2023. 11.

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서

과학기술정보통신부 개인정보보호위원회 KISA 한국인터넷진흥원

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서

2023. 11.

과학기술정보통신부 개인정보보호위원회 KISA 한국인터넷진흥원

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서

• 들어가기 •

이 안내서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 함) 제47조(정보보호 관리체계의 인증) 및 「개인정보 보호법」 제32조의2(개인정보 보호 인증), 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」(과학기술정보통신부고시 제2023-33호, 개인정보보호위원회고시 제2023-8호)에서 규정하고 있는 사항에 대하여 보다 구체적으로 설명함을 목적으로 합니다.

이 안내서는 지속적인 보완 작업을 통하여 변경될 수 있으므로 항상 최신 버전 여부를 확인한 후 사용하여야 합니다. 또한 안내서에 제시된 법령, 고시, 참고자료는 안내서 발간시점(2023년 10월)을 기준으로 작성된 것으로 수시 개정될 수 있으므로 해당 시점에서 최신 버전을 확인하여 적용하여야 합니다.

이 안내서는 ISMS-P 홈페이지(https://isms-p.kisa.or.kr)에 게재되어 있으며, 기타 문의사항이 있으면 아래로 문의해 주시기 바랍니다.

E-mail : isms-p@kisa.or.kr

정보보호 및 개인정보보호 관리체계(ISMS-P)
인증기준 안내서

제1장

정보보호 및
개인정보보호 관리체계(ISMS-P)
인증기준 개요

I 정보보호 및 개인정보보호 관리체계 인증기준 개요

정보보호 및 개인정보보호 관리체계 인증기준은 크게 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항', '3. 개인정보 처리 단계별 요구사항' 3개 영역에서 총 101개의 인증기준으로 구성되어 있다. 정보보호 관리체계(ISMS) 인증을 받고자 하는 신청기관은 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항' 2개 영역에서 80개의 인증기준을 적용받게 되며, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '3. 개인정보 처리 단계별 요구사항'을 포함하여 101개의 인증기준을 적용받게 된다.

정보보호 및 개인정보보호 관리체계 인증기준 구성

영 역	분 야	적용 여부	
		ISMS	ISMS-P
1. 관리체계 수립 및 운영 (16개)	1.1. 관리체계 기반 마련	○	○
	1.2. 위험 관리	○	○
	1.3. 관리체계 운영	○	○
	1.4. 관리체계 점검 및 개선	○	○
2. 보호대책 요구사항 (64개)	2.1. 정책, 조직, 자산 관리	○	○
	2.2. 인적 보안	○	○
	2.3. 외부자 보안	○	○
	2.4. 물리 보안	○	○
	2.5. 인증 및 권한관리	○	○
	2.6. 접근통제	○	○
	2.7. 암호화 적용	○	○
	2.8. 정보시스템 도입 및 개발 보안	○	○
	2.9. 시스템 및 서비스 운영관리	○	○
	2.10. 시스템 및 서비스 보안관리	○	○
	2.11. 사고 예방 및 대응	○	○
	2.12. 재해 복구	○	○
3. 개인정보 처리 단계별 요구사항 (21개)	3.1. 개인정보 수집 시 보호조치	-	○
	3.2. 개인정보 보유 및 이용 시 보호조치	-	○
	3.3. 개인정보 제공 시 보호조치	-	○
	3.4. 개인정보 파기 시 보호조치	-	○
	3.5. 정보주체 권리보호	-	○

관리체계 수립 및 운영

‘관리체계 수립 및 운영’ 영역은 관리체계 기반 마련, 위험 관리, 관리체계 운영, 관리체계 점검 및 개선의 4개 분야 16개 인증기준으로 구성되어 있다. 이러한 관리체계 수립 및 운영은 정보보호 및 개인정보보호 관리체계를 운영하는 동안 지속적이고 반복적으로 실행되어야 한다.

관리체계 수립 및 운영 인증기준

영 역	분 야	항 목
1. 관리체계 수립 및 운영 (16개)	1.1. 관리체계 기반 마련	1.1.1 경영진의 참여
		1.1.2 최고책임자의 지정
		1.1.3 조직 구성
		1.1.4 범위 설정
		1.1.5 정책 수립
		1.1.6 자원 할당
	1.2. 위험 관리	1.2.1 정보자산 식별
		1.2.2 현황 및 흐름분석
		1.2.3 위험 평가
		1.2.4 보호대책 선정
	1.3. 관리체계 운영	1.3.1 보호대책 구현
		1.3.2 보호대책 공유
		1.3.3 운영현황 관리
	1.4. 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토
		1.4.2 관리체계 점검
		1.4.3 관리체계 개선

보호대책 요구사항

‘보호대책 요구사항’ 영역은 12개 분야 64개 인증기준으로 구성되어 있다. 보호대책 요구사항에 따라 신청기관은 관리체계 수립 및 운영 과정에서 수행한 위험평가 결과와 조직의 서비스 및 정보시스템 특성 등을 반영하여 체계적으로 보호대책을 수립·이행하여야 한다.

보호대책 요구사항 인증기준

영 역	분 야	항 목
2. 보호대책 요구사항 (64개)	2.1. 정책, 조직, 자산 관리	2.1.1 정책의 유지관리
		2.1.2 조직의 유지관리
		2.1.3 정보자산 관리
	2.2. 인적 보안	2.2.1 주요 직무자 지정 및 관리
		2.2.2 직무 분리
		2.2.3 보안 서약
		2.2.4 인식제고 및 교육훈련
		2.2.5 퇴직 및 직무변경 관리
		2.2.6 보안 위반 시 조치
	2.3. 외부자 보안	2.3.1 외부자 현황 관리
		2.3.2 외부자 계약 시 보안
		2.3.3 외부자 보안 이행 관리
		2.3.4 외부자 계약 변경 및 만료 시 보안
	2.4. 물리 보안	2.4.1 보호구역 지정
		2.4.2 출입통제
		2.4.3 정보시스템 보호
		2.4.4 보호설비 운영
		2.4.5 보호구역 내 작업
		2.4.6 반출입 기기 통제
		2.4.7 업무환경 보안
	2.5. 인증 및 권한관리	2.5.1 사용자 계정 관리
		2.5.2 사용자 식별
		2.5.3 사용자 인증
		2.5.4 비밀번호 관리
		2.5.5 특수 계정 및 권한관리
		2.5.6 접근권한 검토

영 역	분 야	항 목
2. 보호대책 요구사항 (64개)	2.6. 접근통제	2.6.1 네트워크 접근
		2.6.2 정보시스템 접근
		2.6.3 응용프로그램 접근
		2.6.4 데이터베이스 접근
		2.6.5 무선 네트워크 접근
		2.6.6 원격접근 통제
		2.6.7 인터넷 접속 통제
	2.7. 암호화 적용	2.7.1 암호정책 적용
		2.7.2 암호키 관리
	2.8. 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리
		2.8.4 시험 데이터 보안
		2.8.5 소스 프로그램 관리
		2.8.6 운영환경 이관
	2.9. 시스템 및 서비스 운영관리	2.9.1 변경관리
		2.9.2 성능 및 장애관리
		2.9.3 백업 및 복구관리
		2.9.4 로그 및 접속기록 관리
		2.9.5 로그 및 접속기록 점검
		2.9.6 시간 동기화
		2.9.7 정보자산의 재사용 및 폐기
	2.10. 시스템 및 서비스 보안관리	2.10.1 보안시스템 운영
		2.10.2 클라우드 보안
		2.10.3 공개서버 보안
		2.10.4 전자거래 및 핀테크 보안
		2.10.5 정보전송 보안
		2.10.6 업무용 단말기기 보안
		2.10.7 보조저장매체 관리
		2.10.8 패치관리
		2.10.9 악성코드 통제
	2.11. 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축
		2.11.2 취약점 점검 및 조치
		2.11.3 이상행위 분석 및 모니터링
		2.11.4 사고 대응 훈련 및 개선
		2.11.5 사고 대응 및 복구
	2.12. 재해 복구	2.12.1 재해·재난 대비 안전조치
		2.12.2 재해 복구 시험 및 개선

개인정보 처리 단계별 요구사항

'개인정보 처리 단계별 요구사항' 영역은 개인정보 생명주기에 따른 개인정보 수집 시 보호조치, 개인정보 보유 및 이용 시 보호조치, 개인정보 제공 시 보호조치, 개인정보 파기 시 보호조치와 정보주체 권리보호를 포함하여 5개 분야 21개의 인증기준으로 구성되어 있다. 이 영역은 대부분 법적 요구사항과 직접적으로 관련되어 있으므로 개인정보 흐름분석을 바탕으로 조직이 적용받는 법규 및 세부 조항을 명확히 파악하여 이를 준수하여야 한다.

개인정보 처리 단계별 요구사항 인증기준

영 역	분 야	항 목
3. 개인정보 처리 단계별 요구사항 (21개)	3.1. 개인정보 수집 시 보호조치	3.1.1 개인정보 수집·이용
		3.1.2 개인정보 수집 제한
		3.1.3 주민등록번호 처리 제한
		3.1.4 민감정보 및 고유식별정보의 처리 제한
		3.1.5 개인정보 간접수집
		3.1.6 영상정보처리기기 설치·운영
		3.1.7 마케팅 목적의 개인정보 수집·이용
	3.2. 개인정보 보유 및 이용 시 보호조치	3.2.1 개인정보 현황관리
		3.2.2 개인정보 품질보장
		3.2.3 이용자 단말기 접근 보호
		3.2.4 개인정보 목적 외 이용 및 제공
		3.2.5 가명정보 처리
	3.3. 개인정보 제공 시 보호조치	3.3.1 개인정보 제3자 제공
		3.3.2 개인정보 처리 업무 위탁
		3.3.3 영업의 양도 등에 따른 개인정보 이전
		3.3.4 개인정보 국외이전
	3.4. 개인정보 파기 시 보호조치	3.4.1 개인정보 파기
		3.4.2 처리목적 달성 후 보유 시 조치
	3.5. 정보주체 권리보호	3.5.1 개인정보 처리방침 공개
		3.5.2 정보주체 권리보장
		3.5.3 정보주체에 대한 통지

제2장

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 설명

1. 관리체계 수립 및 운영
2. 보호대책 요구사항
3. 개인정보 처리 단계별 요구사항

1 관리체계 수립 및 운영

1.1. 관리체계 기반 마련

항 목	1.1.1 경영진의 참여
인증기준	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가? • 경영진이 정보보호 및 개인정보보호 활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립·이행하고 있는가?

세부 설명

- 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 의사결정권이 있는 경영진의 참여가 이루어질 수 있도록 보고, 의사결정 등의 책임과 역할을 문서화하여야 한다.
  - 정보보호 및 개인정보보호 정책의 제·개정, 위험관리, 내부감사 등 관리체계 운영의 중요 사안에 대하여 경영진이 참여할 수 있도록 활동의 근거를 정보보호 및 개인정보보호 정책 또는 시행문서에 명시
- 경영진이 정보보호 및 개인정보보호 활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립·이행하여야 한다.
  - 정보보호 및 개인정보보호 관리체계 내 경영진이 참여하는 중요한 활동을 정의하고, 그에 따른 보고체계 마련(정기·비정기 보고, 위원회 참여 등)
  - 경영진이 효과적으로 관리체계 수립·운영에 참여할 수 있도록 조직의 규모 및 특성에 맞게 보고 및 의사결정 절차, 대상, 주기 등 결정
  - 수립된 내부절차에 따라 정보보호 및 개인정보보호 관리체계 내 주요 사항에 대하여 경영진이 보고를 받고 의사결정에 참여

증거자료

예시

- 정보보호 및 개인정보보호 보고 체계(의사소통계획 등)
- 정보보호 및 개인정보보호 위원회 회의록
- 정보보호 및 개인정보보호 정책·지침(경영진 승인내역 포함)
- 정보보호계획 및 내부 관리계획(경영진 승인내역 포함)
- 정보보호 및 개인정보보호 조직도

결함사례

- 사례 1 : 정보보호 및 개인정보보호 정책서에 분기별로 정보보호 및 개인정보보호 현황을 경영진에게 보고하도록 명시하였으나, 장기간 관련 보고를 수행하지 않은 경우
- 사례 2 : 중요 정보보호 활동(위험평가, 위험수용수준 결정, 정보보호대책 및 이행계획 검토, 정보보호대책 이행결과 검토, 보안감사 등)을 수행하면서 관련 활동관련 보고, 승인 등 의사결정에 경영진 또는 경영진의 권한을 위임받은 자가 참여하지 않았거나 관련 증거자료가 확인되지 않은 경우

항 목	1.1.2 최고책임자의 지정
인증기준	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
주요 확인사항	• 최고경영자는 정보보호 및 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가? • 정보보호 최고책임자 및 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 있으며, 관련 법령에 따른 자격요건을 충족하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무), 제31조(개인정보 보호책임자의 지정) • 정보통신망법 제45조의3(정보보호 최고책임자의 지정 등) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 최고경영자는 조직 내에서 정보보호 및 개인정보보호 관리 활동을 효과적으로 추진하기 위하여 이를 총괄하여 책임질 수 있는 정보보호 최고책임자 및 개인정보 보호책임자를 인사발령 등의 절차를 통하여 공식적으로 지정하여야 한다.

▶ 정보보호 최고책임자 및 개인정보 보호책임자는 인사발령 등을 통하여 공식으로 임명하여야 하며, 당연직의 경우 정보보호 및 개인정보보호 정책서에 그 직위를 명시하여야 함

■ 정보보호 최고책임자 및 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 관련 법령에 따른 자격요건을 충족하여야 한다(※ 정보통신망법 시행령 제36조의7 참고).

▶ 정보보호 최고책임자 및 개인정보 보호책임자는 조직의 정보보호 및 개인정보보호 업무를 실질적으로 총괄할 수 있도록 정보보호 및 개인정보보호 관련 지식 및 소양이 있는 자로서 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정

※ 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고. 다만, 대통령령으로 정하는 기준에 해당하는 경우 신고 예외

▶ 정보보호 최고책임자 지정에 대한 법적 요건 준수 필요(※ 정보통신망법 제45조의3 참고)

• 정보보호 최고책임자는 다음 업무 수행

> 1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
> 가. 정보보호 계획의 수립·시행 및 개선
> 나. 정보보호 실태와 관행의 정기적인 감사 및 개선
> 다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련

라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행

2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.

가.「정보보호산업의 진흥에 관한 법률」제13조에 따른 정보보호 공시에 관한 업무

나.「정보통신기반 보호법」제5조제5항에 따른 정보보호 책임자의 업무

다.「전자금융거래법」제21조의2제4항에 따른 정보보호 최고책임자의 업무

라.「개인정보 보호법」제31조제2항에 따른 개인정보 보호책임자의 업무

마. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

- 정보보호 최고책임자 지정요건(※ 정보통신망법 시행령 제36조의7 제1항)

No	구분(정보통신서비스 제공자)	정보보호 최고책임자 지정 요건
1	• 자본금 1억원 이하인 자 • 소기업 • 중기업으로서 전기통신사업자, 정보보호 관리체계 인증을 받아야 하는 자, 개인정보 처리방침을 공개해야 하는 개인정보처리자, 통신판매업자가 아닌 자	• 사업주 또는 대표자
2	• 직전 사업연도 말 기준 자산총액이 5조원 이상인 자 • 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 직전 사업연도 말 기준 자산총액이 5천억원 이상인자	• 이사(「상법」 제401조의2 제1항 제3호에 따른 자와 같은 법 제408조의 2에 따른 집행임원을 포함) ※ 겸직 제한 요건 준수 필요
3	• 위의 1호, 2호에 해당하지 않는 자	• 사업주 또는 대표자 • 이사(「상법」 제401조의2 제1항 제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함) • 정보보호 관련 업무를 총괄하는 부서의 장

▶ 개인정보 보호책임자 지정에 대한 법적 요건 준수 필요(※ 개인정보 보호법 시행령 제32조 등 참고)

- 개인정보 보호책임자는 다음의 업무 수행

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

증거자료

예시

- 정보보호 최고책임자 및 개인정보 보호책임자 임명관련 자료(인사명령, 인사카드 등)
- 정보보호 및 개인정보보호 조직도
- 정보보호 및 개인정보보호 정책·지침
- 직무기술서(정보보호 최고책임자 및 개인정보 보호책임자의 역할 및 책임에 관한 사항)
- 정보보호 최고책임자 신고 내역
- 내부 관리계획(개인정보 보호책임자 지정에 관한 사항)

결함사례

- 사례 1 : 정보통신망법에 따른 정보보호 최고책임자 지정 및 신고 의무 대상자임에도 불구하고 정보보호 최고책임자를 지정 및 신고하지 않은 경우
- 사례 2 : 개인정보 보호와 관련된 실질적인 권한 및 지위를 보유하고 있지 않은 인원을 개인정보 보호 책임자로 지정하고 있어, 개인정보 처리에 관한 업무를 총괄해서 책임질 수 있다고 보기 어려운 경우
- 사례 3 : 조직도상에 정보보호 최고책임자 및 개인정보 보호책임자를 명시하고 있으나, 인사발령 등의 공식적인 지정절차를 거치지 않은 경우
- 사례 4 : ISMS 인증 의무대상자이면서 전년도 말 기준 자산총액이 5천억 원을 초과한 정보통신서비스 제공자이지만 정보보호 최고책임자가 CIO를 겸직하고 있는 경우

항 목	1.1.3 조직 구성
인증기준	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.
주요 확인사항	• 정보보호 최고책임자 및 개인정보 보호책임자의 업무를 지원하고 조직의 정보보호 및 개인정보보호 활동을 체계적으로 이행하기 위하여 전문성을 갖춘 실무조직을 구성하여 운영하고 있는가? • 조직 전반에 걸친 중요한 정보보호 및 개인정보보호 관련사항에 대하여 검토, 승인 및 의사결정을 할 수 있는 위원회를 구성하여 운영하고 있는가? • 전사적 정보보호 및 개인정보보호 활동을 위하여 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자로 구성된 실무 협의체를 구성하여 운영하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

- 조직의 규모, 업무 중요도 등의 특성을 고려하여 정보보호 및 개인정보보호 관리체계를 구축하고 지속적으로 운영하기 위하여 필요한 조직 구성의 근거를 정보보호 및 개인정보보호 정책서 등에 명시하고, 전문성을 갖춘 실무조직을 구성하여 운영하여야 한다.
  - 정보보호 최고책임자, 개인정보 보호책임자, 개인정보보호 실무조직, 위원회 등 정보보호 및 개인정보보호 조직의 구성·운영에 대한 사항을 정책서, 내부 관리계획 등에 명시
  - 실무조직의 구성형태 및 규모는 전사 조직의 규모, 업무, 서비스의 특성, 처리하는 정보 및 개인정보의 중요도, 민감도, 법 규제 등 고려
  - 실무조직은 전담조직 또는 겸임조직으로 구성할 수 있으나, 겸임조직으로 구성하더라도 실질적인 역할 수행이 가능하도록 역할 및 책임이 공식적으로 부여되어야 함
  - 실무조직의 구성원은 정보보호 및 개인정보보호 전문성과 다양한 서비스에 대한 이해도와 경험이 많은 직원으로 구성(관련 학위 및 자격증 보유, 실무 경험 보유, 관련 교육 이수 등)

- 조직 전반에 걸친 중요한 정보보호 및 개인정보보호 관련사항에 대하여 검토, 승인 및 의사결정을 할 수 있는 위원회를 구성하여 운영하여야 한다.
  - 위원회는 정보보호 및 개인정보보호 관련하여 조직 내 이해관계를 대변하고 의사결정을 할 수 있도록 경영진, 임원, 정보보호 최고책임자, 개인정보 보호책임자 등 실질적인 검토 및 의사결정 권한이 있는 임직원으로 구성
  - 정기 또는 사안에 따라 수시로 위원회 개최
  - 위원회는 조직 전반에 걸친 주요 사안에 대한 검토, 승인 및 의사결정 수행

※ 위원회에서 검토 및 의사결정이 필요한 주요 사안(예시)
· 정보보호 및 개인정보보호 정책·지침의 제·개정
· 위험평가 결과
· 정보보호 및 개인정보보호 예산 및 자원 할당
· 내부 보안사고 및 주요 위반사항에 대한 조치
· 내부감사 결과 등

■ 전사적 정보보호 및 개인정보보호 활동을 위하여 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자로 구성된 실무 협의체를 구성하여 운영하여야 한다.

▶ 조직의 규모 및 관리체계 범위 내 서비스의 중요도에 따라 실무 협의체 구성원, 조직체계 등을 결정

▶ 실무 협의체에서는 정보보호 및 개인정보보호 관련 사항에 대하여 실무 차원에서 공유·조정·검토·개선하고, 의사결정 및 경영진 지원이 필요한 경우에는 위원회에 상정하여 논의

증거자료

예시

- 정보보호 및 개인정보보호 위원회 규정·회의록
- 정보보호 및 개인정보보호 실무 협의체 규정·회의록
- 정보보호 및 개인정보보호 조직도
- 내부 관리계획
- 직무기술서

결함사례

- 사례 1 : 정보보호 및 개인정보보호 위원회를 구성하였으나, 임원 등 경영진이 포함되어 있지 않고 실무 부서의 장으로 구성되어 있어 조직의 중요 정보 및 개인정보 보호에 관한 사항을 결정할 수 없는 경우
- 사례 2 : 내부 지침에 따라 중요 정보처리 부서 및 개인정보처리 부서의 장(팀장급)으로 구성된 정보보호 및 개인정보보호 실무 협의체를 구성하였으나, 장기간 운영 실적이 없는 경우
- 사례 3 : 정보보호 및 개인정보보호 위원회를 개최하였으나, 연간 정보보호 및 개인정보보호 계획 및 교육 계획, 예산 및 인력 등 정보보호 및 개인정보보호에 관한 주요 사항이 검토 및 의사결정이 되지 않은 경우
- 사례 4 : 정보보호 및 개인정보보호 관련 심의·의결을 위해 정보보호위원회를 구성하여 운영하고 있으나, 운영 및 IT보안 관련 조직만 참여하고 개인정보보호 관련 조직은 참여하지 않고 있어 개인정보보호에 관한 사항을 결정할 수 없는 경우

항 목	1.1.4 범위 설정
인증기준	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
주요 확인사항	• 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 관리체계 범위를 설정하고 있는가? • 정의된 범위 내에서 예외사항이 있을 경우 명확한 사유 및 관련자 협의·책임자 승인 등 관련 근거를 기록·관리하고 있는가? • 정보보호 및 개인정보보호 관리체계 범위를 명확히 확인할 수 있도록 관련된 내용(주요 서비스 및 업무 현황, 정보시스템 목록, 문서목록 등)이 포함된 문서를 작성하여 관리하고 있는가?

세부 설명

- 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 관리체계 범위를 설정하여야 한다.
  - 관리체계 범위에는 사업(서비스)과 관련된 임직원, 정보시스템, 정보, 시설 등 유·무형의 핵심자산을 누락 없이 포함
  - 특히 정보보호 관리체계 의무대상자의 경우 법적 요구사항에 따른 정보통신서비스 및 관련 정보자산은 의무적으로 포함되도록 범위 설정
- 정의된 범위 내에서 예외사항이 있을 경우 명확한 사유 및 관련자 협의·책임자 승인 등 관련 근거를 기록·관리하여야 한다.
  - 정보보호 관리체계와 개인정보보호 관리체계의 범위가 상이한 경우에는 인증범위 내의 정보자산 목록(개인정보, 시스템, 네트워크 등)을 정보보호 관리체계 및 개인정보보호 관리체계 관점에서 명확하게 식별하여 정의
  - 인증범위에서 제외되는 서비스, 정보시스템 등에 대해서는 내부 협의 및 책임자 승인을 거친 후 그 사유 및 근거에 대하여 기록하여 관리
- 정보보호 및 개인정보보호 관리체계 범위를 명확히 확인할 수 있도록 관련된 내용(주요 서비스 및 업무 현황, 정보시스템 목록, 문서 목록 등)이 포함된 문서를 작성하여 관리하여야 한다.
  - 주요 서비스 및 업무 현황(개인정보 처리 업무 현황 포함)
  - 서비스 제공과 관련된 조직 현황(조직도 등)
  - 정보보호 및 개인정보보호 조직 현황
  - 주요 설비 목록
  - 정보시스템 목록 및 네트워크 구성도
  - 정보자산, 개인정보 관련 자산식별 기준 및 자산현황

- 정보보호 및 개인정보보호 시스템 목록
- 서비스(시스템) 구성도 및 개인정보(수집, 이용, 제공, 저장, 관리, 파기) 처리 흐름
- 문서 목록(예 : 정책, 지침, 매뉴얼, 운영명세서 등)
- 정보보호 및 개인정보보호 관리체계 수립 방법 및 절차, 관련 법적 준거성 검토, 내부감사
- 고객센터, IDC, IT 개발 및 운영 등 외주(위탁)업체 현황 등

증거자료

예시

- 정보보호 및 개인정보보호 관리체계 범위 정의서
- 정보자산 및 개인정보 목록
- 문서 목록
- 서비스 흐름도
- 개인정보 흐름도
- 전사 조직도
- 시스템 및 네트워크 구성도

결함사례

- 사례 1 : 정보시스템 및 개인정보처리시스템 개발업무에 관련한 개발 및 시험 시스템, 외주업체직원, PC, 테스트용 단말기 등이 관리체계 범위에서 누락된 경우
- 사례 2 : 정보보호 및 개인정보보호 관리체계 범위로 설정된 서비스 또는 사업에 대하여 중요 의사결정자 역할을 수행하고 있는 임직원, 사업부서 등의 핵심 조직(인력)을 인증범위에 포함하지 않은 경우
- 사례 3 : 정보시스템 및 개인정보처리시스템 개발업무에 관련한 개발 및 시험 시스템, 개발자 PC, 테스트용 단말기, 개발조직 등이 관리체계 범위에서 누락된 경우

항 목	1.1.5 정책 수립
인증기준	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진의 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
주요 확인사항	• 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책을 수립하고 있는가? • 정보보호 및 개인정보보호 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 지침, 절차, 매뉴얼 등을 수립하고 있는가? • 정보보호 및 개인정보보호 정책·시행문서의 제·개정 시 최고경영자 또는 최고경영자로부터 권한을 위임받은 자의 승인을 받고 있는가? • 정보보호 및 개인정보보호 정책·시행문서의 최신본을 관련 임직원에게 이해하기 쉬운 형태로 제공하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책은 다음 내용을 포함하여 수립하여야 한다.

▶ 조직의 정보보호 및 개인정보보호에 대한 최고경영자 등 경영진의 의지 및 방향

▶ 조직의 정보보호 및 개인정보보호를 위한 역할·책임 및 대상·범위

▶ 조직이 수행하는 관리적·기술적·물리적 정보보호 및 개인정보보호 활동의 근거

■ 정보보호 및 개인정보보호 정책에 명시된 정보보호 및 개인정보보호 사항을 구체적으로 시행하기 위하여 필요한 세부 방법, 절차, 주기, 수행주체 등을 규정하는 지침, 절차, 매뉴얼, 가이드 등의 하위 실행 문서를 조직의 특성에 맞게 수립하여야 한다.

▶ 하위 실행 문서는 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 구체적으로 제시할 수 있어야 하며, 보호 대상 관점 또는 수행주체 관점 등 다양한 관점에서 조직 특성에 맞게 수립

※ 하위 실행 문서(예시)

보호대상 관점	수행주체 관점
• 서버보안 지침 • 네트워크보안 지침 • 데이터베이스보안 지침 • 애플리케이션보안 지침 • 웹서비스 보안 지침 • 클라우드 보안 지침	• 임직원보안 지침 • 개발자보안 지침 • 운영자보안 지침 등

- 정책 및 시행문서(지침, 절차 등)는 조직이 제공하고 있는 서비스, 사업 등에 관련된 개인정보 보호 관련 법적 요구사항(법률, 시행령, 시행규칙, 하위 고시, 가이드 등)을 반영
- 개인정보를 처리하는 경우 개인정보 보호법에 따른 내부 관리계획을 관련 법규에서 요구하는 사항을 모두 포함하여 수립
  - 개인정보 보호법에 따라 내부 관리계획에 포함되어야 하는 사항

1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 그 밖에 개인정보 보호를 위하여 필요한 사항

※ 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략 가능

■ 정보보호 및 개인정보보호 정책·시행문서 제·개정 시 최고경영자 또는 최고경영자로부터 권한을 위임받은 자의 승인을 받아야 한다.

- 정책서와 시행문서를 제·개정하는 경우 이해관계자와 해당 내용을 충분히 협의·검토
- 정책서 및 시행문서 변경으로 인한 조직 업무 및 서비스 영향도, 법적 준거성 등을 고려
- 회의록 등 검토 사항에 대한 기록을 남기고 정책·지침 등에 관련 사항 반영
- 검토가 완료된 정책서 및 시행문서를 경영진에게 보고하고 승인

■ 정보보호 및 개인정보보호 정책·시행문서의 제·개정 시 최신본을 관련 임직원에게 이해하기 쉬운 형태로 제공하여야 한다.

- 임직원 및 외부자가 용이하게 참고할 수 있는 형태(전자게시판, 책자, 교육자료, 매뉴얼 등)로 제공
- 정책서 및 시행문서는 제·개정사항이 발생하면 즉시 공표하고 최신본을 유지

증거자료

예시

- 정보보호 및 개인정보보호 정책·지침·절차서(제·개정 내역 포함)
- 정보보호 및 개인정보보호 정책·지침절차서 제·개정 시 이해관계자 검토 회의록
- 개인정보 내부 관리계획
- 정보보호 및 개인정보보호 정책·지침 제·개정 공지내역(그룹웨어, 사내게시판 등)
- 정보보호 및 개인정보보호 위원회 회의록

결함사례

- 사례 1 : 내부 규정에 따르면 정보보호 및 개인정보보호 정책서 제·개정 시에는 정보보호 및 개인정보보호 위원회의 의결을 거치도록 하고 있으나, 최근 정책서 개정 시 위원회에 안건으로 상정하지 않고 정보보호 최고책임자 및 개인정보 보호책임자의 승인을 근거로만 개정한 경우
- 사례 2 : 정보보호 및 개인정보보호 정책 및 지침서가 최근에 개정되었으나, 해당 사항이 관련 부서 및 임직원에게 공유·전달되지 않아 일부 부서에서는 구버전의 지침서를 기준으로 업무를 수행하고 있는 경우
- 사례 3 : 정보보호 및 개인정보보호 정책 및 지침서를 보안부서에서만 관리하고 있고, 임직원이 열람할 수 있도록 게시판, 문서 등의 방법으로 제공하지 않는 경우

항 목	1.1.6 자원 할당
인증기준	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고 있는가? • 정보보호 및 개인정보보호 관리체계의 효과적 구현과 지속적 운영을 위하여 필요한 자원을 평가하여 필요한 예산과 인력을 지원하고 있는가? • 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립·시행하고, 그 추진결과에 대한 심사분석·평가를 실시하고 있는가?

세부 설명

- 최고경영자는 정보보호 및 개인정보보호 활동을 원활하게 수행하기 위하여 분야별 전문성을 갖춘 인력을 확보하여야 한다.
  - 전문 지식 및 관련 자격 보유(정보보호 및 개인정보보호 관련 학위 또는 자격증 보유)
  - 정보보호 및 개인정보보호 관련 실무 경력 보유
  - 정보보호 및 개인정보보호 관련 직무교육 이수 등
- 최고경영자는 정보보호 및 개인정보보호 관리체계의 효과적 구현과 지속적 운영을 위하여 필요한 자원을 평가하여 필요한 예산과 인력을 지원하여야 한다.
  - 매년 정보보호 및 개인정보보호 관리체계의 효과적 구축 및 지속적 운영을 위하여 필요한 예산과 자원을 평가하여 예산 및 인력운영 계획 수립 및 승인
  - 예산 및 인력운영계획에 따라 필요한 자원(인력, 조직, 예산 등)을 지속적으로 지원
- 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립·시행하고 그 추진결과에 대한 심사분석·평가를 실시하여야 한다.
  - 해당 연도의 정보보호 및 개인정보보호 업무를 효과적으로 수행하기 위한 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립하고 경영진 보고 및 시행
  - 세부추진 계획에 따른 추진결과를 심사분석 및 평가하여 경영진에게 보고

증거자료

예시

- 정보보호 및 개인정보보호 활동 연간 추진계획서(예산 및 인력운영계획)
- 정보보호 및 개인정보보호 활동 결과 보고서
- 정보보호 및 개인정보보호 투자 내역
- 정보보호 및 개인정보보호 조직도

결함사례

- 사례 1 : 정보보호 및 개인정보보호 조직을 구성하는데, 분야별 전문성을 갖춘 인력이 아닌 정보보호 관련 또는 IT 관련 전문성이 없는 인원으로만 보안인력을 구성한 경우
- 사례 2 : 개인정보처리시스템의 기술적·관리적 보호조치의 요건을 갖추기 위한 최소한의 보안 솔루션 도입, 안전조치 적용 등을 위한 비용을 최고경영자가 지원하지 않고 있는 경우
- 사례 3 : 인증을 취득한 이후에 인력과 예산 지원을 대폭 줄이고 기존 인력을 다른 부서로 배치하거나 일부 예산을 다른 용도로 사용하는 경우

1.2. 위험 관리

항 목	1.2.1 정보자산 식별
인증기준	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
주요 확인사항	• 정보자산의 분류기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하고 있는가? • 식별된 정보자산에 대하여 법적 요구사항 및 업무에 미치는 영향 등을 고려하여 중요도를 결정하고 보안등급을 부여하고 있는가? • 정기적으로 정보자산 현황을 조사하여 정보자산목록을 최신으로 유지하고 있는가?

세부 설명

■ 정보자산의 분류기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하여야 한다.

▶ 조직의 특성에 맞게 정보자산의 분류기준을 수립하고, 분류 기준에 따라 정보자산을 빠짐없이 식별

※ 정보자산 분류(예시)

· 자산 유형별 분류 : 서버, 데이터(DBMS), 정보시스템(응용프로그램), 소프트웨어, 네트워크장비, 보안시스템, PC, 정보, 설비, 시설 등

· 자산 유형별 항목(예)

- 서버 : 호스트 명칭, 자산 일련번호, 모델명, 용도, IP주소, 관리 부서명, 관리 실무자, 관리 책임자, 보안등급 등
- 데이터 : 데이터베이스명, 테이블명, (개인)정보 항목명(예: 이름, 성별, 생년월일, 휴대폰번호, 이메일 등), 관리 부서명, 관리 실무자, 관리 책임자, 저장 시스템(호스트 명칭), 저장 위치(IP주소), 보안등급 등
- 정보시스템 : 서버, PC 등 단말기, 보조저장매체, 네트워크 장비, 응용프로그램 등 정보의 수집, 가공, 저장, 검색, 송수신에 필요한 하드웨어 및 소프트웨어
- 보안시스템 : 정보의 훼손, 변조, 유출 등을 방지하기 위하여 구축된 시스템으로 침입차단시스템, 침입탐지시스템, 침입방지시스템, 개인정보유출방지시스템 등을 포함
- 정보 : 문서적 정보와 전자적 정보 모두를 포함(중요정보, 개인정보 등)

▶ 자산명, 용도, 위치, 책임자 및 관리자, 관리 부서 등의 자산정보를 확인하여 목록 작성

▶ 정보자산의 효율적 관리를 위하여 자산관리시스템 활용 또는 문서(엑셀) 등 다양한 형태로 관리

▶ 클라우드 서비스를 이용하는 경우, 클라우드 서비스의 특성을 반영한 분류기준(예를 들어, 가상서버, 오브젝트 스토리지 등)을 마련하고 이에 따라 클라우드 자산을 식별·관리

■ 식별된 정보자산에 대한 법적 요구사항 및 업무에 미치는 영향 등을 고려하여 중요도를 결정하고 보안등급을 부여하여야 한다.

▶ 법적 요구사항이나 업무에 미치는 영향 등 각 자산 특성에 맞는 보안등급 평가기준 결정

※ 보안등급 산정기준(예시)
· 기밀성, 무결성, 가용성, 법적 준거성 등에 따른 중요도 평가
· 서비스 영향, 이익손실, 고객 상실, 대외 이미지 손상 등도 고려

▶ 보안등급 평가기준에 따라 정보자산별 보안등급 산정 및 목록으로 관리

■ 정기적으로 정보자산 현황을 조사하여 정보자산목록을 최신으로 유지하여야 한다.

▶ 신규 도입, 변경, 폐기되는 자산 현황을 확인할 수 있도록 절차 마련

▶ 정기적으로 정보자산 현황 조사를 수행하고 정보자산목록을 최신으로 유지

증거자료

예시

- 정보자산 및 개인정보 자산분류 기준
- 정보자산 및 개인정보 자산목록(자산관리시스템 화면)
- 정보자산 및 개인정보 보안등급
- 자산실사 내역
- 위험분석 보고서(자산식별 내역)

결함사례

- 사례 1 : 정보보호 및 개인정보보호 관리체계 범위 내의 자산 목록에서 중요정보 취급자 및 개인정보 취급자 PC를 통제하는 데 사용되는 출력물 보안, 문서암호화, USB매체제어 등의 내부정보 유출통제 시스템이 누락된 경우
- 사례 2 : 정보보호 및 개인정보보호 관리체계 범위 내에서 제3자로부터 제공받은 개인정보가 있으나, 해당 개인정보에 대한 자산 식별이 이루어지지 않은 경우
- 사례 3 : 내부 지침에 명시된 정보자산 및 개인정보 보안등급 분류 기준과 자산관리 대장의 분류 기준이 일치하지 않은 경우
- 사례 4 : 온프레미스 자산에 대해서는 식별이 이루어졌으나, 외부에 위탁한 IT 서비스(웹호스팅, 서버호스팅, 클라우드 등)에 대한 자산 식별이 누락된 경우(단, 인증범위 내)
- 사례 5 : 고유식별정보 등 개인정보를 저장하고 있는 백업서버의 기밀성 등급을 (하)로 산정하는 등 정보자산 중요도 평가의 합리성 및 신뢰성이 미흡한 경우

항 목	1.2.2 현황 및 흐름분석
인증기준	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
주요 확인사항	• 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화하고 있는가? • 관리체계 범위 내 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여 개인정보 흐름도 등으로 문서화하고 있는가? • 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 개인정보 흐름을 주기적으로 검토하여 흐름도 등 관련 문서의 최신성을 유지하고 있는가?

세부 설명

■ 현황 및 흐름분석은 위험분석의 사전단계로 다양한 관점에서 위험분석을 진행할 수 있는 기초자료가 된다. 또한 경영진이 정보보호 현황을 이해하고 위험관리를 위한 의사결정을 내리는 데 효과적으로 활용할 수 있다.

▶ 현황분석은 인증기준과 운영현황을 비교하는 GAP 분석표를 통하여 인증기준과 운영현황과의 차이를 확인

▶ 흐름분석은 정보서비스 흐름분석과 개인정보 처리단계별 흐름분석으로 구분되며, 그 결과는 흐름표 또는 흐름도로 도식화

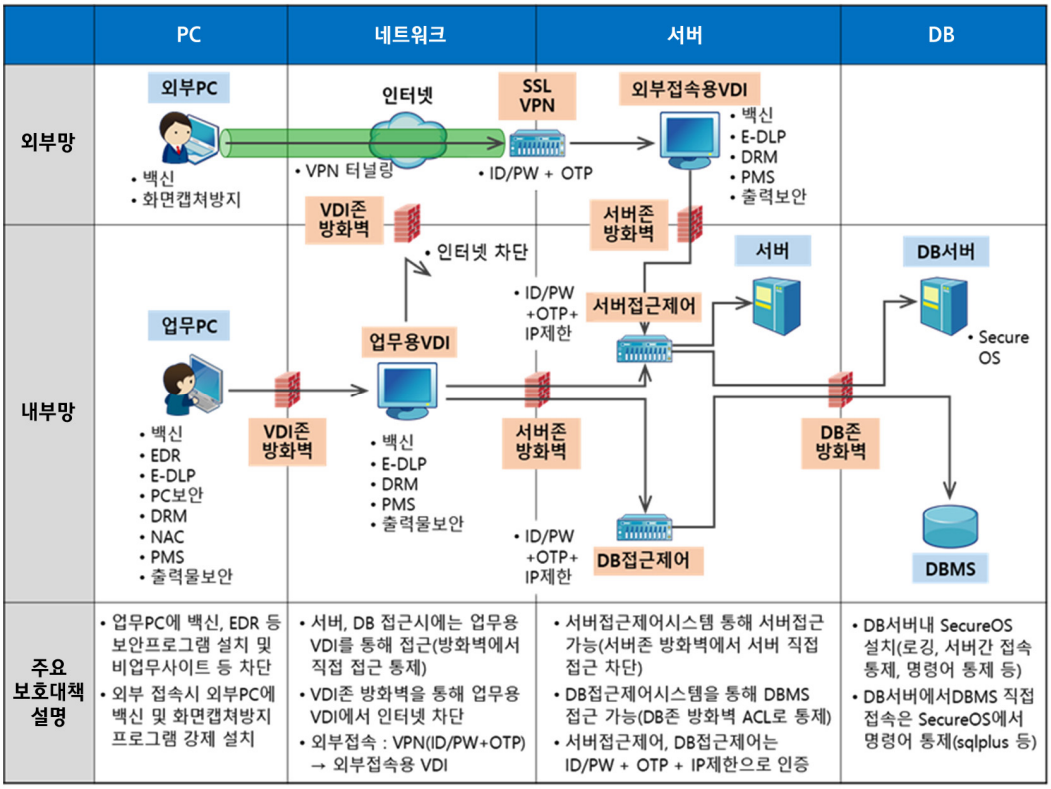
※ 정보서비스 흐름도는 조직의 업무절차, 정보보호 요구사항, 보안통제의 상호연계를 사용자 기반으로 도식화한 접근통제 개념도를 의미함

※ 개인정보 흐름도는 수집, 보유, 이용·제공, 파기되는 개인정보 처리단계별로 흐름을 한눈에 확인할 수 있도록 도식화한 개념도를 의미함

■ 관리체계 전 영역에 대한 정보서비스 현황을 식별하고, 업무 절차와 흐름을 파악하여 문서화하여야 한다.

- 관리체계 범위 내의 모든 정보서비스 현황 식별
- 정보서비스별 업무 절차 및 흐름 파악
- 업무 절차 및 흐름에 대한 문서화 : 업무현황표, 업무흐름도 등

• 정보서비스 흐름도(시스템 운영자 예시)



■ 관리체계 범위 내 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여 개인정보 흐름표, 개인정보 흐름도 등으로 문서화하여야 한다(ISMS-P 인증인 경우).

▶ (1단계) 개인정보 처리가 이루어지는 단위 업무를 식별

▶ (2단계) 각 단위 업무에 대한 개인정보 생명주기별 개인정보 흐름표 작성

※ 개인정보 흐름표 작성 예시(출처 : 개인정보 영향평가 수행안내서)

• 수집 흐름표 예시

업무명	수집					
	수집항목	수집경로	수집대상	수집주기	수집담당자	수집근거
회원관리 (회원가입)	필수: 성명, 생년월일, 성별, 장애 구분, 회원ID, 비밀번호, 주소 직업, 전화번호, 휴대전화, 이메일, 선택: OOO, 장애인증명파일, OOO성명, 관심분야, OOO, 인근OOO정보	홈페이지 (온라인)	정보주체	수시	홈페이지 담당자	정보주체 동의

• 보유·이용 흐름표 예시

업무명	보유, 이용					
	보유 형태	암호화 항목	이용항목	이용목적	개인정보 취급자	이용방법
회원관리 (회원가입)	DB	비밀번호 (SHA-256)	필수: 성명, 생년월일, 성별, 장애 구분, 회원ID, 비밀번호, 주소 직업, 전화번호, 휴대전화, 이메일, 선택: OOO, 장애인증명파일, OOO성명, 관심분야, OOO, 인근OOO정보	담당자가 회원 정보를 관리	홈페이지 담당자	개인 PC를 이용하여 홈페이지에 접속한 후 해당메뉴 선택하여 회원정보 조회

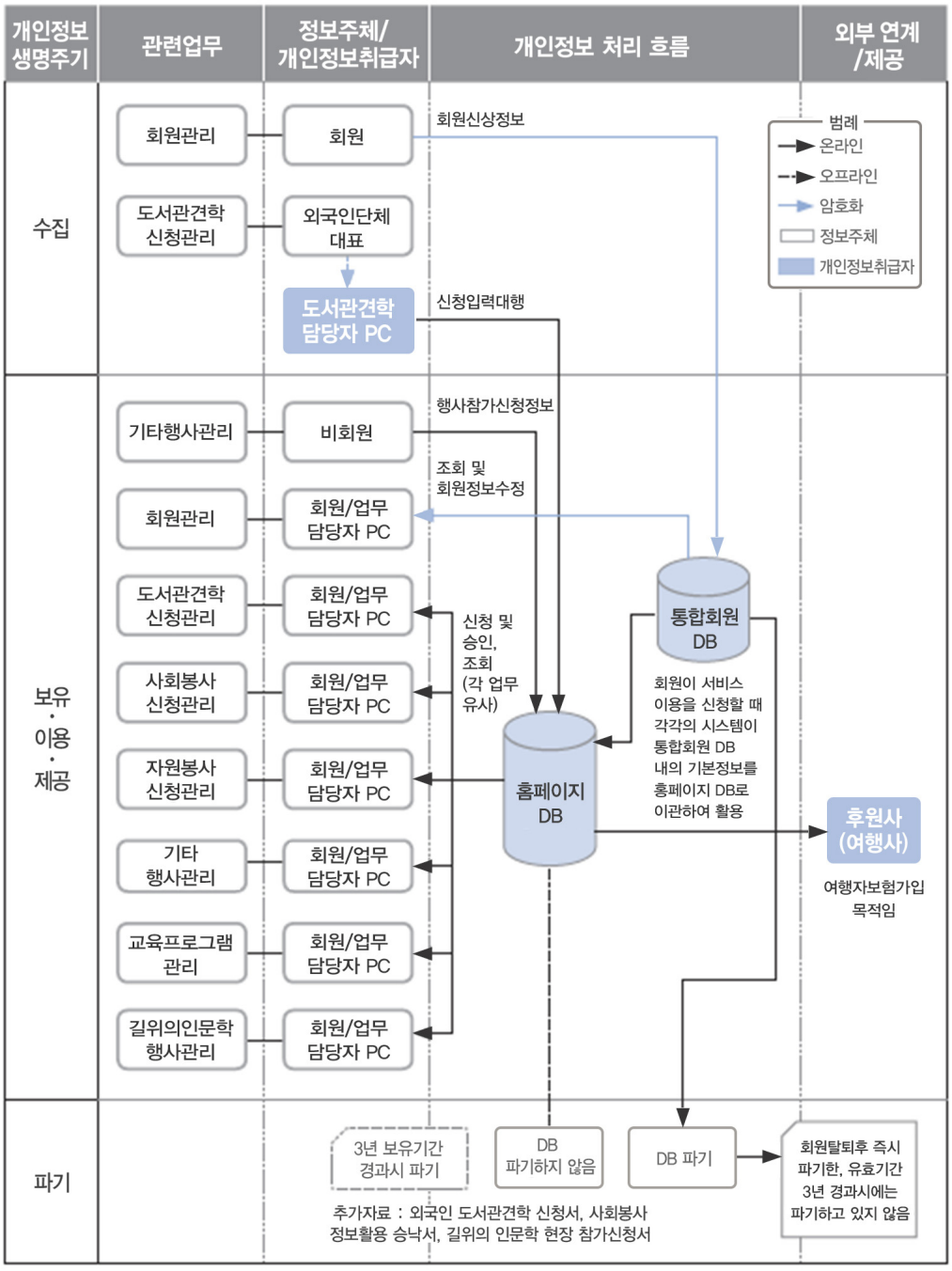
• 파기 흐름표 예시

업무명	파기			
	보관기관	파기담당자	파기절차	분리보관
회원관리(회원가입)	회원탈퇴 후 지체없이 삭제 또는 최대3년	홈페이지 담당자	목적 달성시 테이블에서 해당 레코드 삭제. 그러나 기간경과 후 파기하지 않음	

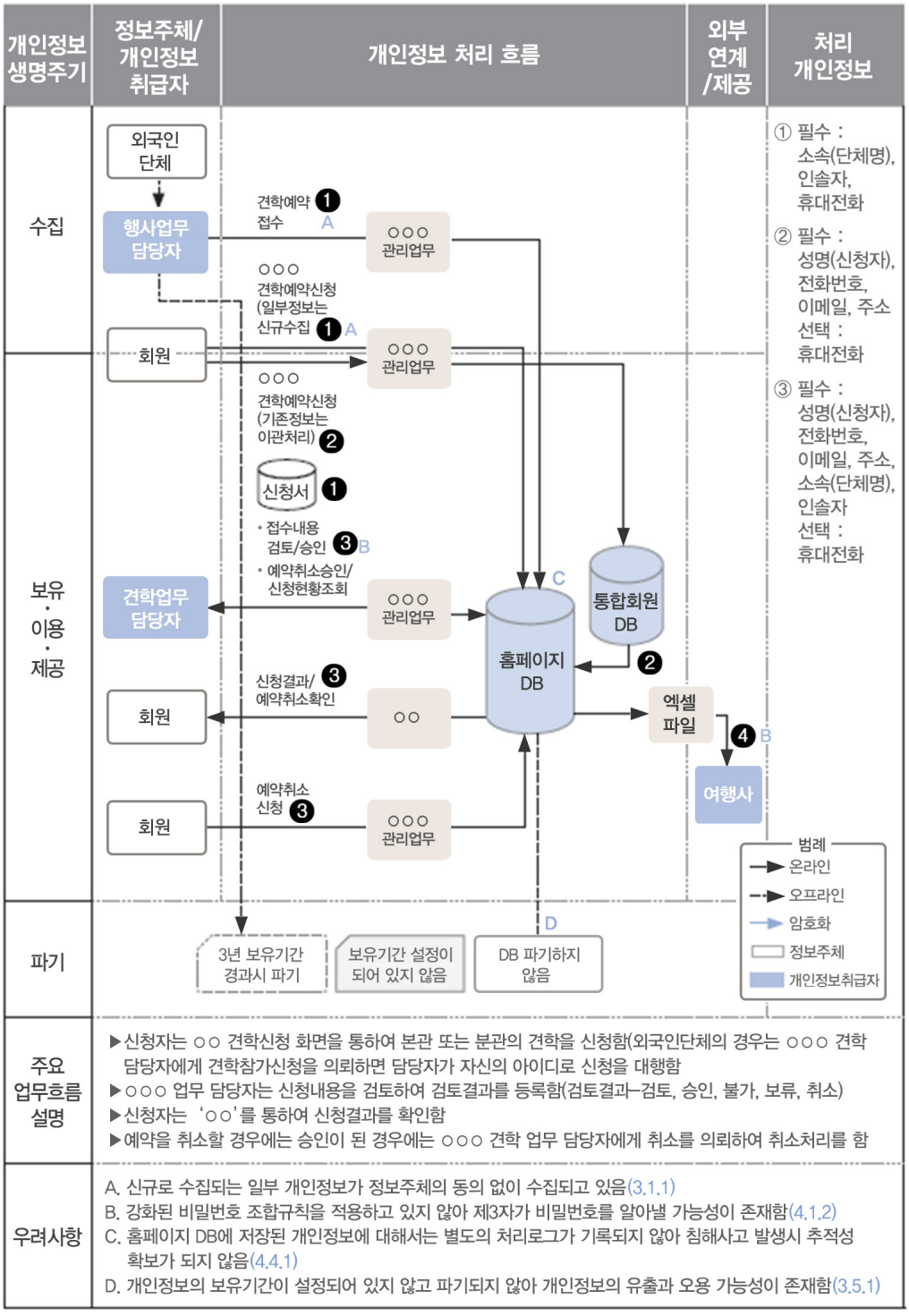
▶ (3단계) 작성된 개인정보 흐름표를 기반으로 수집, 보유, 이용·제공, 파기되는 개인정보 처리 단계별로 흐름을 한눈에 파악할 수 있도록 총괄 개인정보 흐름도 및 업무별 개인정보 흐름도 작성

※ 개인정보 흐름도 작성 예시(출처 : 개인정보 영향평가 수행안내서)

• 개인정보 흐름도 예시 – 총괄(통합) 흐름도



• 업무별 개인정보 흐름도(상세) 예시



- 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 개인정보 흐름을 다음 관점을 참고하여 주기적으로(최소 연 1회 이상) 검토하고, 최신성이 유지되도록 관리하여야 한다.
  - 기존 서비스, 업무 및 개인정보 흐름의 변화 여부(신규 서비스 오픈 또는 개편, 업무절차의 변경, 개인정보 처리 방법 변화, 조직의 변경, 외부 연계 및 제공 흐름 변경 등)
  - 처리되는 중요정보, 개인정보 항목의 변화 여부
  - 정보시스템 및 개인정보처리시스템의 종류, 구성, 기능 등의 변경 여부
  - 신규 개인정보 처리업무 및 흐름 발생 여부
  - 법규 개정, 신규 취약점의 발생 등 외부 환경의 변화 여부 등

증거자료

예시

- 정보서비스 현황표
- 정보서비스 업무흐름표·업무흐름도
- 개인정보 처리 현황표(ISMS-P 인증인 경우)
- 개인정보 흐름표·흐름도(ISMS-P 인증인 경우)

결함사례

- 사례 1 : 관리체계 범위 내 주요 서비스의 업무 절차·흐름 및 현황에 문서화가 이루어지지 않은 경우
- 사례 2 : 개인정보 흐름도를 작성하였으나, 실제 개인정보의 흐름과 상이한 부분이 다수 존재하거나 중요한 개인정보 흐름이 누락되어 있는 경우
- 사례 3 : 최초 개인정보 흐름도 작성 이후에 현행화가 이루어지지 않아 변화된 개인정보 흐름이 흐름도에 반영되지 않고 있는 경우

항 목	1.2.3 위험 평가
인증기준	조직의 대내외 환경분석을 통하여 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.
주요 확인사항	• 조직 또는 서비스의 특성에 따라 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하고 있는가? • 위험관리 방법 및 절차(수행인력, 기간, 대상, 방법, 예산 등)를 구체화한 위험관리계획을 매년 수립하고 있는가? • 위험관리계획에 따라 연 1회 이상 정기적으로 또는 필요한 시점에 위험평가를 수행하고 있는가? • 조직에서 수용 가능한 목표 위험수준을 정하고, 그 수준을 초과하는 위험을 식별하고 있는가? • 위험식별 및 평가 결과를 경영진에게 보고하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

- 조직의 특성을 반영하여 관리적·기술적·물리적·법적 분야 등 다양한 측면에서 발생할 수 있는 정보보호 및 개인정보보호 관련 위험을 식별하고 평가할 수 있도록 위험평가 방법을 정의하고 문서화하여야 한다.
  - 위험평가 방법 선정 : 베이스라인 접근법, 상세위험 분석법, 복합 접근법, 위협 및 시나리오 기반 등
  - 비즈니스 및 조직의 특성 반영 : 조직의 비전 및 미션, 비즈니스 목표, 서비스 유형, 컴플라이언스 등
  - 다양한 관점 고려 : 해킹, 내부자 유출, 외부자 관리·감독 소홀, 개인정보 관련 법규 위반 등
  - 최신 취약점 및 위협동향 고려
  - 위험평가 방법론은 조직의 특성에 맞게 자체적으로 정하여 적용할 수 있으나, 위험평가의 과정은 합리적이어야 하고, 위험평가 결과는 실질적인 위험의 심각성을 대변할 수 있어야 함
- 위험관리 방법 및 절차(수행인력, 기간, 대상, 방법, 예산 등)를 구체화한 위험관리계획을 수립하여야 한다.
  - 수행인력 : 위험관리 전문가, 정보보호·개인정보보호 전문가, 법률 전문가, IT 실무 책임자, 현업부서 실무 책임자, 외부 전문컨설턴트 등 참여(이해관계자의 참여 필요)
  - 기간 : 최소 연 1회 이상 수행될 수 있도록 일정 수립
  - 대상 : 인증 범위 내 모든 서비스 및 자산(정보자산, 개인정보, 시스템, 물리적 시설 등) 포함
  - 방법 : 조직의 특성을 반영한 위험평가 방법론 정의
  - 예산 : 위험 식별 및 평가 시행을 위한 예산 계획을 매년 수립하고 정보보호 최고책임자 등 경영진 승인

- 위험관리계획에 따라 정보보호 및 개인정보보호 관리체계 범위 전 영역에 대한 위험평가를 연 1회 이상 정기적으로 또는 필요한 시점에 수행하여야 한다.
  - 사전에 수립된 위험관리 방법 및 계획에 따라 체계적으로 수행
  - 위험평가는 연 1회 이상 정기적으로 수행하되 조직의 변화, 신규시스템 도입 등 중요한 사유가 발생한 경우 해당 부분에 대하여 정기적인 위험평가 이외에 별도로 위험평가 수행
  - 서비스 및 정보자산의 현황과 흐름분석 결과 반영
  - 최신 법규를 기반으로 정보보호 및 개인정보보호 관련 법적 요구사항 준수 여부 확인
  - 정보보호 및 개인정보보호 관리체계 인증기준의 준수 여부 확인
  - 기 적용된 정보보호 및 개인정보보호 대책의 실효성 검토 포함
- 조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별하여야 한다.
  - 각종 위험이 조직에 미치는 영향(발생가능성, 심각도 등)을 고려하여 위험도 산정기준 마련
  - 위험도 산정기준에 따라 식별된 위험에 대하여 위험도 산정
  - 수용 가능한 목표 위험수준(DoA, Degree of Assurance)을 정보보호 최고책임자, 개인정보 보호책임자 등 경영진의 의사결정에 의하여 결정
  - 수용 가능한 목표 위험수준을 초과하는 위험을 식별하고 문서화
- 위험 식별 및 평가 결과를 정보보호 최고책임자, 개인정보 보호책임자 등 경영진이 이해하기 쉽게 작성하여 보고하여야 한다.
  - 식별된 위험에 대한 평가보고서 작성
  - 식별된 위험별로 관련된 이해관계자에게 내용 공유 및 논의(실무 협의체, 위원회 등)
  - IT, 법률적 전문 용어보다는 경영진의 눈높이에서 쉽게 이해하고 의사 결정할 수 있도록 보고서를 작성하여 보고

증거자료

예시

- 위험관리 지침
- 위험관리 매뉴얼·가이드
- 위험관리 계획서
- 위험평가 결과보고서
- 정보보호 및 개인정보보호 위원회 회의록
- 정보보호 및 개인정보보호 실무 협의회 회의록
- 정보자산 및 개인정보자산 목록
- 정보서비스 및 개인정보 흐름표·흐름도

결함사례

- 사례 1 : 수립된 위험관리계획서에 위험평가 기간 및 위험관리 대상과 방법이 정의되어 있으나, 위험관리 수행 인력과 소요 예산 등 구체적인 실행계획이 누락되어 있는 경우
- 사례 2 : 전년도에는 위험평가를 수행하였으나, 금년도에는 자산 변경이 없었다는 사유로 위험 평가를 수행하지 않은 경우
- 사례 3 : 위험관리 계획에 따라 위험 식별 및 평가를 수행하고 있으나, 범위 내 중요 정보자산에 대한 위험 식별 및 평가를 수행하지 않았거나, 정보보호 관련 법적 요구 사항 준수 여부에 따른 위험을 식별 및 평가하지 않은 경우
- 사례 4 : 위험관리 계획에 따라 위험 식별 및 평가를 수행하고 수용 가능한 목표 위험수준을 설정하였으나, 관련 사항을 경영진(정보보호 최고책임자 등)에 보고하여 승인받지 않은 경우
- 사례 5 : 내부 지침에 정의한 위험 평가 방법과 실제 수행한 위험 평가 방법이 상이할 경우
- 사례 6 : 정보보호 관리체계와 관련된 관리적·물리적 영역의 위험 식별 및 평가를 수행하지 않고, 단순히 기술적 취약점진단 결과를 위험 평가 결과로 갈음하고 있는 경우
- 사례 7 : 수용 가능한 목표 위험수준(DoA)을 타당한 사유 없이 과도하게 높이는 것으로 결정함에 따라, 실질적으로 대응이 필요한 주요 위험들이 조치가 불필요한 위험(수용 가능한 위험)으로 지정된 경우

항 목	1.2.4 보호대책 선정
인증기준	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
주요 확인사항	• 식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 보호대책을 선정하고 있는가? • 보호대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호대책 이행계획을 수립하고 경영진에 보고하고 있는가?

