개인정보의 안전성 확보조치 미흡사례 조치

안내서

2026.10



보건복지부

한국사회보장정보원 개인정보보호센터

여러분의 기관에서 관리하는 개인정보처리시스템에 보관된 개인정보는 안전한가요?

개인정보보호센터는 2026년도 개인정보보호 컨설팅을 수행하며
자주 확인되는 주요 미흡사례 12종을 선정하고,
이에 대한 자가진단 요령과 실무 조치 방안을 알기 쉽게 정리하였습니다.

본 안내서가 개인정보보호 담당자분들의 실무에 도움이 되기를 바라며,
앞으로도 개인정보보호센터는 각 기관이 안전하고 신뢰할 수 있는
개인정보 처리 환경을 조성할 수 있도록 함께 고민하는
든든한 조력자가 되겠습니다.

2026. 10.

일러두기

[관련 근거]
「개인정보 보호법」 법률 제21445호 (2026. 3. 10. 공포, 2026. 9. 11. 시행)
「개인정보의 안전성 확보조치 기준」 개인정보보호위원회고시 제2026-9호(2026. 7. 1. 시행)

[참고] 개정 「개인정보 보호법」 제재 규정 안내

- ✓ **경제적 제재 중심 전환**: 안전조치의무(법 제29조) 위반 시 형사처벌 규정은 폐지되었으며, 과태료(최대 3천만 원) 및 과징금(매출액의 3% 이하, 산정 곤란 시 20억 원 이하, 고의·중과실 시 최대 10%) 중심으로 처분이 이루어집니다.
- ✓ **보호 투자에 대한 과징금 감경 규정 신설**: 개정법은 개인정보 보호를 위한 예산 투입, 보안 시스템 도입, 취약점 조치 등 사전 노력을 성실히 기울인 기관에 대해 과징금을 감경할 수 있도록 명시하고 있습니다. 따라서 본 안내서의 조치사항 이행은 사고 예방뿐만 아니라 제재 감경의 객관적 증빙이 됩니다.
- ✓ **기관 대표자의 책임 강화**: 개인정보 보호책임자(CPO)의 독립성 보장 및 기관 대표자의 최종 관리 책임이 법적으로 강화되었으므로, 필요한 시스템 개선 및 예산 확보를 적극적으로 경영진에 건의하시기 바랍니다.

- ❖ 2026년 10월 31일 시행 예정인 고시 개정사항은 본문에 별도 시행일을 표기하였으며, 이후 법령 개정 시 최신 내용을 확인하시기 바랍니다.
- ❖ 본 안내서에서는 **「개인정보 보호법」**을 **「법」**으로, **「개인정보 보호법 시행령」**을 **「영」**으로, **「개인정보의 안전성 확보조치 기준」**을 **「고시」**로 축약하여 표기합니다.

목차



분야 1 접근 권한의 관리

사례 1 관리자 권한을 아무나 사용하고 있어요. 1
사례 2 여러 사람이 같은 계정을 공유하고 있어요. 4
사례 3 권한을 누가, 언제, 왜 바꿨는지 기록이 없어요. 6

분야 2 접근통제

사례 4 관리자 페이지가 인터넷에 노출되어 있어요. 8
사례 5 비밀번호만으로 로그인하고 있어요.(안전한 인증수단(2차 인증, MFA) 부재) 10
사례 6 일정 시간 지나도 자동 로그아웃(세션 타임아웃)이 안 돼요. 12

분야 3 개인정보의 암호화

사례 7 주민등록번호, 외국인등록번호, 계좌번호, 신용카드번호, 비밀번호가 암호화되지 않은 상태로 저장돼 있어요. 14
사례 8 오래된 암호화 방식을 사용하고 있어요. 17
사례 9 암호화 키를 어디에 어떻게 보관하는지 정해진 게 없어요. 19

분야 4 접속기록의 보관 및 점검

사례 10 누가 언제 접속했는지 기록이 남지 않고 있어요. 21

분야 5 악성프로그램 등 방지

사례 11 기술지원이 종료된 운영체제(OS)를 아직 사용하고 있어요. 24

분야 6 개인정보의 파기

사례 12 언제, 무엇을, 어떻게 파기했는지 기록이 없어요. 26

사례 01

관리자 권한을 아무나 사용하고 있어요.



1 문제가 뭔가요?

개인정보처리시스템 및 서버(웹, DB, 리눅스 등)에서 내부 업무 담당자나 유지보수 용역업체 직원(수탁사 인력)이 작업 시 root(최고 관리자) 권한이나 DBA(데이터베이스 전체 관리자) 권한으로 접속하도록 허용하고 있는 경우가 많습니다. 이 권한은 시스템의 모든 데이터에 접근이 가능하고 조회/수정/삭제 등의 작업을 할 수 있는 가장 강력한 권한이기 때문에, 실제 업무에 꼭 필요한 사람에게만, 필요한 시간으로 한정하여 **제한적으로 부여**해야 합니다.

쉽게 말하면

✓ 은행 금고의 마스터키를 직원 모두가 돌려쓰는 것과 같습니다.

✓ 누가 무슨 일을 했는지 추적도 안 되고, 사고가 나면 책임 소재도 불분명해집니다.

2 왜 위험한가요?

▸ 「고시」 제5조제1항에 따라 개인정보처리시스템 접근권한은 **업무 수행에 필요한 최소한의 범위**로 차등 부여해야 합니다.

※ 2026. 10. 31. 개정 고시 안내 : 최소권한 부여 및 인증 실패 시 접근제한(제5조) 대상이 '정당한 권한을 가진 자 전체'로 확대되므로 시스템 개편 시 참고하시기 바랍니다.

