정보보호규정

1. 적용범위

1.1 목적

SK 스퀘어주식회사(이하 "회사")의 정보자산을 도난, 파손, 변조, 유출 등으로부터 안전하고 효과적으로 지키기 위하여 정보보호 관리체계의 운영기준을 만들고 이를 임직원이 준수함으로써 회사가 경쟁력을 강화하고 안전한 기업경영 환경에서 영구히 존속 발전할 수 있도록 함을 목적으로 한다.

1.2 적용범위

이 규정은 회사의 모든 임직원과 회사가 보유하고 있는 유·무형의 모든 정보자산에 대하여 적용한다.

1.3 정의

이 규정에서 사용하는 주요 용어의 뜻은 "정보보호 용어정의" [별지 #7]를 따른다.

1.4 규정 및 지침 검토

1) 내부 규정 및 지침은 정기적으로 타당성 검토를 실시하고 결과에 따라 제·개정을 수행하여야 한다.
2) 정보보호 관련 법적 요구사항을 지속적으로 파악하여 최신성을 유지하기 위하여 다음의 절차에 따라 법규 준수 여부를 수행하여야 한다.
   (1) 정보보호 관련 법규 변경 시 정보보호규정 및 관련 절차에 미치는 영향을 파악하여 이를 반영하도록 하며, 이때 반드시 법무부서 및 이해관계자의 검토를 거치도록 한다
   (2) 주관부서는 검토가 완료된 개정안에 대하여 해당 규정에서 요구하는 승인을 득한 후 전사 공표 및 시행을 한다

(3) 정보보호 관련 법적 요구사항에 대한 검토는 정기/비정기로 수행한다 (정기 : 연 1 회, 비정기 : 법률 제·개정 시)

2. 임직원의 역할 및 책임

2.1 임직원의 역할 및 책임

1) 임직원은 회사의 정보자산을 보호하여야 하며, 회사의 정보보호 정책과 프로세스를 준수하여야 한다.
2) 임직원은 정보보호를 위해서 다음 각호의 사항을 준수할 의무를 가진다.
   (1) 회사 정보자산의 업무 용도 사용 이외의 사적 용도 사용 금지
   (2) 회사 승인 없이 정보 자산의 내·외부 임의 유출 및 제공 금지
   (3) 정보자산의 외부 반출 또는 송신 시 사전 통제 절차 준수
   (4) 허가 범위 내의 정보자산만 이용하여야 하며 허가 받지 않은 정보자산 접근 또는 허가된 권한 이외의 권한획득 시도 금지
   (5) 회사에서 승인 받지 않은 소프트웨어 및 정보저장 매체 사용 금지
   (6) 보관기간이 지난 문서의 폐기 및 사용자 단말 저장 금지
   (7) 사무 환경의 생활 보안 준수
   (8) 정보보호사고 징후 발견, 정보보호사고 발생 시 정보보호부서 신고
   (9) 기타 회사의 정보자산에 Risk 를 증가시키는 행위 등의 금지
3) 임직원은 아래와 같은 사유로 외부통신망을 통해 내부 업무망에서의 업무수행이 필요한 경우 "원격근무 보안관리지침" [별지 #8]의 수칙을 준수하여야 한다.
   (1) 출장, 회의 등의 업무상 외부 네트워크 환경에서의 업무 수행이 필요한 경우
   (2) 재해, 재난, 전염병 등 물리적인 사무실 출근이 제한되는 경우
   (3) 정보시스템 장애대응 및 신속한 업무지원이 필요한 경우
   (4) 그 밖에 업무상 사외 근무가 필요한 경우
4) 그 외 임직원 및 외부인에 대한 보안관리기준은 "인력보안관리지침" [별지 #2]를 참고한다.

