Autonomous™

문서관리번호	2025-ENV-S010
최종 수정일	2025. 6. 30
문서 관리자	기획팀

㈜오토기기 정보보안 사고대응 절차서

2025. 06. 30

목차

1. 개요

1.1 목적

본 절차서는 주식회사 오토기기(이하 '회사')에서 발생할 수 있는 정보보안 사고에 대해 체계적이고 효과적으로 대응하기 위한 표준 절차를 제공하는 데 그 목적이 있다. 본 절차서를 통해 정보보안 사고 발생 시 신속하게 탐지하고, 적절히 대응하며, 피해를 최소화하고, 정상 업무로 복귀하는 과정을 체계화하여 회사의 정보자산을 보호하고자 한다.

구체적인 목적은 다음과 같다:

정보보안 사고의 신속한 탐지 및 보고 체계 확립

사고 유형 및 심각도에 따른 체계적인 대응 절차 제공

사고 대응 과정에서의 역할과 책임 명확화

사고로 인한 피해 최소화 및 신속한 복구 지원

사고 재발 방지를 위한 사후 관리 방안 제시

법적 요구사항 및 규제 준수

1.2 적용범위

본 절차서는 다음과 같은 범위에 적용된다:

대상 시스템

회사가 소유하거나 관리하는 모든 정보시스템

서버, 네트워크 장비, 보안 장비

데스크톱, 노트북, 모바일 기기 등 업무용 단말기

클라우드 서비스 및 외부 호스팅 시스템

대상 정보

회사의 모든 전자적, 비전자적 정보자산

고객 정보, 개인정보

기술 정보, 영업 비밀

업무 관련 데이터 및 문서

적용 대상자

회사의 모든 임직원

계약직, 파견직 직원

외부 협력업체 직원(회사 시스템에 접근하는 경우)

정보보안 사고 대응팀(CERT) 구성원

적용 상황

모든 정보보안 사고 및 의심 상황

내부 또는 외부로부터의 보안 위협

우발적 또는 의도적인 보안 위반

자연재해로 인한 정보시스템 피해

1.3 용어 정의

정보보안 사고: 정보자산의 기밀성, 무결성, 가용성을 침해하거나 침해할 가능성이 있는 모든 사건

정보보안 이벤트: 시스템, 서비스 또는 네트워크에서 발생하는 식별 가능한 상태의 변화로, 정보보안 정책 위반 또는 보안 통제 실패의 가능성을 나타내는 사건

CERT(Computer Emergency Response Team): 정보보안 사고에 대응하기 위해 구성된 전담 조직

침해사고: 해킹, 악성코드, 서비스 거부 공격 등 전자적 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위

악성코드: 시스템을 파괴하거나 정보를 유출하는 등의 악의적인 목적을 가진 프로그램 또는 코드

랜섬웨어: 시스템이나 데이터를 암호화하여 접근을 차단하고 금전을 요구하는 악성 소프트웨어

피싱(Phishing): 신뢰할 수 있는 기관이나 개인을 사칭하여 개인정보나 금융정보를 탈취하려는 사회공학적 공격

APT(Advanced Persistent Threat): 특정 대상을 겨냥한 지속적이고 지능적인 사이버 공격

포렌식(Forensics): 디지털 증거를 수집, 분석하여 법적 증거로 활용하기 위한 과학적 기법

IoC(Indicators of Compromise): 시스템이나 네트워크가 침해되었음을 나타내는 증거나 흔적

1.4 관련 문서

정보보안 정책

정보보안 표준운영절차(SOP)

개인정보 보호지침

업무 연속성 계획(BCP)

재해복구 계획(DRP)

위기관리 매뉴얼

2. 정보보안 사고 대응 체계

2.1 정보보안 사고 대응팀(CERT) 구성

정보보안 사고 대응팀(CERT)은 다음과 같이 구성된다:

CERT 총괄책임자

정보보안 최고책임자(CISO)가 담당

사고 대응 전반에 대한 총괄 책임

중대 사고 발생 시 비상대책위원회 소집 및 운영

CERT 운영책임자

정보보안팀장이 담당

사고 대응 활동 조정 및 관리

사고 조사 및 분석 총괄

기술 대응팀

구성: 정보시스템팀, 보안운영 담당자

역할: 기술적 분석, 증거 수집, 시스템 복구

관리 대응팀

구성: 정보보안팀, 법무팀, 인사팀, 홍보팀 담당자

역할: 내외부 커뮤니케이션, 법적 대응, 인적 조치

외부 전문가 그룹

필요시 외부 보안 전문업체, 법률 자문, 디지털 포렌식 전문가 등 활용

2.2 역할 및 책임

2.2.1 CERT 총괄책임자

중대 보안사고 발생 시 비상대책위원회 소집

대응 전략 및 방향 결정

주요 의사결정 승인

경영진 및 이사회 보고

외부 기관 대응 총괄

2.2.2 CERT 운영책임자

사고 대응 활동 실무 총괄

사고 심각도 평가 및 대응 수준 결정

대응팀 인력 배정 및 업무 조정

사고 조사 및 분석 지휘

대응 상황 모니터링 및 보고

2.2.3 기술 대응팀

사고 탐지 및 초기 분석

기술적 증거 수집 및 보존

영향 범위 파악 및 피해 시스템 식별

공격 경로 및 방법 분석

시스템 복구 및 보안 강화 조치 이행

기술적 대응 방안 수립 및 실행

2.2.4 관리 대응팀

내부 임직원 공지 및 안내

외부 이해관계자 커뮤니케이션

법적 대응 및 규제 준수 검토

인적 보안 조치 검토 및 이행

언론 대응 자료 준비 및 대응

사고 관련 문서화 및 기록 관리

2.2.5 부서별 책임

정보보안팀: 사고 대응 총괄, 보안 정책 검토 및 개선

정보시스템팀: 시스템 복구, 기술적 대응 조치 이행

법무팀: 법적 이슈 검토, 외부 신고 및 소송 대응

인사팀: 인적 보안 조치, 징계 절차 검토

홍보팀: 내외부 커뮤니케이션, 언론 대응

개인정보보호팀: 개인정보 유출 관련 대응 및 신고

2.3 비상연락체계

2.3.1 내부 비상연락망

CERT 구성원 연락처(사무실, 휴대전화, 이메일)

부서별 책임자 연락처

경영진 비상연락망

연락 우선순위 및 에스컬레이션 절차

2.3.2 외부 비상연락망

보안 관제 서비스 제공업체

외부 보안 컨설팅 업체

법률 자문

디지털 포렌식 전문가

하드웨어/소프트웨어 벤더 기술지원

2.3.3 관련 기관 연락처

한국인터넷진흥원(KISA) 사이버침해대응센터: 국번없이 118

개인정보보호위원회

경찰청 사이버수사대

국가정보원 산업기밀보호센터

금융감독원(금융 관련 사고의 경우)

2.3.4 비상연락 프로세스

사고 발견자는 즉시 정보보안팀에 보고

정보보안팀은 심각도 평가 후 CERT 운영책임자에게 보고

CERT 운영책임자는 CERT 총괄책임자 및 필요 대응팀에 통지

심각도 '높음' 이상 사고는 경영진에게 즉시 보고

필요시 외부 전문가 및 관련 기관에 통지

3. 정보보안 사고 유형 및 심각도

3.1 정보보안 사고 유형

3.1.1 악성코드 관련 사고

바이러스, 웜, 트로이목마 감염

랜섬웨어 감염

봇넷 감염

루트킷, 백도어 설치

3.1.2 해킹 및 침해 사고

시스템 침입

계정 탈취

권한 상승

웹사이트 변조

APT 공격

3.1.3 정보 유출 사고

개인정보 유출

기밀정보 유출

영업비밀 유출

내부자에 의한 정보 유출

실수에 의한 정보 노출

3.1.4 서비스 장애 사고

DoS/DDoS 공격

리소스 고갈

설정 오류로 인한 장애

시스템 과부하

3.1.5 사회공학적 공격

피싱/스피어피싱

스미싱

비즈니스 이메일 침해(BEC)

보이스피싱

3.1.6 물리적 보안 사고

장비 도난/분실

무단 접근

시설 파괴/손상

자연재해로 인한 피해

3.2 심각도 분류

정보보안 사고의 심각도는 다음과 같이 4단계로 분류한다:

3.2.1 심각(Critical)

정의: 회사의 핵심 업무에 심각한 영향을 미치거나, 대규모 정보 유출 또는 재정적 손실이 발생한 사고

예시:

고객 개인정보 대량 유출

핵심 시스템 장기간(4시간 이상) 마비

회사 핵심 기술 정보 유출

전사적 랜섬웨어 감염

언론 보도 가능성이 높은 사고

3.2.2 높음(High)

정의: 주요 업무에 상당한 영향을 미치거나, 중요 정보의 유출 또는 상당한 재정적 손실이 발생한 사고

예시:

주요 시스템 일시적(1~4시간) 장애

중요 정보 일부 유출

다수 시스템 악성코드 감염

부서 단위 업무 중단

외부 공격자의 시스템 침투 확인

3.2.3 중간(Medium)

정의: 일부 업무에 제한적 영향을 미치거나, 민감하지 않은 정보의 유출 또는 경미한 재정적 손실이 발생한 사고

예시:

단일 시스템/서버 장애(1시간 미만)

일반 정보 유출

개별 PC 악성코드 감염

사용자 계정 탈취

비인가 접근 시도 탐지

3.2.4 낮음(Low)

정의: 업무에 거의 영향이 없거나, 정보 유출 없이 단순 보안 정책 위반이 발생한 사고

예시:

스팸 이메일 수신

단순 보안 정책 위반

쉽게 차단/제거 가능한 악성코드 발견

비인가 소프트웨어 설치

실패한 해킹 시도

3.3 사고 등급별 대응 수준

3.3.1 심각(Critical) 등급 대응

대응팀: 전체 CERT 소집, 비상대책위원회 구성

보고: 즉시 CISO 및 경영진 보고, 이사회 보고 검토

대응시간: 24시간 대응 체제 가동

복구우선순위: 최우선 자원 배정

외부기관: 필요시 외부 전문가 즉시 투입, 관련 기관 신고

커뮤니케이션: 전사 공지, 고객/파트너 통지, 언론 대응 준비

3.3.2 높음(High) 등급 대응

대응팀: 핵심 CERT 멤버 소집

보고: 4시간 이내 CISO 보고, 24시간 이내 경영진 보고

대응시간: 업무 시간 외 대응 필요시 연장 근무

복구우선순위: 높은 우선순위 자원 배정

외부기관: 필요시 외부 전문가 지원 요청 검토

커뮤니케이션: 관련 부서 공지, 필요시 고객/파트너 통지

3.3.3 중간(Medium) 등급 대응

대응팀: 정보보안팀 및 관련 부서 담당자

보고: 24시간 이내 정보보안팀장 보고, 주간 보고서에 포함

대응시간: 업무 시간 내 대응

복구우선순위: 일반 우선순위 자원 배정

외부기관: 내부 역량으로 해결, 필요시 벤더 기술지원 요청

커뮤니케이션: 관련자에 제한적 공지

3.3.4 낮음(Low) 등급 대응

대응팀: 정보보안팀 담당자

보고: 주간/월간 보안 보고서에 포함

대응시간: 일반 업무 프로세스에 따라 처리

복구우선순위: 일반 업무의 일부로 처리

외부기관: 내부 역량으로 해결

커뮤니케이션: 관련자에게만 통지

4. 정보보안 사고 대응 프로세스

4.1 탐지 및 보고

4.1.1 사고 탐지 경로

보안 모니터링 시스템(IDS/IPS, SIEM, EDR 등)

로그 분석 및 이상 징후 탐지

임직원 보고

외부 기관 또는 고객 통보

정기 보안 점검 및 취약점 진단

4.1.2 초기 보고 절차

사고 발견자는 정보보안팀에 즉시 보고

전화: 내선 1234

이메일: security@autonomouskr.com

메신저: 보안사고 신고 채널

보고 시 포함할 내용

발견 일시 및 보고자 정보

사고 유형 및 증상

영향받는 시스템 또는 정보

현재까지 취한 조치

사고 증거(화면 캡처, 로그 등)

정보보안팀은 초기 보고 접수 후 사고 기록 생성

사고 ID 부여

사고 기록 시작

초기 대응 담당자 지정

4.1.3 초기 대응 조치

추가 피해 방지를 위한 긴급 조치

증거 보존을 위한 조치

필요시 시스템 격리

초기 상황 기록

4.2 평가 및 분류

4.2.1 사고 평가

사고의 실제 여부 확인

사고 유형 판단

영향 범위 및 피해 규모 초기 평가

추가 확산 가능성 검토

4.2.2 심각도 평가

3.2 심각도 분류 기준에 따라 심각도 판정

평가 요소:

영향받는 시스템의 중요도

영향받는 정보의 민감도

업무 중단 정도

재정적 손실 규모

법적/규제적 영향

회사 평판에 미치는 영향

4.2.3 대응팀 구성

심각도에 따른 대응팀 소집

사고 유형에 따른 전문가 포함

역할 및 책임 할당

대응 계획 수립

4.2.4 에스컬레이션

심각도에 따른 보고 체계 가동

필요시 경영진 보고

외부 전문가 지원 요청 결정

관련 기관 신고 필요성 검토

4.3 대응 및 조치

4.3.1 봉쇄(Containment)

추가 피해 확산 방지 조치

영향받는 시스템 격리

취약점 임시 조치

공격 경로 차단

4.3.2 근절(Eradication)

악성코드 제거

취약점 패치 및 보완

침해된 계정 처리

비인가 접근 차단

4.3.3 조사 및 분석

사고 원인 및 경로 분석

공격자 식별 시도

피해 범위 상세 파악

유사 취약점 존재 여부 확인

4.3.4 증거 수집

로그 데이터 수집

시스템 이미지 확보

네트워크 트래픽 분석

사용자 인터뷰

4.4 복구

4.4.1 복구 계획 수립

복구 우선순위 결정

필요 자원 식별

복구 절차 수립

복구 일정 계획

4.4.2 시스템 복구

백업에서 데이터 복원

시스템 재설치 또는 복구

패치 및 보안 업데이트 적용

보안 강화 조치 적용

4.4.3 운영 재개

복구된 시스템 검증

보안 테스트 수행

단계적 서비스 재개

정상 운영 확인

4.4.4 모니터링 강화

복구 후 집중 모니터링

이상 징후 지속 관찰

재발 징후 확인

추가 공격 시도 감시

4.5 사후 관리

4.5.1 사고 분석 보고서 작성

사고 개요 및 경과

원인 및 취약점 분석

대응 활동 및 결과

피해 현황 및 영향

4.5.2 재발 방지 대책

기술적 보안 강화 방안

정책 및 절차 개선

교육 및 인식 제고 방안

모니터링 체계 강화

4.5.3 교훈 도출 및 공유

사고 대응 과정 평가

개선점 도출

유사 사고 예방 지침 마련

교훈 사항 공유

4.5.4 후속 조치

개선 대책 이행 계획 수립

이행 상황 모니터링

효과성 평가

정보보안 정책 및 절차 업데이트

5. 정보보안 사고 유형별 대응 절차

5.1 악성코드 감염

5.1.1 초기 대응

감염 의심 시스템 네트워크 격리

악성코드 샘플 및 관련 로그 확보

악성코드 유형 및 특성 분석

감염 경로 및 확산 범위 파악

5.1.2 조치 사항

최신 백신으로 악성코드 검사 및 제거

필요시 시스템 초기화 또는 재설치

감염 경로 차단(취약점 패치, 이메일 필터링 강화 등)

유사 시스템 점검 및 예방 조치

5.1.3 랜섬웨어 특화 대응

감염 시스템 즉시 네트워크 분리 및 전원 차단

암호화된 파일 및 랜섬노트 보존(증거 확보)

랜섬웨어 유형 식별 및 복구 가능성 검토

백업에서 데이터 복원

절대 몸값 지불하지 않음

필요시 사이버수사대 신고

5.2 해킹 및 침해 사고

5.2.1 초기 대응

침해 의심 시스템 격리

로그 및 증거 자료 확보

침해 범위 및 피해 현황 파악

침입 경로 및 취약점 식별

5.2.2 조치 사항

모든 계정 패스워드 변경(특히 관리자 계정)

악성 파일 및 백도어 제거

취약점 패치 및 보안 강화

시스템 재구성 또는 복구

추가 침해 여부 모니터링

5.2.3 APT 공격 특화 대응

전문 포렌식 팀 투입

장기간 활동 흔적 조사

지속적인 접근 수단(백도어 등) 완전 제거

공격 주체 및 목적 분석

유사 공격 탐지를 위한 IoC 확보 및 적용

5.3 정보 유출

5.3.1 초기 대응

유출 정보 범위 및 영향 파악

유출 경로 및 원인 식별

추가 유출 방지를 위한 조치

법적 의무사항 검토(개인정보 유출 통지 등)

