EAT-IT 보안정책서

EAT-IT 보안정책서

제 1 장 총칙

제 1 조(목적)

본 정책은 EAT-IT 에서 운영하는 밥세권서비스 및 관련 시스템의 기밀성·무결성·가용성을 확보하기 위한 정보보안 관리 기준을 정의하여 회사의 정보자산을 안전하게 관리함을 목적으로 한다.

제 2 조(근거 법령)

본 정책은 다음의 법 및 기준을 준수한다

1. 개인정보 보호법 및 시행령
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령
3. 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드
4. 전자금융기반시설 보안 취약점 평가기준 안내서
5. 개인정보의 안전성 확보조치 기준
6. 전자금융거래법 및 시행령
7. 신용정보법 및 시행령
8. 전자서명법
9. 전자문서 및 전자거래 기본법
10. ISMS-P 인증 기준
11. NIST, OWASP, CIS Benchmark 등 국제 표준

제 3 조(적용 범위)

본 정책은 회사가 소유·관리·운영하는 모든 정보 자산과 이를 취급하는 임직원, 계약직, 협력업체 및 외부 개발·운영 인력에 적용한다.

1. EAT-IT 임직원 및 협력업체, 외부 개발·운영 인력
2. 밥세권서비스 운영을 위해 사용하는 서버, DB, 네트워크, 보안장비
3. 웹 서비스 및 내부 업무 시스템
4. 서비스 개발·운영·유지보수 과정에서 취급되는 모든 정보 자산

제 4 조(정의)

본 정책에서 사용하는 용어의 정의는 다음과 같다. 세부 정의는 정책 부속문서에서 규정한다.

1. 정보 자산: 회사가 보유하거나 서비스 운영에 사용되는 모든 데이터, 문서, 시스템, 네트워크 장비 등을 의미한다.
2. 정보시스템: 서버, DBMS, 웹·API, 네트워크 장비 등 정보처리에 필요한 일체의 시스템을 의미한다.
3. 취약점 분석·평가: 정보시스템의 보안 취약점을 식별하고 위험도를 분류하는 활동을 의미한다.
4. 모의 침투: 공격자 관점에서 실제 공격 기법을 활용하여 시스템의 보안수준을 검증하는 활동을 의미한다.
5. 개인정보: 개인을 식별할 수 있는 모든 정보를 의미한다.
6. 위험 수용: 식별된 위험요소 중 조치가 불가능하거나 비효율적일 때, 문서화된 사유를 기반으로 일정 조건하에 조치를 유예하는 것을 의미한다.

제 2 장 보안 대상 및 조직

제 5 조(정보보호 조직)

정보보호 조직은 회사의 정보자산을 안정적으로 보호하기 위해 다음과 같이 구성하며, 각 역할별 책임과 교육 기준을 적용한다.

1. 정보보호책임자(CISO)는 정보보호 전략 수립, 보안 예산 승인 요청, 보안정책 운영의 총괄 책임을 가진다.
    1. 연 1 회 이상 정보보호 책임자 교육을 이수한다.
2. 개인정보보호책임자(CPO) 는 개인정보 처리 및 보호 업무를 총괄하며, 개인정보 안전성 확보조치 준수 여부를 관리한다.
    1. 연 1 회 이상 개인정보보호 책임자 교육을 이수한다.
3. 보안관리자는 CISO·CPO 의 지시에 따라 보안정책 운영, 시스템·네트워크·DB 보안 조치 이행, 보안점검 계획 수립 및 실행 등을 담당한다.
    1. 연 1 회 이상 정보보안 전문 교육을 이수한다.
4. 정보보안담당자는 취약점 분석·평가, 사고 대응, 접근통제 점검, 로그 분석 등 기술적 보호조치를 수행하며, 보안장비 및 시스템 보안 구성의 유지관리를 담당한다.
    1. 연 1 회 이상 실무 보안 교육 및 보안 위협 대응 교육을 이수한다.
5. 협력업체 및 외부 운영 인력은 회사의 정보보안 정책·절차·지침을 준수해야 하며, 필요 시 정보보호책임자(CISO) 또는 보안관리자의 요청에 따라 보안 교육 또는 준수 서약서를 제출해야 한다.

