

보안 규정·지침·절차 검토

결과 보고서

작성기관 : 푸드파이터

작성자 : 김기수

작성일 : 2025-12-05

버전 : 1.00

목차

■ 1. 개요.....	4
1.1 보고서 목적.....	4
1.2 검토 범위.....	4
1.3 검토 대상 문서 목록.....	4
■ 2. 검토 방법론.....	5
2.1 검토 기준.....	5
2.2 검토 절차.....	5
■ 3. 문서별 검토 결과.....	5
3.1 보안정책서.....	5
3.2 계정 관리 지침.....	5
3.3 접근통제 지침.....	6
3.4 시스템 보안 지침.....	6
3.5 암호화 및 키 관리 지침.....	6
3.6 로그 및 모니터링 지침.....	6
3.7 취약점 분석 및 모의침투 지침.....	6
3.8 사고 대응 지침.....	7
3.9 백업 및 복구 지침.....	7
3.10 보안 교육 지침.....	7
3.11 물리적 보안 지침.....	7
3.12 별지 양식(사용자 계정 신청서).....	8

■ 4. 규정·지침·절차 정합성 분석.....	8
4.1 정책-지침 매핑 결과.....	8
4.2 절차(Procedure) 구현 수준.....	9
■ 5. 미흡사항 및 리스크 분석.....	9
5.1 주요 미흡사항 요약.....	9
5.2 리스크 평가.....	9
■ 6. 개선방안 및 이행 로드맵.....	10
6.1 우선순위별 개선방안.....	10
6.2 단기·중기 이행계획(안).....	10
■ 7. 결론.....	10
■ 부록 A. 검토 대상 문서 목록(표).....	11
■ 부록 B. 정책-지침 매핑표.....	12
■ 부록 C. 미흡사항 및 개선방안 요약표.....	13

■ 1. 개요

1.1 보고서 목적

본 보고서는 EAT-IT 이 운영하는 밥세권 서비스의 보안정책서와 10 개 보안 지침, 그리고 별지 사용자 계정 신청서를 대상으로 문서 간 정합성, 내용의 충분성, 실제 운영 관점에서의 적정성, 법적·기술적 준거성을 검토하여 현 보안 문서 체계의 성숙도와 개선 방향을 제시하는 것을 목적으로 한다.

1.2 검토 범위

본 검토는 보안정책서 v1.00, 10 개 보안 지침 v1.00, 별지 사용자 계정 신청서 v1.00 을 범위로 한다. 문서 검토는 정책-지침 간 정합성, 절차 지원 여부, 미흡사항 및 개선방안 도출을 중심으로 수행하였다.

1.3 검토 대상 문서 목록

구분	문서명	버전	비고
정책	EAT-IT 보안정책서	v1.00	상위 보안 원칙 규정
지침	계정 관리 지침	v1.00	계정 생성/변경/삭제 절차
	접근통제 지침	v1.00	네트워크·서버·DB 접근 기준
	시스템 보안 지침	v1.00	OS·서버·애플리케이션 보안 구성
	암호화 및 키 관리 지침	v1.00	암호화·Key Vault 기준
	로그 및 모니터링 지침	v1.00	로그 수집/보관/경보 기준
	취약점 분석 및 모의침투 지침	v1.00	정기 점검·모의해킹 기준
	사고 대응 지침	v1.00	탐지→격리→분석→복구 절차
	백업 및 복구 지침	v1.00	백업·DR·복원 테스트 기준
	보안 교육 지침	v1.00	정기·신규자·역할 기반 교육 기준
	물리적 보안 지침	v1.00	중요구역 출입통제·장비 반출입·DR 구역 운영 기준
별지	사용자 계정 신청서	v1.00	계정 발급 절차 양식

■ 2. 검토 방법론

2.1 검토 기준

문서 검토는 완전성, 일관성, 적정성, 준거성 네 가지 기준에 따라 수행하였다.