세부 설명

■ 식별된 위험에 대한 처리 전략(위험감소, 위험회피, 위험전가, 위험수용 등)을 수립하고, 이에 따라 위험별로 위험처리를 위한 적절한 정보보호 및 개인정보보호 대책을 선정하여야 한다.

▶ 위험수준 감소를 목표로 위험 처리전략을 수립하는 것이 일반적이며, 상황에 따라 위험회피, 위험전가, 위험수용의 전략 고려

※ 위험처리 전략(예시)

· 위험감소 : 패스워드 도용의 위험을 줄이기 위하여 개인정보처리시스템의 로그인 패스워드 복잡도와 길이를 3가지 문자조합 및 8글자 이상으로 강제 설정되도록 패스워드 설정모듈을 개발하여 적용한다.

· 위험회피 : 회사 홍보용 인터넷 홈페이지에서는 회원 관리에 따른 위험이 크므로 회원 가입을 받지 않는 것으로 변경하고 기존 회원정보는 모두 파기한다.

· 위험전가 : 중요정보 및 개인정보 유출 시 손해배상 소송 등에 따른 비용 손실을 줄이기 위하여 관련 보험에 가입한다.

· 위험수용 : 유지보수 등 협력업체, 개인정보 처리 수탁자 중 당사에서 직접 관리·감독할 수 없는 PG사, 본인확인기관 등과 같은 대형 수탁자에 대하여는 해당 수탁자가 법령에 의한 정부감독을 받거나 정부로부터 보안인증을 획득한 경우에는 개인정보 보호법에 따른 문서체결 이외의 별도 관리·감독은 생략할 수 있도록 한다.

▶ 보호대책을 선정할 때에는 정보보호 및 개인정보보호 대책은 정보보호 및 개인정보보호 관리체계 인증기준과의 연계성 고려

▶ 불가피한 사유가 있는 경우에는 위험수용 전략을 선택할 수 있으나 무조건적인 위험수용은 지양하여야 하며, 불가피한 사유의 적정성, 보완대책 적용가능성 등을 충분히 검토한 후 명확하고 객관적인 근거에 기반하여 위험수용 전략 선택

▶ 법률 위반에 해당하는 위험은 수용 가능한 위험에 포함되지 않도록 주의

▶ 수용 가능한 위험수준을 초과하지 않은 위험 중 내·외부 환경의 변화에 따라 위험수준이 상승할 가능성이 높거나 조직이 중요하다고 판단하는 부분에 대해서는 보호대책 수립 고려

■ 정보보호 및 개인정보보호 대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호대책 이행계획을 수립하고, 정보보호 최고책임자 및 개인정보 보호책임자 등 경영진에 보고하여야 한다.

- ▶ 위험의 심각성 및 시급성, 구현의 용이성, 예산 할당, 자원의 가용성, 선후행 관계 등을 고려하여 우선순위 결정
- ▶ 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 정보보호 및 개인정보보호 대책 이행계획을 수립하여 경영진에게 보고 및 승인

증거자료

예시

- 정보보호 및 개인정보보호 이행계획서·위험관리계획서
- 정보보호 및 개인정보보호 대책서
- 정보보호 및 개인정보보호 마스터플랜
- 정보보호 및 개인정보보호 이행계획 경영진 보고 및 승인 내역

결함사례

- 사례 1 : 정보보호 및 개인정보보호 대책에 대한 이행계획은 수립하였으나, 정보보호 최고책임자 및 개인정보 보호책임자에게 보고가 이루어지지 않은 경우
- 사례 2 : 위험감소가 요구되는 일부 위험의 조치 이행계획이 누락되어 있는 경우
- 사례 3 : 법에 따라 의무적으로 이행하여야 할 사항, 보안 취약성이 높은 위험 등을 별도의 보호조치 계획 없이 위험수용으로 결정하여 조치하지 않은 경우
- 사례 4 : 위험수용에 대한 근거와 타당성이 미흡하고, 시급성 및 구현 용이성 등의 측면에서 즉시 또는 단기 조치가 가능한 위험요인에 대해서도 특별한 사유 없이 장기 조치계획으로 분류한 경우

1.3. 관리체계 운영

항 목	1.3.1 보호대책 구현
인증기준	선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
주요 확인사항	• 이행계획에 따라 보호대책을 효과적으로 구현하고 이행결과의 정확성 및 효과성 여부를 경영진이 확인할 수 있도록 보고하고 있는가? • 관리체계 인증기준별로 보호대책 구현 및 운영 현황을 기록한 운영명세서를 구체적으로 작성하고 있는가?

세부 설명

- 이행계획에 따라 선정된 보호대책을 효과적으로 구현하고 그 이행결과를 정보보호 최고책임자, 개인정보 보호책임자 등 경영진에게 보고하여 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.
  - 이행계획에 따른 진행경과에 대하여 정기적으로 완료 여부, 진행 사항, 미이행 또는 지연이 있는 경우 사유 등을 파악하여 정보보호 최고책임자, 개인정보 보호책임자 등 경영진에게 보고
  - 경영진은 정보보호 및 개인정보보호 대책이 이행계획에 따라 정확하고 효과적으로 이행되었는지 여부를 검토
  - 미이행, 일정지연 등이 발생한 경우 이에 대한 원인을 분석하여 필요시 이행계획을 변경하고 경영진에게 보고 및 승인
  - 구현 결과에 대한 효과성 및 정확성 검토 결과 적절한 대책으로 판단하기 어렵거나 효과성에 상당한 의문이 제기되는 경우 대안을 수립하거나 추가 위험평가를 통하여 보완할 수 있는 절차 마련
- 관리체계 인증기준별 보호대책 구현 및 운영 현황을 기록한 운영명세서를 구체적으로 작성하여야 한다.
  - 인증기준 선정 여부(Yes/No) 확인 : '관리체계 수립 및 운영' 영역은 필수사항
  - 운영 현황 : 해당기관의 정책 및 인증기준 대비 운영 현황을 상세히 기재
  - 관련문서(정책, 지침 등) : 해당 기준에 해당되는 관련 문서명과 세부 문서번호를 명확히 기재
  - 기록(증거자료) : 관련 문서, 결재 내용, 회의록 등 해당 기준이 실제 운영되는 과정에서 생성되는 문서 또는 증거자료 제시
  - 인증기준 미선정 시 사유 : 인증범위 내의 서비스, 시스템 등이 해당 항목에 전혀 관련이 없는 경우에 미선정 사유를 상세하게 기입

증거자료

예시

- 정보보호 및 개인정보보호 이행계획서·위험관리계획서
- 정보보호 및 개인정보보호 대책서
- 정보보호 및 개인정보보호 이행계획 경과보고서(경영진 보고 포함)
- 정보보호 및 개인정보보호 이행 완료 보고서(경영진 보고 포함)
- 정보보호 및 개인정보보호 운영명세서

결함사례

- 사례 1 : 정보보호 및 개인정보보호 대책에 대한 이행완료 결과를 정보보호 최고책임자 및 개인정보보호책임자에게 보고하지 않은 경우
- 사례 2 : 위험조치 이행결과보고서는 '조치 완료'로 명시되어 있으나, 관련된 위험이 여전히 존재하거나 이행결과의 정확성 및 효과성이 확인되지 않은 경우
- 사례 3 : 전년도 정보보호대책 이행계획에 따라 중·장기로 분류된 위험들이 해당연도에 구현이 되고 있지 않거나 이행결과를 경영진이 검토 및 확인하고 있지 않은 경우
- 사례 4 : 운영명세서에 작성된 운영 현황이 실제와 일치하지 않고, 운명명세서에 기록되어 있는 관련 문서, 결재 내용, 회의록 등이 존재하지 않는 경우
- 사례 5 : 이행계획 시행에 대한 결과를 정보보호 최고책임자 및 개인정보 보호책임자에게 보고하였으나, 일부 미이행된 건에 대한 사유 보고 및 후속 조치가 이루어지지 않은 경우

항 목	1.3.2 보호대책 공유
인증기준	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.
주요 확인사항	• 구현된 보호대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하고 있는가? • 구현된 보호대책을 운영 또는 시행할 부서 및 담당자에게 관련 내용을 공유 또는 교육하고 있는가?

세부 설명

■ 구현된 보호대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하여야 한다.

※ 보호대책의 운영 또는 시행 부서(예시)
· 인프라 운영부서 : 서버 및 네트워크 장비 보안설정, 인프라 운영자 계정관리·권한관리 등
· 개발 부서 : 개발보안, 소스코드보안, 개발환경에 대한 접근 등
· 개인정보 취급부서 : 취급자 권한 관리(응용프로그램), 개인정보 파기, PC 저장 시 암호화 등
· 정보보호 운영부서 : 접근통제 장비 운영, 보안 모니터링 등
· 인사부서 : 퇴직자 보안관리 등

■ 정보보호 및 개인정보보호 관리체계를 내재화하기 위하여 구현된 보호대책을 운영 또는 시행할 부서 및 담당자에게 관련 내용을 공유 또는 교육하여야 한다.

▶ 공유 내용 : 정보보호 및 개인정보보호 정책과 시행문서의 제·개정 사항, 정보보호 및 개인정보보호 대책 이행계획 및 구현결과, 보안시스템 신규 도입 및 개선사항 등

▶ 공유 대상 : 해당 정책·지침 및 보호대책을 실제 운영 또는 시행할 부서 및 담당자

▶ 공유 방법 : 게시판 및 이메일 공지(간단한 이슈인 경우), 회의, 설명회, 교육 등

증거자료

예시

- 정보보호 및 개인정보보호 대책별 운영부서 또는 시행부서 현황
- 정보보호 및 개인정보 관리계획 내부공유 증거자료(공지 내역, 교육자료, 공유 자료 등)

결함사례

- 사례 1 : 정보보호대책을 마련하여 구현하고 있으나, 관련 내용을 충분히 공유·교육하지 않아 실제 운영 또는 수행 부서 및 담당자가 해당 내용을 인지하지 못하고 있는 경우

항 목	1.3.3 운영현황 관리
인증기준	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
주요 확인사항	• 관리체계 운영을 위하여 주기적 또는 상시적으로 수행하여야 하는 정보보호 및 개인정보보호 활동을 문서화하여 관리하고 있는가? • 경영진은 주기적으로 관리체계 운영활동의 효과성을 확인하고 이를 관리하고 있는가?
관련 법규	• 개인정보 보호법 제31조(개인정보 보호책임자의 지정) • 정보통신망법 제45조의3(정보보호 최고책임자의 지정 등)

세부 설명

■ 관리체계의 효과적인 운영을 위하여 일·주·월·분기·반기·년 단위의 주기적 또는 상시적인 활동이 요구되는 정보보호 및 개인정보보호 활동을 식별하고, 그 운영현황을 쉽게 확인할 수 있도록 수행 주기 및 시점, 수행 주체(담당부서, 담당자) 등을 정의한 문서(운영현황표)를 작성하여 관리하여야 한다.

※ 주기적인 정보보호 및 개인정보보호 활동(예시)
- 주요직무자, 개인정보취급자의 접속기록 검토
- 주요직무자의 접근권한 검토
- 정기 정보보호 및 개인정보보호 위원회 개최
- 정보보호 및 개인정보보호 교육
- 사무실 보안점검
- 정보보호 및 개인정보보호 정책·지침 개정 검토
- 법적 준거성 검토
- 침해 대응 모의훈련, IT 재해 복구 모의훈련
- 내부감사 등

■ 경영진은 주기적으로 관리체계 운영활동의 효과성을 확인하고, 문제점이 발견된 경우 이를 개선하는 등 관리하여야 한다.

▶ 관리체계 운영활동이 운영현황표에 따라 주기적·상시적으로 이루어지고 있는지 정기적으로 확인하여 경영진에게 보고

▶ 경영진은 관리체계 운영활동의 효과성을 평가하여 필요시 개선 조치(수행주체 변경, 수행 주기 조정, 운영활동의 추가·변경·삭제 등)

증거자료

예시

- 정보보호 및 개인정보보호 연간계획서
- 정보보호 및 개인정보보호 운영현황표
- 정보보호 및 개인정보보호 활동 수행 여부 점검 결과

결함사례

- 사례 1 : 정보보호 및 개인정보보호 관리체계 운영현황 중 주기적 또는 상시적인 활동이 요구되는 활동 현황을 문서화하지 않은 경우
- 사례 2 : 정보보호 및 개인정보보호 관리체계 운영현황에 대한 문서화는 이루어졌으나, 해당 운영현황에 대한 주기적인 검토가 이루어지지 않아 월별 및 분기별 활동이 요구되는 일부 정보보호 및 개인정보보호 활동이 누락되었고 일부는 이행 여부를 확인할 수 없는 경우

1.4. 관리체계 점검 및 개선

항 목	1.4.1 법적 요구사항 준수 검토
인증기준	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
주요 확인사항	• 조직이 준수하여야 하는 정보보호 및 개인정보보호 관련 법적 요구사항을 파악하여 최신성을 유지하고 있는가? • 법적 요구사항의 준수 여부를 연 1회 이상 정기적으로 검토하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 조직이 준수하여야 하는 정보보호 및 개인정보보호 관련 법적 요구사항을 파악하여 최신성을 유지하여야 한다.

▶ 조직이 준수하여야 하는 정보보호 및 개인정보보호 관련 법규 파악

※ 정보보호 및 개인정보보호 관련 법률(예시)
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 보호법
- 신용정보의 이용 및 보호에 관한 법률
- 위치정보의 보호 및 이용 등에 관한 법률
- 전자금융거래법
- 전자상거래 등에서의 소비자보호에 관한 법률
- 저작권법
- 정보통신기반 보호법
- 전자서명법
- 산업기술의 유출방지 및 보호에 관한 법률
- 부정경쟁방지 및 영업비밀보호에 관한 법률
- 정보보호산업의 진흥에 관한 법률
- 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률
- 전자정부법
- 소프트웨어 진흥법
- 통신비밀보호법
- 전기통신사업법
- 특정 금융거래정보의 보고 및 이용 등에 관한 법률
- 가상자산 이용자 보호 등에 관한 법률 등

▶ 관련 법규의 제·개정 현황을 지속적으로 모니터링하여 제·개정이 이루어질 경우 조직에 미치는 영향을 분석하고 필요시 내부 정책·지침 및 체크리스트 등에 반영하여 최신성 유지

▶ [참고] 정보보호 공시 제도

· 근거 : 정보보호산업법 제13조(정보보호 공시) 및 동법 시행령 제8조
· 공시내용 : ▲정보보호 투자 현황, ▲정보보호 인력 현황, ▲정보보호 관련 인증·평가·점검 등에 관한 사항, ▲정보보호 활동을 정보보호 현황 서식에 작성
· 공시기한 : 매년 6월 30일까지 정보보호 현황 제출(자율·의무공시)
· 정보보호 공시 의무대상 기준(다만 공공기관, 소기업, 금융회사, 일부 전자금융업자는 예외)

사업분야	· 회선설비 보유 기간통신사업자(ISP)	※ 전기통신사업법 제6조제1항
	· 집적정보 통신시설 사업자(IDC)	※ 정보통신망법 제46조
	· 상급종합병원	※ 의료법 제3조의4
	· 클라우드컴퓨팅 서비스제공자	※ 클라우드컴퓨팅법 시행령 제3조제1호
매출액	· 정보보호 최고책임자 지정·신고 상장법인 중 매출액 3,000억 원 이상	
이용자 수	· 정보통신서비스 일일평균 이용자 수 100만 명 이상(전년도 말 직전 3개월간)	

■ 법적 요구사항의 준수 여부를 연 1회 이상 정기적으로 검토하여야 한다.

▶ 법적 요구사항의 준수 여부를 정기적으로 검토할 수 있는 절차 수립(검토 주기, 대상, 담당자, 방법 등) 및 이행

▶ 법적 요구사항 준수 검토 결과 발견된 문제점에 대하여 신속하게 개선조치

증거자료

예시

- 법적 준거성 검토 내역
- 정보보호 및 개인정보보호 정책·지침 검토 및 개정이력
- 정책·지침 신구대조표
- 법 개정사항 내부공유 자료
- 개인정보 손해배상 책임보장 입증 자료(사이버보험 약정서 등)
- 정보보호 공시 내역

결함사례

- 사례 1 : 정보통신망법 및 개인정보 보호법이 최근 개정되었으나 개정사항이 조직에 미치는 영향을 검토하지 않았으며, 정책서·시행문서 및 법적준거성 체크리스트 등에도 해당 내용을 반영하지 않아 정책서·시행문서 및 법적준거성 체크리스트 등의 내용이 법령 내용과 일치하지 않은 경우
- 사례 2 : 조직에서 준수하여야 할 법률이 개정되었으나, 해당 법률 준거성 검토를 장기간 수행하지 않은 경우
- 사례 3 : 법적 준거성 준수 여부에 대한 검토가 적절히 이루어지지 않아 개인정보 보호법 등 법규 위반 사항이 다수 발견된 경우
- 사례 4 : 개인정보 보호법에 따라 개인정보 손해배상책임 보장제도 적용 대상이 되었으나, 이를 인지하지 못하여 보험 가입이나 준비금 적립을 하지 않은 경우 또는 보험 가입을 하였으나 이용자 수 및 매출액에 따른 최저가입금액 기준을 준수하지 못한 경우
- 사례 5 : 정보보호 공시 의무대상 사업자이지만 법에 정한 시점 내에 정보보호 공시가 시행되지 않은 경우
- 사례 6 : 모바일앱을 통해 위치정보사업자로부터 이용자의 개인위치정보를 전송받아 서비스에 이용하고 있으나, 위치기반서비스사업 신고를 하지 않은 경우
- 사례 7 : 국내에 주소 또는 영업소가 없는 개인정보처리자로서 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 국내 정보주체의 수가 일일평균 100만명 이상인 자에 해당되어 국내대리인 지정의무에 해당됨에도 불구하고, 국내대리인을 문서로 지정하지 않은 경우

항 목	1.4.2 관리체계 점검
인증기준	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
주요 확인사항	• 법적 요구사항 및 수립된 정책에 따라 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검 계획을 수립하고 있는가? • 관리체계 점검 계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 경영진에게 보고하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 법적 요구사항 및 수립된 정책에 따라 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검 계획을 수립하고 경영진에게 보고하여야 한다.

- ▶ 점검기준 : 정보보호 및 개인정보보호 관리체계 인증기준 포함
- ▶ 점검범위 : 전사 또는 인증범위 포함
- ▶ 점검주기 : 최소 연 1회 이상 수행 필요
- ▶ 점검인력 자격요건 : 점검의 객관성, 독립성 및 전문성을 확보할 수 있도록 자격 요건 정의

■ 관리체계 점검 계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 정보보호 최고책임자, 개인정보 보호책임자 등 경영진에게 보고하여야 한다.

- ▶ 점검의 객관성, 독립성 및 전문성을 확보할 수 있도록 점검조직 구성
- ▶ 점검 계획에 따라 연 1회 이상 점검 수행
- ▶ 점검 결과보고서를 작성하여 정보보호 최고책임자 및 개인정보 보호책임자 등 경영진에게 보고

증거자료

예시

- 관리체계 점검 계획서(내부점검 계획서, 내부감사 계획서)
- 관리체계 점검 결과보고서
- 정보보호 및 개인정보보호 위원회 회의록

결함사례

- 사례 1 : 관리체계 점검 인력에 점검 대상으로 식별된 전산팀 직원이 포함되어 전산팀 관리 영역에 대한 점검에 관여하고 있어, 점검의 독립성이 훼손된 경우
- 사례 2 : 금년도 관리체계 점검을 실시하였으나, 점검범위가 일부 영역에 국한되어 있어 정보보호 및 개인정보보호 관리체계 범위를 충족하지 못한 경우
- 사례 3 : 관리체계 점검팀이 위험평가 또는 취약점 점검 등 관리체계 구축 과정에 참여한 내부 직원 및 외부 컨설턴트로만 구성되어, 점검의 독립성이 확보되었다고 볼 수 없는 경우

항 목	1.4.3 관리체계 개선
인증기준	법적 요구사항 준수검토 및 관리체계 점검을 통하여 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.
주요 확인사항	• 법적 요구사항 준수검토 및 관리체계 점검을 통하여 식별된 관리체계상의 문제점에 대한 근본 원인을 분석하여 재발방지 및 개선 대책을 수립·이행하고 있는가? • 재발방지 및 개선 결과의 정확성 및 효과성 여부를 확인하기 위한 기준과 절차를 마련하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 법적 요구사항 준수검토 및 관리체계 점검을 통하여 식별된 관리체계상의 문제점에 대한 근본 원인을 분석하여 재발방지 및 개선 대책을 수립·이행하여야 한다.

▶ 점검 결과 발견된 문제점에 대해서는 조치계획을 수립·이행하고, 조치 완료 여부에 대하여 추가 확인

▶ 식별된 관리체계상의 문제점 및 결함사항에 대한 근본 원인 분석

▶ 근본원인 분석결과를 바탕으로 발견된 문제점의 재발방지 및 개선을 위한 대책의 수립·이행

※ 재발방지 대책(예시)
- 정보보호 및 개인정보보호 정책·지침·절차 개정
- 임직원 및 외부자에 대한 교육 강화 또는 개선
- 이상행위 등에 대한 모니터링 강화
- 정보보호 및 개인정보보호 운영 자동화(계정관리 등)
- 정보보호 및 개인정보보호 관련 검토·승인 절차 개선
- 내부점검 체크리스트 또는 방식 개선 등

▶ 수립된 재발방지 대책에 대하여 관련자들에게 공유 및 교육 실시

■ 재발방지 및 개선 결과의 정확성 및 효과성 여부를 확인하기 위한 기준과 절차를 마련하여야 한다.

▶ 재발방지 및 개선조치의 정확성 및 효과성을 측정하기 위하여 관리체계 측면에서의 핵심성과지표(보안성과지표) 도출

※ 재발방지 및 개선조치 관련 보안성과지표(예시)
- 보안 정책·지침 위반율(외부 전송규정 위반율, 보안우회 시도율 등)
- 보안 예외 승인 건수
- 보안 프로그램 설치율

· 악성프로그램 감염률
· 자가점검 수행률 등

- 핵심성과지표(보안성과지표)에 대한 측정 및 모니터링 절차 수립·이행
- 재발방지 및 개선조치의 정확성·효과성에 대한 확인 및 측정 결과는 경영진에게 보고

증거자료

예시

- 관리체계 점검 결과보고서
- 관리체계 점검 조치계획서·이행조치결과서
- 재발방지 대책
- 효과성 측정 지표 및 측정 결과(경영진 보고 포함)

결함사례

- 사례 1 : 내부점검을 통하여 발견된 정보보호 및 개인정보보호 관리체계 운영상 문제점이 매번 동일하게 반복되어 발생되는 경우
- 사례 2 : 내부 규정에는 내부점검 시 발견된 문제점에 대해서는 근본원인에 대한 분석 및 재발방지 대책을 수립하도록 되어 있으나, 최근에 수행된 내부점검에서는 발견된 문제점에 대하여 근본원인 분석 및 재발방지 대책이 수립되지 않은 경우
- 사례 3 : 관리체계상 문제점에 대한 재발방지 대책을 수립하고 핵심성과지표를 마련하여 주기적으로 측정하고 있으나, 그 결과에 대하여 경영진 보고가 장기간 이루어지지 않은 경우
- 사례 4 : 관리체계 점검 시 발견된 문제점에 대하여 조치계획을 수립하지 않았거나 조치 완료 여부를 확인하지 않은 경우

2 보호대책 요구사항

2.1. 정책, 조직, 자산 관리

항 목	2.1.1 정책의 유지관리
인증기준	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 관련 정책 및 시행문서에 대한 정기적인 타당성 검토 절차를 수립·이행하고 있는가? • 조직의 대내외 환경에 중대한 변화 발생 시 정보보호 및 개인정보보호 관련 정책 및 시행문서에 미치는 영향을 검토하고 필요시 제·개정하고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 시 이해 관계자의 검토를 받고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 내역에 대하여 이력관리를 하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 정보보호 및 개인정보보호 관련 정책 및 시행문서(지침, 절차, 가이드 문서 등)에 대하여 정기적인 타당성 검토 절차를 수립·이행하고, 필요시 관련 정책 및 시행문서를 제·개정하여야 한다.

▶ 정보보호 및 개인정보보호 관련 정책과 시행문서의 정기 타당성 검토 절차 수립

※ 정기 타당성 검토 절차에 포함되어야 할 사항(예시)
· 검토 주기 및 시기 : 연 1회 이상 검토 필요
· 관련 조직별 역할 및 책임
· 담당 부서 및 담당자
· 검토 방법
· 후속조치 절차 : 정책 및 시행문서 제·개정이 필요한 경우 관련 절차, 내부 협의 및 보고 절차 등

▶ 법령 및 규제, 상위 조직 및 관련기관의 정책과의 연계성, 조직의 대내외 환경변화 등을 반영할 수 있도록 다음 사항을 고려하여 타당성 검토 수행

• 상위조직 및 관련기관의 정보보호 및 개인정보보호 정책과의 연계성 등을 분석하여 상호 부합되지

않은 요소 존재 여부, 정책 간 상하체계 적절성 여부 검토

- 정보보호 및 개인정보보호 활동의 주기, 수준, 방법 등 문서 간 일관성 유지 여부 검토
- 정보보호 및 개인정보보호 관련 법규 제·개정사항(예정 사항 포함) 발생 여부 및 이러한 사항이 정책과 시행문서에 적절히 반영되었는지 여부 검토
- 위험평가 및 관리체계 점검 결과 반영
- 새로운 위협 및 취약점 발견, 비즈니스 환경의 변화, 신기술 도입 등 IT 환경의 변화, 정보보호 및 개인정보보호 환경의 변화 등 반영

■ 다음과 같이 조직의 대내외 환경에 중대한 변화 발생 시 정보보호 및 개인정보보호 관련 정책 및 시행문서에 미치는 영향을 검토하고 필요시 제·개정하여야 한다.

▶ 정보보호 및 개인정보보호 관련 법규 제·개정

▶ 비즈니스 환경의 변화(신규 사업 영역 진출, 대규모 조직개편 등)

▶ 정보보호, 개인정보보호 및 IT 환경의 중대한 변화(신규 보안시스템 또는 IT 시스템 도입 등)

▶ 내·외부의 중대한 보안사고 발생

▶ 새로운 위협 또는 취약성 발견 등

■ 정보보호 및 개인정보보호 관련 정책 및 시행문서를 제·개정하는 경우 이해관계자와 해당 내용을 충분히 협의·검토하여야 한다.

▶ 정보보호 최고책임자 및 개인정보 보호책임자, 정보보호 및 개인정보보호 관련 조직, IT 부서, 중요정보 및 개인정보 처리부서, 중요정보취급자 및 개인정보취급자 등 이해관계자 식별 및 협의

▶ 정보보호 및 개인정보보호 관련 정책 및 시행문서 변경으로 인한 업무 영향도, 법적 준거성 등 고려

▶ 회의록 등 검토 사항에 대한 증거자료를 남기고 정책·지침 등에 관련 사항 반영

■ 정보보호 및 개인정보보호 관련 정책 및 시행문서의 변경사항(제정, 개정, 배포, 폐기 등)에 관한 이력을 기록·관리하기 위하여 문서관리 절차를 마련하고 이행하여야 한다.

▶ 문서 내에 문서버전, 일자, 개정 사유, 작성자, 승인자 등 개정이력을 기록하여 관리

▶ 관련 임직원들이 항상 최신본을 참조할 수 있도록 배포 및 관리

증거자료

예시

- 정보보호 및 개인정보보호 정책 및 시행문서(지침, 절차, 가이드, 매뉴얼 등)
- 정책·지침 정기·비정기 타당성 검토 결과
- 정책·지침 관련 부서와의 검토 회의록, 회람내용
- 정책·지침 제·개정 이력

결함사례

- 사례 1 : 지침서와 절차서 간 패스워드 설정 규칙에 일관성이 없는 경우
- 사례 2 : 정보보호 활동(정보보호 교육, 암호화, 백업 등)의 대상, 주기, 수준, 방법 등이 관련 내부 규정, 지침, 절차에 서로 다르게 명시되어 일관성이 없는 경우
- 사례 3 : 데이터베이스에 대한 접근 및 작업이력을 효과적으로 기록 및 관리하기 위하여 데이터베이스 접근통제 솔루션을 신규로 도입하여 운영하고 있으나, 보안시스템 보안 관리지침 및 데이터베이스 보안 관리지침 등 내부 보안지침에 접근통제, 작업이력, 로깅, 검토 등에 관한 사항이 반영되어 있지 않은 경우
- 사례 4 : 개인정보보호 정책이 개정되었으나 정책 시행 기준일이 명시되어 있지 않으며, 관련 정책의 작성일, 작성자 및 승인자 등이 누락되어 있는 경우
- 사례 5 : 개인정보 보호 관련 법령, 고시 등에 중대한 변경사항이 발생하였으나, 이러한 변경이 개인정보보호 정책 및 시행문서에 미치는 영향을 검토하지 않았거나 변경사항을 반영하여 개정하지 않은 경우

항 목	2.1.2 조직의 유지관리
인증기준	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 관련 책임자와 담당자의 역할 및 책임을 명확히 정의하고 있는가? • 정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하고 있는가? • 정보보호 및 개인정보보호 관련 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계 및 절차를 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무), 제31조(개인정보 보호책임자의 지정) • 정보통신망법 제45조의3(정보보호 최고책임자의 지정 등) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 정보보호 및 개인정보보호 업무 수행과 관련된 조직의 특성을 고려하여 관련 책임자와 담당자의 역할 및 책임을 시행문서에 구체적으로 정의하여야 한다.

▶ 정보보호 최고책임자 및 개인정보 보호책임자

▶ 정보보호, 개인정보보호 관리자 및 담당자

▶ 부서별 정보보호, 개인정보보호 책임자 및 담당자

▶ 정보보호 최고책임자, 개인정보 보호책임자는 법적 요구사항 등을 반영하여 다음과 같은 업무를 수행

정보보호 최고책임자	개인정보 보호책임자
• 정보보호 관리체계의 수립·시행 및 개선 • 정보보호 실태와 관행의 정기적인 감사 및 개선 • 정보보호 위험의 식별 평가 및 정보보호 대책 마련 • 정보보호 교육과 모의 훈련 계획의 수립 및 시행 • 그 밖에 정보통신망법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행	• 개인정보 보호 계획의 수립 및 시행 • 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 • 개인정보 처리와 관련한 불만의 처리 및 피해 구제 • 개인정보 유출 및 오·남용 방지를 위한 내부통제 시스템의 구축 • 개인정보 보호 교육 계획의 수립 및 시행 • 개인정보파일의 보호 및 관리·감독 • 개인정보 처리방침의 수립·변경 및 시행 • 개인정보보호 관련 자료의 관리 • 처리목적이 달성되거나 보유기간이 경과한 개인정보의 파기

▶ 정보보호 및 개인정보보호 관리자, 보호담당자, 보호실무자 등이 정보보호 최고책임자 및 개인정보보호책임자의 관리 업무를 실무적으로 지원·이행할 수 있도록 직무기술서 등을 통하여 책임 및 역할을

구체적으로 정의

- 정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하여야 한다.
  - 조직 내 핵심성과지표(KPI), MBO(Management By Objectives), 인사평가 등 정보보호 및 개인정보보호 활동을 평가할 수 있는 방안을 마련하여 주기적으로 평가
- 정보보호 및 개인정보보호 관련 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계 및 절차를 수립·이행하여야 한다.
  - 정보보호 및 개인정보보호 관련 의사소통 관리 계획 수립 및 이행

※ 정보보호 및 개인정보보호 관련 의사소통 관리계획(예시)
· 의사소통 관리 계획 개요 : 목적 및 범위
· 의사소통 체계 : 전사 협의체, 실무 협의체, 위원회 등 보고 및 협의체 운영방안, 참여 대상, 참여대상별 역할 및 책임, 주기 등
· 의사소통 방법 : 보고 및 회의(월간보고, 주간보고 등), 공지, 이메일, 메신저, 정보보호포털 등
· 의사소통 양식 : 유형별 보고서 양식, 회의록 양식 등

증거자료

예시

- 정보보호 및 개인정보보호 조직도
- 정보보호 및 개인정보보호 조직 직무기술서
- 정보보호 및 개인정보보호 업무 분장표
- 정보보호 및 개인정보보호 정책·지침, 내부 관리계획
- 정보보호 및 개인정보보호 의사소통 관리계획
- 의사소통 수행 이력(월간보고, 주간보고, 내부공지 등)
- 의사소통 채널(정보보호포털, 게시판 등)

결함사례

- 사례 1 : 내부 지침 및 직무기술서에 정보보호 최고책임자, 개인정보 보호책임자 및 관련 담당자의 역할과 책임을 정의하고 있으나, 실제 운영현황과 일치하지 않는 경우
- 사례 2 : 정보보호 최고책임자 및 관련 담당자의 활동을 주기적으로 평가할 수 있는 목표, 기준, 지표 등의 체계가 마련되어 있지 않은 경우
- 사례 3 : 내부 지침에는 부서별 정보보호 담당자는 정보보호와 관련된 KPI를 설정하여 인사평가 시 반영하도록 되어 있으나, 부서별 정보보호 담당자의 KPI에 정보보호와 관련된 사항이 전혀 반영되어 있지 않은 경우
- 사례 4 : 정보보호 최고책임자 및 개인정보 보호책임자가 지정되어 있으나, 관련 법령에서 요구하는 역할 및 책임이 내부 지침이나 직무기술서 등에 구체적으로 명시되어 있지 않은 경우

항 목	2.1.3 정보자산 관리
인증기준	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
주요 확인사항	• 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호대책을 정의하고 이행하고 있는가? • 식별된 정보자산에 대하여 책임자 및 관리자를 지정하고 있는가?

세부 설명

- 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기 등)를 정의하고, 이에 따라 암호화, 접근통제 등 적절한 보호대책을 정의하고 이행하여야 한다.
  - 임직원이 정보자산별 보안등급(기밀, 대외비, 일반 등)을 식별할 수 있도록 표시
    - (전자)문서 : 문서 표지 또는 워터마킹 등을 통하여 표시
    - 서버 등 하드웨어 자산 : 자산번호 또는 바코드 표시 등을 통한 보안등급 확인
  - 정보자산 보안등급별로 취급절차(생성·도입, 저장, 이용, 파기 등) 및 보안통제 기준 수립·이행
- 식별된 정보자산에 대하여 자산 도입, 변경, 폐기, 반출입, 보안관리 등의 책임을 질 수 있는 책임자와 자산을 실제 관리·운영하는 책임자, 관리자(또는 담당자)를 지정하여 책임소재를 명확하게 하여야 한다.
  - 정보자산별로 책임자 및 관리자 지정하고 자산목록에 기록
  - 퇴직, 전보 등 인사이동이 발생하거나 정보자산의 도입·변경·폐기 등으로 정보자산 현황이 변경될 경우 정보자산별 책임자 및 담당자를 파악하여 자산목록에 반영

증거자료

예시

- 정보자산 목록(책임자, 담당자 지정)
- 정보자산 취급 절차(문서, 정보시스템 등)
- 정보자산 관리 시스템 화면
- 정보자산 보안등급 표시 내역

결함사례

- 사례 1 : 내부 지침에 따라 문서에 보안등급을 표기하도록 되어 있으나, 이를 표시하지 않은 경우
- 사례 2 : 정보자산별 담당자 및 책임자를 식별하지 않았거나, 자산목록 현행화가 미흡하여 퇴직, 전보 등 인사이동이 발생하여 주요 정보자산의 담당자 및 책임자가 변경되었음에도 이를 식별하지 않은 경우
- 사례 3 : 식별된 정보자산에 대한 중요도 평가를 실시하여 보안등급을 부여하고 정보 자산목록에 기록하고 있으나, 보안등급에 따른 취급절차를 정의하지 않은 경우

2.2. 인적 보안

항 목	2.2.1 주요 직무자 지정 및 관리
인증기준	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.
주요 확인사항	• 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하고 있는가? • 주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고 그 목록을 최신으로 관리하고 있는가? • 업무상 개인정보를 취급하는 자를 개인정보취급자로 지정하고 목록을 최신으로 관리하고 있는가? • 업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제28조(개인정보취급자에 대한 감독), 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하여야 한다.

※ 주요 직무의 기준(예시)
· 중요정보(개인정보, 인사정보, 영업비밀, 산업기밀, 재무정보 등) 취급
· 중요 정보시스템(서버, 데이터베이스, 응용프로그램 등) 및 개인정보처리시스템 운영·관리
· 정보보호 및 개인정보보호 관리 업무 수행
· 보안시스템 운영 등

■ 주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고 그 목록을 최신으로 관리하여야 한다.

▶ 주요 직무자 현황을 파악하여 주요 직무자로 공식 지정
▶ 지정된 주요 직무자에 대하여 목록으로 관리
▶ 주요 직무자의 신규 지정 및 변경, 해제 시 목록 업데이트
▶ 정기적으로 주요 직무자 지정 현황 및 적정성을 검토하여 목록 최신화

■ 업무상 개인정보를 취급하는 자를 개인정보취급자로 지정하고 목록을 최신으로 관리하여야 한다.

▶ 업무상 개인정보를 처리하는 개인정보취급자에 대해서는 목록으로 관리
▶ 개인정보취급자 목록에는 개인정보 처리업무에 대한 위탁을 받은 수탁자의 개인정보취급자도 포함(다만 수탁자의 개인정보취급자 중 개인정보처리시스템에 접근권한이 없는 개인정보취급자에 대한 목록관리는

수탁자 자체적으로 관리 가능)

- 정기적으로 개인정보취급자 지정 현황 및 적정성을 검토하여 목록 최신화

※ 개인정보취급자의 정의
· 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자

■ 업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하여야 한다.

- 업무상 반드시 필요한 경우에 한하여 주요 직무자 및 개인정보취급자로 지정
- 주요 직무자 및 개인정보취급자 권한 신청 및 부여에 대한 승인 절차 마련
- 주요 직무자 및 개인정보취급자에 대한 관리 및 통제방안 수립·이행(교육, 모니터링 등)

증거자료

예시

- 주요 직무 기준
- 주요직무자 목록
- 개인정보취급자 목록
- 중요 정보시스템 및 개인정보처리시스템 계정 및 권한 관리 대장
- 주요 직무자에 대한 관리 현황(교육 결과, 보안서약서 등)

결함사례

- 사례 1 : 주요 직무자 명단(개인정보취급자 명단, 비밀정보관리자 명단 등)을 작성하고 있으나, 대량의 개인정보 등 중요정보를 취급하는 일부 임직원(DBA, DLP 관리자 등)을 명단에 누락한 경우
- 사례 2 : 주요 직무자 및 개인정보취급자 목록을 관리하고 있으나, 퇴사한 임직원이 포함되어 있고 최근 신규 입사한 인력이 포함되어 있지 않는 등 현행화 관리가 되어 있지 않은 경우
- 사례 3 : 부서 단위로 개인정보취급자 권한을 일괄 부여하고 있어 실제 개인정보를 취급할 필요가 없는 인원까지 과다하게 개인정보취급자로 지정된 경우
- 사례 4 : 내부 지침에는 주요 직무자 권한 부여 시에는 보안팀의 승인을 받고 주요 직무에 따른 보안서약서를 작성하도록 하고 있으나, 보안팀 승인 및 보안서약서 작성 없이 등록된 주요 직무자가 다수 존재하는 경우

항 목	2.2.2 직무 분리
인증기준	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
주요 확인사항	• 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하여 적용하고 있는가? • 직무 분리가 어려운 경우 직무자 간 상호 검토, 상위관리자 정기 모니터링 및 변경사항 승인, 책임추적성 확보 방안 등의 보완통제를 마련하고 있는가?

세부 설명

- 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 다음과 같이 직무 분리 기준을 수립하여 적용하여야 한다.
  - 개발과 운영 직무 분리
  - 정보보호담당자, 개인정보취급자와 정보보호 및 개인정보 모니터링 직무 분리
  - 정보시스템 및 개인정보처리시스템(서버, 데이터베이스 등) 간 운영직무 분리
  - 정보보호 및 개인정보보호 관리와 정보보호 및 개인정보보호 감사 업무 분리
  - 개인정보보호 관리와 개인정보처리시스템 운영직무 분리
  - 개인정보보호 관리와 개인정보처리시스템 개발직무 분리 등
  - 외부 위탁업체 직원에게 사용자 계정 등록·삭제(비활성화) 및 접근권한 등록·변경·삭제 설정 권한 부여 금지(다만 불가피한 경우 보완통제 적용)
- 조직 규모가 작거나 인적 자원 부족 등의 사유로 인하여 불가피하게 직무 분리가 어려운 경우 직무자 간의 상호 검토, 직무자의 책임추적성 확보 등의 보완통제를 마련하여야 한다.
  - 직무자 간 상호 검토, 상위관리자 승인 등으로 오·남용이 발생하지 않도록 관리
  - 개인별 계정 사용, 로그기록 및 감사·모니터링을 통한 책임추적성 확보 등

증거자료

예시

- 직무 분리 관련 지침(인적 보안 지침 등)
- 직무기술서(시스템 운영·관리, 개발·운영 등)
- 직무 미분리 시 보완통제 현황

결함사례

- 사례 1 : 조직의 규모와 인원이 담당자별 직무 분리가 충분히 가능한 조직임에도 업무 편의성만을 사유로 내부 규정으로 정한 직무 분리 기준을 준수하고 있지 않은 경우
- 사례 2 : 조직의 특성상 경영진의 승인을 받은 후 개발과 운영 직무를 병행하고 있으나, 직무자 간 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경 사항 검토·승인, 직무자의 책임추적성 확보 등의 보완통제 절차가 마련되어 있지 않은 경우

항 목	2.2.3 보안 서약
인증기준	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
주요 확인사항	• 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받고 있는가? • 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가? • 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가? • 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보관하고 필요시 쉽게 찾아볼 수 있도록 관리하고 있는가?

세부 설명

- 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받아야 한다.
  - 신규 인력이 입사하는 경우 정보보호 및 개인정보보호의 필요성과 책임, 내부 정책 및 관련 법규 준수, 비밀 유지 의무에 대하여 명시된 서약서 서명
  - 고용 조건의 변경 등 중요 변경사항 발생 시 서약서 재작성 등의 조치 수행
- 임시직원, 외주용역직원 등 외부자에게 정보자산(개인정보 포함), 정보시스템 등에 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 작성하도록 하여야 한다.
  - 정보보호 및 개인정보보호 책임, 비밀유지 의무, 내부 규정 및 관련 법규 준수 의무, 관련 의무의 미준수로 인한 사건·사고 발생 시 손해배상 책임 등 필요한 내용 포함
- 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받아야 한다.
  - 퇴직자에게 정보유출 발생 시 그에 따르는 법적 책임이 있음을 명확히 인식시킬 수 있도록 비밀유지 서약서 징구(퇴직 절차 내 포함)
- 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보존하고, 필요시 쉽게 찾아볼 수 있도록 관리하여야 한다.
  - 법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있도록 잠금장치가 있는 캐비닛 또는 출입통제가 적용된 문서고 등에 안전하게 보관·관리

증거자료

예시

- 정보보호 및 개인정보보호 서약서(임직원, 외부인력)
- 비밀유지서약서(퇴직자)

결함사례

- 사례 1 : 신규 입사자에 대해서는 입사 절차상에 보안서약서를 받도록 규정하고 있으나, 최근에 입사한 일부 직원의 보안서약서 작성이 누락된 경우
- 사례 2 : 임직원에 대해서는 보안서약서를 받고 있으나, 정보처리시스템에 직접 접속이 가능한 외주 인력에 대해서는 보안서약서를 받지 않은 경우
- 사례 3 : 제출된 정보보호 및 개인정보보호 서약서를 모아 놓은 문서철이 비인가자가 접근 가능한 상태로 사무실 책상에 방치되어 있는 등 관리가 미흡한 경우
- 사례 4 : 개인정보취급자에 대하여 보안서약서만 받고 있으나, 보안서약서 내에 비밀유지에 대한 내용만 있고 개인정보보호에 관한 책임 및 내용이 포함되어 있지 않은 경우

항 목	2.2.4 인식제고 및 교육훈련
인증기준	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 교육 계획을 수립하고 경영진의 승인을 받고 있는가? • 관리체계 범위 내 모든 임직원과 외부자를 대상으로 연간 교육 계획에 따라 연 1회 이상 정기적으로 교육을 수행하고, 관련 법규 및 규정의 중대한 변경 시 이에 대한 추가교육을 수행하고 있는가? • 임직원 채용 및 외부자 신규 계약 시 업무 시작 전에 정보보호 및 개인정보보호 교육을 시행하고 있는가? • IT 및 정보보호, 개인정보보호 조직 내 임직원은 정보보호 및 개인정보보호와 관련하여 직무별 전문성 제고를 위한 별도의 교육을 받고 있는가? • 교육시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가?
관련 법규	• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한), 제28조(개인정보취급자에 대한 감독), 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

세부 설명

■ 연간 정보보호 및 개인정보보호 교육 계획은 다음과 같이 교육의 시기, 기간, 대상, 내용, 방법 등의 내용을 구체적으로 포함하여 교육 계획을 수립하고 경영진의 승인을 받아야 한다.

▶ 교육 유형 : 임직원 인식제고 교육, 주요직무자, 개인정보취급자 교육, 수탁자 교육, 전문 교육 등

▶ 교육 계획 : 교육 목적, 교육 대상, 교육 내용, 교육방법, 교육 일정, 교육 시간 등(사업규모, 개인정보 보유수, 업무성격, 교육대상, 교육유형 등에 따라 차등화)

▶ 교육 승인 : 교육 계획을 검토, 승인하여 계획에 따라 이행될 수 있도록 예산 배정 지원 등

■ 관리체계 범위 내 모든 임직원과 외부자를 대상으로 연간 교육 계획에 따라 연 1회 이상 정기적으로 교육을 수행하고, 관련 법규 및 규정의 중대한 변경 시 이에 대한 추가교육을 수행하여야 한다.

▶ 정보자산에 직·간접적으로 접근하는 임직원, 임시직원, 외주용역업체 직원 등 모든 인력 포함

▶ 수탁자 및 파견된 직원인 경우 해당 업체가 교육 수행할 수 있도록 관련 자료 제공, 시행 여부를 관리·감독

▶ 최소 연 1회 이상 교육 수행(특히 개인정보취급자의 경우 법적 요구사항에 따라 연 1회 이상 개인정보보호 교육 필요)

- 교육 내용에는 임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고, 이를 준수할 수 있도록 필요한 내용을 모두 포함하여야 함

※ 정보보호 및 개인정보보호 관련 교육에 포함될 내용(예시)
· 정보보호 및 개인정보보호의 기본 개요, 관리체계 구축 및 방법, 관련 법률
· 정보보호 및 개인정보보호 관련 내부규정, 관리적·기술적·물리적 조치사항
· 중요정보 및 개인정보 침해(유출)사고 사례 및 대응방안, 규정 위반 시 법적 책임 등

- 출장, 휴가, 업무 등으로 인하여 교육에 참석하지 못한 인력에 대한 교육 방법을 마련하여 시행(불참자 대상 추가교육, 전달 교육, 온라인교육 등)
- 내부 규정 및 절차의 중대한 변경, 조직 내·외부 침해사고 발생, 관련 법규 변경 등 발생 시 이에 대한 추가교육 수행(다만 사안이 중요하지 않을 경우에는 게시판 공지, 이메일 안내, 책자 배포 등으로 대체)

■ 임직원 채용 및 외부자 신규 계약 시 업무 시작 전에 정보보호 및 개인정보보호 교육을 시행하여야 한다.

- 신규 인력 발생 시점 또는 업무 수행 전에 정보보호 및 개인정보보호 교육을 시행하여 조직 정책, 주의사항, 규정 위반 시 법적 책임 등에 대한 내용 숙지

■ IT 및 정보보호, 개인정보보호 조직 내 임직원이 정보보호 및 개인정보보호와 관련하여 직무별 전문성 제고를 위한 별도의 교육을 받을 수 있도록 하여야 한다.

- 관련 직무자 : IT 직무자, 정보보호 최고책임자, 개인정보 보호책임자, 개인정보취급자, 정보보호 직무자 등
- 교육과정 : 정보보호 및 개인정보보호 관련 콘퍼런스·세미나·워크숍 참가, 교육 전문기관 위탁 교육, 외부 전문가 초빙을 통한 내부교육 등

■ 교육시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하여야 한다.

- 교육시행 후 교육 공지, 교육자료, 출석부 등과 같은 기록을 남기고, 미리 마련된 평가기준에 따라 설문 또는 테스트 등을 통하여 교육 내용의 적절성과 효과성 평가
- 교육평가 결과 내용에서 도출된 개선점에 대한 대책을 마련하고 차기 교육 계획 수립 시 반영

증거자료

예시

- 정보보호 및 개인정보보호 교육 계획서
- 교육 결과보고서
- 공통, 직무별 교육자료
- 교육참석자 목록

결함사례

- 사례 1 : 전년도에는 연간 정보보호 및 개인정보보호 교육 계획을 수립하여 이행하였으나, 당해 연도에 타당한 사유 없이 연간 정보보호 및 개인정보보호 교육 계획을 수립하지 않은 경우
- 사례 2 : 연간 정보보호 및 개인정보보호 교육 계획에 교육 주기와 대상은 명시하고 있으나, 시행 일정, 내용 및 방법 등의 내용이 포함되어 있지 않은 경우
- 사례 3 : 연간 정보보호 및 개인정보보호 교육 계획에 전 직원을 대상으로 하는 개인정보보호 인식 교육은 일정시간 계획되어 있으나, 개인정보 보호책임자 및 개인정보담당자 등 직무별로 필요한 개인정보보호 관련 교육 계획이 포함되어 있지 않은 경우
- 사례 4 : 정보보호 및 개인정보보호 교육 계획서 및 결과 보고서를 확인한 결과, 인증범위 내의 정보자산 및 설비에 접근하는 외주용역업체 직원(전산실 출입 청소원, 경비원, 외주개발자 등)을 교육 대상에서 누락한 경우
- 사례 5 : 당해 연도 정보보호 및 개인정보보호 교육을 실시하였으나, 교육시행 및 평가에 관한 기록(교육 자료, 출석부, 평가 설문지, 결과보고서 등) 일부를 남기지 않고 있는 경우
- 사례 6 : 정보보호 및 개인정보보호 교육 미이수자를 파악하지 않고 있거나, 해당 미이수자에 대한 추가교육 방법(전달교육, 추가교육, 온라인교육 등)을 수립·이행하고 있지 않은 경우

항 목	2.2.5 퇴직 및 직무변경 관리
인증기준	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
주요 확인사항	• 퇴직, 직무변경, 부서이동, 휴직 등으로 인한 인사변경 내용이 인사부서, 정보보호 및 개인정보보호 부서, 정보시스템 및 개인정보처리시스템 운영부서 간 공유되고 있는가? • 조직 내 인력(임직원, 임시직원, 외주용역직원 등)의 퇴직 또는 직무변경 시 지체 없는 정보자산 반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

세부 설명

■ 퇴직, 직무변경, 부서이동, 휴직 등으로 인한 인사변경 내용이 인사부서, 정보보호부서, 개인정보보호부서, 시스템 운영부서 등 관련 부서 간 신속히 공유되어야 한다.

▶ 관련 조직 및 시스템 간 인사변경 내용이 신속하게 공유될 수 있도록 절차 수립·이행

※ 인사 변경 내용에 대한 신속한 공유 절차(예시)
· 정보처리시스템을 인사시스템과 연동하여 실시간 또는 일배치로 계정정보 동기화
· 협력업체 인원에 대한 통합 계정 등록·관리시스템을 구축하여 개별 시스템과 계정 동기화
· 퇴직 프로세스 내에 관련 부서에 퇴직자 정보를 관련 부서에 공유하는 절차 포함 등

■ 조직 내 인력(임직원, 임시직원, 외주용역직원 등)의 퇴직 및 직무변경 시 지체 없는 정보자산 반납, 접근권한 회수·조정, 결과 확인 등 절차를 수립·이행하여야 한다.