2.2 임원의 역할 및 책임

1) 임원은 담당 조직의 보안 수준이 지속적으로 유지될 수 있도록 하여야 하며 조직 구성원들이 보안 정책을 준수할 수 있도록 독려하고 정보보호 리더로서 솔선수범 하여야 한다.
2) 임원은 담당비서가 다음 각 호의 사항을 준수하도록 관리하여야 한다.
   (1) 임원의 부재 시 노트북 및 출입문 잠금 상태 확인 등
   (2) 임원의 이메일 계정 직접 관리 금지 등
   (3) 임원용 기밀문서 PC 저장 및 임의 취급 금지 등

2.3 조직장의 역할 및 책임

1) 조직장은 단위조직의 정보보호에 대한 일차적인 책임자임을 인식하고 단위조직의 정보보호 수준을 유지할 책임과 의무가 있다.
2) 조직장은 소속사원과 단위조직에서 관리하는 협력직원 및 용역직원이 정보보호 정책과 프로세스를 준수 할 수 있도록 독려하고 정보보호에 대한 교육과 감독을 수행한다.
3) 조직장은 단위조직의 정보자산에 대한 취약점이 발생하지 않도록 예방하여야 하며, 정보보호사고 징후 발견 또는 보안 취약점이 발견되는 경우 정보보호부서에 신속하게 신고하여야 한다.

3. 정보보호 조직의 책임 및 역할

3.1 정보보호최고책임자 및 정보보호 담당부서

1) 회사는 임원급의 임직원을 대상으로 정보보호최고책임자(이하 CISO)를 선임하여, 정보보호 정책 수립, 정보보호위원회의 구성 및 운영, 위험분석 및 관리, 보안사고 대응 및 복구 등 회사의 정보보호에 관한 업무를 총괄·관리하도록 한다.
2) 정보보호 담당부서는 CISO 의 업무를 보좌하여 전사 정보보호 총괄업무 및 의사결정을 지원한다. CISO 의 상세 역할에 관하여는 "정보보호 조직 및 역할" [별지 #1]을 참조한다.

3.2 업무 영역별 정보보호책임자 및 정보보호 담당부서

1) 회사는 업무 영역별로 각각 정보보호 담당자를 두며 세부 내용에 관하여는 "정보보호 조직 및 역할"[별지 #1]을 참조한다.
2) 제 3.2 항 1 호에 명시적으로 포함되지 않는 경우에는 정보보호 담당부서에서
   관련업무의 역할을 조정한다.

3.3 부서별 정보보호 및 보안담당자

1) CISO 는 필요시 전사 정보보호활동을 효율적으로 수행하기 위해서 일정 규모 이상 조직에 대해서는 정보보호 담당자를 지정할 수 있으며,
   필요시 자체 보안 진단 실시 등 보안관리 업무와 정보보호 담당부서에서 주관하는 보안 교육에 참석할 수 있으며, 부서 내 전파를 수행할 수 있다.

3.4 정보보호위원회 구성 및 운영

1) 정보보호위원회는 회사의 정보보호 현안에 대한 협의를 진행하기 위해 운영된다.
2) 정보보호위원회 위원장은 CISO 가 역임하며, 영역별 정보보호 담당자로 정보보호위원회를 구성하고 운영한다.
3) 정보보호위원회의 역할은 다음 각 호와 같다.
   (1) 주요 정보보호 정책과 보안 관련 안건의 검토 및 승인
   (2) 정보보호를 강화하기 위한 중요 사업 검토
   (3) 정보보호 계획, 인식, 이행, 침해사고 대응 활동 방안 등의 검토
   (4) 전사 정보보호 활동 계획 협의 및 시행
   (5) 전사 차원의 정보보호 관련 프로세스 수립
   (6) 전사 보안 관련 업무 협의
4) 정보보호위원회는 정기적으로 개최되며, 필요 시 CISO 가 소집할 수 있다.

4. 정보자산 관리

4.1 정보자산 관리

1) 정보자산 관리는 정보보호의 기본 대상이 되는 정보자산을 식별, 분류, 중요도 평가, 등급 분류 등을 하여 지속적으로 관리하는 것을 말한다.
2) 정보보호 담당부서는 정보자산 소유부서에 정보자산 관리를 요청할 수 있다.
3) 정보자산 관리는 "위험분석 및 자산관리 기준" [별지 #9]을 따르며 업무 영역, 정보시스템 환경 특성에 따라 별도의 기준을 수립하여 관리할 수 있다.

