이인후

정보보호 컨설턴트 포트폴리오

me@inhoolee.com / 010-8075-3280

소개

전문성 있는 정보보호 컨설턴트로 성장하는 것이 목표인 이인후입니다.
기술과 법, 양쪽 방면에서 전문성을 갖추려고 합니다.
ISMS 인증 컨설팅과 운영관리를 맡아 실무 능력을 쌓고 있습니다.

직무 경험

아이시큐어 **2026.09 ~ 재직중**
정보보안 컨설턴트

코드박스
소프트웨어 엔지니어 2022.11 ~ 2024.12
정보보호담당자 (ISMS 최초 인증 대응) 2023.08 ~ 2024.12

교육

KISIA 보안전문가 과정 2026.07 ~ 2026.08
숭실대학교 소프트웨어학부 2016.03 ~ 2022.02

자격증

CPPG (개인정보관리사) 2026.09.09 취득
정보보안기사 필기 합격 · 실기 준비중
정보처리기사 필기 합격 · 실기 준비중
네트워크관리사 2급 2026.09.22 취득
SQLD 2021.09.05 취득



ISMS-P 인증 컨설팅

플랫폼 기업 ISMS-P 간편인증 컨설팅

기간
2026.10 ~ 진행중

역할
아이시큐어 정보보안 컨설턴트 (컨설턴트 3인 팀)

담당
현황분석, 위험평가

대상
민감정보를 처리하는 플랫폼 기업 (간편인증 최초심사)

1. 부서별 인터뷰 인사 · CS · 영업 · 개발 · 마케팅 팀 인터뷰에 참여해 업무별 처리 현황 파악

2. 서비스 점검 웹 · 앱 가입 · 예약 과정 파악 및실제 수집 항목 · 동의 항목 확인

3. 처리방침 점검 작성지침 기재사항과 실제 처리 현황을 조항별로 대조해 누락 · 불일치 도출

4. 개정(안) 작성 조항별 개정 문구와 근거 법령 · 사유를 정리해 단계별로 공유

5. 처리 화면 개선(안) 수집 · 이용 동의, 대리 입력, 앱 권한 안내 화면의 개선 방안 작성

컨설팅 기준

2026 개인정보 처리방침 작성지침 - 기재사항 · 작성 예시 기준
개인정보 보호법 · 시행령 - 처리 근거 · 국외 이전 · 아동 개인정보

결과 및 산출물

- X 개인정보 처리방침 개정(안)
- X 처리방침 작성지침 기재사항 점검표
- X 개인정보 처리 화면 개선(안)

01 처리방침 작성지침 기재사항 점검표



개인정보처리방침 기재 사항 점검 — 개인정보 처리방침 작성지침 (2026.04)

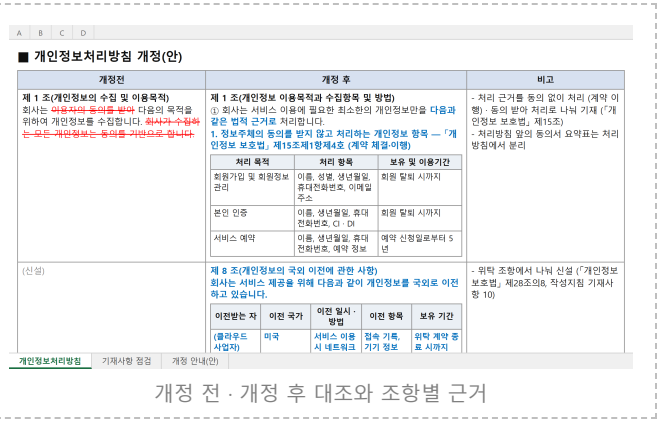
점검 기준: 개인정보보호위원회 「2026 개인정보 처리방침 작성지침」

구분	기재사항	필수 여부	원문	해당 조항	비고
1	제목 및 서문	필수	있음	머리말	- 공개 근거를 「개인정보 보호법」 제30조로 변경
2	개인정보의 처리 목적	필수	있음	제1조	- 처리 항목과 함께 기재 (작성 예시 2 통합 행)
3	처리하는 개인정보의 항목	필수	있음	제1조	- 동의 없이 처리 (계약 이행) · 동의 받아 처리로 나눠 기재
4	14세 미만 아동의 개인정보 처리에 관한 사항	해당 시	확인	제4조	- 보호자가 대신 입력하는 경우의 항목 · 법정대리인 확인 방법
5	개인정보의 처리 및 보유 기간	필수	있음	제3조	
6	개인정보의 파기 절차 및 방법에 관한 사항	필수	있음	제5조	
7	개인정보의 제3자 제공에 관한 사항	해당 시	있음	제6조	- 제공받는 자 · 목적 · 항목 최신화 확인 요청
8	추가적인 이용·제공이 지속적으로 발생 시 판단 기준	해당 시	없음	제11조	- 판단 기준 조항 신설 (법 제15조제3항)
9	개인정보 처리업무의 위탁에 관한 사항	해당 시	있음	제7조	
10	개인정보의 국외 수집 및 이전에 관한 사항	해당 시	분문에만	제8조	- 위탁 조항에서 나눠 제8조로 신설 (법 제28조의8)

개인정보처리방침 | 기재사항 점검 | 개정 안내(안)

작성지침 기재사항별 원문 기재 여부 · 해당 조항

02 개인정보 처리방침 개정(안)



■ 개인정보처리방침 개정(안)

개정전	개정 후	비고
제 1 조(개인정보의 수집 및 이용목적) 회사는 ~~아용자의 동의를 받아~~ 다음의 목적을 위하여 개인정보를 수집합니다. ~~회사가 수집하는 모든 개인정보는 동의를 기반으로 합니다.~~	제 1 조(개인정보 이용목적과 수집항목 및 방법) ① 회사는 서비스 이용에 필요한 최소한의 개인정보만을 다음과 같은 법적 근거로 처리합니다. 1. 정보주체의 동의를 받지 않고 처리하는 개인정보 항목 — 「개인정보 보호법」 제15조제1항제4호 (계약 체결·이행) 처리 목적 / 처리 항목 / 보유 및 이용기간 회원가입 및 회원정보 관리 / 이름, 성별, 생년월일, 휴대전화번호, 이메일 주소 / 회원 탈퇴 시까지 본인 인증 / 이름, 생년월일, 휴대전화번호, CI · DI / 회원 탈퇴 시까지 서비스 예약 / 이름, 생년월일, 휴대전화번호, 예약 정보 / 예약 신청일로부터 5년	- 처리 근거를 동의 없이 처리 (계약 이행) · 동의 받아 처리로 나눠 기재 (「개인정보 보호법」 제15조) - 처리방침 앞의 동의서 요약표는 처리방침에서 분리
(신설)	제 8 조(개인정보의 국외 이전에 관한 사항) 회사는 서비스 제공을 위해 다음과 같이 개인정보를 국외로 이전하고 있습니다. 이전받는 자 / 이전 국가 / 이전 일시·방법 / 이전 항목 / 보유 기간 (클라우드 사업자) / 미국 / 서비스 이용 시 네트워크 / 접속 기록, 기기 정보 / 위탁 계약 종료 시까지	- 위탁 조항에서 나눠 신설 (「개인정보 보호법」 제28조의8, 작성지침 기재사항 10)

개인정보처리방침 | 기재사항 점검 | 개정 안내(안)

개정 전 · 개정 후 대조와 조항별 근거

03 개인정보 처리 화면 현황 점검



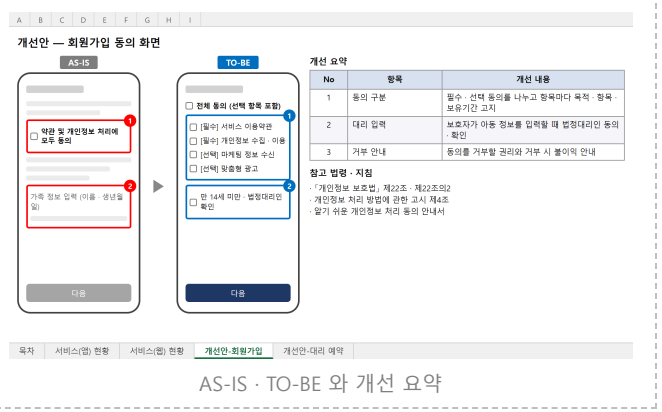
서비스(앱) 현황

항목	개인정보 처리항목	체크리스트	준수 여부	개선안	근거	우선순위
회원가입	이름, 생년월일, 휴대전화번호, 이메일	필수 · 선택 동의를 나눠 받는가	N	필수 · 선택 동의 분리, 전체 동의는 선택 항목까지 펼쳐 보이기	법 제22조제1항	상
		수집 항목 · 목적 · 보유기간을 알리는가	△	동의 화면에 보유 기간 추가	법 제15조제2항	중
대리 예약	가족 · 지인의 이름, 생년월일, 휴대전화번호	만 14세 미만 정보 입력 시 법정대리인 확인	N	보호자 입력 안내 · 법정대리인 확인 절차 추가	법 제22조의2	상
앱 권한	위치, 카메라, 알림	필수 · 선택 권한을 나눠 안내하는가	△	선택 권한은 사용 시점에 안내	정보통신망법 제22조의2	중
마케팅 수신	휴대전화번호, 이메일	광고성 정보 수신 동의를 따로 받는가	Y	-	정보통신망법 제50조	-
하단 링크	-	처리방침 링크를 굵게 · 다른 색으로	Y	-	작성지침 II-3	-