▶ 퇴직 및 직무변동 시 출입증 및 자산 반납, 계정 삭제 또는 잠금, 접근권한 회수·조정, 보안점검 등의 절차를 수립·이행

▶ 불가피하게 계정을 공유 사용하고 있었다면 해당 계정의 비밀번호를 즉시 변경

▶ 관련 기록을 보존하고 퇴직 절차 준수 여부에 대하여 정기적으로 검토 등

증거자료

예시

- 퇴직 및 직무변경 절차서
- 퇴직 시 자산(계정) 반납관리대장
- 퇴직자 보안점검 체크리스트 및 점검 내역

결함사례

- 사례 1 : 직무 변동에 따라 개인정보취급자에서 제외된 인력의 계정과 권한이 개인정보처리시스템에 그대로 남아 있는 경우
- 사례 2 : 최근에 퇴직한 주요직무자 및 개인정보취급자에 대하여 자산반납, 권한 회수 등의 퇴직절차 이행 기록이 확인되지 않은 경우
- 사례 3 : 임직원 퇴직 시 자산반납 관리는 잘 이행하고 있으나, 인사규정에서 정한 퇴직자 보안점검 및 퇴직확인서를 작성하지 않은 경우
- 사례 4 : 개인정보취급자 퇴직 시 개인정보처리시스템의 접근 권한은 지체 없이 회수되었지만, 출입통제 시스템 및 VPN 등 일부 시스템의 접근 권한이 회수되지 않은 경우

항 목	2.2.6 보안 위반 시 조치
인증기준	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.
주요 확인사항	• 임직원 및 관련 외부자가 법령과 규제 및 내부정책에 따른 정보보호 및 개인정보보호 책임과 의무를 위반한 경우에 대한 처벌 규정을 수립하고 있는가? • 정보보호 및 개인정보 보호 위반 사항이 적발된 경우 내부 절차에 따른 조치를 수행하고 있는가?

세부 설명

- 임직원 및 관련 외부자가 법령과 규제 및 내부정책에 따른 정보보호 및 개인정보보호 책임과 의무를 위반한 경우에 대한 처벌 규정을 수립하여야 한다.
  - 관련 법규 및 내부 규정 미준수, 책임 미이행, 중요 정보 및 개인정보의 훼손, 유·노출, 오·남용 등이 발견된 경우 조사, 소명, 징계 등의 조치 기준 및 절차 수립
  - 정보보호 및 개인정보보호 책임과 의무를 충실히 이행한 경우에 대한 보상 방안도 고려
- 정보보호 및 개인정보 보호 위반 사항이 적발된 경우 내부 절차에 따른 조치를 수행하여야 한다.
  - 상벌 규정에 따른 조치를 수행하고 결과 기록
  - 필요한 경우 전사 공지 또는 교육 사례로 활용 등

증거자료

예시

- 인사 규정(정보보호 및 개인정보보호 관련 규정 위반에 따른 처벌규정)
- 정보보호 및 개인정보보호 지침 위반자 징계 내역
- 사고 사례(전사 공지, 교육 내용)

결함사례

- 사례 1 : 정보보호 및 개인정보보호 규정 위반자에 대한 처리 기준 및 절차가 내부 규정에 전혀 포함되어 있지 않은 경우
- 사례 2 : 보안시스템(DLP, 데이터베이스 접근제어시스템, 내부정보유출통제시스템 등)을 통하여 정책 위반이 탐지된 관련자에게 경고 메시지를 전달하고 있으나, 이에 대한 소명 및 추가 조사, 징계 처분 등 내부 규정에 따른 후속 조치가 이행되고 있지 않은 경우

2.3. 외부자 보안

항 목	2.3.1 외부자 현황 관리
인증기준	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
주요 확인사항	• 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의 이용 현황을 식별하고 있는가? • 업무 위탁 및 외부 시설·서비스의 이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호대책을 마련하고 있는가?
관련 법규	• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) • 정보통신망법 제50조의3(영리목적의 광고성 정보 전송의 위탁 등)

세부 설명

■ 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의 이용 현황을 명확히 식별하여야 한다.

▶ 관리체계 범위 내 업무위탁 및 외부 시설·서비스 이용현황 파악

※ 업무 위탁 및 외부 시설·서비스 이용(예시)
- IT 및 보안 업무 위탁 : 정보시스템 개발·운영, 유지보수, 서버·네트워크·보안장비 운영, 보안관제, 출입관리 및 경비, 정보보호컨설팅 등
- 개인정보 처리업무 위탁 : 개인정보 수집 대행, 고객 상담, 개인정보처리시스템 운영 등
- 외부 시설 이용 : 집적정보 통신시설(IDC) 등
- 외부 서비스 이용 : 클라우드 서비스, 애플리케이션서비스(ASP) 등

▶ 업무위탁 및 외부 시설·서비스 이용현황에 대한 목록 작성 및 지속적인 현행화 관리

※ 업무 위탁 및 외부 시설·서비스 이용현황 목록에 포함되어야 할 사항(예시)
- 수탁자 및 외부 시설·서비스명
- 위탁하는 업무의 내용 및 외부 서비스 내용
- 담당부서 및 담당자명
- 위탁 및 서비스 이용 기간
- 계약서 작성 여부, 보안점검 여부 등 관리·감독에 관한 사항 등

■ 업무 위탁 및 외부 시설·서비스의 이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호대책을 마련하여야 한다.

- ▶ 개인정보 처리업무 위탁에 해당되는지 확인
- ▶ 개인정보 등의 국외 이전에 해당되는지 확인
- ▶ 개인정보 보호법, 정보통신망법 등 관련된 법적 요구사항 파악
- ▶ 법적 요구사항을 포함하여 업무 위탁 및 외부 시설·서비스 이용에 따른 위험평가 수행
- ▶ 위험평가 결과를 반영하여 적절한 보호대책 마련 및 이행(예를 들어, 고위험의 수탁자에 대해서는 점검주기 및 점검항목을 달리하여 집중 현장점검 수행 등)

증거자료

예시

- 외부 위탁 및 외부 시설·서비스 현황
- 외부 위탁 계약서
- 위험분석 보고서 및 보호대책
- 위탁 보안관리 지침, 체크리스트 등

결함사례

- 사례 1 : 내부 규정에 따라 외부 위탁 및 외부 시설·서비스 현황을 목록으로 관리하고 있으나, 몇 개월 전에 변경된 위탁업체가 목록에 반영되어 있지 않은 등 현행화 관리가 미흡한 경우
- 사례 2 : 관리체계 범위 내 일부 개인정보처리시스템을 외부 클라우드 서비스로 이전하였으나, 이에 대한 식별 및 위험평가가 수행되지 않은 경우

항 목	2.3.2 외부자 계약 시 보안
인증기준	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.
주요 확인사항	• 중요정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁 업체를 선정하는 경우 정보보호 및 개인정보 보호 역량을 고려하도록 절차를 마련하고 있는가? • 외부 서비스 이용 및 업무 위탁에 따른 정보보호 및 개인정보보호 요구사항을 식별하고 이를 계약서 또는 협정서에 명시하고 있는가? • 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수하여야 할 정보보호 및 개인정보보호 요구사항을 계약서에 명시하고 있는가?
관련 법규	• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)

세부 설명

■ 주요정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁 업체를 선정하는 경우 정보보호 및 개인정보 보호 역량을 고려하도록 절차를 마련하여야 한다.

▶ 정보보호 및 개인정보보호 역량이 있는 업체가 선정될 수 있도록 관련 요건을 제안요청서(RFP) 및 제안평가항목에 반영하여 업체 선정 시 적용

■ 조직의 정보처리 업무를 외부자에게 위탁하거나 외부 서비스를 이용하는 경우 다음과 같은 보안 요구사항을 정의하여 계약 시 반영하여야 한다.

▶ 정보보호 및 개인정보보호 관련 법률 준수, 정보보호 및 개인정보보호 서약서 제출

▶ 위탁 업무 수행 직원 대상 주기적인 정보보호 교육 수행 및 주기적 보안점검 수행

▶ 업무수행 관련 취득한 중요정보 유출 방지 대책

▶ 외부자 인터넷접속 제한, 물리적 보호조치(장비 및 매체 반출입 등), PC 등 단말 보안(백신설치, 안전한 비밀번호 설정 및 주기적 변경, 화면보호기 설정 등), 무선 네트워크 사용 제한

▶ 정보시스템 접근 허용 시 과도한 권한이 부여되지 않도록 접근권한 부여 및 해지 절차

▶ 재위탁 제한 및 재위탁이 필요한 경우의 절차와 보안 요구사항 정의

▶ 보안 요구사항 위반 시 처벌, 손해배상 책임, 보안사고 발생에 따른 보고 의무 등

※ 개인정보 처리업무 위탁 시 문서에 포함되어야 할 사항(개인정보 보호법 제26조제1항 및 동법 시행령 제28조제1항)

· 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

· 개인정보의 기술적·관리적 보호조치에 관한 사항

· 위탁업무의 목적 및 범위

· 재위탁 제한에 관한 사항
· 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
· 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
· 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

■ 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수하여야 할 정보보호 및 개인정보보호 요구사항을 계약서에 명시하여야 한다.

- ▶ 정보보호 및 개인정보보호 관련 법적 요구사항 준수
- ▶ 안전한 코딩 표준 준수 등 개발보안 절차 적용
- ▶ 개발 완료된 정보시스템 및 개인정보처리시스템에 대한 취약점 점검 및 조치
- ▶ 개발 관련 산출물, 소스 프로그램, 개발용 데이터 등 개발환경에 대한 보안관리
- ▶ 개발 과정에서 취득한 정보에 대한 비밀유지 의무
- ▶ 위반 시 손해배상 등 책임에 대한 사항 등

증거자료

예시

- 위탁 계약서
- 정보보호 및 개인정보보호 협약서(약정서, 부속합의서)
- 위탁 관련 내부 지침
- 위탁업체 선정 관련 RFP(제안요청서), 평가표

결함사례

- 사례 1 : IT 운영, 개발 및 개인정보 처리업무를 위탁하는 외주용역업체에 대한 위탁계약서가 존재하지 않는 경우
- 사례 2 : 개인정보 처리업무를 위탁하는 외부업체와의 위탁계약서상에 개인정보 보호법 등 법령에서 요구하는 일부 항목(관리·감독에 관한 사항 등)이 포함되어 있지 않은 경우
- 사례 3 : 인프라 운영과 개인정보 처리업무 일부를 외부업체에 위탁하고 있으나, 계약서 등에는 위탁업무의 특성에 따른 보안 요구사항을 식별·반영하지 않고 비밀유지 및 손해배상에 관한 일반 사항만 규정하고 있는 경우

항 목	2.3.3 외부자 보안 이행 관리
인증기준	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.
주요 확인사항	• 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 있는가? • 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선계획을 수립·이행하고 있는가? • 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 동의를 받도록 하고 있는가?
관련 법규	• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) • 정보통신망법 제50조의3(영리목적의 광고성 정보 전송의 위탁 등)

세부 설명

■ 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하여야 한다.

▶ 외부자와 계약 시 정의한 보안 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사 수행

▶ 외부자에 대한 점검 또는 감사는 업무 시작 전, 업무 진행되는 과정, 종료 시점에 진행하되 필요한 경우 수시로 진행

▶ 수탁자의 정보보호 및 개인정보보호 역량, 자체 시스템 보유 여부, 처리하는 정보의 수량 및 민감도 등을 고려하여 실태점검 주기 및 방법 결정

■ 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선계획을 수립·이행하여야 한다.

▶ 점검 및 감사 결과에 대하여 공유하고 발견된 문제점에 대한 개선방법 및 재발 방지대책을 수립하여 이행

▶ 개선 조치 완료 여부에 대한 이행점검 수행

■ 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 동의를 받도록 하여야 한다.

▶ 개인정보 처리 수탁자는 위탁자의 동의를 받은 경우에 한하여 재위탁하고, 위탁자가 수탁자에게 요구하는 동일한 수준의 기술적·관리적 보호조치를 재수탁자가 이행하도록 관리·감독

★ [참고] 개인정보 처리업무 재위탁 시 조치사항(개인정보 보호법 제26조제6항)

⑥ 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하려는 경우에는 위탁자의 동의를 받아야 한다.

증거자료

예시

- 외부자 및 수탁자 보안점검 결과
- 외부자 및 수탁자 교육 내역(교육 결과, 참석자 명단, 교육교재 등)
- 개인정보 위탁 계약서
- 개인정보 처리업무 재위탁 시 위탁자 동의 증거자료

결함사례

- 사례 1 : 회사 내에 상주하여 IT 개발 및 운영 업무를 수행하는 외주업체에 대해서는 정기적으로 보안점검을 수행하고 있지 않은 경우
- 사례 2 : 개인정보 수탁자에 대하여 보안교육을 실시하라는 공문을 발송하고 있으나, 교육 수행 여부를 확인하고 있지 않은 경우
- 사례 3 : 수탁자가 자체적으로 보안점검을 수행한 후 그 결과를 통지하도록 하고 있으나, 수탁자가 보안점검을 충실히 수행하고 있는지 여부에 대하여 확인하는 절차가 존재하지 않아 보안점검 결과의 신뢰성이 매우 떨어지는 경우
- 사례 4 : 개인정보 처리업무 수탁자 중 일부가 위탁자의 동의 없이 해당 업무를 제3자에게 재위탁한 경우
- 사례 5 : 영리 목적의 광고성 정보전송 업무를 타인에게 위탁하면서 수탁자에 대한 관리·감독을 수행하지 않고 있는 경우

항 목	2.3.4 외부자 계약 변경 및 만료 시 보안
인증기준	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.
주요 확인사항	• 외부자 계약만료, 업무 종료, 담당자 변경 시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근계정 삭제, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하고 있는가? • 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할 수 있도록 절차를 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) • 정보통신망법 제50조의3(영리목적의 광고성 정보 전송의 위탁 등)

세부 설명

■ 외부자 계약만료, 업무 종료, 담당자 변경 시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하여야 한다.

▶ 담당조직이 외부자 계약만료, 업무 종료, 담당자 변경이 발생하였음을 신속하게 인지할 수 있도록 정보공유 방안 마련

▶ 외부자 계약만료, 업무 종료, 담당자 변경에 따른 보안대책 수립 및 이행

※ 외부자 계약만료, 업무 종료, 담당자 변경 시 보안대책(예시)
· 사용 중인 정보자산 반납(업무용 PC, 스마트 디바이스 등)
· 정보시스템 접근계정 삭제(VPN 등 관련된 모든 계정 포함)
· 접근권한의 회수 또는 변경
· 공용 계정 비밀번호 변경
· 출입증 회수 및 출입권한 삭제
· 비밀유지 확약서 징구 등

■ 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할 수 있도록 절차를 수립·이행하여야 한다.

▶ 개인정보 등 중요정보를 회수·파기하기 위하여 수탁자의 사무실 직접 방문 또는 원격으로 개인정보를 파기한 후 파기 확약서 작성

▶ 정보시스템과 담당자 PC뿐 아니라, 메일 송수신함 등 해당 정보가 저장되어 있는 모든 장치 및 매체에 대한 삭제 조치 필요

▶ 해당 정보가 복구·재생되지 않도록 안전한 방법으로 파기

증거자료

예시

- 정보보호 및 개인정보보호 서약서
- 비밀유지 확약서
- 정보 및 개인정보 파기 확약서
- 외부자 계약 종료와 관련된 내부 정책, 지침

결함사례

- 사례 1 : 일부 정보시스템에서 계약 만료된 외부자의 계정 및 권한이 삭제되지 않고 존재하는 경우
- 사례 2 : 외주용역사업 수행과정에서 일부 용역업체 담당자가 교체되거나 계약 만료로 퇴직하였으나, 관련 인력들에 대한 퇴사 시 보안서약서 등 내부 규정에 따른 조치가 이행되지 않은 경우
- 사례 3 : 개인정보 처리 위탁한 업체와 계약 종료 이후 보유하고 있는 개인정보를 파기하였는지 여부를 확인·점검하지 않은 경우

2.4. 물리 보안

항 목	2.4.1 보호구역 지정
인증기준	물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접견구역 등 물리적 보호구역을 지정하고 구역별 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역 지정기준을 마련하고 있는가? • 물리적 보호구역 지정기준에 따라 보호구역을 지정하고 구역별 보호대책을 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

세부 설명

■ 물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역 지정기준을 마련하여야 한다.

▶ 접견구역, 제한구역, 통제구역 등으로 물리적 보호구역을 지정

▶ 보호구역의 용어와 구분은 조직의 환경에 맞게 선택

※ 물리적 보호구역(예시)
· 접견구역 : 외부인이 별다른 출입증 없이 출입이 가능한 구역(예 : 접견장소 등)
· 제한구역 : 비인가 접근을 방지하기 위하여 별도의 출입통제 장치 및 감시시스템이 설치된 장소로 출입 시 직원카드와 같은 출입증이 필요한 장소(예 : 부서별 사무실 등)
· 통제구역 : 제한구역의 통제항목을 모두 포함하고 출입자격이 최소인원으로 유지되며 출입을 위하여 추가 절차가 필요한 곳(예 : 전산실, 통신장비실, 관제실, 공조실, 발전실, 전원실 등)

■ 물리적 보호구역 지정기준에 따라 보호구역을 지정하고 구역별 보호대책을 수립·이행하여야 한다.

▶ 구역별로 출입통제 방식(ID카드, 생체인식 등), 출입 가능자, 출입 절차, 영상감시 등 보호대책 적용

▶ 통제구역은 조직 내부에서도 출입 인가자를 최소한으로 제한하고 있으므로 필요시 통제구역임을 표시하여 접근시도 자체를 원천적으로 차단하고 불법적인 접근시도 여부를 주기적으로 검토

증거자료

예시

- 물리적 보안 지침(보호구역 지정 기준)
- 보호구역 지정 현황
- 보호구역 표시
- 보호구역별 보호대책 현황

결함사례

- 사례 1 : 내부 물리보안 지침에는 개인정보 보관시설 및 시스템 구역을 통제구역으로 지정한다고 명시되어 있으나, 멤버십 가입신청 서류가 보관되어 있는 문서고 등 일부 대상 구역이 통제구역에서 누락된 경우
- 사례 2 : 내부 물리보안 지침에 통제구역에 대해서는 지정된 양식의 통제구역 표지판을 설치하도록 명시하고 있으나, 일부 통제구역에 표시판을 설치하지 않은 경우

항 목	2.4.2 출입통제
인증기준	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
주요 확인사항	• 보호구역은 출입절차에 따라 출입이 허가된 자만 출입하도록 통제하고 있는가? • 각 보호구역에 대한 내·외부자 출입기록을 일정기간 보존하고 출입기록 및 출입권한을 주기적으로 검토하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

세부 설명

■ 보호구역별로 허가된 자만이 출입할 수 있도록 내·외부자 출입통제 절차를 마련하고, 출입 가능한 인원 현황을 관리하여야 한다.

- ▶ 보호구역별로 출입 가능한 부서·직무·업무를 정의, 출입권한이 부여된 임직원을 식별하고 그 현황을 관리
- ▶ 통제구역의 경우 업무목적에 따라 최소한의 인원만 출입할 수 있도록 통제
- ▶ 출입절차 : 출입신청, 책임자 승인, 출입권한 부여 및 회수, 출입내역 기록, 출입기록 정기적 검토 등
- ▶ 출입통제 장치 설치 : 비밀번호 기반, ID카드 기반, 생체정보 기반 등
- ▶ 출입통제 절차 수립·운영 : 출입자 등록·삭제, 출입권한 관리, 방문자 관리, 출입대장 관리 등

■ 각 보호구역에 대한 내·외부자 출입기록을 일정기간 보존하고, 출입기록 및 출입권한을 주기적으로 검토하여야 한다.

- ▶ 출입기록을 일정기간 보존하여 사후 모니터링이 가능하도록 문서적 또는 전자적으로 보존
- ▶ 출입기록 및 출입권한 검토 : 장기 미출입자, 비정상적인 출입 시도, 출입권한 과다부여 여부 등
- ▶ 비인가자 출입 시도, 장기 미출입자 등을 확인하여 그 사유를 확인하고 조치
- ▶ 주기적 검토를 통하여 퇴직자 출입증 회수 및 출입권한 삭제, 직무변경에 따른 출입권한 조정
- ▶ 시스템적으로 출입로그를 남길 수 없는 경우 출입대장을 작성하여 출입기록 확인

증거자료

예시

- 출입 관리대장 및 출입로그
- 출입 등록 신청서 및 승인 내역
- 출입기록 검토서
- 출입통제시스템 관리화면(출입자 등록 현황 등)

결함사례

- 사례 1 : 통제구역을 정의하여 보호대책을 수립하고 출입 가능한 임직원을 관리하고 있으나, 출입기록을 주기적으로 검토하지 않아 퇴직, 전배 등에 따른 장기 미출입자가 다수 존재하고 있는 경우
- 사례 2 : 전산실, 문서고 등 통제구역에 출입통제 장치가 설치되어 있으나, 타당한 사유 또는 승인 없이 장시간 개방 상태로 유지하고 있는 경우
- 사례 3 : 일부 외부 협력업체 직원에게 과도하게 전 구역을 상시 출입할 수 있는 출입카드를 부여하고 있는 경우

항 목	2.4.3 정보시스템 보호
인증기준	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
주요 확인사항	• 정보시스템의 중요도, 용도, 특성 등을 고려하여 배치 장소를 분리하고 있는가? • 정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안을 마련하고 있는가? • 전력 및 통신케이블을 외부로부터의 물리적 손상 및 전기적 영향으로부터 안전하게 보호하고 있는가?

세부 설명

- 정보시스템의 중요도, 용도, 특성을 고려하여 배치 장소를 분리하여야 한다.
  - 정보시스템, 개인정보처리시스템, 네트워크 장비, 보안시스템, 백업 장비 등 정보시스템의 특성에 따라 전산랙을 이용하여 시스템을 외부로부터 보호
  - 개인정보처리시스템 등 중요도가 높은 경우에는 최소한의 인원만 접근이 가능하도록 전산랙에 잠금장치 설치, 별도의 물리적 안전장치가 있는 케이지(cage) 등에서 관리
- 정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안(배치도, 자산목록 등)을 마련하여야 한다.
  - 보안사고, 장애 발생 시 신속한 조치를 위한 물리적 배치도(시설 단면도, 배치도 등), 자산목록 관리
  - 자산목록 등에 물리적 위치 항목을 포함하고 현행화하여 최신본 유지
- 전력 및 통신케이블을 물리적 손상 및 전기적 영향으로부터 안전하게 보호하여야 한다.
  - 물리적으로 구분·배선, 식별 표시, 상호 간섭받지 않도록 거리 유지, 케이블 매설 등 조치
  - 배전반, 강전실, 약전실 등에는 인가된 최소한의 인력만 접근할 수 있도록 접근통제

증거자료

예시

- 정보처리시설 도면
- 정보시스템 배치도
- 자산목록

결함사례

- 사례 1 : 시스템 배치도가 최신 변경사항을 반영하여 업데이트되지 않아 장애가 발생된 정보시스템을 신속하게 확인할 수 없는 경우
- 사례 2 : 서버실 바닥 또는 랙에 많은 케이블이 정리되지 않고 뒤엉켜 있어 전기적으로 간섭, 손상, 누수, 부주의 등에 의한 장애 발생이 우려되는 경우

항 목	2.4.4 보호설비 운영
인증기준	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다.
주요 확인사항	• 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립하여 운영하고 있는가? • 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?
관련 법규	• 정보통신망법 제46조(집적된 정보통신시설의 보호) • 집적정보 통신시설 보호지침 • 소방시설 설치 및 관리에 관한 법률(소방시설법) 제12조(특정소방대상물에 설치하는 소방시설의 관리 등), 제16조(피난시설, 방화구역 및 방화시설의 관리)

세부 설명

■ 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립하여 운영하여야 한다.

※ 물리적 보호설비(예시)
· 온·습도 조절기(항온항습기 또는 에어컨)
· 화재감지 및 소화설비
· 누수감지기
· UPS, 비상발전기
· 전압유지기, 접지시설
· 이중전원선
· 침입 경보기
· CCTV
· 출입통제시스템(ID카드, 생체인식, 무게감지 등)
· 비상등, 비상로 안내표지 등

■ 외부 집적정보 통신시설(IDC)에 위탁 운영하는 경우 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영 상태를 주기적으로 검토하여야 한다.

▶ 정보보호 관련 법규 준수, 화재, 전력 이상 등 재해·재난 대비, 출입통제, 자산 반출입 통제, 영상감시 등 물리적 보안통제 적용 및 사고 발생 시 손해 배상에 관한 사항 등

▶ IDC의 책임보험 가입 여부(미가입 시 2천만원 이하의 과태료 부과)

※ 집적정보 통신시설 관련 참고 법령 및 고시

· 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조(집적된 정보통신시설의 보호)
· 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제38조(보험가입)
· 집적정보 통신시설 보호지침
· 방송통신발전 기본법 제35조의3(통신시설의 등급 지정), 제36조(방송통신재난관리기본계획의 수립 절차), 제36조의2(방송통신재난관리계획의 이행)
· 방송통신발전 기본법 시행령 제23조(주요방송통신사업자), 제23조의3(통신시설의 등급 분류기준 등)
· 주요통신사업자의 통신시설 등급 지정 및 관리 기준

증거자료

예시

- 물리적 보안 지침(보호설비 관련)
- 전산실 설비 현황 및 점검표
- IDC 위탁운영 계약서, SLA 등

결함사례

- 사례 1 : 본사 전산실 등 일부 보호구역에 내부 지침에 정한 보호설비를 갖추고 있지 않은 경우
- 사례 2 : 전산실 내에 UPS, 소화설비 등의 보호설비는 갖추고 있으나, 관련 설비에 대한 운영 및 점검 기준을 수립하고 있지 않은 경우
- 사례 3 : 운영지침에 따라 전산실 내에 온·습도 조절기를 설치하였으나, 용량 부족으로 인하여 표준 온·습도를 유지하지 못하여 장애발생 가능성이 높은 경우

항 목	2.4.5 보호구역 내 작업
인증기준	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.
주요 확인사항	• 정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업신청 및 수행 절차를 수립·이행하고 있는가? • 보호구역 내 작업이 통제 절차에 따라 적절히 수행되었는지 여부를 확인하기 위하여 작업 기록을 주기적으로 검토하고 있는가?

세부 설명

- 정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업신청 및 수행 절차를 수립·이행하여야 한다.
  - 작업 절차 : 통제구역에서 작업 수행 시 작업 신청, 승인, 작업 기록 작성 등
  - 작업 기록 : 작업일시, 작업목적 및 내용, 작업업체 및 담당자명, 검토자 및 승인자 등
  - 통제 방안 : 작업 수행을 위한 보호구역 출입 절차, 작업내역에 대한 책임추적성 확보 및 모니터링 방안 등
- 보호구역 내 작업이 통제 절차에 따라 적절히 수행되었는지 여부를 확인하기 위하여 작업 기록을 주기적으로 검토하여야 한다.
  - 작업 검토 : 사전 승인 내역, 출입기록, 작업 기록 등에 대한 정기적 검토 수행 등
  - 검토 방법 : 출입 신청서와 출입 내역(관리대장, 시스템 로그 등) 일치성 등

증거자료

예시

- 작업 신청서, 작업 일지
- 통제구역 출입 대장
- 통제구역에 대한 출입기록 및 작업 기록 검토 내역

결함사례

- 사례 1 : 전산실 출입로그에는 외부 유지보수 업체 직원의 출입기록이 남아 있으나, 이에 대한 보호구역 작업 신청 및 승인 내역이 존재하지 않은 경우(내부 규정에 따른 보호구역 작업 신청 없이 보호구역 출입 및 작업이 이루어지고 있는 경우)
- 사례 2 : 내부 규정에는 보호구역 내 작업 기록에 대하여 분기별 1회 이상 점검하도록 되어 있으나, 특별한 사유 없이 장기간 동안 보호구역 내 작업 기록에 대한 점검이 이루어지고 있지 않은 경우

항 목	2.4.6 반출입 기기 통제
인증기준	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.
주요 확인사항	• 정보시스템, 모바일 기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하고 있는가? • 반출입 통제절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

세부 설명

■ 정보시스템, 모바일 기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하여야 한다.

▶ 반출입 통제 대상 : 정보시스템(서버, 네트워크 장비 등), 모바일 기기(노트북, 스마트패드, 스마트폰 등), 저장매체(HDD, SDD, USB메모리, 외장하드디스크, CD/DVD, 테이프 등) 등

▶ 반출입 통제 절차 : 보호구역 출입통제 책임자 사전승인, 반출입 관리대장 기록, 반출입 기기에 대한 보안점검 수행(백신설치 여부, 보안업데이트 여부, 악성코드 감염 여부, 보안스티커 부착 여부, 중요정보 유출 여부 등), 반출입 내역 주기적 검토 등

▶ 예외 사용 절차 : 예외 신청·승인, 반출입 관리대장 기록 등

※ 반출입 관리대장 기록사항(예시)
· 반출입 일시 및 장소
· 사용자 정보
· 기종(모델), 기기식별정보(시리얼번호 등)
· 반출입 사유
· 보안 점검 결과
· 관리자 확인 서명 등

■ 반출입 통제절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검하여야 한다.

▶ 보호구역 내 반출입 이력에 대한 기록 유지(반출입 관리대장, 반출입 통제시스템 로그 등)

■ 반출입 이력을 주기적으로 점검하여 보호구역 내 반출입이 통제 절차에 따라 적절하게 수행되었는지 여부 검토

증거자료

예시

- 보호구역 내 반출입 신청서
- 반출입 관리대장
- 반출입 이력 검토 결과

결함사례

- 사례 1 : 이동컴퓨팅기기 반출입에 대한 통제 절차를 수립하고 있으나, 통제구역 내 이동컴퓨팅기기 반입에 대한 통제를 하고 있지 않아 출입이 허용된 내·외부인이 이동컴퓨팅기기를 제약 없이 사용하고 있는 경우
- 사례 2 : 내부 지침에 따라 전산장비 반출입이 있는 경우 작업계획서에 반출입 내용을 기재하고 관리책임자의 서명을 받도록 되어 있으나, 작업계획서의 반출입 기록에 관리책임자의 서명이 다수 누락되어 있는 경우

항 목	2.4.7 업무환경 보안
인증기준	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통하여 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호대책을 수립·이행하고 있는가? • 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유·노출을 방지하기 위한 보호대책을 수립·이행하고 있는가? • 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 보호조치를 하고 있는가? • 개인 및 공용업무 환경에서의 정보보호 준수 여부를 주기적으로 검토하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치), 제12조(출력·복사시 안전조치)

세부 설명

■ 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용기기에 대한 보호대책을 수립·이행하여야 한다.

- ▶ 문서고 : 출입인원 최소화, 부서·업무별 출입 접근권한 부여, 출입 이력관리
- ▶ 공용PC : 담당자 지정, 화면보호기 설정, 로그인 암호설정, 주기적 패스워드 변경, 중요정보 저장 제한, 백신 설치, 보안업데이트 등
- ▶ 공용사무기기 : 팩스, 복사기, 프린트 등의 공용사무기기 주변에 중요 문서 방치 금지
- ▶ 파일서버 : 부서별·업무별 접근권한 부여, 불필요한 정보공개 최소화, 사용자별 계정 발급
- ▶ 공용 사무실 : 회의실, 프로젝트룸 등 공용사무실 내 중요정보(개인정보) 문서 방치 금지
- ▶ 기타 공용업무환경에 대한 보호대책 수립

■ 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유·노출을 방지하기 위한 보호대책을 수립·이행하여야 한다.

- ▶ 이석 시 보호조치 : 개인정보 및 개인정보가 포함된 서류와 보조저장매체 방치 금지(**클린데스크**), 화면보호기 및 비밀번호 설정 등
- ▶ 모니터 및 책상 등에 로그인 정보(비밀번호 등) 노출 금지
- ▶ 개인정보 및 중요정보가 포함된 서류 및 보조저장매체는 잠금장치가 있는 안전한 장소에 보관
- ▶ 개인정보 및 중요정보가 포함된 서류는 세절기 등을 이용하여 복구되지 않도록 파쇄
- ▶ 인가받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 등

■ 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 통한 개인정보의 분실·도난·유출 등을 방지하고 출력·복사물을 안전하게 관리하기 위하여 필요한 보호조치를 하여야 한다.

※ 출력·복사물 보호조치(예시)
· 출력·복사물 보호 및 관리 정책, 규정, 지침 등 마련
· 출력·복사물 생산·관리 대장 마련 및 기록
· 출력·복사물 운영·관리 부서 지정 및 운영
· 출력·복사물 외부반출 및 재생산 통제·신고·제한
· 인쇄자, 인쇄일시 등 출력·복사물 기록 저장·관리
· 종이 인쇄물에 대한 파기 절차, 파기여부 확인 등을 포함하는 파기계획 수립 및 주기적 점검
· 복합기 보안, 출력물 워터마크 등 출력·복사물 보안기술 적용 등

■ 개인 및 공용업무 환경에서의 정보보호 준수 여부를 주기적으로 검토하여야 한다.

▶ 개인 및 공용업무 환경 보안규정 미준수자는 상벌규정에 따라 관리

※ 사무실 보안점검 방안(예시)
· 개인업무 환경 : 정보보호 준수 여부를 자가진단, 주기적으로 관리 부서에서 정보보호 준수 여부 점검
· 공용업무 환경 : 공용업무 보호대책 준수 여부를 주기적으로 점검, 미준수 사항은 공지 또는 교육 수행

증거자료

예시

- 사무실 및 공용공간 보안점검 보고서
- 사무실 및 공용공간 보안점검표
- 미준수자에 대한 조치 사항(교육, 상벌 등)
- 출력·복사물 보호조치 현황

결함사례

- 사례 1 : 개인정보 내부 관리계획서 내 개인정보보호를 위한 생활보안 점검(클린데스크 운영 등)을 정기적으로 수행하도록 명시하고 있으나, 이를 이행하지 않은 경우
- 사례 2 : 멤버십 가입신청서 등 개인정보가 포함된 서류를 잠금장치가 없는 사무실 문서함에 보관한 경우
- 사례 3 : 직원들의 컴퓨터 화면보호기 및 패스워드가 설정되어 있지 않고, 휴가자 책상 위에 중요문서가 장기간 방치되어 있는 경우
- 사례 4 : 회의실 등 공용 사무 공간에 설치된 공용PC에 대한 보호대책이 수립되어 있지 않아 개인정보가 포함된 파일이 암호화되지 않은 채로 저장되어 있거나, 보안 업데이트 미적용, 백신 미설치 등 취약한 상태로 유지하고 있는 경우

2.5. 인증 및 권한관리

항 목	2.5.1 사용자 계정 관리
인증기준	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
주요 확인사항	• 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한의 등록·변경·삭제에 관한 공식적인 절차를 수립·이행하고 있는가? • 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성·등록·변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가? • 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시키고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

세부 설명

- 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하기 위하여 다음 사항을 고려하여 공식적인 사용자 계정 및 접근권한 등록·변경·삭제·해지 절차를 수립·이행하여야 한다.
  - 사용자 및 개인정보취급자별로 고유한 사용자 계정 발급 및 공유 금지
  - 사용자 및 개인정보취급자에 대한 계정 발급 및 접근권한 부여·변경 시 승인 절차 등을 통한 적절성 검토
  - 전보, 퇴직 등 인사이동 발생 시 지체 없이 접근권한 변경 또는 말소(계정 삭제 또는 비활성화 포함)
  - 정보시스템 설치 후 제조사 또는 판매사의 기본 계정, 시험 계정 등은 제거하거나 추측하기 어려운 계정으로 변경
  - 사용자 계정 및 접근권한의 등록·변경·삭제·해지 관련 기록의 유지·관리 등
- 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성·등록·변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하여야 한다.
  - 정보시스템 및 개인정보처리시스템에 대한 접근권한은 업무 수행 목적에 따라 최소한의 범위로 업무담당자에게 차등 부여
  - 중요 정보 및 개인정보에 대한 접근권한은 알 필요(need-to-know), 할 필요(need-to-do)의 원칙에 따라 업무적으로 꼭 필요한 범위에 한하여 부여
  - 불필요하거나 과도하게 중요 정보 또는 개인정보에 접근하지 못하도록 권한 세분화
  - 권한 부여 또는 변경 시 승인절차 등을 통하여 적절성 검토 등

- 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시켜야 한다.
  - 정보보호 및 개인정보보호 정책, 서약서 등에 계정에 대한 책임과 의무를 명기(타인에게 본인 계정 및 비밀번호 공유 대여 금지, 공공장소에서 로그인 시 주의사항 등)
  - 서약서, 이메일, 시스템 공지, 교육 등 다양한 방법 활용

증거자료

예시

- 사용자 계정 및 권한 신청서
- 사용자 계정 및 권한 관리대장 또는 화면
- 정보시스템 및 개인정보처리시스템별 접근권한 분류표
- 정보시스템 및 개인정보처리시스템별 사용자, 관리자, 개인정보취급자 목록

결함사례

- 사례 1 : 사용자 및 개인정보취급자에 대한 계정·권한에 대한 사용자 등록, 해지 및 승인절차 없이 구두 요청, 이메일 등으로 처리하여 이에 대한 승인 및 처리 이력이 확인되지 않는 경우
- 사례 2 : 개인정보취급자가 휴가, 출장, 공가 등에 따른 업무 백업을 사유로 공식적인 절차를 거치지 않고 개인정보취급자로 지정되지 않은 인원에게 개인정보취급자 계정을 알려주는 경우
- 사례 3 : 정보시스템 또는 개인정보처리시스템 사용자에게 필요 이상의 과도한 권한을 부여하여 업무상 불필요한 정보 또는 개인정보에 접근이 가능한 경우

항 목	2.5.2 사용자 식별
인증기준	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
주요 확인사항	• 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가? • 불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 보완대책을 마련하여 책임자의 승인을 받고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

세부 설명

- 정보시스템 및 개인정보처리시스템에 대한 사용자 등록 시 사용자 및 개인정보취급자별로 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다.
  - 1인 1계정 발급을 원칙으로 하여 사용자에 대한 책임추적성 확보
  - 계정 공유 및 공용 계정 사용 제한
  - 시스템이 사용하는 운영계정은 일반 사용자의 접근 제한
  - 시스템 설치 후 제조사 또는 판매사의 기본계정 및 시험계정은 제거 또는 추측이 어려운 계정으로 변경하여 사용(디폴트 패스워드 변경 포함)
  - 관리자 및 특수권한 계정은 쉽게 추측 가능한 식별자(root, admin, administrator 등)의 사용을 제한
- 업무상 불가피하게 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
  - 업무 분장상 정·부의 역할이 구분되어 관리자 계정을 공유하는 경우에도 사용자 계정을 별도로 부여하고 사용자 계정으로 로그인 후 관리자 계정으로 변경
  - 유지보수 업무 등을 위하여 임시적으로 계정을 공유한 경우 업무 종료 후 즉시 해당 계정의 비밀번호 변경
  - 업무상 불가피하게 공용계정 사용이 필요한 경우 그 사유와 타당성을 검토하여 책임자의 승인을 받고 책임추적성을 보장할 추가 통제방안 적용

증거자료

예시

- 정보시스템 및 개인정보처리시스템 로그인 화면
- 정보시스템 및 개인정보처리시스템 관리자, 사용자, 개인정보취급자 계정 목록
- 예외 처리에 대한 승인 내역

결함사례

- 사례 1 : 정보시스템(서버, 네트워크, 침입차단시스템, DBMS 등)의 계정 현황을 확인한 결과, 제조사에서 제공하는 기본 관리자 계정을 기술적으로 변경 가능함에도 불구하고 변경하지 않고 사용하고 있는 경우
- 사례 2 : 개발자가 개인정보처리시스템 계정을 공용으로 사용하고 있으나, 타당성 검토 또는 책임자의 승인 등이 없이 사용하고 있는 경우
- 사례 3 : 외부직원이 유지보수하고 있는 정보시스템의 운영계정을 별도의 승인 절차 없이 개인 계정처럼 사용하고 있는 경우

항 목	2.5.3 사용자 인증
인증기준	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
주요 확인사항	• 정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 따라 통제하고 있는가? • 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리), 제6조(접근통제)

세부 설명

■ 정보시스템 및 개인정보처리시스템에 대한 접근 시 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 따라 통제하여야 한다.

▶ 사용자 인증 수단 예시

구 분	인증 수단	비 고
지식 기반	비밀번호	• 안전한 비밀번호 작성규칙 적용 및 변경주기 고려 • 비밀번호 도용, 무작위 대입 공격 등에 대한 대응 필요 • 시스템 설치 시 제품 등에서 제공하는 디폴트 계정 및 비밀번호 사용정지 또는 변경 필요
소유 기반	인증서(PKI)	• 개인키의 안전한 보관 필요(안전한 보안매체에 보관 권고)
	OTP (One Time Password)	• OTP토큰, 모바일OTP 등 다양한 방식 존재
	기타	• 스마트 카드 방식 • 물리적 보안토큰 방식 등
생체 기반	지문, 홍채, 얼굴 등	• 생체인식정보의 안전한 관리 필요 ※ 참고 : FIDO(Fast Identity Online)
기타 방식 (사용자 인증의 보완통제로 적용 가능)	IP주소	• 특정 IP주소에서만 해당 ID로 접속할 수 있도록 제한하는 방식
	MAC주소	• 단말기의 MAC주소를 기반으로 등록된 단말기에서만 접속할 수 있도록 제한하는 방식
	기기 일련번호	• 특정 PC 또는 특정 디바이스(스마트폰 등)에서만 접속할 수 있도록 제한하는 방식
	기타	• 위치정보를 기반으로 접속을 제한하는 방식 등

▶ 계정 도용 및 불법적인 인증시도 통제방안 예시

구 분	설명
인증 실패횟수 제한	• 일정 횟수 이상 인증에 실패한 경우 접근 제한 ※ 개인정보의 안전성 확보조치 기준 제5조제6항
접속 유지시간 제한	• 접속 후 일정시간 이상 업무처리를 하지 않은 경우 자동으로 접속 차단 (Session Timeout 또는 Idle Timeout 등) ※ 개인정보의 안전성 확보조치 기준 제6조제4항
동시 접속 제한	• 동일 계정으로 동시 접속 시 접속차단 조치 또는 알림 기능 등
불법 로그인 시도 경고	• 국외 IP주소 등 등록되지 않은 IP주소에서의 접속 시 차단 및 통지 • 주말, 야간 접속 시 문자 알림 • 관리자 등 특수권한 로그인 시 알림 등

▶ 업무의 편리성을 제공하기 위하여 싱글사인온(Single Sign-On)을 사용하는 경우에는 계정 도용 시 피해 확대 가능성이 있으므로 위험평가에 기반하여 강화된 인증 적용, 중요 시스템 접속 시 재인증 요구 등 추가 보호대책 마련

■ 인터넷 등 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증수단을 적용하여야 하며, 다만 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

▶ 안전한 인증수단 적용이란 개인정보처리시스템에 사용자계정과 비밀번호를 입력하여 정당한 개인정보 취급자 여부를 식별·인증하는 절차 이외에 추가적인 인증 수단의 적용을 말함

▶ 안전한 인증수단 예시 : 인증서, 보안토큰, 일회용 비밀번호(OTP) 등

▶ 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템 접속 시 인증수단 적용 관련 법적 요구사항 준수 필요

대상 개인정보처리시스템	이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템	이용자의 개인정보를 처리하는 개인정보처리시스템
적용 필요 사항	• 안전한 접속수단 또는 안전한 인증수단 적용 ※ 안전한 접속수단 : 가상사설망(VPN) 등	• 안전한 인증수단 적용

★ [참고] 외부 접속 시 안전한 인증수단 적용(개인정보의 안전성 확보조치 기준 제6조제2항)

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

증거자료

예시

- 정보시스템 및 개인정보처리시스템 로그인 화면
- 로그인 횟수 제한 설정 화면
- 로그인 실패 메시지 화면
- 외부 접속 시 절차(외부접속 신청서, 외부접속자 현황 등)

결함사례

- 사례 1 : 개인정보취급자가 공개된 외부 인터넷망을 통하여 이용자의 개인정보를 처리하는 개인정보처리시스템에 접근 시 안전한 인증수단을 적용하지 않고 ID·비밀번호 방식으로만 인증하고 있는 경우
- 사례 2 : 정보시스템 및 개인정보처리시스템 로그인 실패 시 해당 ID가 존재하지 않거나 비밀번호가 틀림을 자세히 표시해 주고 있으며, 로그인 실패횟수에 대한 제한이 없는 경우

항 목	2.5.4 비밀번호 관리
인증기준	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
주요 확인사항	• 정보시스템에 대한 안전한 사용자 비밀번호 관리절차 및 작성규칙을 수립·이행하고 있는가? • 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립·이행하고 있는가? • 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

세부 설명

■ 사용자 및 관리자가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 관리절차 및 작성규칙을 수립·이행하여야 한다.

▶ 비밀번호 작성규칙 예시(불가피한 경우를 제외하고는 시스템적으로 강제화)

구 분	내 용
조합 규칙 적용	• 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 8자리 이상 • 문자로만 구성한 경우 최소 10자리 이상(단, 숫자로만 구성할 경우 취약할 수 있음)
변경주기 설정	• 비밀번호 유효기간을 설정하여 주기적으로 변경(단, 주기적 변경 여부 및 변경주기는 위험평가 결과 등을 고려하여 자체적으로 결정)
추측하기 쉬운 비밀번호 설정 제한	• 동일한 문자 반복, 키보드 상에서 나란히 있는 문자열, 일련번호, 연속적인 숫자, 생일, 전화번호 등 추측하기 쉬운 개인정보 및 ID와 비슷한 비밀번호 사용 제한
동일한 비밀번호 재사용 제한	• 비밀번호 변경 시 이전에 사용한 비밀번호 재사용 제한

▶ 비밀번호 관리절차 예시

- 시스템 도입 시 설정된 초기 또는 임시 비밀번호의 변경 후 사용
- 비밀번호 처리(입력, 변경) 시 마스킹 처리
- 종이, 파일, 모바일 기기 등에 비밀번호 기록·저장을 제한하고, 부득이하게 기록·저장하여야 하는 경우 암호화 등의 보호대책 적용
- 침해사고 발생 또는 비밀번호의 노출 징후가 의심될 경우 지체 없이 비밀번호 변경
- 비밀번호 분실 등에 따른 재설정 시 본인확인 절차 수행
- 관리자 비밀번호는 비밀등급에 준하여 관리 등

- 정보주체(이용자)가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 수립·이행하여야 한다.
  - 사용자 및 개인정보취급자 비밀번호 작성규칙을 참고하되, 서비스의 특성 및 위험도 등을 고려하여 적절한 수준에서 비밀번호 작성규칙 적용
  - 비밀번호 분실, 도난 시 본인확인 등을 통한 안전한 재발급 절차 마련 등
- 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.
  - 개인정보취급자 또는 정보주체의 인증수단으로 비밀번호를 사용할 경우 안전한 비밀번호 작성규칙을 수립·적용
  - 비밀번호 외의 인증수단(인증서, PIN, 생체인식, 보안토큰 등)을 사용할 경우 해당 인증수단이 비인가자에게 탈취되거나 도용되지 않도록 보호대책 적용

★ [참고] 개인정보취급자 또는 정보주체의 인증수단 적용·관리(개인정보의 안전성 확보조치 기준 제5조제5항)
⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.

증거자료

예시

- 웹페이지, 정보시스템 및 개인정보처리시스템 비밀번호 설정 화면
- 비밀번호 관리 정책 및 절차

결함사례

- 사례 1 : 정보보호 및 개인정보보호 관련 정책, 지침 등에서 비밀번호 생성규칙의 기준을 정하고 있으나, 일부 정보시스템 및 개인정보처리시스템에서 내부 지침과 상이한 비밀번호를 사용하고 있는 경우
- 사례 2 : 비밀번호 관련 내부 규정에는 비밀번호를 초기화 시 임시 비밀번호를 부여받고 강제적으로 변경하도록 되어 있으나, 실제로는 임시 비밀번호를 그대로 사용하고 있는 경우
- 사례 3 : 비밀번호 관련 내부 규정에는 사용자 및 개인정보취급자의 비밀번호 변경주기를 정하고 이행하도록 하고 있음에도 불구하고 변경하지 않고 그대로 사용하고 있는 경우

항 목	2.5.5 특수 계정 및 권한 관리
인증기준	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.
주요 확인사항	• 관리자 권한 등 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하고 있는가? • 특수 목적을 위하여 부여한 계정 및 권한을 식별하고 별도 목록으로 관리하는 등 통제절차를 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

세부 설명

■ 관리자 등 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하여야 한다.

▶ 정보시스템 관리, 개인정보 및 중요정보 관리 등 특수목적을 위한 계정 및 권한 유형 정의

※ 특수권한(예시)
· 관리자 권한(Root, Administrator, admin, sys, system, sa 등 최상위 권한)
· 배치프로그램 실행을 위하여 부여된 권한
· 보안시스템 관리자 권한
· 계정 생성 및 접근권한을 설정할 수 있는 권한 등

▶ 특수 계정 및 권한이 필요한 경우 공식적인 절차에 따라 신청 및 승인이 이루어질 수 있도록 '특수 계정·권한 발급·변경·해지 절차'를 수립·이행

▶ 특수 계정·권한을 최소한의 업무 수행자에게만 부여할 수 있도록 일반 사용자 계정·권한 발급 절차보다 엄격한 기준 적용(임원 또는 보안책임자 승인 등)

■ 특수 목적을 위하여 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하는 등 통제절차를 수립·이행하여야 한다.

▶ 특수권한자 목록 작성·관리

▶ 특수권한자에 대해서는 예외처리 최소화, 모니터링 강화 등의 통제절차 수립·이행

▶ 정보시스템 유지보수 등 외부자에게 부여하는 특수권한은 필요시에만 생성, 업무 종료 후에는 즉시 삭제 또는 정지하는 절차를 적용

▶ 특수권한자 현황을 정기적으로 검토하여 목록 현행화

증거자료

예시

- 특수권한 관련 지침
- 특수권한 신청·승인 내역
- 특수권한자 목록
- 특수권한 검토 내용

결함사례

- 사례 1 : 정보시스템 및 개인정보처리시스템의 관리자 및 특수권한 부여 등의 승인 이력이 시스템이나 문서상으로 확인이 되지 않거나, 승인 이력과 특수권한 내역이 서로 일치되지 않는 경우
- 사례 2 : 내부 규정에는 개인정보 관리자 및 특수권한 보유자를 목록으로 작성·관리하도록 되어 있으나 이를 작성·관리하고 있지 않거나, 보안시스템 관리자 등 일부 특수권한이 식별·관리되지 않는 경우
- 사례 3 : 정보시스템 및 개인정보처리시스템의 유지보수를 위하여 분기 1회에 방문하는 유지보수용 특수계정이 사용기간 제한없이 상시로 활성화되어 있는 경우
- 사례 4 : 관리자 및 특수권한의 사용 여부를 정기적으로 검토하지 않아 일부 특수권한자의 업무가 변경되었음에도 불구하고 기존 관리자 및 특수권한을 계속 보유하고 있는 경우

항 목	2.5.6 접근권한 검토
인증기준	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
주요 확인사항	• 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남기고 있는가? • 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토주체, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하고 있는가? • 접근권한 검토 결과 접근권한 과다 부여, 권한부여 절차 미준수, 권한 오·남용 등 문제점이 발견된 경우 그에 따른 조치절차를 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

세부 설명

■ 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남겨야 한다.

▶ 사용자 계정 및 접근권한에 대한 내역은 책임추적성을 확보할 수 있도록 필요한 사항을 모두 포함하여 기록

- 계정·접근권한 신청정보 : 신청자 또는 대리신청자, 신청일시, 신청목적, 사용기간 등
- 계정·접근권한 승인정보 : 승인자, 승인 또는 거부 여부, 사유 및 일시 등
- 계정·접근권한 등록정보 : 등록자, 등록일, 등록방법(결재시스템 연동, 수작업 등록 등)
- 계정·접근권한 정보 : 대상 시스템명, 권한명, 권한 내역 등

▶ 접근권한 기록은 법적 요구사항 등을 반영하여 일정기간 이상 보관

- 「개인정보 보호법」에 따른 개인정보처리자 : 최소 3년간 보관

■ 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토주체, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하여야 한다.

▶ 접근권한 검토 주체, 방법, 기준 주기(최소 분기 1회 이상 권고), 결과보고 등 검토 절차 수립

※ 접근권한 부여의 적정성 검토 항목(예시)
· 공식적인 절차에 따른 접근권한 부여 여부
· 접근권한 분류체계의 업무목적 및 보안정책 부합 여부
· 접근권한 승인자의 적절성
· 직무변경 시 기존 권한 회수 후 신규 업무에 대한 적절한 권한 부여 여부
· 업무 목적 외 과도한 접근권한 부여 여부

· 특수권한 부여·변경·발급 현황 및 적정성
· 협력업체 등 외부자 계정·권한 발급 현황 및 적정성
· 접근권한 신청·승인 내역과 실제 접근권한 부여 현황의 일치 여부
· 장기 미접속자 계정 현황 및 삭제(또는 잠금) 여부
· 휴직, 퇴직 시 지체 없이 계정 및 권한 회수 여부 등

■ 접근권한 검토 결과 접근권한 과다 부여, 권한부여 절차 미준수, 권한 오·남용 등 문제점이 발견된 경우 그에 따른 조치절차를 수립·이행하여야 한다.

▶ 접근권한 검토 결과 권한의 과다 부여, 절차 미준수, 권한 오·남용 등 의심스러운 상황이 발견된 경우 소명요청 및 원인분석, 보완대책 마련, 보고체계 등이 포함된 절차 수립·이행

▶ 접근권한 검토 후 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지

▶ 유사한 문제가 반복될 경우 근본 원인 분석 및 재발방지 대책 수립 등

증거자료

예시

- 접근권한 검토 기준 및 절차
- 접근권한 검토 이력
- 접근권한 검토 결과보고서 및 후속조치 내역

결함사례

- 사례 1 : 접근권한 검토와 관련된 방법, 점검주기, 보고체계, 오·남용 기준 등이 관련 지침에 구체적으로 정의되어 있지 않아 접근권한 검토가 정기적으로 수행되지 않은 경우
- 사례 2 : 내부 정책, 지침 등에 장기 미사용자 계정에 대한 잠금(비활성화) 또는 삭제 조치하도록 되어 있으나, 6개월 이상 미접속한 사용자의 계정이 활성화되어 있는 경우(접근권한 검토가 충실히 수행되지 않아 해당 계정이 식별되지 않은 경우)
- 사례 3 : 접근권한 검토 시 접근권한의 과다 부여 및 오·남용 의심사례가 발견되었으나, 이에 대한 상세조사, 내부보고 등의 후속조치가 수행되지 않은 경우

2.6. 접근통제

항 목	2.6.1 네트워크 접근
인증기준	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.
주요 확인사항	• 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가? • 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하고 있는가? • 네트워크 대역별 IP주소 부여 기준을 마련하고 데이터베이스 서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가? • 물리적으로 떨어진 IDC, 지사, 대리점 등과의 네트워크 연결 시 전송구간 보호대책을 마련하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

■ 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고, 네트워크에 대한 비인가 접근 등 관련 위험을 효과적으로 예방·대응할 수 있도록 네트워크 접근통제 관리절차를 수립·이행하여야 한다.

▶ 정보시스템, 개인정보처리시스템, PC 등에 IP주소 부여 시 승인절차에 따라 부여하는 등 허가되지 않은 IP사용 통제

▶ 비인가자 및 단말의 내부 네트워크 접근 통제

▶ 네트워크 장비에 설치된 불필요한 서비스 및 포트 차단 등

■ 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하여야 한다.