- 최고 관리자(root/DBA) 권한이 남용되면, 시스템 정보는 물론이고, 업무범위를 초과하여 개인정보까지 접근이 가능하므로, 개인정보 유출 등의 사고 발생 시 행위자 추적이 불가능합니다. 따라서, 불필요한 관리자 권한은 회수하고, **필요한 관리 작업은 개인별 식별·승인·기록이 가능하도록 통제**해야합니다.
- 불필요한 관리자 권한 부여는 접근 권한 관리(최소 권한 부여) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있으며, 사고 발생 시 **기관 대표자 및 보호책임자의 관리 책임**이 엄중히 물어질 수 있습니다.(단, 사전 예방 조치를 성실히 이행·입증한 경우 제재 감경 가능)

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
서버에 root 권한을 가진 계정이 몇 개인가요?	**서버 담당자에게 다음 관리자 권한 설정 조사를 요청하세요.** **(리눅스 서버)** wheel/sudo 그룹 확인, /etc/sudoers 및 /etc/sudoers.d/ 디렉터리 내 개별 설정 파일 확인 **(UID 0 계정 확인)** root 외에 UID가 0으로 설정된 슈퍼유저 계정이 존재하는지 확인 (awk -F: '($3 == 0) {print $1}' /etc/passwd)
DB에 DBA 권한을 가진 계정이 몇 개인가요?	**DB 담당자에게 DBMS별 최고 관리자 계정 및 권한 목록을 요청하세요.** **(DBA 롤 및 상속 권한 확인)** DBMS별(Oracle, MySQL, PostgreSQL 등) 시스템 롤(DBA, ALL PRIVILEGES) 부여 계정뿐만 아니라, 롤 상속을 통해 관리자 권한을 보유한 계정까지 전수 확인
유지보수 용역업체 직원(수탁사 인력)에게 root 나 DBA 권한을 주고 있나요?	**계정 관리 대장이 있다면 유지보수 용역업체 직원(수탁사 인력)에게 부여된 권한을 함께 확인하고, 없다면 즉시 작성을 요청하여 확인하세요.**

4 어떻게 해결하나요?

내부 조치 사항

① 계정 관리 대장을 만들어 내부 직원뿐만 아니라 협력기관 및 유지보수용 계정까지 누락 없이 기록하세요.
② 인사이동이나 사업 종료 시 계정을 즉시 삭제/잠금 처리하는 절차를 문서로 만들어 공유하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"우리 시스템의 모든 서버와 DB에 대해, root 또는 DBA 권한을 사용하는 계정 목록을 제출해 주세요. 그리고 업무에 꼭 필요한 최소 권한만 남기고 불필요한 관리자 권한은 모두 회수해 주세요. 또한 최고 관리자 계정으로 접근이 가능한 단말기를 지정하여 IP주소를 설정해 주세요."

01 | 접근 권한의 관리

- **리눅스 서버:** root 직접 접속을 차단하고 개인 계정 기반의 sudo를 적용하되, 편집기(vi), 셸(/bin/sh) 등 권한 상승(Privilege Escalation)을 유발할 수 있는 명령어는 sudo 허용 대상에서 제외하도록 통제
- **계정 용도 분리:** 상시 운영용 개인 계정과 별도로, 자동화 데몬용 '서비스 계정' 및 시스템 장애 대응용 '비상복구 계정'은 분리하여 엄격히 통제·기록
- **DB 서버:** 불필요한 DBA 롤을 회수하고, 업무에 꼭 필요한 시스템·객체 최소 권한(SELECT, INSERT 등)만 직접 부여
- 작업 완료 후 실제 적용된 권한 목록 및 변경 결과서를 문서로 제출받아 보관

사례
02 여러 사람이 같은 계정을 공유하고 있어요.



1 문제가 뭔가요?

내부 직원끼리, 또는 내부 직원과 유지보수 용역업체 직원(수탁사 인력)이 **하나의 계정을 공유**해서 시스템에 접속하는 경우입니다. 예를 들어 admin이라는 계정 하나를 여러 명이 같이 쓰는 상황입니다.

쉽게 말하면

✓ 사무실 출입 카드를 여러 명이 돌려쓰는 것과 같습니다.
✓ 출입 사실은 알 수 있지만 출입한 사람이 누구인지는 전혀 알 수 없습니다.

2 왜 위험한가요?

- 「고시」 제5조제4항에 따라 **정당한 사유가 없는 한 취급자별로 1인 1계정을 발급**해야 하며, **계정 공유는 원칙적으로 금지**됩니다. **단, 시스템이 제공하는 고정 계정(root 등) 등 기술적으로 개별 발급이 불가능한 경우 계정 관리 대장 및 접근제어시스템 등 보완통제**를 통해 실제 접속자를 식별할 수 있어야 합니다.
- 하나의 계정을 여럿이 쓰면 로그가 남아도 실제 작업자를 특정할 수 없어 **책임추적성이 상실**되고, 내부 유출 사고 시 결백을 소명할 수도 없습니다.
- 계정 공유 행위는 접근 권한 관리(계정 공유 금지) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
공유 계정이 존재하나요?	유지보수 용역업체(수탁사)에 "현재 사용 중인 모든 계정 목록을 실제 사용자 이름과 함께 제출해 달라"고 요청하세요.
동시에 여러 사람이 같은 계정으로 접속할 수 있나요?	리눅스/윈도우 서버에서 동일 계정으로 동시 접속(중복 로그인)이 가능한지 확인 요청하세요.

4 어떻게 해결하나요?

내부 조치 사항

① 계정 공유 금지를 내부 규정에 명시하고, 신규직원/유지보수 용역업체 직원(수탁사 인력) 투입 시 필수 교육에 포함하세요.

② 개인정보처리시스템 사용자 계정은 1인 1계정 발급이 원칙이며 공유를 엄격히 금지하세요. 부득이 시스템 유지보수 등을 위해 공용 계정 사용이 필요한 경우 **사전 승인** 하에 사용하고 **작업한 내용을 대장에 기록**하도록 하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"현재 여러 사람이 공유해서 쓰는 계정이 있다면 모두 찾아서 알려주세요. 각 업무 담당자별로 개인 계정을 새로 발급하고, 공유 계정은 모두 삭제해 주세요. 부득이하게 삭제가 어렵다면 동시 접속을 차단하고 계정 사용 대장을 작성하도록 조치해 주세요."

