SK플래닛 정보보호 규정

1 목적

1.1 본 규정은 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법, 전자금융거래법 등에 따라 SK planet(주)(이하 회사라 한다)의 모든 임직원과 회사의 정보를 다루는 모든 협력회사 및 계약사의 임직원에게 회사의 IT 보안에 대한 조직·역할 및 기본 원칙을 제시함으로써 회사의 보안성 강화 및 경쟁력 제고를 목적으로 한다.

2 적용 범위

2.1 본 규정은 회사의 모든 임직원과 회사의 정보를 다루는 모든 협력회사 및 계약사의 임직원에 대해 적용되며, 회사가 보유하고 있는 유·무형의 자산 및 영업비밀 등 모든 정보 자산에 대해 적용한다.

3 용어 정의

3.1 본 규정에서 사용하는 주요 용어의 뜻은 "보안 절차 규정"의 용어 정의를 따른다.

4 정보보호 최고책임자

4.1 정보보호 최고책임자는 다음 각호의 역할을 수행한다.

1) 정보보호 정책 수립 및 관리 체계 구축
2) 정보보호 수준 모니터링 및 진단 관리
3) 정보보호 조직 운영
4) 정보보호 현안 보고
5) 정보보호 관련 대외 협력
6) 정보보호 위험의 식별 평가 및 정보보호 대책 마련
7) 정보보호 교육과 모의 훈련 계획의 수립 및 시행

5 정보보호 관리자

5.1 정보보호 관리자는 다음 각호의 역할을 수행한다.

1) 정보보호 정책 수립, 관리
2) 정보보호 관련 법률 분석 및 규제 대응
3) 정보보호 서비스 제공
4) IT 보안 점검 수행 및 감사 지원
5) 내부정보 유출 모니터링
6) 보안솔루션 도입, 구축, 개선
7) 정보보호 관제 및 침해사고 대응

8) IT 보안 취약점 진단, 모니터링

9) IT 보안 기술 교육 수행

6 정보보호 담당자

6.1 정보보호 담당자는 다음 각 호의 역할을 수행한다.

1) 회사 정보보호 관련 사규 수립 및 운영

2) 정보보호 교육 계획 수립 및 운영

3) 정보시스템 운영에 따른 정보보호 관련 업무 총괄

4) 위험요인에 대한 보안대책 강구 및 이행

5) 취약점 진단에 대한 이행계획 수립 및 수행

6) 침해사고에 대한 모니터링 및 대응계획 수립과 대응

7 정보보호 담당 부서 및 사용자

7.1 정보보호 담당 부서는 CISO의 업무를 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위한 전문성을 갖춘 보안 조직으로 해당 팀장을 정보보호 관리자로 지정하고, 실무적인 역할을 수행하는 정보보호담당자를 선임한다.

8 정보보호위원회

8.1 보안 업무를 효율적으로 수행하고 주요 사업계획 등에 대한 사전 보안대책을 심의·의결하기 위해 정보보호위원회(이하 "위원회"라 한다)를 두며 정보보호위원회는 다음 각 사항 등을 심의·의결한다

1) 정보보호 업무의 계획·조정에 관한 사항

2) 취약점 분석 및 평가에 관한 사항

3) 주요 사업계획을 수립할 때의 사전 보안대책 수립에 관한 사항

4) 사회적으로 큰 이슈를 야기하고 있는 보안 위험 대두 시

5) 사내 중대 보안 사고 발생 시

6) 기타 주요 보안 업무처리에 관한 사항

9 자산관리

9.1 회사 내의 모든 정보는 회사의 중요한 자산이며, 회사가 그 소유권을 갖는다.

9.2 자산은 자산의 가치를 평가해 중요도에 따라 등급을 구분해 관리한다.

9.3 정보자산 및 정보시스템 자산은 주기적으로 위험을 분석해 그 결과에 따라 적절한 보안 통제를 적용해야 한다.

9.4 자산관리에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

10 사용자 계정 관리

10.1. 사용자에게 부여한 사용자 계정을 등록하고 등록에 관한 사항을 기록, 유지, 관리해야 하며, 주기적으로 유효성을 확인해야 한다.

10.2. 사용자 계정 관리에 관한 상세 기준은 "IT보안절차 규정"을 따른다.

11 비밀번호

11.1. 모든 사용자는 반드시 추측하기 힘든 고유한 비밀번호를 가져야 하며 타인과 공유 해서는 안 된다.