- 완전성: 정책 요구사항이 지침·별지 문서에 누락 없이 구현되었는지 확인
- 일관성: 문서 간 용어, 절차 흐름, 역할·책임이 충돌하지 않는지 검토
- 적정성: 실제 서비스 인프라·조직 환경에서 적용 가능한 수준인지 평가
- 준거성: 관련 법령 및 보안 가이드 대비 적합성 검토

2.2 검토 절차

- ① 문서 목록 정리 및 정책·지침·별지 분류
- ② 정책-지침 매핑 분석으로 구현 수준 평가
- ③ 계정, 접근통제, 로그, 사고 대응 등 보안 영역별 세부 내용 검토
- ④ 미흡사항 및 리스크 도출
- ⑤ 개선방안 및 이행 로드맵 수립

■ 3. 문서별 검토 결과

3.1 보안정책서

보안정책서는 상위 보안 원칙을 역할·책임 기반으로 정의하고 있으며 지침들과의 연계가 양호하다. 다만 일부 조항은 절차 수준으로 세분화되면 운영 명확성이 향상될 수 있다.

3.2 계정 관리 지침

계정 관리 지침은 계정 생성·변경·삭제 기준이 명확하며 별지 사용자 계정 신청서와 연계되어 있다. 관리자 페이지 및 내부 운영 페이지 계정 관리 기준이 포함되어 있어 서비스 운영 환경에 필요한 계정 통제가 가능하며, 승인 체계 또한 책임과 역할을 명확히 구분할 수 있도록

구성되어 있다. 다만 계정 승인 흐름을 도식화한 절차서가 제공된다면 실무적인 이해도가 더욱 높아질 수 있다.

3.3 접근통제 지침

접근통제 지침은 네트워크·서버·DB 자산에 대한 접근 기준을 구조적으로 정의하고 있으며, 허용/차단 정책과 관리자 접근 통제 기준이 포함되어 있다. ACL 변경 절차와 검증 기준이 명시되면 운영 측면에서 완성도가 더 높아질 수 있다.

3.4 시스템 보안 지침

시스템 보안 지침은 OS·애플리케이션 보안 설정, 계정 관리, 패치 적용 기준 등을 포함하고 있어 기본적인 보안 베이스라인으로 적정하다. 운영 점검 항목이 더 구체적으로 정의되면 점검 효율성이 향상될 수 있다.

3.5 암호화 및 키 관리 지침

암호화 및 키 관리 지침은 저장·전송 구간 암호화 기준과 키 수명주기 관리, 보관 위치 등에 대한 기준을 제시하고 있다. 민감 정보 보호 측면에서 준거성이 높으나, 키 접근 로그 관리 기준이 추가되면 실무 적용성이 더욱 향상될 수 있다.

3.6 로그 및 모니터링 지침

로그 및 모니터링 지침은 수집 대상 로그 항목과 보존 기간, 전송 방식 등을 정의하고 있으며, 관제 시스템과의 연계도 고려하고 있다. 다만 실제 탐지 임계값과 SIEM 룰에 대한 내용은 부족하여 별도의 로그 운영가이드가 필요하다.

3.7 취약점 분석 및 모의침투 지침

취약점 분석 및 모의침투 지침은 정기 점검 주기와 대상, 보고 절차를 정의하고 있으며, 클라우드 환경을 포함한 취약점 점검 항목과 활용 가능한 취약점 분석 도구 목록을 명확히

제시하고 있어 점검 범위와 일관성이 유지되도록 하고 있다. 추가로 점검 결과 보고서 템플릿이 제공된다면 현업 적용성이 한층 더 향상될 수 있다.

3.8 사고 대응 지침

사고 대응 지침은 탐지→분석→격리→복구 단계로 대응 절차를 구분하고 있으며, 등급 분류 및 보고 체계를 포함하고 있다. 개인정보 관련 사고 발생 시 개인정보보호책임자(CPO)에게 보고하는 절차 또한 명확히 규정되어 있어 사고 대응 책임 체계가 정립되어 있다. 다만 연락체계와 외부기관 신고 기준이 더 상세히 정의되면 좋다.

3.9 백업 및 복구 지침

백업 및 복구 지침은 백업 유형과 주기, 보존 기간, DR 기준을 포함하고 있으며, 정기적인 복구 테스트 수행을 요구하고 있다. 복구 테스트 결과를 기록하는 양식이 추가되면 관리 효율성이 향상될 수 있다.