- **리눅스:** 동일 계정 동시 접속 차단 설정 적용
- **윈도우:** 원격 데스크톱 동시 세션 제한 설정 적용

사례
03 권한을 누가, 언제, 왜 바꿨는지 기록이 없어요.



1 문제가 뭔가요?

직원에게 시스템 접근권한을 부여하거나, 인사이동(승진, 부서 이동, 휴직, 퇴사 등)에 따른 시스템 접근권한 변경 시, **시스템에 그 기록이 남아 있지 않거나**, 기록을 남기더라도 **법정 보관 기간인 3년 이상 보관하지 않는** 경우입니다.

쉽게 말하면

- ✓ 중요 보안 시설의 열쇠를 직원들에게 불출·회수하면서 '열쇠 관리 대장'을 전혀 쓰지 않고 방치한 것과 같습니다.
- ✓ 퇴사자가 열쇠를 그대로 갖고 있어도 알 수 없고, 사고나 감사 시 정당하게 관리했음을 입증할 증빙이 전혀 없습니다.

2 왜 위험한가요?

- 「고시」 제5조제3항에 따라 권한의 부여·변경·말소 내역은 최소 **3년간 의무적으로 보관**해야 합니다.
- 권한의 부여·변경·말소 등의 이력이 없으면 퇴직자나 인사이동자의 권한이 방치되어 권한이 없는 사람이 개인정보에 접근하는 위험에 노출될 수 있고, 개인정보 유출 등의 사고로 이어질 수 있습니다.
- 권한의 부여·변경·말소 내역 미보관(또는 3년 미만 보관)은 접근 권한 관리(권한 변경 내역 보관) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
권한 변경 이력이 기록되고 있나요?	유지보수 용역업체(수탁사)에 "권한을 부여·변경·말소할 때마다 작업자, 작업일시, 작업 전후 권한을 기록하고 있나요?"라고 물어보세요.
권한 변경 기록이 3년 이상 보관되고 있나요?	로그 데이터 보관주기는 3년 이상으로 설정되어 있는지, 저장용량 초과로 과거 로그가 덮어써지지 않도록 안전하게 백업되고 있는지 확인하세요.

4 어떻게 해결하나요?

내부 조치 사항

1. 접근권한 변경 시 **신청 → 승인 → 적용 → 기록**에 이르는 **표준 절차**를 「내부 관리계획」에 명시하세요.
2. 접근권한 신청 시 신청자, 승인자, 신청 사유, 변경 전·후 권한, 적용 일시를 명확히 기록·관리하세요.
3. 인사 발령 문서와 실제 시스템상 접근권한 내역을 대조하는 주기적(반기별 또는 분기별) 점검을 수행하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"시스템에서 권한이 변경될 때마다 [신청자(대상자), 승인자, 조치 일시, 조치 전/후 권한, 근거 문서] 항목이 자동으로 기록되도록 개선해 주세요. 이 기록은 최소 3년 이상 보관해야 하므로, 용량 초과로 과거 데이터가 삭제되지 않도록 안전하게 백업 및 분리 보관되도록 설정해 주세요."

- 서버 용량 증설 대신, 안전한 외부 스토리지로 주기적인 로그 백업 및 이관 설정
- 애플리케이션에 접근권한 변경 이력 테이블 신설 또는 감사 로그 기능 추가

사례
04

관리자 페이지가 인터넷에 노출되어 있어요.



1 문제가 뭔가요?

내부 직원만 사용해야 하는 관리자 페이지, 서버 관리 화면, 데이터베이스 접속 포트가 **인터넷 어디에서나 접속 가능한 상태**인 경우입니다. 내부 업무망에서만 접근하게 해야 하는데, 외부(인터넷)에서도 접속 주소만 알면 누구나 로그인 화면에 도달할 수 있습니다.

쉽게 말하면

✓ 사무실 내부 회의실 문이 길거리에 그대로 열려 있는 것과 같습니다.

✓ 비밀번호만 알게 되면 내부 자료가 모두 노출됩니다.

2 왜 위험한가요?

- 「고시」 제6조제1항·제2항·제3항에 따라 비인가자 접근을 차단하고, 외부 접속 시 **가상사설망(VPN) 등 안전한 접속수단**을 적용해야 합니다.
- 관리자 페이지가 인터넷에 그대로 노출되거나 불필요한 공인 IP가 할당될 경우, 해커의 직접적인 표적이 될 수 있어 매우 위험합니다.
- 불필요한 인터넷 노출 및 접근통제 미비는 접근통제(비인가 접근 차단) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
관리자 페이지가 인터넷에서 열리나요?	유지보수 용역업체(수탁사)에 "우리 시스템의 관리자 페이지 URL이 외부(인터넷망)에서도 접속되나요?"라고 물어보세요.
서버에 공인 IP가 할당되어 있나요?	내부 운영 서버(DB, WAS 등)의 IP주소 목록을 받아서, 불필요하게 공인 IP가 할당된 장비가 있는지 확인해 달라고 요청하세요.
DMZ 구간은 분리되어 있나요?	외부에 노출되어야 하는 서버(WEB)만 DMZ 구간에 있고, DB 등 내부 서버는 사설 IP로 분리되어 있는지 확인하세요.

4 어떻게 해결하나요?

내부 조치 사항

① 전체 서버 목록과 IP 현황을 파악하세요. (유지보수 용역업체(수탁사)에 요청)
② "인터넷에서 접근할 수 있는 장비 목록"을 따로 관리하고, 그 외의 장비가 접근할 수 없도록 즉시 조치하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"내부 관리자만 접근해야 하는 페이지의 URL을 정리해서 알려주세요. 이 페이지들이 외부(인터넷)에서 접속되지 않도록 방화벽에서 접근을 차단해 주세요. (특정 사내 단말기 IP에서만 접속 허용 설정)"

"또한 운영 장비(DB, 파일 서버 등)에 공인 IP가 할당된 장비가 있는지 전수 조사하고, 네트워크 주소 변환(NAT)을 통해 모두 사설 IP로 전환해 주세요."

