트용 데이터는 적절하게 관리해야 하며, 사용 이후 삭제 및 이력을 관리해야 한다.

제 58 조 [정보시스템 도입 및 구축]

① 정보시스템 도입 및 구축 주관 부서는 정보시스템 신규 도입, 구축 시 보안 요구사항을 고려해야 한다.

② 신규 도입 및 구축한 정보시스템을 대상으로 취약점 점검 및 모의해킹을 수행해야 하며, 도출된 문제점에 대해 반드시 보호 조치를 적용해야 한다.

제 59 조 [사전 보안성 검토]

① 신규 도입, 구축 및 개발한 정보시스템을 운영단계로 이관하기 전에 정보보호 관리자로부터 사전 보안성 검토를 받아야 한다.

② 정보보호 주관부서는 신규 정보시스템에 대한 보안성 검토를 실시하고, 그 결과를 문서화하여 관리해야 한다.

③ 신규 도입, 구축 및 개발한 정보시스템으로 인해 회사의 정보보호 수준이 저하될 경우, 정보보호 관리자는 서비스 시작을 제한할 수 있다.

④ 다음 각 호의 업무를 준비하는 경우에는 정보보호 주관부서에 보안성 심의를 신청해야 한다.

1. 외부에서 접근 가능한 시스템 신규 개발 및 재구축 시
2. 개인정보처리시스템 신규 개발 및 재구축 시
3. 전산실/네트워크 이전・도입 시

제 12 장 파트너사 관리

제 60 조 [사업 준비단계 보안]

① 파트너사와 사업을 계약할 경우 다음 각 호의 내용을 반영해야 한다.

1. 사업 계약 시, 보안준수 사항 및 손해배상 책임 등을 문서화해야 한다.
2. 수탁 업체가 사업의 일부 또는 전부에 대하여 재 위탁 계약을 체결하는 경우, 반드시 회사의 동의 하에 진행되어야 하며, 본 계약 수준의 보안 준수 사항을 포함해야 하고 위반 시 손해배상 책임 등을 문서화해야 한다.
3. 기타 법령에서 요구하는 보안조치 사항

제 61 조 [사업 수행단계 보안]

① 사업 주관 부서는 사업 참여인력에 대하여 보안서약서를 징구해야 한다.

② 외부 인력의 PC 를 회사 내부 네트워크에 연결하는 경우 임직원과 동일한 보안 정책을 적용해야 한다.

③ 사업 주관 부서는 파트너사에게 업무상 필요한 최소한의 정보 및 권한을 제공해야 한다.

④ 사업 주관 부서는 파트너사에게 제공한 정보 또는 수행 중 생성된 산출물에 대하여 인터넷, 웹하드 등의 자료 공유사이트에 업로드를 금지하고, 전자우편으로 수·발신하는 것을 금지해야 한다.

⑤ 사업 주관 부서는 정보보호 주관부서에서 제공하는 파트너사 보안교육을 진행하고 결과를 관리하여야 한다.

제 62 조 [사업 종료단계 보안]

① 사업 주관 부서는 사업의 최종 산출물 중 보안이 요구되는 자료를 기밀 또는 대외비로 등록하여 관리해야 한다.

② 사업 주관 부서는 사업 완료 시 다음 각 호의 항목을 수행해야 한다.

1. 파트너사에게 부여한 물리적, 논리적 접근권한 및 정보자산을 회수해야 한다.
2. 외부 인력의 PC, 노트북 및 기타 저장장치내의 모든 자료를 복구가 불가능한 방법으로 삭제해야 한다.
3. 사업 수행 중 획득한 정보에 대한 비밀 유지 의무를 설명하고, 서약서를 징구해야 한다.

제 13 장 침해사고 및 연속성 관리

제 63 조 [침해사고의 정의]

① 회사는 다음의 내용을 해당하는 경우 침해사고로 분류하여 관리해야 한다.