3.10 보안 교육 지침

보안 교육 지침은 정기 교육, 신규자 교육, 역할 기반 교육 등에 대한 기준을 정의하고 있다. 교육 효과 측정 방식이 추가되면 보안 인식 수준을 지속적으로 관리하는 데 도움이 될 것이다.

3.11 물리적 보안 지침

물리적 보안 지침은 서버실·전산실·네트워크 장비실 등 중요 구역에 대한 출입통제 기준과 장비 반출입 절차, DR·백업구역 관리 등을 정의하고 있다. 출입기록 보관, 직무 변경 시 권한 회수, 방문자 관리 등 운영 기준이 구체적으로 명시되어 있어 물리적 접근으로 인한 보안사고를 예방하는 데 효과적이다. 다만 물리적 보안 점검 체크리스트나 정기 점검 절차가 추가된다면 관리 효율성은 더욱 향상될 수 있다.

3.12 별지 양식(사용자 계정 신청서)

사용자 계정 신청서는 계정 요청 항목과 승인 절차를 명확하게 표현하고 있으며, 승인 대상은 시스템 관리자로 지정되어 있어 운영 책임자 중심의 계정 관리 흐름과 일관성을 유지하고 있다. 다만 계정 및 접근통제 절차와의 흐름도가 함께 제공되면 이해도가 더욱 높아질 수 있다.

■ 4. 규정·지침·절차 정합성 분석

4.1 정책-지침 매핑 결과

정책 조항	대응 지침	구현 수준
제 6 조 계정·접근통제	계정 관리 지침 / 접근통제 지침	양호
제 7 조 네트워크 보호	접근통제 지침	양호
제 7-1 조 보안장비	접근통제 지침 / 로그 및 모니터링 지침	양호
제 8 조 시스템 보안	시스템 보안 지침	양호
제 9 조 암호화	암호화 및 키 관리 지침	양호
제 10 조 로그 및 모니터링	로그 및 모니터링 지침	양호
제 11 조 결제 보안	접근통제·암호화·로그·백업 지침	매우 양호
제 12 조 취약점 분석 및 모의침투	취약점 분석 및 모의침투 지침	양호
제 13 조 사고 대응	사고 대응 지침	양호
제 14 조 백업 및 복구	백업 및 복구 지침	양호
제 15 조 보안 교육	보안 교육 지침	양호
제 16 조 물리적 보안(출입 통제)	물리적 보안 지침	양호

전반적으로 정책의 요구사항은 대응되는 지침에서 구현되어 있으며, 특히 결제·접근·로그·백업 등 중요 영역은 다층적인 통제를 구성하고 있다. 각 지침은 정책서의 요구사항을 기반으로 영역별 통제를 명확히 정의하고 있으며, 계정·접근통제, 시스템 보안, 물리적 보안, 취약점 분석·사고 대응 등 주요 보안 분야를 일관성 있게 반영하고 있다.

4.2 절차(Procedure) 구현 수준

정책과 지침은 구성 요소별 요구사항을 충족하지만, 계정 발급·변경, 사고 대응, 로그 분석 등 핵심 업무에 대한 절차 문서가 별도로 존재하지 않아 운영 표준화, 책임 구분, 감사 대응 측면에서 리스크가 존재한다.

■ 5. 미흡사항 및 리스크 분석

5.1 주요 미흡사항 요약

미흡사항	내용	영향도	개선 필요성
절차서 부재	정식 절차문서가 별도 존재하지 않음	High	운영 표준화 및 감사 대응 위해 필수
변경관리 부족	설정·배포 변경 이력이 체계적으로 관리되지 않음	High	장애 원인 분석 및 추적이 어려움
로그/탐지 기준 부족	SIEM 탐지 임계치, 경보 처리 기준이 미흡	Medium	침해사고 초기 탐지 지연 가능성
용어 정의 불일치	문서별 일부 용어 정의 및 표현 상이	Low	문서 이해도 및 유지보수성 저하
신청서 연계 약함	사용자 계정 신청서와 지침 간 절차 흐름 설명 부족	Medium	계정·권한 허름 인지 어려움
물리적 보안 운영 기준의 절차 부족	출입통제·반출입 절차는 정의되어 있으나, 정기 점검 절차·점검표 부재	Medium	물리적 접근 사고 예방을 위해 절차 보완 필요