4.2 정보자산 식별 및 분류

1) 정보자산은 정보자산 소유부서에서 식별할 기본적인 책임이 있으며, 정보보호 담당부서는 필요 시 소유부서에 정보자산 식별을 요청할 수 있다.
2) 식별된 정보자산은 "위험분석 및 자산관리 기준" [별지 #9]의 정보자산 유형 기준에 따라 식별 및 분류하여야 하며 부서의 업무 특성에 따라서 분류 기준을 조정할 수 있다.

4.3 정보자산 중요도 평가 및 보안등급 분류

1) 정보자산 보유부서는 식별된 정보자산의 중요도를 평가하고 보안 등급을 부여 하여야 한다.
2) 정보보호 담당부서는 중요도 평가 기준과 보안등급 분류 기준을 수립하여야 하며 정보자산 보유부서의 중요도 평가와 보안등급 분류 결과를 검토하여 유사한 정보자산이 부서별로 차이가 발생하지 않도록 조정 할 수 있다.
3) 정보자산 보유부서는 주기적으로 자산의 중요도 및 보안등급의 적절성 여부를 재평가하여야 한다.

5. 주요 업무영역 별 정보보호

5.1 IT보안영역

IT 보안영역의 대상은 사내망, 대외서비스에 포함된 정보시스템, 인력, 시설 등을 말한다.

5.2 IT보안 정보보호활동

1) 정보보호 담당부서 IT 보안영역에 대한 정보보호활동을 수행하여야 하며, IT 보안관리자는 "정보보호 조직 및 역할" [별지 #1]의 상세 역할을 수행한다.
2) 정보시스템 운영부서는 보안정책 및 프로세스를 준수하여 정보시스템을 운영하여야 하며, 보안취약점이 발견되면 확인 후 즉시 조치하여야 한다.
3) IT 보안의 세부 내용에 관하여는 "IT 보안절차규정" 을 따른다.

5.3 인적·물리적 보안영역

인적·물리적 보안영역의 대상은 임직원, 협력직원, 용역직원 및 회사를 방문하는 방문자에 대한 인적 영역과 회사 사옥, 임대 사무실 및 시설의 물리적 영역을 말한다.

5.4 인적·물리적 정보보호활동

1) 인적·물리적 보안관리부서는 인적·물리적 보안영역에 대한 정보보호활동을 수행하여야 하며, 인적·물리적 보안담당자는 "정보보호 조직 및 역할" [별지 #1]의 상세 역할을 수행한다.
2) 인적·물리적 정보보호활동은 업무 특성을 고려하여 정보보호 담당부서에서 직접 수행 할 수 있다.
3) 인적 보안의 세부 내용에 관하여는 "인적보안 관리기준" [별지 #2]을 따르고 물리적 보안에 관하여는 인적·물리적 보안관리부서의 내규에 따른다.

6. 정보보호 진단

6.1 정보보호 진단 수행

1) 정보보호 진단은 정보보호영역에 대해서 정보보호정책과 프로세스 준수, 정보보호활동의 이행 여부를 확인 하는 것을 말한다.
2) 정보보호 담당부서는 연간 계획을 수립하고, 정보보호 진단을 수행 할 책임이 있다.
3) 정보보호 진단 수행 시 수검부서의 임직원은 적극적으로 협력하여야 한다.
4) 정보보호진단은 다음 각 호와 같이 수행 한다.

(1) 보안 정책 및 프로세스 이행 진단 등
(2) 모의 해킹
(3) 정보시스템 보안 진단
(4) PC 보안점검
(5) 모의 보안 훈련
(6) 신규 기술 보안 진단 등
(7) 기타 보안 취약점 관련 진단 활동 추가 수행

6.2 정보보호진단 통보 및 조치

1) 정보보호진단부서는 정보보호진단 결과를 수검부서에 통보하여야 하며, 수검 부서는 진단 결과에 따른 조치 계획을 수립 및 이행 하여야 한다.
2) 정보보호 담당부서는 진단 결과와 수검부서의 조치 계획을 취합하여 CISO 에게 보고하고, 조치가 완료 될 때 까지 이행 여부를 관리하여야 한다.
3) 기술적 취약점의 경우 심각도와 시스템 상황에 따라서 단계적으로 조치를 수행 할 수 있으나, 정보보호사고 발생 가능성이 있는 심각한 취약점의 경우 즉시 조치를 수행하여야 한다.

