

발 간 등 록 번 호

11-1790365-000038-14

개인정보의 안전성 확보조치 기준 안내서

2024. 10.



개인정보보호위원회

personal Information Protection Commission

발 간 등 록 번 호
11-1790365-000038-14

개인정보의 안전성 확보조치 기준 안내서

2024. 10.



개인정보보호위원회

personal Information Protection Commission

개인정보의 안전성 확보조치 기준 안내서

안내 사항

발간 목적

본 안내서는 「개인정보 보호법」과 「개인정보의 안전성 확보조치 기준」 등에 따라 개인정보처리자가 조치하여야 하는 최소한의 안전성 확보 기준을 안내하고 있습니다. 개인정보처리자는 본 안내서의 보호조치 이외에 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하여 필요하다면 추가적인 보호조치를 적용하시기 바랍니다.

제·개정 이력

개인정보보호 관련 법·제도 및 환경 변화를 반영하여 다음과 같이 개정하였습니다.

일자	주요 내용
'24. 10. 발간	개인정보 보호법 및 시행령 개정('23.9.)에 따른 '개인정보의 안전성 확보조치 기준 안내서' 통합본 발간

재검토 기한

안내서의 최신성을 유지하기 위해 발간일(2024년 10월)을 기준으로 매 3년이 되는 시점(매 3년째의 12.31.까지를 말함)마다 보완 및 개선 등의 조치를 취할 예정입니다.

저작권 표시

본 안내서 내용의 무단전재를 금하며, 가공·인용할 때는 출처를 밝혀 주시기 바랍니다.

* 출처 : 개인정보보호위원회, 「개인정보의 안전성 확보조치 기준 안내서」 2024.10.

문의처

본 안내서 내용 관련 문의는 개인정보보호위원회 신기술개인정보과(☎02-2100-3067, 3028)로, 개인정보보호 법령 질의 등에 관한 사항은 개인정보보호위원회 법령해석 지원센터(☎02-2100-3043)로 문의주시기 바랍니다.

관계법령

「개인정보 보호법」 제29조 및 같은 법 시행령 제16조제2항, 제30조, 제30조의2 등

※ 법령 최신 자료는 국가법령정보센터(www.law.go.kr), 개인정보 보호 안내서 최신 자료는 개인정보보호위원회 누리집*, 개인정보 포털**을 참고

* 개인정보보호위원회 누리집(www.pipc.go.kr) : 법령 > 법령정보 > 안내서

** 개인정보 포털(www.privacy.go.kr) : 자료 > 자료보기 > 안내서



I

「개인정보의 안전성 확보조치 기준」 개요 _1

1. 개요	2
2. 법적 근거	3

II

「개인정보의 안전성 확보조치 기준」 전문_7

III

「개인정보의 안전성 확보조치 기준」 해설_19

제1장 총칙	21
[제1조] 목적	21
[제2조] 정의	26
제2장 개인정보의 안전성 확보조치	35
[제3조] 안전조치의 적용 원칙	35
[제4조] 내부 관리계획의 수립·시행 및 점검	36
[제5조] 접근 권한의 관리	59
[제6조] 접근통제	66
[제7조] 개인정보의 암호화	78
[제8조] 접속기록의 보관 및 점검	88
[제9조] 악성프로그램 등 방지	93

[제10조] 물리적 안전조치	97
[제11조] 재해·재난 대비 안전조치	100
[제12조] 출력·복사시 안전조치	103
[제13조] 개인정보의 파기	105

제3장 공공시스템운영기관 등의 개인정보 안전성

확보조치	109
[제14조] 공공시스템운영기관의 안전조치 기준 적용	109
[제15조] 공공시스템운영기관의 내부 관리계획의 수립·시행	113
[제16조] 공공시스템운영기관의 접근 권한의 관리	119
[제17조] 공공시스템운영기관의 접속기록의 보관 및 점검	125
[제18조] 재검토 기한	129
[부칙]	129

IV

부록_131

제1장 자주 묻는 질문과 답변	132
제2장 인터넷망 차단 조치 해설	161
제3장 개인정보 위험도 분석 기준 해설	175
제4장 암호화 조치 관련 참고 웹사이트	201

개인정보의 안전성
확보조치 기준 안내서





「개인정보의 안전성 확보조치 기준」 개요

1. 개요
2. 법적 근거

I

「개인정보의 안전성 확보조치 기준」
개요

1 | 개요

구 분	「개인정보의 안전성 확보조치 기준」
법적 근거	<ul style="list-style-type: none"> • 개인정보 보호법 제29조(안전조치의무) • 개인정보 보호법 시행령 제16조제2항(개인정보의 파기방법), 제30조(개인정보의 안전성 확보 조치), 제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등)
적용 대상	<ul style="list-style-type: none"> • 개인정보처리자 • 개인정보처리자로부터 개인정보를 제공받은 자 • 개인정보처리자로부터 개인정보 처리를 위탁받은 자(이하 '수탁자', 준용)
목 적	<ul style="list-style-type: none"> • 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정함
성 격	<ul style="list-style-type: none"> • 반드시 준수해야 하는 최소한의 기준
주요 내용	<ul style="list-style-type: none"> • 내부 관리계획의 수립·시행 • 접근 권한의 관리 • 접근통제 • 개인정보의 암호화 • 접속기록의 보관 및 점검 • 악성프로그램 등 방지 • 물리적 안전조치 • 출력·복사시 안전조치 • 재해·재난 대비 안전조치 • 개인정보의 파기 • 공공시스템운영기관의 안전조치 기준 적용 • 공공시스템운영기관의 접근 권한의 관리 • 공공시스템운영기관의 접속기록의 보관 및 점검 등
과징금 및 과태료	<ul style="list-style-type: none"> • 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금(법 제64조의2제1항제9호) • 3천만원 이하의 과태료(법 제75조제2항제5호)

2 법적 근거

- 이 기준은 「개인정보 보호법」 제29조 및 같은 법 시행령 제16조제2항, 제30조, 제30조의 2에 근거한다.
- 따라서, 개인정보처리자는 개인정보를 처리할 때 이 기준을 준수하여야 한다.
- 이 기준에 따른 안전성 확보조치를 하지 아니한 자 등에게는 관련 법률에 따라 과징금, 과태료를 부과할 수 있다.

「개인정보 보호법」

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

제64조의2(과징금의 부과) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보 처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

9. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

「개인정보 보호법 시행령」

제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 해야 한다.

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제. 다만, 기술적 특성으로 영구 삭제가 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치해야 한다.
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 보호위원회가 정하여 고시한다.

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검
가. 법 제28조제1항에 따른 개인정보취급자(이하 “개인정보취급자”라 한다)에 대한 관리·감독 및 교육에 관한 사항
나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항
다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항
 2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치
가. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템(이하 “개인정보 처리시스템”이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행
나. 정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영
다. 그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치
 3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치
가. 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치
나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항 제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.
다. 그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치
 4. 개인정보를 안전하게 저장·전송하는데 필요한 다음 각 목의 조치
가. 비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치
나. 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치
다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 통하여 정보주체의 개인정보 또는 인증정보를 송신·수신하는 경우 해당 정보의 암호화 또는 이에 상응하는 조치
라. 그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치
 5. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 다음 각 목의 조치
가. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독
나. 개인정보처리시스템에 대한 접속기록의 안전한 보관
다. 그 밖에 접속기록 보관 및 위조·변조 방지를 위하여 필요한 조치
 6. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치
 7. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치
 8. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치
- ② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.
- ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) ① 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는기준에 해당하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은법 제29조에 따라 이영 제30조의 안전성 확보 조치 외에 다음 각 호의 조치를 추가로 해야 한다.

1. 제30조 제1항 제1호에 따른 내부 관리계획에 공공시스템별로 작성한 안전성 확보 조치를 포함할 것
2. 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 이 조에서 “공공시스템이용기관”이라 한다)이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치
3. 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치

② 공공시스템운영기관 및 공공시스템이용기관은 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우에는 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지해야한다. 이 경우 다음 각 호의 어느 하나에 해당하는 경우에는 통지를 한 것으로 본다.

1. 법 제34조 제1항에 따라 정보주체에게 개인정보의 분실·도난·유출에 대하여 통지한 경우
2. 다른 법령에 따라 정보주체에게 개인정보에 접근한 사실과 피해 예방 등을 위해 필요한 사항을 통지한 경우

③ 공공시스템운영기관(공공시스템을 개발하여 배포하는 공공기관이 따로 있는 경우에는 그 공공기관을 포함한다. 이하 이 조에서 같다)은 해당 공공시스템의 규모와 특성, 해당 공공시스템이용기관의 수 등을 고려하여 개인정보의 안전한 관리에 관련된 업무를 전담하는 부서를 지정하여 운영하거나 전담인력을 배치해야 한다.

④ 공공시스템운영기관은 공공시스템별로 해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정해야 한다. 다만, 해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 업무 관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 관리책임자를 지정해야 한다.

⑤ 공공시스템운영기관은 공공시스템의 안전성 확보 조치 이행상황 점검 및 개선에 관한 사항을 협의하기 위하여 다음 각 호의 기관으로 구성되는 공공시스템운영협의회를 공공시스템별로 설치·운영해야 한다. 다만, 하나의 공공기관이 2개 이상의 공공시스템을 운영하는 경우에는 공공시스템운영협의회를 통합하여 설치·운영할 수 있다.

1. 공공시스템운영기관
2. 공공시스템의 운영을 위탁하는 경우 해당 수탁자
3. 공공시스템운영기관이 필요하다고 인정하는 공공시스템이용기관

⑥ 보호위원회는 공공시스템운영기관이 개인정보의 안전성 확보 조치를 이행하는데 필요한 지원을 할 수 있다.

⑦ 제1항부터 제6항까지에서 규정한 사항 외에 공공시스템운영기관 등의 개인정보의 안전성 확보 조치에 필요한 사항은보호위원회가 정하여 고시한다.

개인정보의 안전성
확보조치 기준 안내서





「개인정보의 안전성 확보조치 기준」 전문

II

「개인정보의 안전성 확보조치 기준」 전문

[일부개정 2023. 9. 22. 개인정보보호위원회 고시 제2023-6호]

■ 개인정보의 안전성 확보조치 기준

제1장 총칙

제1조(목적) 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제29조와 같은 법 시행령(이하 “영”이라 한다) 제16조제2항, 제30조 및 제30조의2에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
2. “이용자”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
3. “접속기록”이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신 가능한 상태를 말한다.