5.2 리스크 평가

절차서와 변경관리 문서의 부재는 운영은 잘 되어도 문서 상 근거가 부족해 보이는 문제를 유발할 수 있다. 이는 인증 심사나 외부 감사, 고객사 보안 요구 사항 검토 시 형식적 미비 사항으로 지적될 가능성이 크다. 로그 운영가이드와 신청서 연계 부족은 실무자마다 다른

방식으로 업무를 수행하게 만들 수 있으며, 신규 인력이나 외부 점검자가 문서를 해석할 때 이해를 어렵게 만든다는 점에서 중간 수준의 리스크로 판단된다.

■ 6. 개선방안 및 이행 로드맵

6.1 우선순위별 개선방안

우선순위	개선 항목	개선 내용
1	절차서 신규 작성	계정·접근·사고 대응·로그 분석 등 핵심 업무에 대한 절차 문서 작성
1	변경관리 프로세스 구축	설정 변경 승인·검증·롤백 기준과 이력 관리 체계 수립
2	로그 운영가이드 작성	SIEM 탐지 임계치, 경보 레벨, 처리 절차를 정의한 운영가이드 수립
2	신청서 흐름 명확화	사용자 계정 신청서가 계정 관리·접근 통제 절차에서 어떻게 사용되는지 흐름도 작성
3	용어 표준화	전사 공통 용어집을 작성하여 정책·지침·절차서에 동일 용어 사용

6.2 단기·중기 이행계획(안)

단계	기간	주요 내용
단기	1 개월	절차서 초안 작성 및 변경관리 기준 수립
중기	2~3 개월	로그 운영가이드 수립 및 SIEM 탐지 룰 정비
장기	3 개월+	문서 일관성 관리 및 용어 표준화 체계 정착

■ 7. 결론

EAT-IT의 보안 문서 체계는 정책과 지침이 상호 연계되어 있으며, 주요 보안 영역을 폭넓게 포함하고 있다. 다만 절차 문서 및 운영 가이드의 부족으로 인해 운영 효율성과 감사 대응 측면에서 개선이 필요하다. 본 보고서는 이러한 문서 체계의 고도화를 위한 기반 자료로 활용될 수 있다.

■ 부록 A. 검토 대상 문서 목록(표)

구분	문서명	버전	비고
단기	1 개월	절차서 초안 작성 및 변경관리 기준 수립	
중기	2~3 개월	로그 운영가이드 수립 및 SIEM 탐지 룰 정비	
장기	3 개월+	문서 일관성 관리 및 용어 표준화 체계 정착	

■ 부록 B. 정책-지침 매핑표

정책 조항	대응 지침	구현 수준
제 6 조 계정·접근통제	계정 관리 지침 / 접근통제 지침	양호
제 7 조 네트워크 보호	접근통제 지침	양호
제 7-1 조 보안장비	접근통제 지침 / 로그 및 모니터링 지침	양호
제 8 조 시스템 보안	시스템 보안 지침	양호
제 9 조 암호화	암호화 및 키 관리 지침	양호
제 10 조 로그 및 모니터링	로그 및 모니터링 지침	양호
제 11 조 결제 보안	접근통제·암호화·로그·백업 지침	매우 양호
제 12 조 취약점 분석 및 모의침투	취약점 분석 및 모의침투 지침	양호
제 13 조 사고 대응	사고 대응 지침	양호
제 14 조 백업 및 복구	백업 및 복구 지침	양호
제 15 조 보안 교육	보안 교육 지침	양호
제 16 조 물리적 보안	물리적 보안 지침	양호

■ 부록 C. 미흡사항 및 개선방안 요약표

미흡사항	영향도	개선 항목	비고
절차서 부재	High	절차서 신규 작성	운영 표준화 및 감사 대응
변경관리 부족	High	변경관리 프로세스 구축	장애 원인 분석 및 추적
로그/탐지 기준 부족	Medium	로그 운영가이드 작성	SIEM 탐지 기준 명확화
용어 정의 불일치	Low	용어 표준화	문서 이해도 향상
신청서 연계 약함	Medium	신청서 흐름 명확화	계정·권한 흐름 가시화