제 3 장 정보보호 통제 정책

제 6 조(계정 및 접근통제)

계정 및 접근통제 정책은 다음 사항을 적용한다.

1. 모든 시스템 접근은 최소 권한 원칙을 적용한다.
2. 외부 접속은 VPN 및 암호화된 통신(TLS)을 통해서만 허용한다.
3. Root/Administrator 직접 로그온을 금지한다.
4. 90 일 이상 미사용 계정은 자동 잠금 한다.

제 7 조(네트워크 보호)

네트워크 보호 통제는 다음 사항을 준수하여 설정, 운영한다.

1. 네트워크는 업무 특성 및 보안 등급에 따라 존(Zone)으로 분리하여 운영한다(DMZ/서버 존/업무 존 등).
2. 방화벽 정책은 기본 차단(Default Deny) 방식으로 운영한다(Allow by Exception).
3. 포트·프로토콜·IP 허용 요청은 사유 및 위험 분석을 포함하며, 정보보호책임자(CISO) 승인 후 적용한다.
4. 외부 위험국가 IP 또는 공격 출처 IP 는 차단한다.

제 7-1 조(보안장비)

보안장비(WAF, UTM)의 효과적인 운영 및 서비스 보호를 위해 다음 기준을 적용한다.

1. UTM 과 WAF 는 밥세권서비스의 네트워크·웹·결제·관리자 페이지 전반을 보호하기 위한 핵심 보안장비로 운영한다.
2. 모든 보안장비 정책은 최소 권한 원칙(Allow by Exception)에 따라 구성하며, 정책 변경 시 사유·위험 분석·적용 범위를 포함하여 정보보호책임자(CISO) 승인 후 반영한다.
3. UTM 은 DMZ, 내부망, 서버존 간 트래픽을 통제하며 IPS 기능을 활성화하여 Injection, RCE, Brute Force, Port Scan 등 주요 공격 패턴을 탐지·차단한다.
4. 악성 URL·피싱 사이트 차단(URL Filtering)을 활성화하여 관리자·사용자 환경 전체의 위협을 선제적으로 차단한다.
5. WAF 는 웹·API·결제·관리자 페이지의 공격 방어를 위해 운영하며, SQL Injection, XSS, File Upload 우회, Command Injection 등 주요 웹 공격에 대한 차단 Rule 을 적용한다.
6. IPS/WAF 시그니처 및 보안정책은 최소 월 1 회 이상 업데이트를 수행하고, 서비스 변경 시 즉시 정책을 재검토한다.
7. 보안장비 장애 발생 또는 탐지 이벤트 발생 시 즉시 정보보호책임자(CISO)에 보고하고, 분석·조치 내용을 기록한다.

제 8 조(시스템 보안)

시스템 보안을 위해 다음 사항을 적용한다.

1. 서버 및 OS 는 주요정보통신기반시설의 기술적 취약점 분석 · 평가를 준수한다.
2. 설치된 서비스 중 불필요한 기능·포트는 즉시 제거한다.
3. 패치 및 업데이트는 정기적으로 수행하며, 심각(Critical) 위험 패치는 즉시 반영한다.
4. Root 권한은 최소 인원만 관리하고 사용 이력을 기록한다.

제 9 조(계정 및 접근통제)

암호화 및 키 관리는 다음 기준을 적용한다.

1. 저장 데이터는 AES-256 이상의 알고리즘을 적용한다.
2. 전송 구간은 TLS 1.2 이상을 필수 적용한다.
3. 암호 키 접근 권한은 최소 인원으로 제한한다.
4. 주요 암호 키는 연 1 회 이상 교체한다.

제 10 조(로그 및 모니터링)

로그 및 모니터링 체계를 운영하기 위해 다음 기준을 적용한다.

1. 모든 대상 시스템의 로그를 중앙 서버로 안정적으로 수집하고 데이터 누락을 방지한다.
2. 로그의 위·변조를 방지하고 접근을 통제한다.
3. 개인정보보호법 고시 기준(최소 1 년)을 충족하며 스토리지 비용을 효율화 한다.
   또한, 법령에서 요구하는 경우 기간을 확장한다.
4. 심각한 보안 및 운영 이벤트 발생 시 즉시 감지하고 정보보호책임자(CISO)에게 보고한다.

