PULSACORE / PRIVACY MANAGEMENT

펄사코어 개인정보 접속기록 관리시스템

누가, 언제, 어떤 개인정보를 처리했는지 기록하고 위험을 찾아, 조치까지 관리합니다.

접속기록·이상행위·소명·감사와 보안제품 버전·취약점·점검 이행을 연결하는 개인정보 보호 전용 솔루션

개인정보 보호 업무의 전 과정

수집 DB · WAS → **분석** 이상행위 → **조치** 소명 · 점검 → **증빙** 감사 · 보고



기관별 개인정보 보호 관리

관공서 · 공공기관 · 기업 · 교육기관
업무시스템은 유지하고 보호 관리만 통합

개인정보 접속기록 관리 | 독립 제품 구성안

2026.11.24 기준 · 화면은 개발 시안이며, 기존 에이전트 개발 결과를 기반으로 제품화 범위를 정리했습니다.

01 법적 의무와 보관 기준

접속기록은 선택이 아닌 개인정보 안전조치의 핵심입니다

개인정보 보호법과 시행령, 개인정보보호위원회 고시에 따라 개인정보처리자는 접속기록의 저장·점검 및 안전한 보관 등 필요한 조치를 이행해야 합니다.

법 제29조	내부 관리계획, 접속기록 보관 등 기술적·관리적·물리적 안전조치 의무.
시행령 제30조 제1항 제5호	접속일시·처리내역 등을 저장·점검하고 확인·감독하며, 위·변조 방지와 안전한 보관 조치를 이행.
고시 제8조	접속기록 보관, 접속기록 및 개인정보 다운로드 상황 점검, 기록의 위·변조·도난·분실 방지.

1년 이상

일반 보관 기준

정보주체 본인을 제외한 접속자의 접속기록

2년 이상

다음 중 하나에 해당

① 5만 명 이상 정보주체 처리 시스템
② 고유식별정보 또는 민감정보 처리 시스템
③ 등록·신고 기간통신사업자인 개인정보처리자

점검 주기: 기관의 내부 관리계획에 따라 이행

현행 고시 제8조제2항은 점검 주기·방법·사후조치 절차를 정해 이행하도록 규정합니다. 월별 점검·보고는 기관 정책에 따라 설정합니다.

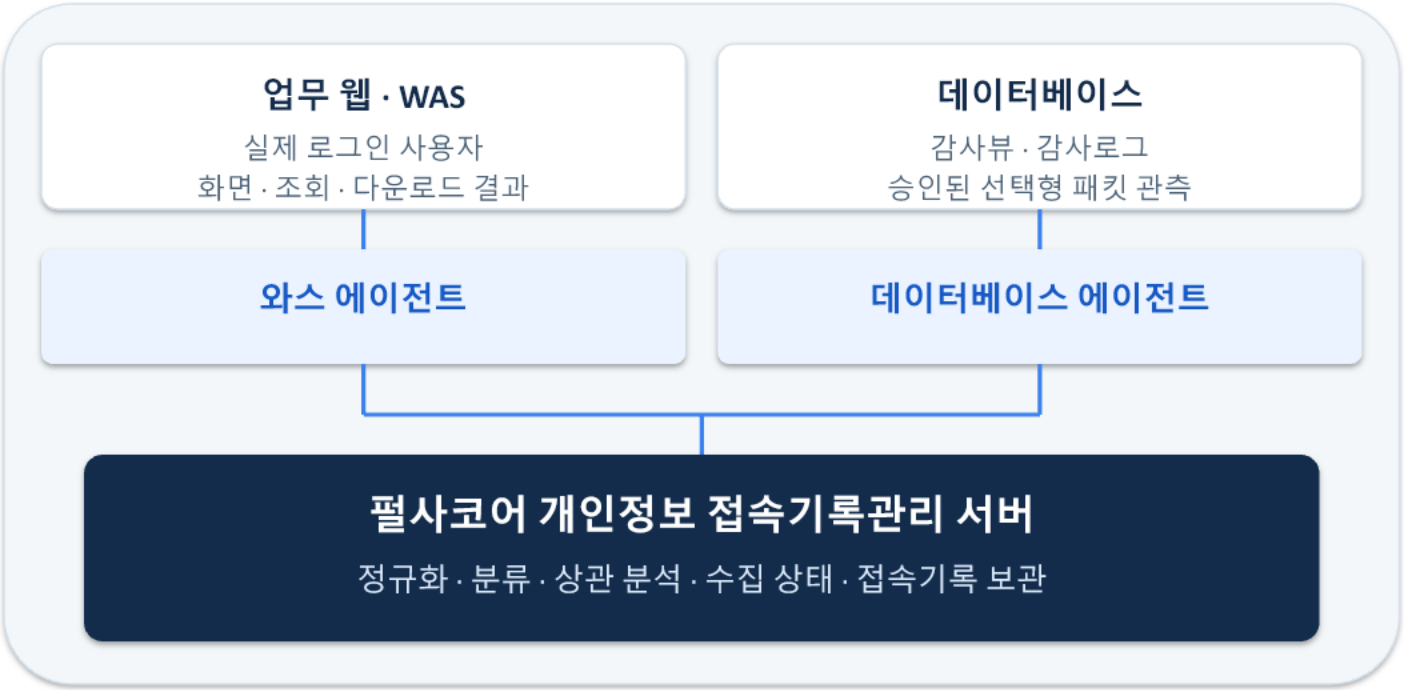
안전조치 위반 시 3천만원 이하 과태료 부과 가능
개인정보 보호법 제75조제2항제5호. 부과 여부와 금액은 위반 사실에 따라 판단됩니다.

