Kolmar	정보보호 사고대응지침 (Information Security Incident Response)	문서번호	ISPG-03
		개정번호	1.2

개정이력

Rev No.	제・개정일	개 정 사 유	작 성	검토	승인
1.0	2021-08-28	최 초 제 정	임헌재	최종환	전태영
1.1	2021-03-31	조직 변경	임헌재	최종환	박상용
1.2	2022-08-24	조직 변경	강민지	전지현	안순식

목차

제 3 장 정보보호 사고 대응 지침

제 1 절 적용범위

제 1 조 목적 및 범위

① 정보보호 사고 대응 지침(이하 '지침')은 내부 혹은 외부로부터 발생된 보안사고 인지 및 접수, 사고대응, 조치, 사후관리까지 정보보호 사고로 인한 피해의 신속한 복구와 조치가 가능하도록하여 업무에 미치는 위험을 최소화하는데 그 목적이 있다.

② 본 지침은 한국콜마홀딩스㈜ (이하 '지주회사')와 계열사 및 관계사의 모든 정보자산을 대상으로 하며, 정보자산의 피해(손실, 파괴, 변조, 유출 등)로 인해 발생되는 업무에 지장을 초래하는 모든 정보보호 사고에 적용된다.

제 2 조 용어 정의

① 이 지침에 사용되는 용어 정의는 다음과 같다.

가) 정보보호사고: 회사의 정보보호 정책이나 통제를 우회하거나 회피하여 중요한 정보자산 등을 변조, 파괴, 유출하는 등 회사 사업에 영향을 주는 모든 일련의 행위를 말한다.

나) 정보보호사고대응: 보안사고 발생 시 보안사고로 인한 피해를 최소화하기 위한 사고 접수, 조사, 분석, 처리 등 일련의 정의된 절차에 따라 업무를 수행하는 것을 말한다.

다) 침해사고: 해킹, 컴퓨터 바이러스, 랜섬웨어, 서비스 거부 또는 고출력 전자기파 등의 방법으로 네트워크 또는 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

라) 백도어: 백도어는 시스템의 보안이 제거된 비밀 통로로서, 서비스 기술자나 유지 보수 프로그래머들의 액세스 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 것을 말한다.

마) DOS 공격: DOS(Denial of Services)는 공격자의 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다.

제 2 절 정보보호 사고정의

① 정보보호사고정의는 일반적으로 관련 법, 규정 등 회사정책 통제정책을 위배하여 정보 자산에 변조, 손실, 파괴, 유출 등이 발생하여 업무에 지장을 초래 하는 사고를 말하며 다

음의 사건 이 발생할 경우 정보보호사고로 규정한다.

- 비인가자의 정보시스템 접근
- 정보자산 유출, 변조, 손실(DATA, 문서, 계정 및 패스워드 등)
- 정보시스템의 자원의 오용 및 손실, 절도, 파괴 등
- 악성 프로그램(바이러스, 백도어 등) 유포
- 정보시스템의 DOS공격 등 서비스거부 공격
- 네트워크장비, 시스템, 서버 및 PC 해킹
- 통제구역, 제한구역 등 불법구역 침입

제 3 절 정보보호 사고 대응 절차

제 1 조 정보보호 사고 인지 및 탐지

① IT인프라운영 부서는 시스템의 로그를 주기적으로 점검하여 비 정상적인 징후를 발견할 경우 부서장 또는 정보보호 담당자에게 신고한다.

② IT인프라운영 부서는 시스템 로그분석을 통해 외부에서 내부로 IT시스템의 침투흔적을 모니터링 한다.

③ 보안담당부서는 정보보호 유관기관, 백신업체, 보안뉴스 등 다양한 채널을 통해서 보안 취약점 및 해킹기법을 수집 확인하여 침투흔적을 모니터링 한다.

제 2 조 정보보호 사고 신고 및 접수

① 회사의 임직원 및 협력업체 직원은 업무 수행 시 정보보호 사고에 대한 징후를 인지한 경우, 임의로 문제해결을 시도 하지 말고, 즉시 정보보호담당자에게 신고하여야 한다.

제 3 조 정보보호사고 대응 및 보고

① 정보보호담당자는 정보보안 책임관리자에게 사고내용을 보고 하며 보고된 내용을 검토하여 사고피해 확산을 차단하기 위한 초기 대응이 이루어지도록 한다.

② 정보보호담당자는 사고의 긴급성을 판별하여 긴급 사고의 경우, 선 조치 후 보고할 수 있으며, 이에 대한 “정보보호 사고 보고서' 작성 시 정보보호 책임관리자에게 보고해야 한다.

③ 정보보호책임관리자는 사고 범위, 행위 주체, 경로 등 사건 관련 세부 내역을 파악하고 분석 업무 수행을 지시하며 그 결과를 지속적으로 모니터링, 취합하고, 상황 변화에 따

라 적절한 대응을 실시하여야 한다.