5.3.2 조치 사항

유출 경로 차단

유출된 정보의 삭제 또는 회수 시도

관련 계정 및 접근 권한 재설정

유출 관련자 조사 및 조치

5.3.3 개인정보 유출 특화 대응

개인정보 유출 신고(개인정보보호위원회, 한국인터넷진흥원)

1천명 이상 유출 시 의무 신고

유출 사실 인지 후 24시간 이내 신고

정보주체 통지

유출 항목, 시점, 경위

피해 최소화 방법

기관 대응 조치

피해 신고 접수 부서 및 연락처

유출 사실 홈페이지 게시(필요시)

피해 구제 절차 마련

5.4 서비스 거부(DoS/DDoS) 공격

5.4.1 초기 대응

공격 유형 및 트래픽 패턴 분석

네트워크/시스템 모니터링 강화

공격 근원지 및 대상 식별

트래픽 로그 확보

5.4.2 조치 사항

방화벽, IPS 등 보안장비 필터 설정

대역폭 확장 또는 부하 분산

ISP 또는 DDoS 방어 서비스 제공업체 협조 요청

트래픽 우회 또는 차단

5.4.3 서비스 복구

공격 중단 확인

시스템 및 서비스 상태 점검

단계적 서비스 재개

재공격 대비 모니터링 강화

5.5 내부자 위협

5.5.1 초기 대응

의심 활동 증거 확보

관련 계정 접근 로그 검토

정보 접근 및 사용 내역 분석

법무팀 및 인사팀 협조

5.5.2 조치 사항

필요시 해당 계정 접근 제한

중요 정보 접근 권한 재검토

증거 자료 보존

내부 조사 진행

5.5.3 후속 조치

조사 결과에 따른 인사 조치

정보 접근 통제 강화

내부자 모니터링 체계 개선

필요시 법적 조치 검토

5.6 물리적 보안 사고

5.6.1 장비 도난/분실

분실 장비 정보 확인(일련번호, 저장 정보 등)

원격 잠금 또는 초기화 조치(가능한 경우)

접근 계정 패스워드 변경

중요 정보 포함 여부 확인 및 영향 평가

필요시 관할 경찰서 신고

5.6.2 무단 접근

침입 경로 및 방법 확인

CCTV 및 출입 기록 확인

접근된 시설 및 장비 점검

물리적 보안 통제 강화

5.6.3 자연재해

인명 안전 최우선 확보

2차 피해 방지 조치

장비 및 시설 피해 현황 파악

업무 연속성 계획(BCP)에 따른 복구 진행

6. 증거 수집 및 보존

6.1 증거 수집 원칙

6.1.1 기본 원칙

증거의 무결성 보장

증거 수집 과정 문서화

증거 수집 시 원본 데이터 변경 최소화

증거 수집 담당자 지정 및 책임 부여

법적 효력을 고려한 증거 수집

6.1.2 증거 수집 시 고려사항

휘발성 데이터 우선 수집

시간 정보의 정확성 확보

증거 수집 도구의 신뢰성

증거 수집 순서 및 방법 준수

증거 수집 과정의 연속성 유지

6.2 증거 수집 방법

6.2.1 시스템 메모리 및 휘발성 데이터

실행 중인 프로세스 목록

네트워크 연결 상태

로그인 사용자 정보

열린 파일 목록

시스템 메모리 덤프

6.2.2 저장 매체 데이터

디스크 이미지 생성

파일 시스템 분석

삭제된 파일 복구

파일 메타데이터 수집

레지스트리 데이터 수집

6.2.3 네트워크 데이터

네트워크 트래픽 캡처

방화벽 및 IDS/IPS 로그

라우터/스위치 로그

DNS 쿼리 로그

프록시 서버 로그

6.2.4 로그 데이터

시스템 로그

애플리케이션 로그

보안 장비 로그

인증 로그

데이터베이스 로그

6.3 증거 보존 절차

6.3.1 증거 식별 및 라벨링

증거 고유 식별자 부여

수집 일시 및 담당자 기록

증거 유형 및 설명 기록

증거 출처 및 위치 기록

해시값 생성(MD5, SHA-256 등)