▶ 위험평가를 통하여 핵심 업무영역의 네트워크 분리 및 영역 간 접근통제 수준 결정

접근통제 영역	접근통제 적용 예시
DMZ	• 외부 서비스를 위한 웹서버, 메일서버 등 공개서버는 DMZ에 위치 • DMZ를 경유하지 않은 인터넷에서 내부 시스템으로의 직접 연결은 차단
서버팜	• 다른 네트워크 영역과 구분하여 구성 • 인가받은 내부 사용자의 접근만 허용하도록 접근통제 정책 적용

접근통제 영역	접근통제 적용 예시
DB존	• 개인정보 등 중요정보가 저장된 데이터베이스가 위치한 네트워크 영역은 다른 네트워크 영역과 분리
운영자 환경	• 서버, 보안장비, 네트워크 장비 등을 운영하는 운영자 네트워크 영역은 일반 사용자 네트워크 영역과 분리
개발 환경	• 개발업무(개발서버, 테스트서버 등)에 사용되는 네트워크는 운영 네트워크와 분리
외부자 영역	• 외부 인력이 사용하는 네트워크 영역(외주용역, 민원실, 교육장 등)은 내부 업무용 네트워크와 분리
기타	• 업무망의 경우 업무의 특성, 중요도에 따라 네트워크 대역 분리기준을 수립하여 운영 • 클라우드 서비스를 이용하는 경우 클라우드 환경의 특성을 반영한 접근통제 기준을 수립·이행 • 다만 기업의 규모 등을 고려하여 서버팜과 데이터베이스팜 등을 구분하기 어려운 경우 위험평가 결과 등을 기반으로 보완대책을 적용할 필요가 있음 (호스트 기반 접근통제 등)

- ▶ 접근통제 정책에 따라 분리된 네트워크 영역 간에는 침입차단시스템, 네트워크 장비 ACL 등을 활용하여 네트워크 영역 간 업무수행에 필요한 서비스의 접근만 허용하도록 통제

■ 네트워크 대역별 IP주소 부여 기준을 마련하고 데이터베이스 서버 등 중요 시스템이 외부와의 연결을 필요로 하지 않은 경우 사설 IP로 할당하여 외부에서 직접 접근이 불가능하도록 설정하여야 한다.

- ▶ IP주소 할당 현황을 최신으로 유지하고, 외부에 유출되지 않도록 대외비 이상으로 안전하게 관리
- ▶ 내부망에서의 주소 체계는 사설 IP주소 체계를 사용하고 외부에 내부 주소체계가 노출되지 않도록 NAT(Network Address Translation) 기능 적용
- ▶ 사설 IP주소를 할당하는 경우 국제표준에 따른 사설 IP주소 대역 사용

※ 사설 IP주소 대역
· A Class : 10.0.0.1 ~ 10.255.255.255
· B Class : 172.16.0.1 ~ 172.31.255.255
· C Class : 192.168.0.1 ~ 192.168.255.255

■ 물리적으로 떨어진 IDC, 지사, 대리점, 협력업체, 고객센터 등과의 네트워크 연결 시 전용회선 또는 VPN (가상사설망) 등을 활용하여 안전한 접속환경을 구성하여야 한다.

증거자료

예시

- 네트워크 구성도
- IP 관리대장
- 정보자산 목록
- 방화벽룰

결함사례

- 사례 1 : 네트워크 구성도와 인터뷰를 통하여 확인한 결과, 외부 지점에서 사용하는 정보시스템 및 개인정보처리시스템과 IDC에 위치한 서버 간 연결 시 일반 인터넷 회선을 통하여 데이터 송수신을 처리하고 있어 내부 규정에 명시된 VPN이나 전용망 등을 이용한 통신이 이루어지고 있지 않은 경우
- 사례 2 : 내부망에 위치한 데이터베이스 서버 등 일부 중요 서버의 IP주소가 내부 규정과 달리 공인 IP로 설정되어 있고, 네트워크 접근 차단이 적용되어 있지 않은 경우
- 사례 3 : 서버팜이 구성되어 있으나, 네트워크 접근제어 설정 미흡으로 내부망에서 서버팜으로의 접근이 과도하게 허용되어 있는 경우
- 사례 4 : 외부자(외부 개발자, 방문자 등)에게 제공되는 네트워크를 별도의 통제 없이 내부 업무 네트워크와 분리하지 않은 경우
- 사례 5 : 내부 규정과는 달리 MAC주소 인증, 필수 보안 소프트웨어 설치 등의 보호대책을 적용하지 않은 상태로 네트워크 케이블 연결만으로 사내 네트워크에 접근 및 이용할 수 있는 경우

항 목	2.6.2 정보시스템 접근
인증기준	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
주요 확인사항	• 서버, 네트워크시스템, 보안시스템 등 정보시스템별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가? • 정보시스템에 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가? • 정보시스템의 사용목적과 관계 없는 서비스를 제거하고 있는가? • 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

- 서버, 네트워크시스템, 보안시스템 등 정보시스템별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하여야 한다.
  - 계정 및 권한 신청·승인 절차
  - 사용자별로 개별 계정 부여 및 공용 계정 사용 제한
  - 계정 사용 현황에 대한 정기 검토 및 현행화 관리 : 장기 미사용 계정, 불필요한 계정 존재 여부 등
  - 접속 위치 제한 : 접속자 IP주소 제한 등
  - 관리자 등 특수권한에 대한 강화된 인증수단 고려 : 인증서, OTP 등
  - 안전한 접근수단 적용 : SSH, SFTP
  - 동일 네트워크 영역 내 서버 간 접속에 대한 접근통제 조치 등
- 정보시스템에 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 조치하여야 한다.
  - 서버별 특성, 업무 환경, 위험의 크기, 법적 요구사항 등을 고려하여 세션 유지시간 설정
- 정보시스템의 사용 목적과 관련이 없거나 침해사고를 유발할 수 있는 서비스 또는 포트를 확인하여 제거 또는 차단하여야 한다.
  - 안전하지 않은 서비스, 프로토콜, 데몬에 대해서는 추가 보안기능 구현
  - Netbios, File-Sharing, Telnet, FTP 등과 같은 안전하지 않은 서비스·프로토콜은 불가피한 사유가 없는 한 사용을 제한하고 SSH, SFTP, IPSec VPN 등과 같은 안전한 기술 사용
- 주요서비스를 제공하는 서버는 독립된 서버로 운영하여야 한다.

▶ 외부에 직접 서비스를 제공하거나 민감한 정보를 보관·처리하고 있는 웹서버, 데이터베이스 서버, 응용프로그램 등은 공용 장비로 사용하지 않고 독립된 서버 사용

증거자료

예시

- 정보시스템 운영체제 계정 목록
- 서버 보안 설정
- 서버접근제어 정책(SecureOS 관리화면 등)
- 서버 및 네트워크 구성도
- 정보자산 목록

결함사례

- 사례 1 : 사무실에서 서버관리자가 IDC에 위치한 윈도우 서버에 접근 시 터미널 서비스를 이용하여 접근하고 있으나, 터미널 서비스에 대한 세션 타임아웃 설정이 되어 있지 않아 장시간 아무런 작업을 하지 않아도 해당 세션이 차단되지 않는 경우
- 사례 2 : 서버 간 접속이 적절히 제한되지 않아 특정 사용자가 본인에게 인가된 서버에 접속한 후 해당 서버를 경유하여 다른 인가받지 않은 서버에도 접속할 수 있는 경우
- 사례 3 : 타당한 사유 또는 보완 대책 없이 안전하지 않은 접속 프로토콜(telnet, ftp 등)을 사용하여 접근하고 있으며, 불필요한 서비스 및 포트를 오픈하고 있는 경우
- 사례 4 : 모든 서버로의 접근은 서버접근제어 시스템을 통하도록 접근통제 정책을 가져가고 있으나, 서버접근제어 시스템을 통하지 않고 서버에 접근할 수 있는 우회 경로가 존재하는 경우

항 목	2.6.3 응용프로그램 접근
인증기준	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
주요 확인사항	• 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 차등 부여하고 있는가? • 일정시간 동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가? • 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하고 있는가? • 개인정보 및 중요정보의 표시제한 보호조치의 일관성을 확보할 수 있도록 관련 기준을 수립하여 적용하고 있는가? • 개인정보 및 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하여 운영하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근권한의 관리), 제6조(접근통제), 제12조(출력·복사시 안전조치)

세부 설명

■ 중요정보의 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 차등 부여하여야 한다.

▶ 내부에서 사용하는 응용프로그램(백오피스시스템, 회원관리시스템 등)을 명확하게 식별

▶ 응용프로그램 중 개인정보를 처리하는 개인정보처리시스템 식별

▶ 최소권한 원칙에 따른 사용자 및 개인정보취급자 접근권한 분류체계(권한분류표 등) 마련

▶ 중요정보 및 개인정보 처리(입력, 조회, 변경, 삭제, 다운로드, 출력 등) 권한을 세분화하여 설정할 수 있도록 응용프로그램 기능 구현

▶ 식별된 응용프로그램 및 개인정보처리시스템에 대한 계정 및 권한을 부여하는 절차 수립·이행

▶ 권한 부여·변경·삭제 관련 기록을 보관하여 접근권한의 타당성 검토

■ 일정시간 동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하여야 한다.

▶ 응용프로그램 및 업무별 특성, 위험의 크기 등을 고려하여 접속유지 시간 결정 및 적용

▶ 개인정보처리시스템의 경우 법적 요구사항에 따라 일정시간 이상 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 조치

▶ 동일 계정으로 동시 접속 시 경고 문자 표시 및 접속 제한

■ 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하여야 한다.

▶ 관리자 전용 응용프로그램의 외부 공개 차단 및 IP주소 등을 통한 접근제한 조치

▶ 불가피하게 외부 공개가 필요한 경우 안전한 인증수단(OTP 등) 또는 안전한 접속수단(VPN 등) 적용

▶ 관리자(사용자), 개인정보취급자의 접속 로그 및 이벤트 로그에 대한 정기적 모니터링

▶ 이상징후 발견 시 세부조사, 내부보고 등 사전에 정의된 절차에 따라 이행

■ 개인정보 및 중요정보 표시제한 조치의 일관성 확보를 위하여 관련 기준을 수립·적용하여야 한다.

▶ 개인정보 및 중요정보 표시제한 조치 기준 예시

1. 성명 : 성명의 가운데 글자(단, 성명이 2글자인 경우 뒷글자, 성명이 4글자 이상인 경우 첫 번째 글자와 마지막 글자를 제외한 글자)
2. 주민등록번호 : 13자리 중 뒤 7자리
3. 전화번호, 휴대전화 : 국번
4. 주소 : 도로명 이하의 건물번호 및 상세주소의 숫자
5. 이메일주소 : ID 중 앞 2자리를 제외한 나머지
6. 카드번호 : 7번째 번호부터 6자리
7. IP 주소 : 17-24비트(Ver. 4), 113-128비트(Ver. 6) 등

※ 개인정보 및 중요정보 표시제한 조치 적용(예시)
· 성명 : 현*, 김*하, 김*우, 선**녀
· 주민등록번호 : 040101-*******
· 휴대전화번호 : 010-****-0913
· 주소 : 서울시 성북구 북악산로 *** ***동 ****호
· 이메일주소 : ma******@abcd.com
· 카드번호 : 4558-12**-****-0116
· IP주소 : 123.123.***.123

■ 개인정보 및 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하여 운영하여야 한다.

▶ 응용프로그램(개인정보처리시스템 등)에서 개인정보 및 중요정보 출력 시(인쇄, 화면표시, 다운로드 등) 용도를 특정하고 용도에 따라 출력항목 최소화

▶ 업무 수행 형태 및 목적, 유형, 장소 등 여건 및 환경에 따라 개인정보처리시스템에 대한 접근권한 범위 내에서 최소한의 개인정보 출력

▶ 업무상 반드시 필요한 경우가 아니라면 개인정보 검색 시 like 검색이 되지 않도록 조치

▶ 개인정보 검색 시에는 불필요하거나 과도한 정보가 조회되지 않도록 일치검색(equal검색) 또는 두 가지 항목 이상의 검색조건 사용 등

- 오피스 파일(엑셀 등)에서 개인정보가 숨겨진 필드 형태로 저장되지 않도록 조치
- 웹페이지 소스 보기 등을 통하여 불필요한 개인정보가 출력되지 않도록 조치 등

증거자료

예시

- 응용프로그램 접근권한 분류 체계
- 응용프로그램 계정·권한 관리 화면
- 응용프로그램 사용자·관리자 화면(개인정보 조회 등)
- 응용프로그램 세션 타임 및 동시접속 허용 여부 내역
- 응용프로그램 관리자 접속로그 모니터링 내역
- 정보자산 목록
- 개인정보처리시스템의 개인정보 조회, 검색 화면
- 개인정보 마스킹 표준
- 개인정보 마스킹 적용 화면

결함사례

- 사례 1 : 응용프로그램의 개인정보 처리화면 중 일부 화면의 권한 제어 기능에 오류가 존재하여 개인정보 열람 권한이 없는 사용자에게도 개인정보가 노출되고 있는 경우
- 사례 2 : 응용프로그램의 관리자 페이지가 외부인터넷에 오픈되어 있으면서 안전한 인증수단이 적용되어 있지 않은 경우
- 사례 3 : 응용프로그램에 대하여 타당한 사유 없이 세션 타임아웃 또는 동일 사용자 계정의 동시 접속을 제한하고 있지 않은 경우
- 사례 4 : 응용프로그램을 통하여 개인정보를 다운로드받는 경우 해당 파일 내에 주민등록번호 등 업무상 불필요한 정보가 과도하게 포함되어 있는 경우
- 사례 5 : 응용프로그램의 개인정보 조회화면에서 like 검색을 과도하게 허용하고 있어, 모든 사용자가 본인의 업무 범위를 초과하여 성씨만으로도 전체 고객 정보를 조회할 수 있는 경우
- 사례 6 : 개인정보 표시제한 조치 기준이 마련되어 있지 않거나 이를 준수하지 않는 등의 사유로 동일한 개인정보 항목에 대하여 개인정보처리시스템 화면별로 서로 다른 마스킹 기준이 적용된 경우
- 사례 7 : 개인정보처리시스템의 화면상에는 개인정보가 마스킹되어 표시되어 있으나, 웹브라우저 소스보기를 통하여 마스킹되지 않은 전체 개인정보가 노출되는 경우

항 목	2.6.4 데이터베이스 접근
인증기준	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
주요 확인사항	• 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 있는가? • 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제5조(접근권한의 관리), 제6조(접근통제)

세부 설명

- 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 지속적으로 현행화하여 관리하여야 한다.
  - 데이터베이스에서 사용되는 테이블 목록, 저장되는 정보, 상관관계 등을 식별
  - 중요정보 및 개인정보의 저장 위치(데이터베이스 및 테이블명·컬럼명) 및 현황(건수, 암호화 여부 등) 식별
  - 데이터베이스 현황에 대하여 정기적으로 조사하여 현행화 관리
- 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하여야 한다.
  - 데이터베이스 접속 권한을 관리자(DBA), 사용자로 구분하여 직무별 접근통제 정책 수립·이행(최소권한 원칙에 따른 테이블, 뷰, 컬럼, 쿼리 레벨에서 접근통제 등)
  - 중요정보가 포함된 테이블, 컬럼은 업무상 처리 권한이 있는 자만 접근할 수 있도록 제한
  - DBA 권한이 부여된 계정과 조회 등 기타 권한이 부여된 계정 구분
  - 응용프로그램에서 사용하는 계정과 사용자 계정의 공용 사용 제한
  - 계정별 사용 가능 명령어 제한
  - 사용하지 않는 계정, 테스트용 계정, 기본 계정 등 삭제
  - 일정시간 이상 업무를 수행하지 않는 경우 자동 접속차단
  - 비인가자의 데이터베이스 접근 제한
  - 개인정보를 저장하고 있는 데이터베이스는 DMZ 등 공개된 네트워크에 위치하지 않도록 제한
  - 다른 네트워크 영역 및 다른 서버에서의 비인가 접근 차단
  - 데이터베이스 접근을 허용하는 IP주소, 포트, 응용프로그램 제한
  - 일반 사용자는 원칙적으로 응용프로그램을 통해서만 데이터베이스에 접근 가능하도록 조치 등

증거자료

예시

- 데이터베이스 현황(테이블, 컬럼 등)
- 데이터베이스 접속자 계정·권한 목록
- 데이터베이스 접근제어 정책(데이터베이스 접근제어시스템 관리화면 등)
- 네트워크 구성도(데이터베이스존 등)
- 정보자산 목록

결함사례

- 사례 1 : 대량의 개인정보를 보관·처리하고 있는 데이터베이스를 인터넷을 통하여 접근 가능한 웹 응용프로그램과 분리하지 않고 물리적으로 동일한 서버에서 운영하고 있는 경우
- 사례 2 : 개발자 및 운영자들이 응응 프로그램에서 사용하고 있는 계정을 공유하여 운영 데이터베이스에 접속하고 있는 경우
- 사례 3 : 내부 규정에는 데이터베이스의 접속권한을 오브젝트별로 제한하도록 되어 있으나, 데이터베이스 접근권한을 운영자에게 일괄 부여하고 있어 개인정보 테이블에 접근할 필요가 없는 운영자에게도 과도하게 접근 권한이 부여된 경우
- 사례 4 : 데이터베이스 접근제어 솔루션을 도입하여 운영하고 있으나, 데이터베이스 접속자에 대한 IP주소 등이 적절히 제한되어 있지 않아 데이터베이스 접근제어 솔루션을 우회하여 데이터베이스에 접속하고 있는 경우
- 사례 5 : 개인정보를 저장하고 있는 데이터베이스의 테이블 현황이 파악되지 않아, 임시로 생성된 테이블에 불필요한 개인정보가 파기되지 않고 대량으로 저장되어 있는 경우

항 목	2.6.5 무선 네트워크 접근
인증기준	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위하여 인증, 송수신 데이터 암호화 등 보호대책을 수립·이행하고 있는가? • 인가된 임직원만이 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립·이행하고 있는가? • AD Hoc 접속 및 조직 내 허가받지 않은 무선 AP 탐지·차단 등 비인가된 무선네트워크에 대한 보호대책을 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

- 무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위하여 인증, 송수신 데이터 암호화 등 다음의 사항을 고려하여 보호대책을 수립·이행하여야 한다.
  - 무선네트워크 장비(AP 등) 목록 관리
  - 사용자 인증 및 정보 송수신 시 암호화 기능 설정(WPA2-Enterprise mode, WPA3-Enterprise mode 등)
  - 무선 AP 접속 단말 인증 방안(MAC 인증 등)
  - SSID 숨김 기능 설정
  - 무선네트워크에 대한 ACL 설정
  - 무선 AP의 관리자 접근 통제(IP제한) 등
- 인가된 임직원만이 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립·이행하여야 한다.
  - 무선네트워크 사용권한 신청 및 승인 절차(사용자 및 접속단말 등록 등)
  - 퇴직, 기간 만료 등의 사유로 무선네트워크 사용이 필요하지 않은 경우 접근권한 해지 절차
  - 외부인에게 제공하는 무선네트워크는 임직원이 사용하는 무선네트워크와 분리 등
- AD Hoc 접속 및 조직 내 허가받지 않은 무선 AP 탐지·차단 등 비인가된 무선네트워크에 대한 보호대책을 수립·이행하여야 한다.
  - WIPS(무선침입방지시스템) 설치·운영, 주기적으로 비인가 AP(Rogue AP) 설치 여부 점검 등

증거자료

예시

- 네트워크 구성도
- AP 보안 설정 내역
- 비인가 무선 네트워크 점검 이력
- 무선네트워크 사용 신청·승인 이력

결함사례

- 사례 1 : 외부인용 무선 네트워크와 내부 무선 네트워크 영역대가 동일하여 외부인도 무선네트워크를 통하여 별도의 통제 없이 내부 네트워크에 접근이 가능한 경우
- 사례 2 : 무선 AP 설정 시 정보 송수신 암호화 기능을 설정하였으나, 안전하지 않은 방식으로 설정한 경우
- 사례 3 : 업무 목적으로 내부망에 연결된 무선AP에 대하여 무선AP 관리자 비밀번호 노출(디폴트 비밀번호 사용), 접근제어 미적용 등 보안 설정이 미흡한 경우

항 목	2.6.6 원격접근 통제
인증기준	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 장애대응 등 부득이하게 허용하는 경우 보완대책을 마련하고 있는가? • 내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가? • 재택근무, 원격협업, 스마트워크 등과 같은 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호대책을 수립·이행하고 있는가? • 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리시스템에 접속하는 단말기는 관리용 단말기로 지정하고 임의조작 및 목적 외 사용 금지 등 안전조치를 적용하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

- 인터넷과 같은 외부 네트워크를 통한 중요정보(개인정보) 처리, 정보시스템, 개인정보처리시스템과 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 원격운영은 원칙적으로 금지하고 부득이하게 허용하는 경우 다음과 같은 대책을 수립·이행하여야 한다.
  - 원격 운영 및 접속에 대한 책임자의 승인
  - 안전한 인증수단(인증서, OTP 등) 적용
  - 안전한 접속수단(VPN 등) 적용
  - 한시적 접근권한 부여 및 권한자 현황 관리
  - 백신 설치, 보안패치 등 접속 단말 보안
  - 원격운영 현황 모니터링(VPN 계정 발급·사용 현황의 주기적 검토 등)
  - 원격접속 기록 로깅 및 주기적 분석
  - 원격 운영 관련 보안인식 교육 등
- 내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하여야 한다.
  - 접속 가능한 단말을 IP주소, MAC주소 등으로 제한
  - 정상적인 원격접속 경로를 우회한 접속경로 차단 등

- 재택근무, 원격협업, 스마트워크 등과 같은 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호대책을 수립·이행하여야 한다.
  - 스마트워크 업무형태 정의 : 재택근무, 스마트워크 센터, 원격협업, 모바일오피스 환경
  - 스마트워크 업무형태에 따른 업무 허가 범위 설정 : 내부 시스템 및 서비스 원격접근 허용 범위
  - 스마트워크 업무 승인절차 : 스마트워크를 위한 원격접근 권한 신청, 승인, 회수 등
  - 원격접근에 필요한 기술적 보호대책 : 전송구간 암호화(VPN 등), 강화된 사용자 인증(OTP 등)
  - 접속 단말(PC, 모바일 기기 등) 보안 : 백신 설치, 보안패치 적용, 단말 인증, 분실·도난 시 대책(신고절차, 단말잠금, 중요정보 삭제 등), 중요정보 저장 금지(필요시 암호화 조치) 등
  - 스마트워크 업무환경 정보보호지침 수립 및 교육 등
- 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리시스템에 접속하는 단말기(관리용 단말기 또는 중요단말기)에 대하여 다음과 같은 보호조치를 적용하여야 한다.
  - 관리용 단말기 지정 및 목록관리
  - 인가받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
  - 등록된 관리용 단말기 이외에는 접근하지 못하도록 조치
  - 본래 목적 외로 사용되지 않도록 조치
  - 관리용 단말기에 악성프로그램 감염 방지 등을 위한 보호조치 적용 등

증거자료

예시

- VPN 등 사외접속 신청서
- VPN 계정 목록
- VPN 접근제어 정책 설정 현황
- IP 관리대장
- 원격 접근제어 설정(서버 설정, 보안시스템 설정 등)
- 관리용 단말기 지정 및 관리 현황
- 네트워크 구성도

결함사례

- 사례 1 : 내부 규정에는 시스템에 대한 원격 접근은 원칙적으로 금지하고 불가피한 경우 IP 기반의 접근통제를 통하여 승인된 사용자만 접근할 수 있도록 명시하고 있으나, 시스템에 대한 원격 데스크톱 연결, SSH 접속이 IP주소 등으로 제한되어 있지 않아 모든 PC에서 원격 접속이 가능한 경우
- 사례 2 : 원격운영관리를 위하여 VPN을 구축하여 운영하고 있으나, VPN에 대한 사용 승인 또는 접속 기간 제한 없이 상시 허용하고 있는 경우
- 사례 3 : 외부 근무자를 위하여 개인 스마트 기기에 업무용 모바일 앱을 설치하여 운영하고 있으나, 악성코드, 분실·도난 등에 의한 개인정보 유출을 방지하기 위한 적절한 보호대책(백신, 초기화, 암호화 등)을 적용하고 있지 않은 경우
- 사례 4 : 외부 접속용 VPN에서 사용자별로 원격접근이 가능한 네트워크 구간 및 정보시스템을 제한하지 않아 원격접근 인증을 받은 사용자가 전체 내부망 및 정보시스템에 과도하게 접근이 가능한 경우

항 목	2.6.7 인터넷 접속 통제
인증기준	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스 (P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
주요 확인사항	• 주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제정책을 수립·이행하고 있는가? • 주요 정보시스템(DB서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가? • 관련 법령에 따라 인터넷망 차단 의무가 부과된 경우 대상자를 식별하여 안전한 방식으로 인터넷망 차단 조치를 적용하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

■ 인터넷을 통한 정보유출, 악성코드 감염, 내부망 침투 등의 위험을 적절한 수준으로 감소시키기 위하여 주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제정책을 수립·이행하여야 한다.

▶ 인터넷 연결 시 네트워크 구성 정책

▶ 외부 이메일 사용, 인터넷 사이트 접속, 소프트웨어 다운로드 및 전송 등 사용자 접속정책

▶ 유해사이트(성인, 오락 등) 접속 차단 정책

▶ 정보 유출 가능 사이트(웹하드, P2P, 원격접속 등) 접속 차단 정책

▶ 망분리 또는 인터넷망 차단 조치 관련 정책(망분리 적용 여부, 망분리 대상자, 망분리 방식, 망간 자료전송 절차 등)

▶ 인터넷 접속내역 검토(모니터링) 정책 등

■ 주요 정보시스템(데이터베이스 서버 등)에서 불필요한 외부 인터넷 접속을 통제하여야 한다.

▶ 악성코드 유입, 정보 유출, 역방향 접속 등이 차단되도록 내부 서버(DB서버, 파일서버 등) 에서 외부 인터넷 접속 제한

▶ 불가피한 사유가 있는 경우 위험분석을 통하여 보호대책을 마련하고 책임자의 승인 후 허용

■ 관련 법령에 따라 인터넷망 차단 의무가 부과된 경우 인터넷망 차단 대상자를 식별하여 안전한 방식으로 인터넷망 차단 조치를 적용하여야 한다.

▶ 개인정보 보호법에 따른 인터넷망 차단 조치 적용 대상

• (의무대상 개인정보처리자) 전년도 말 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상인 개인정보처리자

• (의무대상 컴퓨터 등) 개인정보처리시스템에서 개인정보를 다운로드, 파기, 접근권한을 설정할 수

개인정보취급자의 컴퓨터 등

- (외부 클라우드서비스 이용 시 조치사항) 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치 적용

▶ 다음 사항을 고려하여 안전한 방식으로 인터넷망 차단 조치 적용

- 인터넷망 차단 조치 의무대상 여부 검토 및 의무 대상인 경우 인터넷망 차단 조치 대상자 식별
- 인터넷망 차단 조치 의무대상이 아닌 경우 위험분석 결과 등에 따라 인터넷망 차단 조치 여부 결정
- 물리적(네트워크가 분리된 2대의 PC 구성 등) 또는 논리적(VDI와 같은 가상화 기술 활용 등) 방식으로 인터넷망 차단 조치 적용
- 인터넷망 차단 조치 우회 경로 파악 및 통제대책 적용
- 인터넷망 차단 조치가 적용된 컴퓨터의 안전한 자료전송을 위한 통제 방안 마련
- 인터넷망 차단 조치 환경의 적정성 및 취약점 존재 여부에 대한 정기 점검 수행 등

증거자료

예시

- 비업무사이트(P2P 등) 차단정책(비업무사이트 차단시스템 관리화면 등)
- 인터넷 접속내역 모니터링 이력
- 인터넷망 차단조치 대상자 목록
- 망간 자료 전송 절차 및 처리내역(신청·승인내역 등)
- 네트워크 구성도

결함사례

- 사례 1 : 개인정보 보호법에 따라 인터넷망 차단 조치를 적용하였으나, 개인정보처리시스템의 접근권한 설정 가능자 등 일부 의무대상자에 대하여 인터넷망 차단 조치 적용이 누락된 경우
- 사례 2 : 개인정보 보호법에 따른 인터넷망 차단 조치 의무대상으로서 인터넷망 차단 조치를 적용하였으나, 다른 서버를 경유한 우회접속이 가능하여 인터넷망 차단 조치가 적용되지 않은 환경에서 개인정보처리시스템에 접속하여 개인정보의 다운로드, 파기 등이 가능한 경우
- 사례 3 : DMZ 및 내부망에 위치한 일부 서버에서 불필요하게 인터넷으로의 직접 접속이 가능한 경우
- 사례 4 : 인터넷 PC와 내부 업무용 PC를 물리적 망분리 방식으로 인터넷망 차단 조치를 적용하고 망간 자료전송시스템을 구축·운영하고 있으나, 자료 전송에 대한 승인 절차가 부재하고 자료 전송 내역에 대한 주기적 검토가 이루어지고 있지 않은 경우
- 사례 5 : 내부 규정에는 개인정보취급자가 P2P 및 웹하드 사이트 접속 시 책임자 승인을 거쳐 특정 기간 동안만 허용하도록 되어 있으나, 승인절차를 거치지 않고 예외 접속이 허용된 사례가 다수 존재하는 경우

2.7. 암호화 적용

항 목	2.7.1 암호정책 적용
인증기준	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
주요 확인사항	• 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는가? • 암호정책에 따라 개인정보 및 주요정보의 저장, 전송, 전달 시 암호화를 수행하고 있는가?
관련 법규	• 개인정보 보호법 제24조의2(주민등록번호 처리의 제한), 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

세부 설명

■ 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하여야 한다.

▶ 암호화 대상 : 법적 요구사항, 처리 정보 민감도 및 중요도에 따라 정의

<table>
<tr><th colspan="2" rowspan="2">구분</th><th colspan="2">개인정보 보호법에 따른 암호화 대상 개인정보</th></tr>
<tr><th>이용자가 아닌 정보주체의 개인정보</th><th>이용자의 개인정보</th></tr>
<tr><td rowspan="2">정보통신망을 통한 송·수신 시</td><td>정보통신망</td><td colspan="2">인증정보(비밀번호, 생체인식정보 등)</td></tr>
<tr><td>인터넷망</td><td colspan="2">개인정보
※ 단, 종전의 개인정보의 안전성 확보조치 기준 적용대상의 경우 2024.9.15 시행</td></tr>
<tr><td rowspan="4">저장 시</td><td rowspan="2">저장 위치 무관</td><td colspan="2">인증정보(비밀번호, 생체인식정보 등)
※ 단, 비밀번호는 일방향암호화</td></tr>
<tr><td colspan="2">주민등록번호
※ 법 제24조의2 제2항에 따라 암호화</td></tr>
<tr><td>인터넷구간, DMZ</td><td>고유식별정보</td><td rowspan="2">주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보
※ 저장 위치 무관</td></tr>
<tr><td>내부망</td><td>※ 단, 주민등록번호 외의 고유식별정보를 내부망에 저장하는 경우에는 개인정보 영향평가의 결과 또는 위험도 분석에 따른 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행 가능</td></tr>
<tr><td colspan="2">개인정보취급자 컴퓨터, 모바일기기, 보조저장매체 등에 저장 시</td><td>고유식별정보, 생체인식정보</td><td>개인정보</td></tr>
</table>

▶ 암호화 알고리즘 : 법적 요구사항 등을 고려하여 안전한 암호화 알고리즘 및 보안강도 선택

※ 안전한 암호 알고리즘(예시)('개인정보의 암호화 조치 안내서' 참고)

구분	알고리즘 명칭
대칭키 암호 알고리즘	SEED, ARIA-128/192/256, AES-128/192/256, HIGHT, LEA 등
공개키 암호 알고리즘	RSAES-OAEP 등
일방향 암호 알고리즘	SHA-256/384/512 등

■ 암호정책에 따라 개인정보 및 주요정보의 저장, 전송, 전달 시 암호화를 수행하여야 한다.

▶ 암호화 위치, 시스템 특성 등을 고려하여 암호화 방식 선정 및 적용

※ 암호화 방식(예시)

구분	암호화 방식
정보통신망을 통한 송·수신 시	1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화 송수신 2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송수신 3. 그 밖에 암호화 기술 활용 : VPN, PGP 등
개인정보처리시스템 등 저장 시	1. 응용프로그램 자체 암호화(API 방식) 2. 데이터베이스 서버 암호화(Plug-in 방식) 3. DBMS 자체 암호화(TDE 방식) 4. DBMS 암호화 기능 호출 5. 운영체제 암호화(파일암호화 등) 6. 그 밖의 암호화 기술 활용
업무용 컴퓨터 및 모바일 기기 저장 시	1. 문서도구 자체 암호화(오피스 등에서 제공하는 암호 설정 기능 활용) 2. 암호 유틸리티를 이용한 암호화 3. DRM(Digital Right Management) 기술 적용 등
보조저장매체 저장 시	1. 암호화 기능을 제공하는 보안 저장매체 이용(보안USB 등) 2. 해당 정보를 암호화한 후 보조저장매체에 저장 등

증거자료

예시

- 암호통제 정책(대상, 방식, 알고리즘 등)
- 암호화 적용현황(저장 및 전송 시)
- 위험도 분석 결과(내부망에서 주민등록번호 이외의 고유식별정보 암호화 미적용 시)
- 암호화 솔루션 관리 화면

결함사례

- 사례 1 : 내부 정책·지침에 암호통제 관련 법적 요구사항을 고려한 암호화 대상, 암호 강도, 저장 및 전송 시 암호화 방법, 암호화 관련 담당자의 역할 및 책임 등에 관한 사항이 적절히 명시되지 않은 경우
- 사례 2 : 암호정책을 수립하면서 해당 기업이 적용받는 법규를 잘못 적용하여 암호화 관련 법적 요구사항을 준수하지 못하고 있는 경우(예를 들어, 이용자의 계좌번호를 저장하면서 암호화 미적용)
- 사례 3 : 개인정보취급자 및 정보주체의 비밀번호에 대하여 일방향 암호화를 적용하였으나, 안전하지 않은 MD5 알고리즘을 사용한 경우
- 사례 4 : 개인정보처리자가 관련 법규 및 내부 규정에 따라 인터넷 쇼핑몰에 대하여 보안서버를 적용하였으나, 회원정보 조회 및 변경, 비밀번호 찾기, 비밀번호 변경 등 이용자의 개인정보가 전송되는 일부 구간에 암호화 조치가 누락된 경우
- 사례 5 : 정보시스템 접속용 비밀번호, 인증키 값 등이 시스템 설정파일 및 소스코드 내에 평문으로 저장되어 있는 경우

항 목	2.7.2 암호키 관리
인증기준	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.
주요 확인사항	• 암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가? • 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

세부 설명

- 암호키 생성, 이용, 보관, 배포, 파기에 대하여 다음과 같은 내용이 포함된 정책 및 절차를 수립하여야 한다.
  - 암호키 관리 담당자
  - 암호키 생성, 보관(소산 백업 등) 방법
  - 암호키 배포 대상자 및 배포방법(복호화 권한 부여 포함)
  - 암호키 사용 유효기간(변경 주기) : 암호키 변경 시 비용, 업무중요도 등을 고려하여 결정
  - 암호키 복구 및 폐기 절차와 방법
  - 소스코드에 하드코딩 방식의 암호키 기록 금지에 관한 사항 등
- 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하여야 한다.
  - 암호키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 암호키는 별도의 매체에 저장한 후 안전한 장소에 보관(암호키 관리시스템, 물리적 분리된 곳 등)
  - 암호키에 대한 접근권한 최소화 및 접근 모니터링 등

증거자료

예시

- 암호키 관리정책
- 암호키 관리대장 및 관리시스템 화면

결함사례

- 사례 1 : 암호 정책 내에 암호키 관리와 관련된 절차, 방법 등이 명시되어 있지 않아 담당자별로 암호키 관리 수준 및 방법 상이 등 암호키 관리에 취약사항이 존재하는 경우
- 사례 2 : 내부 규정에 중요 정보를 암호화 할 경우 관련 책임자 승인 하에 암호화 키를 생성하고 암호키 관리대장을 작성하도록 정하고 있으나, 암호키 관리대장에 일부 암호키가 누락되어 있거나 현행화되어 있지 않은 경우
- 사례 3 : 개발시스템에 적용되어 있는 암호키와 운영시스템에 적용된 암호키가 동일하여, 암호화된 실데이터가 개발시스템을 통해 쉽게 복호화가 가능한 경우

2.8. 정보시스템 도입 및 개발 보안

항 목	2.8.1 보안 요구사항 정의
인증기준	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.
주요 확인사항	• 정보시스템을 신규로 도입·개발 또는 변경하는 경우 정보보호 및 개인정보보호 측면의 타당성 검토 및 인수 절차를 수립·이행하고 있는가? • 정보시스템을 신규로 도입·개발 또는 변경하는 경우 법적 요구사항, 최신 취약점 등을 포함한 보안 요구사항을 명확히 정의하고 설계 단계에서부터 반영하고 있는가? • 정보시스템의 안전한 구현을 위한 코딩 표준을 수립하여 적용하고 있는가?

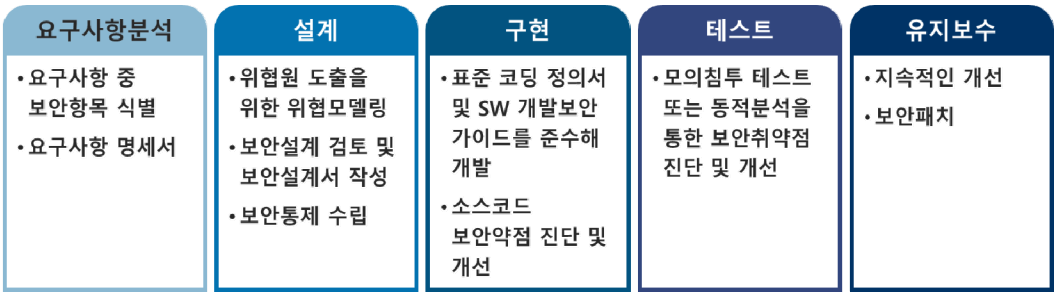
세부 설명

- 정보시스템을 신규로 도입·개발 또는 변경하는 경우 정보보호 및 개인정보보호 측면의 타당성을 검토하고 인수할 수 있도록 절차를 수립·이행하여야 한다.
  - 새로운 정보시스템(서버, 네트워크 장비, 상용 소프트웨어 패키지) 및 보안시스템 도입 시 도입 타당성 분석 등의 내용이 포함된 도입계획 수립
    - 현재 시스템 자원의 이용률, 사용량, 능력한계에 대한 분석
    - 성능, 안정성, 보안성, 신뢰성 및 기존시스템과의 호환성, 상호 운용성 요건
    - 개인정보처리시스템에 해당될 경우 개인정보 보호법(개인정보의 안전성 확보조치 기준 고시 포함) 등에서 요구하는 법적 요구사항 준수
  - 정보보호 및 개인정보보호 측면의 요구사항을 제안요청서(RFP)에 반영하고 업체 또는 제품 선정 시 기준으로 활용
  - 정보시스템 인수 여부를 판단하기 위한 시스템 인수기준 수립
    - 도입계획 수립 시 정의된 성능, 보안성, 법적 요구사항 등을 반영한 인수 승인기준 수립
    - 시스템 도입 과정에서 인수기준을 준수하도록 구매계약서 등에 반영
- 정보시스템을 신규로 도입·개발 또는 변경하는 경우 법적 요구사항, 최신 취약점 등을 포함한 보안 요구사항을 명확히 정의하고 설계 단계에서부터 반영하여야 한다.
  - 개인정보보호 관련 법적 요구사항 : 접근 권한, 접근통제, 암호화, 접속기록 등
  - 상위 기관 및 내부 규정에 따른 정보보호 및 개인정보보호 요구사항
  - 정보보호 관련 기술적 요구사항 : 인증, 개발보안 등
  - 최신 보안취약점 등

■ 정보시스템의 안전한 구현을 위한 코딩 표준을 마련하고 적용하여야 한다.

- ▶ 알려진 기술적 보안 취약점으로 인한 위협을 최소화하기 위하여 안전한 코딩 표준 및 규약 마련
- ▶ Java, PHP, ASP, 웹, 모바일 등 관련된 개발 언어 및 환경을 모두 포함
- ▶ 안전한 코딩 표준 및 규약에 대하여 개발자 대상 교육 수행

※ 소프트웨어 개발보안 방법론(예시)



〈출처〉 소프트웨어 개발보안 가이드(행안부, KISA)

증거자료

예시

- 정보시스템 인수 기준 및 절차
- 정보시스템 도입 RFP(제안요청서) 및 구매계약서
- 개발 산출물(사업수행계획서, 요구사항정의서, 화면설계서, 보안아키텍처 설계서, 시험계획서 등)
- 시큐어 코딩 표준

결함사례

- 사례 1 : 정보시스템 인수 전 보안성 검증 기준 및 절차가 마련되어 있지 않은 경우
- 사례 2 : 신규 시스템 도입 시 기존 운영환경에 대한 영향 및 보안성을 검토하도록 내부 규정을 마련하고 있으나, 최근 도입한 일부 정보시스템에 대하여 인수 시 보안요건에 대해 세부 기준 및 계획이 수립되지 않았으며, 이에 따라 인수 시 보안성검토가 수행되지 않은 경우
- 사례 3 : 개발 관련 내부 지침에 개발과 관련된 주요 보안 요구사항(인증 및 암호화, 보안로그 등)이 정의되어 있지 않은 경우
- 사례 4 : '개발표준정의서'에 사용자 패스워드를 안전하지 않은 암호화 알고리즘(MD5, SHA1)으로 사용하도록 되어 있어 관련 법적 요구사항을 적절히 반영하지 않는 경우

항 목	2.8.2 보안 요구사항 검토 및 시험
인증기준	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.
주요 확인사항	• 정보시스템의 도입, 개발, 변경 시 분석 및 설계 단계에서 정의한 보안 요구사항이 효과적으로 적용되었는지를 확인하기 위한 시험을 수행하고 있는가? • 정보시스템이 안전한 코딩 기준 등에 따라 안전하게 개발되었는지를 확인하기 위한 취약점 점검이 수행되고 있는가? • 시험 및 취약점 점검 과정에서 발견된 문제점이 신속하게 개선될 수 있도록 개선계획 수립, 이행점검 등의 절차를 이행하고 있는가? • 공공기관은 관련 법령에 따라 개인정보처리시스템 신규 개발 및 변경 시 분석·설계 단계에서 영향평가기관을 통하여 영향평가를 수행하고 그 결과를 개발 및 변경 시 반영하고 있는가?
관련 법규	• 개인정보 보호법 제33조(개인정보 영향평가) • 개인정보 영향평가에 관한 고시

세부 설명

■ 정보시스템의 도입, 개발, 변경 시 분석 및 설계 단계에서 정의한 보안 요구사항이 효과적으로 적용되었는지를 확인하기 위한 검토기준과 절차를 수립하고 이에 따른 시험을 수행하여야 한다.

▶ 정보시스템 인수 전 인수기준 적합성 여부를 확인하기 위한 시험 수행

- 정보시스템이 사전에 정의한 보안 요구사항을 만족하여 개발·변경 및 도입되었는지 확인하기 위한 인수기준 및 절차 수립
- 정보시스템을 인수하기 전 사전 정의한 인수기준과의 적합성 여부를 테스트 등을 통하여 확인한 후 인수 여부를 결정
- 시스템 보안 설정, 불필요한 디폴트 계정 제거 여부, 최신 보안취약점 패치 여부 등 확인 필요

▶ 개발·변경 및 구현된 기능이 사전에 정의된 보안 요구사항을 충족하는지 시험 수행

- 시험 계획서, 체크리스트, 시험 결과서 등에 반영

■ 정보시스템이 안전한 코딩 기준 등에 따라 안전하게 개발되었는지를 확인하기 위한 취약점 점검을 수행하여야 한다.

▶ 코딩 완료 후 안전한 코딩 표준 및 규약 준수 여부를 점검하고 기술적 보안 취약점이 존재하는 지 점검 수행

- 시스템이 안전한 코딩표준에 따라 구현하는지 소스코드 검증(소스코드 검증도구 활용 등)
- 코딩이 완료된 프로그램은 운영환경과 동일한 환경에서 취약점 점검도구 또는 모의진단을 통한 취약점 노출 여부 점검

■ 시험 및 취약점 점검 과정에서 발견된 문제점이 신속하게 개선될 수 있도록 개선계획 수립, 이행점검 등의 절차를 이행하여야 한다.

▶ 발견된 문제점은 시스템 오픈 전에 개선될 수 있도록 개선계획 수립, 내부 보고, 이행점검 등의 절차 수립·이행

▶ 불가피한 사유로 시스템 오픈 전에 개선이 어려울 경우에는 이에 따른 영향도 평가, 보완 대책, 내부 보고 등 위험을 줄일 수 있는 대책 마련

■ 공공기관은 관련 법령에 따라 개인정보처리시스템 신규 개발 및 변경 시 분석·설계 단계에서 영향평가기관을 통하여 개인정보 영향평가를 수행하고 그 결과를 개발 및 변경 시 반영하여야 한다.

▶ 공공기관은 개인정보처리시스템 신규 개발 또는 변경을 위한 계획 수립 시 개인정보 영향평가 의무대상 여부를 검토하여 의무 대상인 경우에 영향평가 계획을 수립하고 관련 예산 확보

★ 개인정보 영향평가 의무 대상(개인정보 보호법 시행령 제35조)

1. (5만 명 조건) 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 : 구축·운용 또는 변경하려는 개인정보파일에 5만명 이상의 정보주체에 관한 개인정보가 포함된 경우
2. (50만 명 조건) 다른 개인정보파일과 연계하려는 경우 : 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계한 결과 50만명 이상의 정보주체에 관한 개인정보가 포함된 경우
3. (100만 명 조건) 일반적인 개인정보 파일 : 구축·운용 또는 변경하려는 개인정보파일에 100만명 이상의 정보주체에 관한 개인정보가 포함된 경우
4. (변경 시) 영향평가를 받은 후 개인정보 검색 체계 등 개인정보파일의 운용 체계를 변경하려는 경우 : 해당 개인정보파일 중 변경된 부분

※ 대상 개인정보파일 : 개인정보를 전자적으로 처리할 수 있는 개인정보파일

▶ 공공기관은 개인정보처리시스템 신규 개발 및 변경 시 분석·설계 단계에서 개인정보 보호위원회가 지정한 영향평가기관을 통하여 영향평가를 수행하고 그 결과를 개발 및 변경 시 반영

- 영향평가기관 지정현황은 '개인정보 포털(www.privacy.go.kr)'에서 확인 가능
- 영향평가 수행절차, 평가기준 등은 '개인정보 영향평가 수행안내서' 참고

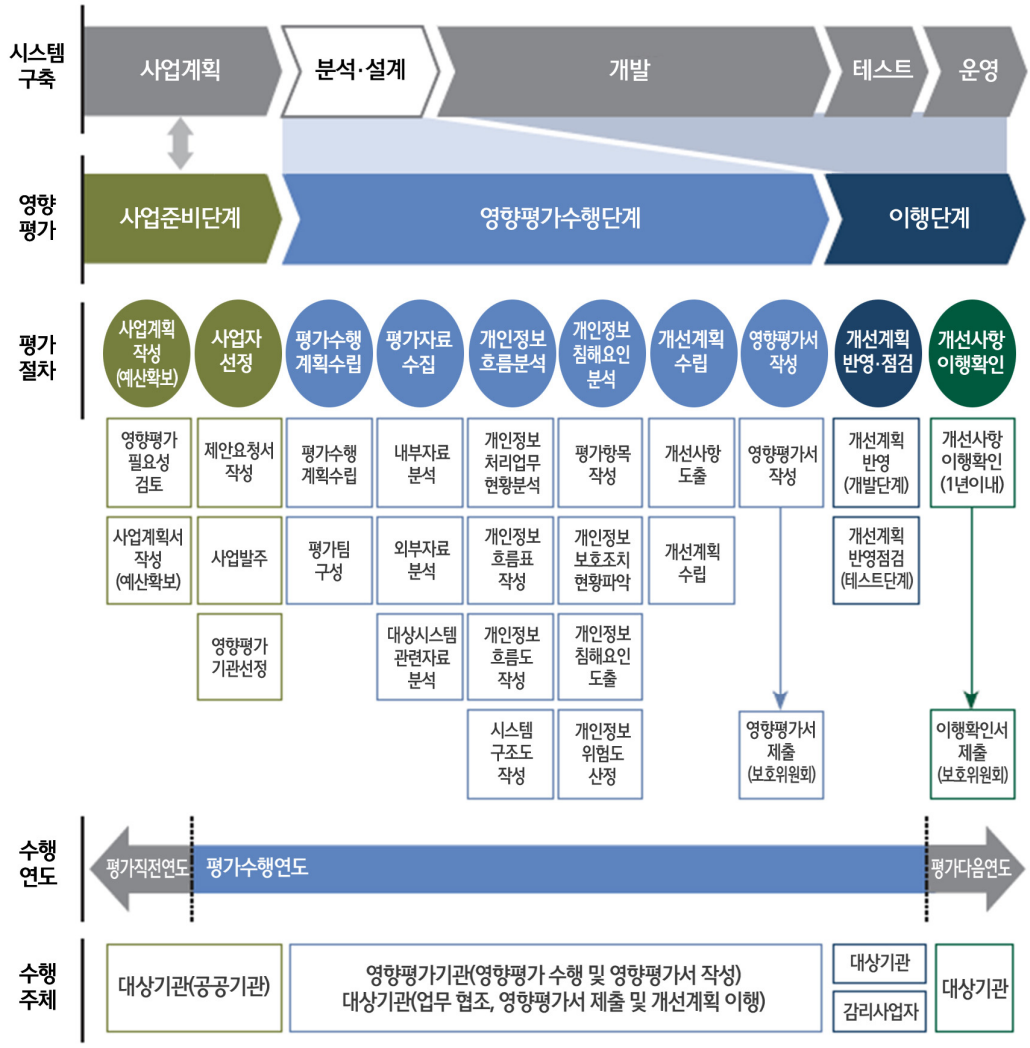
▶ 공공기관은 개인정보 영향평가서를 개인정보처리시스템 오픈 전 및 영향평가 종료 후 2개월 이내에 개인정보 보호위원회에 제출

- 개인정보보호 종합지원시스템(intra.privacy.go.kr)에 영향평가서 등록
- 개인정보 보호위원회 또는 공공기관의 장은 영향평가서를 요약한 내용을 공개할 수 있음

▶ 개인정보 영향평가 결과에 따른 개선요구사항에 대하여 이행 여부를 관리

- 개선요구사항에 대한 상세 이행계획 수립
- 정기적인 이행 상황 점검
- 불가피하게 기간 내 조치가 어려운 경우 타당한 사유를 기록·보고하고 향후 조치를 위한 이행계획 수립
- 영향평가서를 받은 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행현황을 1년 이내에 개인정보 보호위원회에 제출(개선계획 이행점검 확인서)

※ 개인정보 영향평가 절차



〈출처〉 개인정보 영향평가 수행안내서(개인정보 보호위원회, KISA)

증거자료

예시

- 정보시스템 인수 시험 결과
- 요구사항 추적 매트릭스
- 시험 계획서, 시험 결과서
- 취약점 점검 결과서
- 개인정보 영향평가서
- 개인정보 영향평가 개선계획 이행점검 확인서

결함사례

- 사례 1 : 정보시스템 구현 이후 개발 관련 내부 지침 및 문서에 정의된 보안 요구사항을 시험하지 않고 있는 경우
- 사례 2 : 응용프로그램 테스트 시나리오 및 기술적 취약점 점검항목에 입력값 유효성 체크 등의 중요 점검항목 일부가 누락된 경우
- 사례 3 : 구현 또는 시험 과정에서 알려진 기술적 취약점이 존재하는지 여부를 점검하지 않거나, 타당한 사유 또는 승인 없이 확인된 취약점에 대한 개선조치를 이행하지 않은 경우
- 사례 4 : 공공기관이 5만 명 이상 정보주체의 고유식별정보를 처리하는 등 영향평가 의무 대상 개인정보 파일 및 개인정보처리시스템을 신규로 구축하면서 영향평가를 실시하지 않은 경우
- 사례 5 : 공공기관이 영향평가를 수행한 후 영향평가기관으로부터 영향평가서를 받은 지 2개월이 지났음에도 불구하고 영향평가서를 개인정보 보호위원회에 제출하지 않은 경우
- 사례 6 : 신규 시스템 도입 시 기존 운영환경에 대한 영향 및 보안성을 검토(취약점 점검 등)하도록 내부 지침을 마련하고 있으나, 최근 도입한 일부 정보시스템에 대하여 인수 시 취약점 점검 등 보안성검토가 수행되지 않은 경우

항 목	2.8.3 시험과 운영 환경 분리
인증기준	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
주요 확인사항	• 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가? • 불가피한 사유로 개발과 운영환경의 분리가 어려운 경우 상호검토, 상급자 모니터링, 변경 승인, 책임추적성 확보 등의 보안대책을 마련하고 있는가?

세부 설명

- 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하여야 한다.
  - 개발 및 시험 시스템과 운영시스템은 원칙적으로 분리하여 구성
  - 개발자가 불필요하게 운영시스템에 접근할 수 없도록 개발 및 시험 시스템과 운영시스템 간 접근통제 방안 수립·이행
- 불가피한 사유로 개발과 운영환경의 분리가 어려운 경우 상호검토, 상급자 모니터링, 변경 승인, 책임추적성 확보 등의 보안대책을 마련하여야 한다.
  - 조직 규모가 매우 작거나 인적 자원 부족, 시스템 특성 등의 사유로 인하여 불가피하게 개발과 운영환경의 분리가 어려운 경우, 이에 따른 보안 위험을 감소할 수 있도록 적절한 보완통제 수단 적용
    - 직무자 간 상호검토
    - 변경 승인
    - 상급자의 모니터링 및 감사
    - 백업 및 복구 방안, 책임추적성 확보 등

증거자료

예시

- 네트워크 구성도(시험환경 구성 포함)
- 운영 환경과 개발·시험 환경 간 접근통제 적용 현황

결함사례

- 사례 1 : 타당한 사유 또는 승인 없이 별도의 개발환경을 구성하지 않고 운영환경에서 직접 소스코드 변경을 수행하고 있는 경우
- 사례 2 : 불가피하게 개발시스템과 운영시스템을 분리하지 않고 운영 중에 있으나, 이에 대한 상호 검토 내역, 모니터링 내역 등이 누락되어 있는 경우
- 사례 3 : 개발시스템이 별도로 구성되어 있으나, 개발환경으로부터 운영환경으로의 접근이 통제되지 않아 개발자들이 개발시스템을 경유하여 불필요하게 운영시스템 접근이 가능한 경우

항 목	2.8.4 시험 데이터 보안
인증기준	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
주요 확인사항	• 정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가? • 불가피하게 운영데이터를 시험 환경에서 사용할 경우 책임자 승인, 접근 및 유출 모니터링, 시험 후 데이터 삭제 등의 통제 절차를 수립·이행하고 있는가?

세부 설명

- 정보시스템의 개발 및 시험 과정에서 실제 운영데이터의 사용을 제한하여야 한다.
  - 개인정보 및 중요 정보가 시스템 시험과정에서 유출되는 것을 방지하기 위하여 시험데이터는 임의의 데이터를 생성하거나 운영데이터를 가공·변환한 후 사용
  - 시험데이터 변환 및 사용에 따른 기준·절차 수립·이행
- 불가피하게 운영데이터를 시험 환경에서 사용할 경우 책임자 승인, 접근 및 유출 모니터링, 시험 후 데이터 삭제 등의 통제 절차를 수립·이행하여야 한다.
  - 운영데이터 사용 승인 절차 마련 : 데이터 중요도에 따른 보고 및 승인체계 정의 등
  - 시험 기한 만료 후 데이터 폐기절차 마련 및 이행
  - 운영데이터 사용에 대한 시험환경에서의 접근통제 대책 적용
  - 운영데이터 복제·사용에 대한 모니터링 및 정기검토 수행 등

증거자료

예시

- 시험데이터 현황
- 시험데이터 생성 규칙
- 운영데이터를 시험환경에 사용한 경우, 관련 승인 이력

결함사례

- 사례 1 : 개발 서버에서 사용할 시험 데이터 생성에 대한 구체적 기준 및 절차가 수립되어 있지 않은 경우
- 사례 2 : 타당한 사유 및 책임자 승인 없이 실 운영데이터를 가공하지 않고 시험 데이터로 사용하고 있는 경우
- 사례 3 : 불가피한 사유로 사전 승인을 받아 실 운영데이터를 시험 용도로 사용하면서, 테스트 데이터베이스에 대하여 운영 데이터베이스와 동일한 수준의 접근통제를 적용하고 있지 않은 경우
- 사례 4 : 실 운영데이터를 테스트 용도로 사용한 후 테스트가 완료되었음에도 실 운영데이터를 테스트 데이터베이스에서 삭제하지 않은 경우

항 목	2.8.5 소스 프로그램 관리
인증기준	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.
주요 확인사항	• 비인가자에 의한 소스 프로그램 접근을 통제하기 위한 절차를 수립·이행하고 있는가? • 소스 프로그램은 장애 등 비상시를 대비하여 운영환경이 아닌 곳에 안전하게 보관하고 있는가? • 소스 프로그램에 대한 변경이력을 관리하고 있는가?