목차 | 서비스(앱) 현황 | 서비스(웹) 현황 | 개선안-회원가입 | 개선안-대리 예약

화면별 체크리스트 · 준수 여부 · 우선순위

04 개인정보 처리 화면 개선(안)



개선안 — 회원가입 동의 화면

AS-IS

약관 및 개인정보 처리에 모두 동의

가족 정보 입력 (이름 · 생년월일)

다음

TO-BE

전체 동의 (선택 항목 포함)

[필수] 서비스 이용약관

[필수] 개인정보 수집 · 이용

[선택] 마케팅 정보 수신

[선택] 맞춤형 광고

만 14세 미만 · 법정대리인 확인

다음

개선 요약

No	항목	개선 내용
1	동의 구분	필수 · 선택 동의를 나누고 항목마다 목적 · 항목 · 보유기간 고지
2	대리 입력	보호자가 아동 정보를 입력할 때 법정대리인 동의 · 확인
3	거부 안내	동의를 거부할 권리와 거부 시 불이익 안내

참고 법령 · 지침
· 「개인정보 보호법」 제22조 · 제22조의2
· 개인정보 처리 방법에 관한 고시 제4조
· 알기 쉬운 개인정보 처리 동의 안내서

목차 | 서비스(앱) 현황 | 서비스(웹) 현황 | 개선안-회원가입 | 개선안-대리 예약

AS-IS · TO-BE 와 개선 요약

아이시큐어 · ISMS-P 인증 컨설팅 업무 경험

정보보호 운영관리

ISMS 인증 기업 월간 운영관리

기간
2026.09 ~ 재직중

역할
아이시큐어 정보보안 컨설턴트

대상
ISMS 인증 이커머스 기업 5곳

방식
월 1회 방문 점검 · 문서 작성

1. 자료 수집 관리자 로그 · 보안장비 월간 보고서 요청 및 수령

2. 로그 검토 관리자 로그인 · 대량 조회 · 접속 IP 변동 · 건수 급증 도출

3. 방문 점검 파일서버 로그 · 계정, 관리자 비밀번호 변경 등 현장 확인

4. 문서 작성 점검대장 · 로그 검토 보고서 작성, 고객사 회신 사유 반영

5. 사후관리 ISMS 심사 결함 보완조치 내역서 · 증적 정리 지원

운영관리 항목

관리자 로그 검토
서버 · DB

월간 특이사항 보고서 작성
서버 · DB · 관리자 권한

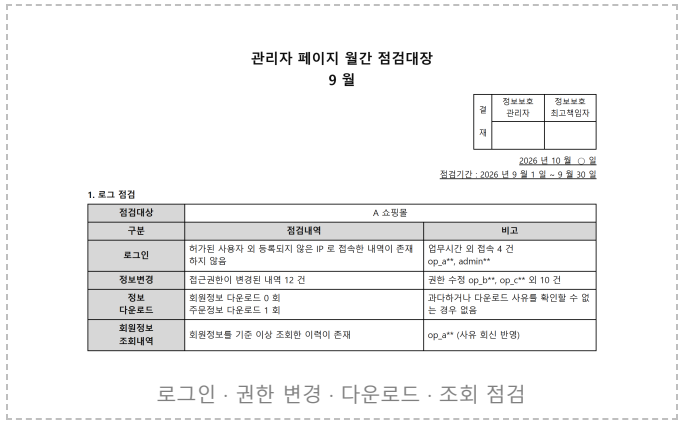
솔루션 월간 보고서 작성
방화벽 · DLP · 백신

운영 자동화
직접 개발

결과 및 산출물

- W 관리자 페이지 월간 점검대장
- W 정보시스템 로그 검토 보고서
- W 보안장비 월간 점검대장 (DLP · 백신)
- X 로그 특이사항 · 사유 요청 목록

01 관리자 페이지 월간 점검대장



관리자 페이지 월간 점검대장
9 월

결재	정보보호 관리자	정보보호 최고책임자

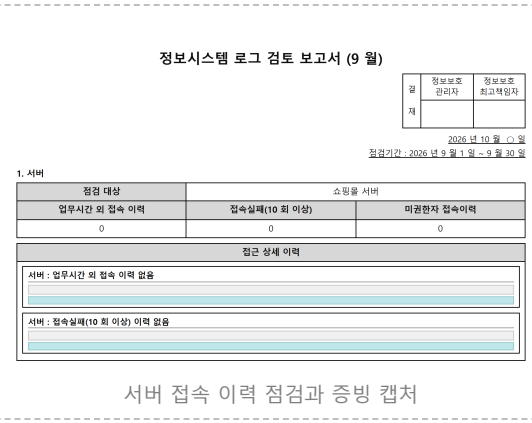
2026 년 10 월 ○ 일
점검기간 : 2026 년 9 월 1 일 ~ 9 월 30 일

1. 로그 점검

점검대상	A 쇼핑몰	
구분	점검내역	비고
로그인	허가된 사용자 외 등록되지 않은 IP 로 접속한 내역이 존재하지 않음	업무시간 외 접속 4 건 op_a**, admin**
정보변경	접근권한이 변경된 내역 12 건	권한 수정 op_b**, op_c** 외 10 건
정보 다운로드	회원정보 다운로드 0 회 주문정보 다운로드 1 회	과다하거나 다운로드 사유를 확인할 수 없는 경우 없음
회원정보 조회내역	회원정보를 기준 이상 조회한 이력이 존재	op_a** (사유 회신 반영)

로그인 · 권한 변경 · 다운로드 · 조회 점검

02 정보시스템 로그 검토 보고서



정보시스템 로그 검토 보고서 (9 월)

결재	정보보호 관리자	정보보호 최고책임자

2026 년 10 월 ○ 일
점검기간 : 2026 년 9 월 1 일 ~ 9 월 30 일

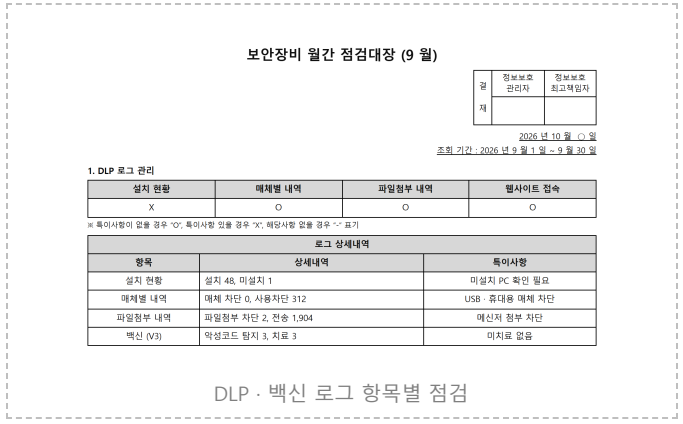
1. 서버

점검 대상	쇼핑몰 서버	
업무시간 외 접속 이력	접속실패(10 회 이상)	미권한자 접속이력
0	0	0

접근 상세 이력
서버 : 업무시간 외 접속 이력 없음
서버 : 접속실패(10 회 이상) 이력 없음

서버 접속 이력 점검과 증빙 캡처

03 보안장비 월간 점검대장 (DLP · 백신)



보안장비 월간 점검대장 (9 월)

결재	정보보호 관리자	정보보호 최고책임자

2026 년 10 월 ○ 일
조회 기간 : 2026 년 9 월 1 일 ~ 9 월 30 일

1. DLP 로그 관리

설치 현황	매체별 내역	파일첨부 내역	웹사이트 접속
X	O	O	O

※ 특이사항이 없을 경우 "O", 특이사항 있을 경우 "X", 해당사항 없을 경우 "-" 표기

로그 상세내역		
항목	상세내역	특이사항
설치 현황	설치 48, 미설치 1	미설치 PC 확인 필요
매체별 내역	매체 차단 0, 사용차단 312	USB · 휴대용 매체 차단
파일첨부 내역	파일첨부 차단 2, 전송 1,904	메신저 첨부 차단
백신 (V3)	악성코드 탐지 3, 치료 3	미치료 없음

DLP · 백신 로그 항목별 점검

04 로그 특이사항 · 사유 요청 목록



구분	해당 건수
업무시간외 · 외부IP 로그인	6
과다한 회원조회	2
과다한 주문조회	0
회원 다운로드	0
외주계정 IP 불일치	1

판단기준
* 주말, 공휴일, 평일 새벽시간(00시 ~ 6시)
* 기준 건수 이상 조회
* 다운로드 사유 확인 불가
* 외주 계정이 등록된 IP 가 아닌 곳에서 접속

일시	계정	접속 IP	구분	고객사 회신 사유
2026-09-06 (토) 10:12	op_a**	112.***.***.20	업무시간 외 로그인	주말 이벤트 운영 대응
2026-09-14 (월) 21:40	admin**	211.***.***.7	업무시간 외 로그인	배송 오류 긴급 처리
2026-09-17 (수) 15:03	op_b**	175.***.***.88	과다한 회원조회	CS 문의 일괄 확인
2026-09-22 (월) 02:16	dev_c**	58.***.***.143	외주계정 IP 불일치	외주 작업자 재택 접속 — IP 등록 요청
2026-09-27 (토) 11:30	op_a**	112.***.***.20	업무시간 외 로그인	주말 이벤트 운영 대응