제 11 조(계정 및 접근통제)

결제 기능 운영 시 결제 데이터의 기밀성·무결성·가용성을 확보하기 위해 다음 기준을 적용한다.

1. 결제 처리 과정에서 카드번호, CVC, 유효기간 등 민감정보는 서버에 저장을 금지한다.
2. 결제 데이터 전송 구간은 TLS 1.2 이상을 필수 적용한다.
3. 결제 API Key·Secret Key 는 안전한 Key Vault 또는 보안장비(HSM)에 저장하며, 접근 권한은 최소 인원으로 제한한다.
4. Webhook·Callback URL 은 무결성 검증(Signature 또는 Token)을 통해 요청을 검증한다.
5. PG 연동 IP 는 화이트리스트 기반으로 제한하고, 비인가 IP 접근은 차단한다.
6. 결제 요청 및 결과값에 대해 파라미터 변조 차단을 위한 서명값 또는 해시값 검증을 적용한다.

7. 결제 관련 로그(거래내역, Transaction ID, 요청/응답 로그)는 위·변조 방지 후 5 년 이상 보관한다.
8. 결제 영역은 OWASP TOP 10 및 금융보안원 가이드에 따라 연 1 회 이상 보안 점검을 시행한다.
9. 결제 오류(중복결제, 미완료 결제 등)는 재현 가능한 로그 및 원인 분석 자료를 기반으로 즉시 대응한다.

제 4 장 관리적 보안

제 12 조(취약점 분석 및 모의 침투)

취약점 관리와 모의 침투 수행을 위해 다음 기준을 적용한다.

1. 취약점 분석·평가는 연 1 회 이상 수행한다.
2. 중요 서비스에 대해서는 반기 1 회 이상 모의 침투(모의해킹)를 수행한다.
3. 식별된 취약점은 High → Medium → Low 등급으로 분류하여 우선 조치한다.
4. 취약점 및 조치 결과는 문서로 기록하고 관리한다.

제 13 조(사고 대응)

보안사고 대응을 위해 다음 절차를 적용한다.

1. 사고 대응 절차는 다음을 따른다.
   탐지 → 격리 → 분석 → 복구 → 재발방지
2. 사고 발생 시 즉시 정보보호책임자(CISO) 및 보안관리 부서에 보고한다.
3. 사고 대응 결과 및 근본 원인 분석을 문서화하여 재발을 방지한다.
4. 개인정보 유출 사고 발생 시, 지체 없이 유출된 개인정보 항목 및 경위 등 상세 사항을 정보주체에게 통지하고 관계 기관에 신고해야 한다.

제 14 조(백업 및 복구)

백업 및 복구 체계를 유지하기 위한 기준은 다음과 같다.

1. 주요 데이터는 최소 일 1 회 이상 증분 백업 한다.
2. 매달 1 일은 전체 백업을 실시한다.
3. 백업본 무결성 검증을 정기적으로 수행한다.
4. 복구 테스트는 연 1 회 이상 실시한다.
5. 데이터 가용성과 재해복구 보장을 위해 이중화된 백업 시스템을 구축하고, 본사-지사 간 교차 백업을 의무적으로 시행해야 한다.
6. 재해복구 기준 및 절차는 다음과 같이 운영한다.
    1. RTO 는 4 시간 이내, RPO 는 24 시간 이내로 설정한다.

2. 재해 발생 시 상황보고 → DR 전환 결정 → 백업본 복구 → 서비스 점검 → 정상화 순으로 복구 절차를 수행한다.
3. DR 환경 구성(백업 스토리지·DR 서버·네트워크 이중화 등)을 유지하고, 관련 계획은 연 1 회 이상 점검 및 갱신한다.

제 15 조(보안 교육)

임직원의 정보보안 인식 제고를 위해 다음 기준을 적용한다.

1. 전 임직원은 연 1 회 이상 정보보안 교육을 필수 이수한다.
2. 피싱·랜섬웨어 대응 교육 및 모의 훈련을 정기적으로 수행한다.
3. 신규 입사자는 입사 즉시 보안교육을 이수한다.