세부 설명

- 비인가자에 의한 소스 프로그램 접근을 통제하기 위한 절차를 수립·이행하여야 한다.
  - 소스 프로그램의 접근 및 사용에 대한 절차 수립
  - 인가된 개발자 및 담당자만이 접근할 수 있도록 접근권한을 부여하고 비인가자의 접근 차단
  - 소스 프로그램이 보관된 서버(형상관리서버 등)에 대한 접근통제 조치
- 소스 프로그램은 장애 등 비상시를 대비하여 운영환경이 아닌 곳에 안전하게 보관하여야 한다.
  - 최신 소스 프로그램 및 이전 소스 프로그램에 대한 백업 보관
  - 운영환경이 아닌 별도의 환경에 저장·관리
  - 소스 프로그램 백업본에 대한 비인가자의 접근 통제
- 소스 프로그램에 대한 변경이력을 관리하여야 한다.
  - 소스 프로그램 변경 절차 수립 : 승인 및 작업 절차, 버전관리 방안 등
  - 소스 프로그램 변경 이력관리 : 변경·구현·이관 일자, 변경 요청사유, 담당자 등
  - 소스 프로그램 변경에 따른 시스템 관련 문서(설계서 등)에 대한 변경통제 수행
  - 소스 프로그램 변경 이력 및 변경통제 수행내역에 대한 정기적인 검토 수행 등

증거자료

예시

- SVN 등 형상관리시스템 운영 현황(접근권한자 목록 등)
- 소스 프로그램 변경 이력

결함사례

- 사례 1 : 별도의 소스 프로그램 백업 및 형상관리시스템이 구축되어 있지 않으며, 이전 버전의 소스 코드를 운영 서버 또는 개발자 PC에 승인 및 이력관리 없이 보관하고 있는 경우
- 사례 2 : 형상관리시스템을 구축하여 운영하고 있으나 형상관리시스템 또는 형상관리시스템에 저장된 소스코드에 대한 접근제한, 접근 및 변경이력이 적절히 관리되지 않고 있는 경우
- 사례 3 : 내부 규정에는 형상관리시스템을 통하여 소스 프로그램 버전관리를 하도록 되어 있으나, 최신 버전의 소스 프로그램은 개발자 PC에만 보관되어 있고 이에 대한 별도의 백업이 수행되고 있지 않은 경우

항 목	2.8.6 운영환경 이관
인증기준	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.
주요 확인사항	• 신규 도입·개발 및 변경된 시스템을 운영환경으로 안전하게 이관하기 위한 통제 절차를 수립·이행하고 있는가? • 운영환경으로 이관 시 발생할 수 있는 문제에 대한 대응 방안을 마련하고 있는가? • 운영환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?

세부 설명

■ 신규 도입·개발 및 변경된 시스템을 운영환경으로 안전하게 이관하기 위한 통제 절차를 수립·이행하여야 한다.

▶ 개발자 본인 이외의 이관담당자 지정

▶ 시험 완료 여부 확인

▶ 이관 전략(단계적 이관, 일괄적 이관 등)

▶ 이관 시 문제 대응 방안(복귀 방안, 이전 버전의 시스템 보관 방안 등)

▶ 이관에 대한 책임자 승인

▶ 이관에 대한 기록 보존 및 검토 등

※ 클라우드 환경에서 DevOps 방식을 적용한 경우, CI/CD 파이프라인 상에서 통제된 절차에 따라 운영환경으로의 안전한 배포가 수행될 수 있도록 DevSecOps 관점의 통제 방안 적용

■ 운영환경으로 이관 시 발생할 수 있는 문제에 대한 대응 방안을 마련하여야 한다.

▶ 운영환경으로 정보시스템 이관이 원활하게 이루어지지 않았을 경우 복귀(Rollback) 방안

▶ 이전 버전의 시스템 보관 방안(소프트웨어, 부가 프로그램, 구성파일, 파라미터 등) 등

■ 운영환경에는 서비스 실행에 필요한 파일만을 설치하여야 한다.

▶ 운영환경에는 승인되지 않은 개발도구(편집기 등), 소스 프로그램 및 백업본, 업무 문서 등 서비스 실행에 불필요한 파일이 존재하지 않도록 관리

증거자료

예시

- 이관 절차
- 이관 내역(신청·승인, 시험, 이관 등)

결함사례

- 사례 1 : 개발·변경이 완료된 소스 프로그램을 운영환경으로 이관 시 검토·승인하는 절차가 마련되어 있지 않은 경우
- 사례 2 : 운영서버에 서비스 실행에 불필요한 파일(소스코드 또는 배포모듈, 백업본, 개발 관련 문서, 매뉴얼 등)이 존재하는 경우
- 사례 3 : 내부 지침에 운영환경 이관 시 안전한 이관·복구를 위하여 변경작업 요청서 및 결과서를 작성하도록 정하고 있으나, 관련 문서가 확인되지 않은 경우
- 사례 4 : 내부 지침에는 모바일 앱을 앱마켓에 배포하는 경우 내부 검토 및 승인을 받도록 하고 있으나, 개발자가 해당 절차를 거치지 않고 임의로 앱마켓에 배포하고 있는 경우

2.9. 시스템 및 서비스 운영관리

항 목	2.9.1 변경관리
인증기준	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
주요 확인사항	• 정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립·이행하고 있는가? • 정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가?

세부 설명

■ 정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립·이행하여야 한다.

▶ 운영체제 업그레이드, 상용 소프트웨어 설치, 운영 중인 응용프로그램 기능 개선, 네트워크 구성 변경, CPU·메모리·저장장치 증설 등 정보시스템 관련 자산 변경이 필요한 경우 변경을 위한 공식적인 절차 수립 및 이행

※ 변경절차에 포함되어야 할 사항(예시)
· 변경 요청
· 책임자 검토 및 승인
· 변경 확인 및 검증
· 관련 문서 식별 및 변경(자산목록, 운영 매뉴얼, 구성도 등)
· 변경 이력관리 등

■ 정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하여야 한다.

▶ 정보시스템 관련 정보자산 변경이 필요한 경우 변경에 따른 보안, 성능, 업무 등에 미치는 영향을 분석(방화벽 등 보안시스템 정책 변경 필요성, 정책 변경 시 문제점 및 영향도 등)

▶ 변경에 따른 영향을 최소화할 수 있도록 변경을 이행

▶ 변경 실패에 따른 복구방안을 사전에 고려

증거자료

예시

- 변경관리 절차
- 변경관리 수행 내역(신청·승인, 변경 내역 등)
- 변경에 따른 영향분석 결과

결함사례

- 사례 1 : 최근 DMZ 구간 이중화에 따른 변경 작업을 수행하였으나, 변경 후 발생할 수 있는 보안위험성 및 성능 평가에 대한 수행·승인 증거자료가 확인되지 않은 경우
- 사례 2 : 최근 네트워크 변경 작업을 수행하였으나 관련 검토 및 공지가 충분히 이루어지지 않아 네트워크 구성도 및 일부 접근통제시스템(침입차단시스템, 데이터베이스 접근제어시스템 등)의 접근통제 리스트(ACL)에 적절히 반영되어 있지 않은 경우
- 사례 3 : 변경관리시스템을 구축하여 정보시스템 입고 또는 변경 시 성능 및 보안에 미치는 영향을 분석·협의하고 관련 이력을 관리하도록 하고 있으나, 해당 시스템을 통하지 않고도 시스템 변경이 가능하며, 관련 변경사항이 적절히 검토되지 않는 경우

항 목	2.9.2 성능 및 장애관리
인증기준	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.
주요 확인사항	• 정보시스템의 가용성 보장을 위하여 성능 및 용량을 지속적으로 모니터링할 수 있는 절차를 수립·이행하고 있는가? • 정보시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우에 대한 대응절차를 수립·이행하고 있는가? • 정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립·이행하고 있는가? • 장애 발생 시 절차에 따라 조치하고 장애조치보고서 등을 통하여 장애조치내역을 기록하여 관리하고 있는가? • 심각도가 높은 장애의 경우 원인분석을 통한 재발방지 대책을 마련하고 있는가?

세부 설명

- 정보시스템의 가용성 보장을 위하여 성능 및 용량을 지속적으로 모니터링할 수 있도록 다음 사항을 포함한 절차를 수립·이행하여야 한다.
  - 성능 및 용량관리 대상 식별 기준 : 서비스 및 업무 수행에 영향을 줄 수 있는 주요 정보시스템 및 보안시스템을 식별하여 대상에 포함
  - 정보시스템별 성능 및 용량 요구사항(임계치) 정의 : 정보시스템 가용성에 영향을 줄 수 있는 CPU, 메모리, 저장장치 등의 임계치 결정
  - 모니터링 방법 : 성능 및 용량 임계치 초과 여부를 지속적으로 모니터링하고 대처할 수 있는 방법 수립(예 : 알람 등)
  - 모니터링 결과 기록, 분석, 보고
  - 성능 및 용량 관리 담당자 및 책임자 지정 등
- 정보시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우에 대한 대응절차를 수립·이행하여야 한다.
  - 정보시스템의 성능 및 용량 현황을 지속적으로 모니터링하여 요구사항(임계치)을 초과하는 경우 조치방안(예 : 정보시스템, 메모리, 저장장치 증설 등)을 수립·이행
- 정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 다음 항목을 포함하여 수립·이행하여야 한다.
  - 장애유형 및 심각도 정의
  - 장애유형 및 심각도별 보고 절차
  - 장애유형별 탐지 방법 수립 : NMS(Network Management System) 등 관리시스템 활용
  - 장애 대응 및 복구에 관한 책임과 역할 정의
  - 장애기록 및 분석

- 대고객 서비스인 경우 고객 안내 절차
- 비상연락체계(유지보수업체, 정보시스템 제조사) 등

■ 장애 발생 시 절차에 따라 조치하고, 장애조치보고서 등을 통하여 장애조치내역을 기록하여 관리하여야 한다.

※ 장애조치보고서에 포함되어야 할 사항(예시)
· 장애일시
· 장애심각도(예: 상, 중, 하)
· 담당자, 책임자명(유지보수업체 포함)
· 장애내용(장애로 인한 피해 또는 영향 포함)
· 장애원인, 조치내용, 복구내용, 재발방지대책 등

■ 심각도가 높은 장애의 경우 원인분석을 통하여 재발방지 대책을 마련하여야 한다.

- 일상 업무가 중단되는 장애, 과다한 비용(피해)을 초래한 장애, 반복적으로 발생하는 장애 등과 같은 심각한 장애의 경우 원인을 규명하고 재발을 방지하기 위한 대책을 수립·이행하여야 함

증거자료

예시

- 성능 및 용량 모니터링 절차
- 성능 및 용량 모니터링 증거자료(내부보고 결과 등)
- 장애대응 절차
- 장애조치보고서

결함사례

- 사례 1 : 성능 및 용량 관리를 위한 대상별 요구사항(임계치 등)을 정의하고 있지 않거나 정기 점검보고서 등에 기록하고 있지 않아 현황을 파악할 수 없는 경우
- 사례 2 : 성능 또는 용량 기준을 초과하였으나 관련 검토 및 후속조치방안 수립·이행이 이루어지고 있지 않은 경우
- 사례 3 : 전산장비 장애대응절차를 수립하고 있으나 네트워크 구성 및 외주업체 변경 등의 내·외부 환경변화가 적절히 반영되어 있지 않은 경우
- 사례 4 : 장애처리절차와 장애유형별 조치방법 간 일관성이 없거나 예상소요시간 산정에 대한 근거가 부족하여 신속·정확하고 체계적인 대응이 어려운 경우

항 목	2.9.3 백업 및 복구관리
인증기준	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
주요 확인사항	• 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하고 있는가? • 백업된 정보의 완전성과 정확성, 복구절차의 적절성을 확인하기 위하여 정기적으로 복구 테스트를 실시하고 있는가? • 중요정보가 저장된 백업매체의 경우 재해·재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치 의무) • 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

세부 설명

■ 재해·재난, 장애, 침해사고 등으로 인한 정보시스템 손상 시 적시에 복구가 가능하도록 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하여야 한다.

- ▶ 백업대상 선정기준 수립
- ▶ 백업담당자 및 책임자 지정
- ▶ 백업대상별 백업 주기 및 보존기한 정의
- ▶ 백업방법 및 절차 : 백업시스템 활용, 매뉴얼 방식 등
- ▶ 백업매체 관리(예 : 라벨링, 보관장소, 접근통제 등)
- ▶ 백업 복구 절차 : 주요 정보시스템의 경우 IT 재해 복구 측면에서 백업정보의 완전성, 정확성 등을 점검하기 위하여 정기적인 복구 테스트 수행 필요
- ▶ 백업관리대장 관리 등

※ 주요 백업 대상(예시)(대상 정보 및 정보시스템의 중요도를 고려하여 선정)
- 중요정보(개인정보, 기밀정보 등)
- 중요 데이터베이스
- 각종 로그(정보시스템 감사로그, 이벤트 로그, 보안시스템 이벤트 로그 등)
- 환경설정 파일 등

■ 백업된 정보의 완전성과 정확성, 복구절차의 적절성을 확인하기 위하여 정기적으로 복구 테스트를 실시하여야 한다.

- ▶ 복구테스트 계획(복구테스트 주기 및 시점, 담당자, 방법 등)
- ▶ 복구테스트 시나리오 수립

- 복구테스트 실시 및 결과 보고
- 복구테스트 결과 문제점 발견 시 개선계획 수립 및 이행

■ 중요정보가 저장된 백업매체의 경우 재해·재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하여야 한다.

- 중요정보가 저장된 백업매체는 운영 중인 정보시스템 또는 백업시스템이 위치한 장소로부터 물리적으로 거리가 있는 곳에 소산 보관하고 관리대장으로 소산 이력을 관리
  - 소산일자(반출, 반입 등)
  - 소산 백업매체 및 백업정보 내용
- 소산이 적절히 이루어지고 있는지 여부에 대하여 주기적으로 점검
- 소산장소에 대하여 다음과 같은 보안대책 마련
  - 화재, 홍수와 같은 자연재해에 대한 대책(예 : 내화금고, 방염처리 등)
  - 소산장소 및 매체에 대한 접근통제 등

증거자료

예시

- 백업 및 복구 절차
- 복구테스트 결과
- 소산백업 현황

결함사례

- 사례 1 : 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구 절차가 수립되어 있지 않은 경우
- 사례 2 : 백업정책을 수립하고 있으나 법적 요구사항에 따라 장기간(6개월, 3년, 5년 등) 보관이 필요한 백업 대상 정보가 백업 정책에 따라 보관되고 있지 않은 경우
- 사례 3 : 상위 지침 또는 내부 지침에 따라 별도로 백업하여 관리하도록 명시된 일부 시스템(보안시스템 정책 및 로그 등)에 대한 백업이 이행되고 있지 않은 경우
- 사례 4 : 상위 지침 또는 내부 지침에는 주기적으로 백업매체에 대한 복구 테스트를 수행하도록 정하고 있으나 복구테스트를 장기간 실시하지 않은 경우

항 목	2.9.4 로그 및 접속기록 관리
인증기준	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실되지 않도록 안전하게 보존·관리하여야 한다.
주요 확인사항	• 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그관리 절차를 수립하고 이에 따라 필요한 로그를 생성하여 보관하고 있는가? • 정보시스템의 로그기록은 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 로그기록에 대한 접근권한은 최소화하여 부여하고 있는가? • 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 필요한 항목을 모두 포함하여 일정기간 안전하게 보관하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

세부 설명

■ 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그관리 절차를 수립하고, 이에 따라 필요한 로그를 생성하여 보관하여야 한다.

▶ 보존이 필요한 로그유형 및 대상시스템 식별

※ 주요 로그유형(예시)

· 시스템 이벤트 로그 : 운영체제 구성요소에 의하여 발생하는 로그(시스템 시작, 종료, 상태, 에러 코드 등)

· 네트워크 이벤트 로그 : IP주소 할당, 주요 구간 트래픽 로그

· 보안시스템 로그 : 관리자 접속, 보안정책(룰셋) 등록·변경·삭제 등

· 보안관련 감사 로그 : 사용자 접속기록, 인증 성공/실패 로그, 파일 접근, 계정 및 권한 등록·변경·삭제 등(서버, 응용프로그램, 보안시스템, 네트워크시스템, 데이터베이스 등)

· 개인정보처리시스템 접속기록 : 개인정보취급자가 개인정보처리시스템에 접속한 사실을 알 수 있는 접속자 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등

· 기타 정보보호 관련 로그

▶ 각 시스템 및 장비별 로그 형태, 보존기간, 로그 보존(백업) 방법 등 정의

▶ 로그관리 절차 수립 및 이에 따른 로그 생성·보관

■ 정보시스템의 로그기록은 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고, 로그기록에 대한 접근권한은 최소화하여 부여하여야 한다.

▶ 로그기록은 스토리지 등 별도 저장장치를 사용하여 백업하고 로그기록에 대한 접근권한 부여는 최소화하여 비인가자에 의한 로그기록 위·변조 및 삭제 등이 발생하지 않도록 하여야 함

■ 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 필요한 항목을 모두 포함하여 전자적으로 기록하고 일정기간 안전하게 보관하여야 한다.

▶ 개인정보처리시스템 접속기록에 반드시 포함되어야 할 항목

항목	설명
식별자	개인정보취급자 ID 등 접속한 자의 식별정보
접속일시	접속한 시간 또는 업무를 수행한 시간 (연월일 및 시분초)
접속지 정보	접속자 IP주소 등
처리한 정보주체 정보	정보주체의 ID, 고객번호, 학번, 사번 등
수행업무	개인정보 조회, 변경, 입력, 삭제, 출력, 다운로드 등

▶ 개인정보처리시스템 접속기록 보존기간

구분		보존 기간
개인정보취급자의 접속기록	5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우	최소 2년 이상
	고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우	
	개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우	
	위의 3가지 조건에 해당하지 않을 경우	최소 1년 이상

▶ 개인정보 접속기록이 위·변조, 도난, 분실되지 않도록 안전하게 보관 필요

※ 접속기록의 안전한 보관방법(예시)

· 상시적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치, 오브젝트 스토리지 등에 보관

· 접속기록에 대한 위·변조를 방지하기 위해서는 CD-ROM, DVD-R, WORM(Write Once Read Many) 등과 같은 덮어쓰기 방지 매체를 사용

· 접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보(MAC값, 전자서명값 등)를 별도의 장비에 보관·관리 등

증거자료

예시

- 로그관리 절차
- 로그기록 내역
- 로그 저장장치에 대한 접근통제 내역
- 개인정보 접속기록 내역

결함사례

- 사례 1 : 로그 기록 대상, 방법, 보존기간, 검토 주기, 담당자 등에 대한 세부 기준 및 절차가 수립되어 있지 않은 경우
- 사례 2 : 보안 이벤트 로그, 응용프로그램 및 서비스 로그(윈도우 2008 서버 이상) 등 중요 로그에 대한 최대 크기를 충분하게 설정하지 않아 내부 기준에 정한 기간 동안 기록·보관되고 있지 않은 경우
- 사례 3 : 중요 Linux/UNIX 계열 서버에 대한 로그 기록을 별도로 백업하거나 적절히 보호하지 않아 사용자의 명령 실행 기록 및 접속 이력 등을 임의로 삭제할 수 있는 경우
- 사례 4 : 개인정보처리시스템에 접속한 기록을 확인한 결과 접속자의 계정, 접속 일시, 접속자 IP주소 정보는 남기고 있으나, 처리한 정보주체 정보 및 수행업무(조회, 변경, 삭제, 다운로드 등)와 관련된 정보를 남기고 있지 않은 경우
- 사례 5 : 로그 서버의 용량의 충분하지 않아서 개인정보처리시스템 접속기록이 2개월 밖에 남아 있지 않은 경우
- 사례 6 : 개인정보처리자가 정보주체 10만 명의 개인정보를 처리하는 개인정보처리시스템의 개인정보취급자 접속기록을 1년간만 보관하고 있는 경우

항 목	2.9.5 로그 및 접속기록 점검
인증기준	정보시스템의 정상적인 사용을 보장하고 사용자 오·남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.
주요 확인사항	• 정보시스템 관련 오류, 오·남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차를 수립·이행하고 있는가? • 로그 검토 및 모니터링 결과를 책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하고 있는가? • 개인정보처리시스템의 접속기록은 관련 법령에서 정한 주기에 따라 정기적으로 점검하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

세부 설명

- 정보시스템 관련 오류, 오·남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차를 수립·이행하여야 한다.
  - 검토 주기
  - 검토 대상
  - 검토 기준 및 방법
  - 검토 담당자 및 책임자
  - 이상징후 발견 시 대응절차 등
- 로그 검토 및 모니터링 결과를 책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하여야 한다.
  - 로그 검토 및 모니터링 기준에 따라 검토를 수행한 후 이상징후 발견 여부 등 그 결과를 관련 책임자에게 보고
  - 이상징후 발견 시 정보유출, 해킹, 오·남용, 부정행위 등 발생 여부를 확인하기 위한 절차를 수립하고 절차에 따라 대응
  - 개인정보를 다운로드한 것이 확인된 경우 내부 관리계획 등 로그검토 기준에서 정하는 바에 따라 그 사유를 확인하고, 개인정보의 오·남용이나 유출 목적으로 다운로드한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등의 필요한 조치 이행
- 개인정보처리시스템의 접속기록은 관련 법령에서 정한 주기에 따라 정기적으로 점검하여야 한다.
  - 법령에 따른 개인정보 접속기록 점검 주기 : 월 1회 이상

증거자료

예시

- 로그 검토 및 모니터링 절차
- 로그 검토 및 모니터링 결과(검토 내역, 보고서 등)
- 개인정보 접속기록 점검 내역
- 개인정보 다운로드 시 사유 확인 기준 및 결과
- 이상징후 발견 시 대응 증거자료

결함사례

- 사례 1 : 중요 정보를 처리하고 있는 정보시스템에 대한 이상접속(휴일 새벽 접속, 우회경로 접속 등) 또는 이상행위(대량 데이터 조회 또는 소량 데이터의 지속적·연속적 조회 등)에 대한 모니터링 및 경고·알림 정책(기준)이 수립되어 있지 않은 경우
- 사례 2 : 내부 지침 또는 시스템 등에 접근 및 사용에 대한 주기적인 점검·모니터링 기준을 마련하고 있으나 실제 이상접속 및 이상행위에 대한 검토 내역이 확인되지 않은 경우
- 사례 3 : 개인정보처리자가 개인정보처리시스템의 접속기록 점검 주기를 분기 1회로 정하고 있는 경우
- 사례 4 : 개인정보처리자의 내부 관리계획에는 1,000명 이상의 정보주체에 대한 개인정보를 다운로드한 경우에는 사유를 확인하도록 기준이 책정되어 있는 상태에서 1,000건 이상의 개인정보 다운로드가 발생하였으나 그 사유를 확인하지 않고 있는 경우

항 목	2.9.6 시간 동기화
인증기준	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.
주요 확인사항	• 정보시스템의 시간을 표준시간으로 동기화하고 있는가? • 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하고 있는가?

세부 설명

- 로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 각 정보시스템의 시간을 표준시간으로 동기화하여야 한다.
  - NTP(Network Time Protocol) 등의 방법을 활용하여 시스템 간 시간 동기화
  - 시간 정확성이 요구되는 모든 정보시스템은 빠짐없이 동기화 필요(출입통제시스템, CCTV저장장치 등)
- 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하여야 한다.
  - 시간 동기화 오류 발생 여부, OS재설치 또는 설정변경 등에 따른 시간동기화 적용 누락 여부 등 점검

증거자료

예시

- 시간 동기화 설정
- 주요 시스템 시간 동기화 증거자료

결함사례

- 사례 1 : 일부 중요 시스템(보안시스템, CCTV 등)의 시각이 표준시와 동기화되어 있지 않으며, 관련 동기화 여부에 대한 주기적 점검이 이행되고 있지 않은 경우
- 사례 2 : 내부 NTP 서버와 시각을 동기화하도록 설정하고 있으나 일부 시스템의 시각이 동기화되지 않고 있고, 이에 대한 원인분석 및 대응이 이루어지고 있지 않은 경우

항 목	2.9.7 정보자산의 재사용 및 폐기
인증기준	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구·재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.
주요 확인사항	• 정보자산의 안전한 재사용 및 폐기에 대한 절차를 수립·이행하고 있는가? • 정보자산 및 저장매체를 재사용 및 폐기하는 경우 개인정보 및 중요정보를 복구되지 않는 방법으로 처리하고 있는가? • 자체적으로 정보자산 및 저장매체를 폐기할 경우 관리대장을 통하여 폐기이력을 남기고 폐기확인 증적을 함께 보관하고 있는가? • 외부업체를 통하여 정보자산 및 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전히 폐기하였는지 여부를 확인하고 있는가? • 정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장매체 내 정보를 보호하기 위한 대책을 마련하고 있는가?
관련 법규	• 개인정보 보호법 제21조(개인정보의 파기) • 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

세부 설명

■ 정보자산의 안전한 재사용 및 폐기에 대한 절차를 수립·이행하여야 한다.

▶ 정보자산 재사용 절차 : 데이터 초기화 방법, 재사용 프로세스 등

▶ 정보자산 폐기 절차 : 폐기 방법, 폐기 프로세스(승인 등), 폐기 확인, 폐기관리대장 기록 등

■ 정보자산 및 저장매체를 재사용 및 폐기하는 경우 개인정보 및 중요정보가 복구되지 않는 방법으로 처리하여야 한다.

▶ 개인정보를 파기할 때에는 법령에 따라 복구·재생되지 않도록 안전하게 파기 필요

※ 복원이 불가능한 파기 방법(예시)
1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비(디가우저)를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

▶ '복원이 불가능한 방법'이란 현재의 기술 수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말함(표준 개인정보 보호지침 제10조)

■ 자체적으로 정보자산 및 저장매체를 폐기할 경우 다음 내용이 포함된 관리대장을 통하여 폐기이력을 남기고 폐기확인 증거자료를 함께 보관하여야 한다.

▶ 폐기 일자

▶ 폐기 담당자, 확인자명

- 폐기 방법
- 폐기확인 증거자료(사진 등) 등

■ 외부업체를 통하여 정보자산 및 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고, 해당 절차에 따라 완전히 폐기되었는지 확인하여야 한다.

- 폐기 절차 및 보호대책, 책임소재 등에 대하여 계약서에 반영
- 계약서에 반영된 폐기 절차에 따라 이행되고 있는지 사진촬영, 실사 등의 이행 증거자료 확인

■ 정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장매체 내 정보를 보호하기 위한 대책을 마련하여야 한다.

- 유지보수 신청 전 데이터 이관 및 파기
- 데이터 암호화
- 계약 시 비밀유지 서약
- 데이터 완전삭제 또는 저장매체 완전파기 조치 등

증거자료

예시

- 정보자산 폐기 및 재사용 절차
- 저장매체 관리대장
- 정보자산 및 저장매체 폐기 증거자료
- 정보자산 및 저장매체 폐기 관련 위탁계약서

결함사례

- 사례 1 : 개인정보취급자 PC를 재사용할 경우 데이터 삭제프로그램을 이용하여 완전삭제 하도록 정책 및 절차가 수립되어 있으나, 실제로는 완전삭제 조치 없이 재사용하거나 기본 포맷만 하고 재사용하고 있는 등 관련 절차가 이행되고 있지 않은 경우
- 사례 2 : 외부업체를 통하여 저장매체를 폐기하고 있으나, 계약 내용상 안전한 폐기 절차 및 보호대책에 대한 내용이 누락되어 있고 폐기 이행 증거자료 확인 및 실사 등의 관리·감독이 이루어지지 않은 경우
- 사례 3 : 폐기된 HDD의 일련번호가 아닌 시스템명을 기록하거나 폐기 대장을 작성하지 않아 폐기 이력 및 추적할 수 있는 증거자료를 확인할 수 없는 경우
- 사례 4 : 회수한 폐기 대상 하드디스크가 완전삭제 되지 않은 상태로 잠금장치가 되지 않은 장소에 방치되고 있는 경우

2.10. 시스템 및 서비스 보안관리

항 목	2.10.1 보안시스템 운영
인증기준	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
주요 확인사항	• 조직에서 운영하고 있는 보안시스템에 대한 운영절차를 수립·이행하고 있는가? • 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? • 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가? • 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가? • 보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가? • 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 관련 법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

■ 조직에서 운영하고 있는 보안시스템에 대하여 다음 내용을 포함한 운영절차를 수립·이행하여야 한다.

- ▶ 보안시스템 유형별 책임자 및 관리자 지정
- ▶ 보안시스템 정책(룰셋 등) 적용(등록, 변경, 삭제 등) 절차
- ▶ 최신 정책 업데이트 방안 : IDS, IPS 등의 보안시스템의 경우 새로운 공격기법을 탐지하기 위한 최신 패턴(시그너처) 및 엔진의 지속적 업데이트
- ▶ 보안시스템 이벤트 모니터링 절차(정책에 위배되는 이상징후 탐지 및 확인 등)
- ▶ 보안시스템 접근통제 정책(사용자 인증, 관리자 단말 IP 또는 MAC 등)
- ▶ 보안시스템 운영현황의 주기적 점검
- ▶ 보안시스템 자체에 대한 접근통제 방안 등

※ 보안시스템 유형(예시)
· 네트워크 보안시스템 : 침입차단시스템(방화벽), 침입방지시스템(IPS), 침입탐지시스템(IDS), 네트워크 접근제어(NAC), DDoS대응시스템, 가상사설망(VPN) 등
· 서버 보안시스템 : 시스템 접근제어, 보안운영체제(SecureOS)
· 데이터베이스 보안시스템 : 데이터베이스 접근제어

· 정보유출 방지시스템 : Network DLP(Data Loss Prevention), Endpoint DLP 등
· 개인정보보호 시스템 : 개인정보 검출솔루션, 출력물 보안, 개인정보 접속기록관리솔루션 등
· 암호화 솔루션 : 데이터베이스암호화, DRM 등
· 악성코드 대응 솔루션 : 백신, 패치관리시스템(PMS), EDR(Endpoint Detection Response) 등
· 기타 : APT대응솔루션, SIEM(Security Incident & Event Monitoring), 웹방화벽 등

■ 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하여야 한다.

▶ 강화된 사용자 인증(OTP 등), 관리자 단말 IP 또는 MAC 접근통제 등의 보호대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제

▶ 주기적인 보안시스템 접속로그 분석을 통하여 비인가자에 의한 접근시도 여부 점검

■ 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하여야 한다.

▶ 방화벽, DLP 등 보안시스템별 정책 등록, 변경, 삭제를 위한 신청 및 승인 절차

▶ 책임추적성을 확보할 수 있도록 보안시스템 정책 신청·승인·적용 기록 보존

▶ 보안시스템 정책(룰셋) 적용 시 고려사항

- 최소권한의 원칙에 따라 업무상 필요한 최소한의 권한만 부여
- 네트워크 접근통제 정책은 전체 차단을 기본으로 하되 업무상 허용하여야 하는 IP와 Port만 개별적으로 추가하여 관리
- 보안정책 설정 시 목적에 따라 사용기간을 한정하여 적용
- 보안정책의 등록·변경은 공식적인 절차를 통하도록 관리 등

■ 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하여야 한다.

▶ 신청사유의 타당성 검토

▶ 보안성 검토 : 예외 정책에 따른 보안성 검토 및 보완대책 마련

▶ 예외 정책 신청·승인 : 보안시스템별로 책임자 또는 담당자 승인

▶ 예외정책 만료 여부 및 예외 사용에 대한 모니터링 등

■ 보안시스템에 설정된 정책의 타당성 여부를 다음 사항을 고려하여 주기적으로 검토하여야 한다.

▶ 내부 보안정책·지침 위배(과다 허용 규칙 등)

▶ 공식적인 승인절차를 거치지 않고 등록된 정책

▶ 장기 미사용 정책

▶ 중복 또는 사용기간 만료 정책

▶ 퇴직 및 직무변경자 관련 정책

▶ 예외 관련 정책 등

■ 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하여야 한다.

▶ 개인정보보호 관련 법령에서 요구하는 접근통제 시스템 필수 요구 기능

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

▶ 클라우드 환경에서 개인정보처리시스템을 구성한 경우, 클라우드서비스 제공자가 제공하는 보안기능 또는 서비스를 이용하여 접근통제 기능 구현 가능

증거자료

예시

- 보안시스템 구성
- 네트워크 구성
- 보안시스템 운영절차
- 방화벽 정책
- 방화벽 정책 설정·변경 요청서
- 보안시스템 예외자 목록
- 보안시스템별 관리 화면(방화벽, IPS, 서버접근제어, DLP, DRM 등)
- 보안시스템 정책 검토 이력

결함사례

- 사례 1 : 침입차단시스템 보안정책에 대한 정기 검토가 수행되지 않아 불필요하거나 과도하게 허용된 정책이 다수 존재하는 경우
- 사례 2 : 보안시스템 보안정책의 신청, 변경, 삭제, 주기적 검토에 대한 절차 및 기준이 없거나, 절차는 있으나 이를 준수하지 않은 경우
- 사례 3 : 보안시스템의 관리자 지정 및 권한 부여 현황에 대한 관리감독이 적절히 이행되고 있지 않은 경우
- 사례 4 : 내부 지침에는 정보보호담당자가 보안시스템의 보안정책 변경 이력을 기록·보관하도록 정하고 있으나, 정책관리대장을 주기적으로 작성하지 않고 있거나 정책관리대장에 기록된 보안정책과 실제 운영 중인 시스템의 보안정책이 상이한 경우

항 목	2.10.2 클라우드 보안
인증기준	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가? • 클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하고 있는가? • 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가 접근, 권한 오·남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하고 있는가? • 클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가?

세부 설명

■ 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고, 이를 계약서(SLA 등)에 반영하여야 한다.

▶ 클라우드 서비스 유형에 따른 역할 및 책임(예시)

클라우드 서비스 유형	클라우드 서비스 제공자	클라우드 서비스 이용자
IaaS	• 물리적 영역의 시설 보안 및 접근통제 • 호스트 OS에 대한 보안 패치 • 하이퍼바이저 등 가상머신에 대한 보안 관리 등	• 게스트 OS, 미들웨어 및 애플리케이션 보안 패치 • 게스트 OS, 미들웨어, 애플리케이션, 사설 네트워크 영역에 대한 보안 구성 및 설정 • 데이터 보안 • 관리자, 사용자 권한 관리 등
PaaS	• IaaS 영역에서 클라우드 서비스 제공자의 역할 및 책임 • 네트워크 영역의 보안 설정 • 게스트 OS 및 미들웨어 영역에 대한 보안패치, 보안 구성 및 설정	• 애플리케이션 보안 패치 및 보안 설정 • 데이터 보안 • 관리자, 사용자 권한관리 등
SaaS	• IaaS, PaaS 영역에서 클라우드 서비스 제공자의 역할 및 책임 • 애플리케이션 보안 패치 및 보안 설정 • 데이터 보안(데이터 레벨의 접근통제, 암호화 등) 등	• 애플리케이션 관리자, 사용자 권한 관리 등

※ 클라우드 서비스 사업자, 서비스 구성 및 특성 등에 따라 달라질 수 있음

■ 클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하여야 한다.

▶ 외부 클라우드 서비스 이용에 따른 위험 평가 : 서비스 품질 및 연속성, 법적 준거성, 보안성 측면 등 고려

▶ 클라우드 서비스에 대한 위험평가 결과를 반영한 보안통제 정책 수립·이행

※ 클라우드 서비스 보안통제 정책(예시)(클라우드 서비스 유형에 따른 특성 반영 필요)
- 보안 관리 관련 역할 및 책임
- 가상네트워크 보안 구성 및 접근통제
- 클라우드 서비스 관리자 계정 및 권한 관리(최고관리자 및 분야별 관리자 등)
- 클라우드 서비스 관리자에 대한 강화된 인증(OTP 등)
- 보안 설정 기준(인증, 암호화, 세션관리, 접근통제, 공개설정, 장기미사용 잠금, 로그기록, 백업 등)
- 보안 설정 등록·변경·삭제 절차(신청, 승인 등)
- 보안 구성 및 설정에 대한 적절성 검토
- 클라우드 관리콘솔에 대한 접근통제 및 권한 관리 절차
- Access Key의 발급, 이용, 회수 등에 대한 관리 절차
- 클라우드 서비스 원격접속 경로 및 방법(VPN, IP주소 제한, 2 Factor 인증 등)
- 클라우드 서비스 보안 관제 및 알람·모니터링 방안
- 보안감사 절차 등

■ 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고, 관리자 권한에 대한 비인가 접근, 권한 오·남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하여야 한다.

▶ 클라우드 서비스 관리자 권한 세분화 : 최고관리자, 가상네트워크 관리자, 보안관리자, DevOps 관리자 등

▶ 업무 및 역할에 따라 관리자 권한 최소화 부여

▶ 클라우드 관리자 권한 접속에 대한 강화된 인증 적용 : OTP, 보안키 등

▶ 원격 접속 구간에 대한 통신 암호화 또는 VPN 적용

▶ 클라우드 관리자 접속, 권한 설정에 대한 상세 로그 기록 및 모니터링 등

■ 클라우드 서비스 보안 설정 변경, 운영 현황 등을 모니터링하고, 그 적절성을 정기적으로 검토하여야 한다.

▶ 클라우드 서비스에 대한 승인받지 않은 환경설정 및 보안설정 변경을 적발할 수 있도록 알람 설정 및 모니터링

▶ 클라우드 서비스 보안설정의 적정성 여부를 정기적으로 검토 및 조치

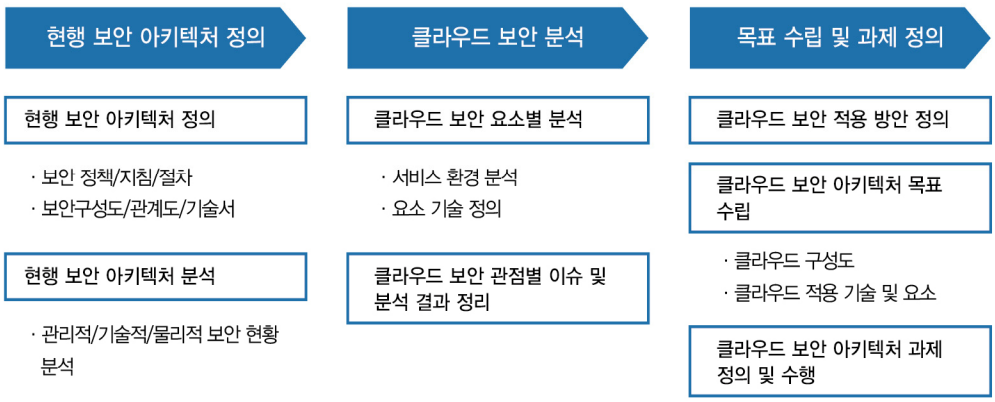
※ 주의사항
- 클라우드 환경에서의 네트워크 접근, 정보시스템 접근, 데이터베이스 접근, 응용프로그램 접근 등 접근통제의 적절성, 인증 및 권한관리, 암호화, 시스템 및 서비스 보안관리 등 기타 필요한 보호조치가 모두 적용되어야 함

[CSA 클라우드서비스의 보안위협 현황]

※CSA : Cloud Security Alliance

〈출처〉 클라우드 정보보호 안내서(KISA)

[클라우드 보안 아키텍처 수립 절차 예시]



〈출처〉 클라우드 정보보호 안내서(KISA)

증거자료

예시

- 클라우드 서비스 관련 계약서 및 SLA
- 클라우드 서비스 위험분석 결과
- 클라우드 서비스 보안통제 정책
- 클라우드 서비스 관리자 권한 부여 현황
- 클라우드 서비스 구성도
- 클라우드 서비스 보안설정 현황
- 클라우드 서비스 보안설정 적정성 검토 이력

결함사례

- 사례 1 : 클라우드 서비스 계약서 내에 보안에 대한 책임 및 역할 등에 대한 사항이 포함되어 있지 않은 경우
- 사례 2 : 클라우드 서비스의 보안설정을 변경할 수 있는 권한이 업무상 반드시 필요하지 않은 직원들에게 과도하게 부여되어 있는 경우
- 사례 3 : 내부 지침에는 클라우드 내 사설 네트워크의 접근통제 룰(Rule) 변경 시 보안책임자 승인을 받도록 하고 있으나, 승인절차를 거치지 않고 등록·변경된 접근제어 룰이 다수 발견된 경우
- 사례 4 : 클라우드 서비스의 보안설정 오류로 내부 로그 파일이 인터넷을 통하여 공개되어 있는 경우

항 목	2.10.3 공개서버 보안
인증기준	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 공개서버를 운영하는 경우 이에 대한 보호대책을 수립·이행하고 있는가? • 공개서버는 내부 네트워크와 분리된 DMZ 영역에 설치하고 침입차단시스템 등 보안시스템을 통하여 보호하고 있는가? • 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시절차를 수립·이행하고 있는가? • 조직의 중요정보가 웹사이트 및 웹서버를 통하여 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하고 있는가?

세부 설명

- 웹서버 등 공개서버를 운영하는 경우 이에 대한 보호대책을 수립·이행하여야 한다.
  - 웹서버를 통한 개인정보 송수신 시 SSL(Secure Socket Layer)/TLS(Transport Layer Security) 인증서 설치 등 보안서버 구축
  - 백신설치 및 업데이트 설정
  - 응용프로그램(웹서버, openssl 등), 운영체제 등에 대한 최신 보안패치 설치
  - 불필요한 서비스 제거 및 포트 차단
  - 불필요한 소프트웨어, 스크립트, 실행파일 등 설치 금지
  - 에러 처리 페이지, 테스트 페이지 등 불필요한 페이지 노출 금지
  - 주기적 취약점 점검 수행 등
- 공개서버는 내부 네트워크와 분리된 DMZ 영역에 설치하고 침입차단시스템 등 보안시스템을 통하여 보호하여야 한다.
  - 공개서버가 침해당하더라도 공개서버를 통한 내부 네트워크 침입이 불가능하도록 침입차단시스템 등을 통한 접근통제 정책을 적용
  - DMZ의 공개서버가 내부 네트워크에 위치한 데이터베이스, WAS(Web Application Server) 등의 정보시스템과 접속이 필요한 경우 엄격하게 접근통제 정책 적용
- 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시절차를 수립·이행하여야 한다.
  - 원칙적으로 DMZ 구간의 웹서버 내에 개인정보 및 중요정보의 저장을 금지하고, 업무상 불가피하게 필요한 경우 허가 절차 및 보호대책 적용
  - 웹사이트에 개인정보 및 중요정보를 게시할 경우 사전 검토 및 승인 절차 수행
  - 외부 검색엔진 등을 통하여 접근권한이 없는 자에게 개인정보 및 중요정보가 노출되지 않도록 조치

■ 조직의 중요정보가 웹사이트 및 웹서버를 통하여 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하여야 한다.

▶ 검색엔진 등을 통하여 주기적으로 점검 및 필요한 조치 적용

▶ 중요정보 노출을 인지한 경우 웹사이트에서 차단조치 및 해당 검색엔진 사업자에게 요청하여 캐시 등을 통하여 계속적으로 노출되지 않도록 조치

증거자료

예시

- 네트워크 구성도
- 웹사이트 정보공개 절차 및 내역(신청·승인·게시 이력 등)
- 개인정보 및 중요정보 노출 여부 점검 이력

결함사례

- 사례 1 : 인터넷에 공개된 웹사이트의 취약점으로 인하여 구글 검색을 통하여 열람 권한이 없는 타인의 개인정보에 접근할 수 있는 경우
- 사례 2 : 웹사이트에 개인정보를 게시하는 경우 승인 절차를 거치도록 내부 규정이 마련되어 있으나, 이를 준수하지 않고 개인정보가 게시된 사례가 다수 존재한 경우
- 사례 3 : 게시판 등의 웹 응용프로그램에서 타인이 작성한 글을 임의로 수정·삭제하거나 비밀번호로 보호된 글을 열람할 수 있는 경우

항 목	2.10.4 전자거래 및 핀테크 보안
인증기준	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위하여 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
주요 확인사항	• 전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호대책을 수립·이행하고 있는가? • 전자거래 및 핀테크 서비스 제공을 위하여 결제시스템 등 외부 시스템과 연계하는 경우 송수신되는 관련 정보의 보호를 위한 대책을 수립·이행하고 안전성을 점검하고 있는가?

세부 설명

■ 전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호대책을 수립·이행하여야 한다.

▶ '전자거래'는 재화나 용역을 거래할 때 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래를 말함(전자문서 및 전자거래 기본법 제2조)

▶ '전자상거래'는 전자거래의 방법으로 상행위를 하는 것을 말함(전자상거래 등에서의 소비자보호에 관한 법률 제2조)

▶ '핀테크(Fintech)'란 금융(Finance)과 기술(Technology)의 합성어로, 금융과 IT의 융합을 통한 금융서비스 및 산업의 변화를 통칭함(금융위원회 금융용어사전)

▶ 전자(상)거래사업자 및 핀테크 서비스제공자는 전자(상)거래 및 핀테크 서비스의 안전성과 신뢰성을 확보하기 위하여 이용자의 개인정보, 영업비밀(거래처 식별정보, 재화 또는 용역 가격 등 공개 시 영업에 손실을 초래할 수 있는 거래 관련 정보), 결제정보 수집, 저장관리, 파기 등의 과정에서의 침해사고를 예방하기 위한 보호대책(인증, 암호화, 접근통제 등)을 수립하여 이행하여야 함

▶ 핀테크 서비스의 경우 핀테크 서비스의 유형 및 특성을 반영하여 해당 핀테크 서비스로 인하여 발생 가능한 위험요인을 빠짐없이 식별하여 필요한 보호대책 적용 필요

※ 전자거래 및 핀테크 보호대책 수립 시 고려하여야 할 법률(예시)
· 전자문서 및 전자거래 기본법
· 전자상거래 등에서의 소비자 보호에 관한 법률
· 전자금융거래법
· 금융소비자 보호에 관한 법률
· 정보통신 이용촉진 및 정보보호 등에 관한 법률
· 신용정보법
· 개인정보 보호법 등

■ 전자거래 및 핀테크 서비스 제공을 위하여 결제시스템 등 외부 시스템과 연계하는 경우 송수신되는 관련 정보의 보호를 위한 대책을 수립·이행하고 안전성을 점검하여야 한다.

▶ '전자결제업자'는 전자결제수단의 발행자, 전자결제서비스 제공자, 해당 전자결제수단을 통한 전자결제서비스의 이행을 보조하거나 중개하는 자를 말하며(전자상거래 등에서의 소비자 보호에 관한 법률 시행령 제8조), 다음에 해당하는 자를 말함

- 금융회사, 신용카드업자, 결제수단 발행자(전자적 매체 또는 정보처리시스템에 화폐가치 또는 그에 상응하는 가치를 기록·저장하였다가 재화 등의 구매 시 지급하는 자), 통신과금서비스제공자, 전자결제대행 또는 중개서비스 사업자(PG사 등)

※ PG(Payment Gateway)사는 인터넷상에서 금융기관과의 거래를 대행해 주는 서비스로서 신용카드, 계좌이체, 휴대폰 이용 결제, ARS 결제 등 다양한 소액 결제 서비스를 대신 제공해 주는 회사

▶ 전자(상)거래사업자와 전자결제업자 또는 핀테크 서비스 제공자 간 송수신되는 결제관련 정보의 유출, 조작, 사기 등의 침해사고로 인한 거래당사자 간 피해가 발생하지 않도록 적절한 보호대책을 수립·이행하고 안전성을 점검하여야 함

증거자료

예시

- 전자거래 및 핀테크 서비스 보호대책
- 결제시스템 연계 시 보안성 검토 결과

결함사례

- 사례 1 : 전자결제대행업체와 위탁 계약을 맺고 연계를 하였으나, 적절한 인증 및 접근제한 없이 특정 URL을 통하여 결제 관련 정보가 모두 평문으로 전송되는 경우
- 사례 2 : 전자결제대행업체와 외부 연계 시스템이 전용망으로 연결되어 있으나, 해당 연계 시스템에서 내부 업무 시스템으로의 접근이 침입차단시스템 등으로 적절히 통제되지 않고 있는 경우
- 사례 3 : 내부 지침에는 외부 핀테크 서비스 연계 시 정보보호팀의 보안성 검토를 받도록 되어 있으나, 최근에 신규 핀테크 서비스를 연계하면서 일정상 이유로 보안성 검토를 수행하지 않은 경우

항 목	2.10.5 정보전송 보안
인증기준	다른 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통하여 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.
주요 확인사항	• 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 있는가? • 업무상 조직 간 개인정보 및 중요정보를 상호교환하는 경우 안전한 전송을 위한 협약체결 등 보호대책을 수립·이행하고 있는가?

세부 설명

■ 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하여야 한다.

▶ 정보전송 기술 표준 : 암호화 방식, 키 교환 및 관리, 전문 규칙, 연계 및 통신 방식 등

▶ 정보전송 검토 절차 : 보고 및 승인, 관련 조직 간 역할 및 책임, 보안성 검토 등

▶ 정보전송 협약 기준 : 표준 보안약정서 또는 계약서 양식

▶ 기타 보호조치 적용 기준 : 법적 요구사항을 반영한 보호조치 기준 등

■ 업무상 조직 간 중요정보 및 개인정보를 상호교환하는 경우 안전한 전송을 위한 협약체결 등 보호대책을 수립·이행하여야 한다.

▶ 조직 또는 계열사 간 다음과 같은 업무수행을 위하여 중요정보를 전자적으로 상호교환하는 경우 안전한 전송을 위한 협약(보안약정서, 계약서, 부속합의서, SLA 등)을 체결하고 이에 따라 이행하여야 함

- 관련 업무 정의 : DM 발송을 위한 개인정보 DM업체 전달, 채권추심업체에 추심정보 전달, 개인정보 제3자 제공, 신용카드결제 정보 VAN(Value Added Network)社 전달 등
- 정보전송 범위 정의 : 법규 준수 또는 정보유출 위험을 예방하기 위하여 업무상 필요한 최소한의 정보만을 송수신
- 담당자 및 책임자 지정
- 정보 전송 기술 표준 정의
- 정보 전송, 저장, 파기 시 관리적·기술적·물리적 보호대책 등

※ DM(Direct Mail) : 우편물을 통한 홍보활동을 의미하며, 편지·엽서·안내장·리플렛·카탈로그· 청구서 등의 인쇄물을 우편물 등의 형태로 직접 또는 우편 수단을 이용하여 전달하는 커뮤니케이션 수단

증거자료

예시

- 정보전송 협약서 또는 계약서
- 정보전송 기술표준
- 정보전송 관련 구성도, 인터페이스 정의서

결함사례

- 사례 1 : 대외 기관과 연계 시 전용망 또는 VPN을 적용하고 중계서버와 인증서 적용 등을 통하여 안전하게 정보를 전송하고 있으나, 외부 기관별 연계 시기, 방식, 담당자 및 책임자, 연계 정보, 법적 근거 등에 대한 현황관리가 적절히 이루어지지 않고 있는 경우
- 사례 2 : 중계과정에서의 암호 해제 구간 또는 취약한 암호화 알고리즘(DES, 3DES) 사용 등에 대한 보안성 검토, 보안표준 및 조치방안 수립 등에 대한 협의가 이행되고 있지 않은 경우

항 목	2.10.6 업무용 단말기기 보안
인증기준	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
주요 확인사항	• PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 등의 보안 통제 정책을 수립·이행하고 있는가? • 업무용 단말기를 통하여 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료공유프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하고 있는가? • 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 보안대책을 적용하고 있는가? • 업무용 단말기기에 대한 접근통제 대책의 적절성에 대하여 주기적으로 점검하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

■ PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 등의 보안 통제 정책을 수립·이행하여야 한다.

- ▶ 업무용 단말기 허용기준
- ▶ 업무용 단말기 통한 업무 사용범위
- ▶ 업무용 단말기 사용 시 승인 절차 및 방법
- ▶ 업무망 연결 시 인증 방안 : 기기인증, MAC 인증 등
- ▶ 백신 설치, 보안프로그램 설치 등 업무용 단말기 사용에 따른 보안 설정 정책
- ▶ 업무용 단말기 사용에 따른 보안 설정 정책 및 오·남용 모니터링 대책 등

※ 업무용 단말기 사용에 따른 보안관리 및 모니터링 대책(예시)

· 업무용 단말기에 대한 사용자 보안 설정 정책(백신설치, 보안패치, 공공장소에서의 사용주의, 분실 시 데이터초기화 등)
· 개인정보 및 내부자료 유출 방지를 위한 정책, 교육, 책임부여, 처벌기준
· 업무용 기기의 오·남용 여부를 파악할 수 있는 모니터링 대책
· 업무용 기기에 설치되는 소프트웨어의 안전성 점검대책
· 업무용 기기 악성코드 방지 대책
· 인터넷, 공개된 무선망 등을 통한 개인정보 유·노출을 방지하기 위한 업무용기기 접근통제 조치

■ 업무용 단말기를 통하여 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료공유프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하여야 한다.

- ▶ 불가피하게 공유설정 등을 할 때에는 업무용 단말기에 접근권한 비밀번호를 설정하고, 사용이 완료된 후에는 공유설정 제거
- ▶ 파일 전송이 주된 목적일 때에는 읽기 권한만을 부여하고 상대방이 쓰기를 할 때만 개별적으로 쓰기 권한 설정
- ▶ P2P 프로그램, 상용 웹메일, 웹하드, 메신저, SNS 서비스 등을 통하여 고의·부주의로 인한 개인정보 및 중요정보의 유·노출 방지
- ▶ WPA2(Wi-Fi Protected Access 2) 등 보안 프로토콜이 적용된 무선망 이용 등

■ 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 비밀번호 설정 등의 보안대책을 적용하여야 한다.

※ 업무용 모바일 기기 분실·도난 대책(예시)
· 비밀번호, 패턴, PIN, 지문, 홍채 등을 사용하여 화면 잠금 설정
· 디바이스 암호화 기능 등을 사용하여 애플리케이션, 데이터 등 암호화
· 모바일 기기 제조사 또는 이동통신사에서 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제(킬 스위치 서비스 등)
· 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속통제 등

■ 업무용 단말기기에 대한 접근통제 대책의 적절성에 대하여 주기적으로 점검하여야 한다.

- ▶ 업무용 단말기 신청·승인, 등록·해제, 기기인증 이력
- ▶ 업무용 단말기 보안설정 현황 등

증거자료

예시

- 업무용 단말기 보안통제 지침 및 절차
- 업무용 단말기 등록현황
- 업무용 단말기 보안설정
- 업무용 단말기 기기인증 및 승인 이력
- 업무용 단말기 보안점검 현황

결함사례

- 사례 1 : 업무적인 목적으로 노트북, 태블릿PC 등 모바일 기기를 사용하고 있으나, 업무용 모바일 기기에 대한 허용 기준, 사용 범위, 승인 절차, 인증 방법 등에 대한 정책이 수립되어 있지 않은 경우
- 사례 2 : 모바일 기기 보안관리 지침에서는 모바일 기기의 업무용 사용을 원칙적으로 금지하고 필요시 승인 절차를 통하여 제한된 기간 동안 허가된 모바일 기기만 사용하도록 정하고 있으나, 허가된 모바일 기기가 식별·관리되지 않고 승인되지 않은 모바일 기기에서도 내부 정보시스템 접속이 가능한 경우
- 사례 3 : 개인정보 처리업무에 이용되는 모바일 기기에 대하여 비밀번호 설정 등 도난·분실에 대한 보호대책이 적용되어 있지 않은 경우
- 사례 4 : 내부 규정에서는 업무용 단말기의 공유폴더 사용을 금지하고 있으나, 이에 대한 주기적인 점검이 이루어지고 있지 않아 다수의 업무용 단말기에서 과도하게 공유폴더를 설정하여 사용하고 있는 경우

항 목	2.10.7 보조저장매체 관리
인증기준	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장 매체는 안전한 장소에 보관하여야 한다.
주요 확인사항	• 외장하드, USB메모리, CD 등 보조저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하고 있는가? • 보조저장매체 보유현황, 사용 및 관리실태를 주기적으로 점검하고 있는가? • 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용을 제한하고 있는가? • 보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가? • 개인정보 또는 중요정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

세부 설명

- 외장하드, USB메모리, CD 등 보조저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하여야 한다.
  - 보조저장매체 보유 현황 관리 방안 : 보조저장매체 관리대장 등
  - 보조저장매체 사용허가 및 등록 절차
  - 보조저장매체 반출·입 관리 절차
  - 보조저장매체 폐기 및 재사용 절차
  - 보조저장매체 사용 범위 : 통제구역, 제한구역 등 보호구역별 사용 정책 및 절차
  - 보조저장매체 보호대책 등
- 보조저장매체 보유현황, 사용 및 관리 실태를 주기적으로 점검하여야 한다.
  - 보조저장매체 사용 승인 증거자료, 보유 현황, 관리 대장, 사용이력 확인 등 관리 실태 점검
- 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용을 제한하여야 한다.
  - 불가피하게 사용할 경우 책임자의 허가절차를 거친 후 적법한 절차에 따른 사용
  - 통제구역, 중요 제한구역 내 보조저장매체 사용 현황에 대한 정기적인 검토 수행
- 보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하여야 한다.
  - 보조저장매체 자동실행 방지 및 백신프로그램 검사 후 사용 등 보호대책 수립·이행

■ 개인정보 또는 중요정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하여야 한다.