11.2. 비밀번호에 관한 상세 기준은 "IT보안절차 규정"을 따른다.

12 접근권한 관리

12.1 회사의 임직원 및 계약 관계에 있는 모든 사용자의 정보 자산에 대한 접근은 알 필요 원칙과 최소 권한 부여의 원칙에 따라 결정해야 한다

12.2 접근권한 관리에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

13 접근 통제

13.1 사용자는 상대방의 승인 없이 시스템에 접근을 시도해서는 안 된다.

13.2 외부에서 내부 네트워크에 접속 시 반드시 허가된 작업만 실행해야 하며, 정보보호 관련 사항은 외부에 유출 또는 공개해서는 안 된다.

13.3 접근 통제에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

14 보안성 검토

14.1 하드웨어와 소프트웨어는 규정된 구매 절차를 통해 도입하고, 모든 서비스 프로그램은 보안을 고려해 개발해야 하며, 반드시 정보보호 기능에 대해 정보보호 진단 담당자의 보안성 검토를 받아야 한다.

14.2 보안성 검토에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

15 소프트웨어

15.1 사용자는 불법 소프트웨어를 사용해서는 안 되며, 불법 소프트웨어 사용으로 인한 모든 책임은 사용자에게 있다.

15.2 소프트웨어의 사용에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

16 컴퓨터 바이러스 통제

16.1. 정보보호 관리자는 회사의 모든 컴퓨터에 바이러스를 검색하고 치유할 수 있는 백신 소프트웨어를 설치해야 한다.

16.2 컴퓨터 바이러스 통제에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

17 점검 활동

17.1 정보보호 관리자는 주기적인 보안 수준 점검 활동을 통해 본 규정 및 하위 절차 규정의 준수 여부를 확인하고, 필요시 대책을 권고한다.

17.2 점검 활동에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

18 사고보고

18.1 보안사고 및 정보 유출을 인지한 모든 임직원은 즉시 정보보호 관리자에게 보고해야 한다.

18.2 사고 보고와 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

19 교육 및 훈련

19.1 회사 및 회사의 임직원과 업무상 계약 관계에 있는 모든 사용자는 회사 자산의 지속적인 보호를 위해 정보보호 관련 규정과 절차 규정에서 정하고 있는 교육 및 훈련을 준수해야 한다.

19.2 교육 및 훈련에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다

20 재해복구

20.1 정보시스템 운영 담당자는 재해 시 복구를 위해 정보 자산 별 복구 우선 순위, 작업 절차, 비상연락망, 테스트 절차 및 점검 주기 등이 포함된 재해복구 계획을 별도로 정해 시행 해야 한다.

20.2 재해복구에 관한 상세 기준은 "IT보안절차 규정"을 따른다.

21 침해사고 대응

21.1 정보보호 최고책임자는 침해사고가 발생할 경우 효과적인 대응을 위해 한시적으로 침해사고 대응팀을 구성해 운영할 수 있다.

21.2 침해사고 대응 담당자는 사후 조사를 위한 관련 증거 확보를 지원하고 침해사고의 원인을 분석해 빠른 시간 안에 서비스가 복구될 수 있도록 해야 한다.

21.3 침해사고 대응에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

22 징계의 종류

22.1 징계의 종류는 인사 규정의 징계 규정을 따른다. 단, 징계를 위한 인사위원회의 심의 결과에 따라 징계 대상자에 대해 징계를 하지 아니하고 경고를 할 수 있다.

22.2 징계의 종류에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

23 IT 보안 관리 규정의 유지 관리

23.1 정보보호 정책 담당자는 IT 보안 관리 규정 및 절차 규정 등의 타당성을 연 1회 정기적으로 검토해야 하며, 필요시 추가 검토를 수행할 수 있다.

23.2 IT 보안 관리 규정은 해당 실무자들과 함께 개정 요인을 검토 후 정보보호 최고책임자의 승인을 득해야 한다

23.3 IT 보안 관리 규정의 유지 관리에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.

24 정보 보호 관리 체계의 운영

24.1 정보보호 담당 부서는 회사의 핵심 서비스에 영향을 주는 유·무형의 자산을 모두 식별해 정보보호 관리체계 범위를 설정하고, 이를 유지하기 위해 적절한 정보보호 계획을 매년 수립·운용해야 한다.

24.2 정보보호 관리체계의 운영에 관한 상세 기준은 "IT 보안 절차 규정"을 따른다.