"관리자 페이지는 사내 내부망(사설 IP)에서만 접근 가능하도록 방화벽 정책을 적용해 주세요. 부득이 외부 원격 접속이 필요한 경우 사전에 인가된 PC에서 SSL-VPN 등을 통해서만 접근할 수 있도록 구성해 주세요."

- 방화벽에 내부 IP 대역에서만 접근 허용하는 화이트리스트 정책 적용
- DMZ 구간 재정비 (WEB 서버만 DMZ, DB/WAS 등은 내부망)

사례 05

비밀번호만으로 로그인하고 있어요.

(안전한 인증수단(2차 인증, MFA) 부재)



1 문제가 뭔가요?

시스템 로그인 시 아이디와 비밀번호만으로 접속하고, 추가적인 안전한 인증수단(2차 인증, MFA : 인증서, 보안토큰, 일회용 비밀번호(OTP), 휴대폰 인증 등)이 적용되어 있지 않은 상태입니다. 특히 인터넷을 통해 외부에서 접속할 때 비밀번호 하나에만 의존하면 계정 탈취 공격에 무방비로 노출됩니다.

쉽게 말하면

✓ 집 현관문이 비밀번호 하나에만 의존하는 것과 같습니다.

✓ 비밀번호가 노출되면 누구나 바로 문을 열고 들어올 수 있어 매우 위험합니다.

2 왜 위험한가요?

▸ 「고시」 제6조제2항에 따라 **정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우** 인증서, 보안토큰, 일회용 비밀번호 등 **안전한 인증수단(2차 인증, MFA)을 적용**해야 합니다.(단, 이용자가 아닌 정보주체의 개인정보를 처리하는 시스템은 가상사설망(VPN) 등 안전한 접속수단 또는 안전한 인증수단 중 선택 적용이 가능하며, 내부망 접속 관리자 계정의 경우 보안을 위해 안전한 인증수단의 적용을 권고하고 있습니다.)

※ 2026. 10. 31. 개정 고시 안내 : 안전한 인증수단 적용(제6조제2항) 의무 대상이 내부 취급자뿐만 아니라 '정당한 권한을 가진 자 전체(정보주체 제외)'로 확대 시행되므로 향후 시스템 개편 시 참고하시기 바랍니다.

- 비밀번호만 사용하는 경우 피싱, 악성코드 등으로 계정이 탈취되면 누구든 시스템에 쉽게 침입하여 대규모 개인정보를 유출할 수 있습니다.
- 안전한 인증수단(2차 인증, MFA) 미적용은 접근통제(안전한 인증수단 적용) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있으며, 이로 인해 개인정보 유출 사고가 발생할 경우 **과징금 가중 처분**은 물론 정보주체에 대한 **민사상 손해배상 책임**까지 부담할 수 있습니다.(단, 선제적 보호조치를 입증한 경우 과징금 감경 가능)

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
관리자 계정에 안전한 인증수단 (2차 인증)이 적용되어 있나요?	직접 관리자 페이지에 로그인해 보세요. 아이디/비밀번호 외에 OTP, 보안토큰 등 2차 인증 단계가 있는지 확인하세요
외부 사용자(협력 기관, 병원 등)는 어떻게 인증하나요?	외부 사용자 로그인 시 인증서, OTP 등이 적용되어 있는지 물어보세요.

4 어떻게 해결하나요?

내부 조치 사항

① 시스템 사용자 구분 및 적용 대상 식별
- 내부 개인정보취급자(시스템 관리자 포함)
- 정당한 접근 권한을 가진 외부 접속자(유지보수 용역업체(수탁사), 연계·협력 기관 등)
- 일반 이용자(정보주체/대민 서비스 이용자)

② 관리자와 외부 취급자는 반드시 추가 인증을 적용한다는 원칙을 수립하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"관리자 계정과 외부에서 접속하는 모든 사용자 계정에 대해 아이디/비밀번호 외에 추가 인증을 적용해 주세요. 예산이 있다면 OTP(일회용 비밀번호 생성기) 방식을, 제한되면 휴대폰 SMS 인증이나 인증서 방식을 검토해 주세요."

- **안전한 인증수단 예시:** OTP 앱/토큰, SMS 인증, 카카오톡 인증, 공동인증서
- **우선 적용 대상:** 최소한 관리자 계정과 외부 접속 계정부터
- **[2026. 10. 31. 개정 대비 연계 개발]:** 2차 인증 적용을 위한 로그인 화면 개편 시, 향후 의무화되는 '비밀번호 연속 오류(예: 5회) 차단 및 계정 잠금 기능'도 사전에 함께 구축하도록 요청하세요.

사례
06

일정 시간 지나도 자동 로그아웃(세션 타임아웃)이 안 돼요.



1 문제가 뭔가요?

시스템에 로그인한 후 일정 시간(기관의 시스템 위험도와 업무 특성에 맞게 개인정보처리자가 정하여 규정 및 매뉴얼 등에 반영, 예: 15분) 동안 아무 작업을 하지 않아도 **자동으로 로그아웃되지 않고 계속 접속 상태가 유지되는** 경우입니다. 웹 서버뿐 아니라 서버에 직접 접속하는 단말(리눅스, 윈도우 원격 접속)에도 해당됩니다.

쉽게 말하면

✓ 은행 ATM에서 돈을 뽑고 떠났는데, 다음 사람이 내 카드가 그대로 꽂혀 있는 상태에서 계속 거래할 수 있는 상황입니다.

2 왜 위험한가요?

- 「고시」 제6조제4항에 따라 개인정보취급자가 개인정보처리시스템에 접속하여 일정 시간동안 업무처리를 하지 않는 경우에는 자동으로 접속을 차단(세션 타임아웃)해야 합니다.
- 자리를 비우거나 공용 PC를 사용한 후 로그아웃하지 않으면, 화면에 노출된 개인정보를 타인이 무단 열람하거나 탈취할 위험이 큽니다.
- 자동 로그아웃(세션 타임아웃) 미설정은 접근통제(자동 접속 차단) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
웹 시스템이 자동 로그아웃 되나요?	직접 시스템에 로그인한 후 10~15분간 아무 작업도 하지 말고, 다시 사용하려 할 때 로그아웃되었는지 확인하세요.
서버 접속도 타임아웃이 설정되어 있나요?	유지보수 용역업체(수탁사)에 "리눅스/윈도우 서버의 세션 타임아웃이 몇 분으로 설정되어 있나요?"라고 물어보세요.