1. 회사의 기밀정보 또는 개인정보가 유·노출되거나 위·변조된 경우
2. 주요 정보자산(H/W, S/W, DB 등)이 유출, 절도, 파괴된 경우
3. 악성코드 등에 의해 회사 서비스가 지연 및 중단된 경우(웹해킹, DDoS 공격 등)
4. 비 인가자가 회사의 정보시스템을 공격하거나 침투한 경우
5. 내부자 및 접근이 허용된 외부자에 의한 내부 자원의 오용
6. 물리적인 통제구역 또는 내부 전산망의 무단 침입

제 64 조 [침해사고 대응체계 구축]

① 침해사고 대응을 위해 정보보호 최고책임자를 중심으로 침해사고 대응조직을 구성하고, 대응체계를 수립 운영해야 한다.

② 정보보호 주관부서는 정보자산에 영향을 미치는 침해사고의 심각한 정도를 정의해야 한다.

③ 정보보호 주관부서는 정보자산에 발생할 수 있는 침해사고의 예방 및 신속한 복구를 위해 침해사고 대응계획을 수립·운영해야 한다.

④ 침해사고 여부 등 이상징후를 파악하기 위해 모니터링 및 정기적인 로그 분석을 수행해야 한다.

제 65 조 [침해사고 예방]

① 정보보호 관리자는 침해사고의 효율적인 예방을 위해 다음 각 호의 사항을 포함한 침해사고 예방 활동을 시행해야 한다.

1. 침해사고 대응 교육 및 훈련
2. 정보보호시스템 운영
3. 접근통제 실시
4. 정기적 취약점 평가 실시
5. 규칙적인 백업 수행 및 소산 관리
6. 주요 정보시스템 이중화
7. 침해사고 대응 조직 구성 및 관련 비상 연락망 구축

② 침해사고 대응 조직은 침해사고 시 지체 없이 대응할 수 있도록 주기적인 모의훈련을 수행해야 한다.

1. 그룹 정보보호 조직이 주관하는 침해사고 대응 모의훈련에 연 1 회 이상 참여해야 한다.
2. 회사의 침해사고 대응체계 점검 및 보고체계 점검을 위한 모의훈련을 연 1 회 이상 수행해야 한다.

제 66 조 [침해사고 보고]

① 임직원 및 정보시스템 운영자는 침해사고가 발생하거나 징후를 포착하면 즉시 정보보호 주관부서에 신고해야 한다.

② 정보보호 주관부서는 침해사고 발생 또는 징후를 접수하였을 경우 해당 내용을 기록 및 관리해야 한다.

③ 정보보호 주관부서는 초기 접수 내용을 분석하여 그룹 정보보호 주관부서 및 관련 대외 기관에 신고해야 한다.

④ 정보보호 주관부서는 사고의 처리가 완료되면 침해사고에 대한 보고서를 작성해야 한다.

제 14 장 개인정보보호

제 67 조 [개인정보내부관리지침 수립·시행]

① 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보내부관리지침을 수립·시행해야 한다.

1. 개인정보보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보내부관리지침의 수립 및 승인에 관한 사항
4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부점검에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 개인정보취급자에 대한 교육에 관한 사항
7. 접근 권한의 관리에 관한 사항
8. 접근 통제에 관한 사항
9. 개인정보의 암호화 조치에 관한 사항
10. 접속기록 보관 및 점검에 관한 사항
11. 악성프로그램 등 방지에 관한 사항
12. 물리적 안전조치에 관한 사항
13. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
14. 개인정보 유출사고 대응 계획 수립 및 시행에 관한 사항
15. 위험도 분석 및 대응방안 마련에 관한 사항
16. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
17. 그 밖에 개인정보보호를 위해 필요한 사항

② 제 1 항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 개인정보내부관리지침을 수정하여 시행하고, 그 수정 이력을 관리해야 한다.

제 68 조 [개인정보 위탁 관리]

① 개인정보 처리를 위탁하는 경우, 해당 위탁 업무의 내용과 수탁자에 대한 내용을 정보주체에게 공개해야 한다.

② 파트너사와 개인정보 관련하여 업무를 수행할 경우 개인정보 보호와 관련하여 다음 각 호의 요건을 계약서, 약정서 등에 문서화해야 한다.