요약 | 업무시간외 로그인 | 과다 조회 | 외주계정 IP

판단기준별 건수와 고객사 회신 사유

아이시큐어 · ISMS 인증 기업 운영관리 업무 경험

ISMS 인증

ISMS 최초 인증 심사 대응

기간
2023.08 ~ 2024.12

역할
개발팀 소속 정보보호담당자

협업
CISO · 인사팀

결과
2024.08 ISMS 최초 인증 취득

1. **자산 식별** 외부 인증 컨설팅 기반 정보자산 내역 정리
2. **갭 분석** 인증 기준 대비 미비사항 도출 및 개선 일정 수립
3. **취약점 개선** 외부 모의해킹 결과 기반 조치
4. **보안장비 운영** NAC · WIPS 모니터링 및 월별 보고서 작성
5. **권한 관리** 개인정보처리 · 정보시스템 권한 검토 및 월별 보고

작업 환경 및 도구

서버 · DB · 개인정보처리시스템 **GCP 클라우드 환경**	인적관리 결재 · 증적 연동 **Flex**
NAC 네트워크 접근제어 **Genian**	WIPS 무선침입방지 **Bluemax**
DLP 정보유출방지 **오피스키퍼**	MDM 단말관리 **Kandji**

결과 및 산출물

- ISMS 인증 심사 증적 자료
- 월별 권한 검토 · 보안장비 점검 보고서

항목	증적 자료	종류	점검내역	완료사항	미비사항
2.2 인적 보안 2.2.1 주요직무자 지정 및 관리	주요시스템 계정 등록/삭제 현황 개인정보취급자 목록	월별	시스템 사용자 변동 내역 보고서	2023.12 이후 월별 변동 사항 내역	완료
2.2 인적 보안 2.2.5 퇴직 및 관리	퇴사 시 계정 삭제 내역	루틴	일반, 관리자 계정 삭제 내역 확인	2023.11 이후 월별 변동 사항 내역	완료
2.5 인증 및 권한 관리 2.5.1 사용자 계정 관리	개인정보처리시스템 접근권한 관리 기준	루틴	사용자 계정 및 권한 신청서 사용자 계정 및 권한 관리대장 정보시스템 및 개인정보처리시스템별 • 접근권한 분류표 • 사용자, 관리자, 개인정보취급자 목록	2024.05 이후 월별 변동 사항 내역	완료
2.5 인증 및 권한 관리 2.5.2 사용자 식별	정보보호서버접근제어시스템 개인정보처리시스템 계정 목록	반기별	정보시스템 및 개인정보처리시스템 • 로그인 화면 • 관리자, 사용자, 개인정보취급자 계정 목록 예외 처리에 대한 승인 내역	2024.03 이후 월별 변동 사항 내역	완료
2.5 인증 및 권한 관리 2.5.3 사용자 인증	정보보호서버접근제어시스템 개인정보처리시스템 로그인 처리 방법	루틴	정보시스템 및 개인정보처리시스템 로그인 화면 로그인 횟수 제한 설정 화면 로그인 실패 메시지 화면 외부 접속 시 절차(외부접속 신청서, 외부접속자 현황 등)	시스템 로그인 과정 캡쳐 외부 접속 신청서 외부 접속자 현황 캡쳐	완료
2.5 인증 및 권한 관리 2.5.4 비밀번호 관리	비밀번호 생성 규칙 설정 계정 안전성 검사 보고서	1회성	정보보호 관리규정	정보보호관리 문서	완료
2.5 인증 및 권한 관리 2.5.5 특수 계정 및 권한 관리	계정 권한 신청 기안 (서버접근제어시스템 / DB접근제어시스템 / 각종SW접근권한)	루틴	특수권한 관련 지침 특수권한 신청·승인 내역 특수권한자 목록 특수권한 검토 내용	특수 권한자 목록 NAC, WIPS 화면 캡쳐	완료

인증심사 증적 요약

코드박스 · ISMS 심사 대응 업무 경험

ISMS-P 인증 컨설팅 프로젝트

가상기업 보안 인증 컨설팅 — 자산 식별 및 위험평가

가상기업 대상 정보자산 식별부터 위험도 산정, 보호대책 수립까지 인증 기준에 맞춰 전 과정을 수행했습니다.

1. **정보자산 식별** 정보자산 분류 및 C·I·A 기준 중요도 등급 산정
2. **현황 및 흐름분석** 운영 현황 분석 및 개인정보흐름도 작성
3. **위험평가** 위험관리 계획 수립 및 중요도 × 위협 × 취약점 위험도 산출
4. **보호대책 선정** DoA 초과 항목 대상 개인정보 보호대책 수립

컨설팅 기준

ISMS 인증 기준 안내서(2023.11) - 관리체계 수립 및 운영 위험 관리 파트 기준

결과 및 산출물

- X 정보자산 식별기준 및 자산목록
- P 서비스 개인정보흐름도
- W 위험관리 계획서
- W 개인정보보호 이행계획서

01 정보자산 식별기준 및 자산목록



자산 목록 및 중요도 평가

(주)라엣하루 | 문서번호 MH-RA-001 | 대외비

※ 파란 글씨 셀은 평가자 입력값이며, 합계·자산중요도·등급명은 수식으로 자동 산출됩니다.

자산 번호	자산 분류	자산명	자산 설명	소유 부서	관리자 (직무)	위치 / 구성	개인정보 포함여부
A-01	데이터베이스	MEMBER DB	회원 식별정보, 인증정보, 본인확인 결과(CI/DI) 저장	서비스운영팀	DBA	AWS RDS (ap-northeast-2)	포함
A-02	데이터베이스	ORDER DB	주문·결제·환불 정보 및 비회원 주문정보 저장	커머스운영팀	DBA	AWS RDS (ap-northeast-2)	포함
A-03	데이터베이스	DORMANT DB	장기 미이용자 분리보관 데이터베이스	서비스운영팀	DBA	AWS RDS (별도 인스턴스)	포함
A-04	데이터베이스	CONTENT DB	리뷰·문의 게시판 게시물 저장	커머스운영팀	DBA	AWS RDS	포함
A-05	데이터베이스	EVENT DB	이벤트 응모자 및 경품 당첨자 정보 저장	마케팅팀	DBA	AWS RDS	포함
A-06	스토리지	S3 첨부파일 스토리지	게시판 첨부 이미지 및 상품 이미지 저장	커머스운영팀	인프라 담당	AWS S3	포함
A-07	애플리케이션	자사몰 웹 애플리케이션	PC·모바일 웹 쇼핑몰 서비스	서비스운영팀	개발팀장	AWS EC2 (Auto Scaling)	포함
A-08	애플리케이션	모바일 앱 (iOS/Android)	자체 개발 쇼핑몰 앱	서비스운영팀	개발팀장	앱스토어 배포	포함
A-09	애플리케이션	관리자 백오피스	회원·주문·상품 관리용 내부 관리자 시스템	서비스운영팀	개발팀장	AWS EC2	포함

식별 자산 분류 및 중요도(C·I·A) 등급

02 서비스 개인정보흐름표



개인정보 흐름표

(주)라엣하루 | 문서번호 MH-PA-001 | 대외비

※ 처리단계(수집 → 보유·이용 → 제공·위탁 → 파기) 순으로 열이 구성되어 있습니다.

연번	업무 대분류	세부 업무	정보주체 유형	수집 항목 (필수)	수집 항목 (선택)	고유식별정보 / 민감정보 여부	수집 경로	수집·이용의 법적 근거	동의 분리
1	회원관리	회원가입	회원	이름, 아이디, 비밀번호, 휴대전화번호, 이메일 주소	-	해당없음	웹 회원가입 화면	정보주체 동의 (개인정보보호법 제15조제1항제1호)	필수·선택 분리 동의
2	회원관리	간편가입 (소셜 로그인)	회원	소셜 계정 식별자, 이름, 이메일주소	프로필 이미지	해당없음	간편로그인 API 연동 (카카오·네이버)	정보주체 동의 (개인정보보호법 제15조)	필수 동의
3	회원관리	본인확인	회원, 비회원	이름, 생년월일, 성별, 내·외국인 구분, 휴대전화번호, CI/DI	-	고유식별정보 대체 수단 (CI/DI)	본인확인기관 연계 (PASS)	정보통신망법 제23조의3 (본인확인기관 지정)	필수 동의
4	회원관리	만 14세 미만 아동 확인	회원	생년월일	-	해당없음	웹 회원가입 화면	개인정보보호법 제22조의2 (아동의 개인정보 보호)	-
5	회원관리	장기 미이용자 관리	회원	회원 식별정보 일체	-	해당없음	내부 시스템 자동 전환 (서면 취합 X)	내부 정책 및 이용약관	-
6	회원관리	회원 탈퇴 처리	회원	탈퇴 사유, 회원 식별정보(휴대전화번호)	-	해당없음	마이페이지 탈퇴 화면	정보주체 동의	-
7	주문·결제	주문 접수	회원, 비회원	주문자 성명, 연락처, 주소, 주문내역, 결제수단	배송 요청사항	해당없음	웹 앱 주문서 화면	계약의 이행 (개인정보보호법 제15조제3항제4호)	동의 필요 (계약 이행)

수집·이용·제공·보관·파기 단계별 흐름

03 위험관리 계획서



위험처리계획 (DoA 초과 위험 대상)

