

## 별첨 #7. 사고 대응 지침

# 제 1 장 총칙

---

## 제 1 조(목적)

본 지침은 「법세권 서비스 보안정책서」 제 13 조(사고 대응)에 근거하여 보안사고 발생 시 조직 전체가 일관되고 신속하게 대응할 수 있도록 사고 탐지·분석·격리·복구·사후조치 절차를 정의함을 목적으로 한다.

## 제 2 조(적용 범위)

본 지침은 다음 사고 유형에 모두 적용한다.

- 시스템 해킹·권한 탈취
- 데이터 유출(개인정보 포함)
- 악성코드·랜섬웨어 감염
- 내부자 위협·비인가 접근
- 결제 오류·파라미터 변조 등 결제 관련 사고
- 네트워크 공격(Brute Force, Port Scan, DDoS 등)
- WAF/UTM/IPS 고위험 이벤트
- 서비스 장애 및 운영정보 위변조

## 제 3 조(책임과 역할)

- 정보보호책임자(CISO)
    - 사고 대응 총괄
    - 외부 기관 신고 판단
    - 개인정보 유출 통지 승인
  - 개인정보보호책임자(CPO)
    - 개인정보 유출 판단 및 행정처리
    - 유출 통지 및 신고 문서 검토
  - 정보보안담당자
    - 사고 탐지·초기분석
    - 공격 경로 파악 및 증거 확보
    - 보안 이벤트 모니터링
  - 시스템/네트워크 관리자
    - 격리·차단 조치 실행
    - 로그 확보 및 서비스 복구
  - 보안팀
    - 애플리케이션 측 취약점 조치
    - 결제 오류·거래 분석 및 재현
-

6. 대표자
- 법정 의무 통지 책임자(개인정보 유출 시)

## 제 2 장 사고 분류

### 제 4 조(사고 등급 분류)

모든 로그는 \*\*중앙 로그 서버(SIEM, Log Storage 등)\*\*로 수집한다.

등급	설명	예시
Critical	서비스 중단·개인정보 유출 등 심각	결제정보 유출, DB 침해
High	공격 성공·중대한 위협	관리자 계정 탈취, RCE
Medium	공격 시도·일부 영향	WAF/IPS 차단 이벤트
Low	경미·권고 수준	반복 로그인 실패 등

## 제 3 장 사고 대응 절차(핵심)

### 제 6 조(격리—Containment)

공격 확산을 막기 위한 즉각적 조치

- 네트워크 차단
  - 공격 IP 차단
  - 방화벽/UTM 정책 즉시 적용
  - 침해 서버 VLAN 격리
- 계정 차단
  - 도용 의심 계정 잠금
  - 루트/관리자 세션 강제 종료
- 프로세스·서비스 차단
  - 악성 프로세스 종료
  - 의심 서비스 중단 후 원인 파악
- 결제 사고 시
  - 결제 API 사용 제한
  - PG 사에 즉시 조치 요청

### 제 7 조(분석—Analysis)

- 로그 확보: 아래 로그를 즉시 백업하여 별도 서버로 보관
  - 시스템 로그
  - WAF·IPS·UTM 로그

- 결제 로그(거래 내역, Webhook 요청, 서명값 등)
  - DB 접근 로그
  - 애플리케이션 오류 로그
2. 공격 경로 분석
    - 최초 침입 지점 식별
    - 취약점 존재 여부 확인
    - 관리자 계정 탈취 여부 분석
  3. 영향도 분석
    - 개인정보 영향 범위
    - 결제 오류/중복 결제 여부
    - DB 및 파일 변조 여부
    - 서비스 장애 범위

## 제 8 조(복구—Recovery)

문제 원인을 제거하고 정상 운영으로 복구.

1. 취약점 조치
  - 패치 적용
  - 설정 변경
  - WAF Rule 신설
  - Key/API Secret 교체
2. 시스템 복구
  - 백업본으로 데이터 복원
  - 서비스 정상 기동 확인
  - 재발행된 Key-Credential 적용 확인
3. 결제 기능 복구
  - PG 사 연동 점검
  - 결제 트랜잭션 무결성 확인
  - 고객 피해 보상 안내 준비

## 제 9 조(재발방지—Post-Incident)

1. 근본원인 분석(RCA)
  - 기술적 원인
  - 조직적 문제(절차 미준수 여부)
  - 개발 코드 문제 등
2. 정책·절차 개선
  - 방화벽 정책 개선
  - 코드·구성 보완
  - 모니터링 룰 강화
3. 사고 보고서 작성

보고서 구성:

- 사고 개요
- 영향 범위
- 공격/침해 분석
- 조치 내용
- 예방대책
- 향후 계획

보고서는 CISO 승인 후 보관(1 년 이상)

## 제 4 장 개인정보 유출 사고 대응

---

### 제 10 조(개인정보 유출 대응 절차)

법령(개인정보보호법)에 따라 다음을 즉시 수행한다.

1. 유출항목·유출범위 식별
2. 유출 경위 조사
3. 정보주체 통지(지체 없이)
  - 유출 항목
  - 시점
  - 대응 방안
  - 문의 연락처
4. 관계기관 신고
  - 개인정보보호위원회
  - 과기정통부(정보통신망법 적용 시)
5. CISO 와 CPO 공동 점검 후 필요 시 언론 공지

## 제 5 장 증적 확보 및 보존

---

### 제 11 조(증적 보존 기준)

1. 로그는 원본 그대로 보관해야 한다.
  2. 변조 방지 적용
    - Hash
    - WORM 저장소
  3. 시스템 이미지(디스크 이미지) 필요 시 생성
  4. 증적은 최소 1 년 이상 보관
-

## 제 6 장 위기 커뮤니케이션

---

### 제 12 조(내부 보고 및 협력)

1. Critical 사고 → 즉시 CISO·대표자·CPO 보고
2. 운영팀·개발팀과 사고 범위 공유
3. PG 사·클라우드사 등 외부 파트너와 협력

### 제 13 조 (외부 커뮤니케이션)

CISO 승인 없이 외부 발표·문의 응대 금지

1. 언론 대응
2. 고객 공지
3. 외부기관 신고

## 제 7 장 예외관리

---

### 제 14 조(예외 승인)

1. 절차적 예외가 필요한 경우
2. 사유·위험 분석·대체 통제 포함
3. CISO 승인 후 한시적으로 적용
4. 만료 즉시 원복

## 제 8 장 부칙

---

### 제 15 조(시행일)

1. 본 지침은 2025 년 12 월 29 일부터 시행한다.

### 제 16 조(개정)

본 지침은 정보보호책임자(CISO)의 검토 후 개정한다.

---