▶ 개인정보 또는 중요정보가 포함된 보조저장매체(이동형 하드디스크, USB메모리, SSD 등)는 금고, 잠금장치가 있는 안전한 장소에 보관

증거자료

예시

- 보조저장매체(USB, CD 등) 차단 정책
- 보조저장매체 관리대장
- 보조저장매체 실태점검 이력

결함사례

- 사례 1 : 통제구역인 서버실에서의 보조저장매체 사용을 제한하는 정책을 수립하여 운영하고 있으나, 예외 승인 절차를 준수하지 않고 보조저장매체를 사용한 이력이 다수 확인되었으며, 보조저장매체 관리실태에 대한 주기적 점검이 실시되지 않아 보조저장매체 관리대장의 현행화가 미흡한 경우
- 사례 2 : 개인정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하지 않고 사무실 서랍 등에 방치하고 있는 경우
- 사례 3 : 보조저장매체 통제 솔루션을 도입·운영하고 있으나, 일부 사용자에 대하여 적절한 승인 절차 없이 예외처리되어 쓰기 등이 허용된 경우
- 사례 4 : 전산실에 위치한 일부 공용 PC 및 전산장비에서 일반 USB메모리에 대한 쓰기가 가능한 상황이나 매체 반입 및 사용 제한, 사용이력 기록 및 검토 등 통제가 적용되고 있지 않은 경우

항 목	2.10.8 패치관리
인증기준	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.
주요 확인사항	• 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치관리 정책 및 절차를 수립·이행하고 있는가? • 주요 서버, 네트워크시스템, 보안시스템 등의 경우 설치된 OS, 소프트웨어 패치 적용 현황을 주기적으로 관리하고 있는가? • 서비스 영향도 등에 따라 취약점을 조치하기 위한 최신의 패치 적용이 어려운 경우 보완대책을 마련하고 있는가? • 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가? • 패치관리시스템을 활용하는 경우 접근통제 등 충분한 보호대책을 마련하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지)

세부 설명

- 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 OS와 소프트웨어의 패치관리 정책 및 절차를 수립·이행하여야 한다.
  - 패치 적용 대상 : 서버, 네트워크시스템, DBMS, 응용프로그램, 상용소프트웨어, 오픈소스, 보안시스템, PC 등
  - 패치 주기 : 자산 중요도 및 특성 반영
  - 패치 정보 확인 방법
  - 패치 배포 전 사전 검토 절차
  - 긴급 패치 적용 절차
  - 패치 미적용 시 보안성 검토
  - 패치 담당자 및 책임자
  - 패치 관련 업체(제조사) 연락처 등
- 주요 서버, 네트워크시스템, 보안시스템 등의 경우 설치된 OS, 소프트웨어 패치 적용 현황을 주기적으로 관리하여야 한다.
  - 주요 서버, 네트워크시스템, 보안시스템 등에 설치된 운영체제 및 소프트웨어의 버전 정보, 패치 적용현황, 패치별 적용일자 등을 확인할 수 있도록 목록으로 관리
  - 최신 보안패치 적용 필요 여부를 주기적으로 확인

※ 주요 OS별 서비스 지원 종료(EOS 또는 EOL) 시점 확인 사이트(예시)
- MS 윈도우 : https://support.microsoft.com/ko-kr/lifecycle/search
- 레드햇 리눅스 : https://access.redhat.com/support/policy/updates/errata
- CentOS : https://wiki.centos.org/About/Product
- AIX : https://www-01.ibm.com/support/docview.wss?uid=isg3T1012517
- HP-UX : https://hpe.com/info/hpuxservermatrix
- Solaris : https://www.oracle.com/technetwork/server-storage/solaris/overview/releases-jsp-140987.html

■ 서비스 영향도 등에 따라 취약점을 조치하기 위한 최신의 패치 적용이 어려운 경우 보완대책을 마련하여야 한다.
  ▶ 운영시스템에 패치를 적용하는 경우 시스템 가용성에 영향을 미칠 수 있으므로 운영시스템의 중요도와 특성을 고려하여 영향도 분석 등 정해진 절차에 따라 충분하게 영향을 분석한 후 적용
  ▶ 운영환경에 따라 즉시 패치 적용이 어려운 경우 그 사유와 추가 보완대책을 마련하여 책임자에게 보고하고 그 현황을 관리

■ 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하여야 한다.
  ▶ 다만, 불가피한 경우 사전 위험분석을 통하여 보호대책을 마련하여 책임자 승인 후 적용

■ 패치관리시스템(PMS)을 활용하는 경우 내부망 서버 또는 PC에 악성코드 유포지로 악용될 수 있으므로 패치관리시스템 서버, 관리 콘솔 등에 접근통제 등 충분한 보호대책을 마련하여야 한다.
  ▶ 패치관리시스템 자체에 대한 접근통제 조치 : 허가된 관리자 외 접근 차단, 기본 패스워드 변경, 보안 취약점 제거 등
  ▶ 업데이트 파일 배포 시 파일 무결성 검사 등

증거자료

예시

- 패치 적용 관리 정책·절차
- 시스템별 패치 적용 현황
- 패치 적용 관련 영향도 분석 결과

결함사례

- 사례 1 : 일부 시스템에서 타당한 사유나 책임자 승인 없이 OS패치가 장기간 적용되고 있지 않은 경우
- 사례 2 : 일부 시스템에 서비스 지원이 종료(EOS)된 OS버전을 사용 중이나, 이에 따른 대응계획이나 보완대책이 수립되어 있지 않은 경우
- 사례 3 : 상용 소프트웨어 및 OS에 대해서는 최신 패치가 적용되고 있으나, 오픈소스 프로그램(openssl, openssh, Apache 등)에 대해서는 최신 패치를 확인하고 적용하는 절차 및 담당자가 지정되어 있지 않아 최신 보안패치가 적용되고 있지 않은 경우

항 목	2.10.9 악성코드 통제
인증기준	바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용단말기 등을 보호하기 위하여 보호대책을 수립·이행하고 있는가? • 백신 소프트웨어 등 보안프로그램을 통하여 최신 악성코드 예방·탐지 활동을 지속적으로 수행하고 있는가? • 백신 소프트웨어 등 보안프로그램은 최신의 상태로 유지하고 필요시 긴급 보안 업데이트를 수행하고 있는가? • 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지)

세부 설명

- 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용단말기 등을 보호하기 위하여 보호대책을 다음과 같은 내용을 포함하여 수립·이행하여야 한다.
  - 사용자 PC 사용지침(불분명한 이메일 및 파일 열람 금지, 허가받지 않은 프로그램 다운로드 및 설치 금지 등)
  - 정보시스템 및 개인정보처리시스템에서의 악성코드 대응지침
  - 백신프로그램 설치 범위(악성프로그램 감염이 가능한 정보자산 대상)
  - 백신프로그램 설치 절차
  - 백신프로그램 등을 통한 최신 악성코드 예방, 탐지 활동
  - 백신프로그램 등을 통한 주기적인 악성코드 감염 여부 모니터링 정책
  - 백신 소프트웨어 등 보안프로그램의 자동 업데이트 기능 설정 또는 일 1회 이상 업데이트 방법
  - 정보시스템, 업무용 컴퓨터에 P2P, 웹 하드 등과 같은 비인가 프로그램 설치 금지
  - 사용자 교육 및 정보제공 등
- 백신 소프트웨어 등 보안프로그램을 통하여 최신 악성코드 예방·탐지 활동을 지속적으로 수행하여야 한다.
  - 이메일 등 첨부파일에 대한 악성코드 감염 여부 검사
  - 실시간 악성코드 감시 및 치료
  - 주기적인 악성코드 점검 : 자동 바이러스 점검 일정 설정
  - 백신엔진 최신버전 유지 : 주기적 업데이트 등

- 백신 소프트웨어 등 보안프로그램은 최신의 상태로 유지하고, 필요시 긴급 보안업데이트를 수행하여야 한다.
  - 백신 업데이트 주기 준수 : 자동 업데이트 또는 일 1회 이상 업데이트
  - 악성프로그램 관련 경보가 발령되거나 긴급 업데이트 공지가 있는 경우 이에 따른 업데이트 수행
  - 백신 중앙관리시스템을 이용하여 백신프로그램을 관리하는 경우 관리서버에 대한 접근통제, 배포 파일에 대한 무결성 검증 등 보호대책 마련
- 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 수립·이행하여야 한다.
  - 악성코드 감염 발견 시 대응 절차(예 : 네트워크 케이블 분리 등)
  - 비상연락망(예: 백신업체 담당자, 관련 기관 연락처 등)
  - 대응보고서 양식(발견일시, 대응절차 및 방법, 대응자, 방지대책 포함) 등

증거자료

예시

- 악성프로그램 대응 지침·절차·매뉴얼
- 백신프로그램 설치 현황
- 백신프로그램 설정 화면
- 악성프로그램 대응 이력(대응 보고서 등)

결함사례

- 사례 1 : 일부 PC 및 서버에 백신이 설치되어 있지 않거나, 백신 엔진이 장기간 최신 버전으로 업데이트되지 않은 경우
- 사례 2 : 백신 프로그램의 환경설정(실시간 검사, 예약검사, 업데이트 설정 등)을 이용자가 임의로 변경할 수 있음에도 그에 따른 추가 보호대책이 수립되어 있지 않은 경우
- 사례 3 : 백신 중앙관리시스템에 접근통제 등 보호대책이 미비하여 중앙관리시스템을 통한 침해사고발생 가능성이 있는 경우 또는 백신 패턴에 대한 무결성 검증을 하지 않아 악의적인 사용자에 의한 악성코드 전파 가능성이 있는 경우
- 사례 4 : 일부 내부망 PC 및 서버에서 다수의 악성코드 감염이력이 확인되었으나, 감염 현황, 감염 경로 및 원인 분석, 그에 따른 조치내역 등이 확인되지 않은 경우

2.11. 사고 예방 및 대응

항 목	2.11.1 사고 예방 및 대응체계 구축
인증기준	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
주요 확인사항	• 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가? • 보안관제서비스 등 외부 기관을 통하여 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응절차의 세부사항을 계약서에 반영하고 있는가? • 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?
관련 법규	• 개인정보 보호법 제34조(개인정보의 유출 등의 통지·신고) • 정보통신망법 제48조의3(침해사고의 신고 등), 제48조의4(침해사고의 원인분석 등)

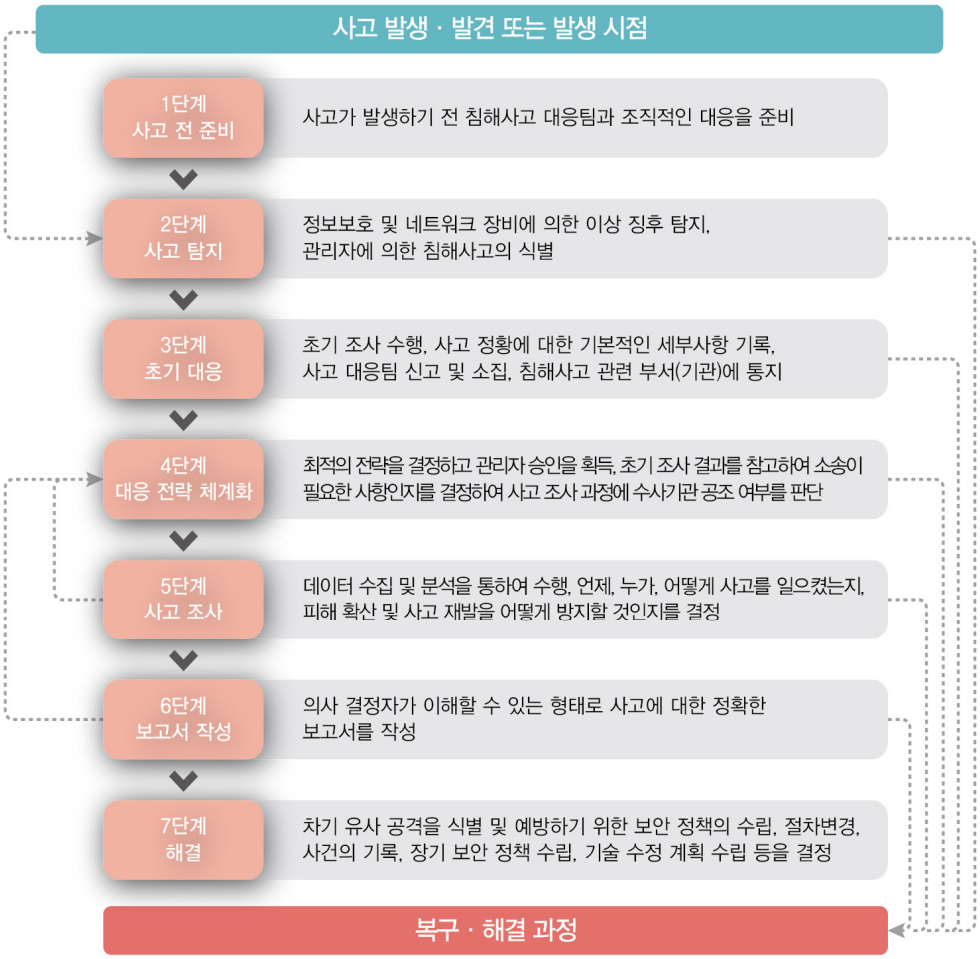
세부 설명

■ 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 다음 내용을 포함하여 마련하여야 한다.

- 침해사고의 정의 및 범위(개인정보 유출사고, 해킹 사고, 서비스거부공격 등)
- 침해사고 유형 및 중요도
- 침해사고 선포절차 및 방법
- 비상연락망 등의 연락체계
- 침해사고 탐지 체계
- 침해사고 발생 시 기록, 보고절차
- 침해사고 신고 및 통지 절차(관계기관, 정보주체 및 이용자 등)
- 침해사고 보고서 작성
- 침해사고 중요도 및 유형에 따른 대응 및 복구 절차
- 침해사고 복구조직의 구성, 책임 및 역할
- 침해사고 복구장비 및 자원조달
- 침해사고 대응 및 복구 훈련, 훈련 시나리오
- 외부 전문가 및 전문기관의 활용방안
- 기타 보안사고 예방 및 복구를 위하여 필요한 사항 등

- 보안관제서비스 등 외부 기관을 통하여 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응절차의 세부사항을 계약서(SLA 등)에 반영하여야 한다.
  - 보안관제서비스의 범위
  - 침해 징후 발견 시 보고 및 대응 절차
  - 침해사고 발생 시 보고 및 대응절차
  - 침해사고 발생에 따른 책임 및 역할에 관한 사항 등
- 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과 협조체계를 수립하여야 한다.

침해사고 대응 7단계



〈출처〉 민간부문 침해사고 대응 안내서(과기정통부, KISA)

증거자료

예시

- 침해사고 대응 지침·절차·매뉴얼
- 침해사고 대응 조직도 및 비상연락망
- 보안관제서비스 계약서(SLA 등)

결함사례

- 사례 1 : 침해사고에 대비한 침해사고 대응 조직 및 대응 절차를 명확히 정의하고 있지 않은 경우
- 사례 2 : 내부 지침 및 절차에 침해사고 단계별(사고 전, 인지, 처리, 복구, 보고 등) 대응 절차를 수립하여 명시하고 있으나, 침해사고 발생 시 사고 유형 및 심각도에 따른 신고·통지 절차, 대응 및 복구 절차의 일부 또는 전부를 수립하고 있지 않은 경우
- 사례 3 : 침해사고 대응 조직도 및 비상연락망 등을 현행화하지 않고 있거나, 담당자별 역할과 책임이 명확히 정의되어 있지 않은 경우
- 사례 4 : 침해사고 신고·통지 및 대응 협조를 위한 대외기관 연락처에 기관명, 홈페이지, 연락처 등이 잘못 명시되어 있거나, 일부 기관 관련 정보가 누락 또는 현행화되지 않은 경우
- 사례 5 : 외부 보안관제 전문업체 등 유관기관에 침해사고 탐지 및 대응을 위탁하여 운영하고 있으나, 침해사고 대응에 대한 상호 간 관련 역할 및 책임 범위가 계약서나 SLA에 명확하게 정의되지 않은 경우
- 사례 6 : 침해사고 대응절차를 수립하였으나, 개인정보 침해 신고 기준, 시점 등이 법적 요구사항을 준수하지 못하는 경우

항 목	2.11.2 취약점 점검 및 조치
인증기준	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고, 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고, 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
주요 확인사항	• 정보시스템 취약점 점검 절차를 수립하고, 정기적으로 점검을 수행하고 있는가? • 발견된 취약점에 대한 조치를 수행하고, 그 결과를 책임자에게 보고하고 있는가? • 최신 보안취약점 발생 여부를 지속적으로 파악하고, 정보시스템에 미치는 영향을 분석하여 조치하고 있는가? • 취약점 점검 이력을 기록관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대하여 보호대책을 마련하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검), 제6조(접근통제)

세부 설명

■ 정보시스템 취약점 점검 절차를 수립하고, 정기적으로 점검을 수행하여야 한다.

▶ 취약점 점검 절차에 포함되어야 할 사항

- 취약점 점검 대상(예 : 서버, 네트워크 장비 등)
- 취약점 점검 주기(법적 요구사항, 중요도 등 고려)
- 취약점 점검 담당자 및 책임자 지정
- 취약점 점검 절차 및 방법 등
- 중요도에 따른 조치 기준
- 취약점 점검 결과 보고 절차
- 미조치 취약점에 대한 보안성 검토 등
- 기타 보안사고 예방 및 복구를 위하여 필요한 사항 등

▶ 취약점 점검 대상

- 라우터, 스위치 등 네트워크시스템 구성 및 설정 취약점
- 서버 OS 보안 설정 취약점
- 방화벽 등 보안시스템 취약점
- 애플리케이션 취약점
- 웹서비스 취약점
- 스마트기기 및 모바일 서비스(모바일 앱 등) 취약점 등

- 취약점 점검 시 회사의 규모 및 보유하고 있는 정보의 중요도에 따라 모의침투테스트를 수행하는 것을 고려
- 개인정보처리자는 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항을 내부 관리계획에 포함하여 수립·시행 필요(개인정보의 안전성 확보조치 기준 제4조제1항제10호)

■ 발견된 취약점에 대한 조치를 수행하고, 그 결과를 책임자에게 보고하여야 한다.

- 취약점 점검 시 이력관리가 될 수 있도록 점검일시, 점검대상, 점검방법, 점검내용 및 결과, 발견사항, 조치사항 등이 포함된 보고서 작성
- 취약점별로 대응조치 완료 후 이행점검 등을 통하여 완료 여부 확인
- 불가피하게 조치할 수 없는 취약점에 대해서는 그 사유를 명확하게 확인하고, 이에 따른 위험성, 보완대책 등을 책임자에게 보고

■ 최신 보안취약점 발생 여부를 지속적으로 파악하고, 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.

- 정기적인 보안취약점 점검 외에도 지속적으로 최신 보안취약점 파악
- 최신 보안취약점이 발견된 경우 해당 보안취약점이 정보시스템에 미치는 영향을 분석하여 필요시 대응 조치

■ 취약점 점검 이력을 기록관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대한 보호대책을 마련하여야 한다.

- 취약점 점검 이력에 대한 기록관리
- 취약점 점검 시 지난 취약점 점검결과와 비교 분석하여 취약점 재발 여부 확인
- 유사한 취약점이 재발되고 있는 경우 근본원인 분석 및 재발방지 대책 마련

증거자료

예시

- 취약점 점검 계획서
- 취약점 점검 결과보고서(웹, 모바일 앱, 서버, 네트워크시스템, 보안시스템, DBMS 등)
- 취약점 점검 이력
- 취약점 조치계획서
- 취약점 조치완료보고서
- 모의해킹 계획서·결과보고서

결함사례

- 사례 1 : 내부 규정에 연 1회 이상 주요 시스템에 대한 기술적 취약점 점검을 하도록 정하고 있으나, 주요 시스템 중 일부가 취약점 점검 대상에서 누락된 경우
- 사례 2 : 취약점 점검에서 발견된 취약점에 대한 보완조치를 이행하지 않았거나, 단기간 내에 조치할 수 없는 취약점에 대한 타당성 검토 및 승인 이력이 없는 경우

항 목	2.11.3 이상행위 분석 및 모니터링
인증기준	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.
주요 확인사항	• 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가? • 침해시도, 개인정보유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제6조(접근통제)

세부 설명

■ 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링 하여야 한다.

▶ 이상행위 판단을 위하여 정보시스템, 보안시스템, 응용프로그램, 네트워크 장비 등의 로그를 수집하고 분석하는 체계를 갖추어야 함

- 이벤트 로그를 수집하거나 모니터링 하여야 할 대상 및 범위
- 수집 및 분석, 모니터링 방법
- 담당자 및 책임자 지정
- 분석 및 모니터링 결과 보고 체계
- 이상행위 발견 시 대응 절차 등

▶ 조직의 규모 및 정보시스템의 중요도가 높은 경우 24시간 실시간 모니터링 고려

■ 침해시도, 개인정보유출 시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고, 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지도록 하여야 한다.

▶ 이상행위 판단을 위한 이상행위 식별기준 및 임계치를 설정하고, 필요시 시스템에 반영

▶ 설정된 기준 및 임계치를 주기적으로 검토하여 최적화

▶ 이상행위가 확인된 경우 규정에 따라 긴급 대응, 소명 요청, 원인 조사 등 사후조치 수행

증거자료

예시

- 이상행위 분석 및 모니터링 현황
- 이상행위 발견 시 대응 증거자료

결함사례

- 사례 1 : 외부로부터의 서버, 네트워크, 데이터베이스, 보안시스템에 대한 침해 시도를 인지할 수 있도록 하는 상시 또는 정기적 모니터링 체계 및 절차를 마련하고 있지 않은 경우
- 사례 2 : 외부 보안관제 전문업체 등 외부 기관에 침해시도 모니터링 업무를 위탁하고 있으나, 위탁업체가 제공한 관련 보고서를 검토한 이력이 확인되지 않거나, 위탁 대상에서 제외된 시스템에 대한 자체 모니터링 체계를 갖추고 있지 않은 경우
- 사례 3 : 내부적으로 정의한 임계치를 초과하는 이상 트래픽이 지속적으로 발견되고 있으나, 이에 대한 대응조치가 이루어지고 있지 않은 경우

항 목	2.11.4 사고 대응 훈련 및 개선
인증기준	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.
주요 확인사항	• 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련계획을 수립하고 이에 따라 연 1회 이상 주기적으로 훈련을 실시하고 있는가? • 침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하고 있는가?

세부 설명

- 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련계획을 수립하고, 이에 따라 연 1회 이상 주기적으로 훈련을 실시하여야 한다.
  - 침해사고 대응 절차의 적절성을 검토하고, 사고 발생 시 신속한 대응이 가능하도록 모의훈련 계획의 수립 및 이행
  - 최신 침해 사고 사례, 해킹 동향, 비즈니스 특성 등을 반영하여 현실적이고 실질적인 모의훈련 시나리오 마련
  - 정보보호, 개인정보보호, IT, 법무, 인사, 홍보 등 침해사고 대응과 관련된 조직이 모두 참여할 수 있도록 모의훈련 조직 구성
  - 관련 임직원이 침해사고 대응 절차를 숙지할 수 있도록 연 1회 이상 주기적으로 모의훈련 수행
- 침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하여야 한다.
  - 모의훈련 시행 후 결과보고서 작성 및 내부 보고
  - 모의훈련 결과를 바탕으로 개선사항을 도출하여 필요시 대응 절차에 반영

증거자료

예시

- 침해사고 및 개인정보 유출사고 대응 모의훈련 계획서
- 침해사고 및 개인정보 유출사고 대응 모의훈련 결과서
- 침해사고 대응 절차

결함사례

- 사례 1 : 침해사고 모의훈련을 수행하지 않았거나 관련 계획서 및 결과보고서가 확인되지 않은 경우
- 사례 2 : 연간 침해사고 모의훈련 계획을 수립하였으나 타당한 사유 또는 승인 없이 해당 기간 내에 실시하지 않은 경우
- 사례 3 : 모의훈련을 계획하여 실시하였으나, 관련 내부 지침에 정한 절차 및 서식에 따라 수행하지 않은 경우

항 목	2.11.5 사고 대응 및 복구
인증기준	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.
주요 확인사항	• 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응 절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가? • 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체 통지 및 관계기관 신고 절차를 이행하고 있는가? • 침해사고가 종결된 후 사고의 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하고 있는가? • 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하고 있는가?
관련 법규	• 개인정보 보호법 제34조(개인정보의 유출 등의 통지·신고) • 정보통신망법 제48조의3(침해사고의 신고 등), 제48조의4(침해사고의 원인분석 등)

세부 설명

■ 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응절차에 따라 신속하게 대응 및 보고가 이루어져야 한다.

▶ 침해사고 초기 대응 및 증거 보존 조치

- 침해가 의심되는 정보시스템의 접속권한 삭제·변경 또는 접속차단 조치
- 네트워크, 방화벽 등 대내외 시스템 보안점검 및 취약점 보완 조치
- 사고 조사에 필요한 외부의 접속기록 등 증거 보존 조치
- 로그 분석 등을 통한 개인정보 및 중요정보 유출 여부 확인 등

▶ 다음 사항을 포함한 침해사고보고서 작성 및 내부 보고

- 침해사고 발생일시
- 보고자와 보고일시
- 사고내용(발견사항, 피해내용 등)
- 사고대응 경과 내용
- 사고대응까지의 소요시간 등

▶ 침해사고가 조직에 미치는 영향이 심각할 경우 보고절차에 따라 최고경영진까지 신속히 보고

■ 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체 통지 및 관계기관 신고 절차를 이행하여야 한다.

▶ 개인정보의 분실·도난·유출(이하 유출등)에 따른 정보주체 통지 요건

구분	내용
통지 사항	1. 유출등이 된 개인정보의 항목 2. 유출등이 된 시점 및 경위 3. 유출등으로 인해 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 4. 개인정보처리자의 대응조치 및 피해 구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 ※ 통지 사항 중 1호, 2호 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 통지해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지
통지 방법	• 서면등의 방법(서면, 전자우편, 팩스, 전화, 문자전송 등)
통지 시기	• 유출등을 알게 된 때로부터 72시간 이내 • 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있음 1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우 2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우
통지 예외	• 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 인터넷 홈페이지에 30일 이상 위의 5가지 통지 사항을 게시하는 것으로 통지 갈음 가능 • 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 위의 5가지 통지 사항을 30일 이상 게시

▶ 개인정보의 유출등에 따른 관계기관 신고 요건

구분	내용
신고 사항	1. 유출등이 된 개인정보의 항목 2. 유출등이 된 시점 및 경위 3. 유출등으로 인해 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 4. 개인정보처리자의 대응조치 및 피해 구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 ※ 신고 사항 중 1호, 2호 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고
신고 기관	• 개인정보 보호위원회 또는 한국인터넷진흥원
신고 방법	• 서면등의 방법(서면, 전자우편, 팩스, 전화, 문자전송 등) ※ 개인정보 포털(www.privacy.go.kr)을 통해 신고 가능
신고 시기	• 유출등을 알게 된 때로부터 72시간 이내 • 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고

구분	내용
신고 대상	1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우 2. 민감정보 또는 고유식별정보가 유출등이 된 경우 3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우 ※ 다만, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 미신고 가능

- 침해사고가 종결된 후 사고 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하여야 한다.
  - 침해사고가 처리되고 종결된 후 이에 대한 사고 원인에 대한 분석을 수행하고 결과보고서를 작성하여 책임자에게 보고
  - 침해사고 정보와 발견된 취약점 및 원인, 조치방안 등을 관련 조직 및 인력에게 공유
- 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하여야 한다.
  - 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 반복되지 않도록 하는 재발방지 대책 수립
  - 분석된 결과에 따라 필요한 경우 침해사고 대응절차, 정보보호 정책 및 절차 등 침해사고 대응체계에 대한 변경 수행

증거자료

예시

- 침해사고 대응 절차
- 침해사고 대응보고서
- 침해사고 관리대장
- 개인정보 유출신고서
- 비상연락망

결함사례

- 사례 1 : 내부 침해사고 대응지침에는 침해사고 발생 시 내부 정보보호위원회 및 이해관계 부서에게 보고하도록 정하고 있으나, 침해사고 발생 시 담당 부서에서 자체적으로 대응 조치 후 정보보호위원회 및 이해관계 부서에 보고하지 않은 경우
- 사례 2 : 최근 DDoS 공격으로 의심되는 침해사고로 인하여 서비스 일부가 중단된 사례가 있으나, 이에 대한 원인분석 및 재발방지 대책이 수립되지 않은 경우
- 사례 3 : 외부 해킹에 의해 개인정보 유출사고가 발생하였으나, 유출된 개인정보 건수가 소량이라는 이유로 72시간 이내에 통지 및 신고가 이루어지지 않은 경우
- 사례 4 : 담당자의 실수에 의해 인터넷 홈페이지 게시판을 통해 1천명 이상 정보주체에 대한 개인정보 유출이 발생하였으나, 해당 정보주체에 대한 유출 통지가 이루어지지 않은 경우

2.12. 재해 복구

항 목	2.12.1 재해·재난 대비 안전조치
인증기준	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고, 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.
주요 확인사항	• 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고, 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별하고 있는가? • 핵심 IT 서비스 및 시스템의 중요도 및 특성에 따른 복구 목표시간, 복구 목표시점을 정의하고 있는가? • 재해·재난 발생 시에도 핵심 서비스 및 시스템의 연속성을 보장할 수 있도록 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구 계획을 수립·이행하고 있는가?
관련 법규	• 개인정보 보호법 제29조(안전조치의무) • 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

세부 설명

■ 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고, 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별하여야 한다.

▶ 자연재해, 해킹, 통신장애 등 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형 식별

※ IT 서비스 중단을 초래할 수 있는 IT 재해 유형(예시)
· 자연재해 : 화재, 홍수, 지진, 태풍 등
· 외부요인 : 해킹, 통신장애, 정전 등
· 내부요인 : 시스템 결함, 기계적 오류, 사용자 실수, 의도적·악의적 운영, 핵심 운영자 근무 이탈(사망, 병가, 휴가, 이직 등), 환경설정 오류 등

▶ 다음 사항을 고려하여 재해 유형별 조직의 핵심 서비스(업무) 중단 시 피해규모 및 영향을 분석하여 핵심 IT 서비스 및 시스템을 식별

- 매출감소, 계약위약금 지급 등 재무적 측면
- 손해배상 소송 등 법적 측면
- 대외 이미지 하락, 경쟁력 손상 등 정성적 측면

■ 핵심 IT 서비스 및 시스템의 중요도 및 특성에 따른 복구 목표시간, 복구 목표시점을 정의하여야 한다.

▶ IT 서비스 및 시스템 중단시점부터 복구되어 정상가동될 때까지의 복구 목표시간(RTO : Recovery Time Objective)과 데이터가 복구되어야 하는 복구 목표시점(RPO : Recovery Point Objective)을 정의

■ 재해·재난 발생 시에도 핵심 서비스 및 시스템의 연속성을 보장할 수 있도록 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구 계획을 수립·이행하여야 한다.

▶ IT 재해 발생 시 사전 정의한 서비스 및 시스템 복구 목표시간 및 복구 목표시점을 달성할 수 있도록 비용효과적인 복구전략 및 대책 수립

▶ IT 재해 발생 시 신속한 복구가 가능하도록 다음 내용을 포함한 IT 재해 복구 체계 구축

- 재해 시 복구조직 및 역할 정의 : IT 재해 발생 시 복구를 위한 관련부서 및 담당자 역할과 책임 부여
- 비상연락체계 : 조직 내 관련 부서 담당자, 유지보수 업체 등 복구 조직상 연락체계 구축
- 복구 전략 및 대책 수립방법론 : 업무영향분석, 복구 목표시간 및 복구 목표시점 정의, 핵심 IT 서비스 및 시스템 식별 등
- 복구 순서 정의 : 복구 목표 시간별로 정보시스템의 복구 순서 정의
- 복구 절차 : 재해 발생, 복구 완료, 사후관리 단계 포함

▶ 개인정보처리자의 경우 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 함(개인정보의 안전성 확보조치 기준 제11조)

※ 개인정보처리시스템 위기대응 매뉴얼 및 백업·복구 계획(예시)
· 개인정보처리시스템 구성 요소(개인정보 보유량, 종류·중요도, 시스템 연계 장비·설비 등)
· 재해·재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안
· 개인정보처리시스템 백업 및 복구 우선순위, 복구 목표시점, 복구 목표시간
· 개인정보처리시스템 백업 및 복구 방안(복구센터 마련, 백업계약 체결, 비상가동 등)
· 업무분장, 책임 및 역할
· 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등

증거자료

예시

- IT 재해 복구 지침·절차
- IT 재해 복구 계획(RTO, RPO 정의 포함)
- 비상연락망
- 개인정보처리시스템 위기대응 매뉴얼

결함사례

- 사례 1 : IT 재해 복구 절차서 내에 IT 재해 복구 조직 및 역할 정의, 비상연락체계, 복구 절차 및 방법 등 중요한 내용이 누락되어 있는 경우
- 사례 2 : 비상사태 발생 시 정보시스템의 연속성 확보 및 피해 최소화를 위하여 백업센터를 구축하여 운영하고 있으나, 관련 정책에 백업센터를 활용한 재해 복구 절차 등이 수립되어 있지 않아 재해 복구 시험 및 복구가 효과적으로 진행되기 어려운 경우
- 사례 3 : 서비스 운영과 관련된 일부 중요 시스템에 대한 복구 목표시간이 정의되어 있지 않으며, 이에 대한 적절한 복구 대책을 마련하고 있지 않은 경우
- 사례 4 : 재해 복구 관련 지침서 등에 IT 서비스 또는 시스템에 대한 복구 우선순위, 복구 목표시간, 복구 목표시점 등이 정의되어 있지 않은 경우
- 사례 5 : 현실적 대책 없이 복구 목표시간을 과도 또는 과소하게 설정하고 있거나, 복구 목표시점과 백업정책(대상, 주기 등)이 적절히 연계되지 않아 복구 효과성을 보장할 수 없는 경우

항 목	2.12.2 재해 복구 시험 및 개선
인증기준	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.
주요 확인사항	• 수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험계획을 수립·이행하고 있는가? • 시험결과, 정보시스템 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토·보완하고 있는가?

세부 설명

■ 수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험계획을 수립·이행하여야 한다.

※ IT 재해 복구 시험계획에 포함되어야 할 사항(예시)
· 재해 복구 시험 일정(일시 및 장소)
· 참여인원
· 범위
· 방법 및 시나리오
· 절차 등

▶ 시험계획에 따라 정기적인 시험을 실시하여 복구 전략 및 대책이 효과적인지, 비상시 복구 조직 구성원이 복구절차에 따라 신속하게 대응하는지 등을 점검

■ 시험결과, 정보시스템 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토·보완하여야 한다.

▶ IT 재해 복구 계획에 대한 공식적인 변화관리 절차 마련

▶ 재해 복구 시험 결과와 정보시스템 환경변화 등을 고려하여 복구 계획을 정기적으로 검토·보완

증거자료

예시

- IT 재해 복구 절차서
- IT 재해 복구 시험 계획서
- IT 재해 복구 시험 결과서

결함사례

- 사례 1 : 재해 복구 훈련을 계획·시행하지 않았거나 관련 계획서 및 결과보고서가 확인되지 않은 경우
- 사례 2 : 재해 복구 훈련 계획을 수립하였으나, 타당한 사유 또는 승인 없이 계획대로 실시하지 않았거나 관련 결과보고가 확인되지 않은 경우
- 사례 3 : 재해 복구 훈련을 계획하여 실시하였으나, 내부 관련 지침에 정한 절차 및 서식에 따라 이행되지 않아 수립한 재해 복구 절차의 적정성 및 효과성을 평가하기 위한 훈련으로 보기 어려운 경우

3 개인정보 처리 단계별 요구사항

3.1. 개인정보 수집 시 보호조치

항 목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 14세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	• 개인정보를 수집하는 경우 정보주체 동의, 법령상 의무준수, 계약 체결·이행 등 적법 요건에 따라 수집하고 있는가? • 정보주체에게 개인정보 수집 동의를 받는 경우 동의방법 및 시점은 적절하게 되어 있는가? • 정보주체에게 개인정보 수집 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 알아보기 쉽게 표시하고 있는가? • 만 14세 미만 아동의 개인정보에 대해 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받고 있는가? • 법정대리인의 동의를 받기 위하여 필요한 최소한의 개인정보만을 수집하고 있으며, 법정대리인이 자격 요건을 갖추고 있는지 확인하는 절차와 방법을 마련하고 있는가? • 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항 등의 고지 시 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 표현하고 있는가? • 정보주체 및 법정대리인에게 동의를 받은 기록을 보관하고 있는가? • 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하거나 정보주체에게 알리고 있는가? • 정보주체의 동의 없이 개인정보의 추가적인 이용 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 이용이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보 처리방침에 공개하고 이를 점검하고 있는가?
관련 법규	• 개인정보 보호법 제15조(개인정보의 수집·이용), 제22조(동의를 받는 방법), 제22조의2(아동의 개인정보 보호) • 개인정보 처리 방법에 관한 고시

세부 설명

■ 개인정보를 수집하는 경우 정보주체 동의, 법령상 의무준수, 계약 체결·이행 등 관련 법률에 따른 적법 요건을 명확히 식별하고 이에 따라 개인정보를 적법하게 수집하여야 한다.

▶ 개인정보 수집 경로 별로 개인정보 수집의 적법 요건을 명확히 식별하고, 이를 입증할 수 있도록 관련 근거를 기록·관리

- 예를 들어, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 정보주체 동의 없이 개인정보를 수집하는 경우, 해당 법률 또는 법령의 조항 등 관련 근거를 문서화

▶ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용 가능

★ 개인정보의 수집이 가능한 경우(개인정보 보호법 제15조제1항)

1. 정보주체의 동의를 받는 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우
5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

■ 정보주체에게 개인정보 수집 동의를 받는 경우에는 개인정보 수집매체의 특성을 반영하여 적절한 방법으로 정보주체의 동의를 받아야 하며, 해당 정보가 필요한 시점에 수집하여야 한다.

▶ 개인정보 수집 동의는 수집매체의 특성에 따라 다음의 사항을 고려하여 적절한 방법으로 정보주체의 동의를 받아야 함

★ 개인정보 처리에 대한 동의를 받는 방법(개인정보 보호법 시행령 제17조제2항)

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

▶ 회원가입 단계에서 개인정보를 미리 포괄적으로 수집하지 말아야 하며, 해당 정보가 필요한 시점에 수집하여야 함

- 서비스 개시를 위하여 필요한 개인정보에 한하여 수집·이용 동의를 받아야 하며, 이후에 제공되는 서비스의 경우 해당 서비스 제공시점에 동의를 받아야 함
- 웹사이트 회원가입 시 웹사이트 내 특정 서비스 이용에만 필요한 개인정보는 해당 서비스 이용시점에 수집

- 다만, 반복적인 서비스의 경우로서 최초 서비스 이용 시점에 선택 동의 항목으로 분류하여 동의를 받는 경우에는 수집·이용 가능

■ 정보주체에게 개인정보 수집 동의를 받는 경우에는 법정 고지사항에 대해 명확하게 고지하고 동의를 받아야 하며, 법령에서 정한 중요 내용에 대해 명확히 표시하여 정보주체가 이를 알아보기 쉽게 하여야 한다.

▶ 정보주체로부터 개인정보 수집·이용 동의를 받을 때에는 4가지의 법정 고지사항을 구체적이고 명확하게 알리고 동의를 받아야 함

★ 개인정보의 수집·이용 동의 시 고지사항(개인정보 보호법 제15조제2항)
1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

▶ 정보주체의 동의가 적법하기 위해서는 정보주체의 자유로운 의사에 따른 동의 여부 결정, 동의 내용의 구체성 및 명확성 등 적법 요건을 모두 충족하여야 함

★ 정보주체의 동의를 받을 때 충족해야 하는 조건(개인정보 보호법 시행령 제17조제1항)
1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의를 받으려는 내용이 구체적이고 명확할 것
3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

※ 단, 본 규정은 2024년 9월 15일부터 시행

▶ 개인정보 보호법 제22조(동의를 받는 방법)제2항에 따라 개인정보 처리에 대한 동의를 서면(전자문서 및 전자거래기본법 제2조제1호에 따른 전자문서를 포함)으로 받을 때에는 다음과 같이 중요한 내용을 명확히 표시하여 알아보기 쉽게 하여야 함

★ 명확히 표시하여야 하는 중요한 내용(개인정보 보호법 시행령 제17조제3항)
· 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
· 처리하려는 개인정보 항목 중 민감정보, 여권번호, 운전면허번호, 외국인등록번호
· 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
· 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

★ 중요한 내용의 표시 방법(개인정보 처리 방법에 관한 고시 제4조)
· 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
· 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

※ 종이 인쇄물, 컴퓨터 표시화면 등 서면 동의를 요구하는 매체의 특성과 정보주체의 이용환경 등을 고려하여 정보주체가 쉽게 알아볼 수 있도록 표시

※ 상세한 내용은 '개인정보 처리 동의 안내서(개인정보 보호위원회)' 참고

■ 만 14세 미만 아동에 대하여 개인정보를 수집·이용·제공 등 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받아야 한다.

▶ 만 14세 미만 아동의 개인정보를 처리할 필요가 없는 경우에는 적절한 연령확인 절차를 통해 만 14세 미만 아동의 개인정보를 수집하지 않도록 조치

▶ 만 14세 미만 아동의 개인정보를 처리할 필요가 있는 경우에는 별도의 수집 동의 양식과 법정대리인 확인 절차를 마련하여 법정대리인의 동의를 받을 수 있도록 조치

★ 법정대리인이 동의했는지를 확인하는 방법(개인정보 보호법 시행령 제17조의2제1항)

1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 개인정보처리자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법
2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법
3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법
4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나 우편 또는 팩스를 통하여 전달하고, 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법
6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 받는 방법
7. 그 밖에 제1호부터 제6호까지의 규정에 준하는 방법으로서 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

■ 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보(성명·연락처에 관한 정보)만을 수집하여야 하며, 법정대리인이 자격요건을 갖추고 있는지 확인하는 절차와 방법을 마련하여야 한다.

▶ 법정대리인 동의를 받기 위하여 필요한 최소한의 정보(법정대리인의 성명·연락처에 관한 정보)는 법정대리인의 동의 없이 아동으로부터 직접 수집이 가능함

- 다만 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 이름과 연락처를 수집하고자 하는 이유를 알려야 함(표준 개인정보 보호지침 제13조제1항)
- 아동으로부터 수집한 법정대리인의 개인정보는 동의를 얻기 위한 용도로만 활용하여야 함

▶ 법정대리인의 동의를 얻기 위해서는 아동이 제공한 정보가 진정한 법정대리인의 정보인지와 법정대리인의 진위 여부를 확인하여야 함

- 법정대리인의 미성년자 여부 확인
- 아동과의 나이 차이 확인 등

※ (참고)미성년자의 법정대리인

· 1차적으로 아동의 부모 등 친권자가 법정대리인에 해당(민법 제911조)

· 미성년자에게 부모가 없거나 부모가 친권을 행사할 수 없는 때에는, 2차적으로 후견인이 법정대리인이 되며, 후견인은 지정후견인(민법 제931조), 선임후견인(민법 제932조) 순서를 따름

- 법정대리인이 동의를 거부하거나, 법정대리인의 동의 의사가 확인되지 않은 경우 수집일로부터 5일 이내에 파기하여야 함(표준 개인정보 보호지침 제13조제2항)

■ 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항 등의 고지 시 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 표현하여야 한다.

- 아동이 이해하기 쉬운 언어, 그림, 동영상 등 아동 친화적인 방식으로 정보를 투명하게 전달
- 연령대별 아동의 역량과 이용행태 등을 고려

※ 상세한 내용은 '아동·청소년 개인정보 보호 가이드라인(개인정보 보호위원회)' 참고

■ 개인정보 수집·이용 동의에 따른 적법 근거를 입증할 수 있도록 정보주체 및 법정대리인에게 동의를 받은 기록을 남기고 보존하여야 한다.

- 기록으로 남겨야 할 사항 : 동의 일시, 동의 항목, 동의자(법정대리인이 동의한 경우 법정대리인 정보), 동의 방법 등
- 보존기간 : 회원탈퇴 등으로 인하여 해당 개인정보를 파기할 때까지

■ 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하거나 서면등의 방법으로 정보주체에게 알려야 한다.

- 정보주체의 동의 없이 개인정보 수집·이용이 가능한 경우 : 개인정보 보호법 제15조제1항 제2호부터 제7호에 해당하는 경우
- 정보주체에게 알려야 할 사항 : 동의 없이 처리할 수 있는 개인정보 항목 및 처리의 법적 근거
- 정보주체에게 알리는 방법 : 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하거나 서면등의 방법(서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법)으로 정보주체에게 통지

■ 정보주체의 동의 없이 개인정보의 추가적인 이용 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등 고려사항에 대한 판단기준을 수립·이행하여야 하며, 추가적인 이용이 지속적으로 발생하는 경우 이를 개인정보 처리방침에 공개하고 기준 준수여부를 점검하여야 한다.

★ 개인정보의 추가적인 이용 시 고려사항(개인정보 보호법 시행령 제14조의2제1항)

1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

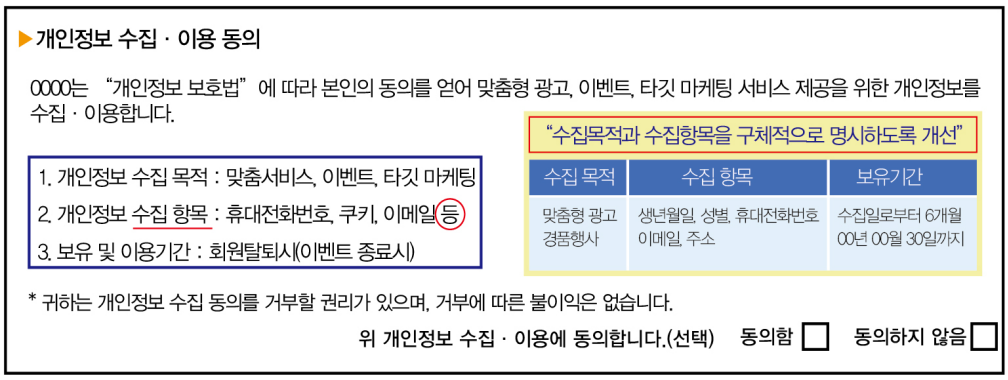
증거자료

예시

- 온라인 개인정보 수집 양식(홈페이지 회원가입 화면, 모바일앱 회원가입 화면, 이벤트 참여 등)
- 오프라인 개인정보 수집 양식(회원가입신청서 등)
- 개인정보 수집 동의 기록(회원 데이터베이스 등)
- 법정대리인 동의 기록
- 개인정보 처리방침

결함사례

- 사례 1 : 개인정보 보호법을 적용받는 개인정보처리자가 개인정보 수집 동의 시 고지 사항에 '동의 거부 권리 및 동의 거부에 따른 불이익 내용'을 누락한 경우
- 사례 2 : 개인정보 수집 동의 시 수집하는 개인정보 항목을 구체적으로 명시하지 않고 '~ 등'과 같이 포괄적으로 안내하는 경우



- 사례 3 : 쇼핑몰 홈페이지에서 회원가입 시 회원가입에 필요한 개인정보 외에 추후 물품 구매 시 필요한 결제·배송 정보를 미리 필수 항목으로 수집하는 경우
- 사례 4 : Q&A, 게시판을 통하여 비회원의 개인정보(이름, 이메일, 휴대폰번호)를 수집하면서 개인정보 수집 동의 절차를 거치지 않은 경우
- 사례 5 : 만 14세 미만 아동의 개인정보를 수집하면서 법정대리인의 동의를 받지 않은 경우
- 사례 6 : 만 14세 미만 아동에 대하여 서비스를 제공하고 있지 않지만, 회원가입 단계에서 입력받는 생년월일을 통하여 나이 체크를 하지 않아 법정대리인 동의 없이 가입된 만 14세 미만 아동 회원이 존재한 경우
- 사례 7 : 법정대리인의 진위 여부를 확인하는 절차가 미흡하여 미성년자 등 아동의 법정대리인으로 보기 어려운데도 법정대리인 동의가 가능한 경우
- 사례 8 : 만 14세 미만 아동으로부터 법정대리인 동의를 받는 목적으로 법정대리인의 개인정보(이름, 휴대폰번호)를 수집한 이후 법정대리인의 동의가 장기간 확인되지 않았음에도 이를 파기하지 않고 계속 보유하고 있는 경우
- 사례 9 : 법정대리인 동의에 근거하여 만 14세 미만 아동의 개인정보를 수집하였으나, 관련 기록을 보존하지 않아 법정대리인 동의와 관련된 사항(법정대리인 이름, 동의 일시 등)을 확인할 수 없는 경우

항 목	3.1.2 개인정보 수집 제한
인증기준	개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을 수집하여야 하며, 정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 않아야 한다.
주요 확인사항	• 개인정보를 수집하는 경우 그 목적에 필요한 범위에서 최소한의 정보만을 수집하고 있는가? • 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 있는가? • 정보주체가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?
관련 법규	• 개인정보 보호법 제16조(개인정보의 수집제한), 제22조(동의를 받는 방법)

세부 설명

■ 개인정보를 수집하는 경우 법률 근거, 법령상 의무준수, 계약의 체결·이행 등 그 목적에 필요한 범위에서 최소한의 정보만을 수집하여야 한다.

▶ 정보주체의 동의를 받거나 법률 근거, 법령상 의무준수, 계약의 체결·이행 등을 근거로 정보주체 동의 없이 개인정보를 수집하는 경우에도 그 목적에 필요한 최소한의 개인정보만을 수집하여야 함

▶ 최소한의 개인정보에 대한 입증책임은 개인정보처리자가 부담하므로 필수로 수집하는 정보에 대하여 서비스 제공 등에 필요한 최소한의 개인정보임을 입증할 수 있어야 함(이때 최소한의 개인정보란 해당 서비스의 본질적 기능을 위하여 반드시 필요한 정보를 말함)

※ 최소정보(예시)

· 쇼핑업체가 고객에게 상품을 배송하기 위하여 수집한 이름, 주소, 전화번호 등은 필요 최소한의 개인정보라고 할 수 있으나, 직업, 생년월일 등 배송과 관련 없는 개인정보를 요구하는 것은 최소정보의 범위를 벗어난 것임

· 경품 행사에 응모한 고객에게 경품추첨 사실을 알리는데 필요한 개인정보 외에 응모자의 성별, 자녀수, 동거 여부 등 사생활의 비밀에 관한 정보, 고유식별정보 등을 요구하는 것은 최소정보의 범위를 벗어난 것임

· 취업 희망자의 경력, 전공, 자격증 등에 관한 정보는 업무 능력을 판단하기 위한 최소한의 정보라고 할 수 있으나, 가족관계, 결혼유무, 본적(원적) 등에 관한 정보는 최소한의 정보를 벗어난 것임

■ 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알려야 한다.

▶ 어떤 정보가 필요 최소한의 정보이고 아닌지를 정보주체가 쉽게 알아볼 수 있도록 구분해서 고지

▶ 필요 최소한의 정보가 아닌 정보에 대해서는 재화 또는 서비스의 이용에 방해를 받음이 없이 자유롭게 동의를 거부할 수 있음을 고지

■ 정보주체가 수집 목적에 필요한 최소한의 정보 이외의 개인정보를 제공하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하여야 한다.

▶ 정보주체가 선택항목에 대한 동의를 거부하더라도 서비스의 이용이 가능하다는 사실을 명확하게 표시하여 알 수 있도록 고지

▶ 회원가입 과정에서 선택정보에 대하여 동의를 하지 않거나 입력을 하지 않더라도 회원가입 등 필수적인 서비스는 이용이 가능하도록 구현

※ 상세한 내용은 '알기쉬운 개인정보 처리 동의 안내서(개인정보 보호위원회)' 참고

증거자료

예시

- 온라인 개인정보 수집 양식(홈페이지 회원가입 화면, 이벤트 참여 화면 등)
- 오프라인 개인정보 수집 양식(멤버십 가입신청서 등)
- 개인정보 처리방침

결함사례

- 사례 1 : 계약의 체결 및 이행을 근거로 정보주체 동의 없이 개인정보를 수집하면서 계약의 체결 및 이행을 위해 반드시 필요하지 않은 개인정보 항목까지 과도하게 수집하는 경우
- 사례 2 : 정보주체로부터 선택사항에 대한 동의를 받으면서 해당 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리지 않은 경우
- 사례 3 : 회원가입 양식에서 필수와 선택 정보를 구분하여 별도 동의를 받도록 되어 있었으나, 선택정보에 대하여 동의하지 않아도 회원가입이 가능함을 정보주체가 인지할 수 있도록 구체적으로 알리지 않은 경우(개인정보 입력 양식에 개인정보 항목별로 필수, 선택 여부가 표시되어 있지 않은 경우 등)
- 사례 4 : 홈페이지 회원가입 화면에서 선택사항에 대하여 동의하지 않거나 선택정보를 입력하지 않으면 다음 단계로 넘어가지 않거나 회원가입이 차단되는 경우
- 사례 5 : 채용 계약 시 채용 예정 직무와 직접 관련이 없는 가족사항 등 과도한 개인정보를 수집하는 경우

사진	이름							
	생년월일							
	주소							
	채용 계약시 가족사항 등 개인정보 수집은 불필요함							
	전화번호	집 전화			E-mail			
		휴대전화			비상연락처			
신체사항	신장	체중	혈액형	시력	기타	종교	취미	특기
가족사항	관계	성명	연령	학력	직업	직위	동거여부	

항 목	3.1.3 주민등록번호 처리 제한
인증기준	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
주요 확인사항	• 주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가? • 주민등록번호의 수집 근거가 되는 법조항을 구체적으로 식별하고 있는가? • 법적 근거에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하고 있는가?
관련 법규	• 개인정보 보호법 제24조의2(주민등록번호 처리의 제한) • 정보통신망법 제23조의2(주민등록번호의 사용 제한)

세부 설명

■ 주민등록번호는 다음과 같이 법적 근거가 있는 경우를 제외하고는 수집 등 처리할 수 없다.

▶ 주민등록번호 수집 등 처리가 가능한 경우(동의에 근거한 수집은 불가함)

개인정보 보호법 제24조의2제1항	정보통신망법 제23조의2제1항
1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 3. 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우	1. 본인확인기관으로 지정받은 경우 2. 「전기통신사업법」 제38조제1항에 따라 기간통신사업자로부터 이동통신서비스 등을 제공받아 재판매하는 전기통신사업자가 제23조의3에 따라 본인확인기관으로 지정받은 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하는 경우

■ 주민등록번호를 처리하는 경우에는 해당 처리의 근거가 되는 법조항을 구체적으로 식별하여 입증할 수 있도록 하여야 한다.