법령 기준: 개인정보 보호법·시행령(2026.9.11 시행), 안전성 확보조치 기준(고시 제2026-9호, 2026.7.1 시행). 기능별 관련 조문은 11쪽 참조.

02 제품 구성과 수집 방식

DB와 WAS의 기록을 연결해 개인정보 처리행위를 파악합니다

데이터베이스 에이전트와 와스(WAS) 에이전트를 역할별로 설치하고, 업무 사용자·화면·처리 항목과 DB의 관측 증거를 연결합니다. 개인정보 원문을 무조건 중앙으로 수집하지 않습니다.



연계 대상 환경

DBMS	Oracle · PostgreSQL · Tibero · MySQL · Microsoft SQL Server
WAS	JEUS · Tomcat · WildFly · WebLogic · OC4J · Node.js

CPU 기반 수집·분석 / 독립형 설치 구성

역할별 설치본 제공, 읽기 전용 감사뷰, 승인 응답 후 전송 위치 갱신, 인증된 HTTPS 수신.

11.21 개발 작업내역서 기준 역할별 설치·합성 데이터 수신 시험 확인. 실제 제품·버전·감사뷰·업무로그 연계는 현장 인수시험 필요.

03 통합관제

여러 시스템의 개인정보 처리 현황을 한 화면에서 확인합니다

개인정보 보호 담당자가 전체 수집 상황과 위험 의심 이벤트, 미처리 소명 건을 확인하고, 필요한 기록으로 이동하도록 구성합니다.



기존 화면개발정의서 W01 통합현황 시안 · 가상 데이터

01 접속 현황

시스템별 처리행위와 수신 현황, 조회 기간별 집계.

02 위험 의심

규칙에 적중한 이벤트와 상세 확인 대상.

03 소명 대기

미제출·검토 대기·기한 경과 건 추적.

04 수집 품질

지연, 중단, 식별 미확인 상태를 별도 표시.

관제·상세 화면은 기존 개발 설계 시안입니다. 실제 운영 대시보드의 완성 및 통합 연동은 독립 제품 검수 범위입니다.

04 접속기록 조회와 개인정보 식별

누가 무엇을 처리했는지 실제 처리항목을 구분합니다

법정 기록 요소에 해당하는 사용자, 접속일시, 접속지, 처리한 정보주체, 수행업무를 연결하고, 업무시스템의 개인정보 항목과 처리 결과를 함께 확인합니다.



기존 화면개발정의서 W03 접속기록 조회 시안 · 가상 데이터

기본 기록 요소와 확인 정보

업무 사용자 ID · 접속시간 · 접속 IP 등 접속지 · 정보주체 참조값 · 조회/수정/삭제/다운로드 등 수행업무 · 성공/거부 여부 · 실제 처리 항목 및 건수

개인정보 유형은 기관 업무에 맞게 설정

우선 탐지: 주민등록번호·외국인등록번호·일반전화·휴대전화.
확장: 여권·운전면허·성명·학번·성적·주소 등 필드 사전으로 분류.

업무 사용자가 미확인인 경우 확정하지 않으며, 처리 행수와 정보주체 수는 별도로 판정합니다. 고시 제2조제3호 및 11.21 개발내역 반영.