4. “정보통신망”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항 제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신 설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
5. “P2P(Peer to Peer)”란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
6. “공유설정”이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
7. “모바일 기기”란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
8. “비밀번호”란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
9. “생체정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
10. “생체인식정보”란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
11. “인증정보”란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.
12. “내부망”이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
13. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
14. “보조저장매체”란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장매체를 말한다.

제2장 개인정보의 안전성 확보조치

제3조(안전조치의 적용 원칙) 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.

제4조(내부 관리계획의 수립·시행 및 점검) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

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

② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상

2. 교육 내용

3. 교육 일정 및 방법

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리 하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.

② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.

⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리 시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

- ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리 시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리 시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.
- ③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.
- ④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.
- ⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
- ⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.

제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호

6. 계좌번호

7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

- ② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.
- ③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

제9조(악성프로그램 등 방지) ① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
 2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
- ② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

제10조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

- ② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
- ③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제11조(재해·재난 대비 안전조치) 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.

1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검
2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련

제12조(출력·복사시 안전조치) ① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)

2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제

3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제

③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

제3장 공공시스템운영기관 등의 개인정보 안전성 확보조치

제14조(공공시스템운영기관의 안전조치 기준 적용) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 “보호위원회”라 한다)가 지정하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템 운영기관”이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.

1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우

- 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
 - 다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템
2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
 3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
 - 다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템
 - 라. 총 사업비가 100억원 이상인 시스템
- ② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리 시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.
1. 체계적인 개인정보 검색이 어려운 경우
 2. 내부적 업무처리만을 위하여 사용되는 경우
 3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우

제15조(공공시스템운영기관의 내부 관리계획의 수립·시행) 공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.

1. 영 제30조의2제4항에 따른 관리책임자(이하 “관리책임자”라 한다)의 지정에 관한 사항
2. 관리책임자의 역할 및 책임에 관한 사항
3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항
4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항
5. 제16조 및 제17조에 관한 사항

제16조(공공시스템운영기관의 접근 권한의 관리) ① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.

② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조제3항에 따른 내역에 포함하여야 한다.

③ 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.

④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.

⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 “공공시스템이용기관”이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.

제17조(공공시스템운영기관의 접속기록의 보관 및 점검) ① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.

② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

제18조(재검토 기한) 개인정보보호위원회는 「행정규제기본법」 제8조 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-6호, 2023. 9. 22.>

이 고시는 발령한 날부터 시행한다. 다만, 다음 각 호의 개정규정은 각 호의 구분에 해당하는 개인정보처리자에 대해서는 2024년 9월 15일부터 시행한다.

1. 제5조제6항, 제7조제6항, 제8조제2항, 제11조의 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회고시 제2021-3호) 적용대상인 개인정보처리자

2. 제7조제4항, 제12조제2항의 개정규정 및 제5조제6항 중 정보주체에 관한 개정규정 :
총전의 「(개인정보보호위원회) 개인정보의 안전성 확보조치 기준」(개인정보보호
위원회고시 제2021-2호) 적용대상인 개인정보처리자
3. 제14조부터 제17조까지의 개정규정 : 공공시스템운영기관과 공공시스템이용기관



「개인정보의 안전성 확보조치 기준」 해설

제1장 총칙

제2장 개인정보의 안전성 확보조치

제3장 공공시스템운영기관 등의 개인정보 안전성
확보조치



「개인정보의 안전성 확보조치 기준」 해설

제1장 총칙

[제1조] 목적

[제2조] 정의

제2장 개인정보의 안전성 확보조치

[제3조] 안전조치의 적용 원칙

[제4조] 내부 관리계획의 수립·시행 및 점검

[제5조] 접근 권한의 관리

[제6조] 접근통제

[제7조] 개인정보의 암호화

[제8조] 접속기록의 보관 및 점검

[제9조] 악성프로그램 등 방지

[제10조] 물리적 안전조치

[제11조] 재해·재난 대비 안전조치

[제12조] 출력·복사시 안전조치

[제13조] 개인정보의 파기

제3장 공공시스템운영기관 등의 개인정보 안전성 확보조치

[제14조] 공공시스템운영기관의 안전조치 기준 적용

[제15조] 공공시스템운영기관의 내부 관리계획의 수립·시행

[제16조] 공공시스템운영기관의 접근 권한의 관리

[제17조] 공공시스템운영기관의 접속기록의 보관 및 점검

[제18조] 재검토기한

[부칙]

제1장 총칙

제1조 목적

제1조(목적) 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제29조와 같은 법 시행령(이하 “영”이라 한다) 제16조제2항, 제30조 및 제30조의2에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.



해설

- 이 기준의 해설은 「개인정보 보호법」 제29조(안전조치의무)와 같은 법 시행령 제16조제2항 (개인정보의 파기방법), 제30조(개인정보의 안전성 확보 조치), 제30조의2 (공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등)에 근거한다.
 - 이 외에, 다른 법률에서 「개인정보 보호법」(이하 “법”이라 한다)의 관련 규정을 준용할 것을 명시하는 경우에도 이 기준이 적용된다.
- 이 기준은 개인정보처리자에게 적용된다. 법 제2조제5호에 따르면 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
- 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치를 하여야 한다.
 - 특히, 개인정보처리자 중 공공시스템을 운영하는 공공시스템운영기관은 영 제30조의 2 및 이 기준 제2장(제3조~제13조)에서 정하는 안전성 확보에 필요한 조치 외에 제3장(제14조~제17조)에서 정한 안전성 확보에 필요한 안전조치를 추가적으로 이행하여야 한다.

「개인정보 보호법」

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보 보호법 시행령」

제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 해야 한다.

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제. 다만, 기술적 특성으로 영구 삭제가 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치해야 한다.
 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각
- ② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 보호위원회가 정하여 고시한다.

- 개인정보처리자가 개인의 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등 정보주체의 사생활을 현저히 침해할 우려가 있는 민감정보 및 개인을 고유하게 구별하기 위하여 부여된 고유식별정보를 처리하는 경우, 법 제23조(민감정보의 처리 제한)제2항, 제24조(고유식별정보의 처리 제한)제3항, 제24조의 2(주민등록번호 처리의 제한)제2항 및 같은 법 시행령 제21조(고유식별정보의 안전성 확보조치), 제21조의2(주민등록번호 암호화 적용 대상 등)제3항에 따라 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 조치를 하여야 한다.

「개인정보 보호법」

제23조(민감정보의 처리 제한) ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

제24조(고유식별정보의 처리 제한) ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

제24조의 2(주민등록번호 처리의 제한) ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

「개인정보 보호법 시행령」

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 “법 제29조”는 “법 제24조제3항”으로, “개인정보”는 “고유식별정보”로 본다.

② 법 제24조제4항에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 1만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 공공기관
2. 보호위원회가 법 위반 이력 및 내용·정도, 고유식별정보 처리의 위험성 등을 고려하여 법 제24조제4항에 따른 조사가 필요하다고 인정하는 공공기관
3. 공공기관 외의 자로서 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자

③ 보호위원회는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 3년마다 1회 이상 조사해야 한다.

④ 다음 각 호의 어느 하나에 해당하는 경우로서 고유식별정보의 안전성 확보 조치에 대한 점검이 이루어진 경우에는 제3항에 따른 조사를 실시한 것으로 본다.

1. 법 제11조의2에 따라 개인정보 보호수준 평가를 받은 경우
2. 법 제32조의2에 따라 개인정보 보호 인증을 받은 경우
3. 「신용정보의 이용 및 보호에 관한 법률」 제45조의5에 따른 개인정보 신용정보 활용·관리 실태에 대한 상시평가 등 다른 법률에 따라 고유식별정보의 안전성 확보 조치 이행 여부에 대한 정기적인 점검이 이루어지는 경우로서 관계 중앙행정기관의 장의 요청에 따라 해당 점검이 제3항에 따른 조사에 준하는 것으로 보호위원회가 인정하는 경우

⑤ 제3항에 따른 조사는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에게 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 한다.

⑥ 법 제24조제5항에서 “대통령령으로 정하는 전문기관”이란 다음 각 호의 기관을 말한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원(이하 “한국인터넷진흥원”이라 한다)
2. 법 제24조제4항에 따른 조사를 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 보호위원회가 정하여 고시하는 법인, 단체 또는 기관

제21조의2(주민등록번호 암호화 적용 대상 등) ③ 보호위원회는 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

- 또한, 개인정보처리자가 가명정보 및 추가 정보를 처리하는 경우, 법 제28조의4(가명정보에 대한 안전조치의무 등) 및 같은 법 시행령 제29조의5(가명정보에 대한 안전성 확보 조치)에 따라 가명정보 및 추가 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치를 하여야 한다.

「개인정보 보호법」

제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보 보호법 시행령」

제29조의5(가명정보에 대한 안전성 확보 조치) ① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 “추가 정보”라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 제30조에 따른 안전성 확보 조치
2. 가명정보와 추가 정보의 분리 보관. 다만, 추가 정보가 불필요한 경우에는 추가 정보를 파기해야 한다.
3. 가명정보와 추가 정보에 대한 접근 권한의 분리. 다만, 「소상공인기본법」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한을 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

- 이 기준은 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정한 것이므로 개인정보처리자는 사업규모, 보유한 개인정보의 수 및 유형, 정보주체에 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 하며, 개인정보의 안전성 확보조치에 필요한 사항을 이 기준 제4조에 따른 내부 관리계획에 포함하여 수립·시행·점검하여야 한다.
- 개인정보처리자가 이 기준을 위반하여 안전성 확보에 필요한 조치를 하지 아니하면 3천만원 이하의 과태료가 부과될 수 있으며, 개인정보가 분실·도난·유출·위조·변조 또는 훼손당한 경우, 안전성 확보에 필요한 조치를 다하지 아니하였다면 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금이 부과될 수 있다.

제64조의2(과징금의 부과) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보 처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

9. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

제2조 정의

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
2. “이용자”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
3. “접속기록”이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
4. “정보통신망”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
5. “P2P(Peer to Peer)”란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
6. “공유설정”이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
7. “모바일 기기”란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
8. “비밀번호”란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
9. “생체정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
10. “생체인식정보”란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
11. “인증정보”란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.
12. “내부망”이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

13. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
14. “보조저장매체”란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장매체를 말한다.



해설

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

- 개인정보, 처리, 정보주체, 개인정보파일, 개인정보처리자, 공공기관 등 개인정보 보호 법령상 규정된 용어의 정의는 법 제2조의 정의와 같다.
- 이 기준에서 정의되지 않은 IT 용어의 정의는 통상적인 IT 용어 정의와 같다.

1. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

- 개인정보처리시스템이란 일반적으로 데이터베이스 내의 개인정보에 접근할 수 있도록 해주는 응용시스템을 말하며, 개인정보 데이터베이스를 구축·운영하거나 데이터베이스와 연동되어 개인정보의 생성, 기록, 저장, 검색, 이용 등 개인정보 처리과정에 관여하는 응용프로그램, 웹서버 등을 포함한다.