▶ '법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우'라 함은 법률 등 중 최소한 어느 하나에 개인정보처리자로 하여금 주민등록번호의 처리를 요구하거나 허용하도록 하는 구체적인 규정이 존재하는 것을 말함

▶ 개인정보 보호법 제24조의2제1항제1호는 주민등록번호를 처리할 수 있는 법령의 범위를 한정하고 있으므로 시행규칙을 근거로는 주민등록번호 처리 불가

▶ 개인정보 보호법 제24조의2제1항제2호에 따라 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우에는 예외적으로 주민등록번호의 처리 가능

▶ 개인정보 보호법 제24조의2제1항 각 호에서 정하는 예외사유에 해당되지 않는 한 주민등록번호를 수집하거나 제3자에게 제공하거나 저장·보유하는 것도 금지됨

※ 주민등록번호 처리 관련 적법성 판단 예시

· 시행규칙 및 각급 행정기관의 훈령·예규·고시 및 지방자치단체의 조례·규칙 등은 주민등록번호 수집의 근거가 될 수 없음

· 법령에서 단순히 신원확인 또는 연령확인 등의 의무만을 규정하고 있다면 이는 주민등록번호에 대한 처리근거를 구체적으로 규정한 것에 해당하지 않음

· 주민등록번호 전체가 아니라 뒤 7자리만 수집·이용하는 것은 주민등록번호의 부여 체계를 활용하여 주민등록번호의 고유한 특성, 즉 유일성과 식별성을 이용하는 행위이므로 이는 주민등록번호 전체를 수집·이용하는 것으로 볼 수 있음(뒤 7자리 중 일부만 처리하는 경우에도 마찬가지임)

· 입사지원자가 최종 합격하여 직원이 되기 전까지는 법률이나 대통령령에서 기업이 해당 지원자의 주민등록번호를 처리하도록 하는 규정이 없으므로, 이력서·지원서 등에 주민등록번호를 기재하도록 하는 것은 금지됨. 다만 최종합격한 후에는 고용보험 등 4대 보험 가입, 급여 원천징수 등을 위해 관련 법률이나 대통령령에서 정하는 바에 따라 기업이 해당 지원자의 주민등록번호를 수집 등 처리하는 것은 가능

· 신분확인 목적으로 주민등록번호가 기재된 신분증을 육안으로 확인하고 돌려주는 행위는 주민등록번호를 수집하는 행위가 아니므로 주민등록번호 처리금지 원칙에 위배되지 않음

■ 법적 근거에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(주민등록번호 대체가입수단)을 제공하여야 한다.

▶ 주민등록번호 대체가입수단 예시 : 아이핀, 휴대전화, 신용카드, 인증서 등

※ 대체가입수단을 이용한 식별값(예시)

· CI(Connection Information, 연계정보) : 본인확인기관에서 대체수단을 통한 본인확인의 경우 생성되는 일방향 암호화된 88byte 문자열, 외부 연계정보로만 활용되어야 하며, 내부 식별용으로는 사용하지 않는 것이 바람직함

· DI(Duplication Information, 중복가입 확인정보) : 본인확인기관에서 대체수단을 통한 본인확인의 경우에 생성되는 일방향 암호화된 64byte 문자열, 사이트 내 이용자의 중복 계정 생성을 제한하기 위하여 사용함

증거자료

예시

- 개인정보 수집 양식(홈페이지 회원가입 화면, 이벤트 참여, 멤버십 가입신청서 등)
- 온라인 개인정보 수집 양식(본인확인 등 대체가입수단 제공 화면)
- 주민등록번호를 처리하는 경우 주민등록번호 처리 근거 증거자료
- 개인정보 처리방침

결함사례

- 사례 1 : 홈페이지 가입과 관련하여 실명확인 등 단순 회원관리 목적을 위하여 정보주체의 동의에 근거하여 주민등록번호를 수집한 경우
- 사례 2 : 정보주체의 주민등록번호를 시행규칙이나 지방자치단체의 조례에 근거하여 수집한 경우
- 사례 3 : 비밀번호 분실 시 본인확인 등의 목적으로 주민등록번호 뒤 6자리를 수집하지만, 관련된 법적 근거가 없는 경우
- 사례 4 : 채용전형 진행단계에서 법적 근거 없이 입사지원자의 주민등록번호를 수집한 경우
- 사례 5 : 콜센터에 상품, 서비스 관련 문의 시 본인확인을 위하여 주민등록번호를 수집한 경우
- 사례 6 : 주민등록번호 수집의 법적 근거가 있다는 사유로 홈페이지 회원가입 단계에서 대체가입수단을 제공하지 않고 주민등록번호를 입력받는 본인확인 및 회원가입 방법만을 제공한 경우

항 목	3.1.4 민감정보 및 고유식별정보의 처리 제한
인증기준	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도 동의를 받아야 한다.
주요 확인사항	• 민감정보는 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가? • 고유식별정보(주민등록번호 제외)는 정보주체로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하고 있는가? • 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알리고 있는가?
관련 법규	• 개인정보 보호법 제23조(민감정보의 처리제한), 제24조(고유식별정보의 처리 제한)

세부 설명

■ 민감정보의 처리는 원칙적으로 금지되며, 다만 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에 한하여 처리할 수 있다.

▶ 민감정보의 범위

1. 사상·신념 : 각종 이데올로기 또는 사상적 경향, 종교적 신념 등
2. 정치적 견해 : 정치적 사안에 대한 입장이나 특정 정당의 지지 여부에 관한 정보
3. 노동조합·정당의 가입·탈퇴 : 노동조합 또는 정당에의 가입·탈퇴에 관한 정보
4. 건강 및 성생활에 관한 정보 : 개인의 과거 및 현재의 병력(病歷), 신체적·정신적 장애(장애등급 유무 등), 성적취향 등에 관한 정보
5. 사생활을 현저하게 침해할 우려가 있는 개인정보

· 유전자 검사 등의 결과로 얻은 유전 정보, 범죄 경력에 관한 정보

· 벌금 이상의 형의 선고·면제 및 선고 유예, 보호감호, 치료감호, 보호관찰, 선고유예의 실효, 집행유예의 취소, 벌금 이상의 형과 함께 부과된 몰수, 추징, 사회봉사명령, 수감명령 등의 선고 또는 처분 등 범죄경력에 관한 정보

· 개인의 신체적·생리적·행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통한 생성한 정보(생체인식 특징정보)

· 인종이나 민족에 관한 정보

▶ 민감정보의 처리가 가능한 경우

1. 정보주체로부터 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

- 고유식별정보(주민등록번호 제외)는 정보주체로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하여야 한다.
  - 고유식별정보의 범위
    1. 주민등록번호(다만 주민등록번호 수집 법정주의에 따라 동의에 근거한 수집은 불가함)
    2. 여권번호
    3. 운전면허번호
    4. 외국인등록번호
  - 고유식별정보(주민등록번호 제외)의 처리가 가능한 경우
    1. 정보주체로부터 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
    2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
- 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알려야 한다.
  - 해당되는 경우 개인정보 처리방침에도 공개 필요

증거자료

예시

- 온라인 개인정보 수집 양식(홈페이지 회원가입 화면, 이벤트 참여 등)
- 오프라인 개인정보 수집 양식(회원가입신청서 등)
- 개인정보 처리방침

결함사례

- 사례 1 : 장애인에 대한 요금감면 등 혜택 부여를 위하여 장애 여부 등 건강에 관한 민감정보를 수집하면서 다른 개인정보 항목에 포함하여 일괄 동의를 받은 경우
- 사례 2 : 회원가입 시 외국인에 한하여 외국인등록번호를 수집하면서 다른 개인정보 항목에 포함하여 일괄 동의를 받은 경우
- 사례 3 : 민감정보 또는 고유식별정보의 수집에 대해 별도의 동의를 받으면서 고지하여야 할 4가지 사항 중에 일부를 누락하거나 잘못된 내용으로 고지하는 경우(동의 거부 권리 및 동의 거부에 따른 불이익 사항을 고지하지 않은 경우 등)

항 목	3.1.5 개인정보 간접수집
인증기준	정보주체 이외로부터 개인정보를 수집하거나 제3자로부터 제공받는 경우에는 업무에 필요한 최소한의 개인정보를 수집하거나 제공받아야 하며, 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
주요 확인사항	• 정보주체 이외의 제3자로부터 개인정보를 제공받는 경우 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통하여 명시하고 있는가? • 공개된 매체 및 장소에서 개인정보를 수집하는 경우 정보주체의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하고 있는가? • 서비스 계약 이행을 위해 필요한 경우로서, 서비스 제공 과정에서 자동수집장치 등에 의하여 수집·생성하는 개인정보의 경우에도 최소수집 원칙을 적용하고 있는가? • 정보주체 이외로부터 수집하는 개인정보에 대해 정보주체의 요구가 있는 경우 즉시 필요한 사항을 정보주체에게 알리고 있는가? • 정보주체 이외로부터 수집한 개인정보를 처리하는 경우 개인정보의 종류·규모 등이 법적 요건에 해당하는 경우 필요한 사항을 정보주체에게 알리고 있는가? • 정보주체에게 수집 출처에 대해 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는가?
관련 법규	• 개인정보 보호법 제16조(개인정보의 수집 제한), 제19조(개인정보를 제공받은 자의 이용·제공 제한), 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 통지)

세부 설명

- 정보주체 이외의 제3자로부터 개인정보를 제공받는 경우 적법한 절차에 따라 수집·제공되는 정보인지 여부를 확인하고 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통하여 구체적으로 명시하여야 한다.
- SNS, 인터넷 홈페이지 등 공개된 매체 또는 장소에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지 등의 표시 내용에 비추어 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 이용할 수 있다(표준 개인정보 보호지침 제6조제4항).
- 서비스 계약 이행을 위하여 필요한 경우로서 서비스 제공과정에서 자동수집장치 등에 의하여 수집·생성되는 개인정보(통화기록, 접속로그, 결제기록, 이용내역 등)에 대해서도 해당 서비스의 계약 이행 및 제공을 위하여 필요한 최소한의 개인정보만을 수집하여야 한다.
  - 다만 서비스 제공 계약 이행과는 무관한 목적으로 이용하기 위하여 수집하는 경우에는 선택 동의 항목으로 분류하여 별도의 사전 동의를 받아야 함(예를 들어, 쿠키를 통하여 수집하는 행태정보를 분석하여 개인별 맞춤형 광고에 활용하는 경우 등)
- 정보주체 이외로부터 수집하는 개인정보에 대해 정보주체의 요구가 있으면 즉시 필요한 사항을 정보주체에게 알려야 한다.

▶ 정보주체의 요구가 있는 경우 알려야 할 사항

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실

▶ 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 알려야 함(표준 개인정보 보호지침 제9조제1항)

▶ 통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있는 등으로 인하여 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 알려야 함(표준 개인정보 보호지침 제9조제2항)

★ 개인정보 수집 출처 통지 거부 사유(개인정보 보호법 제20조제4항)

1. 통지를 요구하는 대상이 되는 개인정보가 개인정보 보호법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일(국가 안전, 외교상 비밀, 범죄의 수사, 다른 법령에 따라 비밀로 분류 등 개인정보파일의 등록 및 공개 제외 대상)에 포함되어 있는 경우
2. 통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

■ 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 개인정보의 종류·규모 등 법적 요건에 해당하는 경우 필요한 사항을 정보주체에게 통지하여야 한다.

▶ 통지 의무 요건 및 방법

구분	내용
통지 의무가 부과되는 조건	• 개인정보 보호법 제17조제1항제1호에 따라 정보주체의 개인정보 제3자 제공 동의를 근거로 다른 개인정보처리자로부터 개인정보를 제공받은 경우
통지 의무가 부과되는 개인정보처리자 요건	• 5만 명 이상 정보주체에 관한 민감정보 또는 고유식별정보를 처리하는 자 • 100만 명 이상의 정보주체에 관한 개인정보를 처리하는 자 ※ (정보주체수 산정기준) 전년도말 기준 직전 3개월 간 일일평균 기준
통지하여야 할 사항	• 개인정보의 수집 출처 • 개인정보의 처리 목적 • 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실
통지 시기	• 개인정보를 제공받은 날로부터 3개월 이내 • 다만, 법 제17조제2항제1호부터 제4호까지의 사항에 대하여 같은 조 제1항제1호에 따라 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상 정보주체에게 알려야 함

구분	내용
통지 방법	• 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법 • 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법
통지 예외	• 통지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우 • 통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 ※ 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한함
기타	• 법 제20조제2항에 따라 개인정보의 수집 출처 등에 관한 사항을 알리는 것과 법 제20조의2제1항에 따른 이용·제공 내역의 통지를 함께 할 수 있음 • 정보주체에게 수집 출처에 대하여 알린 기록을 해당 개인정보의 파기 시까지 보관·관리(정보주체에게 알린 사실, 알린 시기, 알린 방법)

▶ 본 개인정보 수집 출처 통지 의무는 개인정보 보호법 제17조제1항제1호에 따라 정보주체의 동의를 받아 개인정보를 제공한 개인정보처리자로부터 수집한 개인정보에 대해서만 적용되므로 신용정보법에 따라 동의를 받아 개인정보를 제공한 자로부터 수집한 개인정보 또는 법령에 따라 제공받은 개인정보에 대해서는 적용되지 않음(개인정보 보호 법령 및 지침·고시 해설서)

▶ 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 않은 경우에는 알리지 않아도 됨

■ 정보주체에게 수집 출처에 대하여 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하여야 한다.

▶ 수집 출처 통지 관련 보관·관리하여야 할 정보(개인정보 보호법 시행령 제15조의2제4항)

1. 정보주체에게 알린 사실
2. 알린 시기
3. 알린 방법

증거자료

예시

- 개인정보 제공 관련 계약서(제공하는 자와의 계약 사항)
- 개인정보 수집출처에 대한 정보주체 통지 내역
- 개인정보 처리방침

결함사례

- 사례 1 : 인터넷 홈페이지, SNS에 공개된 개인정보를 수집하고 있는 상태에서 정보주체의 수집 출처 요구에 대한 처리절차가 존재하지 않은 경우
- 사례 2 : 개인정보 보호법 제17조제1항제1호에 따라 다른 사업자로부터 개인정보 제공동의를 근거로 개인정보를 제공받았으나, 이에 대하여 해당 정보주체에게 3개월 내에 통지하지 않은 경우(다만 제공받은 자가 5만 명 이상 정보주체의 민감정보 또는 고유식별정보를 처리하거나 100만 명 이상 정보주체의 개인정보를 처리하는 경우)
- 사례 3 : 법적 의무 대상자에 해당되어 개인정보 수집 출처를 정보주체에게 통지하면서 개인정보의 처리목적 또는 동의를 철회할 권리가 있다는 사실 등 필수 통지사항을 일부 누락한 경우
- 사례 4 : 법적 의무 대상자에 해당되어 개인정보 수집 출처를 정보주체에게 통지하였으나, 수집 출처 통지에 관한 기록을 해당 개인정보의 파기 시까지 보관하지 않은 경우

항 목	3.1.6 영상정보처리기기 설치·운영
인증기준	고정형 영상정보처리기기를 공개된 장소에 설치·운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 경우 법적 허용 요건에 해당하는지를 검토하고 있는가? • 공공기관 등이 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계자의 의견을 수렴하고 있는가? • 고정형 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가? • 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기를 운영하는 경우 법적 허용 요건에 해당하는지를 검토하고 있는가? • 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우 불빛, 소리, 안내판 등의 방법으로 촬영 사실을 표시하고 알리고 있는가? • 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는가? • 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 파기하고 있는가? • 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 계약서에 반영하고 있는가?
관련 법규	• 개인정보 보호법 제25조(고정형 영상정보처리기기의 설치·운영 제한), 제25조의2(이동형 영상정보처리기기의 운영 제한)

세부 설명

■ 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 경우 법적 허용 요건에 해당하는지를 검토하여야 한다.

▶ 고정형 영상정보처리기기의 정의 : 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 폐쇄회로 텔레비전 및 네트워크 카메라를 말함(개인정보 보호법 제2조제7호 및 동법 시행령 제3조제1항)

★ 고정형 영상정보처리기기의 범위(개인정보 보호법 시행령 제3조제1항)

1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치
   가. 일정한 공간에 설치된 카메라를 통하여 지속적 또는 주기적으로 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
   나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치

2. 네트워크 카메라: 일정한 공간에 설치된 기기를 통하여 지속적 또는 주기적으로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

▶ 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 경우

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 다음 중 어느 하나에 해당하는 경우로서 촬영된 영상을 별도로 저장하지 아니하는 경우
   · 출입자 수 등 통계값 산출을 위해 필요한 경우
   · 성별, 연령대 등 통계적 특성값을 도출하기 위해 필요한 경우
   · 그 밖에 위의 2가지에 준하는 경우로서 개인정보 보호위원회의 심의·의결을 거친 경우

▶ 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하는 것은 금지됨. 다만 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설(교정시설, 수용시설을 갖추고 있는 정신의료기관, 정신요양시설, 정신재활시설)에 대하여는 예외적으로 허용됨

■ 공공기관 등이 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 등의 법적 절차를 거쳐 관계 전문가 및 이해관계자의 의견을 수렴하여야 한다.

▶ 의견 수렴 절차를 거쳐야 하는 자

1. 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 공공기관의 장
2. 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하려는 교정시설, 정신의료기관, 정신요양시설, 정신재활시설

▶ 의견 수렴 절차

1. 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
2. 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

▶ 의견 수렴 대상자

1. 관계 전문가
2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

■ 고정형 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판을 설치하여야 한다.

▶ 안내판에 포함되어야 할 사항

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 연락처
4. 위탁받은 자의 명칭 및 연락처(영상정보처리기기 설치·운영 사무 위탁 시)

▶ 안내판 설치 예외 사항

1. 군사시설
2. 국가중요시설
3. 국가보안시설

▶ 안내판 설치 시 고려사항

- 정보주체가 쉽게 알아볼 수 있는 위치에 설치
- 건물 안에 여러개의 고정형 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해단 시설 또는 장소 전체가 고정형 영상정보처리기기 설치지역임을 표시하는 안내판 설치 가능
- 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 고정형 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우, 산불감시용 고정형 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우에는 인터넷 홈페이지에 관련 사항 게재 가능

■ 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기를 운영하는 경우 법적 허용 요건에 해당하는지를 검토하고 이에 따른 조치를 이행하여야 한다.

▶ 이동형 영상정보처리기기의 정의 : 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말함(개인정보 보호법 제2조제7호의2 및 동법 시행령 제3조제2항)

★ 이동형 영상정보처리기기의 범위(개인정보 보호법 시행령 제3조제2항)

1. 착용형 장치: 안경 또는 시계 등 사람의 신체 또는 의복에 착용하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치
2. 휴대형 장치: 이동통신단말장치 또는 디지털 카메라 등 사람이 휴대하면서 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치
3. 부착·거치형 장치: 차량이나 드론 등 이동 가능한 물체에 부착 또는 거치(据置)하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치

▶ 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기를 운영할 수 있는 경우

1. 개인정보 보호법 제15조제1항 각 호의 어느 하나에 해당하는 경우(정보주체의 동의 등)
2. 촬영 사실을 명확히 표시하여 정보주체가 촬영사실을 알 수 있도록 하였음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우. 이 경우 정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정
3. 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우

▶ 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할

우려가 있는 장소의 내부를 볼 수 있는 곳에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상 촬영 금지. 다만 범죄, 재난, 화재 또는 이에 준하는 상황에서 인명의 구조·구급 등을 위해 영상 촬영이 필요한 경우에는 예외적으로 촬영 가능

- 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우 불빛, 소리, 안내판 등의 방법으로 촬영 사실을 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다.
  - 촬영 사실 표시 방법 : 불빛, 소리, 안내판, 서면, 안내방송 또는 그 밖에 이에 준하는 수단
  - 촬영 사실 표시 예외 : 드론에 의한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 쉽게 알 수 있도록 표시하고 알리기 어려운 경우에는 개인정보 보호위원회가 이동형 영상정보처리기기의 촬영사실 표시를 지원하기 위하여 구축·운영하는 홈페이지를 통해 촬영 사실 및 목적, 촬영 일시 및 장소 등의 사항을 공지(표준 개인정보 보호지침 제39조의2제2항)
- 영상정보처리기기운영자는 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하여야 한다.
  - 고정형 영상정보처리기기운영자의 경우 고정형 영상정보처리기기 운영·관리 방침을 마련하고, 이동형 영상정보처리기기운영자의 경우 이동형 영상정보처리기기 운영·관리 방침을 마련
  - 영상정보처리기기 운영·관리 방침에 포함하여야 할 사항
    1. 영상정보처리기기의 설치 근거 및 설치 목적
    2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
    3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
    4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
    5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
    6. 정보주체의 영상정보 열람 등 요구에 대한 조치
    7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
    8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항
  - 개인정보 처리방침을 정할 때 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있음
  - 고정형 영상정보처리기기가 설치된 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추지 않도록 규정에 포함하고 관리·감독 수행
  - 고정형 영상정보처리기기의 녹음 기능을 사용할 수 없도록 조치
- 영상정보의 보관 기간을 정하여 보관 기간 만료 시 지체 없이 파기하여야 한다.
  - 영상정보의 보유 목적 달성을 위한 최소한의 기간으로 보관 기간 결정
  - 다만, 영상정보의 보관 기간과 관련하여 다른 법령에 특별한 규정이 있는 경우에는 해당 규정에 따라 보관
  - 영상정보처리기기운영자가 그 사정에 따라 보유 목적 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 함(표준 개인정보 보호지침 제41조제2항)

■ 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 필요한 내용을 계약서에 반영하여야 한다.

▶ 공공기관의 영상정보처리기기 설치·운영 사무 위탁 계약서에 포함되어야 할 내용(개인정보 보호법 시행령 제26조제1항)

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

증거자료

예시

- 영상정보처리기기 운영 현황
- 영상정보처리기기 안내판
- 영상정보처리기기 운영·관리방침
- 영상정보처리기기 관리화면(계정·권한 내역, 영상정보 보존기간 등)
- 영상정보처리기기 운영 수탁자와의 계약서 및 점검 이력

결함사례

- 사례 1 : 영상정보처리기기 안내판의 고지 문구가 일부 누락되어 운영되고 있거나, 영상정보처리기기 운영·관리 방침을 수립·운영하고 있지 않은 경우
- 사례 2 : 영상정보처리기기 운영·관리 방침을 수립 운영하고 있으나, 방침 내용과 달리 보관기간을 준수하지 않고 운영되거나, 영상정보 보호를 위한 접근통제 및 로깅 등 방침에 기술한 사항이 준수되지 않는 등 관리가 미흡한 경우
- 사례 3 : 영상정보처리기기의 설치·운영 사무를 외부업체에 위탁하고 있으나, 영상정보의 관리 현황 점검에 관한 사항, 손해배상 책임에 관한 사항 등 법령에서 요구하는 내용을 영상정보처리기기 업무 위탁 계약서에 명시하지 않은 경우
- 사례 4 : 영상정보처리기기의 설치·운영 사무를 외부업체에 위탁하고 있으나, 영상정보처리기기 안내판에 수탁자의 명칭과 연락처를 누락하여 고지한 경우

항 목	3.1.7 마케팅 목적의 개인정보 수집·이용
인증기준	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.
주요 확인사항	• 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보 처리에 대한 동의를 받는 경우 정보주체가 이를 명확하게 인지할 수 있도록 알리고 별도의 동의를 받고 있는가? • 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 경우 수신자의 명시적인 사전 동의를 받고 있으며, 2년마다 정기적으로 수신자의 수신동의 여부를 확인하고 있는가? • 전자적 전송매체를 이용한 영리목적의 광고성 정보 전송에 대하여 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우 영리목적의 광고성 정보 전송을 중단하도록 하고 있는가? • 영리목적의 광고성 정보를 전송하는 경우 전송자의 명칭, 수신거부 방법 등을 구체적으로 밝히고 있으며, 야간시간에는 전송하지 않도록 하고 있는가?
관련 법규	• 개인정보 보호법 제22조(동의를 받는 방법) • 정보통신망법 제50조(광고성 정보 전송 제한)

세부 설명

■ 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보를 처리하고자 하는 경우에는 정보주체가 명확하게 인지할 수 있도록 알리고 별도의 동의를 받아야 한다.

▶ ‘홍보 및 마케팅’ 목적으로 개인정보를 수집하면서 ‘부가서비스 제공’, ‘제휴 서비스 제공’ 등으로 목적을 기재하는 행위 금지

▶ 상품 홍보, 마케팅 목적으로 수집하는 개인정보는 다른 목적으로 수집하는 정보와 명확하게 구분하여 동의를 받고 수집

▶ 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실을 명확하게 표시하여 알아보기 쉽도록 동의서 양식 구현(글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용을 명확히 표시)

■ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 경우 수신자의 명시적인 사전 동의를 받아야 하며, 2년마다 정기적으로 수신자의 수신동의 여부를 확인하여야 한다.

▶ ‘전자적 전송매체’란 휴대전화, 유선전화, 팩스, 메신저, 이메일, 게시판 등을 말함

▶ 영리목적의 광고성 정보를 전송하려면 문서(전자문서 포함) 또는 구술의 방법으로 수신자의 명시적인 수신동의를 받아야 함

※ 영리목적의 광고성 정보의 개념

· 영리목적의 광고성 정보는 전송자가 경제적 이득을 취할 목적으로 전송하는 ①전송자에 관한 정보, ②전송자가 제공할 재화나 서비스의 내용을 말함. 전송을 하게 한 자도 전송자에 포함됨
· 영업을 하는 자가 고객에게 보내는 정보는 원칙적으로 모두 광고성 정보에 해당함
· 영리법인은 존재목적이 영리추구이기 때문에 원칙적으로 고객에게 전송하는 모든 정보는 영리목적 광고성 정보에 해당하며, 비영리법인은 전송하는 정보의 성격에 따라 영리목적 광고성 여부를 판단함
· 구체적인 재화나 서비스의 홍보가 아니더라도 수신자에게 발송하는 정보가 발신인의 이미지 홍보에 해당하는 경우에는 광고성 정보로 볼 수 있음
· 주된 정보가 광고성 정보가 아니더라도 부수적으로 광고성 정보가 포함되어 있으면 전체가 광고성 정보에 해당함

※ 영리목적의 광고성 정보의 예외

· 수신자와 이전에 체결하였던 거래를 용이하게 하거나, 완성 또는 확인하는 것이 목적인 정보
· 수신자가 사용하거나 구매한 재화 또는 서비스에 대한 설명, 보증, 제품 리콜, 안전 또는 보안 관련 정보
· 고객의 요청에 의하여 발송하는 1회성 정보(견적서 등)
· 수신자가 금전적 대가를 지불하고 신청한 정보(뉴스레터, 주식정보, 축산물 거래정보 등)
· 전송자가 제공하는 재화 또는 서비스에 대하여 수신자가 구매 또는 이용과 관련한 안내 및 확인 정보 등

▶ 개인정보 보호법 제22조제1항제7호에 따른 재화나 서비스 홍보·판매권유 목적의 동의는 전송자가 광고성 정보를 전송하기 위하여 수신자의 개인정보를 수집·이용하는 것에 대한 동의에 해당하고, 정보통신망법 제50조제1항 동의는 전송자가 보내는 광고성 정보를 수신하겠다는 것에 대한 동의에 해당하여 두 개의 동의는 구분 후 별개로 받아야 함

▶ 스마트폰 앱(애플리케이션)을 다운받아 단순히 설치만 한 상태에서는 광고성 정보(앱 푸시 광고)를 전송하여서는 안 되며, 앱을 최초로 실행하는 경우 광고성 정보의 수신동의 여부를 확인하여 동의를 받은 후 광고를 전송하여야 함

▶ 다만 거래관계에 의한 예외에 해당하는 경우에는 수신동의를 받지 않고 광고성 정보 전송이 가능함

※ 거래관계에 의한 광고성 정보전송 수신동의 예외

· 재화 등의 거래관계를 통하여 수신자로부터 직접 연락처를 수집한 자가 거래가 있은 날로부터 6개월 이내에 자신이 처리하고 수신자와 거래한 것과 동종의 재화 등에 대한 영리목적의 광고성 정보를 전송하려는 경우
· 「방문판매 등에 관한 법률」에 따른 전화권유판매자가 육성으로 수신자에게 개인정보의 수집출처를 고지하고 전화권유를 하는 경우

▶ 수신자의 수신동의를 받아 광고성 정보를 전송하는 자는 수신동의 여부를 수신동의를 받은 날부터 2년마다 확인하여야 함

- 수신동의자에게 수신동의 하였다는 사실에 대한 안내의무를 부과한 것이므로 재동의를 받을 필요는 없음

- 수신자가 아무런 의사표시를 하지 않은 경우에는 수신동의 의사가 그대로 유지되는 것으로 봄
- 수신 여부 확인 시 수신자에게 알려야 할 사항

  1. 전송자의 명칭
  2. 수신동의 날짜 및 수신에 동의한 사실
  3. 수신동의에 대한 유지 또는 철회 의사를 표시하는 방법

■ 전자적 전송매체를 이용한 영리목적의 광고성 정보 전송에 대하여 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우 영리목적의 광고성 정보 전송을 중단하여야 한다.

▶ 거래관계가 있더라도 수신자가 수신거부 의사를 표시한 경우 광고성 정보의 전송이 금지됨

▶ 회원탈퇴를 하는 것도 수신거부 의사표시를 한 것으로 볼 수 있으므로 회원탈퇴를 한 수신인에게 광고성 정보를 전송하면 안 됨

▶ 수신자가 특별히 범위를 정하여 수신동의 철회 및 수신거부 의사표시를 한 것이 아니라면 그 효력은 당해 광고만이 아니라 당해 전송자가 보내는 모든 광고에 적용됨

■ 영리목적의 광고성 정보를 전송하는 경우 전송의 명칭, 수신거부 방법 등을 구체적으로 밝혀야 한다.

▶ 전자적 전송매체를 이용하여 영리목적의 광고성 정보 전송 시 함께 알려야 할 사항

1. 전송자의 명칭 및 연락처
2. 수신의 거부 또는 수신동의의 철회 의사표시를 쉽게 할 수 있는 조치 및 방법에 관한 사항

※ 정보통신망법 시행령 별표6(영리목적의 광고성 정보의 명시사항 및 명시방법) 준수

▶ 야간시간(오후 9시부터 그 다음 날 오전 8시까지)에는 전자적 전송매체를 이용하여 영리 목적의 광고성 정보 전송은 금지됨

- 야간시간에 광고성 정보를 전송하기 위해서는 별도의 수신동의가 필요함
- 단, 전자우편의 경우 별도 동의가 없더라도 야간 전송 가능

※ 상세한 내용은 '불법 스팸 방지를 위한 정보통신망법 안내서' 참고

증거자료

예시

- 온라인 개인정보 수집 양식(홈페이지 회원가입 화면, 모바일앱 회원가입 화면, 이벤트 참여 등)
- 오프라인 개인정보 수집 양식(회원가입신청서 등)
- 마케팅 동의 기록
- 광고성 정보전송 수신동의 기록 및 수신동의 의사확인 기록
- 광고성 정보 발송 시스템 관리자 화면(메일, SMS, 앱 푸시 등)
- 광고성 정보 발송 문구
- 개인정보 처리방침

결함사례

- 사례 1 : '홍보 및 마케팅' 목적으로 개인정보를 수집하면서 '부가서비스 제공', '제휴 서비스 제공' 등과 같이 목적을 모호하게 안내하는 경우 또는 다른 목적으로 수집하는 개인정보와 구분하지 않고 포괄 동의를 받는 경우
- 사례 2 : 모바일 앱에서 광고성 정보전송(앱 푸시)에 대하여 거부 의사를 밝혔으나, 프로그램 오류 등의 이유로 광고성 앱 푸시가 이루어지는 경우
- 사례 3 : 온라인 회원가입 화면에서 문자, 이메일에 의한 광고성 정보 전송에 대하여 디폴트로 체크되어 있는 경우
- 사례 4 : 광고성 정보 수신동의 여부에 대하여 2년마다 확인하지 않은 경우
- 사례 5 : 영리목적의 광고성 정보를 전자우편으로 전송하면서 제목이 시작되는 부분에 '(광고)' 표시를 하지 않은 경우

3.2. 개인정보 보유 및 이용 시 보호조치

항 목	3.2.1 개인정보 현황관리
인증기준	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
주요 확인사항	• 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하고 있는가? • 공공기관이 개인정보파일을 운용하거나 변경하는 경우 관련된 사항을 법률에서 정한 관계기관의 장에게 등록하고 있는가? • 공공기관은 개인정보파일의 보유 현황을 개인정보 처리방침에 공개하고 있는가?
관련 법규	• 개인정보 보호법 제32조(개인정보파일의 등록 및 공개)

세부 설명

■ 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 한다.

▶ 개인정보처리자(정보통신서비스 제공자)는 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 근거(동의, 법령 등), 처리목적 및 방법, 보유기간 등을 파악하여 개인정보 현황표, 개인정보 흐름표, 개인정보 흐름도 등을 통하여 기록·관리하여야 함

▶ 또한 정기적으로 개인정보 현황을 점검하고 관련 문서를 최신화하여야 함

■ 공공기관이 개인정보파일을 운용하거나 변경하는 경우 관련된 사항을 법률에서 정한 관계기관의 장에게 등록하여야 하며, 등록된 사항에 변경이 있는 경우에도 그 내용을 등록하여야 한다.

▶ 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 개인정보 보호위원회에 60일 이내에 등록

▶ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 해당 사항(개인정보파일 등록·변경)의 검토 및 적정성 판단을 요청한 후 상위 관리기관의 확인을 받아 개인정보 보호위원회에 60일 이내에 등록

▶ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관 포함)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙을 따름

▶ 다만「개인정보 보호법」제32조제2항에 해당하는 개인정보파일은 개인정보 보호위원회에 등록하지 않아도 됨

★ 개인정보 보호위원회 등록이 면제되는 개인정보파일(공공기관)
1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄 수사, 공소 제기 및 유지, 형 및 감호 집행, 교정 처분, 보호처분, 보안관찰처분과 출입국 관리에

관한 사항을 기록한 개인정보파일

3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 일회성으로 운영되는 파일 등 지속적으로 관리할 필요가 낮다고 인정되어 대통령령으로 정하는 개인정보파일
   - 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일
   - 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
   - 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일
6. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
7. 영상정보처리기기를 통하여 처리되는 개인영상정보파일
8. 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위하여 보유하는 개인정보파일

■ 공공기관은 개인정보파일의 보유 현황을 개인정보 처리방침에 공개하여야 한다.

▶ 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 공개(표준 개인정보 보호지침 제61조)

▶ 개인정보 보호위원회는 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 인터넷에 공개(개인정보 포털, www.privacy.go.kr)

증거자료

예시

- 개인정보 현황표
- 개인정보 흐름표·흐름도
- 개인정보파일 등록 현황
- 개인정보파일 관리대장
- 개인정보 처리방침

결함사례

- 사례 1 : 개인정보파일을 홈페이지의 개인정보파일 등록 메뉴를 통하여 목록을 관리하고 있으나, 그 중 일부 홈페이지 서비스와 관련된 개인정보파일의 내용이 개인정보 처리방침에 누락되어 있는 경우
- 사례 2 : 신규 개인정보파일을 구축한 지 2개월이 경과하였으나, 해당 개인정보파일을 개인정보 보호위원회에 등록하지 않은 경우
- 사례 3 : 개인정보 보호위원회에 등록되어 공개된 개인정보파일의 내용(수집하는 개인정보의 항목 등)이 실제 처리하고 있는 개인정보파일 현황과 상이한 경우
- 사례 4 : 공공기관이 임직원의 개인정보파일, 통계법에 따라 수집되는 개인정보파일에 대해 개인정보파일 등록 예외사항에 해당되지 않음에도 불구하고 해당 개인정보파일을 개인정보 보호위원회에 등록하지 않은 경우

항 목	3.2.2 개인정보 품질보장
인증기준	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체에게 관리절차를 제공하여야 한다.
주요 확인사항	• 개인정보를 최신의 상태로 정확하게 유지하기 위한 절차 및 방안을 수립·이행하고 있는가? • 정보주체가 본인의 개인정보에 대하여 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하고 있는가?
관련 법규	• 개인정보 보호법 제3조(개인정보 보호 원칙)

세부 설명

- 개인정보를 최신의 상태로 정확하게 유지하기 위한 절차 및 방안을 수립·이행하여야 한다.
  - 개인정보의 위조·변조·훼손을 방지하기 위한 안전조치 적용
  - 외부자 해킹, 내부자 권한 오·남용, 재해·재난 등에 의하여 불법적인 개인정보 변경, 손상 등이 발생하더라도 개인정보의 정확성·완전성을 확보할 수 있도록 백업·복구 등의 체계 구축·이행
  - 개인정보취급자에 의한 개인정보 변경 시 오입력 등이 발생하지 않도록 관리적·기술적 조치 적용
  - 정보주체가 개명(改名), 주민등록번호 유출 등에 따라 성명 또는 주민등록번호를 변경한 경우, 이를 반영하여 정보주체의 개인정보를 최신화할 수 있는 절차 수립·이행
- 정보주체가 본인의 개인정보에 대하여 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하여야 한다.
  - 홈페이지를 통한 개인정보 수정이 주기적으로 이루어질 수 있도록 공지
  - 정보주체가 본인의 개인정보 등록 현황을 쉽게 조회하고 변경할 수 있도록 다양한 방법 제공(온라인, 오프라인 등)
  - 개인정보 변경 시 안전한 본인확인 절차 마련 및 시행
  - 정보주체가 수집 및 처리되는 개인정보의 현황을 쉽게 알 수 있도록 개인정보 처리방침의 변경과 이력관련 내용을 쉽게 인지할 수 있도록 게시

증거자료

예시

- 정보주체 개인정보 수정·변경 양식(온라인, 오프라인)
- 개인정보 최신성 유지 절차

결함사례

- 사례 1 : 인터넷 홈페이지를 통하여 회원정보를 변경할 때는 본인확인 절차를 거치고 있으나, 고객센터 상담원과의 통화를 통한 회원 정보 변경 시에는 본인확인 절차가 미흡하여 회원정보의 불법적인 변경이 가능한 경우
- 사례 2 : 온라인 회원에 대해서는 개인정보를 변경할 수 있는 방법을 제공하고 있으나, 오프라인 회원에 대해서는 개인정보를 변경할 수 있는 방법을 제공하고 있지 않은 경우

항 목	3.2.3 이용자 단말기 접근 보호
인증기준	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.
주요 확인사항	• 정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받고 있는가? • 이동통신단말장치 내에서 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우, 정보주체(이용자)가 동의하지 않아도 서비스 제공을 거부하지 않도록 하고 있는가? • 이동통신단말장치 내에서 해당 접근권한에 대한 정보주체(이용자)의 동의 및 철회방법을 마련하고 있는가?
관련 법규	• 정보통신망법 제22조의2(접근권한에 대한 동의)

세부 설명

■ 정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 관련 사항을 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.

※ 이동통신단말장치의 범위
- 스마트폰 및 이동통신이 가능한 태블릿 PC에 적용
- 2G 이동통신 단말장치의 경우, 사실상 앱이 동작할 수 있는 환경이 아니므로 대상에서 제외
- 이동통신망을 이용하지 않고 단순히 블루투스, 와이파이, 테더링 등의 기능만 수행하는 기기는 적용대상에서 제외
- 스마트워치는 화면 크기 제약 등으로 인하여 접근권한에 대한 고지·동의 기능을 당장 구현하기 어려운 점을 고려하여, 우선 필수적 접근권한만 설정하도록 권장(다만 고지·동의 기능이 구현된 기기가 제조된 이후부터는 스마트폰 및 태블릿 PC와 동일하게 적용)

▶ 앱이 스마트폰 내에 저장되어 있는 정보와 설치된 기능에 접근할 수 있는 권한을 서비스에 필요한 범위 내로 최소화하여야 함

▶ 접근권한에 대한 동의를 받기 전에 해당 서비스 제공을 위하여 반드시 필요한 접근권한(이하 '필수적 접근권한'이라 함)과 반드시 필요한 접근권한이 아닌 접근권한(이하 '선택적 접근권한'이라 함)을 구분하여 접근권한이 필요한 항목 및 그 이유 등을 정보주체(이용자)에게 알기 쉽게 고지한 후, 정보주체(이용자)로부터 필수적·선택적 접근권한에 대한 동의를 각각 받아야 함

- (필수적 접근권한인 경우) ①접근권한이 필요한 정보 및 기능의 항목, ②해당 정보 및 기능에 접근이 필요한 이유를 알려야 함

- (선택적 접근권한인 경우) 위의 ①, ②와 함께 ③접근권한 허용에 동의하지 않을 수 있다는 사실을 알려야 함

■ 이동통신단말장치 내에서 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우, 정보주체(이용자)가 동의하지 않아도 서비스 제공을 거부하지 않아야 한다.

■ 이동통신단말장치 내에서 해당 접근권한에 대한 정보주체(이용자)의 동의 및 철회방법을 마련하여야 한다.

▶ (개별 동의 선택이 가능한 방식의 운영체제, 안드로이드 6.0 이상 및 아이폰) 정보주체(이용자)는 접근권한에 이미 동의한 경우일지라도 해당 운영체제에서 제공하는 앱별·접근권한별 동의 철회 기능을 사용하여 각 앱에 대한 접근권한을 재설정할 수 있음

▶ (개별 동의 선택이 불가능한 방식의 운영체제) 접근권한별 거부 기능이 구현되지 않아 원칙적으로 필수적 접근권한만 설정하도록 하였기 때문에 정보주체(이용자)가 이러한 필수적 접근권한에 대한 동의를 철회하고자 한다면 이미 설치한 앱을 삭제하면 됨. 다만 이러한 운영체제임에도 불구하고 앱 자체적으로 선택적 접근권한을 설정하여 이에 대한 동의 여부를 선택할 수 있는 기능을 구현한 경우라면 해당 앱에서 제공하는 동의 철회 기능을 사용하여 접근 권한을 재설정할 수 있음

※ 상세한 내용은 '스마트폰 앱 접근권한 개인정보 보호 안내서' 참고

증거자료

예시

- 앱 접근권한 동의 화면
- 앱 접근권한 설정 현황

결함사례

- 사례 1 : 스마트폰 앱에서 서비스에 불필요함에도 불구하고 주소록, 사진, 문자 등 스마트폰 내 개인정보 영역에 접근할 수 있는 권한을 과도하게 설정한 경우
- 사례 2 : 정보통신서비스 제공자의 스마트폰 앱에서 스마트폰 내에 저장되어 있는 정보 및 설치된 기능에 접근하면서 접근권한에 대한 고지 및 동의를 받지 않고 있는 경우
- 사례 3 : 스마트폰 앱의 접근권한에 대한 동의를 받으면서 선택사항에 해당하는 권한을 필수권한으로 고지하여 동의를 받는 경우
- 사례 4 : 접근권한에 대한 개별동의가 불가능한 안드로이드 6.0 미만 버전을 지원하는 스마트폰 앱을 배포하면서 선택적 접근권한을 함께 설정하여, 선택적 접근권한에 대하여 거부할 수 없도록 하고 있는 경우

항 목	3.2.4 개인정보 목적 외 이용 및 제공
인증기준	개인정보는 수집 시의 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보는 최초 수집 시 정보주체로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가? • 개인정보처리자로부터 개인정보를 제공받은 경우 제공받은 목적의 범위 내에서만 이용·제공하고 있는가? • 개인정보를 수집 목적 또는 개인정보처리자로부터 제공받은 목적의 범위를 초과하여 이용하거나 제공하는 경우 정보주체에게 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는가? • 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하고 있는가? • 공공기관이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하고 있는가? • 공공기관 등이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하는 등 절차를 마련하고 있는가?
관련 법규	• 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한), 제19조(개인정보를 제공받은 자의 이용·제공 제한)

세부 설명

■ 개인정보는 최초 수집 시 정보주체로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 한다.

▶ 정보주체에게 이용·제공의 목적을 고지하고 동의를 받은 범위나 개인정보 보호법 또는 다른 법령에 의하여 이용·제공이 허용된 범위를 벗어나서 개인정보를 이용하거나 제공 금지

※ 개인정보의 목적 외 이용·제공 사례

· 고객만족도 조사, 판촉행사, 경품행사에 응모하기 위하여 입력한 개인정보를 사전에 동의 받지 않고 자사의 할인판매행사 안내용 광고물 발송에 이용

· 홈쇼핑 회사가 주문 상품을 배달하기 위해 수집한 고객정보를 정보주체의 동의 없이 계열 콘도미니엄사에 제공하여 콘도미니엄 판매용 홍보자료 발송에 활용

■ 개인정보처리자로부터 개인정보를 제공받은 경우 제공받은 목적의 범위 내에서만 이용·제공하여야 한다.

▶ 개인정보를 제공받은 자는 해당 개인정보를 제공하거나 제공받은 목적과 다른 용도로 이용하거나 제3자 제공 금지

■ 개인정보를 수집 목적 또는 개인정보처리자로부터 제공받은 목적의 범위를 초과하여 이용하거나 제공하는 경우 정보주체에게 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하여야 한다.

▶ 개인정보를 목적 외의 용도로 이용·제공 가능한 경우(단, 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때는 제외)

No.	목적 외 이용·제공이 가능한 경우	공공기관	공공기관 외
1	정보주체로부터 별도의 동의를 받은 경우	○	○
2	다른 법률에 특별한 규정이 있는 경우	○	○
3	명백히 정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우	○	○
4	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 개인정보 보호위원회의 심의·의결을 거친 경우	○	-
5	조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우	○	-
6	범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우	○	-
7	법원의 재판업무 수행을 위하여 필요한 경우	○	-
8	형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우	○	-
9	공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우	○	○

▶ 개인정보를 목적 외 용도로 이용·제공하기 위하여 동의를 받을 경우 고지사항

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용목적)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용기간)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에 그 불이익의 내용

▶ 다른 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 됨

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

■ 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위해 필요한 조치를 마련하도록 요청하여야 한다.

▶ 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한

▶ 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서 포함)로 요청

▶ 해당 개인정보를 받는 자와 개인정보의 안전성 확보조치에 관한 책임관계 명확화

■ 공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

▶ 목적 외 이용·제공 시 관보 또는 인터넷 홈페이지에 게재하지 않아도 되는 경우(예외 사항)

1. 정보주체의 동의를 근거로 목적 외 이용·제공 시
2. 범죄의 수사와 공소의 제기 및 유지를 위하여 목적 외 이용·제공 시

▶ 관보 또는 인터넷 홈페이지 게재 사항

1. 목적 외 이용 등을 한 날짜
2. 목적 외 이용 등의 법적 근거
3. 목적 외 이용 등의 목적
4. 목적 외 이용 등을 한 개인정보의 항목

▶ 관보 또는 인터넷 홈페이지 게재 시점 및 기간

1. 게재 시점 : 목적 외 이용·제공한 날로부터 30일 이내
2. 게재 기간 : 인터넷 홈페이지에 게재하는 경우 10일 이상

■ 공공기관 등이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하여야 한다.

▶ 공공기관의 경우 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 '개인정보 목적 외 이용 및 제3자 제공대장'에 기록·관리하여야 함

※ '개인정보 목적 외 이용 및 제3자 제공대장'에 기록·관리하여야 하는 사항(「개인정보 처리 방법에 관한 고시」 별지 1호 서식)

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 개인정보 보호를 위하여 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

▶ 사법기관 또는 정부기관의 개인정보 등 자료 제공 요청(영장, 명령, 자료제출 요구 등)에 체계적으로 대응하기 위한 절차를 마련

※ 사법기관 또는 정부기관의 개인정보 등 자료 제공 요청 대응 절차 마련 시 고려사항

· 제공에 대한 법적 근거, 요청 접수창구(담당조직 및 담당자 지정 포함), 정식 공문(영장 등) 요청, 요청기관의 담당자 확인, 최소 정보 제공 원칙, 내부 보고 및 승인 절차, 관련 기록 보존 등의 대응

절차 수립·이행

· 제공 과정에서 개인정보가 유·노출되지 않도록 안전한 절차와 방법을 활용하고 개인정보 제공 내역을 기록하여 일정기간 보관 등

증거자료

예시

- 개인정보 목적 외 이용 및 제3자 제공 내역(요청서 등 관련 증거자료 포함)
- 개인정보 목적 외 이용 및 제3자 제공 대장(공공기관인 경우)
- 홈페이지 또는 관보 게재 내역(공공기관인 경우)
- 자료 제공 요청 대응 지침
- 자료 제공 요청 공문 및 개인정보 제공내역, 대장 등

결함사례

- 사례 1 : 상품배송을 목적으로 수집한 개인정보를 사전에 동의 받지 않은 자사 상품의 통신판매 광고에 이용한 경우
- 사례 2 : 고객 만족도 조사, 경품 행사에 응모하기 위하여 수집한 개인정보를 자사의 할인판매행사 안내용 광고 발송에 이용한 경우
- 사례 3 : 공공기관이 다른 법률에 근거하여 민원인의 개인정보를 목적 외로 타 기관에 제공하면서 관련 사항을 관보 또는 인터넷 홈페이지에 게시하지 않은 경우
- 사례 4 : 공공기관이 범죄 수사의 목적으로 경찰서에 개인정보를 제공하면서 '개인정보 목적 외 이용 및 제3자 제공 대장'에 관련 사항을 기록하지 않은 경우

항 목	3.2.5 가명정보 처리
인증기준	가명정보를 처리하는 경우 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행하여야 한다.
주요 확인사항	• 가명정보를 처리하는 경우 목적 제한, 가명처리 방법 및 기준, 적정성 검토, 재식별 금지 및 재식별 발생 시 조치사항 등 가명정보를 적정하게 처리하기 위한 절차를 수립하고 있는가? • 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이는 개인을 알아볼 수 없도록 적정한 수준으로 가명처리를 수행하고 있는가? • 다른 개인정보처리자와 가명정보를 결합하는 경우 결합전문기관 또는 데이터전문기관을 통해 결합하고 있는가? • 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리, 관련 기록의 작성·보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하고 있는가? • 가명정보 처리목적 등을 고려하여 가명정보의 처리 기간을 적정한 기간으로 정하고 있으며, 해당 기간이 경과한 경우 지체 없이 파기하고 있는가? • 개인정보를 익명처리하는 경우 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 특정 개인을 알아볼 수 없도록 적정한 수준으로 익명처리하고 있는가?
관련 법규	• 개인정보 보호법 제2조(정의), 제28조의2(가명정보의 처리 등), 제28조의3(가명정보의 결합 제한), 제28조의4(가명정보에 대한 안전조치의무 등), 제28조의5(가명정보 처리 시 금지의무 등), 제28조의7(적용범위), 제58조의2(적용제외)

세부 설명

■ 가명정보를 처리하는 경우 목적 제한, 가명처리 방법 및 기준, 적정성 검토, 재식별 금지 및 재식별 발생 시 조치사항 등 가명정보를 적정하게 처리하기 위한 절차를 수립·이행하여야 한다.

- ▶ '가명처리'란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말함
- ▶ '가명정보'란 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보로서 개인정보의 범주에 포함됨
- ▶ 가명정보는 가명정보 처리에 관한 특례에 따라 통계작성, 과학적 연구, 공익적 기록보존 등 3가지 목적에 대하여 정보주체의 동의 없이 이용·제공 등 처리 가능
- ▶ 가명정보 처리에 관한 특례에 따라 정보주체의 동의 없이 처리가 가능한 가명정보는 통계작성, 과학적 연구, 공익적 기록보존 등 목적에 한정되므로 처리 목적이 설정되지 않은 상황에서 보유하고 있는 개인정보를 가명처리하여 보관하는 것은 가명정보 처리에 관한 특례에 근거한 처리로 볼 수 없음
- ▶ 처리 목적 및 이용환경, 데이터 특성 등을 고려하여 적정한 수준으로의 가명처리를 보장하기 위한 가명처리 절차 수립 및 이행

▶ 가명처리 절차 예시(가명정보 처리 가이드라인)

단계	구분	설명
1	목적 설정 등 사전준비	• 개인정보 보호법에서 정한 3가지 목적(통계작성, 과학적 연구, 공익적 기록보존 등) 중에서 가명정보 처리의 목적을 구체적이고 명확하게 설정 • 처리 목적 달성에 필요한 정보의 종류, 범위를 명확히 하여 가명처리 대상을 선정 • 처리 목적의 적합성 검토 • 가명정보 처리를 위한 안전조치 이행(가명정보 처리에 관한 내부 관리계획 수립 등) • 필요 서류 작성 등(가명정보 처리 위탁 시 위탁계약서 작성 등)
2	처리 대상의 위험성 검토	• 가명처리 대상 개인정보파일 및 개인정보항목 선정 • 가명처리 대상 데이터의 위험성 검토 ① 데이터 자체 식별 위험성 : 식별정보, 식별가능정보, 특이정보, 재식별 시 영향도 등 ② 처리 환경 식별 위험성 : 활용 형태(내부 활용, 외부 제공, 외부 결합 등), 처리 장소, 처리 방법
3	가명처리	• 식별 위험성 검토 결과를 기반으로 가명정보의 활용 목적 달성에 필요한 가명처리 방법 및 수준을 정하여 항목별 가명처리 계획 설정 • 항목별 가명처리 계획을 기반으로 가명처리 수행 • 가명처리 과정에서 생성되는 추가 정보는 원칙적으로 파기하고 필요한 경우 가명정보와 분리하여 별도로 저장
4	적정성 검토	• 가명처리에 대해 결과 적정성을 최종 검토 • 가명처리 적정성 검토는 내부 인원을 활용하여 자체적으로 검토하거나, 외부 전문가를 통하여 검토 가능(단, 최소 3명 이상으로 검토위원회를 구성하는 것을 권고) • 적정성 검토 결과 부적정으로 판단될 경우 추가 가명처리 후 다시 적정성 검토 수행
5	안전한 관리	• 사전준비 단계에서 수립한 내부 관리계획에 따라 가명정보에 대한 안전조치 의무 이행(추가정보 분리 보관 또는 삭제, 접근권한 분리 등) • 재식별 금지 및 재식별 가능성 모니터링 • 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기 • 가명정보 처리 관련 기록 작성 및 보관 • 가명정보 처리에 관한 사항을 개인정보 처리방침에 공개 등

▶ 대상 분야에 대한 가명정보 처리 가이드라인이 별도로 존재하는 경우, 해당 가이드라인의 내용을 우선적으로 적용

- 보건의료 데이터 활용 가이드라인(보건복지부), 교육분야 가명·익명정보 처리 가이드라인(교육부), 공공분야 가명정보 제공 실무안내서(행정안전부), 금융분야 가명·익명처리 안내서(금융위원회) 등

■ 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이는 개인을 알아볼 수 없도록 적절한 방법으로 가명처리를 수행하여야 한다.

▶ 개인식별정보는 삭제하거나, 결합 등을 위해 필요한 경우 랜덤값 생성, 해시값 생성 등을 통해 특정

개인을 식별할 수는 없지만 구별은 가능한 값으로 대체

▶ 개인식별가능정보는 가명정보 처리목적 상 반드시 필요하지 않은 경우에는 삭제하고 나머지 개인식별가능정보에 대해서는 처리목적 및 식별 위험성 등을 고려하여 적절한 방법 및 수준으로 가명처리

※ 가명처리·익명처리 방법 예시(가명정보 처리 가이드라인)
· (삭제 기술) 삭제, 부분삭제, 행 항목 삭제, 로컬 삭제, 마스킹
· (통계도구) 총계처리, 부분총계
· (일반화 기술) 일반 라운딩, 랜덤 라운딩, 제어 라운딩, 상하단코딩, 로컬일반화, 범위 방법, 문자데이터 범주화
· (암호화) 양방향 암호화, 일방향 암호화·암호학적 해시함수, 순서보존 암호화, 형태보존 암호화, 동형암호화, 다형성 암호화
· (무작위화 기술) 잡음 추가, 순열(치환), 토근화, (의사)난수생성기
· (기타 기술) 표본추출, 해부화, 합성데이터, 동형비밀분산, 차분프라이버시 등

■ 다른 개인정보처리자와 가명정보를 결합하는 경우 결합전문기관 또는 데이터전문기관을 통해 결합하여야 한다.

▶ 서로 다른 개인정보처리자가 보유한 가명정보를 결합하여 통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 활용하고자 하는 경우에는 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정한 결합전문기관을 통하여 수행

- 결합전문기관 현황 : 가명정보결합종합지원시스템 참고(link.privacy.go.kr)
- 금융회사가 보유한 정보집합물과 결합 시에는 신용정보법에 따른 데이터전문기관을 통하여 수행

▶ 가명정보 결합 절차(가명정보 처리 가이드라인)

단계	구분	설명
1	결합신청	• 결합신청자는 신청자 간 결합신청에 필요한 사항의 협의, 결합신청서 작성 등 가명정보 결합에 필요한 사전 준비사항을 확인하고 결합전문기관에 결합을 신청 • 모의결합, 결합률 확인, 가명정보 추출 등 선택 가능
2	결합 및 추가처리	• 가명정보를 제공하는 결합신청자는 결합키관리기관으로부터 결합키 생성에 이용되는 정보(Salt값)를 수신하여 결합키를 생성하고 결합신청 시 선택한 모의결합, 결합률 확인, 가명정보 추출 등이 완료되면 결합에 필요한 정보를 각 기관에 전송
3	반출 및 활용	• 결합정보 또는 분석결과 등을 반출하려는 경우 결합전문기관에 반출을 신청
4	안전한 관리	• 결합정보를 이용하는 결합신청자는 반출한 결합정보(이하 반출정보)를 당초 결합신청서 및 반출신청서에 기재한 목적에 따라 처리하고 안전조치 의무 등을 준수

■ 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리하고 관련 기록을 작성·보관 등 안전성 확보에 필요한 기술적·관리적·물리적 조치를 하여야 한다.