6.3.2 증거 보관

접근 통제된 안전한 장소에 보관

증거 보관함 또는 금고 사용

디지털 증거의 경우 쓰기 방지 조치

백업 사본 별도 보관

증거 접근 기록 유지

6.3.3 증거 이관 관리

증거 이관 시 인계인수서 작성

이관 과정에서의 무결성 검증

이관 이력 문서화

증거 취급자 최소화

6.3.4 증거 보존 기간

법적 요구사항에 따른 보존 기간 준수

사고 유형별 보존 기간 설정

보존 기간 만료 후 안전한 폐기

중요 사고의 경우 장기 보존 검토

6.4 디지털 포렌식 조사

6.4.1 포렌식 조사 준비

조사 목표 및 범위 설정

필요 도구 및 장비 준비

조사 권한 및 법적 검토

조사팀 구성 및 역할 분담

6.4.2 포렌식 조사 수행

증거 수집 및 보존

데이터 복구 및 분석

타임라인 분석

아티팩트 분석

악성코드 분석

6.4.3 포렌식 조사 보고서

조사 개요 및 목적

조사 방법론 및 도구

증거 목록 및 분석 결과

사고 재구성 및 타임라인

결론 및 권고사항

7. 보고 및 커뮤니케이션

7.1 내부 보고 체계

7.1.1 보고 단계

초기 보고: 사고 발견 즉시

상황 보고: 사고 대응 중 정기적

중간 보고: 주요 진행 상황 발생 시

최종 보고: 사고 대응 완료 후

7.1.2 보고 대상 및 경로

심각도에 따른 보고 대상 결정

낮음/중간: 정보보안팀장

높음: CISO, 관련 부서장

심각: 경영진, 이사회

보고 경로 및 방법

이메일, 전화, 대면 보고

정기 보안 회의

긴급 회의 소집

7.1.3 보고 내용

사고 개요 및 현황

영향 범위 및 피해 상황

대응 조치 및 진행 상황

예상 복구 시간

추가 지원 필요 사항

7.2 외부 기관 신고

7.2.1 신고 대상 사고

개인정보 유출 사고(1천명 이상)

정보통신망법 상 침해사고

산업기술 유출 사고

금융정보 유출 사고

기타 법적 신고 의무가 있는 사고

7.2.2 신고 절차

신고 필요성 검토(법무팀 협조)

신고 내용 및 자료 준비

신고 기관별 요구 양식 작성

신고 실행 및 접수 확인

추가 자료 요청 시 대응

7.2.3 주요 신고 기관 및 방법

개인정보보호위원회: 개인정보 유출 신고

신고 방법: 개인정보보호 포털(www.privacy.go.kr)

신고 기한: 유출 인지 후 24시간 이내

한국인터넷진흥원(KISA): 침해사고 신고

신고 방법: 국번없이 118 또는 홈페이지

신고 내용: 사고 일시, 유형, 피해 현황, 조치 사항

경찰청 사이버수사대: 해킹, 악성코드 등 사이버 범죄

신고 방법: 경찰청 사이버범죄 신고시스템

금융감독원: 금융 관련 정보 유출

신고 방법: 금융감독원 사이버안전센터

7.3 고객 및 이해관계자 통지

7.3.1 통지 대상 결정

법적 통지 의무 대상

계약상 통지 의무 대상

사고로 영향받는 고객 및 파트너

기타 이해관계자

7.3.2 통지 내용

사고 개요 및 발생 경위

유출/침해된 정보의 항목

피해 최소화를 위한 조치 방법

회사의 대응 조치 및 지원 내용

문의 및 피해 신고 창구

7.3.3 통지 방법 및 시점

개별 통지: 이메일, SMS, 우편

일괄 통지: 홈페이지 공지, 언론 보도

통지 시점: 법적 기한 준수(개인정보 유출의 경우 5일 이내)

단계적 통지: 상황에 따라 초기/중간/최종 통지

7.3.4 통지 후 대응

고객 문의 대응 체계 구축

FAQ 작성 및 배포

콜센터 대응 스크립트 준비

피해 구제 절차 마련

7.4 언론 대응

7.4.1 언론 대응 원칙

단일 창구를 통한 일관된 메시지 전달

사실에 기반한 정확한 정보 제공

투명하고 책임있는 태도 유지

피해자 보호 및 개인정보 보호 준수

법적 책임 고려한 발언

7.4.2 언론 대응 절차

언론 대응팀 구성(홍보팀, 법무팀, 정보보안팀)