※ 클라우드컴퓨팅서비스를 통해 개인정보의 생성, 기록, 저장, 검색, 이용 등 개인정보 처리 기능을 구현한 경우 해당 클라우드컴퓨팅서비스는 개인정보처리시스템으로 볼 수 있음



개인정보처리시스템 (예시)

- ▶ 데이터베이스를 구성·운영하는 시스템 그 자체
- ▶ 데이터베이스의 개인정보를 처리할 수 있도록 구성한 응용프로그램(Web서버, WAS 등)
- ▶ 개인정보 처리를 위해 구성된 파일처리시스템(FTP서버, 백업서버 등)
- ▶ 개인정보의 처리를 위해 클라우드컴퓨팅 환경에 구축한 시스템 또는 서비스

- 업무용 컴퓨터의 경우에도 데이터베이스 응용프로그램이 설치·운영되어 개인정보취급자가 개인정보를 처리할 수 있도록 체계적으로 구성되어 있다면 개인정보처리시스템에 해당될 수 있다.
 - 다만, 데이터베이스 응용프로그램이 설치·운영되지 않는 컴퓨터, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외된다.

2. “이용자”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

- 정보통신서비스제공자는 「전기통신사업법」에 따른 전기통신사업자 (기간·부가통신사업자)와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말하며, 정보통신서비스는 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.



TIP

- 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자는 인터넷 홈페이지 등을 이용하여 정보 및 서비스를 제공하는 자를 의미하며, 보통 영업 행위를 하는 주체가 홈페이지를 개설하고 회원가입을 받을 때에는 모두 적용 대상이 된다(‘영리를 목적’은 자기 또는 제3자의 재산적 이익을 얻기 위한 목적을 말하는 것으로 해석하고 있으며 여기서의 이익은 계속적, 반복적일 필요가 없다.).

3. “접속기록”이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리 시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

- 접속기록은 개인정보처리시스템에 접속하는 자가 개인정보처리시스템 접속 및 운영 등에 관하여 수행한 업무내역 등 이력을 남기는 기록으로서, 접속에 관한 정보와 수행한 업무내역에 관한 정보 등을 개인정보처리시스템의 로그(Log) 파일 또는 로그관리시스템 등에 전자적으로 기록한 것을 말한다.
 - 전자적으로 기록한 것이란 수기로 문서를 작성한 것이 아니라 개인정보처리시스템의 로그(Log) 파일 또는 로그관리시스템 등에 기록한 것을 말한다.
- “식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무”는 개인정보취급자 등 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속한 사실과 접속하여 수행한 업무내역을 확인하는 데 필요한 정보를 말한다.

필수 기록 항목	설 명
① 식별자	• 개인정보처리시스템에 접속한 자를 식별할 수 있도록 부여된 ID 등 식별자
② 접속 일시	• 개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)
③ 접속지 정보	• 개인정보처리시스템에 접속한 자의 컴퓨터, 모바일기기 등 단말기 또는 서버의 IP 주소 등 접속지 정보
④ 처리한 정보주체 정보	• 처리한 개인정보의 정보주체가 누구인지 식별할 수 있는 정보(ID, 고객정보, 학번, 사번 등)
⑤ 수행 업무	• 개인정보처리시스템에 접속한 자가 개인정보처리시스템에서 수행한 업무 내용(검색, 열람, 조회, 입력, 수정, 삭제, 출력, 다운로드 등)을 알 수 있는 정보



- “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

4. “정보통신망”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항 제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신 설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

- 정보통신망은 전기통신을 하기 위한 기계·기구·선로 기타 전기통신에 필요한 설비를 이용하거나 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 의미한다.

5. “P2P(Peer to Peer)”란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.

- P2P는 서버 등의 중간매개자 없이 정보 제공자(개인)와 정보 수신자(개인)가 직접 연결되어 각 개인이 가지고 있는 파일 등을 공유하는 것을 말한다(개인↔개인).
- 정보 제공자 및 정보 수신자 모두가 동시에 접속하지 않고서도 정보 제공자가 어떠한 파일을 공유하면 정보 수신자가 그 파일을 내려받을 수 있는 형태를 말한다.
 - 개인이 인터넷상에서 정보 검색 등을 통해 파일을 찾는 방식(개인↔서버)과는 다른 개념이다.

6. “공유설정”이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.

- 공유설정은 컴퓨터 소유자의 파일, 폴더 등을 타인이 접근하여 조회, 변경, 복사 등을 할 수 있도록 권한을 설정하는 것을 말한다.
 - 원격데스크톱 연결 등 원격접속 설정을 통해 타인이 원격에서 컴퓨터 소유자의 파일, 폴더 등 자원에 접근하도록 설정하는 것이 포함되며, 여기에는 클라우드, NAS, 파일서버 등을 통해 공유하는 형태도 해당된다.

7. “모바일 기기”란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

- 모바일 기기는 이동통신망, 와이파이(Wi-Fi) 등의 무선망을 이용하여 개인정보 처리에 이용되는 휴대용 기기로서, 스마트폰, 태블릿 컴퓨터 등이 있다.

[모바일 기기의 예시]



- “개인정보 처리에 이용되는 휴대용 기기”는 개인정보처리자가 업무를 목적으로 개인정보 취급자로 하여금 개인정보 처리에 이용하도록 하는 휴대용 기기를 말한다.
 - 개인 소유의 휴대용 기기라 할지라도 개인정보처리자의 업무 목적으로 개인정보 처리에 이용되는 경우 “모바일 기기”에 포함되며, 개인정보처리자의 “업무 목적”으로 “개인정보 처리”에 이용되지 않는 휴대용 기기는 “모바일 기기”에서 제외된다.

8. “비밀번호”란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

- 비밀번호란 개인정보취급자 또는 정보주체 등이 개인정보처리시스템, 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는

것을 식별·인증할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

- 식별자는 개인정보처리시스템에 접속하는 자를 식별하기 위한 목적으로 사용되는 ID, 사용자 이름, 사용자 계정명 등을 말한다.
- 문자열은 영대문자(A~Z), 영소문자(a~z), 숫자(0~9), 특수문자(~, !, @ 등) 등을 말한다.
- 타인에게 공개되지 않은 정보의 의미는 타인(정당한 접속 권한을 가지고 있지 않은 자)이 비밀번호를 파악할 수 있도록 관리되어서는 안 된다는 것이다. 이는 본인 이외의 내부직원 또는 비인가자나 공격자 등이 개인정보처리시스템 등에 접속하여 개인정보를 유출하는 등 불법행위가 가능하기 때문이다.

9. “생체정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

- 생체정보는 특정 개인을 인증·식별하거나 개인의 특징을 알아보기 위한 목적으로 처리되는 정보로서 신체적 특징, 생리적 특징과 행동적 특징을 기반으로 생성된 정보로 구분할 수 있다.
 - 신체적 특징: 지문, 얼굴, 홍채·망막의 혈관 모양, 손바닥·손가락의 정맥 모양, 장문, 귓바퀴의 모양 등
 - 생리적 특징: 뇌파, 심전도, 유전정보 등
 - 행동적 특징: 음성, 필적, 걸음걸이, 자판입력 간격·속도 등
- ‘특정 개인을 인증·식별’은 지문·홍채·얼굴 등에서 추출한 특징점 등을 이용(비교·대조)하여 특정 개인임을 확인하는 것을 의미하고, ‘개인에 관한 특징을 알아보기 위해’는 인증·식별 이외의 목적으로 사람의 연령·성별·감정 등의 상태를 확인 또는 분류하는 것을 의미한다.
- 열람·보관 등을 목적으로 수집하는 일반적인 얼굴 사진, 음성파일 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보가 ‘특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 기술적으로 처리’되지 않는다면 생체정보에는 해당되지 않는다.

10. “생체인식정보”란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

- 지문, 얼굴, 홍채, 정맥, 음성, 필적 등의 생체정보가 특정 개인을 인증 또는 식별할 목적으로 사용되는 경우 생체인식정보에 해당한다.

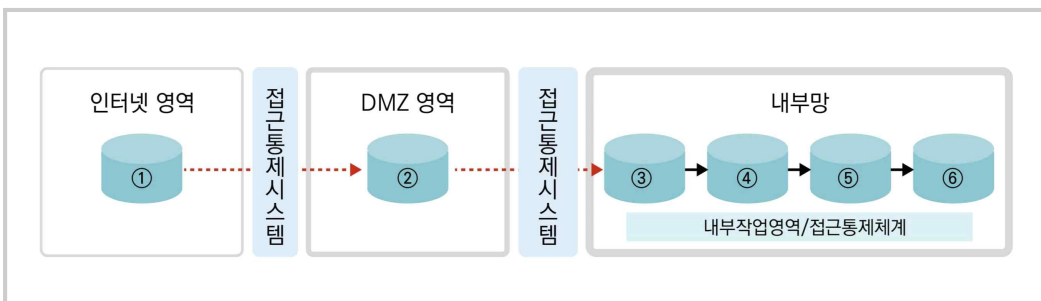
11. “인증정보”란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.

- ‘신원을 검증하는 데 사용되는 정보’는 해당 시스템에서 업무를 수행할 수 있는 정당한 식별자임을 증명하기 위하여 식별자와 연계된 정보로서 비밀번호, 생체인식정보, 전자서명값, 인증토큰 등이 있다.

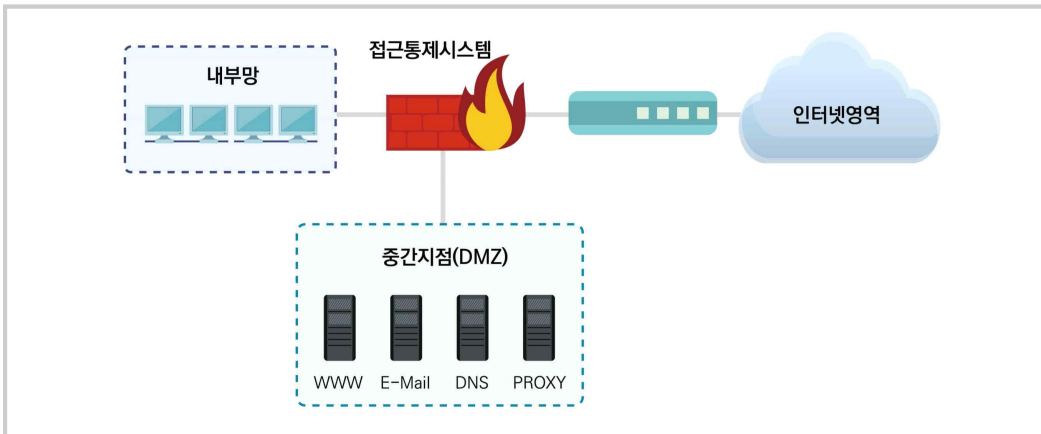
12. “내부망”이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

- 내부망이란 인터넷 구간과 물리적으로 망이 분리되어 있거나 비인가된 불법적인 접근을 차단하는 기능 등을 가진 접근통제시스템에 의하여 인터넷 구간에서의 직접 접근이 불가능하도록 통제·차단되어 있는 구간을 말한다.