05 이상행위 탐지와 알림

정상 업무와 다른 접근을 찾아 담당자가 신속하게 검토합니다

기관의 개인정보 취급 기준과 업무 특성에 맞춰 위험 탐지 규칙을 설정하고, 근거가 있는 의심 사건을 선별하여 검토를 지원합니다.



기존 화면개발정의서 W05 탐지규칙 시험 시안 · 임계값은 설정 예시

01 대량 조회·다운로드

짧은 시간에 많은 정보주체 조회 또는 반복 반출 시도.

02 업무 외 시간 접근

심야·휴일 접근 등 기관 근무 기준 대비 이상 징후.

03 권한·접속지 이상

권한 거부 반복, 승인된 접속지·업무 범위 이탈 후보.

04 반복·집중 접근

특정 대상자 반복 조회, 시스템 간 의심 패턴 확인.

위험 의심은 위반 확정이 아닙니다. 관리자 검토로 판단합니다.

탐지 임계값은 법정 수치가 아닌 기관 정책입니다. 알림·규칙 시험·예외 승인·사건 관리 기능은 독립 제품 개발 및 검수 범위입니다.

06 소명 및 후속조치

탐지에서 끝나지 않고 소명·검토·조치까지 이어집니다

개인정보 보호 담당자가 의심 접근과 다운로드 기록을 확인한 후 필요한 소명을 요청하고, 담당자가 사유와 증빙을 제출하면 검토 결과와 후속조치를 관리합니다.

탐지 근거 확인 → **요청** 사유·기한 → **제출** 소명·증빙 → **검토** 적정성 판단 → **종결** 조치·이력



기존 화면개발정의서 W06 소명 요청 시안 · 가상 데이터

소명 대상자 본인 사건에 필요한 범위만 확인하고 업무 사유·증빙을 제출합니다.

검토 담당자 소명과 원천 증거를 비교해 적정·부적정·보류·보완 요청을 기록합니다.

소명·조치 이력은 승인된 역할 범위에서 관리합니다. 지정 공공시스템은 고시 제17조에 따른 탐지·소명 등 조치 의무를 별도 적용.

07 정기 점검·보관·감사

법적 의무 이행을 위한 점검 결과와 증빙을 체계화합니다

내부 관리계획에 맞춘 정기 점검과 다운로드 확인, 접속기록의 안전한 보관, 결과 보고가 연결되는 운영 체계를 제공합니다.

개인정보 보호 점검 보고서

점검 대상: 예시 업무시스템 | 기간: 2026.11 | 시안

수집 상태	위험 의심	소명	조치
점검대상 12	검토대상 18	대기 7	종결 11

점검 항목	확인 내용	결과
접속기록·다운로드	정책 기간·사유 확인	검토중
보관 및 무결성	보존·백업 상태 확인	확인 필요
이상행위 및 소명	미처리·후속조치 확인	진행중

보고서 화면 구성 예시 · 수치 및 내용은 가상이며 실제 실적이 아닙니다.

01 보관정책 관리

시스템별 1년·2년 이상 정책과 추가 증적 보존 기간 설정.

02 안전한 기록 보관

접근 제한, 무결성 검증, 백업·복구 검증 및 삭제 승인.

03 점검과 보고

접속기록·다운로드 점검 계획, 결과, 후속조치 보고.

04 관리자 감사

열람·내보내기·정책 변경 등 관리자의 행위 기록.

보호 책임자와 감사 담당자의 확인 업무를 한곳에.

기록 수집 성공만이 아니라 점검·조치·보존의 증거를 확인합니다.

근거: 법 제29조, 시행령 제30조, 안전성 확보조치 기준 제8조. 보관·무결성·보고서 기능은 독립 제품의 개발 및 인수시험 범위입니다.

08 정보보안시스템 버전 관리

설치 버전과 업데이트 상태를 시스템별로 확인합니다

개인정보처리시스템을 보호하는 보안제품과 OS·DBMS·WAS의 설치정보를 연결해, 업데이트 누락과 기술지원 종료 여부를 확인하도록 구성합니다.