4 어떻게 해결하나요?

내부 조치 사항

① 기관의 개인정보 민감도와 업무 환경을 고려하여, 시스템 자동 접속 차단 기준시간(예: 15분)을 「내부 관리계획」 등에 명시하세요.

② 「내부 관리계획」 기준에 맞춰 웹 시스템과 관리자 화면이 지정된 시간에 정상 로그아웃되는지 주기적으로 확인하세요.

③ 시스템 자동 차단과 더불어, 취급자 PC의 화면보호기 자동 잠금 설정(예: 10분) 및 이석 시 화면 잠금(Windows 키 + L) 생활화 교육을 병행하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"웹 시스템과 서버 모두 15분(예시) 동안 사용하지 않으면 자동으로 로그아웃되도록 설정해 주세요. 설정 후에는 실제로 동작하는지 테스트하고 결과를 알려주세요."

- 웹 서버(WEB/WAS): 세션 타임아웃 15분으로 설정
- **윈도우 서버:** 그룹 정책(gpedit.msc)에서 원격 데스크톱 세션 시간제한 15분 설정
- **리눅스 서버:** .bash_profile 또는 /etc/profile에 TMOUT=900(15분=900초) 설정

사례 07

주민등록번호, 외국인등록번호, 계좌번호, 신용카드번호, 비밀번호가 암호화되지 않은 상태로 저장돼 있어요.



1 문제가 뭔가요?

주민등록번호, 외국인등록번호, 계좌번호, 신용카드번호, 비밀번호 등의 중요 정보가 데이터베이스에 **암호화되지 않은 평문(원본 그대로)으로** 저장된 상태입니다. 이는 가장 심각한 수준의 위반 사항입니다.

쉽게 말하면

- ✓ 고객의 주민등록번호와 계좌번호 등이 적힌 종이를 아무 잠금장치 없는 책상 위에 올려둔 것과 같습니다.
- ✓ DB가 해킹되거나 유출되면 모든 정보가 그대로 노출됩니다.

2 왜 위험한가요?

- ▸ 「법」 제24조의2 및 「고시」 제7조에 따라 주민등록번호, 비밀번호 및 정보통신서비스 이용자의 고유식별정보·계좌번호 등은 **반드시 암호화하여 저장**해야 합니다.(단, 이용자가 아닌 수급자·민원인 등의 계좌번호는 고시상 의무 대상은 아니나 재산 피해 방지를 위해 암호화 저장 권장)
- ▸ DB 해킹이나 백업 파일 유출 시, 평문으로 저장된 정보가 그대로 노출되어 2차 범죄와 심각한 피해로 이어집니다.

▸ 주요 개인정보의 평문 저장은 개인정보 암호화(암호화 저장) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있으며, 이로 인해 개인정보 유출 사고가 발생할 경우 **과징금 산정에서 중대한 가중 사유**로 작용할 수 있습니다.(단, 평소 암호화 조치 투자 및 기술적 보호를 충실히 입증한 경우 과징금 대폭 감경 가능)

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
주민등록번호, 외국인등록번호, 계좌번호, 신용카드번호가 암호화되어 저장되어 있나요?	유지보수 용역업체(수탁사)에 "데이터베이스에서 주민등록번호, 외국인 등록번호, 계좌번호, 신용카드번호 컬럼을 직접 조회했을 때 원본 번호가 보이나요?"라고 물어보세요. 원본이 보이면 암호화되지 않은 것입니다.
비밀번호도 암호화되어 있나요?	마찬가지로 DB의 비밀번호 칼럼이 암호화되어 저장되고 있는지 확인 요청하세요.
암호화되지 않은 개인정보가 또 있나요?	DB 전체 테이블을 대상으로 민감정보(건강, 복지 등), 일반정보(이름, 연락처 등), 첨부파일(신분증 사본 등)이 그대로 저장된 곳이 없는지 전수 점검을 요청하세요.

4 어떻게 해결하나요?

내부 조치 사항

① 이 문제는 즉시 조치가 필요한 최우선 과제입니다. 지체하지 말고 유지보수 용역업체(수탁사)에 조치를 요청하세요.

② 암호화 대상 개인정보 목록을 구분하여 파악하세요.

- [법적 의무 대상]
  1) 모든 시스템 공통: 주민등록번호(저장위치 무관), 비밀번호(일방향 암호화)
  2) '이용자'(포털·웹 회원 등): 계좌번호, 신용카드번호, 여권·운전면허·외국인등록번호, 생체인식정보
  3) '이용자가 아닌 정보주체'(수급자·민원인 등): 고유식별정보(여권·운전면허·외국인등록번호는 내부망 저장 시 위험도 분석에 따라 적용)
- [보안 권고 대상]
  1) '이용자가 아닌 정보주체'의 계좌번호: 법적 의무는 아니나, 재산 피해 방지를 위해 암호화 강력 권고

유지보수 용역업체(수탁사)에 요청할 사항

"(긴급) 데이터베이스에 평문으로 저장된 주민등록번호, 외국인등록번호, 계좌번호, 신용카드번호, 비밀번호를 전수 조사해 목록을 제출해 주세요. 그리고 해당 데이터들을 즉시 암호화해 주세요. 암호화 방식은 다음과 같이 적용해 주세요."

▸ **비밀번호 등 인증정보:** 복호화가 불가능한 안전한 일방향 암호화(SHA-256, SHA-384, SHA-512 등 + Salt 적용)

- **주민등록번호/외국인등록번호/계좌번호/신용카드번호 및 개인정보:** 업무상 복호화가 필요한 경우 안전한 양방향 암호화 적용(권장: 국산 검증 알고리즘(ARIA, SEED, LEA) 또는 AES 128/192/256비트)
- **암호화 완료 후:** 기존 평문 저장 영역은 복구가 불가능한 방식으로 안전하게 영구 삭제

> ※ **[공공기관 확인사항]** 국가 중요 정보 또는 대민 행정서비스를 처리하는 공공기관은 국가정보원 검증필 암호모듈(KCMVP) 탑재 대상 여부를 소관 부처 지침을 통해 반드시 확인하세요.