[내부망 구성도 예시 1]



[내부망 구성도 예시 2]



13. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.

- 위험도 분석은 개인정보처리시스템에 적용하고 있는 개인정보 안전조치 이행 여부와 개인정보 유출 시 정보주체의 권리를 침해할 위험의 정도를 위험도 분석 기준을 이용하여 분석하는 행위를 의미한다.

14. “보조저장매체”란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장매체를 말한다.

- 보조저장매체에는 이동형 하드디스크(HDD), 유에스비(USB)메모리 등이 있다. 경우에 따라서는 스마트폰도 보조저장매체가 될 수 있다.

[보조저장매체 예시]



제2장 | 개인정보의 안전성 확보조치

제3조 안전조치의 적용 원칙

제3조(안전조치의 적용 원칙) 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.



- 이 기준은 개인정보처리자가 개인정보를 처리할 때 개인정보가 분실·도난·유출·위조·변조 또는 훼손 등이 되지 않도록 기술적·관리적·물리적 안전조치에 관한 최소한의 기준을 정한 것으로, 개인정보처리자는 개인정보의 안전성 확보를 위해 다음과 같은 사항 등을 고려하여 필요한 개인정보 보호조치 기준을 수립하여 적용하여야 한다.
 - 이 기준에서 정하는 개인정보의 안전성 확보에 필요한 안전조치에 관한 사항을 모두 포함하여야 한다.
 - 개인정보처리자는 개인정보의 보유 수, 유형, 중요도, 개인정보를 처리하는 방법 및 환경, 정보주체에게 미치는 영향 등을 고려하여 이 기준에서 정한 것 이외에 필요한 추가적인 안전조치의 기준을 수립 및 적용, 점검하여 개인정보의 안전성 확보조치를 강화하여야 한다.



추가적인 안전조치 기준 수립 예시

- ▶ 이 기준에서 최소한으로 정하는 수준 이상의 기술적·관리적·물리적 안전조치
 - * 제6조(접근통제) 제2항에서 언급하는 안전한 인증수단을 마련하기 위해 이중인증 방식을 도입하였으나, 여기에 VPN을 추가적으로 적용하는 경우
- ▶ 시스템 구성을 고려하여 추가 보안 장비를 도입하고, 정책설정, 이상행위 탐지·대응 관련 운영·관리 방안을 수립하는 등 개인정보처리자의 판단에 따라 개인정보 보호를 위해 추가로 필요한 사항 등

제4조 내부 관리계획의 수립·시행 및 점검

제4조(내부 관리계획의 수립·시행 및 점검) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

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

② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리 하여야 한다.



해설

① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

- 개인정보처리자는 개인정보를 처리하면서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적·물리적 안전조치에 관한 내부 관리계획을 수립하고 시행하여야 한다.
 - 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에도 이 기준에서 정한 내부 관리계획 외에 개인정보 보호를 위하여 필요한 계획(예: 체크리스트)을 자율적으로 수립하여 시행할 수 있다. 그러나 그 외 이 기준에서 정한 해당되는 다른 안전조치 의무사항은 이행하여야 한다.



■ '소상공인'이란 「소상공인기본법」 제2조에 해당하는 자로 광업·제조업·건설업 및 운수업은 상시 근로자 수가 10명 미만, 그 외 업종은 상시 근로자 수가 5명 미만인 자를 말한다.

- 내부 관리계획에는 개인정보의 안전한 처리를 위하여 필요한 안전조치의 이행에 관한 세부적인 추진방안을 포함해 수립하여야 한다.
 - 내부 관리계획의 세부적인 추진방안에는 이 기준에서 정하는 기술적·관리적·물리적 안전조치에 관한 사항이 모두 포함되어야 하며, 개인정보처리자가 스스로 정하는 개인정보의 안전성 확보에 필요한 기준에 관한 사항도 포함되어야 한다.

참 고

- ▶ 내부 관리계획의 문서 제목은 가급적 “내부 관리계획”이라는 용어를 사용하는 것이 바람직하나, 개인정보 처리자의 내부 방침에 따라 다른 용어를 사용할 수 있다.
 - ▶ 다른 용어를 사용하는 경우에도 이 기준 제4조에 관한 사항을 이행하여야 한다.
 - ▶ 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안 위험요인 등을 고려하여야 한다.
-
- 내부 관리계획을 수립할 때에는 이 기준에서 정하는 사항을 포함하여야 한다. 다만, 해당하는 사항이 없는 경우에는 목차에서 제외하거나 “해당 사항 없음”으로 작성할 수 있다. 내부 관리계획에서 제외한 사유에 대해서는 “13. 위험 분석 및 관리에 관한 사항” 등에서 관련 사항을 작성할 수 있다.
 - 내부 관리계획은 전사적인 계획 내에서 개인정보를 관리할 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원과 관련자에게 알려 이를 준수하도록 하여야 한다.

참 고

- ▶ ‘내부 관리계획’은 ‘개인정보 처리방침(법 제30조)’과 목적, 포함되어야 하는 내용, 그 대상 등에 차이가 있다.
 - ※ 개인정보 처리방침: 개인정보 처리에 관한 사항을 정보주체에게 홈페이지 등에서 공개(근거: 법 제30조 (개인정보 처리방침의 수립 및 공개))
 - ※ 개인정보 내부 관리계획: 개인정보를 안전하게 처리하기 위한 조직(회사) 전체 대상(근거: 법 제29조 (안전조치의무))



개인정보 내부 관리계획 목차 예시

제1장 총칙

- 제1조(목적)
- 제2조(용어정의)
- 제3조(적용범위)

제2장 내부 관리계획의 수립·시행 및 점검

- 제4조(내부 관리계획의 수립, 변경 및 승인)

- 제5조(내부 관리계획의 공표)
- 제6조(내부 관리계획의 이행 실태 점검)

제3장 개인정보 보호 조직의 구성 및 운영

- 제7조(개인정보 보호 조직)
- 제8조(개인정보 보호책임자의 자격요건)
- 제9조(개인정보 보호책임자의 지정)
- 제10조(개인정보 보호책임자의 역할 및 책임)
- 제11조(개인정보취급자의 역할 및 책임)
- 제12조(개인정보취급자에 대한 관리 및 감독)

제4장 개인정보 보호 교육 계획 수립 및 시행

- 제13조(개인정보 보호책임자 교육)
- 제14조(개인정보취급자 교육)

제5장 기술적 안전조치

- 제15조(접근 권한의 관리)
- 제16조(접근통제)
- 제17조(개인정보의 암호화)
- 제18조(접속기록의 보관 및 점검)
- 제19조(악성프로그램 등 방지)
- 제20조(개인정보 유출 방지 취약점 점검)

제6장 관리적 안전조치

- 제21조(개인정보 유출사고 대응 계획 수립 및 시행)
- 제22조(위험 분석 및 관리)
- 제23조(수탁자에 대한 관리 및 감독)
- 제24조(개인정보의 파기)

제7장 물리적 안전조치

- 제25조(물리적 안전조치)
- 제26조(재해 및 재난 대비 안전조치)
- 제27조(출력 및 복사시 보호조치)

제8장 그 밖에 개인정보 보호를 위하여 필요한 사항

1. 개인정보 보호 조직의 구성 및 운영에 관한 사항

- 개인정보처리자는 개인정보 처리과정 전반에 걸쳐 개인정보를 안전하게 관리하고 보호하기 위하여 개인정보 보호조직을 구성하고 운영하여야 한다.
- 개인정보처리자는 처리하는 개인정보의 종류, 중요도 및 보유량, 개인정보를 처리하는 방법 및 내·외부 환경 등을 종합적으로 검토하고, 개인정보처리자의 환경에 맞게 보호 업무 수행 체계 및 규모 등을 고려하여, 개인정보 보호 조직을 구성 및 운영하여야 한다.
- 개인정보 보호조직은 업무분장 등을 내부 관리계획 등에 명시하여야 하며, 인력의 지정에 관한 사항, 역할 및 책임 그리고 역량 및 요건 등 적정성에 관한 사항 등을 포함하여야 한다.



개인정보 보호조직 구성도 예시



2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항

- 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호 책임자를 지정하여야 하고, 내부 관리계획에 개인정보 보호책임자의 자격 요건 및 지정에 관한 사항을 포함하여야 한다.

- 다만, 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 경우에는 개인정보 보호책임자를 지정하지 않을 수 있으며, 이 경우에는 그 사업주 또는 대표자가 개인정보 보호책임자가 된다.

- 개인정보 보호책임자는 개인정보 처리에 관한 총괄책임자로서 의사결정을 할 수 있는 지위에 있어야 하며, 개인정보보호 법·제도·기술 등에 대해 풍부한 지식을 보유한 자로 지정해야 한다.

- 특히, 개인정보처리자가 연간 매출액 등이 1,500억 원 이상이고, 5만명 이상의 정보주체에 대하여 민감정보 또는 고유식별정보를 처리하거나 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 등 시행령 제32조 제4항 각호 하나에 해당하는 경우, 개인정보 보호책임자로 지정되는 사람은 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고, 그중 개인정보보호 경력을 최소 2년 이상 보유해야 한다.

「개인정보 보호법」

제31조(개인정보 보호책임자의 지정 등) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자의 경우에는 지정하지 아니할 수 있다.

② 제1항 단서에 따라 개인정보 보호책임자를 지정하지 아니하는 경우에는 개인정보처리자의 사업주 또는 대표자가 개인정보 보호책임자가 된다.

제65조(고발 및 징계권고) ① 보호위원회는 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다.

② 보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 보호위원회에 통보하여야 한다.

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 하거나 소속 기관·단체 등의 장에게 제2항에 따른 징계권고를 할 수 있다. 이 경우 제2항에 따른 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 관계 중앙행정기관의 장에게 통보하여야 한다.

제75조(과태료) ④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

9. 제31조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제1항 단서에서 “종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 개인정보처리자를 말한다.

③ 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.