(주)라엣하루 | DoA = 35점 초과 위험 20건에 대한 대응계획

※ 예상 잔여위험 = 자산중요도 × 위협 발생가능성 × 조치 후 취약점 상각도 (조치 효과 반영)

연번	위협 번호	위협 요약	현재 위험도	위협 등급	개선과제명	세부 조치 내용	조치 유형	담당 부서	목표 시점
1	R-01	법적 근거 없는 고유식별정보 수집으로 인한 행정처분 및 과징금 부과	80	매우높음	경품 응모 프로세스 개인정보 수집 사항 분리	응모 단계에서 주민등록번호 입력 항목을 삭제하고, 당첨 확정 후 재세금과금 대상자에 한해 별도 라인에서 수집하도록 프로세스를 재설계한다. 가수집된 마케팅과 주민등록번호는 즉시 파기하고 파기 확인서를 작성한다.	관리적/기술적	마케팅팀	1분기
2	R-02	면강정보의 근거 없는 수집으로 인한 법률 위반 및 정보주체 권리 침해	60	매우높음	채용 지원서 면접정보 수집 항목 점검	정책·보호 미부 수집 항목을 지원서에서 제거한다. 법정 의무 고용 확인 등 수집이 불가피한 경우 별도 동의 화면을 분리 구현하고 수집 근거를 내부 규정에 명문화한다. 가수집 데이터는 파기한다.	관리적	인사팀	1분기
3	R-03	국외 이전 고지 등의 미이행으로 인한 시정명령 및 과징금 부과	60	매우높음	맞춤 SaaS 국외이전 절차 정비	국외 이전에 관한 고지·동의 화면을 신설하고, 개인정보처리방침에 이전 국가·시기·방법·수탁자·이전 정목 보호조치를 기재한다. 수탁사와 국외이전 관련 조항을 포함한 계약서를 재체결한다.	관리적	CS팀	1분기
4	R-12	관리자 계정 탈취를 통한 대량 개인정보 유출	80	매우높음	관리자 백오피스 접근통제 강화	관리자 페이지를 VPN 내부망에서만 접근 가능하도록 전환하고, 허용 IP 대역을 화이트리스트로 관리한다. 관리자 계정 전체에 다중인증(MFA)을 의무 적용한다.	기술적	정보보안팀	1분기
5	R-14	클라우드 최상위 권한 탈취로 인한 인프라 전체 장악	75	매우높음	클라우드 권한 체계 재정비	루트 계정에 MFA를 적용하고 일상 운영에서 사용을 금지한다. IAM 정책을 직무별 최소권한으로 재설계하고 분기 1회 권한 검토 프로세스를 수립한다.	기술적/관리적	정보보안팀	1분기
6	R-06	만 14세 미만 아동의 법정대리인 동의 없는 가입 절차	60	매우높음	만 14세 미만 아동 가입 차단 로직 개선	본인확인 결과의 생년월일과 가입 입력값을 교차검증하는 로직을 구현하고, 만 14세 미만 판별 시 가입을 차단한다. 기가입 아동 계정을 전수 조사하여 조치한다.	기술적	서비스운영팀	2분기
7	R-15	개발자의 운영 DB 직접 접근을 통한 개인정보 유출	60	매우높음	운영 DB 접근 절차 정비	개발자의 운영 DB 상시 접근 권한을 회수하고, 장애 대응 시 사전 신청·승인 후 한시적으로 부여하는 절차를 수립한다. 접근 종료 시 자동 회수되도록 설정한다.	관리적/기술적	정보보안팀	2분기

위험도 산출 및 DoA 초과 항목 도출

04 개인정보보호 이행계획서



인증 취득 이행 로드맵

(주)라엣하루 | 12개월 기준 | ● 조치 수행 / ◇ 준비·설계

※ 1순위 과제는 법정 위반에 직결되어 인증 신청 전 반드시 조치가 완료되어야 합니다.

과제 번호	개선과제명	관련 인증기준	관련 위험	담당 부서	1Q	2Q	3Q	4Q	핵심 산출물 (증적)
G-01	경품 응모 주민등록번호 수집 시점 분리	3.1.3	R-01	마케팅팀	●				변경된 응모 화면, 기수집 데이터 파기 확인서, 수집 근거 검토서
G-02	채용 지원서 면접정보 수집 항목 정비	3.1.4	R-02	인사팀	●				변경된 지원서, 별도 동의 화면, 수집 근거 내부규정
G-03	국외이전 고지·동의 절차 및 계약 정비	3.3.4	R-03	CS팀	●				고지·동의 화면, 개정된 처리방침, 재체결 계약서
G-04	관리자 백오피스 접근통제 강화 (내부망 전환·MFA)	2.5.3, 2.6.6	R-12	정보보안팀	●				접근 제한 설정 내역, MFA 적용 화면, 접속 로그
G-05	법적 요구사항 목록 작성 및 준수 검토 체계 수립	1.4.1		개인정보보호팀	●				법적 요구사항 목록, 준수 검토 결과서, 구매안전서비스 가입 증빙, 의무대상 판단 근거
G-34	앱 접근권한 고지·동의 체계 정비	3.2.3		개발팀	●	●			접근권한 고지 화면, 권한 항목·목적 정의서, 철회 안내 화면
G-35	인증 범위 및 보호구역 재정의	1.1.4, 2.4.1		정보보안팀	●				범위 정의서, 사업장별 차단 목록, 보호구역 지정 문서, 물류센터 배치도
G-06	클라우드 권한 체계 재정비 (루트 MFA·최소권한)	2.5.5, 2.10.2	R-14	정보보안팀	●				IAM 정책, 권한 매트릭스, 특수계정 목록
G-07	보유기간 경과 개인정보 파기 체계 개선	3.4.1	R-16	커머스운영팀	●				파기 배치 로그, 파기 대장, 검증 결과

우선순위별 대응 방안 및 이행 계획

ISMS-P 인증 컨설팅 프로젝트

가상기업 보안 인증 컨설팅 — 개인정보 처리 정책 수립

개인정보 생명주기 전 단계에 적용할 내부 처리 기준을 문서화하고, 처리 유형별 준수 사항을 정리했습니다.

1. **내부 관리 계획 수립** 보호책임자 지정, 취급자 권한 관리, 교육·점검 주기 정의
2. **민감·고유식별정보 기준** 별도 동의 및 암호화·접근통제 등 안전성 확보조치 정리
3. **가명정보 처리 절차** 가명처리·결합·활용·파기 단계별 요건과 금지사항 정의

컨설팅 기준

ISMS 인증 기준 안내서(2023.11) - 개인정보 처리 단계별 요구사항 기준

결과 및 산출물

- 개인정보 내부 관리 계획 지침서
- 민감·고유식별정보 처리 안내서
- 가명정보 처리 안내서

01 개인정보 내부 관리 계획 지침서



개인정보 내부 관리계획 지침서

(주)마켓하루 | 문서번호(안) MH-PP-001 | 대외비 | 개인정보보호법 제29조 · 안전성 확보조치 기준 제4조 대응

가상 기업 시나리오 · 시행일 (기입) · 작성 개인정보보호팀 · 승인 개인정보 보호책임자

1. 목적 및 적용 범위

본 지침서는 「개인정보의 안전성 확보조치 기준」 제4조에 따라 (주)마켓하루가 수립·시행하는 내부 관리계획으로, 개인정보 보호 조직의 역할과 책임, 개인정보취급자의 권한 관리, 교육 및 점검의 기준과 주기를 정한다. 적용 범위는 인증 범위인 자사몰 및 앱 서비스 및 이를 지원하는 전 업무이며, 회원 약 52만명·개인정보취급자 34명·수탁사 8개사를 포함한다.

2025년 10월 31일 시행된 개정 고시(보호위 고시 제2025-9호)로 내부 관리계획의 점검 주기·방법을 개인정보처리자가 자율 설정할 수 있게 되었으므로, 본 지침서는 §5에서 마켓하루의 처리 규모와 위험도를 근거로 주기를 명시한다.

2. 개인정보 보호 조직 및 책임

역할	지정 대상	주요 책임	근거
개인정보 보호책임자 (CPO)	CISO 겸직 1명 — 경력 적정성 제한 없음	내부 관리계획 승인, 처리방침 관리, 유출 대응 총괄, 연 1회 이상 대표이사 보고	법 제31조
개인정보보호 실무 책임자	개인정보보호팀장	보호조치(암호·접근통제) 현황점검, 권한 검토 주관, 교육 시행, 점검 결과 취합	고시 제4조
정보보호 실무 책임자	정보보안팀장 (팀원 3명)	접근통제·암호화·접속기록 관리, 취약점 진단, 침해사고 대응	고시 제5·9조
부서별 개인정보 관리자	서비스운영·커머스운영·마케팅·홈쿠션·CS 인사 각 1명	취급자 지정·변경 신청, 부서 보유 개인정보 현황 관리	고시 제4조
개인정보취급자	34명	업무 목적 범위 내 처리, 보안서약, 연 2회 교육 이수	법 제28조
수탁사 관리 담당	위탁 업무 소관 부서 (수탁 8개사)	위탁계약 문서화, 연 1회 이상 교육·점검, 점검 결과 보고	법 제26조

