

보안 사고 관리 지침

제 1 조 [목적]

이 정책은 주식회사 팬택씨앤아이 계열 지주사 및 계열 회사(이하 '회사'라 한다)의 보안 사고 예방 및 보안 사고 발생 시의 대응 방안을 제시하여 회사 정보 자산에 대한 대/내외 침해 위협 요소를 제거하여 안정적인 운용을 목적으로 한다.

제 2 조 [적용 범위]

회사의 서버 및 네트워크 등 정보시스템, 주요 사업 정보 및 개인 정보를 포함한 정보 자산을 범위로 한다.

제 3 조 [용어의 정의]

이 지침에서 사용하는 용어의 정의는 다음과 같다

1. 보안 사고 : 외부 또는 내부의 악의적인 사용자에게 의해 회사의 정보 자산에 대한 피해 또는 자료의 유출 등이 발생하는 것.
2. 보안 사고 대응팀 : 회사 정보 자산에 대해 보안 사고를 예방하기 위한 대책을 제시하고, 보안 사고 발생 시 신속하게 원인을 규명하여 사고 확산을 억제하기 위한 역할을 수행하는 조직.
3. 감사 추적 : 시스템 접근 단계에서 종료 단계까지의 일련의 과정에서 행한 모든 활동을 재생, 검토, 조사할 수 있는 시스템 활동의 시간 별 기록을 추적하는 것.
4. 로그 : 서버, 네트워크, 업무시스템 등 장비 및 시스템 사용에 관련된 전체의 기록.
5. 악성 소프트웨어 : 서버, 네트워크, 업무시스템 등 장비 및 시스템에 위해를 가할 목적으로 제작된 바이러스, 웜, 랜섬웨어 등 모든 소프트웨어.
6. 취약성 : 조직 내부 혹은 정보 시스템을 사용하는 환경에 내재된 약점으로 위협에 의해 자산이나 조직의 업무 환경에 피해를 입힐 수 있는 가능성을 제공하는 요소.

제 4 조 [보안사고 대응 체계]

보안 사고를 효과적으로 예방 및 모니터링하고 대응하기 위하여 다음과 같은 중앙집중적인 대응 체계가 구축되어야 한다.

1. 보안 사고 대응 체계 구성 및 역할

- ① 정보보호 책임자

보안 사고 예방 및 보안 사고 대응 전반에 대한 관리의 책임을 가지며, 보안사고에 대하여 보고를

받고 사고의 영향을 파악하며 이를 보고하는 역할을 수행한다.