공식 입장 및 보도자료 작성

대변인 지정 및 브리핑 준비

예상 질문 및 답변 준비

언론 모니터링 및 추가 대응

7.4.3 언론 대응 시 유의사항

확인되지 않은 정보 언급 자제

책임 소재에 대한 섣부른 판단 자제

기술적 세부사항 과도한 공개 자제

진행 중인 조사 방해 가능성 고려

피해자 정보 보호

8. 교육 및 훈련

8.1 교육 계획

8.1.1 교육 대상별 프로그램

일반 임직원 대상 기본 교육

CERT 구성원 대상 전문 교육

관리자 대상 리더십 교육

IT 담당자 대상 기술 교육

신입사원 대상 입문 교육

8.1.2 교육 내용

정보보안 사고 유형 및 사례

사고 탐지 및 보고 방법

초기 대응 요령

증거 보존 방법

비상연락망 및 에스컬레이션 절차

8.1.3 교육 주기 및 방법

정기 교육: 연 1회 이상

수시 교육: 주요 보안 위협 발생 시

온라인 교육: 기본 과정

오프라인 교육: 실습 및 토론

외부 전문 교육: CERT 구성원 대상

8.2 모의 훈련

8.2.1 모의 훈련 유형

테이블탑 훈련: 시나리오 기반 토론식 훈련

기능 훈련: 특정 기능/역할 중심 훈련

종합 훈련: 실제 사고 대응 전 과정 훈련

불시 훈련: 사전 공지 없는 훈련

8.2.2 훈련 시나리오

랜섬웨어 감염 대응

개인정보 유출 대응

APT 공격 대응

DDoS 공격 대응

내부자 위협 대응

8.2.3 훈련 실행

훈련 계획 수립

참가자 및 평가자 지정

시나리오 및 상황 부여

훈련 실행 및 모니터링

훈련 결과 평가 및 피드백

8.2.4 훈련 주기

테이블탑 훈련: 분기 1회

기능 훈련: 반기 1회

종합 훈련: 연 1회

불시 훈련: 비정기적

8.3 인식 제고

8.3.1 인식 제고 활동

보안 뉴스레터 발행

보안 포스터 및 안내문 게시

보안 캠페인 실시

최신 보안 위협 정보 공유

사고 사례 및 교훈 공유

8.3.2 인식 측정 및 개선

보안 인식 수준 평가

모의 피싱 테스트

보안 퀴즈 및 설문

인식 제고 활동 효과성 측정

개선 활동 수립 및 이행

9. 부록

9.1 정보보안 사고 대응 양식

9.1.1 정보보안 사고 보고서

정보보안 사고 보고서

[사고 기본 정보]

사고 ID: IR-YYYY-NNN

보고일시: YYYY-MM-DD HH:MM

보고자: 이름/부서/연락처

사고 유형: □악성코드 □해킹 □정보유출 □서비스장애 □기타( )

심각도: □심각 □높음 □중간 □낮음

[사고 개요]

발생일시:

발견일시:

발견경로:

영향범위:

피해현황:

[초기 대응 조치]

조치일시:

조치내용:

[현재 상황]

진행상태:

예상복구시간:

[향후 계획]

추가조치계획:

필요지원사항:

[첨부자료]

9.1.2 정보보안 사고 분석 보고서

정보보안 사고 분석 보고서

[사고 기본 정보]

사고 ID: IR-YYYY-NNN

분석 기간: YYYY-MM-DD ~ YYYY-MM-DD

분석 담당자:

[사고 요약]

사고 유형:

발생 원인:

영향 범위:

피해 규모:

[상세 분석]

1. 공격 벡터 및 경로

2. 사용된 도구 및 기법

3. 취약점 분석

4. 타임라인 분석

5. 피해 시스템 및 정보 분석

[대응 조치]

1. 초기 대응

2. 봉쇄 조치

3. 근절 조치

4. 복구 조치

[교훈 및 개선 사항]