1 접근권한의 관리
2 접근통제
3 개인정보의 암호화
4 접속기록의 보관 및 점검
5 악성프로그램 등 방지
6 개인정보의 파기

사례 08

오래된 암호화 방식을 사용하고 있어요.



1 문제가 뭔가요?

비밀번호나 개인정보를 암호화할 때 **MD5, DES** 같은 오래된 알고리즘을 사용하는 경우입니다. 이 알고리즘들은 이미 보안 취약점이 발견되어 **현재는 사용하지 말아야 할 방식**입니다.

쉽게 말하면

✓ 녹슬거나 조잡한 자물쇠로 문을 잠그는 것과 같습니다.

✓ 겉으로는 잠겨 있어 안전하게 보이지만, 전문가 도구로 쉽게 열 수 있습니다.

2 왜 위험한가요?

- 「고시」 제7조제5항 및 관련 가이드에 따라 **안전성이 검증된 알고리즘(SHA-256 이상, ARIA·SEED·AES 등)을 사용**해야 합니다.
- MD5, DES 등의 구형 알고리즘은 이미 해독 기술이 공개되어 있으므로 암호화하지 않은 것과 같으며, 단시간 내에 평문이 복원될 수 있습니다.
- 취약한 알고리즘 사용은 개인정보 암호화(안전한 알고리즘 적용) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
어떤 암호화 알고리즘을 사용하고 있나요?	유지보수 용역업체(수탁사)에 "현재 비밀번호 저장과 개인정보 암호화에 사용 중인 알고리즘이 무엇인가요?"라고 물어보세요.
MD5나 DES가 사용되고 있나요?	만약 "MD5", "DES", "3DES"라는 답변이 나오면 교체가 필요합니다.

4 어떻게 해결하나요?

내부 조치 사항

① 암호화 알고리즘 목록을 확보하고, MD5/DES 사용 여부를 확인하세요.
② 안전한 알고리즘으로의 세부 교체 계획을 수립하고, 이에 필요한 소요 예산 및 외부 전문 인력 활용 방안을 마련하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"현재 사용 중인 암호화 알고리즘을 전부 확인하고, MD5, DES, 3DES 등 취약한 알고리즘을 사용 중이라면 아래 기준으로 교체해 주세요."

- **일방향 암호화(비밀번호 등):** SHA-224, SHA-256, SHA-384, SHA-512 + Salt(충분한 길이의 난수) 적용
- **양방향 암호화(개인정보 등):** 국산 암호 알고리즘(ARIA, SEED, LEA) 및 AES (128/192/256비트)
- **즉시 사용 중단 대상:** 보안 취약점이 확인된 구형 알고리즘(MD5, SHA-1, DES, 3DES/TDEA)은 전면 교체

※ **[공공기관 확인사항]** 검증필 암호모듈 적용 대상 공공기관 시스템인 경우, 국가정보원 검증필 암호모듈(KCMVP) 탑재 제품군으로 교체 요청

사례 09

암호화 키를 어디에 어떻게 보관하는지 정해진 게 없어요.



1 문제가 뭔가요?

데이터를 암호화했더라도, **그 암호를 풀 수 있는 열쇠(= 암호화 키)**를 어떻게 관리할지에 대한 절차나 규정이 없는 상태입니다. 암호화 키가 유출되면 암호화는 아무 의미가 없습니다.

쉽게 말하면

✓ 금고 비밀번호를 포스트잇에 적어 금고 옆에 붙여둔 것과 같습니다.

✓ 아무리 튼튼한 금고라도 비밀번호가 노출되면 소용없습니다.

2 왜 위험한가요?

- 「고시」 제7조제6항에 따라 **암호키의 생성·보관·배포·파기 등에 관한 관리 절차를 수립·시행**해야 합니다.
- 암호화 키가 소스코드 또는 서버 내 평문으로 관리될 경우, 암호화된 개인정보와 키가 함께 유출되어 즉시 복호화되는 치명적인 보안 취약점이 발생할 수 있습니다.
- 암호키 관리 절차가 마련되어 있지 않거나 암호키가 평문으로 저장되어 있는 등 암호키 관리 소홀 시 개인정보 암호화(암호키 관리) 의무 위반으로 시정조치 명령 및 과태료 부과 대상이 될 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
암호화 키 관리 절차 문서가 있나요?	담당 부서에 "암호화 키를 어떻게 관리하는지 문서로 만든 절차가 있나요?"라고 확인하세요.
암호화 키는 어디에 보관되나요?	"키는 누가, 어디에, 어떻게 보관하고 있나요?" (소스코드 내 하드코딩 여부 확인 필수)

4 어떻게 해결하나요?

내부 조치 사항

① 암호화 키 관리 정책 문서를 작성하세요. 포함해야 할 항목:

- 키 관리 담당자 지정
- 키 생성 방법 및 주기
- 키 보관 방법 (물리적.논리적 분리, 백업)
- 키 배포 대상자 및 절차
- 키 사용 유효기간(변경 주기)
- 키 복구 및 폐기 절차와 방법

유지보수 용역업체(수탁사)에 요청할 사항

"암호화 키가 소스코드 안에 직접 적혀 있거나 서버 내에 평문으로 저장되어 있지 않은지 확인해 주세요. 키는 별도의 안전한 저장소(예: 별도 보안 서버, HSM 등)에 보관하고, 접근권한을 최소화해 주세요. 또한 키 관리 절차 수립에 필요한 현재 키 현황을 문서로 제출해 주세요."

- 키를 소스코드에서 분리하여 별도 보안 저장소에 보관
- 키 접근권한을 최소 인원으로 제한

사례 10

누가 언제 접속했는지 기록이 남지 않고 있어요.



1 문제가 뭔가요?