② 정보보호 관리자

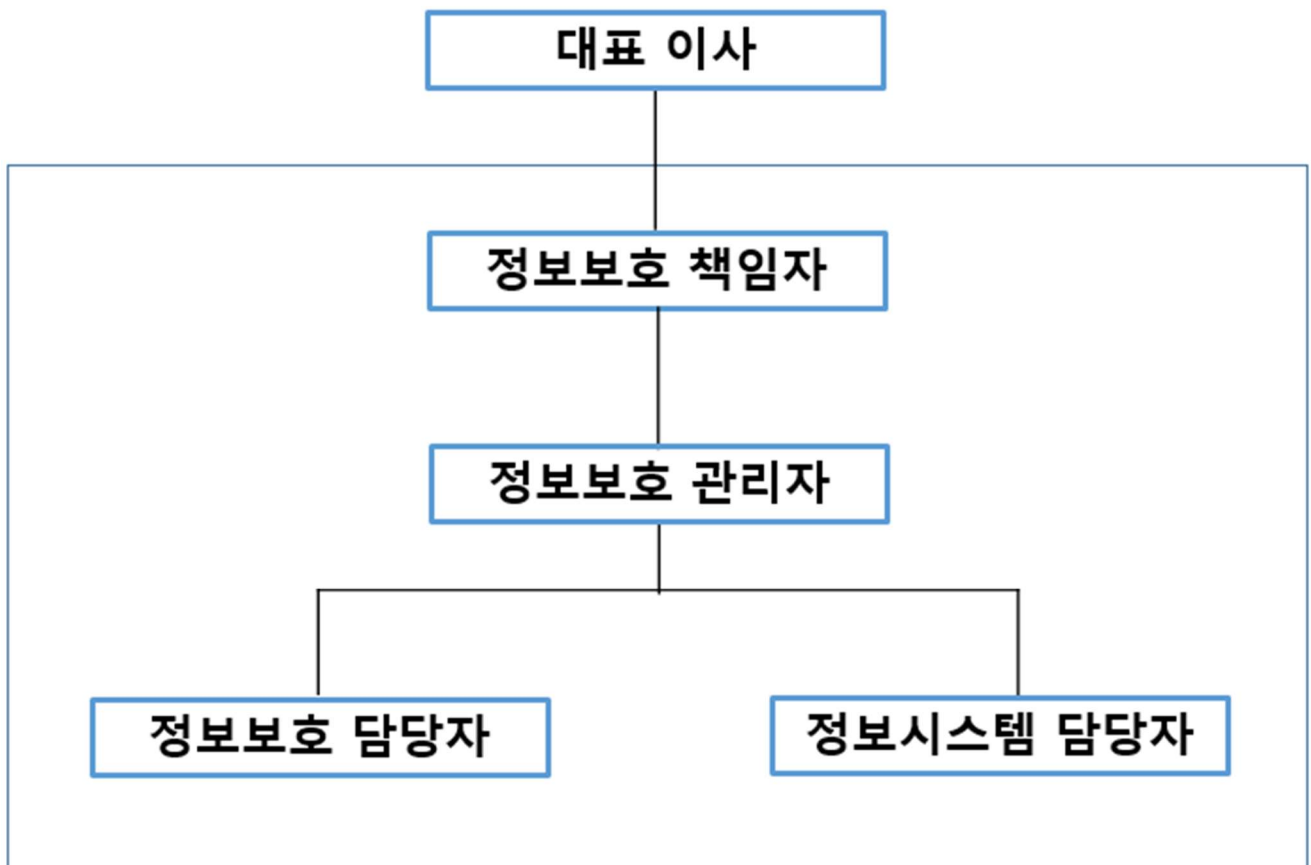
보안 사고 예방을 위하여 정보 자산에 대한 주기적인 점검을 수행해야 하며 정보보호 담당자 혹은 정보시스템 운영 담당자가 수행한 보안 점검 결과를 바탕으로 취약성 보완 계획을 수립 및 시행한다.

③ 정보보호 담당자

정보 자산에 대한 주기적인 보안 점검의 실무를 담당하며, 보안 점검 결과를 정보보호 관리자에게 보고하고 취약성 보완 계획을 수행한다. 보안 사고 발생 시, 대응 수행의 실무를 담당한다.

④ 정보시스템 담당자

보안 사고 발생 시, 대응 및 복구 수행의 실무를 담당한다.



2. 보안 사고 대응팀 구성 및 역할

① 보안 사고 발생 시 대응을 위해 보안 사고 대응팀을 구성한다.

② 보안 사고 대응팀은 정보보호 담당 조직, 보안 사고 발생 현업 조직, 법적 문제에 대응할 법무 조직 등 관련 조직 및 담당자로 구성한다.

③ 보안 사고 대응팀은 회사 보안 사고에 대해 총괄 대응을 담당하고, 보안 사고의 분석 및 대응책 수립, 복구 수행, 물적 및 인적 자원을 지원한다.

