PC&I-R-078

개정 이력

일자	버전	내용	작성자
2022.12.09	1.0	신규 제정	황종현

정보 보호 정책

제 1 장 총칙

제 1 조 [목적]

이 정책은 주식회사 팬택씨앤아이 계열 지주사 및 계열 회사(이하 '회사'라 한다)의 정보 보호를 위한 최상위 정책으로서 비인가자에 의한 정보의 오남용, 훼손, 위변조, 유출 등의 위협으로부터 중요 정보 자산을 보호하기위한 기본 방침을 정립하는 것을 목적으로 한다.

제 2 조 [적용 범위]

이 정책은 회사의 전 직원 및 제 3자에 적용하며, 제 3자에는 외부 출입자, 일용 근로자 및 회사와 계약 관계에 있는 자 등을 포함한 모든 외부인을 포함한다.

제 3 조 [용어의 정의]

이 정책에서 사용하는 용어의 정의는 다음과 같다

1. 정보 보호 : 정보의 생성, 저장, 처리, 송수신 시에 발생할 수 있는 정보의 훼손, 위변조, 유출 등을 비용 대비 효과적으로 방지하여 정보에 대한 기밀성, 무결성, 가용성을 확보하는 것이다.
2. 정보 자산 : 회사가 보유하고 있는 정보 자체는 물론 그 정보를 만들거나 보관, 전송하는 장치 또는 시설물, 기록 문서, 인쇄물, 도면, 전산 시스템 등 영업상의 비밀을 포함하고 있는 모든 물질
3. 기밀성 : 자산이 적절한 수준의 비밀을 유지하면서 공개되지 않으며, 오직 인가된 사람만이 정보에 접근할 수 있다.
4. 무결성 : 자산의 고유 성질이 인가되지 않은 내부 또는 외부로부터 변경 또는 변조되지 않고 정확성과 완전성을 유지할 수 있다.
5. 가용성 : 인가된 사용자가 자산을 이용하고자 할 때 해당 자산의 이용 가능한 정도를 나타내며 해당 정보와 관련한 자산에 접근할 수 있음을 보장하는 것이다.

제 4 조 [정보 자산 소유권]

모든 정보 자산은 중요한 자산으로서 회사가 그 소유권을 갖는다. 따라서 정보 자산은 업무 목적으로만 사용될 수 있으며, 개인의 이익을 위해 사용될 수 없다. 회사는 정보 생산 시, 해당 정보에 대한 소유권자, 운영자, 사용자를 지정해야 한다.

1. 소유권자는 해당 부서의 직책자(팀장 등)로서 정보 자산의 생산, 분류, 보관, 접근 승인, 폐기 등의 권한과 책임을 가지며 운영자, 사용자를 지정한다.

2. 운영자는 소유권자의 지침에 따라 특정 정보 자산에 접근 권한을 승인하고 이에 따른 위험을 예방, 관리하는 자이다.
3. 사용자는 소유권자 및 운영자로부터 특정 정보 자산에 접근 권한을 받아 사용하는 자이다.

제 5 조 [정보 보호 범위]

1. 정보 보호는 회사의 전 조직을 대상으로 한다. 정보 보호 대상이 되는 회사의 자산은 다음을 포함한다.
    ① 정보 자산
    ② 문서 자산
    ③ 소프트웨어 자산
    ④ 하드웨어 자산
    ⑤ 기타 자산
2. 회사가 책임이 있거나 통제를 하고 있는 외부의 공급자나 고객과의 모든 의사 소통 인터페이스를 포함하며, 회사가 고객에게 공급하여 고객 사이트에 위치한 장비 또한 회사의 자산이므로 정보 보호 범위에 포함시킨다.

제 6 조 [책임 사항]

회사의 정보 보호에 대한 책임은 전 임직원에게 있으며 이를 위하여 정보 보호 관련 정책, 지침을 모든 임직원이 준수해야 한다.