개인정보처리시스템에 누가, 언제, 어디서, 무엇을 했는지에 대한 접속기록(로그)이 생성되지 않거나, 생성되더라도 충분히 보관·점검되지 않는 상태입니다.

쉽게 말하면

✓ 회사 건물에 CCTV가 전혀 없는 것과 같습니다.

✓ 사고가 나도 누가, 언제, 무엇을 했는지 전혀 알 수 없습니다.

2 왜 위험한가요?

- 「고시」 제8조에 따라 시스템 접속기록을 1년(5만 명 이상 또는 민감정보 처리 시 2년) 이상 보관해야 하며, **월 1회 이상 이상유무를 정기적으로 점검**해야 합니다.
- 내부 개인정보취급자뿐만 아니라 시스템에 접속하는 취급자 및 유지보수 용역업체 직원(수탁사 인력)의 접속기록이 누락 없이 남도록 조치해야 합니다.

※ 2026. 10. 31. 개정 고시 안내 : 접속기록 생성 대상이 '개인정보처리시스템에 접속한 자 전체(정보주체 제외)'로 명확화되며, 접속기록 점검은 「내부 관리계획」으로 정한 주기·방법에 따라 이행하도록 개정되므로 규정 정비 시 참고하시기 바랍니다.

- 접속기록이 누락되거나 부실할 경우, 개인정보의 무단 열람·다운로드 등 유출 징후를 탐지할 수 없으며, 사고 발생 시 행위자 추적 및 책임 규명이 어려울 수 있습니다.
- 접속기록 미생성 및 정기 점검 누락은 접속기록 관리(생성 및 점검) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있으며, 이로 인해 개인정보 유출 사고가 발생할 경우 **과징금 산정에서 중대한 가중 사유**로 작용할 수 있습니다.(단, 상시 점검 체계를 갖추고 보호 투자를 충실히 입증한 경우 과징금 감경 가능)

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
접속기록이 생성되고 있나요?	유지보수 용역업체(수탁사)에 "우리 시스템에 접속한 사용자의 로그인/로그아웃·작업 내역이 기록되고 있나요? 기록 화면이나 파일을 보여 달라"고 요청하세요.
기록에 법정 5대 필수 항목이 모두 포함되어 있나요?	접속기록 로그에 「고시」 제2조에 따른 5가지 필수항목 [식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무]이 빠짐없이 남는지 확인하세요.
접속기록을 정기적으로 점검하나요?	「내부 관리계획」으로 정한 주기에 따라 접속기록을 확인하고 이상징후를 점검하는지 확인하세요.

4 어떻게 해결하나요?

내부 조치 사항

① 「내부 관리계획」에 접속기록 점검 주기와 담당자를 지정하세요.
② 점검 결과를 문서로 남기고, 이상징후 발견 시 대응 절차를 마련하세요.
③ 개인정보 파일 다운로드 시 사유를 반드시 소명받고 점검대장에 기록하도록 규정하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"현재 접속기록이 생성되지 않거나 누락되고 있다면, 아래 항목을 포함한 접속기록이 생성되도록 시스템을 개선해 주세요. 또한 기록이 위·변조되지 않도록 별도 로그 서버에 저장하거나 WORM(쓰기 한 번만 가능한 저장장치) 방식을 검토해 주세요."

04 | 접속기록의 보관 및 점검

- 접속기록 법정 5대 필수 항목 준수
  1) 식별자: 접속을 시도·수행한 자를 식별할 수 있는 고유 ID
  2) 접속일시: 시스템 로그인·로그아웃 및 작업 수행 일시(초 단위까지 기록)
  3) 접속지 정보: 접속자의 PC/단말기 IP주소 (필요 시 MAC 주소 등)
  4) 처리한 정보주체 정보: 업무 수행 시 조회·수정·출력된 대상 고객/수급자/민원인 등의 식별정보 (계정, 등록번호 등)
  5) 수행업무: 조회(SELECT), 수정(UPDATE), 삭제(DELETE), 삽입(INSERT), 출력, 다운로드 등 구체적 행위 구분
- **보관 기간:** 최소 1년 이상(다음 중 어느 하나에 해당하는 경우 2년 이상 보관)
  1) 대규모 개인정보 처리: **5만 명 이상**의 정보주체에 관한 개인정보를 처리
  2) 중요정보 처리: **고유식별정보 또는 민감정보**를 처리
  3) 특정사업자: 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 **기간통신사업자**
- **보관 방법:** 덮어쓰기가 불가능한 저장 방식 권장, 주기적 백업

사례 11

기술지원이 종료된 운영체제(OS)를 아직 사용하고 있어요.



1 문제가 뭔가요?

기술 지원이 종료된(EOS, End of Support) 운영체제를 서버나 업무용 PC에서 계속 사용하는 경우입니다. 예를 들어 CentOS 7, Windows 10, Windows Server 2012 등은 이미 제조사 보안 업데이트가 중단된 상태입니다.

쉽게 말하면

✓ 이미 단종되어 부품도, 수리도 안 되는 오래된 자동차를 계속 타는 것과 같습니다.

✓ 새로 발견된 결함(보안 취약점)을 고칠 방법이 없습니다.

2 왜 위험한가요?

▸ 「고시」 제9조제2항에 따라 운영체제(OS) 및 소프트웨어 제작사의 보안 업데이트 공지가 있는 경우 **정당한 사유가 없는 한 즉시 업데이트를 적용**해야 합니다.

※ **[권장 기준]** 백신 등 보안프로그램은 실시간 자동 업데이트 또는 일 1회 이상 최신 상태를 유지하세요.