- ④ 보안 사고에 대한 신속한 대응을 위한 유지보수 업체 등의 관련 기관을 포함한 비상연락체계를 구축한다.
- ⑤ 개인정보와 관련된 보안 사고일 경우, 이용자의 손실과 기업 이미지 손상 등 법적 문제 발생 소지에 대해 법무 조직과 협력 체계를 구축한다.
- ⑥ 보안사고 대응팀은 보안 사고와 관련된 이상 징후를 발견 시, 이에 대한 증거를 확보하고 대응하며 대표이사에게 보고한다.

3. 외부 기관 협력

사고 사안에 따라 다음의 외부 기관과 협력하여 대응할 수 있다

- ① 정보보호 서비스 전문 기업
- ② 한국인터넷진흥원(KISA)
- ③ 국가사이버안전센터(국정원)
- ④ 사이버 수사대 및 사이버 테러 대응센터(경찰청)
- ⑤ 그 외 보안사고대응전문 기관

제 5 조 [보안 사고 예방]

1. 보안 사고 대응 계획

보안 사고가 발생했을 경우 신속히 대응하기 위한 보안사고 대응 계획은 다음의 사항을 포함하여 수립한다.

- ① 보안 사고의 정의 및 범위
- ② 긴급연락체계 구축
- ③ 보안 사고 발생 시 보고 및 대응 절차
- ④ 사고 대응 조직 구성
- ⑤ 보안 사고 교육 계획

2. 보안 사고 재발 방지 대책 및 대응 체계 변경

보안사고 분석 결과, 기존 대응 절차 및 계획에 따라 대응하기 어렵거나 대응 절차상에 문제가 발견된 경우에는 유사 사고가 반복되지 않도록 본 지침을 개정한다.

3. 보안 사고 대응 훈련

- ① 회사는 해킹 등 침해 사고에 대한 대응 능력을 확보하기 위해 연 1 회 이상 침해 사고 대응 및 복구 훈련을 계획하고 실시하여야 한다.
- ② 보안 사고 대응 훈련에는 악성 코드 대응 및 해킹 탐지 대응, 복구 훈련을 포함하여야 한다.

제 6 조 [보안 사고 대응 절차]

보안 사고 발생 시 대응 절차는 보안 사고 탐지 및 접수, 사고 분석, 대책 방안 수립 및 전파, 사고 처리 및 복구, 사후 조치의 순서로 구성되며 사고 발생 후 처리 되기까지의 각 단계를 파악할 수 있고 진행 경과를 추적 가능하도록 기록되어야 한다.