관리 구분	주요 확인 항목
방화벽·WAF·IPS·VPN	제품명, 제조사, 모델, 펌웨어, 적용 패치
백신·EDR 등 보안 프로그램	엔진·제품 버전, 탐지정보 갱신일, 실행·업데이트 상태
OS·DBMS·WAS·응용 SW	배포판·에디션·빌드·패키지 리비전, 설치·변경·제거 이력
공통 관리	담당자, 업무 중요도, 외부 노출, 관측 시각, EOS/EOL 근거

공식 공지와 설치정보 비교

제조사 보안 공지의 영향 버전·수정 버전·적용 조건을 대조합니다. 배포판 백포트와 패치 이력도 확인하며, 버전이나 관측 정보가 부족하면 확인 필요로 표시합니다.

자동 연계와 담당자 확인

지원 API·에이전트 연계로 확인 가능한 정보는 수집하고, 연계되지 않은 장비는 담당자가 증빙과 함께 등록합니다. 지원 종료와 미갱신 항목을 별도로 추적합니다.

근거: 고시 제9조, 안내서 본문 96~99쪽. 제품별 수집 범위는 연계 검수로 확정. 보완 기능은 제품 설계·검수 범위입니다.

09 보안취약점과 패치정보 관리

공식 보안 공지를 확인하고 우리 시스템의 영향을 판단합니다

개발사 정보 제공 서버에서 검토한 보안 공지와 기관의 설치 버전을 연결하여, 취약점 확인부터 조치 결과 검증까지 관리하도록 구성합니다.

01 공지 수집·검토

제조사·공식 보안기관 공지에서 제품, 영향 범위, CVE, 공식 위험도, 수정 버전과 출처를 정리합니다. AI 추출 내용은 검토 후 배포합니다.

02 영향 확인·우선순위 결정

기관의 제품·버전·플랫폼·설정 조건과 공지를 대조합니다. 공식 위험도, 악용 정보, 외부 노출과 업무 중요도를 확인하고 관리자가 최종 판단합니다.

03 조치 계획·미적용 사유 관리

담당자와 기한을 지정하고 실제 적용 결과를 등록합니다. 즉시 적용이 어려우면 사유, 보완조치, 승인자와 재검토일을 기록합니다.

04 재확인·이력 보존

적용 후 버전·증빙을 재확인하여 종결합니다. 공지 정정·자산 변경 시 재평가하며, 미확인 상태를 안전한 상태로 판정하지 않습니다.

패치정보만 수집·비교합니다. 패치 파일의 수집·다운로드·자동 설치 기능은 포함하지 않습니다.

근거: 고시 제4조제1항제10호·제9조. 공지·영향 판정·조치 이력과 SLM 설명을 구분하는 기존 PM 설계 반영.

10 안전성 확보조치 기준과 제품 기능

의무별 확인 항목과 이행 증빙을 연결합니다

2026년 11월 안내서의 해설과 고시 조문을 구분해 적용합니다. 법정 의무의 적용 대상·시행일·기관 내부 기준을 등록하여 확인 업무를 지원합니다.

근거	확인할 의무	제품의 지원 기능
제4조제1항 제9·10호	악성프로그램 방지·취약점 점검 사항을 내부 관리계획에 포함	점검 기준·대상·주기·담당자와 계획 이력 관리
제4조제4항	내부 관리계획 이행 실태를 연 1회 이상 점검·관리	책임자 점검 여부, 결과·검토일과 증빙 등록
제8조	접속기록 보관·점검·안전한 보관	기록 수집, 점검·소명, 보관·감사 증빙 연결
제9조제1·2항	보안 프로그램 최신 유지, 경보·보안 공지에 따른 업데이트	버전·업데이트 현황, 미적용 사유·보완조치와 결과 확인
제18조 2027.1.1 시행	공공시스템별 취약점 점검·외부 침투테스트 각 연 1회 이상, 지체 없는 보완조치	연도별 실시 여부, 보고서, 조치·재점검 이력 확인

제4조의 내부 관리계획 이행 점검과 제18조의 취약점 점검·침투테스트는 각각 별도 항목으로 관리합니다.

제18조는 지정 공공시스템 운영기관에 적용합니다. 일반 기관은 내부 관리계획과 적용 법령에 따른 주기를 설정합니다.

11 연간 취약점 점검·침투테스트 실시 여부

연간 점검·침투테스트 실시 여부를 확인합니다

취약점 점검과 외부 침투테스트를 각각 등록하고, 대상 연도·실시일·점검 범위·수행 주체·결과보고서·검토자를 확인합니다.