- 기술지원 종료(EOS) 이후에는 공식 패치를 받을 수 없어 해킹이나 랜섬웨어 공격에 상시 노출되며, 백신 프로그램만으로는 OS의 구조적 결함을 막기 어렵습니다.
- EOS OS 방치는 악성프로그램 등 방지(보안 업데이트 적용) 의무 위반으로 시정조치 명령 및 과태료 부과 대상이 될 수 있습니다. **취약점 방치로 인한 침해사고 발생 시 대표자·책임자의 관리 소홀 책임**이 따릅니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
서버와 PC의 OS 버전이 무엇인가요?	**유지보수 용역업체(수탁사)에 "운영 중인 서버와 업무용 PC의 OS 종류와 버전 목록을 제출해 달라"고 요청하세요.**
기술 지원이 종료된 OS가 있나요?	**현재 지원 종료된 주요 OS** ✓ CentOS 7 이하 (2024년 6월 지원 종료됨) ✓ Windows 10 (2025년 10월 지원 종료됨) ✓ Windows Server 2012 / 2012 R2 (2023년 10월 지원 종료됨) ✓ Windows 7, 8, 8.1 (지원 종료 완료) ✓ Ubuntu 18.04 이하 (2023년 5월 지원 종료됨)

4 어떻게 해결하나요?

내부 조치 사항

① 전체 IT 자산(서버 + PC)의 OS 버전 현황표를 확보하세요.
② EOS OS를 교체하는 계획과 예산을 수립하세요. (우선순위에 따라 단계적 교체)
③ 당장 교체가 어렵다면 해당 장비를 인터넷에서 격리하고, 접근통제를 강화하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"전체 서버와 업무 PC의 OS 현황을 조사해서 기술 지원이 종료된 OS 목록과 대수를 알려주세요. 교체 일정 계획을 함께 수립하고, 교체 전까지 임시 보안 조치(인터넷 격리, 접근통제 강화 등)를 적용해 주세요."

- 기술지원이 종료된 CentOS 7은 Rocky Linux 8/9, AlmaLinux 등 안정성이 검증된 후속 OS로 단계적 교체
- Windows 10 → Windows 11로 업그레이드
- 교체 전까지 해당 장비는 별도 네트워크 분리 또는 인터넷 접속 차단

사례 12

언제, 무엇을, 어떻게 파기했는지 기록이 없어요.



1 문제가 뭔가요?

개인정보를 파기했다고 하지만 파기 절차를 증명할 수 있는 **객관적인 기록**(파기 일시, 파기 대상, 파기 방법, 파기한 데이터양, 파기 작업자 등)을 남기지 않은 상태입니다. "파기했다"라는 말만 있고 증빙이 없는 상황입니다.

쉽게 말하면

- ✓ 회사 금고에 있던 현금을 사용하고는 "전부 규정에 맞게 집행했습니다"라고 말로만 보고하는 것과 같습니다.
- ✓ 돈을 언제, 어디에, 어떻게 썼는지 입증할 출금 전표나 영수증, 담당자 서명 등 그 어떤 기록도 남기지 않은 상황입니다.

2 왜 위험한가요?

▸ 「법」 제21조 및 「영」 제16조에 따라 **처리 목적 달성 등 불필요하게 된 날부터 지체 없이(5일 이내) 파기**해야 하며, 「고시」 제13조에 따라 파기 내역을 기록·관리해야 합니다.

※ 2026. 10. 31. 개정 고시 안내 : 「고시」 제4조제1항제13호에 따라 '개인정보의 파기에 관한 사항'이 「내부 관리계획」의 법정 필수 항목으로 신설되므로, 기관 내부 규정에 파기 기록·관리 절차를 반드시 반영하시기 바랍니다.

- 파기 확인서나 시스템 삭제 로그 등 객관적 증빙이 없는 경우, 개인정보를 파기하지 않고 계속 보유 및 이용할 가능성을 배제할 수 없으므로 법적으로 **파기하지 않고 방치한 것으로 간주**됩니다.
- 기한 내 미파기 및 증빙 부재는 개인정보 파기(기한 내 파기 및 기록 관리) 의무 위반으로 시정조치 명령 및 3천만 원 이하의 과태료 부과 대상이 될 수 있으며, 이로 인해 개인정보 유출 사고가 발생할 경우 피해 규모 확대에 따라 **과징금 산정에서 중대한 가중 사유**로 작용할 수 있습니다.

3 어떻게 확인하나요?

유지보수 용역업체(수탁사)나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
파기 결과를 기록하고 있나요?	"개인정보 파기 후 파기 결과보고서나 파기 확인서를 작성해 보관하고 있나요?"라고 물어보세요.
일부 보관이 필요한 데이터는 어떻게 관리하나요?	법령에 따라 보존해야 하는 데이터(과세, 감사 관련 등)와 파기할 데이터를 분리하는 절차가 있는지 확인하세요.

4 어떻게 해결하나요?

내부 조치 사항

① 개인정보 파기 시 파기 결과 확인서를 의무 작성하도록 규정하세요.(포함할 항목)

- 파기 일시
- 파기 사유 (처리 목적 달성 / 보유기간 만료 / 탈퇴 / 기타)
- 파기 대상 (시스템명, DB 테이블 명, 개인정보 파일명)
- 파기 항목 (이름, 주민번호, 연락처 등 파기한 정보 종류)
- 파기 데이터 수 (건)
- 파기 방법 (DB 레코드 삭제, 파일 완전 삭제, 물리적 파쇄 등)
- 파기 작업자 및 확인자 서명
- 분기별 또는 반기별 파기 이행 실태를 점검하세요.

② 분기별 또는 반기별 파기 이행 실태를 정기적으로 점검하세요.

유지보수 용역업체(수탁사)에 요청할 사항

"개인정보 파기 내역을 자동으로 기록하는 기능을 시스템에 추가하거나, 파기 작업 시 수동으로라도 파기 확인서를 생성해 제출해 주세요. 또한 법령상 보관 의무가 있는 정보와 파기 대상 정보를 분리하여 저장할 수 있도록 조치해 주세요."

- 파기 로그 자동화: 파기 시점, 대상, 작업자 등이 DB 로그로 기록되도록 구현
- 분리보관: 보존 대상 데이터는 별도 테이블로 이관하는 프로세스 구현

발행일 : 2026년 10월 | 발행처 : 보건복지부 · 한국사회보장정보원 개인정보보호센터
이메일 pipc@ssis.or.kr

※ 본 안내서는 보건복지부 소속 및 산하기관의 개인정보의 안전성 확보조치 기술지원을 위한 비매품입니다.