④ 사고발생 시 유관부서 관리자, 운영자는 정보보호담당자 요청 시 사고 분석에 필요한 증거를 제공 하여야 한다.

⑤ 정보보호담당자는 사고 분석에 필요한 증거들을 우선적으로 확보 해야하며, 수집된 증거자료는 분석 시 변조나 삭제가 일어나지 않도록 하여야 한다.

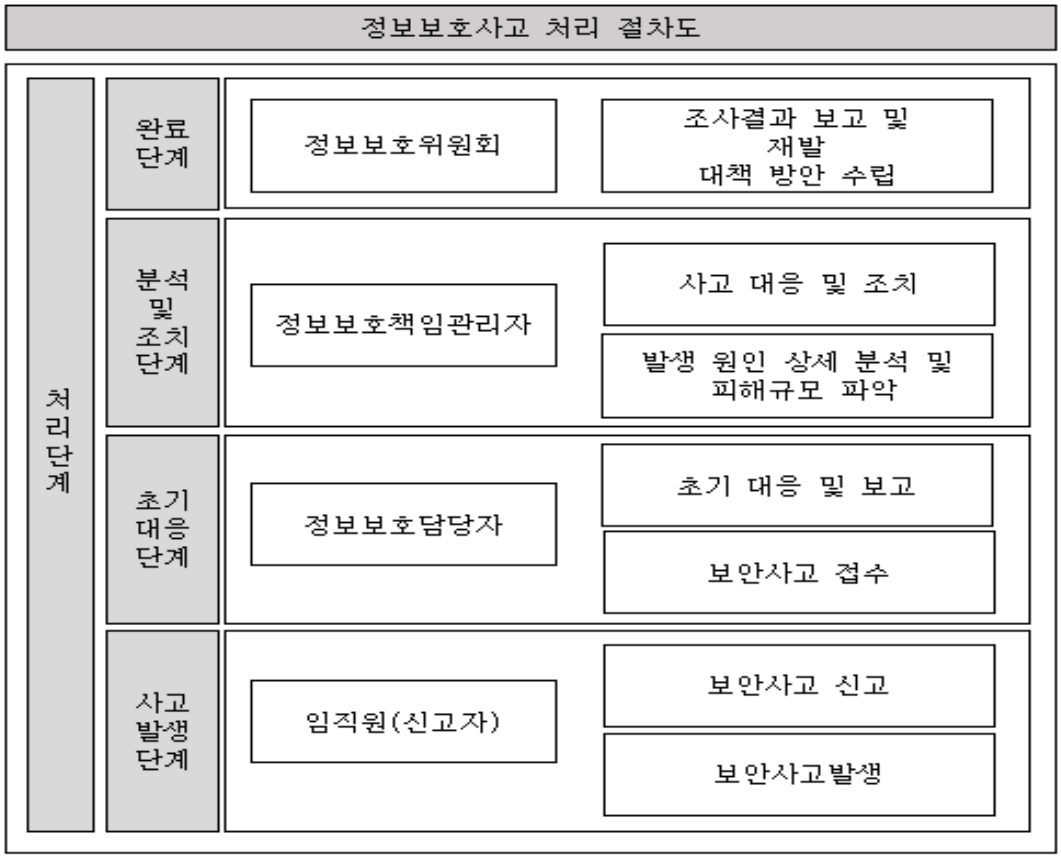
⑥ 원본 증거자료는 원칙적으로 사용을 금하며, 사본을 통해 조사를 실시한다(특히, 대외수사기관 등에 사건 의뢰가 필요한 경우).

- 출입 로그, CCTV 녹화 내용, 시스템 로그(접근, 출력, 다운로드 등), 서비스(그룹웨어, 메일, 웹하드 등) 사용 로그 등
- 사건 대상, 사용 도구 확보: 서버, PC, 대용량 저장매체 등
- 사용자, 서비스 통제: 계정 확보(계정 잠금, 패스워드 변경 등), 권한 회수, 서비스
- 신원확보 등

⑦ 정보보호담당자는 사고발생부터 대응, 처리 및 복구, 종료까지 진행결과를 “정보보호사고보고서”로 작성하여 정보보호 위원회에 보고한다.

⑧ 정보보호 원인과 경위에 대한 조사가 종결될 때까지 외부에 공개하지 않을 수 있다.

⑨ 정보보호 사고 조사 결과는 단계별로 사고결과 보고를 수행한다. 다만 보고 대상은 변경될 수 있다.