1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
 - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위 공무원단에 속하는 공무원(이하 “고위공무원”이라 한다) 또는 그에 상응하는 공무원
 - 나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상응하는 공무원
 - 다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상응하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상응하는 공무원
 - 라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
 - 마. 시·도 및 시·도 교육청: 3급 이상 공무원 또는 그에 상응하는 공무원
 - 바. 시·군 및 자치구: 4급 이상 공무원 또는 그에 상응하는 공무원
 - 사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람. 다만, 제4항제2호에 해당하는 경우에는 교직원을 말한다.
 - 아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.

2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람

- 가. 사업주 또는 대표자
- 나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)는 제3항 각 호의 구분에 따른 사람 중 별표 1에서 정하는 요건을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다.

1. 연간 매출액등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자(제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다)
 - 가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자
 - 나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자
2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교
3. 「의료법」 제3조의4에 따른 상급종합병원
4. 공공시스템운영기관

개인정보 보호책임자의 자격(제32조제4항 관련)

1. 제32조제4항에 따라 개인정보 보호책임자로 지정되는 사람은 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고, 그 중 개인정보보호 경력을 최소 2년 이상 보유해야 한다.
2. 제1호에서 “개인정보보호 경력”이란 공공기관, 기업체, 교육기관 및 연구기관 등에서 개인정보보호 관련 정책 및 제도·개인정보 영향평가·개인정보 보호 인증심사 등 개인정보보호 업무를 수행한 경력, 개인정보보호 관련 컨설팅 또는 법률자문 경력을 말한다.
3. 제1호에서 “정보보호 경력”이란 공공기관, 기업체, 교육기관 및 연구기관 등에서 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호, 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 등 정보보호 업무를 수행한 경력, 정보보호 관련 컨설팅 또는 법률자문 경력을 말한다.
4. 제1호에서 “정보기술 경력”이란 공공기관, 기업체, 교육기관 및 연구기관 등에서 정보통신서비스, 정보통신기기, 소프트웨어 및 컴퓨터 관련 서비스 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 등 정보기술 업무를 수행한 경력, 정보기술 관련 컨설팅 또는 법률자문 경력을 말한다.

비고: 가. 동일 기간에 두 가지 이상 업무가 중복되는 경우에는 하나의 경력만 인정한다.

나. 개인정보보호, 정보보호, 정보기술 관련 학위를 취득한 경우에는 아래의 표에 따라 경력으로 인정한다. 다만, 여러 학위를 취득한 경우에는 개인정보 보호책임자를 지정하려는 개인정보처리자가 정하는 하나의 학위만 경력으로 인정한다.

학 위	경력 인정기간
개인정보보호 관련 박사	개인정보보호 경력 2년
개인정보보호 관련 석사	개인정보보호 경력 1년
개인정보보호 관련 학사	개인정보보호 경력 6개월
정보보호 관련 박사	정보보호 경력 2년
정보보호 관련 석사	정보보호 경력 1년
정보보호 관련 학사	정보보호 경력 6개월
정보기술 관련 박사	정보기술 경력 2년
정보기술 관련 석사	정보기술 경력 1년
정보기술 관련 학사	정보기술 경력 6개월

다. 그 밖에 보호위원회가 정하여 고시하는 자격을 취득하거나 교육을 이수한 경우 등의 해당 취득자격이나 이수교육 등에 대해서는 보호위원회가 정하여 고시하는 바에 따라 개인정보 보호 경력, 정보보호 경력 또는 정보기술 경력으로 인정한다.

참 고

- ▶ 개인정보 보호책임자(CPO)와 「정보통신망법」 제45조의3에서 정하고 있는 정보보호 최고책임자(CISO)는 동일인으로 지정하거나 별도로 지정할 수 있다.

* 다만, 개인정보 활용에 따른 이해충돌 우려, 개인정보 보호 규제 전문성 확보, 개인정보의 안전성 확보조치에 관하여 상호 간의 명확한 업무분장 필요

3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항

- 개인정보 보호책임자는 개인정보 처리에 관한 업무를 총괄하여야 한다.
 - 개인정보 보호 계획의 수립·시행, 개인정보 처리 실태 및 관행에 대한 조사 및 개선, 정보주체의 개인정보 처리와 관련한 불만의 처리, 피해 구제, 개인정보의 유출 및 오남용 방지를 위한 내부통제시스템 구축, 개인정보 보호 교육 계획 수립 및 시행, 개인정보파일 보호 및 관리·감독, 개인정보 처리방침 수립·변경 및 시행, 개인정보 처리와 관련된 인적·물적 자원 및 정보관리, 처리목적 달성 또는 보유기간이 지난 개인정보 파기, 개인정보취급자에 대한 적절한 관리 및 감독 등의 업무를 총괄한다.
 - 아울러, 개인정보 처리 실태 등을 조사하거나 관계 당사자로부터 관련 보고를 받을 수 있으며, 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 한다. 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하는 등 개인정보보호 업무 책임을 맡는다.
- 개인정보처리자는 개인정보 보호책임자가 형식적으로 외부에 보여주기 위한 장치గా 아닌 개인정보처리자의 내부 관리체계를 강화하고 자율규제를 활성화하는 등 개인정보 보호책임자에게 실질적인 권한과 의무를 부여하여야 한다.
 - 특히, 개인정보처리자는 개인정보 보호책임자가 업무를 수행하는 데 정당한 이유 없이 불이익을 주거나 받게 하여서는 안 되며, 업무를 독립적으로 수행할 수 있도록 보장하여야 한다.



개인정보 보호책임자의 주요 업무 및 역할

- ▶ 개인정보보호 관련 계획 수립 및 시행
- ▶ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- ▶ 개인정보 처리와 관련한 불만의 처리 및 피해 구제
- ▶ 개인정보 유출 및 오남용 방지를 위한 내부통제시스템의 구축
- ▶ 개인정보보호 교육 계획 수립 및 시행
- ▶ 개인정보파일의 보호 및 관리·감독
- ▶ 개인정보 처리방침의 수립·변경 및 시행
- ▶ 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리
- ▶ 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 등
- ▶ 그 밖에 개인정보 보호 관련 법령에서 명시하는 사항

- 개인정보취급자는 개인정보가 안전하게 관리될 수 있도록 개인정보처리자의 지휘·감독을 받아 개인정보를 처리(개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위)하는 역할을 한다.



개인정보취급자의 역할 및 업무 예시

- ▶ 내부 관리계획 등 각종 규정, 지침 등 준수
- ▶ 개인정보처리시스템의 안전한 운영 및 관리
- ▶ 개인정보의 안전성 확보조치 기준 이행
- ▶ 개인정보보호 교육 참석
- ▶ 개인정보 침해사고 발생 시 대응 및 보고
- ▶ 개인정보 처리 현황, 처리 체계 등의 점검 및 보고 등

- 개인정보처리자는 스스로의 환경에 맞추어 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항을 내부 관리계획에 포함하여야 한다.

「개인정보 보호법」

제31조(개인정보 보호책임자의 지정 등) ③ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

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 오용·남용 방지를 위한 내부통제시스템의 구축
 5. 개인정보 보호 교육 계획의 수립 및 시행
 6. 개인정보파일의 보호 및 관리·감독
 7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무
- ④ 개인정보 보호책임자는 제3항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
- ⑤ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.
- ⑥ 개인정보처리자는 개인정보 보호책임자가 제3항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 되며, 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하여야 한다.
- ⑨ 제1항에 따른 개인정보 보호책임자의 자격요건, 제3항에 따른 업무 및 제6항에 따른 독립성 보장 등에 필요한 사항은 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정한다.

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ② 법 제31조제3항제7호에서 “대통령령으로 정한 업무”란 다음 각 호와 같다.

1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리
3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
- ⑥ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 법 제31조제6항에 따른 개인정보 보호책임자의 독립성 보장을 위해 다음 각 호의 사항을 준수해야 한다.
 1. 개인정보 처리와 관련된 정보에 대한 개인정보 보호책임자의 접근 보장
 2. 개인정보 보호책임자가 개인정보 보호 계획의 수립·시행 및 그 결과에 관하여 정기적으로 대표자 또는 이사회에 직접 보고할 수 있는 체계의 구축
 3. 개인정보 보호책임자의 업무 수행에 적합한 조직체계의 마련 및 인적·물적 자원의 제공

4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항

- 개인정보처리자는 개인정보를 처리하는 데 개인정보가 안전하게 관리되도록 개인정보 취급자의 범위와 업무를 최소한으로 제한하고, 개인정보취급자에 대한 접근 권한의 차등부여, 인사이동에 따른 변경·말소, 보안서약서 징구 등 개인정보취급자에 대하여 적절한 관리·감독을 하여야 한다.
- 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 필요한 교육을 정기적으로 실시하여야 한다.
- 교육에 관한 사항에는 교육 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함한다. 이를 내부 관리계획 등에 관련 사항을 규정하거나 “○○년 개인정보보호 교육 계획(안)” 등의 형태로 수립할 수 있다.
- 교육 내용은 개인정보취급자의 업무성격, 지위·직책, 담당업무의 내용, 업무 숙련도 등에 따라 차등화하여 실시한다.
- 교육 방법에는 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으며, 조직의 여건 및 환경을 고려하여 집체 교육, 온라인 교육 등 다양한 방법을 활용할 수 있다.



참고자료

개인정보보호위원회가 운영하는 개인정보배움터(<https://www.edu.privacy.go.kr>)에서 제공하는 교육 프로그램, 교육 교재, 전문강사 등 활용 가능

「개인정보 보호법」

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 “개인정보취급자”라 한다)의 범위를 최소한으로 제한하고, 개인정보 취급자에 대하여 적절한 관리·감독을 하여야 한다.