3. 개인정보취급자 권한 관리 기준

구분	기준	주기 / 기한	증적
권한 부여	직무 기반 최소권한 원칙. 개인정보처리시스템별 접근권한 분류표에 정의된 역할만 부여하며, 다운로드·일괄조회 권한은 별도 승인	신청·승인 시	사용자 계정 및 권한 신청서
권한 변경·말소	인사이동·직무변경 원칙 발생 시 5영업일 이내 회수. 퇴직은 인사팀 통보 즉시 계정 잠금	수시	권한 변경 내역, 퇴직자 계정 삭제 확인서
권한 검토	부여 현황과 실제 직무의 일치 여부를 개인정보보호팀·소관 부서 합동 검토. 불일치 항목은 즉시 조정	반기 1회 이상	권한 검토 결과서, 조정 내역
특수 권한 관리	AWS 루트 계정·IAM 관리자·DB 직접 접근 등은 별도 대장 관리, 다중인증(MFA) 의무 적용, 상시 부여 금지	분기 1회 점검	특수 권한자 목록, MFA 적용 화면
기록 보관	권한 부여·변경·말소 기록을 최소 3년 보관	3년	권한 관리대장
계정 인증	비밀번호 복잡도·변경 주기 적용, 외부망에서의 관리자 접근은 VPN 및 MFA 경유	상시	인증 설정 화면

4. 교육 계획

대상	과정	주기	시간	증적
전 임직원 (82명)	개인정보보호 및 정보보호 일반	연 1회	2시간	교육 계획서, 참석자 명부, 이수 현황
개인정보취급자 (34명)	처리 단계별 준수사항, 권한·접속기록, 유출 대응	연 2회	각 2시간	교육 자료, 이해도 평가 결과
개인정보 보호책임자·실무 책임자	법령 개정 동향, 관리체계 운영	연 1회	4시간 (외부)	수료증
신규 입사자·직무 변경자	개인정보보호 기본, 보안서약서 징구	입사·변경 후 30일 이내	1시간	서약서, 이수 기록
수탁사 (8개사)	위탁 업무 법위 내 보호조치, 재위탁 금지	연 1회	1시간	교육 시행 확인서

5. 점검 계획

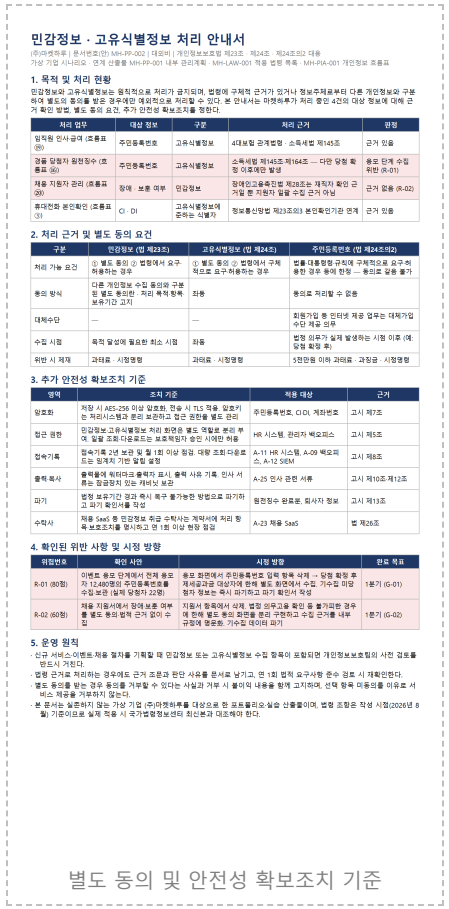
점검 항목	주기	주관	산출물
내부 관리계획 이행 여부 점검	연 1회 이상	개인정보보호팀	내부 관리계획 이행점검 결과서
개인정보처리시스템 접속기록 점검 (5만명 이상 처리 → 2년 보관 대상)	월 1회 이상	정보보안팀	접속기록 점검 결과서
개인정보취급자 권한 검토	반기 1회 이상	개인정보보호팀 · 소관 부서	권한 검토 결과서
수탁사 관리·감독 점검	연 1회 이상	위탁 소관 부서	수탁사 점검 결과보고서
기술적 취약점 진단	연 1회 이상 · 중요 변경 시 수시	정보보안팀	취약점 진단 결과 보고서
법적 요구사항 준수 검토	연 1회 이상	개인정보보호팀	법령 준수 검토 결과서
점검 결과 경영진 정보보호위원회 보고	반기 1회	개인정보 보호책임자	위원회 회의록

6. 문서 관리

- 본 지침서는 연 1회 이상 및 조직·법령·시스템의 중요 변경 발생 시 검토하여 개정하고, 개정 시 개인정보 보호책임자의 승인을 받는다.
- 개정 이력은 문서 말미에 기록하며, 이행 점검 결과와 함께 인증 심사 증적으로 보관한다.
- 연계 산출물: MH-PP-002 민감·고유식별정보 처리 안내서, MH-PP-003 가명정보 처리 안내서, MH-LAW-001 적용 법령 목록.

보호책임자·취급자 권한 및 교육·점검 기준

02 민감·고유식별정보 처리 안내서



민감정보 · 고유식별정보 처리 안내서

(주)마켓하루 | 문서번호(안) MH-PP-002 | 대외비 | 개인정보보호법 제23조 · 제24조 · 제24조의2 대응

가상 기업 시나리오 · 연계 산출물 MH-PP-001 내부 관리계획 · MH-LAW-001 적용 법령 목록 · MH-PIA-001 개인정보 흐름표

1. 목적 및 처리 현황

민감정보와 고유식별정보는 원칙적으로 처리가 금지되며, 법령에 구체적 근거가 있거나 정보주체로부터 다른 개인정보와 구분하여 별도의 동의를 받은 경우에만 예외적으로 처리할 수 있다. 본 안내서는 마켓하루가 처리 중인 4건의 대상 정보에 대해 근거 확인 방법, 별도 동의 요건, 추가 안전성 확보조치를 정한다.

처리 업무	대상 정보	구분	처리 근거	관점
임직원 인사·급여 (조흡표 08)	주민등록번호	고유식별정보	4대보험 관계법령 · 소득세법 제145조	근거 있음
경품 당첨자 원천징수 (조흡표 06)	주민등록번호	고유식별정보	소득세법 제145조·제164조 — 다만 당첨 확정 이후에만 발생	옵트 단계 수집 위반 (R-01)
채용 지원자 관리 (조흡표 09)	장애 · 보훈 여부	민감정보	장애인고용촉진법 제28조는 채직자 확인 근거일 뿐 지원자 일괄 수집 근거 아님	근거 없음 (R-02)
휴대전화 본인확인 (조흡표 03)	CI · DI	고유식별정보에 준하는 식별자	정보통신망법 제23조의3 본인확인기관 연계	근거 있음

2. 처리 근거 및 별도 동의 요건

구분	민감정보 (법 제23조)	고유식별정보 (법 제24조의)	주민등록번호 (법 제24조의2)
처리 가능 요건	① 별도 동의 ② 법령에서 요구·허용하는 경우	① 별도 동의 ② 법령에서 구체적으로 요구·허용하는 경우	법률·대통령령·규칙에 구체적으로 요구·허용한 경우 등에 한정 — 동의로 갈음 불가
동의 방식	다른 개인정보 수집 동의와 구분된 별도 동의만 · 처리 목적 항목 보유기간 고지	좌동	동의로 처리할 수 없음
대체수단	—	—	회원가입 등 인터넷 제공 업무는 대체가입 수단 제공 의무
수집 시점	목적 달성에 필요한 최소 시점	좌동	법정 의무가 실제 발생하는 시점 이후 (예: 당첨 확정 후)
위반 시 제재	과태료 · 시정명령	과태료 · 시정명령	5천만원 이하 과태료 · 과징금 · 시정명령

3. 추가 안전성 확보조치 기준

영역	조치 기준	적용 대상	근거
암호화	저장 시 AES-256 이상 암호화, 전송 시 TLS 적용. 암호키는 처리시스템과 분리 보관하고 접근 권한을 별도 관리	주민등록번호, CI·DI, 계좌번호	고시 제7조
접근 권한	민감정보·고유식별정보 처리 화면은 별도 역할로 분리 부여. 일괄 조회·다운로드는 보호책임자 승인 시에만 허용	HR 시스템, 관리자 백오피스	고시 제5조
접속기록	접속기록 2년 보관 및 월 1회 이상 점검. 대량 조회·다운로드는 즉시적 기반 알림 설정	A-11 HR 시스템, A-09 백오피스, A-12 SIEM	고시 제8조
출력·복사	출력물에 워터마크·출력자 표시. 출력 사유 기록. 인사 서류는 잠금장치 있는 캐비닛 보관	A-25 인사 관련 서류	고시 제10조·제12조
파기	법정 보유기간 경과 후 지체 없이 복구·재생이 불가능한 방법으로 파기하고 파기 확인서를 작성	원천징수 완료분, 회사가 정보	고시 제13조
수탁사	재위 SaaS 등 민감정보 취급 수탁사는 계약서에 처리 항목 보호조치를 명시하고 연 1회 이상 현장 점검	A-23 채용 SaaS	법 제26조

4. 확인된 위반 사항 및 시정 방향

위험번호	확인 사안	시정 방향	완료 목표
R-01 (80점)	이벤트 응모 단계에서 전체 응모자 12,480명의 주민등록번호를 수집·보관 (실제 당첨자 22명)	응모 화면에서 주민등록번호 입력 항목 삭제 → 당첨 확정 후 제세공과금 대상자에 한해 별도 화면에서 수집. 기수집 미당첨자 정보 즉시 파기하고 파기 확인서 작성	1분기 (G-01)
R-02 (60점)	채용 지원서에서 장애·보훈 여부를 별도 동의 없이 수집	지원서 항목에서 삭제. 법정 의무고용 확인 등 불가피한 경우에 한해 별도 동의 화면을 분리 구현하고 수집 근거를 내부 규정에 명문화. 기수집 데이터 파기	1분기 (G-02)

5. 운영 원칙

- 신규 서비스·이벤트·채용 절차를 기획할 때 민감정보 또는 고유식별정보 수집 항목이 포함되면 개인정보보호팀의 사전 검토를 받는다.
- 법령 근거로 처리하는 경우에도 근거 조문과 판단 사유를 문서로 남기고, 연 1회 법적 요구사항 준수 점검 시 재확인한다.
- 별도 동의를 받는 경우 동의를 거부할 수 있다는 사실과 거부 시 불이익 내용을 항목 고지하여, 선택 항목 미동의를 이유로 서비스 제공을 거부하지 않는다.
- 본 문서는 실존하지 않는 가상 기업 (주)마켓하루를 대상으로 한 포트폴리오·실습 산출물이며, 법령 조항은 작성 시점(2026년 8월) 기준이므로 실제 적용 시 국가법령정보센터 최신본과 대조해야 한다.