1. 위탁업무 수행 목적, 범위 및 목적 외 개인정보 처리 금지에 관한 사항
2. 개인정보에 대한 비밀 유지 및 기술적, 관리적 보호 의무 준수
3. 개인정보보호 관리 부실로 인한 문제발생 시 손해배상책임
4. 개인정보 취급 활동에 대한 모니터링 및 감사 권한
5. 재위탁 제한에 관한 사항
6. 기타 개인정보의 안전한 처리를 위한 사항 및 법적 준수 사항

③ 개인정보 위탁 계약서, 약정서 작성 시 표준 양식을 사용할 수 있으며, 법무팀의 검토, 승인을 받아야 한다.

④ 개인정보를 위탁하는 각 부서는 위탁업무 종료 시 수탁업체에 제공한 개인정보의 파기를 요구 및 확인해야 하며, 파기 확인서를 징구해야 한다.

⑤ 개인정보보호 담당자는 개인정보를 취급하는 파트너사의 현황을 유지 및 관리하고, 개인정보보호 관련 위반사항이 없는지 연 1 회 이상 점검해야 한다.

⑥ 개인정보보호 담당자는 수탁사가 개인정보를 수령, 사용, 폐기하는 경우 이에 대한 취급 기록을 작성하고 통제해야 한다.

⑦ 회사의 개인정보 처리 시스템을 파트너사가 개발하는 경우, 개발자의 개인정보 접근에 대한 통제대책을 적용해야 한다.

제 69 조 [가명정보의 처리]

회사는 개인정보를 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 가명처리하여 활용할 경우 기술적·관리적·물리적 안전조치를 이행하고, 재식별되지 않도록 관리하여야 한다.

제 15 장 규정 준수

제 70 조 [규정 준수의 책임과 권한]

① 회사의 임직원은 정보자산 및 중요정보의 안전성을 확보하기 위해 본 규정 및 지침을 숙지하고 준수할 책임이 있다.

② 정보보호위원회는 본 규정을 적절히 유지하고, 회사의 임직원이 준수하도록 교육 및 지원해야 한다.

제 71 조 [자체 점검]

① 정보보호 관리자는 연 1 회 이상 회사의 정보보호 현황에 대해 자체 점검을 수행하여 점검 결과를 정보보호 최고책임자에게 보고해야 한다.

② 정보보호 자체 점검 결과 보고서에는 다음 각 호의 내용을 포함해야 한다.

1. 정보보호 점검 대상 및 범위
2. 정보보호 점검 세부 내용
3. 조치 및 개선 사항

③ 자체 점검 결과에 따라 포상을 할 수 있으며, 중대한 위반 사항을 발견한 경우 사안에 따라 징계를 요구할 수 있다.

④ 정보보호 최고책임자는 점검 결과에 따른 이행조치가 제대로 이루어지는지 지속적으로 점검해야 한다.

⑤ 사업 주관 부서 및 정보보호 주관부서는 사업 프로젝트에 대한 자체 점검을 수행하여 점검 결과를 정보보호 최고책임자에게 보고해야 하며 결과를 관리하여야 한다.

제 72 조 [그룹 정보보호 수준진단]

① 정보보호 주관부서는 그룹 정보보호 위원회가 정보보호 수준진단 수검을 요청하는 경우, 수준진단에 필요한 필요한 자료 및 제반 요청사항을 준비하여 지원해야 한다.

② 그룹 정보보호 수준진단 수검 시 점검 대상 부서는 점검에 성실히 임해야 한다.

제 73 조 [정보보호 공시]

회사는 정보통신서비스를 이용하는 자의 안전한 인터넷 이용을 위하여 정보보호 현황을 공시하여야 한다.

제 74 조 [법률과의 관계]

① 본 규정은 업무를 수행함에 있어 안전성 확보를 위해 적용해야 할 기본적인 사항을 규정하는데 목적이 있다.

② 정보보호 관련 법령에 관해서는 본 규정에 앞서 우선 적용됨을 원칙으로 한다. 다만 관련 법령에서 규정하지 않는 조치사항에 대해서는 본 규정을 적용한다.

부 칙

제 1 조 [시행일]

이 규정은 2023 년 11 월 3 일부터 시행한다.

제 2 조 [경과조치]

이 규정 시행이전에 행한 사항은 이 규정에 의해 시행한 것으로 본다.

제 3 조 [관련사규]

1. 취업규칙
2. 인사위원회규정