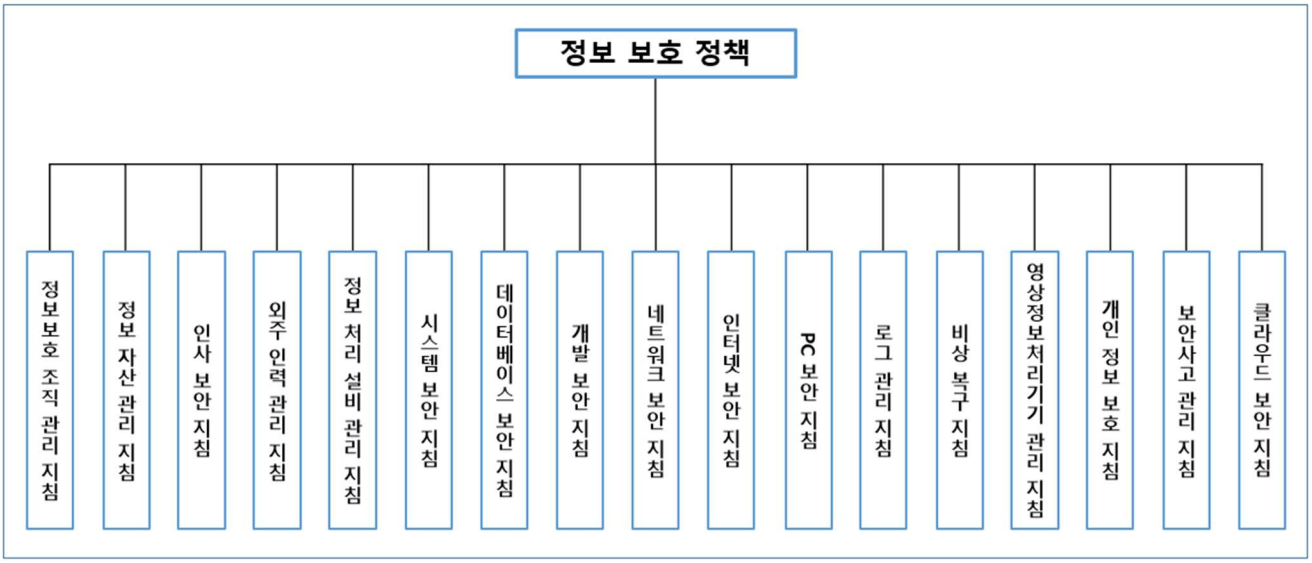
제 2 장 정보 보호 정책

제 7 조 [정보 보호 정책 및 지침 체계]

1. 정보 보호 정책, 지침 체계는 1개의 정보 보호 정책과 17개의 지침으로 이루어진다.
2. 회사의 최상위 정보 보호 정책으로 정책 및 지침의 체계를 선언하며, 각 지침은 임직원 및 실무 정보 보호 관련 업무 직원들이 수행해야 하는 업무 역할 및 수행 내역을 정의한다.

제 8 조 [정보 보호 정책 및 지침 수립]

1. 회사 업무와 정보 위험의 관계를 분석한 후, 사업 수행 영향을 중심으로 정책을 수립한다.
2. 정보 보호 정책의 효과적인 적용을 위해서 적용 대상 그룹별 상이한 정보 보호 요구 수준을 고려하여 지침을 별도 수립한다.
3. 정책 및 지침을 이해관계자들과 검토 및 수정 후, 정보 보호 최고 책임자의 승인을 받는다.



제 9 조 [정보 보호 지침 항목]

1. 정보 보호 조직 관리
   ① 회사 내 정보 보호 활동을 관리하기 위한 정보 보호 책임자, 정보 보호 관리자, 정보 보호 담당자를 포함한 조직 구조를 가져야 한다.
   ② 정보 보호 조직의 역할과 책임을 정의하고 이를 수행한다.
2. 정보 자산 관리
   ① 정보 자산을 분류하고 이에 대한 생성, 변경, 파기에 대한 관리를 수행해야 한다.
   ② 정보 자산의 중요도를 산정하고 등급에 따른 관리 정책을 수립해야 한다.
3. 인사 보안
   ① 입사, 퇴사, 휴직, 복직 및 고용이 유지되는 임직원 관련 인적 보안 활동을 수행한다.
   ② 모든 임직원의 정보 보안 교육 계획을 수립하고 이행해야 한다.
4. 외주 인력 관리
   ① 외주 용역 업체와 계약 체결 시, 정보 자산을 보호하기 위한 요구 사항을 계약서 상에 명시하고 준수 여부를 관리해야 한다.
   ② 외부 인력에 대한 업무 수행 시작부터 계약의 만료 시 수행해야 하는 통제 사항을 마련하여 시행해야 한다.
5. 정보 처리 설비 관리
   ① 정보 처리 설비에 대한 무단 접근, 도난, 파괴 및 업무 방해 행위로부터 물리적 보호를 위하여 보안 구역을 설정하고 물리적 보안 관리를 실시해야 한다.
   ② 물리적 위치 및 배치, 내부 설비, 전원 공급 등 환경상의 위협을 최소화할 수 있는 대책을 마련해야 한다.
6. 시스템 보안
   ① 정보시스템의 기밀성, 무결성, 가용성을 확보하기 위하여 정보시스템의 도입 단계부터 운영 및 폐기 단계까지 체계적인 보안 관리 절차를 수립하고 관리자를 지정하여 이행한다.