1. 보안 사고 탐지 및 접수

- ① 정보 보호 담당자 및 정보시스템 운영 담당자는 정보시스템에 다음과 같은 비정상적인 활동이나 심각한 이상 징후 발견 및 해킹 침입으로 판단될 경우, 이를 확인 및 점검하며 보안 사고로 판단될 시 정보보호 관리자에게 통보한다
 - 가) 연속적인 접속 실패 확인
 - 나) 같은 사용자 이름으로 두 명 이상 동시에 접속되고 있는지 확인
 - 다) 관리자 권한이 필요한 명령어의 비정상적인 사용 또는 적절하지 않은 사용 시도가 있었는지 점검
 - 라) 보안 관련 파일의 수정 및 시도가 불법적으로 이루어졌는지 점검
 - 마) 허가되지 않은 파일 및 자원 또는 서비스의 사용 시도를 확인
 - 바) 네트워크 부하를 가중시키는 비정상적인 프로그램 실행이 있는지 점검
 - 사) 한 사용자가 많은 외부 접속을 시도하고 있는지 점검
 - 아) 서버의 비정상적인 동작에 대하여 외부의 불법적인 침입이 있는지 점검
 - 자) 내부 네트워크에서 침입한 경우 현재의 단말 위치를 확인 및 점검
 - 차) 현재 침입자가 서버에 접속하고 있는 경우, 각종 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집
 - 카) 침입자가 중요한 데이터에 접근할 경우, 또는 침입자를 추적할 수 없을 경우에는 침입자의 접속을 강제로 차단
- ② 정보보호 관리자 및 정보보호 책임자는 다음 사항에 따라 보고 체계를 준수한다.
 - 가) 정보보호 관리자는 현재 상황 및 피해 상황을 파악한 후 즉시 정보보호 책임자에게 보고한다.
 - 나) 정보보호 책임자는 상황을 파악한 후 대표이사에게 보고한다.
 - 다) 보안 사고 대응이 완료되면 사고 발생 및 조치 결과 보고서를 작성하여 보고하고, 관련 조직 및 인력과 공유한다
- ③ 사용자가 다음과 같은 침입 징후를 발견하는 경우 즉시 정보보호 담당자에게 통보한다.
 - 가) 자신의 패스워드가 노출되었다는 의심이 드는 경우
 - 나) 최종 로그인 시간이 자신의 실제 최종 로그인 시간과 다르거나 로그인 시도가 실패했던 흔적이 보이는 경우
 - 다) 기타 정보시스템 사용 중 침입의 징후를 발견하는 경우
- ④ 정보보호 담당자는 접수된 침해 사고에 대해서 대응을 수행한다.
- ⑤ 개인 정보 유출로 확인될 경우, 정당한 사유가 없는 한 5 일 이내에 해당 정보 주체에게 다음 각 호의 사항을 알려야 한다.
 - 가) 유출된 개인 정보의 항목
 - 나) 유출 시점과 경위
 - 다) 유출 피해를 최소화하기 위하여 정보 주체가 할 수 있는 방법 등에 관한 정보
 - 라) 회사의 대응 조치 및 피해 구제 절차
 - 마) 정보주체의 유출 피해 사실 확인을 위한 회사의 담당 부서 및 연락처

- ⑥ 개인 정보 유출로 확인될 경우, 유출 시점과 인지 시점 간 시간적 차이에 대한 과실 유무를 입증하기 위한 기록을 확보하여야 한다.

2. 사고 분석 및 조치

- ① 정보보호 관리자는 접수 및 보고된 보안 사고에 대하여 사실 여부를 확인하고 사실로 확인될 경우 사고의 규모, 경위, 방법, 원인 및 관련자를 조사한다.
- ② 정보보호 관리자는 필요한 경우 정보보호 책임자가 승인한 외부 전문가의 지원을 받아 증거 자료를 수집한다.
- ③ 정보보호 담당자는 보안 시스템 로그를 점검하여 관련 기록이 있을 때에는 모든 로그를 백업한다.
- ④ 침입자가 사라졌거나 로그 파일의 분석을 통해 침입한 흔적이 발견된 경우 보안 진단 도구나 점검 목록을 이용하여 다음 사항을 점검한다.
 - 가) 새로운 계정이 생성 되었는지 확인 후 로그를 백업한다.
 - 나) 서버 및 어플리케이션 변경 및 수정 여부를 확인 후 기록한다.
 - 다) 데이터의 변조나 불법 접근의 흔적이 있을 경우, 해당 서비스를 중지시킨 후 기록한다.
 - 라) 침입자를 식별하기 위한 증거를 수집한다.
- ⑤ 정보보호 담당자는 분석 결과를 바탕으로 사고 조치 및 사후 보안 강화 조치 후, 보안 사고 발생 및 조치 결과 보고서를 작성한다.
- ⑥ 대표이사 및 관련 부서에서는 침해 사고와 관련하여 비즈니스 관점 및 사업 연속성 등을 고려하여 보안 사고에 대한 처리를 결정한다.

3. 대책 방안 수립 및 전파

- ① 정보보호 담당자는 보안사고 대책 방안을 수립하여 정보보호 관리자 및 책임자에게 보고한다.
- ② 승인된 대책 방안은 정보시스템 담당자 및 사용자에게 전파한다.
- ③ 보안 사고와 관련된 취약성 확인을 위해 사내 정보 시스템을 대상으로 모의 해킹 등 취약성 점검을 수행할 수 있다.