② 개인정보처리자는 개인정보의 적절한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

5. 접근 권한의 관리에 관한 사항

- 접근 권한이 없는 자가 개인정보처리시스템 등에 접근하는 것을 방지하기 위하여 이 기준 제5조(접근 권한의 관리)에 관한 사항을 포함하여야 한다.
 - 개인정보취급자에게 업무수행에 필요 최소한의 범위로 접근 권한 차등 부여
 - 개인정보취급자별로 계정 발급
 - 개인정보처리시스템에 대한 접근 권한을 업무 담당자에 따라 차등 부여
 - 일정 횟수 이상 인증을 실패한 경우 접근제한
 - 개인정보취급자 또는 개인정보취급자의 업무 변경 시 지체 없이 접근 권한의 변경 또는 말소
 - 접근 권한의 부여, 변경, 말소에 대한 내역 기록 및 최소 3년간 보관 등

6. 접근 통제에 관한 사항

- 정보통신망을 통한 개인정보처리시스템 등의 불법적인 접근을 차단하고 침해사고를 예방하기 위하여 이 기준 제6조(접근통제)에 관한 사항을 포함하여야 한다.
 - 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단, 침입탐지, 침입방지, 접속차단 등 필요한 조치

- 개인정보 유·노출 방지를 위해 컴퓨터 등에 대한 안전조치
- 개인정보취급자에 대한 안전한 인증수단 또는 접속수단의 적용 및 관리 기준 수립 등

7. 개인정보의 암호화 조치에 관한 사항

- 개인정보처리자는 개인정보의 유·노출 등을 방지하기 위하여 이 기준 제7조(개인정보의 암호화)에 관한 사항을 포함하여야 한다.
 - 비밀번호, 생체인식정보 등 인증정보 저장 및 정보통신망을 통한 송수신 시 암호화
 - 비밀번호 저장 시 복호화되지 않도록 안전한 일방향 암호화 알고리즘으로 저장
 - 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식 정보는 안전한 암호 알고리즘으로 암호화 저장

8. 접속기록 보관 및 점검에 관한 사항

- 개인정보취급자가 개인정보처리시스템에 접속한 정보 등을 확인할 수 있는 중요한 사항으로 이 기준 제8조(접속기록의 보관 및 점검)에 관한 사항을 포함하여야 한다.
 - 개인정보취급자가 개인정보처리시스템에 접속한 기록의 보관기간
 - 개인정보처리시스템의 접속기록 점검주기
 - 개인정보의 다운로드가 확인된 경우 사유를 반드시 확인하여야 하는 기준과 사유 확인에 필요한 사항 등
 - ※ 개인정보처리자의 업무 환경을 고려한 다운로드 기준(다운로드 정보주체의 수, 일정기간 내 다운로드 횟수 등)을 정하여 업무 목적 외의 불법행위 등으로 의심되는 다운로드에 대해 그 사유를 반드시 확인하여야 한다.
 - 접속기록의 위변조, 도난, 분실 방지를 위한 조치

9. 악성프로그램 등 방지에 관한 사항

- 개인정보취급자의 컴퓨터 등을 통한 개인정보 유출을 예방하기 위하여 이 기준 제9조 (악성프로그램 등 방지)에 관한 사항을 포함하여야 한다.
 - 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램 설치·운영
 - 프로그램의 자동 업데이트 기능 등을 사용하여 최신 상태로 유지
 - 발견된 악성프로그램 등에 대한 삭제 조치
 - 악성프로그램 관련 정보가 발령되거나 보안 업데이트 공지(www.boho.or.kr 등)가 있는 경우 정당한 사유가 없는 한 즉시 업데이트 실시

10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항

- 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보를 처리하는 환경, 기기, 설비, 시스템 등의 취약점을 점검하여야 하며, 그 결과에 따라 개선조치를 하여야 한다.
- 개인정보처리시스템을 신규로 도입·개발 또는 변경 시 시큐어 코딩, 최신 취약점 등을 포함한 보안 요구사항을 명확히 정의하고 설계 및 개발 단계에서부터 반영을 고려할 필요가 있다.
- 가령 개인정보를 처리하는 인터넷 홈페이지에 대해서는 다음과 같은 웹, 시스템 애플리케이션 취약점 점검을 실시할 수 있다



웹 취약점 점검 항목 예시

- ▶ 최신 웹 취약점 및 점검 항목 등은 국가정보원 국가사이버안보센터(NCSC), 한국인터넷진흥원 보호나라 & KrCERT/CC, OWASP 등에서 발표하는 자료 참조
- ▶ 웹 취약점 점검 외에도 정기적으로 웹셀 등을 점검하고 조치

- 개인정보의 유출, 도난 방지 등을 위한 취약점 점검 시에는 기록을 남겨 책임 추적성 확보 및 향후 개선조치 등에 활용할 수 있도록 할 필요가 있다.
- 개인정보처리자의 개인정보 처리 업무 및 환경 등에 대한 전반적인 취약점 점검은 개인정보처리자의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 사용할 수 있다.



취약점 점검 및 조치 시 참고자료 예시

- ▶ 취약점 점검 및 조치에 활용할 수 있는 기술문서는 아래와 같다.
 - 공개SW를 활용한 소프트웨어 개발보안 점검 가이드(행정안전부)
 - 소프트웨어 보안약점 진단가이드(행정안전부)
 - 소프트웨어 개발보안 가이드(행정안전부)
 - 주요정보통신기반시설 기술적 취약점 분석, 평가 방법 상세가이드(과학기술정보통신부)

- 개인정보 처리기술 및 서비스가 확대되고, 개인정보를 위협하는 침해요인 증가에 따라 시스템 등에 대한 신규 취약점이 지속적으로 발생하고 있으므로 정기적인 취약점 점검 및 개선조치를 통하여 개인정보 유출을 예방하는 등 적극적인 보호활동을 하여야 한다.

11. 물리적 안전조치에 관한 사항

- 개인정보가 보관되어 있는 물리적 장소나 서류·매체 등을 안전하게 관리하기 위하여 이 기준 제10조(물리적 안전조치)에 관한 사항을 포함하여야 한다.
 - 전산실, 자료보관실 등 물리적 보관 장소를 두고 있는 경우 출입통제 절차 수립·운영
 - 서류, 보조저장매체 등은 잠금장치가 있는 안전한 장소에 보관
 - 보조저장매체의 반출·입 통제를 위한 보안대책 마련 등

12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

- 개인정보 유출사고가 발생한 때에는 신속한 대응 조치를 통해 개인정보의 추가 유출을 막고, 이로 인한 정보주체의 피해를 최소화하기 위한 긴급조치, 유출 신고 및 통지, 피해

신고 접수 및 피해 구제 등과 같은 사항을 포함하는 개인정보 유출 사고 대응 계획을 수립·시행하여야 한다.

- 개인정보 유출 신속 대응체계 구축: 개인정보 유출 사실을 알게 된 때, 개인정보보호 책임자는 즉시 사업주 또는 대표자에게 보고하고 개인정보보호·정보보호 부서를 중심으로 ‘개인정보 유출 등 사고 신속대응팀’을 구성하여, 추가 유출 및 정보주체 피해발생 방지를 위한 조치를 강구하여야 한다.
- 유출 원인 파악 및 추가 유출 방지 조치: 개인정보 유출 원인을 파악한 후 추가 유출 방지를 위해 유출 원인별 보호조치를 실시하여야 한다.
- 개인정보 유출 신고 및 통지:

구 분	조치 사항
신고	<ul style="list-style-type: none"> • (신고 요건에 해당하는 경우에) 개인정보의 유출 사실을 알게 된 때에는 72시간 내에 개인정보 유출 사실을 보호위원회 또는 한국인터넷진흥원에 신고하여야 한다. * (1) 1천 명 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우 (2) 민감정보 또는 고유식별정보가 유출된 경우 (3) 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출된 경우 등
통지	<ul style="list-style-type: none"> • 유출된 개인정보로 인하여 추가적인 피해가 발생하지 않도록 개인정보 유출 사실을 알게 된 때에는 개인정보가 유출된 해당 정보주체에게 법 제34조에 따른 사항을 포함하여 72시간 내에 개인정보 유출 사실을 통지하여야 한다.

- 정보주체의 피해구제 및 재발 방지 대책 마련: 정보주체의 피해구제 방법을 안내하고 유사 사고의 재발 방지를 위한 대책을 마련하여야 한다.

참 고

- ▶ “개인정보 유출 등 사고 대응 매뉴얼”은 개인정보 포털 (<https://www.privacy.go.kr>)에서 다운로드 가능
- ▶ 개인정보 유출로 인한 피해를 막기 위해서는 해커 등 개인정보 유출자 검거를 위해 경찰청 사이버범죄 신고시스템(ECRM)에 신고하여 범인 검거를 위한 수사를 요청하고 유출된 개인정보 회수를 위한 조치 실시
- ▶ 인터넷상 침해사고가 발생하면 과학기술정보통신부 또는 한국인터넷진흥원에 신고(보호나라&KrCERT/CC(<https://www.boho.or.kr>))하여 침해사고 원인분석 및 취약점 보완조치 등을 실시

13. 위험 분석 및 관리에 관한 사항

- 개인정보 처리에 따른 잠재적인 위험을 분석하고 이를 효과적으로 관리하기 위한 방안을 포함하여야 한다.
 - 개인정보 위험 분석이란 개인정보의 처리 방법 및 종류 등에 따라 개인정보의 분실·도난·유출·위조·변조·훼손 등 침해가 발생할 가능성과 정보주체에게 미치는 영향 등 그 위험의 정도를 분석하는 행위를 말한다.
 - 개인정보 위험 분석 및 관리를 위한 방법과 절차는 개인정보처리자의 특성 및 상황 등을 고려하여 자체적으로 마련할 수 있다.
 - 이용자가 아닌 정보주체의 고유식별정보(주민등록번호 제외)에 대한 암호화의 적용여부 및 적용범위를 정하고자 하는 경우에는 본 안내서 부록(개인정보 위험도 분석 기준 해설)을 참고하여 위험도 분석을 수행할 수 있다.

14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

- 개인정보처리자는 개인정보 처리업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 관리·감독하여야 한다.
- 개인정보처리자는 수탁자에 대하여 정기적으로 교육을 실시하고, 수탁자의 개인정보 처리 현황 및 실태, 목적 외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 점검 등 관리·감독하여야 한다.
- 내부 관리계획에는 수탁자에 대한 교육 및 감독의 시기와 방법, 절차, 점검 항목 등을 포함해야 하며, 수탁자 교육 및 감독에 대한 기록을 남기고 문제점이 발견된 경우 그에 따른 개선조치를 하여야 한다.



수탁자 관리 및 감독 예시

- ▶ 관리·감독 대상 및 시기
- ▶ 관리·감독 항목 및 내용
- ▶ 관리·감독 방법 및 절차
- ▶ 관리·감독 결과 기록 및 보관
- ▶ 관리·감독 결과 후속조치(개선, 보고) 등

참 고

- ▶ 사업자 선정부터 사업 종료 시까지 전 과정에 걸쳐 안전성 확보를 위한 보호조치 사항 포함
 - ※ 제안요청서, 계약서 등에 기술적·관리적·물리적 안전조치에 관한 사항을 명시하고, 이에 대한 이행여부를 분기별 또는 반기별로 주기적 관리·감독 및 확인

「개인정보 보호법」

제26조(업무위탁에 따른 개인정보의 처리 제한) ④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

「개인정보 보호법 시행령」

제28조(개인정보의 처리 업무 위탁 시 조치) ① 법 제26조제1항제3호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항

⑥ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우에 법 또는 이 영에 따라 개인정보처리자가 준수하여야 할 사항과 법 제26조제1항 각 호의 사항을 준수하는지를 같은 조 제4항에 따라 감독하여야 한다.