별도 동의 및 안전성 확보조치 기준

03 가명정보 처리 안내서



가명정보 처리 안내서

(주)마켓하루 | 문서번호(안) MH-PP-003 | 대외비 | 개인정보보호법 제28조의2 · 제28조의7 대응

가상 기업 시나리오 · 대상 업무 개인정보 흐름표 09 가명정보 처리 (데이터분석) · 연계 산출물 MH-PP-001 · MH-PIA-001

1. 목적 및 적용 범위

가명정보는 추가 정보를 사용하지 아니하고는 특정 개인을 알아볼 수 없도록 처리한 정보로, 통계작성·과학적 연구·공익적 기록보존 목적에 한하여 정보주체의 동의 없이 처리할 수 있다. 본 안내서는 마켓하루가 처리 중인 4건의 대상 정보에 대해 근거 확인 방법, 별도 동의 요건, 추가 안전성 확보조치를 정한다.

2026년 개정정보 가이드라인이 위임도 기반 체계로 전면 개정될 예정이므로, 본 안내서의 적정성 검토 기준은 개정 가이드라인 확정 시 재검토 대상이다.

2. 정보 유형별 판단 기준

구분	정의	정의 필요 여부	마켓하루 적용
개인정보	살아 있는 개인을 알아볼 수 있는 정보	목적별 등의 필요	MEMBER DB, ORDER DB 원본
가명정보	추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리한 정보. 여전히 개인정보에 해당	통계작성·과학적 연구·공익적 기록보존 목적에 한해 등의 불요	분석용 구매이력 데이터셋
익명정보	시간·비용·기술을 합리적으로 고려할 때 더 이상 개인을 알아볼 수 없는 정보. 개인정보보호법 미적용	불요	집계 통계 리포트

3. 가명처리 절차

단계	수행 내용	산출물 / 증적
1. 목적 설정	통계작성·과학적 연구·공익적 기록보존 등 어디에 해당하는지 특정하고, 목적 달성에 필요한 최소 항목만 정의한다. 마케팅 대상자 선정 등 목적 외 활용은 불가	가명처리 목적 검토서
2. 사전 준비	대상 데이터셋의 식별자·준식별자·민감 항목을 분류하고 재식별 위험 요소를 사전 점검한다	항목 분류표, 위험 요소 목록
3. 가명처리	식별자는 삭제 또는 일방향 암호화, 준식별자는 범주화·라운딩·마스킹을 적용한다. 추가 정보(매핑 테이블)는 분리 보관하고 접근 권한을 별도 관리한다	가명처리 명세서, 처리 전후 샘플
4. 적정성 검토	처리 결과가 재식별되지 않는지 개인정보보호팀·정보보안팀 합동으로 검토하고 승인한다. 필요 시 외부 전문가를 포함한다	적정성 검토 결과서, 승인 내역
5. 사후 관리	활용 이력·접근 로그를 기록하고, 재식별 가능성 변화 여부를 주기적으로 점검한다	활용 대장, 접속기록 점검 결과

4. 결합 및 안전조치 요건

영역	요건	근거
결합 절차	서로 다른 개인정보처리자 간 가명정보 결합은 보호위원회가 지정한 결합전문기관을 통해서만 수행한다. 자체 결합은 금지	법 제28조의3
반출 승인	결합된 정보의 반출은 전문기관의 반출심사위원회 승인을 받은 후에만 가능하며, 반출 범위를 목적 달성에 필요한 최소로 한정한다	법 제28조의3
추가 정보 분리	가명처리에 사용된 추가 정보(매핑 키)는 원본 및 가명정보와 물리적·논리적으로 분리 저장하고 별도 접근 권한을 부여한다	법 제28조의4
안전조치	가명정보에도 접근통제 암호화·접속기록 보관 등 안전성 확보조치를 동일하게 적용한다	법 제28조의4, 고시
처리 기록 보관	가명정보 처리 목적, 이용·제공 내역, 제3자 제공 시 제공받는 자 등을 기록하여 최소 3년 보관한다	법 제28조의4
처리방침 공개	가명정보 처리 목적과 항목을 개인정보 처리방침에 기재하여 공개한다	법 제30조

5. 금지 사항 및 파기

구분	내용	위반 시
재식별 금지	특정 개인을 알아보기 위한 목적으로 가명정보를 처리하서는 안 된다	법 제28조의5 위반 — 형사처벌 및 과징금 대상
재식별 시 조치	처리 과정에서 특정 개인이 식별되는 정보가 생성된 경우 즉시 처리를 중지하고 회수·파기한다	지체 없는 조치 의무
목적 외 활용 금지	마케팅 대상자 선정, 광고 타겟팅 등 통계·연구·공익적 기록보존 외 목적으로 활용할 수 없다	등의 없는 목적 외 이용
파기	분석 목적 달성 시점 가명정보와 추가 정보를 복구 불가능한 방법으로 파기하고 파기 확인서를 작성한다	고시 제13조

6. 문서 관리

- 가명정보 처리 건별로 §3의 산출물을 확보하고, 안전 심사 및 내부심사 시 증적으로 제출한다.
- 가명정보 가이드라인 개정 시 본 안내서의 적정성 검토 기준과 위험도 평가 방법을 재검토하여 개정한다.
- 본 문서는 실존하지 않는 가상 기업 (주)마켓하루를 대상으로 한 포트폴리오·실습 산출물이며, 법령 조항은 작성 시점(2026년 8월) 기준이므로 실제 적용 시 최신본 대조가 필요하다.

가명처리·결합·파기 단계별 요건

주요정보통신기반시설 기술적 취약점 분석·평가 기반 프로젝트

가상기업 기술적 취약점 진단 — Unix 서버 · 웹 서비스

2026 개정 가이드를 기준으로 Unix 서버와 신설된 웹 서비스 분야를 진단하고, 위험도별 조치 방안까지 도출했습니다.

1. **점검 계획 수립** 대상 자산 식별 및 중요도 기준 점검 범위 · 일정 확정
2. **점검 기준 설계** 2026 개정 항목 반영 체크리스트 및 진단 스크립트 작성
3. **취약점 진단** 계정 · 파일 및 디렉터리 · 서비스 · 패치 · 로그 설정값 점검
4. **결과 분석 및 조치** 위험도 산정 후 조치 방안 도출 및 재점검 확인

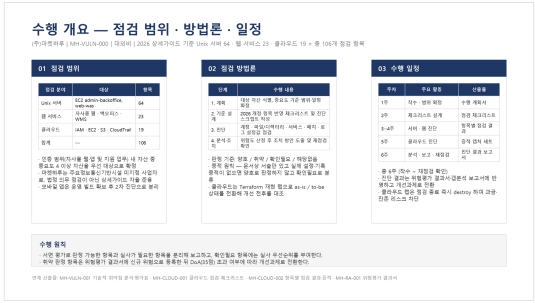
컨설팅 기준

2026 기술적 취약점 분석·평가 상세가이드 - Unix 서버 64개 · 웹 서비스 23개 항목

결과 및 산출물

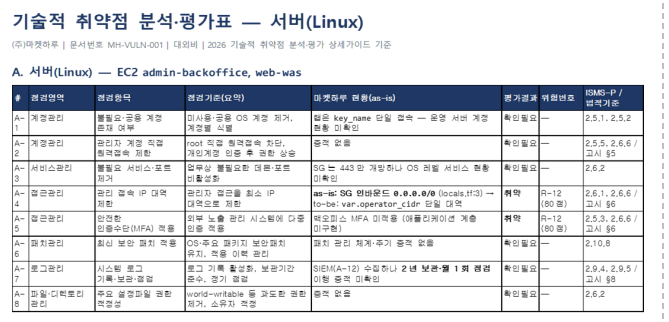
- P 취약점 분석·평가 수행 제안서
- X Unix 서버 점검 체크리스트
- X 웹 서비스 점검 체크리스트
- W 취약점 진단 결과 보고서

