별첨 #3. 시스템 보안 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 8 조(시스템 보안)에 따라 서버·OS·애플리케이션 및 서비스 환경의 보안 수준을 유지하기 위한 세부 기준 및 절차를 규정함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 시스템 전체에 적용한다.

1. 운영 서버(웹·API·백엔드·Cron 서버 등)
2. DBMS 및 캐시 서버(Redis, MySQL, PostgreSQL 등)
3. 미들웨어(Nginx, Apache, WAS 등)
4. CI/CD 서버 및 배포환경
5. 관리자·운영도구(로그 수집기, 모니터링 서버 등)
6. 컨테이너 및 클라우드 인스턴스

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 시스템 보안 정책 승인
   - 예외 승인
2. 정보보안담당자
   - 취약점 점검·모니터링 수행
3. 시스템/서버 관리자
   - OS/서비스 보안 설정 및 패치 적용
4. 개발팀
   - 안전한 코드·환경 설정 유지 및 배포 시 보안 준수

제 2 장 서버 및 OS 보안

제 4 조(서버 초기 구축 보안 설정)

1. 시스템 구축 시 기본 이미지에 다음 항목을 적용한다.
   - 최신 OS 패치
   - 불필요한 패키지 제거
   - 방화벽 기본 차단 정책
   - 관리자 계정 비활성화 또는 비밀번호 변경

2. 서버 배포 시 보안 표준 설정(서버 베이스라인)을 준수한다.
3. 클라우드 사용 시
    - 보안그룹(Security Group) 최소 허용
    - 키페어·IAM Role 최소 권한 구성

제 5 조(OS 계정 관리)

1. Root/Administrator 직접 로그인 금지
2. sudo 또는 권한 상승은 모든 로그 기록 남겨야 한다
3. OS 사용자 계정은 계정관리지침과 동일한 절차로 승인 및 생성
4. 공유계정 사용 금지(서비스 계정 제외)

제 6 조(서비스 및 데몬 관리)

1. 다음과 같은 불필요한 서비스는 비활성화한다.
    - Telnet
    - FTP
    - rlogin, rsh
    - NFS(사용 목적 없을 경우)
    - Finger 등 정보노출 서비스
2. 웹/애플리케이션 서버는 필요한 포트만 허용
3. 서비스 실행 계정은 root 가 아닌 전용 계정으로 운영한다

제 7 조(OS 보안 설정 강화)

1. 패스워드 정책은 계정지침의 비밀번호 기준을 따른다
2. 보안 설정은 CIS Benchmark 또는 OS 기본 보안 정책을 따른다
3. SSH 보안 설정:
    - PermitRootLogin no
    - PasswordAuthentication no
    - SSH Port 변경 가능(필수는 아님)
    - IdleTimeout 설정(10 분)

제 3 장 패치 및 업데이트

제 8 조(OS 및 패치 관리)

1. Critical 패치는 즉시 적용
2. 보통 등급(High/Medium) 패치는 월 1 회 정기 반영
3. 패치 전 변경관리 절차를 준수하고 사전 테스트 수행
4. 패치 이력은 1 년 이상 보관

제 9 조(서버 재부팅 및 가용성)

1. 서비스 영향이 예상되는 경우 사전 공지 및 야간 작업
2. 재부팅 시 서비스 정상 기동 여부 확인
3. 고가용성(HA) 환경에서는 순차 패치 및 롤링 업데이트 수행

제 4 장 파일·디렉토리 보안

제 10 조(파일 권한 관리)

1. /etc/passwd, /etc/shadow 등 주요 파일은 OS 기본 권한 유지
2. 웹 루트디렉토리에는 다음 파일 배치 금지:
    - .env, config.php, DB 설정파일
    - 백업파일(.bak, .old, .zip)
    - 소스코드 원본(예: .git/)
3. 서비스 계정의 홈 디렉토리는 700 이상으로 제한
4. 업로드 폴더 접근권한은 최소권한으로 설정(예: 750)

제 11 조(환경변수 및 설정파일 관리)

1. API Key·Secret Key 는 다음 저장 방식만 허용:
2. 환경파일(.env)은 권한 600 적용
    - Key Vault
    - 보안장비(HSM)
    - Secrets Manager
3. 민감정보는 환경파일 또는 코드 내 하드코딩 금지
4. 설정파일 변경 시 버전관리 및 승인절차 준수

제 5 장 애플리케이션 보안

제 12 조(웹·API 서비스 보안 설정)

1. 서버 정보 노출 방지(ServerTokens/ProductSignature Off)
2. 디렉토리 리스팅 금지
3. 파일 업로드 경로는 외부 접근 불가 영역으로 분리
4. 업로드 파일 MIME 검증 및 확장자 제한
5. HTTPS(TLS 1.2 이상) 강제 적용

제 13 조(로그 및 오류 처리)

1. 시스템 오류 페이지에 다음 내용 표시 금지:
    - DB 오류
    - 경로 정보
    - 환경 정보
    - 내부 IP 정보
2. 애플리케이션 로그는 보안정책 제 10 조 기준 적용
3. 결제 트랜잭션 로그는 변조 방지 적용 후 5 년 보관

제 14 조(코드 및 배포 보안)

1. 배포는 CI/CD 를 사용하고 직접 서버에 접속하여 수정하는 행위 금지
2. 코드 리뷰 필수 항목:
    - 인증/인가 로직
    - 입력값 검증
    - 민감정보 처리
3. 취약점 검사(SAST, DAST)
    - 주요 배포 시: SAST
    - 분기 1 회: DAST

제 6 장 컨테이너 및 가상화 보안

제 15 조(컨테이너 보안)

1. Root 컨테이너 사용 금지
2. Public 이미지 사용 시 무결성 검증
3. 컨테이너 내부에 비밀번호·Key 저장 금지
4. 컨테이너 간 통신은 최소 Port 만 허용

제 16 조(가상머신/클라우드 보안)

1. 인스턴스 메타데이터 접근 제한
2. IAM Role 최소 권한
3. 클라우드 로그(CloudTrail 등) 활성화
4. 보안그룹은 Inbound/Outbound 모두 최소 허용

제 7 장 시스템 모니터링 및 점검

제 17 조(실시간 모니터링)

1. 다음 항목을 중앙 모니터링 시스템과 연동
    - CPU/Mem/Network 사용량
    - Disk I/O
    - 비정상 트래픽
    - 프로세스 장애
    - WAF/UTM 이벤트

제 18 조(정기 점검)

1. 서버 구성 점검: 월 1 회
2. 파일 권한·서비스 설정 점검: 분기 1 회
3. 서버 내 노출파일 점검(phpinfo 등): 월 1 회
4. 결과는 문서화하여 1 년 이상 보관

제 8 장 예외관리

제 19 조(예외 승인 절차)

1. 긴급 패치 불가·구성상 차단이 어려운 경우 예외 적용 가능
2. 반드시 다음 포함:
    - 사유
    - 위험 분석
    - 대체 조치
    - 예외 적용 기간
3. CISO 승인 후 적용하며 만료 즉시 원복

제 9 장 부칙

제 20 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 21 조(개정)

본 지침은 정보보호책임자의 검토 후 개정한다.