15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항

- 개인정보처리자는 스스로의 환경을 고려하여 내부 관리계획의 수립 및 변경과 승인에 관한 사항을 마련하여야 한다.

- 내부 관리계획은 조직(기관, 기업 등) 전체를 대상으로 마련하여야 하며, 이 기준에서 정하는 개인정보의 안전성 확보에 필요한 조치에 관한 사항을 모두 포함하여야 한다.
 - 법률 또는 이 기준에서 규정하는 내용을 그대로 반영하는 것이 아니라, 스스로의 환경에 맞는 내부 관리계획을 수립하여야 한다.
 - 내부 관리계획을 구체적으로 수립하고, 이를 기초로 세부 지침, 절차, 매뉴얼 등을 추가적으로 수립할 수 있다.
- 개인정보 처리 방법 및 환경 등의 변화로 인하여 내부 관리계획에 중요한 변경이 있을 때에는 변경 사항을 즉시 반영하고, 변경된 내부 관리계획에 대해서도 사업주 또는 대표자 등 최고경영층의 승인을 다시 받아야 한다.
 - 또한, 내부 관리계획 수정 및 변경 시 변경된 내용 및 시행 시기 등 그 이력을 관리하여야 한다.

16. 그 밖에 개인정보 보호를 위하여 필요한 사항

- 개인정보처리자는 처리하는 개인정보의 종류 및 중요도, 보유량 그리고 개인정보를 처리하는 방법 및 환경 등을 고려하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 그 밖의 안전조치를 추가적으로 할 수 있다.
- 예를 들어, 인증제도·인증마크의 도입, 소프트웨어 보안취약점 점검 및 모의해킹, 내·외부 관리실태 점검 및 평가, 개인정보 보호 강화기술(PET) 등에 관한 사항이 이에 해당될 수 있다.

참고

- ▶ 그 밖에 개인정보보호를 위해 필요한 사항으로 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안 위험요인 등을 고려한다.



그 밖에 개인정보 보호조치 예시

- ▶ 개인정보보호 관리체계(ISMS-P) 등 개인정보보호 관련 인증 획득
- ▶ 개인정보보호 컨설팅
- ▶ 개인정보처리시스템 설계, 개발, 운영 시 개인정보보호 중심 설계(Privacy by Design) 적용
- ▶ 개인정보 보호 강화기술(PET)의 도입·운영
- ▶ 보안장비 및 보안솔루션 도입 및 운영, 형상·운영 관리 및 기록
- ▶ 개인정보보호 예산 및 인력의 적정수준 반영
- ▶ 개인정보보호 관련 세부 지침, 절차, 매뉴얼 등의 수립 및 시행
- ▶ 개인정보 파기 절차 수립 및 시행 등

② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보 취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

- 개인정보처리자는 개인정보의 안전한 처리를 위하여 개인정보 보호책임자 및 개인정보 취급자에게 차등화하여 필요한 교육을 연 1회 이상 정기적으로 실시하여야 한다.
 - 차등화된 교육의 예로는 대상자 유형별(개인정보 보호책임자, 개인정보 보호담당자, 개인정보 취급자, 수탁자), 업무 유형별(IT 담당자/운영자, 개발자, 일반 개인정보취급자), 권한별(주요직무자, 일반직무자 등), 기타 업무별 특성을 반영한 특화교육이나 신규입사자, 부서장에 대한 직급별 교육 등이 있다.
- 개인정보보호 교육의 구체적인 사항에 교육 목적 및 대상, 교육 내용(프로그램 등), 교육 일정 및 방법 등을 포함한다. 내부 관리계획 등에 관련 규정하거나 “○○년 개인정보보호 교육 계획(안)” 등과 같은 형태로 수립할 수 있다.
- 교육 내용은 개인정보 보호책임자 그리고 개인정보취급자의 지위·직책, 담당 업무의 내용 및 성격, 업무 숙련도 등에 따라 차등화하여야 한다. 해당 업무를 수행하기 위한 분야별 전문기술 교육뿐만 아니라 개인정보보호 관련 법률 및 제도, 내부 관리계획 등 반드시 알아야 하는 사항을 포함하여 교육을 실시해야 한다.



교육 내용의 예시

- ▶ 개인정보 보호의 중요성
 - ▶ 개인정보 내부관리계획 등 규정, 지침의 제·개정예 따른 사항
 - ▶ 개인정보처리시스템의 안전한 운영·사용법(하드웨어, 소프트웨어 등)
 - ▶ 개인정보의 안전성 확보조치 기준
 - ▶ 개인정보 처리업무 위·수탁 시 보호조치
 - ▶ 개인정보 보호업무의 절차, 책임, 방법
 - ▶ 개인정보 처리 절차별 준수사항 및 금지사항
 - ▶ 개인정보 유·노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 절차 등
- 교육 방법에는 사내교육, 외부교육, 위탁교육 등 여러 종류가 있으며, 조직의 여건 및 환경을 고려하여 집체 교육, 온라인 교육 등 다양한 방법을 활용할 수 있다.
 - 교육 내용에는 업무를 수행하는 데 필요한 개인정보 관련 기술교육뿐만 아니라 개인정보 보호 관련 법률 및 제도, 사내규정 등 반드시 알아야 하는 기본적인 사항을 포함하여 목적에 부합하는 교육을 실시하여야 한다.
 - 교육 결과는 “○○년 개인정보보호 교육 결과” 등의 제목으로 작성하고, 교육 일시·내용·참석자 등을 확인할 수 있는 정보를 전자적으로 기록하거나 수기로 작성하여야 한다.

참 고

- ▶ 교육 결과의 세부 실적은 실시한 개인정보보호 관련 사내교육, 외부교육, 위탁교육 등에서 교육 과정별 수료증 등을 발급·보관함으로써 관리할 수 있다.
- ▶ 교육 참석자를 확인할 수 있는 정보로는 해당 교육 시간에 교육장소에 출입한 기록(태그 등), 교육 참석자 명단에 수기로 서명한 자료 등을 활용할 수 있다.



참고자료

개인정보보호위원회가 운영하는 개인정보배움터(<https://edu.privacy.go.kr>)에서 제공하는 교육 프로그램, 교육 교재, 전문강사 등 활용 가능

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

- 개인정보처리자는 개인정보 처리 방법, 처리 환경 및 안전조치 사항 등 내부 관리계획에 중요한 변경이 있는 경우에는 변경사항을 즉시 반영하여 내부 관리계획을 수정·변경해 시행하여야 한다.
- 내부 관리계획의 수정·변경 시에도 내부 의사결정 절차를 통하여 내부 관리계획을 수정하여 시행하여야 한다.
- 내부 관리계획을 수정·변경하는 경우에는 수정된 내용과 시행 시기 등 이력을 관리하여야 한다.
- 또한, 내부 관리계획의 수정·변경 사항을 개인정보취급자 등에게 전파하여 이를 준수하여야 한다.

④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상 점검·관리하여야 한다.

- 개인정보 보호책임자는 내부 관리계획의 적정성과 실효성을 보장하기 위하여 연 1회 이상 내부 관리계획에 따른 기술적·관리적·물리적 안전조치의 이행 여부를 점검·관리하여야 한다.
 - 내부 관리계획의 이행 실태를 점검·관리하기 위한 계획을 수립할 때에는 점검 대상, 점검 항목 및 방법 등을 포함할 필요가 있다.
 - 이행실태 점검은 사내 독립성이 보장되는 부서(감사팀 등), 관련 부서(개인정보 보호팀) 또는 개인정보보호 전문업체 등에서 수행할 수 있다.
 - 이행실태 점검·관리와 관련한 계획은 “○○년 개인정보 보호조치 이행 점검 계획(안)” 등과 같이 수립할 수 있으며, 결과는 “○○년 개인정보 보호조치 이행실태 점검 결과” 등과 같이 작성할 수 있다.



이행실태 점검·관리 계획 예시

- ▶ 점검 대상 및 시기
 - ▶ 점검 조직 및 인력
 - ▶ 점검 항목 및 내용
 - ▶ 점검 방법 및 절차
 - ▶ 점검 결과 기록 및 보관
 - ▶ 점검 결과 후속조치(개선, 보고) 등
-
- 개인정보 보호책임자는 내부 관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취해야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 점검결과를 보고하고, 의사결정 절차를 거쳐 적절한 대책을 마련하여야 한다.

제5조 접근 권한의 관리

- 제5조(접근 권한의 관리)** ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.
- ② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
- ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
- ④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
- ⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.
- ⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.



해설

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여 하여야 한다.

- 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조·훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 개인정보취급자에게 차등 부여하고 접근통제를 위한 안전조치를 취해야 한다.
 - 개인정보처리시스템에 대한 접근 권한은 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 개인정보취급자에게만 부여하여야 한다.
 - 업무 수행에 필요한 최소한의 범위란 개인정보취급자가 각자의 업무를 수행하기 위해 필요한 최소한의 단위로 접근 권한을 구분하는 것을 말한다. 이를 위해 업무별로 접근 가능한 메뉴 및 상세 권한(열람, 입력, 삭제, 수정, 다운로드, 인쇄 등)을 세분화하여 관리하여야 한다.

- 권한을 차등 부여 하는 것은 업무별로 해당 업무를 수행하기 위해 필요한 최소한의 범위를 차등화하여 개별적으로 접근 권한을 부여하는 것을 말한다. 예를 들면, 개인정보처리 시스템에 대한 접근 권한을 부여할 때 열람, 수정, 다운로드 등의 권한을 포괄적으로 부여하지 않고, 단순 열람만으로 업무 처리가 가능한 개인정보취급자에게는 열람 권한만 부여하는 등 업무 수행에 필요한 최소한의 권한을 차등 부여 하여야 한다.
- 여기서 말하는 개인정보취급자의 접근 권한은 본인 이외의 개인정보처리시스템에 대한 접근 권한을 의미하며, 정보주체가 자신의 개인정보를 조회·수정 하는 등의 접근 권한은 포함하지 않는다.



담당자 업무별 접근 권한의 부여 예시

메뉴명		개인정보 처리 여부	권한 그룹																
			최고 관리자					회원 관리자					게시판 관리자					...	
1단계	2단계		조회	쓰기	수정	삭제	다운로드	조회	쓰기	수정	삭제	다운로드	조회	쓰기	수정	삭제	다운로드	...	
회원 관리	회원정보 관리	○	V	V	V	V	V	V	V	V	V	-	-	-	-	-	-		
	문의/상담 관리	○	V	V	V	V	V	V	V	V	V	-	-	-	-	-	-		
	회원 통계	○	V	V	V	V	V	V	V	V	V	-	-	-	-	-	-		
게시판 관리	공지사항	-	V	V	V	V	V	V	-	-	-	-	V	V	V	V	V	-	
	자유게시판	○	V	V	V	V	V	V	-	-	-	-	V	V	V	V	V	-	
...	...																		