제 4 조 정보보호 사고 단계별 대응

사고발생 단계

구분	주요 내용
사고발생	- 사고 확인 및 증상 확인
대응 업무	- 사고 발생 의심 Event로그 등 확인 - 서비스 영향도 파악 - 사고 발생 원인 1차분석 - 사고 범위 확인 - 사고 분석 대상 확인
보고서	- 분석보고서(초기)

사고 분석 및 대응단계

구분	주요 내용
사고분석	- 발생 및 원인, 피해규모 파악 등
대응 업무	- 사고 발생 원인 상세 분석 및 대응 - 진행사항 확인 및 상황 공유 - 실시간 모니터링
보고서	- 분석보고서(중간)

완료 보고 및 재발대책수립 단계

구분	주요 내용
완료 및 보고	- 복구 조치 완료 및 재발대책마련
완료 단계	- 최종 분석 및 완료 보고 -재발대책 방안 수립
보고서	- 완료보고서(최종)

제 5 조 정보보호 사고 기록 및 보관

① 정보보호담당자는 정보보호사고 발생시 사고 일자 및 사고 내용과 사고처리 등의 내용을 “정보보호사고보고서”에 작성 및 안전한 장소에 보관, 관리 한다.

제 6 조 정보보호 사고 공지

① 정보보호 담당자는 동일한 사건의 발생을 방지하기 위해 시스템 장애 및 정보보호 사고 등을 그룹웨어 게시판을 통해 임직원에게 공지한다.

제 7 조 사후관리

① 정보보호담당자는 발생된 정보보호 사고를 유형별로 통계, 분석하여 관리하고, 재검토하여 향후 정보보호 대책에 반영할 수 있도록 하여야 한다.

제 8 조 사고 징계

① 정보보호 지침을 위반하여 회사의 정상적 업무에 지장을 초래한 임직원은 정보보호 위원회 검토 후 사고 경중에 따라 인사위원회에 상정하여 징계 처리할 수 있다.

[부록]

정보보호사고보고서 양식

정보보호사고보고서(초기단계)

문서번호		소속	
사고유형	악성코드	발생일시	
신고자		종결일시	
감염IP		접속IP	
사고분석	Malware: exe, DLL 등의 확장자를 가지고 있는 바이너리 타입의 파일을 다운로드 및 실행하여 운영체제를 감염시키는 악성코드		
조치사항	1. 감염PC 네트워크 단절 2. 백신프로그램 정밀검사 수행 (C:, D: 등 모든 디스크 대상 검사 필요)		
비고	**메일 열람(gwx.XXXX.com) 중 다운로드 받은 악성파일로 인해 발생. (파일명: Settlement XXXXXXXX list.doc)**		
문의사항: 정보전략팀			

정보보호사고보고서(중간보고서)

문서번호		소속	
사고유형	악성코드	발생일시	
신고자		종결일시	
감염IP		접속IP	

피해범위	특정사용자 악성코드 감염
사고분석	Malware: exe, DLL 등의 확장자를 가지고 있는 바이너리 타입의 파일을 다운로드 및 실행하여 운영체제를 감염시키는 악성코드
조치사항	1. 백신 최신 업데이트 실시 2. 백신 유해가능/불필요한 프로그램 탐지 기능 활성화 3. 백신프로그램 정밀검사 수행 (C:, D: 등 모든 디스크 대상 검사 필요) 4. PC 재부팅 후 바이러스 검사 재수행 5. 백신 보안상태 설정 -> 실시간 검사 동작 여부 확인 6. 불필요한 프로그램 (애드웨어 등) 삭제 - 제어판 -> 프로그램제거: 업무외 불필요한 광고성 프로그램 삭제 - P2P 프로그램 사용시(토렌트 or 웹하드 프로그램) 삭제
비고	**메일 열람(gwx.XXXX.com) 중 다운로드 받은 악성파일로 인해 발생. (파일명: Settlement XXXXXXXX list.doc)**
문의사항: 정보전략팀	

정보보호사고보고서(완료보고서)

문서번호		**소속**	
사고유형	악성코드	**발생일시**	
신고자		**종결일시**	
감염IP		**접속IP**	
피해범위	특정사용자 악성코드 감염		
사고분석	Malware: exe, DLL 등의 확장자를 가지고 있는 바이너리 타입의 파일을 다운로드 및 실행하여 운영체제를 감염시키는 악성코드		

조치사항	1. 백신 최신 업데이트 실시 2. 백신 유해가능/불필요한 프로그램 탐지 기능 활성화 3. 백신프로그램 정밀검사 수행 (C:, D: 등 모든 디스크 대상 검사 필요) 4. PC 재부팅 후 바이러스 검사 재수행 5. 백신 보안상태 설정 -> 실시간 검사 동작 여부 확인 6. 불필요한 프로그램 (애드웨어 등) 삭제 - 제어판 -> 프로그램제거: 업무외 불필요한 광고성 프로그램 삭제 - P2P 프로그램 사용시(토렌트 or 웹하드 프로그램) 삭제
재발대책 수립	1. 백신 최신 업데이트 실시 2. 악성 메일 유입경로 차단 3. 임직원 악성메일 훈련 진행
비고	
문의사항: 정보전략팀	