7. 정보보호 교육 및 변화관리

7.1 교육계획 수립 및 수행

1) 정보보호 담당부서는 연간 정보보호 교육 및 변화관리 계획을 수립하고 임직원을 대상으로 정기적으로 수행하여야 한다.
2) 정보보호 교육 및 변화관리는 대상자의 직위 및 담당하는 업무의 특성에 따라 필요한 내용으로 실시하여야 한다.

7.2 교육결과 검토 및 보완

1) 정보보호 담당부서는 실시한 교육 결과 피드백에 대해, 차기 교육 시 개선·반영 될 수 있도록 고려하여야 한다.

8. 정보보호 투자계획 수립 및 관리

8.1 정보보호 투자계획 수립 및 관리

1) 회사의 정보보호 수준을 향상시키고 정보보호활동을 지속적으로 수행할 수 있도록 정보보호 담당부서는 해당 영역에 대한 정보보호 투자계획을 매 년 수립하여야 한다.
2) 정보보호 담당부서는 전사적으로 정보보호 투자계획이 원활하게 실행될 수 있도록 정보보호 투자계획의 이행을 관리하여야 한다.

9. 정보보호사고 대응

9.1 정보보호사고 대응

1) 정보보호사고(및 개인정보사고)가 발생하는 경우 심각도에 따라서 정보보호 종합 상황실 운영 및 영향도를 파악하고 신속한 복구 조치를 통해 회사에 발생할 수 있는 위험을 최소화하여야 한다.
2) 정보보호사고는 해킹, 악성코드 감염 등의 외부적 요인과 정보자산 도난, 파손, 유출 등의 내부적 요인 등 회사의 정보자산 및 고객에게 피해를 입힐 수 있는 복합적인 형태로 발생하며, 상세 유형은 "정보보호사고대응 규정"을 참조한다.

9.2 정보보호사고 대응 관련 조직별 역할 및 주요 활동

1) 정보보호 담당부서는 정보보호사고 상황 통제 및 전파를 하고 정보보호 종합상황실을 운영한다.
2) 정보보호 담당부서는 정보보호사고에 대한 원인 및 피해 규모를 분석하고 정보보호사고 복구를 위한 기술적, 관리적 조치를 취한다.
3) 전사위기대응기구는 언론, 정부, 수사기관의 상황을 파악하고 전사 Risk Mgmt. 체계에 따른 임무를 수행한다.
4) 정보보호 사고 대응의 세부 내용에 관하여는 "정보보호사고대응 규정"을 따른다.

10. 정보보호 포상 및 징계

10.1 정보보호 포상

1) CISO 는 정보보호 및 고객정보보호 실천 우수 조직 또는 보안활동을 적극적으로 수행하여 정보보호 사고를 미연에 방지한 임직원에게 포상을 요청할 수 있다.

10.2 정보보호 징계

1) CISO 는 다음 각 호의 어느 하나가 의심되는 경우 해당하는 조직 또는 임직원에게 내부 규정에 의거하여 주관부서에 징계를 요청 할 수 있다.
   (1) 본 규정 및 회사의 보안 정책, 지침, 가이드를 위반하는 경우
   (2) 정보보호 준수 의무를 이행하지 않는 경우
   (3) 정보보호 조치를 이행하지 않거나 미흡하게 조치하여 보안 사고가 발생하거나 회사의 사고 발생 Risk 가 증가 한 경우
2) 조직, 임직원에 대한 포상 및 징계는 정보보호위원회를 통해 상정되며, 업무 주관부서와 협의하여 요청한다.
3) 회사는 징계 대상자에 대한 관리책임으로 직상위 및 차상위 감독자를 징계할 수 있다.

부칙

본 규정은 2022 년 1 월 3 일부터 시행한다.