▶ (관리적 보호조치) 가명정보 및 추가 정보를 안전하게 관리하기 위한 내부 관리계획의 수립·시행, 가명정보 처리업무 수탁자에 대한 관리·감독, 가명정보 처리업무 위탁 및 제3자 제공 시 계약서 상

재식별 금지 등의 조항 포함, 가명정보 처리와 관련된 개인정보 처리방침의 수립 및 공개, 가명정보 보호에 관한 교육 등의 조치

※ 가명정보 처리업무 위탁계약서에 포함되어야 할 사항(예시)

1. 위탁업무 수행 목적 외 처리금지
2. 가명정보의 안전조치 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한
5. 관리·감독에 관한 사항
6. 수탁자가 준수하여야 할 의무 위반시 손해배상 등 책임에 관한 사항
7. 재식별 금지
8. 재식별 위험 발생 시 통지

▶ (기술적 보호조치) 추가 정보의 분리보관 또는 삭제, 가명정보 및 추가 정보에 대한 접근권한의 분리, 가명정보 처리 관련 기록의 작성·보관 등의 조치

★ 가명정보 처리 관련 기록에 포함되어야 할 사항(개인정보 보호법 시행령 제29조의5제2항)

1. 가명정보 처리의 목적
2. 가명처리한 개인정보의 항목
3. 가명정보의 이용내역
4. 제3자 제공 시 제공받는 자
5. 가명정보의 처리 기간(법 제28조의4제2항에 따라 처리 기간을 별도로 정한 경우에 한한다)
6. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

※ 가명정보 처리 관련 기록은 가명정보를 파기한 날로부터 3년 이상 보관

▶ (물리적 보호조치) 가명정보 또는 추가 정보를 전산실이나 자료보관실에 보관하는 경우 비인가자의 접근으로부터 보호하기 위하여 출입 통제 등의 절차 수립·이행 등

▶ (기타 보호조치) 가명정보도 개인정보에 해당되므로 개인정보 보호법 제29조에 따른 개인정보의 안전성 확보조치 기준 이행, 특정 개인을 알아보기 위한 목적으로의 가명처리 금지 등

▶ (재식별 모니터링 등) 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우 즉시 해당 정보의 처리를 중지하고 지체 없이 회수·파기 조치 등

■ 가명정보 처리목적 등을 고려하여 가명정보의 처리 기간을 적정한 기간으로 정하고, 해당 기간이 경과한 경우 지체 없이 파기하여야 한다.

▶ 가명정보의 처리 기간은 가명정보 처리 목적을 달성하기 위해 필요한 기간으로 적정하게 설정

▶ 가명정보의 처리 기간이 경과한 경우 지체 없이 파기

■ 개인정보를 익명처리하는 경우 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 특정 개인을 알아볼 수 없도록 적정한 수준으로 익명처리 하여야 한다.

▶ '익명정보'란 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보를 말함

★ [참고] 개인정보 보호법 제58조의2(적용 예외)
· 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

▶ 익명처리를 하는 경우 개인식별정보는 삭제되어야 하며, 개인식별가능정보는 익명처리 방법을 복합적으로 활용하여 적정한 수준으로 익명처리하여야 함

▶ 익명처리의 적정성을 보장하기 위하여 내·외부 전문가로 구성된 검토위원회 구성 등 익명처리 적정성 검토 절차를 수립하여 이행할 수 있음

증거자료

예시

- 가명처리·익명처리 적정성 평가 절차 및 결과
- 가명정보 처리 기록
- 개인정보 처리방침(가명정보 이용·제공에 관한 사항) 등

결함사례

- 사례 1 : 통계작성 및 과학적 연구를 위하여 정보주체 동의 없이 가명정보를 처리하면서 가명정보 처리에 관한 기록을 남기고 있지 않거나, 또는 개인정보 처리방침에 관련 사항을 공개하지 않은 경우
- 사례 2 : 가명정보와 동일한 데이터베이스 내에 추가 정보를 분리하지 않고 보관하고 있거나, 또는 가명정보와 추가 정보에 대한 접근권한이 적절히 분리되지 않은 경우
- 사례 3 : 개인정보를 가명처리하여 활용하고 있으나 적정한 수준의 가명처리가 수행되지 않아 추가 정보의 사용 없이도 다른 정보와의 결합 등을 통하여 특정 개인을 알아볼 수 있는 가능성이 존재하는 경우
- 사례 4 : 테스트 데이터 생성, 외부 공개 등을 위하여 개인정보를 익명처리하였으나, 특이치 등으로 인하여 특정 개인에 대한 식별가능성이 존재하는 등 익명처리가 적정하게 수행되었다고 보기 어려운 경우

3.3. 개인정보 제공 시 보호조치

항 목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보를 제3자에게 제공하는 경우 정보주체 동의, 법령상 의무준수 등 적법 요건을 명확히 식별하고 이를 준수하고 있는가? • 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 사항을 명확하게 고지하고 다른 동의사항과 구분하여 적법하게 동의를 받고 있는가? • 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 명확히 표시하여 알아보기 쉽게 하고 있는가? • 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는가? • 개인정보를 제3자에게 제공하는 경우 안전한 절차와 방법을 통해 제공하고 제공 내역을 기록하여 보관하고 있는가? • 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제하고 있는가? • 정보주체의 동의 없이 개인정보의 추가적인 제공 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 제공이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보 처리방침에 공개하고 이를 점검하고 있는가?
관련 법규	• 개인정보 보호법 제17조(개인정보의 제공), 제22조(동의를 받는 방법) • 개인정보 처리 방법에 관한 고시

세부 설명

■ 개인정보를 제3자에게 제공하는 경우 정보주체 동의, 법령상 의무준수 등 관련 법률에 따른 적법 요건을 명확히 식별하고 이에 따라 개인정보를 적법하게 제공하여야 한다.

▶ 제3자의 범위

• 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자(동일한 개인정보처리자 내부의 타 부서 및 조직은 제3자에 해당하지 않음)

※ 개인정보의 제3자 제공(예시)
· 개인정보의 저장매체나 개인정보가 담긴 출력물·책자 등을 물리적으로 이전
· 네트워크를 통한 개인정보의 전송
· 개인정보에 대한 제3자의 접근권한 부여
· 개인정보처리자와 제3자의 개인정보 공유
· 기타 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위

▶ 개인정보 제공 경로 별로 개인정보 제공의 적법 요건을 명확히 식별하고, 이를 입증할 수 있도록 관련 근거를 기록·관리

- 예를 들어, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 정보주체 동의 없이 개인정보를 제공하는 경우, 해당 법률 또는 법령의 조항 등 관련 근거를 문서화

▶ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 제3자에게 제공(공유를 포함)할 수 있음

★ 개인정보의 제3자 제공이 가능한 경우(개인정보 보호법 제17조제1항)

1. 정보주체의 동의를 받는 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
5. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
6. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

※ 위의 2호부터 6호까지에 따라 개인정보를 수집한 목적 범위에서 정보주체의 동의 없이 개인정보 제공 가능

■ 개인정보의 제3자 제공 동의는 수집·이용 등에 대한 동의와 구분하여 받고, 제3자 제공이 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 것이 아니라면 이에 동의하지 않는다는 이유로 서비스의 제공을 거부하지 않아야 한다.

★ 동의 사항의 구분이 필요한 경우(개인정보 보호법 제22조제1항)

1. 제15조제1항제1호에 따라 동의를 받는 경우(개인정보 수집·이용 동의)
2. 제17조제1항제1호에 따라 동의를 받는 경우(개인정보 제3자 제공 동의)
3. 제18조제2항제1호에 따라 동의를 받는 경우(개인정보 목적외 이용·제공 동의)
4. 제19조제1호에 따라 동의를 받는 경우(개인정보를 제공받은 자의 목적외 이용·제공 동의)
5. 제24조제1항제1호에 따라 동의를 받는 경우(민감정보 처리 동의)
6. 제24조제1항제1호에 따라 동의를 받는 경우(고유식별정보 처리 동의)
7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우

※ 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 알 수 있도록 구분하여 표시

■ 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 명확히 표시하여 알아보기 쉽게 하여야 한다.

▶ 정보주체로부터 개인정보 제3자 제공 동의를 받을 때에는 5가지의 법정 고지사항을 구체적이고 명확하게 알리고 동의를 받아야 함

★ 개인정보의 제3자 제공 동의 시 고지사항(개인정보 보호법 제17조제2항)

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

▶ 정보주체의 동의가 적법하기 위해서는 정보주체의 자유로운 의사에 따른 동의 여부 결정, 동의 내용의 구체성 및 명확성 등 적법 요건을 모두 충족하여야 함

★ 정보주체의 동의를 받을 때 충족해야 하는 조건(개인정보 보호법 시행령 제17조제1항)

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의를 받으려는 내용이 구체적이고 명확할 것
3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

※ 단, 본 규정은 2024년 9월 15일부터 시행

▶ 개인정보 보호법 제22조(동의를 받는 방법)제2항에 따라 개인정보 처리에 대한 동의를 서면(전자문서 및 전자거래기본법 제2조제1호에 따른 전자문서를 포함)으로 받을 때에는 다음과 같이 중요한 내용을 명확히 표시하여 알아보기 쉽게 하여야 함

★ 명확히 표시하여야 하는 중요한 내용(개인정보 보호법 시행령 제17조제3항)

· 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
· 처리하는 개인정보 항목 중 민감정보, 여권번호, 운전면허번호, 외국인등록번호
· 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
· 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

★ 중요한 내용의 표시 방법(개인정보 처리 방법에 관한 고시 제4조)

· 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
· 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

※ 상세한 내용은 '알기쉬운 개인정보 처리 동의 안내서(개인정보 보호위원회)' 참고

■ 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하여야 한다.

▶ 동의에 근거한 제3자 제공 시 : 동의 시 고지한 제공 목적을 달성하기 위하여 필요한 최소한의 개인정보 항목만 제공하여야 함

▶ 법령에 근거한 제3자 제공 시 : 법률에서 구체적으로 명시하거나 해당 법령상 의무를 준수하기 위하여

필요한 범위 내에서 최소한의 개인정보 항목만 제공하여야 함

■ 제3자에게 개인정보를 제공하는 과정에서 개인정보가 유·노출되지 않도록 안전한 절차와 방법을 통해 제공하고 관련된 제공 내역은 기록하여 보관하여야 한다.

※ 제3자 제공 시 안전한 절차(예시)
· 개인정보를 제공하는 자와 제공받는 자의 안전성 확보에 관한 책임관계 명확화(계약서 등)
· 제3자 제공과 관련된 승인 절차(담당자에 의한 제공 시)
· 전송 또는 전달 과정의 암호화
· 접근통제, 접근권한 관리 등 안전성 확보 조치 적용
· 제공 기록의 보존 등

※ 제3자 제공 기록에 포함하여야 할 내용(예시)
· 제공받는 자
· 제공 일시
· 제공된 개인정보 : 정보주체 식별정보 및 개인정보 항목
· 제공 목적 또는 근거
· 제공자(담당자) : 승인절차가 있는 경우 승인자 포함
· 제공 방법 : 시스템 연계, 이메일 전송 등
· 기타 필요한 정보

■ 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제하여야 한다.

- ▶ 권한이 있는 자만 접근할 수 있도록 안전한 인증 및 접근통제 조치
- ▶ 전송구간에서의 도청을 방지하기 위한 암호화 조치
- ▶ 책임추적성을 확보할 수 있도록 접속기록 보존 등

■ 정보주체의 동의 없이 개인정보의 추가적인 제공 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등 고려사항에 대한 판단기준을 수립·이행하여야 하며, 추가적인 제공이 지속적으로 발생하는 경우 이를 개인정보 처리방침에 공개하고 기준 준수여부를 점검하여야 한다.

★ 개인정보의 추가적인 제공 시 고려사항(개인정보 보호법 시행령 제14조의2제1항)
1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

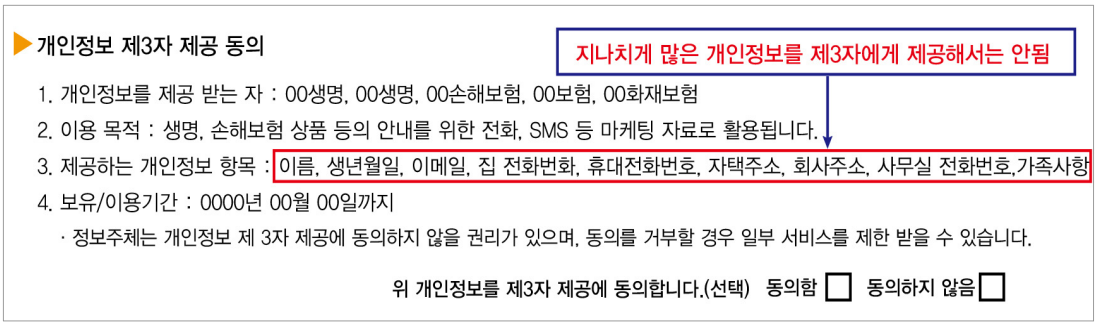
증거자료

예시

- 온라인 개인정보 제3자 제공 관련 양식(홈페이지 회원가입 화면, 개인정보 제3자 제공 동의 화면 등)
- 오프라인 개인정보 제3자 제공 관련 양식(회원가입신청서, 개인정보 제3자 제공 동의서 등)
- 제3자 제공 내역
- 개인정보 처리방침

결함사례

- 사례 1 : 개인정보처리자가 개인정보 제3자 제공 동의를 받을 때 정보주체에게 고지하는 사항 중에 일부 사항(동의 거부권, 제공하는 항목 등)을 누락한 경우
- 사례 2 : 개인정보를 제3자에게 제공하는 과정에서 제3자 제공 동의 여부를 적절히 확인하지 못하여 동의하지 않은 정보주체의 개인정보가 함께 제공된 경우
- 사례 3 : 개인정보를 제공 동의를 받을 때, 제공받는 자를 특정하지 않고 '~ 등'과 같이 포괄적으로 안내하고 동의를 받은 경우
- 사례 4 : 회원 가입 단계에서 선택사항으로 제3자 제공 동의를 받고 있으나, 제3자 제공에 동의하지 않으면 회원 가입 절차가 더 이상 진행되지 않도록 되어 있는 경우
- 사례 5 : 제공받는 자의 이용 목적과 관련 없이 지나치게 많은 개인정보를 제공하는 경우



항 목	3.3.2 개인정보 처리 업무 위탁
인증기준	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 공개하여야 한다. 또한 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.
주요 확인사항	• 개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는가? • 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리고 있는가?
관련 법규	• 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)

세부 설명

■ 개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 정보주체가 언제든지 쉽게 확인할 수 있도록 지속적으로 공개하여야 한다.

▶ 정보주체에게 알려야 할 사항

1. 위탁하는 업무의 내용
2. 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)

※ '수탁자'는 개인정보 처리 업무를 위탁받아 처리하는 자로부터 위탁받은 업무를 다시 위탁받은 제3자(재수탁자)를 포함

▶ 개인정보 처리업무 위탁 사항 공개 방법(개인정보 보호법 시행령 제28조제2항 및 제3항)

- 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법
- 인터넷 홈페이지에 게재할 수 없는 경우 공개 방법(다음 방법 중 하나 이상의 방법 활용)

1. 위탁자의 사업장 등 보기 쉬운 장소에 게시하는 방법
2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
4. 재화나 서비스를 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

▶ 주의사항

- 수탁자의 수가 많을지라도 해당 수탁자명을 모두 열거하여 공개 필요
- 재위탁이 존재하는 경우 재위탁에 관한 사항도 함께 공개 필요

- 위탁하는 업무의 내용 또는 수탁자가 변경된 경우 지체 없이 변경된 내용을 반영하여 인터넷 홈페이지 등을 통하여 공개 필요

■ 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.

▶ 통지방법 : 서면등의 방법(서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법)

▶ 통지사항 : 위탁하는 업무의 내용, 수탁자

※ 개인정보 처리업무의 위탁과 관련된 위탁 계약, 재위탁 시 위탁자 동의, 수탁자 관리·감독 등에 관한 사항은 2.3(외부자 보안) 분야 인증기준 참고

증거자료

예시

- 개인정보 처리방침(개인정보 처리업무 위탁 관련 공개 내역)
- 개인정보 수집 양식
- 개인정보 처리 위탁 계약서
- 재화 또는 서비스 홍보·판매 권유 업무 위탁 관련 정보주체 통지 내역

결함사례

- 사례 1 : 홈페이지 개인정보 처리방침에 개인정보 처리업무 위탁 사항을 공개하고 있으나, 일부 수탁자와 위탁하는 업무의 내용이 누락된 경우
- 사례 2 : 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하면서, 위탁하는 업무의 내용과 수탁자를 서면등의 방법으로 정보주체에게 알리지 않고 개인정보 처리방침에 공개하는 것으로 갈음한 경우
- 사례 3 : 기존 개인정보 처리업무 수탁자와의 계약 해지에 따라 개인정보 처리업무 수탁자가 변경되었으나, 이에 대하여 개인정보 처리방침에 지체 없이 반영하지 않은 경우
- 사례 4 : 개인정보 처리업무를 위탁받은 자가 해당 업무를 제3자에게 재위탁을 하고 있지만, 재위탁에 관한 사항을 인터넷 홈페이지 등에 공개하고 있지 않은 경우

항 목	3.3.3 영업의 양도 등에 따른 개인정보 이전
인증기준	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	• 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 필요한 사항을 사전에 정보주체에게 알리고 있는가? • 개인정보를 이전받는 자는 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실 등 필요한 사항을 정보주체에게 지체 없이 알리고 있는가? • 개인정보를 이전받는 자는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공하고 있는가?
관련 법규	• 개인정보 보호법 제27조(영업양도 등에 따른 개인정보의 이전 제한)

세부 설명

■ 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 다음 사항을 사전에 정보주체에게 알려야 한다.

▶ 알려야 할 사항

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자의 이름, 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 않는 경우 조치할 수 있는 방법 및 절차

▶ 알리는 방법

1. 전자우편·서면·팩스·전화 또는 이와 유사한 방법 중 어느 하나의 방법
2. 과실 없이 정보주체의 연락처를 알 수 없는 등의 이유로 정보주체에게 직접 알릴 수 없는 경우에는 인터넷 홈페이지에 30일 이상 기재
   · 다만, 인터넷 홈페이지를 운영하지 않는 양도자 등의 경우 사업장 등의 보기 쉬운 장소에 30일 이상 게시
   · 또는, 영업양도자등의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문·일반주간신문 또는 인터넷신문에 싣는 방법 활용

■ 영업양수자 등은 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실 등 필요한 사항을 정보주체에게 지체 없이 알려야 한다.

▶ 양도자가 이전 사실을 정보주체에게 알린 경우 양수자는 추가로 알리지 않아도 됨

▶ 다만 영업 양수 등에 따라 개인정보를 이전받았으나 개인정보를 이전하는 자가 이전한 사실을 알리지 않은 경우, 이전 사실을 정보주체에게 알려야 함

■ 개인정보를 이전받는 자는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공하여야 한다.

▶ 개인정보를 이전받은 자가 당초의 목적 범위 외로 개인정보를 이용하거나 제공하고자 하는 경우에는 별도로 정보주체의 동의를 받아야 함

증거자료

예시

- 개인정보 이전 관련 정보주체 고지 내역(영업 양수도 시)
- 개인정보 처리방침

결함사례

- 사례 1 : 개인정보처리자가 영업 양수를 통하여 개인정보를 이전받으면서 양도자가 개인정보 이전 사실을 알리지 않았음에도 개인정보 이전 사실을 정보주체에게 알리지 않은 경우
- 사례 2 : 영업 양수도 등에 의하여 개인정보를 이전받으면서 정보주체가 이전을 원하지 않은 경우 조치할 수 있는 방법과 절차를 마련하지 않거나, 이를 정보주체에게 알리지 않은 경우

항 목	3.3.4 개인정보 국외이전
인증기준	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	• 개인정보를 국외로 이전하는 경우 정보주체에게 국외 이전에 관한 고지 사항을 모두 알리고 별도 동의를 받거나, 인증 또는 인정 등 적법 요건을 준수하고 있는가? • 정보주체와의 계약의 체결 및 이행을 위한 개인정보의 국외 처리위탁·보관에 대해 정보주체에게 알리는 경우 필요한 사항을 모두 포함하여 적절한 방법으로 알리고 있는가? • 개인정보 보호 관련 법령 준수 및 개인정보 보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 있는가? • 개인정보를 국외로 이전하는 경우 개인정보 보호를 위하여 필요한 조치를 취하고 있는가?
관련 법규	• 개인정보 보호법 제28조의8(개인정보의 국외 이전), 제28조의9(개인정보의 국외 이전 중지 명령), 제28조의10(상호주의), 제28조의11(준용규정) • 개인정보 국외 이전 운영 등에 관한 규정

세부 설명

■ 개인정보를 국외의 제3자에게 제공(조회되는 경우 포함)·처리위탁·보관(이하 '이전'이라 함)하는 경우 정보주체에게 국외 이전에 관한 고지 사항을 모두 알리고 별도 동의를 받거나, 인증 또는 인정 등 적법 요건을 준수하여야 한다.

▶ 개인정보의 국외 이전이 가능한 경우(개인정보 보호법 제28조의8제1항)

No	구분	설명
1	별도 동의	• 정보주체로부터 국외 이전에 관한 별도의 동의를 받은 경우
2	법률, 조약 등 근거	• 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우
3	개인정보 처리방침 공개 등 (처리위탁·보관)	• 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁·보관이 필요한 경우로서, 관련 사항을 개인정보 처리방침에 공개하거나 전자우편 등으로 정보주체에게 알린 경우
4	인증	• 개인정보 보호 인증(ISMS-P 인증) 등 보호위원회가 정하여 고시하는 인증을 받은 경우로서 다음 각 목의 조치를 모두 한 경우 가. 개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치 나. 인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위하여 필요한 조치
5	대상국등 인정	• 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우

▶ 개인정보의 국외 이전 동의 시 아래 5가지 사항을 모두 알리고 동의를 받아야 함

★ 개인정보의 국외 이전 동의 시 고지사항(개인정보 보호법 제28조의8제2항)
1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 시기 및 방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭과 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간
5. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과

■ 정보주체와의 계약의 체결 및 이행을 위한 개인정보의 국외 처리위탁·보관에 대해 정보주체에게 알리는 경우 필요한 사항을 모두 포함하여 적절한 방법으로 알려야 한다.

▶ 정보주체에게 알리는 방법

1. 개인정보 처리방침에 공개
2. 서면등의 방법(서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법)

▶ 정보주체에게 알려야 할 사항

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 시기 및 방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭과 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간
5. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과

■ 개인정보 보호 관련 법령 준수 및 개인정보 보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하여야 한다.

▶ 다음의 사항에 관하여 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영

1. 개인정보 보호법 시행령 제30조제1항에 따른 개인정보 보호를 위한 안전성 확보 조치
2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치

■ 정보주체의 개인정보를 국외로 이전하는 경우 개인정보 보호를 위하여 필요한 조치를 취하여야 한다.

▶ 개인정보 국외 이전 시 이행하여야 하는 보호조치

1. 개인정보의 국외 이전 관련 개인정보 보호법 규정 준수
2. 개인정보 보호법 제17조부터 제19조까지의 규정 준수
3. 개인정보 보호법 제5장(정보주체의 권리 보장) 규정 준수
4. 개인정보 보호법 시행령 제30조제1항에 따른 개인정보 보호를 위한 안전성 확보 조치
5. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치
6. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치

증거자료

예시

- 개인정보 국외 이전 관련 동의 양식
- 개인정보 국외 이전 관련 계약서
- 개인정보 처리방침
- 개인정보 국외 처리위탁·보관 관련 통지 또는 공개 내역

결함사례

- 사례 1 : 개인정보를 처리하는 과정에서 국외 사업자에게 개인정보 제3자 제공이 발생하였으나, 인증, 대상국 인정 등 동의 예외 요건에 해당되지 않음에도 불구하고 개인정보 국외 이전에 대한 별도 동의를 받지 않은 경우
- 사례 2 : 국외 클라우드 서비스(국외 리전)를 이용하여 개인정보 처리위탁 및 보관을 하면서 이전되는 국가, 이전 방법 등 관련 사항을 개인정보 처리방침에 공개하거나 정보주체에게 알리지 않은 경우
- 사례 3 : 개인정보 국외 이전에 대한 동의를 받으면서 이전받는 자의 명칭(업체명)만 고지하고 이전되는 국가 등에 대하여 알리지 않은 경우

3.4. 개인정보 파기 시 보호조치

항 목	3.4.1 개인정보 파기
인증기준	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
주요 확인사항	• 개인정보의 보유기간 및 파기와 관련된 내부 정책을 수립하고 있는가? • 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하고 있는가? • 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하고 있는가? • 개인정보 파기에 대한 기록을 남기고 관리하고 있는가?
관련 법규	• 개인정보 보호법 제21조(개인정보의 파기) • 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

세부 설명

■ 개인정보의 보유기간 및 파기와 관련된 내부 정책을 다음 사항을 포함하여 수립하여야 한다.

▶ 수집항목별, 수집목적별, 수집경로별로 보관장소(데이터베이스, 백업데이터 등), 파기방법, 파기시점 법령근거 등

▶ 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 하며, 내부 관리계획에 개인정보 파기계획을 포함할 수 있음(표준 개인정보 보호지침 제55조제2항)

■ 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하여야 한다.

▶ 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료, 법령에 따른 보존기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 함

※ 개인정보 수집 및 이용 목적을 달성한 경우(예시)
- 정보주체가 웹사이트 회원에서 탈퇴한 경우
- 정보주체가 초고속인터넷을 해지한 경우
- 정보주체가 마일리지 회원에서 탈퇴를 요청한 경우
- 개인정보를 수집하는 이벤트가 종료된 경우
- 제3의 업체에게 텔레마케팅을 위하여 정보를 제공한 후 해당 업체의 TM업무가 종료된 경우 등

■ 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하여야 한다. 이때 복원이 불가능한 방법이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

- 완전파괴(소각·파쇄 등)
- 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
- 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

※ 파기방법(예시)
- 완전파괴 : 개인정보가 저장된 회원가입신청서 등의 종이문서, 하드디스크나 자기테이프를 파쇄기로 파기하거나 용해, 또는 소각장, 소각로에서 태워서 파기 등
- 전용 소자장비 이용 시 : 디가우저(Degausser)를 이용하여 하드디스크나 자기테이프에 저장된 개인정보 삭제 등
- 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 시 : 개인정보가 저장된 하드디스크에 대하여 완전포맷(3회 이상 권고), 데이터 영역에 무작위 값, 0, 1 등으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등의 방법 이용

- 개인정보의 일부만을 파기하는 경우 위의 방법으로 파기하는 것이 어려울 때에는 다음의 조치 이행

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 전자적 파일 형태 이외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제

- 기술적 특성으로 인하여 위의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리(익명처리)하여 복원이 불가능하도록 조치

■ 개인정보 파기에 대한 기록을 남기고 관리하여야 한다.
- 개인정보 파기의 시행 및 파기 결과의 확인은 개인정보 보호책임자의 책임 하에 수행되어야 하며, 파기에 관한 사항을 기록·관리
- 개인정보 파기에 대한 기록은 파기 관리대장에 기록하거나 파기 내용을 담은 사진 등을 기록물로 보관
- 공공기관은 개인정보파일을 파기하는 경우 파기 결과를 확인하고, 개인정보파일 파기 관리대장을 작성 (표준 개인정보 보호지침 제55조)

증거자료

예시

- 개인정보 보유기간 및 파기 관련 규정
- 개인정보 파기 결과(회원 데이터베이스 등)
- 개인정보 파기관리대장

결함사례

- 사례 1 : 회원 탈퇴 등 목적이 달성되거나 보유기간이 경과된 경우 회원 데이터베이스에서는 해당 개인정보를 파기하였으나, CRM·DW 등 연계된 개인정보처리시스템에 복제되어 저장되어 있는 개인정보를 파기하지 않은 경우
- 사례 2 : 특정 기간 동안 이벤트를 하면서 수집된 개인정보에 대하여 이벤트가 종료된 이후에도 파기 기준이 수립되어 있지 않거나 파기가 이루어지고 있지 않은 경우
- 사례 3 : 콜센터에서 수집되는 민원처리 관련 개인정보(상담이력, 녹취 등)를 전자상거래법을 근거로 3년간 보존하고 있으나, 3년이 경과한 후에도 파기하지 않고 보관하고 있는 경우
- 사례 4 : 블록체인 등 기술적 특성으로 인하여 목적이 달성된 개인정보의 완전 파기가 어려워 완전파기 대신 익명처리를 하였으나, 익명처리가 적절하게 수행되지 않아 일부 개인정보의 재식별 등 복원이 가능한 경우

항 목	3.4.2 처리목적 달성 후 보유 시 조치
인증기준	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.
주요 확인사항	• 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우, 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하도록 관리하고 있는가? • 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하고 있는가? • 분리 보관하고 있는 개인정보에 대하여 법령에서 정한 목적 범위 내에서만 처리 가능하도록 관리하고 있는가? • 분리 보관하고 있는 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하고 있는가?
관련 법규	• 개인정보 보호법 제21조(개인정보의 파기)

세부 설명

■ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하도록 관리하여야 한다.

▶ 개인정보의 항목을 보유목적에 맞는 최소한의 항목으로 제한

▶ 관련 법령에 따른 최소기간으로 보유기간 설정

※ 타 법령에 따른 보유기간(예시)

· 전자상거래 등에서 소비자 보호에 관한 법률

① 표시·광고에 관한 기록 : 6개월

② 계약 또는 청약철회 등에 관한 기록: 5년

③ 대금결제 및 재화 등의 공급에 관한 기록 : 5년

④ 소비자의 불만 또는 분쟁처리에 관한 기록 : 3년

· 통신비밀보호법

컴퓨터 통신 또는 인터넷의 로그기록 자료, 정보통신기기의 위치를 확인할 수 있는 접속지 추적자료 : 3개월

■ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하여야 한다.

▶ 분리 데이터베이스는 물리적 또는 논리적으로 분리하여 구성

■ 분리 보관하고 있는 개인정보에 대하여 법령에서 정한 목적 범위 내에서만 처리 가능하도록 관리하여야 한다.

- 분리 보관된 개인정보는 마케팅 등 다른 목적으로 활용 금지

■ 분리 보관하고 있는 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하여야 한다.

- 분리 데이터베이스의 접속 권한을 최소인원으로 제한하는 등 접근권한 최소화
- 분리 데이터베이스에 대한 접속기록을 남기고 정기적으로 검토 등

증거자료

예시

- 개인정보 보유기간 및 파기 관련 규정
- 분리 데이터베이스 현황(테이블 구조 등)
- 분리 데이터베이스 접근권한 현황

결함사례

- 사례 1 : 탈퇴회원 정보를 파기하지 않고 전자상거래법에 따라 일정기간 보관하면서 Flag값만 변경하여 다른 회원정보와 동일한 테이블에 보관하고 있는 경우
- 사례 2 : 전자상거래법에 따른 소비자 불만 및 분쟁처리에 관한 기록에 대해 관련 법적 요건을 잘못 적용하여 3년이 아닌 5년간 보존하도록 정하고 있는 경우
- 사례 3 : 분리 데이터베이스를 구성하였으나 접근권한을 별도로 설정하지 않아 업무상 접근이 불필요한 인원도 분리 데이터베이스에 자유롭게 접근이 가능한 경우
- 사례 4 : 탈퇴회원 정보를 파기하지 않고 전자상거래법에 따라 계약 또는 청약철회, 대금결제 및 재화 공급에 관한 기록을 분리하여 보존하였으나, 전자상거래법에 따른 보존의무가 없는 선택정보까지 과도하게 보존한 경우

3.5. 정보주체 권리보호

항 목	3.5.1 개인정보 처리방침 공개
인증기준	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 정보주체가 알기 쉽도록 개인정보 처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
주요 확인사항	• 개인정보 처리방침을 법령에서 요구하는 내용을 모두 포함하여 알기 쉬운 용어로 구체적이고 명확하게 작성하였는가? • 개인정보 처리방침을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하고 있는가? • 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고 정보주체가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하고 있는가?
관련 법규	• 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개), 제30조의2(개인정보 처리방침의 평가 및 개선권고)

세부 설명

■ 개인정보 처리방침을 법령에서 요구하는 내용을 모두 포함하여 알기 쉬운 용어로 구체적이고 명확하게 작성하여야 한다.

▶ 개인정보 처리방침에 포함하여야 할 필수 사항(개인정보 보호법 제30조 및 동법 시행령 제31조 참고)

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다.)
4. 개인정보의 파기절차 및 파기방법(법 제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다.)
5. 법 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다.)
6. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다.)
7. 법 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다.)
8. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
9. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
10. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당되는 경우에만 정한다.)
11. 처리하는 개인정보의 항목
12. 시행령 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항

▶ 개인정보 처리방침에 포함하여야 할 기타 사항(표준 개인정보 보호지침 제19조)

1. 법 제28조의8제1항제3호에 따라 개인정보를 처리위탁·보관하기 위하여 국외이전이 필요한 경우 법 제28조의8제2항 각 호의 사항(해당하는 경우에만 정한다)
2. 개인정보 처리방침의 변경에 관한 사항
3. 법 제31조의2제1항에 따라 국내대리인을 지정하는 경우 국내대리인의 성명, 주소, 전화번호 및 전자우편 주소(해당하는 경우에만 정한다)
4. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
5. 개인정보의 열람청구를 접수·처리하는 부서
6. 정보주체의 권익침해에 대한 구제방법

▶ 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개

▶ 개인정보의 처리목적, 처리하는 개인정보의 항목, 제3자 제공에 관한 사항 등 개인정보 처리방침의 내용은 실제 개인정보 처리현황과 일치하여야 하며, 서비스 및 정보주체의 특성 등을 반영하여 알기 쉬운 용어로 구체적이고 명확하게 작성

1. 개인정보 처리 근거, 정보주체의 권리 보장 등 법에서 개인정보 처리방침에 포함하도록 규정하고 있는 사항을 구체적이고 적정하게 수립
2. 개인정보 처리방침을 명확하고 알기 쉬운 언어로 정보주체가 이해하기 쉽게 수립

▶ 개인정보 보호법에 따른 예외사항에 해당되는 경우 개인정보 처리방침을 수립하지 않을 수 있음

★ 개인정보 처리방침 수립이 면제되는 개인정보파일(공공기관)

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄 수사, 공소 제기 및 유지, 형 및 감호 집행, 교정 처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 일회성으로 운영되는 파일 등 지속적으로 관리할 필요가 낮다고 인정되어 대통령령으로 정하는 개인정보파일
   · 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일
   · 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
   · 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

■ 개인정보 처리방침을 정보주체가 쉽게 확인할 수 있도록 접근성을 확보하여 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하여야 한다.

▶ '개인정보 처리방침'이라는 표준화된 명칭을 사용

▶ 인터넷 홈페이지 첫 화면에 공개하는 경우 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 표시

▶ 인터넷 홈페이지를 운영하지 않는 경우에는 법령에서 정한 다른 방법을 통하여 개인정보 처리방침 공개 가능

★ 인터넷 홈페이지에 게재할 수 없는 경우 개인정보 처리방침 공개 방법(시행령 제31조제3항)
- 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
- 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
- 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
- 재화나 서비스를 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

■ 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고, 정보주체가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하여야 한다.

▶ 정보주체가 언제든지 변경된 사항을 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개

※ 개인정보 처리방침의 변경이유 및 내용을 공지하는 방법(예시)
- 인터넷 홈페이지의 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법
- 서면·팩스·전자우편 또는 이와 비슷한 방법으로 정보주체에게 공지하는 방법
- 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하는 방법

증거자료

예시

- 개인정보 처리방침
- 개인정보 처리방침 개정 관련 공지 내역(게시판 등)

결함사례

- 사례 1 : 개인정보 처리방침에 공개되어 있는 개인정보 수집, 제3자 제공 내역이 실제 수집 및 제공하는 내역과 다른 경우
- 사례 2 : 개인정보 보호책임자의 변경, 수탁자 변경 등 개인정보 처리방침 공개 내용 중에 변경사항이 발생하였음에도 이를 반영하여 변경하지 않은 경우
- 사례 3 : 개인정보 처리방침이 공개는 되어 있으나, 명칭이 '개인정보 처리방침'이 아니라 '개인정보 보호정책'으로 되어 있고 글자 크기, 색상 등을 활용하여 정보주체가 쉽게 찾을 수 있도록 되어 있지 않은 경우
- 사례 4 : 개인정보 처리방침이 몇 차례 개정되었으나, 예전에 작성된 개인정보 처리방침의 내용을 확인할 수 있도록 공개되어 있지 않은 경우
- 사례 5 : 전자상거래법, 상법 등 다른 법령에 따라 개인정보를 파기하지 아니하고 일정기간 보관하고 있으나, 이에 따른 보존근거와 보존하는 개인정보 항목을 개인정보 처리방침에 공개하지 않은 경우

항 목	3.5.2 정보주체 권리보장
인증기준	정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 등 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제요청, 임시조치 등의 기준을 수립·이행하여야 한다.
주요 확인사항	• 정보주체 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지 및 동의 철회 등(이하 '열람등요구'라 함)을 개인정보 수집방법·절차보다 어렵지 아니하도록 권리 행사 방법 및 절차를 마련하여 공개하고 있는가? • 정보주체 또는 그 대리인이 개인정보 열람등요구를 하는 경우 기간 내에 열람등요구에 따른 필요한 조치를 하고 있는가? • 정보주체 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하고 있는가? • 정보주체의 열람등요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는가? • 정보주체의 열람등요구 및 처리 결과에 대하여 기록을 남기고 있는가? • 정보통신망에서 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한 경우 침해를 받은 자가 정보통신서비스 제공자에게 정보의 삭제 요청 등을 할 수 있는 절차를 마련하여 시행하고 있는가?
관련 법규	• 개인정보 보호법 제34조의2(노출된 개인정보의 삭제·차단), 제35조(개인정보의 열람), 제35조의2(개인정보의 전송 요구), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등), 제37조의2(자동화된 결정에 대한 정보주체의 권리 등), 제38조(권리행사의 방법 및 절차) • 정보통신망법 제44조(정보통신망에서의 권리보호), 제44조의2(정보의 삭제요청 등), 제44조의3(임의의 임시조치)

세부 설명

■ 정보주체 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지 및 동의 철회 등(이하 '열람등요구'라 함)을 개인정보 수집방법·절차보다 어렵지 아니하도록 권리 행사 방법 및 절차를 마련하고 공개하여야 한다.

▶ 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 쉽게 알 수 있도록 공개하여야 함

▶ 정보주체의 권리행사 방법 및 절차는 최소한 개인정보 수집절차 또는 회원가입 절차 보다 쉽고 편리하여야 하며, 개인정보 수집 시 요구하지 않던 증빙서류를 추가로 요구하지 않아야 함

▶ 정보주체가 편리하게 선택할 수 있도록 가급적 다양한 권리 행사 방법을 마련하여 제공할 필요가 있음 (방문, 서면, 전화, 전자우편, 인터넷 웹사이트 등)

★ 열람 요구·방법 절차 마련 시 준수사항(개인정보 보호법 시행령 제41조제2항)

1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
2. 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일하게 개인정보의 열람을 요구할 수 있도록 할 것
3. 인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것

※ 방법과 절차 마련 시 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 아니하도록 하여야 함

▶ 열람등요구를 한 자가 정보주체 본인이거나 정당한 대리인인지 확인하여야 하며, 확인 방법은 합리적인 수단이라고 객관적으로 인정되는 방식이어야 함(전자서명, 아이핀, 신분증 확인 등)

★ 대리인의 범위(개인정보 보호법 시행령 제45조)

1. 정보주체의 법정대리인
2. 정보주체로부터 위임을 받은 자(정보주체로부터 위임계약 등에 기하여 대리권을 수여받은 임의대리인)

▶ 개인정보처리자가 공공기관인 경우 「전자정부법」에 따른 행정정보의 공동 이용을 통하여 신분확인이 가능하면 행정정보의 공동이용을 통하여 확인하여야 함

▶ 열람등요구를 한 자에게 관련 업무 수행에 필요한 실비의 범위에서 수수료와 우송료를 청구할 수 있으나, 열람등요구를 하게 된 사유가 해당 개인정보처리자에게 있는 경우에는 수수료와 우송료를 청구할 수 없음

■ 정보주체 또는 그 대리인으로부터 개인정보 열람을 요구받은 경우 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 필요한 조치를 하여야 한다.

▶ 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대해 다음 사항의 열람을 요구할 수 있음

★ 열람 요구 사항(개인정보 보호법 시행령 제41조제1항)

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

▶ 10일 이내에 열람할 수 없는 정당한 사유가 있는 경우 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 개인정보 열람을 연기한 후 그 사유가 소멸하였을 경우 연기사유가 소멸된 날로부터 10일 이내에 열람하도록 하여야 함

▶ 개인정보 열람 제한 및 거절의 사유가 있는 경우 정보주체에게 그 사유를 알리고 열람을 제한 또는 거절할 수 있음

★ 정보주체의 열람요구를 제한·거절할 수 있는 사유(개인정보 보호법 제35조제4항)

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
   가. 조세의 부과·징수 또는 환급에 관한 업무
   나. 「초등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
   다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
   라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
   마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

▶ 열람 요구사항 중 일부가 열람 제한 및 거절의 사유가 있는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분에 대해서는 열람할 수 있도록 하여야 함

■ 법적 의무 대상자에 해당하는 경우 정보주체 또는 대리인으로부터 개인정보 전송 요구에 대응하기 위한 절차와 방안을 수립·이행하여야 한다.

▶ 정보주체의 개인정보 전송 요구를 이행해야 할 법적 의무대상자(정보전송자)

구분	법적 의무대상자	비고
정보주체 자신에게로 전송할 것을 요구	• 개인정보 처리 능력을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자	개인정보 보호법 제35조의2제1항
다른 개인정보처리자에게 전송할 것을 요구 (단, 기술적으로 허용되는 합리적인 범위 내)	• 매출액, 개인정보의 보유 규모, 개인정보 처리 능력, 산업별 특성을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자	개인정보 보호법 제35조의2제2항

▶ 전송 요구를 할 수 있는 정보(아래의 요건을 모두 충족하는 개인정보)

No	전송을 요구할 수 있는 정보의 요건
1	정보주체가 전송을 요구하는 정보가 정보주체 본인에 관한 개인정보로서 다음 각 목의 어느 하나에 해당하는 정보일 것 가. 제15조제1항제1호, 제23조제1항제1호 또는 제24조제1항제1호에 따른 동의를 받아 처리되는 개인정보 나. 제15조제1항제4호에 따라 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 처리되는 개인정보 다. 제15조제1항제2호, 같은 항 제3호, 제23조제1항제2호 또는 제24조제1항제2호에 따라 처리되는 개인정보 중 정보주체의 이익이나 공익적 목적을 위하여 관계 중앙행정기관의 장의 요청에 따라 보호위원회가 심의·의결하여 전송 요구의 대상으로 지정한 개인정보
2	전송을 요구하는 개인정보가 개인정보처리자가 수집한 개인정보를 기초로 분석·가공하여 별도로 생성한 정보가 아닐 것
3	전송을 요구하는 개인정보가 컴퓨터 등 정보처리장치로 처리되는 개인정보일 것

▶ 전송 요구에 따른 개인정보를 전송받을 수 있는 개인정보처리자 요건(정보수신자)

No	정보수신자 요건
1	개인정보 보호법 제35조의3제1항에 따른 개인정보관리 전문기관
2	개인정보 보호법 제29조에 따른 안전조치의무를 이행하고 대통령령으로 정하는 시설 및 기술 기준을 충족하는 자

※ 개인정보 전송 요구권과 관련된 개인정보 보호법 제35조의2의 개정 규정은 공포(2023.3.14) 후 1년이 경과한 날부터 공포 후 2년이 넘지 아니하는 범위에서 대통령령으로 정하는 날 시행

■ 정보주체 또는 그 대리인으로부터 개인정보의 정정·삭제를 요구받은 경우 정보주체의 요구가 정당하다고 판단되면 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

▶ 개인정보 정정·삭제 요구를 받은 날부터 10일 이내에 조치 결과 회신

▶ 외부위탁 또는 제3자에게 제공한 개인정보에 대한 정정요청 및 동의 철회 시에는 수탁자 또는 제3자에게 연락하여 조치 요청

▶ 다른 법령에 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 삭제 요구를 거절할 수 있으며, 이 경우 요구에 따르지 않기로 한 사실, 근거 법령의 내용 및 그 이유와 이의제기 방법을 개인정보 정정·삭제 통지서로 해당 정보주체에게 정정·삭제 요구를 받은 날로부터 10일 이내에 알려야 함(전자상거래법에 따른 계약·청약 철회 기록 등)

■ 정보주체 또는 그 대리인으로부터 개인정보의 처리정지 요구를 받은 경우 특별한 사유가 없는 한 지체 없이 처리의 전부 또는 일부를 정지하고 그 결과를 정보주체에게 알려야 한다.

▶ 개인정보 처리정지 요구를 받은 날부터 10일 이내에 조치 결과 회신

▶ 개인정보의 처리정지를 거절할 수 있는 사유가 있는 경우 관련 사실을 처리정지 요구자에게 요구를 받은 날로부터 10일 이내에 알려야 함

★ 처리정지 요구 거부 사유(개인정보 보호법 제37조제2항)

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 않으면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 않으면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 않은 경우

■ 정보주체 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하여야 한다.

※ 정보주체 동의철회 시 조치(예시)

· 해당 정보주체와 관련된 개인정보의 지체 없는 파기

· 다른 법령에 따라 보존의무가 부여된 경우 해당 법령에 따른 기간 동안 분리하여 보관

· 제3자 제공 동의에 대한 철회인 경우 더 이상 제3자에게 개인정보를 제공하지 않도록 조치
· 홍보, 마케팅 등을 위한 문자, 이메일 등이 더 이상 발송되지 않도록 조치 등

■ 정보주체 또는 대리인이 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함)으로 개인정보를 처리하여 이루어지는 결정(이하 '자동화된 결정'이라 함)을 거부하거나 설명 등을 요구한 경우 필요한 조치를 취하여야 한다.

▶ 정보주체는 자동화된 결정을 거부하거나 설명 등을 요구할 권리를 가짐

★ 자동화된 결정에 대한 정보주체의 권리(개인정보 보호법 제37조의2)
① 정보주체는 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 개인정보를 처리하여 이루어지는 결정(「행정기본법」 제20조에 따른 행정청의 자동적 처분은 제외하며, 이하 이 조에서 "자동화된 결정"이라 한다)이 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에는 해당 개인정보처리자에 대하여 해당 결정을 거부할 수 있는 권리를 가진다. 다만, 자동화된 결정이 제15조제1항제1호·제2호 및 제4호에 따라 이루어지는 경우에는 그러하지 아니하다.
② 정보주체는 개인정보처리자가 자동화된 결정을 한 경우에는 그 결정에 대하여 설명 등을 요구할 수 있다.

▶ 정보주체가 자동화된 결정을 거부하거나 이에 대한 설명 등을 요구한 경우에는 정당한 사유가 없는 한 자동화된 결정을 적용하지 아니하거나 인적 개입에 의한 재처리·설명 등 필요한 조치를 이행할 수 있도록 관련 절차를 수립·이행

▶ 자동화된 결정을 하는 경우, 자동화된 결정의 기준과 절차, 개인정보가 처리되는 방식 등을 정보주체가 쉽게 확인할 수 있도록 공개

※ 자동화된 결정에 대한 거부 및 설명 요구 등과 관련된 개인정보 보호법 제37조의2의 개정 규정은 공포 후 1년이 경과한 날부터 시행(2024.3.15. 시행)

■ 정보주체의 열람등요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하여야 한다.

▶ 이 경우 이의제기 절차는 공정하게 운영될 수 있도록 외부전문가를 참여시키거나 내부의 견제장치 마련 필요

■ 정보주체의 열람등요구를 접수하고 처리한 결과에 대하여 기록을 남겨야 한다.

▶ 정보주체의 열람등요구를 접수하고 처리한 결과를 정기적으로 검토하여 정보주체 권리보장이 적절히 이루어지고 있는지 확인하고 필요시 보완 조치

■ 정보통신망에서 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한 경우 침해를 받은 자가 정보통신서비스 제공자에게 정보의 삭제 요청 등을 할 수 있는 절차를 마련하고 시행하여야 하며, 개인정보가 정보통신망을 통하여 공중에 노출되지 않도록 필요한 조치를 하여야 한다.

▶ 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우, 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박 내용의 게재를 요청할 수 있어야 함

▶ 타인의 권리가 침해된 경우 정보통신서비스 제공자가 해당 정보의 삭제 등을 요청받으면 지체 없이 삭제·

임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보 게재자에게 알려야 함

- 타인의 권리가 침해된 경우에 대한 구제절차 등 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 함
- 개인정보처리자는 고유식별정보, 계좌정보, 신용카드정보 등 개인정보가 정보통신망을 통하여 공중(公衆)에 노출되지 아니하도록 하여야 하며, 공중에 노출된 개인정보에 대하여 개인정보 보호위원회 또는 한국인터넷진흥원의 요청이 있는 경우에는 해당 정보를 삭제하거나 차단하는 등 필요한 조치를 하여야 함

증거자료

예시

- 개인정보 처리방침
- 개인정보 열람등요구 처리 절차, 관련 양식
- 개인정보 열람등요구 시 조치 내역
- 회원 탈퇴 및 동의 철회 절차

결함사례

- 사례 1 : 개인정보의 열람, 정정·삭제, 처리정지 요구 방법을 정보주체가 알 수 있도록 공개하지 않은 경우
- 사례 2 : 개인정보의 열람 요구에 대하여 정당한 사유의 통지 없이 열람 요구를 접수받은 날로부터 10일을 초과하여 회신하고 있는 경우
- 사례 3 : 개인정보의 열람 민원에 대한 처리 내역 기록 및 보관이 이루어지지 않은 경우
- 사례 4 : 정보주체 당사자 또는 정당한 대리인이 맞는지에 대한 확인 절차 없이 열람 통지가 이루어지는 경우
- 사례 5 : 개인정보의 정정·삭제 요구에 대하여 정정·삭제 요구를 접수받은 날로부터 10일을 초과하여 회신하는 경우
- 사례 6 : 회원 가입 시에는 온라인을 통하여 쉽게 회원 가입이 가능하였으나, 회원 탈퇴 시에는 신분증 등 추가 서류를 제출하게 하거나 오프라인 방문을 통해서만 가능하도록 하는 경우

항 목	3.5.3 정보주체에 대한 통지
인증기준	개인정보의 이용·제공 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.
주요 확인사항	• 법적 의무 대상자에 해당하는 경우 개인정보 이용·제공 내역 또는 그 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 정보주체에게 주기적으로 통지하고 있는가? • 개인정보 이용·제공 내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?
관련 법규	• 개인정보 보호법 제20조의2(개인정보 이용·제공 내역의 통지)

세부 설명

■ 법적 의무 대상자에 해당하는 경우 개인정보 이용·제공 내역 또는 그 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 정보주체에게 주기적으로 통지하여야 한다.

▶ 개인정보 이용·제공 내역 통지 관련 법적 요구사항

구분	내용
통지 의무 대상자	1. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자 ※ 정보주체의 수는 전년도 말 기준 직전 3개월 간 일일평균을 기준으로 산정(단, 2024년 1월 1일부터 시행)
통지 방법	1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법 2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법(법 제20조의2제1항에 따른 개인정보의 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하는 경우로 한정한다)
통지 주기	• 연 1회 이상
통지 예외	1. 통지에 대한 거부의사를 표시한 정보주체 2. 개인정보처리자가 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리한 경우 해당 정보주체 3. 개인정보처리자가 업무수행을 위해 다른 공공기관, 법인, 단체의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우 해당 정보주체 4. 법률에 특별한 규정이 있거나 법령 상 의무를 준수하기 위하여 이용·제공한 개인정보의 정보주체 5. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 이용·제공한 개인정보의 정보주체 ※ 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집·보유하지 아니한 경우

■ 개인정보 이용·제공 내역 통지 항목 법적 요구항목을 모두 포함하여야 한다.

▶ 개인정보 이용·제공 내역 통지 항목

1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목
2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목(다만 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외)

증거자료

예시

- 개인정보 이용·제공 내역 통지 기록
- 개인정보 이용·제공 내역 통지 양식 및 문구

결함사례

- 사례 1 : 전년도 말 기준 직전 3개월 간 일일 평균 저장·관리하고 있는 개인정보가 100만명 이상으로서 개인정보 이용제공 내역 통지 의무 대상자에 해당 됨에도 불구하고 금년도에 개인정보 이용·내역을 통지하지 않은 경우
- 사례 2 : 개인정보 이용·제공 내역을 개별 정보주체에게 직접적으로 통지하는 대신 홈페이지에서 단순 팝업창이나 별도 공지사항으로 안내만 한 경우

참고자료(가나다 순)

- 가명정보 처리 가이드라인
- 개인정보 보호 가이드라인(온라인 경품행사 편)
- 개인정보 보호 가이드라인(인사·노무 편)
- 개인정보 보호법 표준 해석례
- 개인정보 손해배상책임 보장제도 안내서
- 개인정보 영향평가 수행안내서
- 개인정보 위험도 분석 기준 및 해설서
- 개인정보 처리방침 작성지침(일반)
- 개인정보 처리방침 작성지침(의료기관 및 약국편)
- 개인정보 처리방침 작성지침(학원 및 교습소편)
- 개인정보 처리방침 작성지침(여행업편)
- 개인정보 처리방침 작성지침(공공기관편)
- 개인정보 처리 위·수탁 안내서
- 개인정보보호 법령 및 지침·고시 해설서
- 개인정보보호 자율점검 가이드라인
- 개인정보의 안전성 확보조치 기준 해설서
- 개인정보의 암호화 조치 안내서
- 공공기관 영상정보처리기기 설치·운영 가이드라인
- 금융분야 개인정보보호 가이드라인
- 모바일 대민서비스 보안취약점 점검 가이드
- 무선랜 보안 안내서
- 민간분야 영상정보처리기기 설치·운영 가이드라인
- 보안서버 구축 안내서
- 보조기억매체 이용 안내서

- 분야별 주민등록번호 처리기준 상담사례집
- 불법 스팸 방지를 위한 정보통신망법 안내서
- 상용 소프트웨어에서의 암호기능 이용 안내서
- 생체정보 보호 가이드라인
- 소프트웨어 개발보안 가이드
- 소프트웨어 보안약점 진단 가이드
- 스마트도시 개인정보 보호 가이드라인
- 스마트폰 앱 개인정보보호 가이드라인
- 스마트폰 앱 접근권한 개인정보보호 안내서
- 시스템 개발·운영자를 위한 개인정보보호 가이드라인
- 아동·청소년 개인정보보호 가이드라인
- 알기쉬운 개인정보 처리 동의 안내서
- 암호 알고리즘 및 키 길이 이용 안내서
- 암호이용 안내서
- 암호정책 수립 기준 안내서
- 암호키 관리 안내서
- 영상정보처리기기 운영·관리 방침 예시
- 웹사이트 회원탈퇴 기능구현 안내서
- 인공지능(AI) 개인정보보호 자율점검표
- 정보보호 공시 가이드라인
- 정보보호 최고책임자 지정·신고 제도 안내서
- 주요정보통신시설 기술적 취약점 분석·평가 방법 상세가이드
- 패스워드 선택 및 이용 안내서
- 표준 개인정보 유출사고 대응 매뉴얼
- 홈페이지 개발 보안 안내서
- 홈페이지 개인정보 노출방지 안내서
- i-PIN 2.0 도입 안내서

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서

과학기술정보통신부
개인정보보호위원회
KISA 한국인터넷진흥원