01 취약점 분석·평가 수행 제안서


수행 개요 — 점검 범위 · 방법론 · 일정

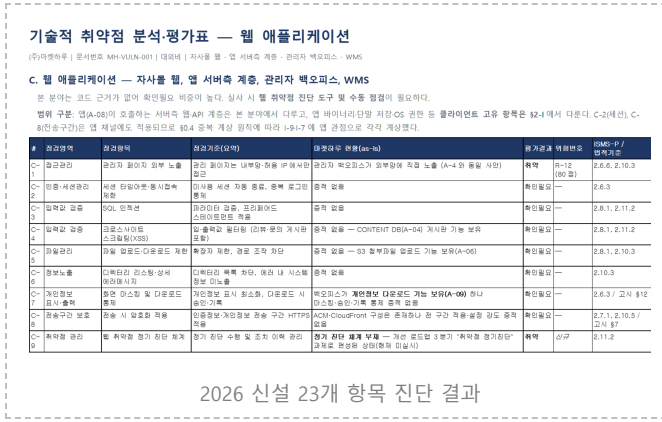
점검 범위 · 방법론 및 수행 일정

02 Unix 서버 점검 체크리스트


기술적 취약점 분석·평가표 — 서버(Linux)

계정 · 파일 · 서비스 · 패치 · 로그 64개 항목

03 웹 서비스 점검 체크리스트


기술적 취약점 분석·평가표 — 웹 애플리케이션

2026 신설 23개 항목 진단 결과

04 취약점 진단 결과 보고서


기술적 취약점 진단 결과 보고서 — 종합 결과

항목별 판정 근거 및 조치 이행계획

주요정보통신기반시설 기술적 취약점 분석·평가 기반 프로젝트

가상기업 기술적 취약점 진단 — 클라우드(AWS) 환경

2026 가이드에 신설된 클라우드 분야 점검 항목을 AWS 환경에 매핑해 진단하고, 설정 개선 방안을 정리했습니다.

1. **클라우드 자산 식별** 계정 · 리전 · 사용 서비스 구성 파악 및 점검 범위 확정
2. **점검 기준 매핑** 가이드 19개 항목을 IAM · EC2 · S3 · CloudTrail 설정에 매핑
3. **설정 점검 수행** 콘솔 · AWS CLI 기반 4개 영역 점검 및 증적 수집
4. **결과 분석 및 개선** 중요도 '상' 7개 항목 우선 조치 및 운영 기준 반영

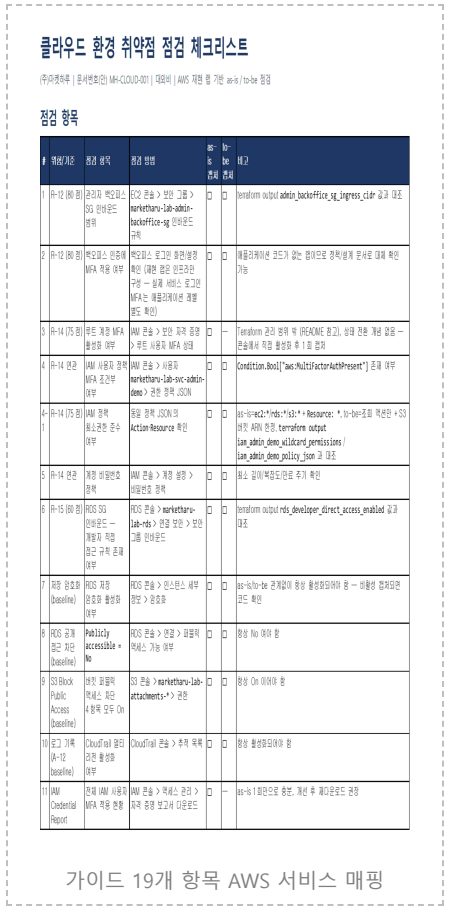
컨설팅 기준

2026 기술적 취약점 분석·평가 상세가이드 - 클라우드 신설 19개 항목 (상 7 / 중·하 12)

결과 및 산출물

- AWS 점검 체크리스트 (19개 항목)
- 점검 항목별 진단 결과 · 증적
- 클라우드 취약점 진단 결과 보고서

01 AWS 점검 체크리스트



클라우드 환경 취약점 점검 체크리스트

(주)어썸하루 | 문서번호(안) MH-CLOUD-001 | 대외비 | AWS 계정 별 기본 as-is / to-be 점검

점검 항목

#	영역/기준	점검 설정	점검 방법	as-is 결과	to-be 결과	비고
1	IA-12 (80 점)	관리자 백업/스냅샷 SG 인바운드 범위	EC2 콘솔 > 보안 그룹 > marketharu-lab-admin-backoffice-sg 인바운드 규칙	☐	☐	terraform output admin_backoffice_sg_ingress_cidr 결과 대조
2	IA-12 (80 점)	백업/스냅샷 인증에 MFA 적용 여부	백업/스냅샷 로그인 정책/설정 확인 (대한 관문 인프라와 구분 — 실제 서비스 로그인 MFA는 계층2에서은 계별 별도 확인)	☐	☐	애플리케이션 코드가 없는 항목이므로 정책/설계 문서로 대체 확인 가능
3	IA-14 (75 점)	루트 계정 MFA 활성화 여부	IAM 콘솔 > 보안 자격 증명 > 루트 사용자 MFA 상태	☐	☐	— Terraform 관리 범위 밖 (README 참고). 상태 전환 계획 없음 — 콘솔에서 직접 활성화 후 1 회 캡처
4	IA-14 연관	IAM 사용자 정책 MFA 조건부 여부	IAM 콘솔 > 사용자 marketharu-lab-svc-admin-demo > 권한 정책 JSON	☐	☐	Condition.Bool["aws:MultiFactorAuthPresent"] 존재 여부
4-1	IA-14 (75 점)	IAM 정책 최소권한 준수 여부	동일 정책 JSON 의 Action·Resource 확인	☐	☐	as-is=ec2:*·rds:*·s3:* + Resource: *, to-be=조회 액션만 + S3 버킷 ARN 한정. terraform output iam_admin_demo_wildcard_permissions / iam_admin_demo_policy_json 과 대조
5	IA-14 연관	계정 비밀번호 정책	IAM 콘솔 > 계정 설정 > 비밀번호 정책	☐	☐	최소 길이/복잡도/만료 주기 확인
6	IA-15 (80 점)	RDS SG 인바운드 — 개발자 직원 접근 규칙 존재 여부	RDS 콘솔 > marketharu-lab-rds > 연결 및 보안 > 보안 그룹 인바운드	☐	☐	terraform output rds_developer_direct_access_enabled 결과 대조
7	재정 검토회 (baseline)	RDS 자격 증명회 활성화 여부	RDS 콘솔 > 인스턴스 세부 정보 > 암호화	☐	☐	as-is/to-be 관계없이 항상 활성화되어야 함 — 비활성 캡처되면 코드 확인
8	RDS 공개 접근 차단 (baseline)	Publicly accessible = No	RDS 콘솔 > 연결 > 퍼블릭 액세스 가능 여부	☐	☐	항상 No 여야 함
9	S3 Block Public Access (baseline)	버킷 퍼블릭 액세스 차단 4 항목 모두 On	S3 콘솔 > marketharu-lab-attachments-* > 권한	☐	☐	항상 On 이어야 함
10	로그 기록 (A-12 (baseline)	CloudTrail 멀티 리전 활성화 여부	CloudTrail 콘솔 > 추적 목록	☐	☐	항상 활성화되어야 함
11	IAM Credential Report	전체 IAM 사용자 MFA 적용 현황	IAM 콘솔 > 액세스 관리 > 아격 증명 보고서 다운로드	☐	—	as-is 1 회만으로 충분. 개선 후 재다운로드 권장

가이드 19개 항목 AWS 서비스 매핑

02 항목별 점검 결과 · 증적



클라우드 항목별 점검 결과 · 증적

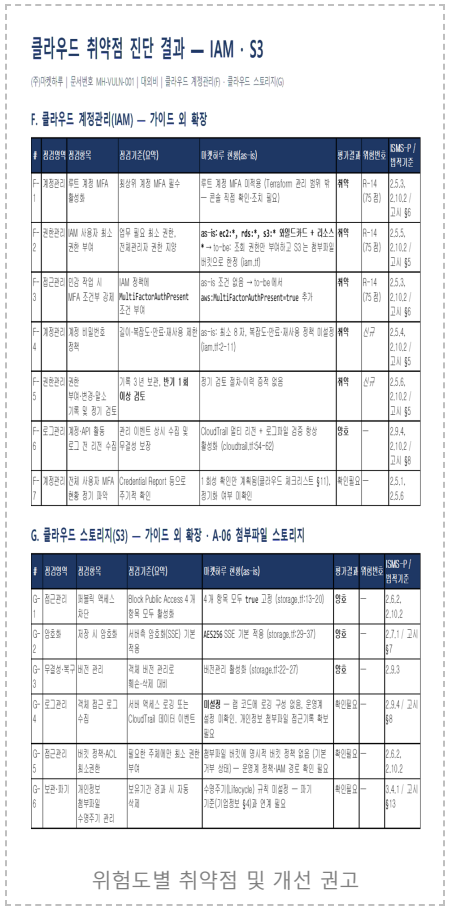
(주)어썸하루 | 문서번호(안) MH-CLOUD-002 | 대외비 | AWS 계정 별(terraform) 기본 as-is / to-be 점검
※ 2026 상세가이드 클라우드 신설 19개 항목 (상 7 / 중·하 12) · 취약 진단 항목 8 · 조치 완료 10 · 가상 조치 1
※ 증적 저장 위치: docs/images/cloud-aws-check/ · 계정별 (라인분리) [accidcloud]_[항목번호]_[영어약칭]_[YYYYMMDD].png