② 회사 중요 정보를 보호하기 위하여 암호 강도, 계정 관리 등 통제 절차를 수립한다.

7. 데이터베이스 보안
   ① 데이터베이스의 기밀성, 무결성, 가용성을 확보하기 위하여 데이터베이스 도입 단계부터 운영 및 폐기단계까지 체계적인 보안 관리 절차를 수립하고 관리자를 지정하여 이행한다
   ② 회사 중요 정보를 보호하기 위하여 계정 관리, 권한, 암호화 항목, 암호화 강도, 암호키 관리 등 통제 절차를 수립한다.
8. 개발 보안
   ① 응용프로그램 개발 시 검토해야할 정보 보호 항목을 작성해야 한다.
   ② 개발을 외주 위탁하는 경우, 정보보호 관련 관리 및 요구 사항을 명확하게 반영할 수 있도록 관리해야 한다.
9. 네트워크 보안
   ① 네트워크를 통해 고의, 과실로 인한 정보 누출, 변조, 파괴하려는 행위로부터 보호해야 한다.
   ② 네트워크 신규 구축, 변경, 중지 등 변화 관리 항목을 수립해야 한다.
10. 인터넷 보안
   ① 사내 인터넷 및 전자 우편과 관련된 보안 관리 방안을 수립하고 실시해야 한다.
11. PC 보안
   ① 사내에 반입되는 모든 사용자의 PC(노트북)에 대한 승인, 이용 및 관리 등 보안 관리 절차를 수립하고 안전한 PC 관리를 위한 통제 방안을 마련해야 한다.
12. 로그 관리
   ① 시스템 로그를 보관하고 관리하는데 필요한 기준을 마련하고 보관된 로그의 무결성을 확보해야 한다.
13. 비상 복구
   ① 정보 시스템 재해 발생을 방지하기위한 사전 대비 및 재해 발생 시 신속한 대응, 복구 계획을 수립해야 한다.
14. 영상정보처리기기 관리
   ① 영상정보처리기기(CCTV) 설치, 운영, 보호 방안을 마련하여 개인 영상 정보의 안전성, 신뢰성을 확보해야 한다.
15. 개인정보 보호
   ① 회원 개인 정보 자산을 체계적으로 관리하고 허가 받지 않은 공개, 오남용, 변경, 파괴로부터 개인 정보를 보호, 관리하기위한 지침을 마련해야 한다.
16. 보안 사고 관리
   ① 각종 보안 사고 예방 및 대응 방안을 수립하여 관리하여야 한다.
17. 클라우드 보안
   ① 클라우드 기반 시스템 도입 및 구축 시, 정보 자산 보호를 위한 방안을 수립하여 관리하여야 한다.

제 3 장 정보 보호 정책 유지 관리

제 10 조 [정보 보호 정책 검토 및 평가]

1. 정보 보호 담당자는 업무 환경 변화에 따라 정보 보호 정책 및 지침의 타당성을 검토해야 하며, 필요 시 추가 검토를 수행하여 변경할 수 있다.
2. 정보 보호 정책 및 지침 평가 시 정책 및 지침의 효과, 관련 법적 요구 사항, 기술 변화 및 보안 사고 발생 유형에 대해 검토해야 한다.

제 11 조 [정보 보호 정책 개정]

3. 정보 보호 담당자는 업무 환경 변화에 따라 정보 보호 정책 및 지침의 타당성을 검토해야 하며, 필요 시 추가 검토를 수행하여 변경할 수 있다.
4. 정책 및 지침 변경 시 다음 절차에 따라 수행한다.
    ① 실무자 및 정보 보호 담당자의 개정 필요성 검토
    ② 개정안 작성 및 정보 보호 책임자 검토
    ③ 최고 책임자 검토 및 승인 절차 진행
    ④ 개정된 정책 및 지침 공표