2027년 이행 현황 예시 · 가상 데이터 · 개발 시안

시스템	적용 기준	취약점 점검	외부 침투테스트
민원시스템	제18조 대상	실시 확인 보고서 검토 완료	미실시 계획 등록
복지시스템	제18조 대상	실시 등록 증빙 확인 중	실시 확인 외부 수행 확인
학사시스템	내부 계획	미실시 기한 임박	기관 계획에 따라 설정

실시 증빙과 조치 결과 확인

실시일·범위·수행기관·보고서·검토자를 확인합니다. 취약점 점검과 외부 침투테스트를 각각 관리하고, 발견사항의 보완조치·재점검 완료는 실시 여부와 구분합니다.

의무 대상과 시행 준비 상태 구분

제18조 대상 여부와 근거를 검토자가 확정합니다. 2026년은 시행 준비로 표시하고, 2027년부터 연간 이행을 확인합니다. 대상 미확정은 적용 제외로 처리하지 않습니다.

근거: 제18조 및 부칙, 안내서 본문 132~134쪽. 법정 의무 대상: 지정 공공시스템 운영기관. 주기 충족과 증빙 검토를 분리합니다.

12 알림과 유지관리 리포트

미실시·미조치 항목을 알리고 책임자의 확인 결과를 남깁니다

보안 업데이트와 연간 점검 의무를 같은 업무 목록에서 추적하되, 실시 여부·증빙 검토·조치 완료 상태를 구분해 보고하도록 구성합니다.

알림 구분	알림 내용과 후속 확인
점검·침투테스트	미실시, 계획 기한 임박·경과, 보고서 미등록, 외부 수행 미확인
버전·보안 공지	신규 영향 공지, 업데이트 누락, 기술지원 종료, 버전 정보 지연
조치·재점검	미조치, 조치 기한 경과, 보완조치 재검토, 재점검 미완료
수집·운영 상태	공지 수신 실패, 에이전트 중단, WAS 이상, DB XID 위험 징후

담당자 알림과 책임자 보고

기관 정책에 따라 화면 알림과 연계 채널을 사용합니다. 담당자 배정, 확인·처리 이력, 중복 억제, 발송 실패와 미처리 재알림을 관리합니다.

정기 유지관리 리포트

시스템·연도별 점검/침투테스트 실시 여부, 증빙 검토, 잔여 취약점, 패치 미적용 사유와 보완조치를 보고합니다. WAS·DB XID·수집 상태도 함께 확인합니다.

알림 시점과 보고 주기는 기관 정책입니다. 알림 확인은 의무 이행·조치 완료를 뜻하지 않습니다. 모니터링 연계는 별도 검수 대상입니다.

13 도입 효과와 적용 범위

기존 업무시스템을 유지하면서 개인정보 보호 관리체계를 강화합니다

기관별 업무와 보안정책을 확인한 뒤 수집 대상과 적용 범위를 정하고, 시험을 통해 접속기록의 식별 정확성과 누락·중복 여부를 검증합니다.

01 감사 대응 효율

접속기록·소명·점검 자료를 연결해 증빙 준비 부담 감소.

02 위험 대응 개선

위험 의심을 조기에 식별하고 검토 및 사후조치 지원.

03 업무 책임성

업무 사용자와 DB 계정을 구분하고 실제 처리항목 확인.

04 운영 일관성

시스템별 수집·보관·점검 기준과 처리 이력 통합.

독립 제품 적용 절차

대상 조사	연계 설정	현장 검증	운영 적용
업무·DB·WAS	감사뷰·로그	식별·누락·중복	점검·소명·보고

개발 상태와 제품 범위

DB·WAS 에이전트는 합성 데이터·로컬 수신 시험 확인. 버전·취약점·연간 실시 확인·증빙·알림·보고는 제품 보완 설계 및 현장 검수 범위.

법령 및 개발자료 근거 | 2026.11.24 확인

01 개인정보 보호법 제2조·제29조·제75조 (국가법령정보센터)

02 개인정보 보호법 시행령 제30조·제30조의2

03 안전성 확보조치 기준 제4·8·9·14·17·18조 및 부칙

04 개인정보보호위원회 안전성 확보조치 기준 안내서(2026.11.)

개발 근거: 기존 화면·에이전트 개발자료 및 v3.2 PM·유지관리 설계. 연간 실시·증빙 확인 기능은 본 보완안에 추가. 제17·18조는 2027.1.1 시행.

도입만으로 모든 법적 의무의 충족을 보장하지 않습니다. 기관의 실제 이행·권한 설정·추가 법령·운영 검증이 필요합니다.