1. 기술적 개선 사항

2. 관리적 개선 사항

3. 정책 및 절차 개선 사항

[첨부 자료]

1. 로그 분석 결과

2. 포렌식 분석 보고서

3. IoC(침해 지표) 목록

9.1.3 정보보안 사고 종결 보고서

정보보안 사고 종결 보고서

[사고 기본 정보]

사고 ID: IR-YYYY-NNN

사고 기간: YYYY-MM-DD ~ YYYY-MM-DD

종결일: YYYY-MM-DD

담당자:

[사고 요약]

사고 유형:

원인:

영향:

최종 피해 현황:

[대응 활동 요약]

주요 대응 활동:

투입 자원:

복구 완료 사항:

[사후 관리]

재발 방지 대책:

이행 계획:

모니터링 계획:

[교훈 및 시사점]

잘된 점:

개선 필요 사항:

향후 적용 사항:

[승인]

CERT 운영책임자: (서명)

CERT 총괄책임자: (서명)

9.1.4 증거 수집 체인 기록부

증거 수집 체인 기록부

[증거 기본 정보]

증거 ID: EV-YYYY-NNN

사고 ID: IR-YYYY-NNN

증거 유형: □하드디스크 □메모리덤프 □로그파일 □네트워크캡처 □기타( )

설명:

[증거 수집]

수집일시: YYYY-MM-DD HH:MM

수집자: 이름/부서/연락처

수집장소:

수집방법:

해시값(MD5):

해시값(SHA-256):

[증거 이관 기록]

No.	이관일시	인계자	인수자	목적	비고
1					
2					
3					

[증거 보관 현황]

보관장소:

보관조건:

접근권한자:

보존기간:

[증거 처분]

처분일시:

처분방법:

처분사유:

처분자:

승인자:

9.2 연락처 목록

9.2.1 내부 비상연락망

[CERT 구성원]

- CERT 총괄책임자: 김OO / 010-XXXX-XXXX / ciso@autonomouskr.com
- CERT 운영책임자: 박OO / 010-XXXX-XXXX / security.manager@autonomouskr.com
- 기술대응팀장: 이OO / 010-XXXX-XXXX / tech.manager@autonomouskr.com
- 관리대응팀장: 최OO / 010-XXXX-XXXX / admin.manager@autonomouskr.com

[주요 부서]

- 정보시스템팀: 02-XXX-XXXX / it@autonomouskr.com
- 법무팀: 02-XXX-XXXX / legal@autonomouskr.com
- 인사팀: 02-XXX-XXXX / hr@autonomouskr.com
- 홍보팀: 02-XXX-XXXX / pr@autonomouskr.com
- 고객지원팀: 02-XXX-XXXX / support@autonomouskr.com

[경영진]

- 대표이사: 02-XXX-XXXX / ceo@autonomouskr.com
- 기술이사: 02-XXX-XXXX / cto@autonomouskr.com
- 재무이사: 02-XXX-XXXX / cfo@autonomouskr.com

9.2.2 외부 연락처

[외부 보안 서비스]

- 보안관제 서비스: OO보안 / 02-XXX-XXXX / 담당자: 김OO / 010-XXXX-XXXX
- 포렌식 전문업체: OO디지털포렌식 / 02-XXX-XXXX / 담당자: 이OO / 010-XXXX-XXXX
- 백업 서비스: OO데이터 / 02-XXX-XXXX / 담당자: 박OO / 010-XXXX-XXXX

[주요 벤더]

- 네트워크 장비: OO네트웍스 / 02-XXX-XXXX / 담당자: 최OO / 010-XXXX-XXXX
- 보안 솔루션: OO시큐리티 / 02-XXX-XXXX / 담당자: 정OO / 010-XXXX-XXXX
- 서버 및 스토리지: OO시스템즈 / 02-XXX-XXXX / 담당자: 강OO / 010-XXXX-XXXX

[관련 기관]

- 한국인터넷진흥원(KISA)
- 개인정보보호위원회
- 경찰청 사이버수사대
- 금융감독원 사이버안전센터
- 국가정보원 산업기밀보호센터

9.3 외부 기관 신고 기준 및 절차

9.3.1 개인정보 유출 신고

신고 기준

1천명 이상의 정보주체에 관한 개인정보 유출 시

신고 기한

유출 사실 인지 후 24시간 이내