제 5 장 물리적 보안

제 16 조(출입 통제)

물리적 보안을 유지하기 위해 다음 기준을 적용한다.

1. 출입 통제 대상 구역은 다음과 같다.중요 구역은 보안등급에 따라 일반구역·제한구역·통제구역으로 구분한다.
    1. 서버실(Server Room) – WEB, DB, MAIL, LOG, BACKUP 서버 등 주요 서비스 장비 위치
    2. 네트워크 장비실(Network Equipment Room) – 스위치, 라우터, 방화벽, UTM·WAF 등 네트워크·보안장비 위치
    3. 전산실(IT Operations Room**)** – 관리용 PC, 관리 콘솔, 모니터링 장비 위치
    4. DR 및 백업구역(Backup/DR Zone) – 백업 스토리지 및 재해복구 장비 위치
    5. 기타 정보보호책임자(CISO)가 지정한 중요 정보처리 공간
2. 서버실·전산실·네트워크 장비실 등 중요 구역은 지정된 인원만 출입할 수 있다.
3. 출입 기록(출입자 정보·출입 일시·출입 목적·카드키/출입증 로그)은 6 개월 이상 보관한다.
4. 출입 권한은 분기 1 회 이상 정기적으로 검토하며, 직무 변경·전출·퇴사 시 즉시 권한을 회수한다.
5. 장비 반출입은 다음 기준을 적용한다.
    1. 서버·네트워크·백업·보안장비 등 중요 장비 반출 시 사전 승인서를 작성해야 한다.
    2. 반출입 내역은 장비관리대장에 기록하고 보안관리자가 검토한다.
    3. 외부 수리 목적 반출은 정보보호책임자(CISO) 승인 후 가능하며, 반입 후 무결성 확인을 수행한다.
6. 방문자 관리 절차는 다음 기준을 적용한다.
    1. 방문객은 출입대장 등록 및 신분증 확인 후 방문자증을 발급받는다.

2. 방문자는 지정된 담당자의 동행(Escort) 하에 작업하며, 단독 출입을 금지한다.
3. 방문자 기록 및 작업 내역은 6 개월 이상 보관한다.

7. 내부 인력 및 외부 인력 출입 기준은 다음과 같다.
    1. 내부 인력**:** 직무상 필요 인원에게만 출입 권한을 부여하며 최소권한 원칙을 적용한다.
    2. 외부 인력(협력업체·점검 인력):
        1. 사전 승인 절차 후 출입 가능
        2. 작업 목적·작업시간·사용 장비를 사전 제출해야 함
        3. 출입 중에는 보안관리자 또는 담당자의 감독하에 작업한다.

제 6 장 문서 관리

제 17 조(문서 관리)

보안 문서의 무결성과 최신성을 유지하기 위해 다음 기준을 적용한다.

1. 모든 보안 문서는 최신 상태로 유지하며 변경 시 버전 관리를 시행한다.
2. 보안 관련 문서는 접근권한을 가진 인원에 한하여 열람할 수 있다.

제 18 조(기록 보존)

보안 로그, 사고 기록, 취약점 점검 및 조치 내역은 1 년 이상 보관한다.

제 7 장 보호대책 수립

제 19 조(단기 보호대책)

다음 항목은 사업기간 내 즉시 개선 대상이다.

1. High Risk 취약점 즉시 조치
2. 암호화 미 적용 구간 해소
3. 계정·권한 구조 재정비
4. 네트워크 구조 재정립
5. 취약한 웹 요소(OWASP TOP 10 에 기반한 취약점) 즉각 차단

제 20 조(중기 보호대책)

회사는 다음 중기 목표 기반 보호대책을 추진한다.

1. ISMS 기반 보안정책 전면 개정 및 운영체계 고도화
2. EDR, WAF, SIEM 등 보안솔루션 도입 및 고도화

3. DR·백업 체계 및 고 가용성 인프라 강화
4. DevSecOps 기반 개발·보안·운영 프로세스 통합

제 8 장 부칙

제 21 조(시행일)

본 정책은 2025 년 12 월 29 일부터 시행한다.

제 22 조(개정)

본 정책은 정보보호책임자의 검토 후 대표자의 승인을 통해 개정한다.