#	점검 영역	점검 항목	위험 / 기준	중요도	as-is 결과	to-be 결과	증적 파일	판정
1	IAM	루트 계정 MFA 활성화 여부	R-14 (75점)	상	미적용 — 가상 MFA 디바이스 없음	가상 MFA 등록 완료	R14_asis/tobe_root_mfa_20260803.png	조치 완료
2	IAM	루트 계정 액세스 키 미사용	R-14 연관	중	액세스 키 없음	동일	R14_asis_root_accesskey_20260803.png	양호
3	IAM	IAM 사용자 정책 MFA 조건부 적용	R-14 연관	중	Condition 절 부재	aws:MultiFactorAuthPresent 조건 추가	R14_asis/tobe_iam_mfa_condition_20260803.png	조치 완료
4	IAM	IAM 정책 최소권한 준수 (와일드카드 금지)	R-14 (75점)	상	ec2:* / rds:* / s3:* + Resource: *	조회 액션 한정 + S3 버킷 ARN 한정	R14_asis/tobe_iam_policy_json_20260803.png	조치 완료
5	IAM	계정 비밀번호 정책	R-14 연관	중	최소 8자, 만료 주기 미설정	최소 12자 · 복잡도 · 90일 만료	R14_asis/tobe_passwordpolicy_20260803.png	조치 완료
6	IAM	Credential Report MFA 적용 현황	고시 제6조	하	사용자 4명 중 2명 미적용	전원 적용	R14_asis/tobe_credential_report_20260803.png	조치 완료
7	IAM	액세스 키 대신 역할 기반 접근 사용	고시 제5조	중	EC2 인스턴스 프로파일 적용	동일	C1D_asis_iam_role_2026080 3.png	양호
8	EC2 · 네트워크	관리자 백오피스 SG 인바운드 범위	R-12 (80점)	상	0.0.0.0/0 전체 개방 (local.tf:3)	var.operator_cidr 단일 대역	R12_asis/tobe_backoffice_sg_inbound_20260803.png	조치 완료
9	EC2 · 네트워크	백오피스 접근 경로 및 MFA 적용	R-12 (80점)	상	외부망 직접 노출 MFA 미적용	VPN 경유 + MFA (설계 문서 기준)	R12_asis_backoffice_access_20260803.png	부분 조치 — 앱 레벨 확인 필요
10	EC2 · 네트워크	RDS SG 개발자 직접 접근 규칙	R-15 (60점)	상	개발자 대역 3206 처 규칙 존재	규칙 삭제 · 배스천 경유로 전환	R15_asis/tobe_rds_sg_inbound_20260803.png	조치 완료
11	EC2 · 네트워크	보안그룹 설정요 포트 개방 여부	고시 제6조	중	22 / 3389 전체 개방 없음	동일	C1D_asis_sg_ports_20260803.png	양호
12	EC2 · 네트워크	EBS 볼륨 암호화	고시 제7조	중	기본 암호화 활성	동일	C1D_asis_ebs_encryption_20260803.png	양호
13	S3	버킷 퍼블릭 액세스 차단 4항목	baseline	상	4개 항목 모두 On	동일	C1D_asis_s3_bpa_20260803.png	양호
14	S3	버킷 기본 암호화 (SSE)	고시 제7조	중	SSE-S3 적용	동일	C1D_asis_s3_sse_20260803.png	양호
15	S3	버킷 버전 관리 활성화	고시 제13조	하	비활성	활성화	C1D_asis/tobe_s3_versioning_20260803.png	조치 완료
16	S3	버킷 서버 액세스 로깅	고시 제8조	하	미설정	전용 로그 버킷 지정	C1D_asis/tobe_s3_logging_20260803.png	조치 완료
17	RDS	저장 암호화 활성화	고시 제7조	중	활성	동일	C1D_asis_rds_encryption_20260803.png	양호
18	RDS	Publicly accessible = No	고시 제6조	하	No	동일	C1D_asis_rds_public_20260803.png	양호
19	CloudTrail	멀티 리전 추적 활성화 · 로그 파일 검증 여부	A-12 baseline	상	멀티 리전 활성 · 로그 파일 검증 활성	동일	C1D_asis/tobe_cloudtrail_20260803.png	조치 완료

결과 요약
중요도 상 7개 항목 중 6개는 to-be 전환으로 조치 완료. #4액세스 MFA는 재현 캡쳐 매뉴얼에서은 계정이 없어 정책 설계 문서로 대체 확인 — 실서 시 상세 보조치 완료 항목은 terraform apply -var="remediated=true" 전후 콘솔/CLI 화면을 as-is / to-be 쌍으로 캡처하여 대조.
점검 종료 후 terraform destroy 미실행 시 관리자 자격으로은 세션 종료 전 반드시 확인 · 앱레벨 AWS 계정 ID이메일은 모자이크 처리

콘솔 · CLI 점검 결과 캡쳐

03 진단 결과 보고서



클라우드 취약점 진단 결과 — IAM · S3

(주)어썸하루 | 문서번호 MH-VULN-001 | 대외비 | 클라우드 계정관리(F) · 클라우드 스토리지(G)

F. 클라우드 계정관리(IAM) — 가이드 외 확장

#	점검영역	점검항목	점검기준(요약)	매핑내규 편람(as-is)	평가결과	위험반응	ISMS-P / 법적기준
F-1	계정관리	루트 계정 MFA 활성화	필성의 계정 MFA 필수	루트 계정 MFA 미적용 (Terraform 관리 범위 밖 — 콘솔 직접 확인·조치 필요)	취약	R-14 (75 점)	2.5.3, 2.10.2 / 고시 §6
F-2	권한관리	IAM 사용자 최소 권한 부여	업무 필요 최소 권한, 전체관리자 권한 지양	as-is: ec2:*, rds:*, s3:* 와일드카드 + 리소스 * → to-be: 조회 권한만 부여하고 S3 는 첨부파일 버킷으로 한정 (iam.tf)	취약	R-14 (75 점)	2.5.5, 2.10.2 / 고시 §5
F-3	접근관리	인증 적합 시 MFA 조건부 강제	IAM 정책에 MultiFactorAuthPresent 조건 부여	as-is: 조건 없음 → to-be 에서 aws:MultiFactorAuthPresent=true 추가	취약	R-14 (75 점)	2.5.3, 2.10.2 / 고시 §6
F-4	계정관리	계정 비밀번호 정책	길이·복잡도·만료·재사용 제한	as-is: 최소 8 자, 복잡도·만료·재사용 정책 미설정 (iam.tf:2~11)	취약	신규	2.5.4, 2.10.2 / 고시 §5
F-5	권한관리	권한 부여·변경·삭제 기록 및 정기 검토	기록 3 년 보관, 반기 1 회 이상 검토	정기 검토 절차·이력 증적 없음	취약	신규	2.5.6, 2.10.2 / 고시 §5
F-6	로그관리	계정·API 활동 로그 전 리전 수집	관리 이벤트 상시 수집 및 무결성 보장	CloudTrail 멀티 리전 + 로그파일 검증 항상 활성화 (cloudtrail.tf:54~62)	양호	—	2.9.4, 2.10.2 / 고시 §8
F-7	계정관리	전체 사용자 MFA 적용 정기 점검	Credential Report 등으로 주기적 확인	정기 검토 절차·이력 증적 없음	확인필요	—	2.5.1, 2.5.6

G. 클라우드 스토리지(S3) — 가이드 외 확장 · A-06 첨부파일 스토리지

#	점검영역	점검항목	점검기준(요약)	매핑내규 편람(as-is)	평가결과	위험반응	ISMS-P / 법적기준
G-1	접근관리	퍼블릭 액세스 차단	Block Public Access 4 개 항목 모두 활성화	4 개 항목 모두 true 고정 (storage.tf:13~20)	양호	—	2.6.2, 2.10.2
G-2	암호화	저장 시 암호화	서버측 암호화(SSE) 기본 적용	AES256 SSE 기본 적용 (storage.tf:26~27)	양호	—	2.7.1 / 고시 §7
G-3	무결성·복구	버전 관리	객체 버전 관리로 훼손·삭제 대비	버전관리 활성화 (storage.tf:22~27)	양호	—	2.9.3
G-4	로그관리	객체 접근 로그 수집	서버 액세스 로깅 또는 CloudTrail 데이터 이벤트	미설정 — 환 코드에 로깅 구성 없음. 운영계 설정 미확인. 개인정보 첨부파일 접근기록 확보 필요	확인필요	—	2.9.4 / 고시 §8
G-5	접근관리	버킷 정책·ACL 최소권한	필요한 주체에만 최소 권한 부여	첨부파일 버킷에 명시적 버킷 정책 없음 (기본 거부 상태) — 운영계 정책·IAM 권한 확인 필요	확인필요	—	2.6.2, 2.10.2
G-6	보관·파기	개인정보 첨부파일 수명주기 관리	보유기간 경과 시 자동 삭제	수명주기(lifecycle) 규칙 미설정 — 파기 기준(기업정보 §4)과 연계 필요	확인필요	—	3.4.1 / 고시 §13

위험도별 취약점 및 개선 권고

감사합니다

me@inhoolee.com / 010-8075-3280