접근 권한을 차등화하여 부여하지 않은 사례

- ▶ 개발 초기 및 설치 시 부여되었던 관리자 권한, 디폴트 권한 등을 일괄 부여 한 경우
- ▶ 회계부서가 영업부서의 화면에 접근한 경우
- ▶ 열람 권한과 다운로드 권한이 분리되지 않아 열람 권한만 부여하여도 다운로드 권한이 자동으로 부여되는 경우
- ▶ 부서 단위로 접근 권한을 부여하여 개인정보 처리 업무를 하지 않는 부서 내 직원도 개인정보를 처리하는 화면에 접근할 수 있는 경우
- ▶ 단순 조회 업무만 담당하는 아르바이트 직원에게 팀 관리자 권한을 부여한 경우

- 개인정보처리시스템의 데이터베이스에 직접 접근할 수 있는 권한은 데이터베이스 운영·관리자에게만 부여하고 개인정보취급자가 허용된 권한 내에서만 데이터베이스를 사용할 수 있도록 접근 권한 및 역할을 세분화하는 등의 안전조치를 적용해야 한다.

- 개인정보처리자가 가명정보를 처리하는 경우, 가명정보에 접근 권한이 있는 담당자가 특정 개인을 알아보기 위한 목적으로 가명정보를 처리하는 것을 방지하기 위하여 가명정보에 접근할 수 있는 담당자와 추가 정보에 접근할 수 있는 담당자를 반드시 구분하여야 한다.
 - 이 경우 가명정보에 접근 권한이 있는 담당자가 특정 개인을 알아보기 위해 사용·결합될 수 있는 정보(추가 정보)에 접근할 수 없도록 역할 및 접근권한을 제한하여야 한다.
 - 가명정보와 추가정보는 물리적으로 분리하여 보관하는 것을 원칙으로 하고, 불가피한 사유로 물리적인 분리가 어려운 경우에는 데이터베이스 테이블 등을 논리적으로 분리하는 것도 가능함(논리적 분리의 경우 보다 엄격한 접근통제를 적용하여야 함).
 - 가명정보와 추가 정보에 대한 접근 권한의 분리가 어려운 정당한 사유가 있는 경우 (소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등), 업무 수행에 필요한 최소한의 접근 권한을 부여하고, 접근 권한의 보유 현황 및 이용 현황을 기록으로 보관하고, 접근 권한 및 이력을 상호 검토, 책임 추적성 확보 등의 보완 통제를 하여야 한다.

② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

- 개인정보취급자의 전보 또는 퇴직, 휴직 등 인사이동이 발생하거나 수탁자와의 계약 변경 또는 종료 등에 따라 개인정보취급자가 변경된 경우에는 지체 없이 해당 개인정보취급자의 계정 또는 접근 권한을 변경·회수하는 등 필요한 조치를 하여야 한다.
- 또한, 조직 변경 또는 조직 내 업무 조정 등으로 개인정보취급자의 업무가 변경되었을 경우에도 지체 없이 해당 개인정보취급자의 계정 또는 접근 권한을 변경·회수하는 등 필요한 조치를 하여야 한다.
- 예를 들어, 퇴사자 발생 시 해당 직원의 계정을 지체 없이 말소하는 조치 등을 내부 관리계획 등에 반영하여 이행하도록 할 수 있다. 또한, 퇴사자 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용자 계정 말소 항목을 반영하여, 개인정보처리 시스템에서 계정이 삭제되었는지 확인하는 절차를 마련해야 한다.
 - 개인정보 처리 업무의 위수탁 관련 계약 사항에 변경이 발생하는 경우에도 개인정보취급자의 개인정보처리시스템에 대한 접근 권한을 변경 또는 말소하여야 한다.

- 개인정보처리자는 불완전한 접근 권한의 변경 또는 말소 조치로 인하여 정당한 권한이 없는 자가 개인정보처리시스템에 접근될 수 없도록 하여야 한다.



접근 권한 변경·말소 미조치 예시

- ▶ 다수 시스템의 접근 권한 변경·말소가 필요함에도 일부 시스템의 접근 권한만 변경·말소할 때
- ▶ 접근 권한의 전부를 변경·말소하여야 함에도 일부만 변경·말소할 때
- ▶ 접근 권한 말소가 필요한 계정을 삭제 또는 접속차단조치를 하였으나, 해당 계정의 인증값 등을 이용하여 우회 접근이 가능할 때 등
- ▶ 취급자 계정을 삭제하지 않고 비밀번호만 초기화하는 경우

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

- 개인정보처리자는 개인정보처리시스템에 대한 접근 권한 부여, 변경, 말소에 대한 내역을 기록하고 해당 기록을 최소 3년간 보관하여야 한다.
- 접근 권한 부여 내역에는 신청자 정보, 신청일시, 승인자 및 발급자 정보, 접근 권한에 관한 정보, 신청 및 발급 사유 등 접근 권한의 발급 과정과 이력 등을 확인할 수 있는 정보를 포함하여 기록하여야 하며, 접근 권한 변경 및 말소 시에도 관련 과정과 이력 등을 확인할 수 있도록 필요한 정보를 포함하여 기록하여야 한다.



접근 권한 내역·보관 기록 예시

번호	사용자ID	사용자명	권한명	권한ID	유형	일자	작업자	사유	...
...									
51503	cskim	김철수	회원관리자	S0002	부여	20190220 10:22:01	gdhong	담당업무 변경	...
51504	yhkim	김영희	상담관리자	C0005	부여	20181210 09:50:33	gdhong	상담팀 입사	...
51505	yhkim	김영희	상담관리자	C0005	말소	20190420 13:55:20	gdhong	퇴사	...
...									



접근 권한 부여·변경·말소 내역 보관 미조치 예시

- ▶ 부서 이동에 따라 개인정보취급자의 업무 변경이 발생하였음에도 권한 변경 이력이 확인되지 않는 경우
- ▶ 개인정보 접근 권한의 내역은 보관하고 있으나, 최근 6개월 치만 보관·관리하고 있는 경우
- ▶ 개인정보 접근 권한의 내역은 보관하고 있으나, 발급·변경 사유 등이 확인되지 않는 경우

④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자별로 계정을 발급하고 다른 개인정보취급자와 공유하지 않도록 하여야 한다.

- 개인정보처리시스템에 접근할 수 있는 계정은 정당한 사유가 없는 한 개인정보취급자별로 발급하고 다른 개인정보취급자와 공유하지 않도록 하여야 한다.
 - ‘정당한 사유’란 개인정보취급자의 계정은 원칙적으로 개별로 발급되어야 하나, 시스템이 제공하는 고정된 계정(root 등)과 같이 기술적으로 개별 발급이 불가능한 경우 등을 말한다.
 - 다만, 정당한 사유에 따라 계정의 개별 발급이 불가능한 경우에도 계정 관리 대장, 접근제어 시스템 도입 등 관리적 또는 기술적 보완통제로써 실제 개인정보처리시스템에 접속한 자를 식별할 수 있도록 하여야 함
- 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 계정을 공유하지 않도록 개인정보취급자별로 ID 등의 계정을 발급하여 사용하도록 하여, 각 개인정보취급자별 개인정보 처리내역에 대한 책임 추적성을 확보하여야 한다.

※ 책임 추적성이란 개인정보 취급에 따른 문제 발생 시 사용자 계정을 기반으로 책임소재를 파악하는 것을 말한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.

- 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체를 인증하기 위하여 스스로의 환경에 맞는 인증수단을 안전하게 적용하고 관리하여야 한다.

- 인증수단은 개인정보보호를 위해 필요한 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용하여야 한다.
- 인증수단은 정당한 접근 권한을 가지지 않은 자가 쉽게 추출하거나 탈취하는 등 비인가자가 접근을 시도하기 어렵도록 적용하고 관리하여야 한다.
- 인증수단은 개인정보처리자 스스로의 환경, 개인정보 보유 수, 정보주체에 미치는 영향 등을 종합적으로 고려하여 자율적으로 정하여 안전하게 적용하여야 한다.



인증수단의 예시

- ▶ 비밀번호 인증: 문자열로 구성된 인증번호를 입력
- ▶ 일회용 비밀번호(OTP) 인증: 한 번의 로그인 시도 또는 거래에 사용하기 위해 무작위로 생성되어 사용자에게 전송된 일회용 인증번호를 입력
- ▶ 생체인증: 홍채, 지문 등의 생체정보를 입력하여 본인 여부를 확인
- ▶ SMS 인증: 본인 명의의 휴대폰에서 문자로 받은 인증번호를 입력
- ▶ 전화 인증: 본인 명의의 휴대폰에서 ARS 안내에 따라 본인 여부를 확인
- ▶ 소셜 로그인: 포털사이트 등에서 제공하는 인증수단을 이용하여 본인 여부를 확인

참 고

- ▶ 비밀번호 등 인증정보의 분실 등을 이유로 재발급을 해야 할 때에는 정당한 사용자인지를 확인할 수 있는 수단(SMS, 이메일 등)을 활용하여 임시 인증정보를 부여하고 이용자가 확인 후 사이트에 접속하여 비밀번호 등 인증정보를 변경하여 사용하도록 한다.

⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리 시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

- 개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 일정 횟수 이상 인증이 실패한 경우 개인정보처리시스템에 접근을 제한하는 등의 필요한 조치를 하여야 한다.

- 인증 실패 횟수는 개인정보처리시스템의 특성, 위험 분석 결과 등을 고려하여 정할 수 있다
(예: 5회 등).
- 일정 횟수 이상 인증에 실패하여 접근이 제한된 개인정보취급자 또는 정보주체에게 개인정보처리시스템에 대한 접근을 재부여하는 경우에는 반드시 정당한 개인정보취급자 또는 정보주체 여부를 확인한 후 접근 제한 해제 등의 조치를 하여야 한다.

제6조 접근통제

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 허가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응
- 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.
- ③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.
- ④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.
- ⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
- ⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리 시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.



해설

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

- 개인정보처리시스템에 대한 불법적인 접근 및 침해사고를 방지하기 위한 접근 제한 기능 및 유출 탐지를 위한 안전조치를 하는 경우에는 아래의 기능을 모두 포함하여야 한다.
 - 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소, 포트(Port), MAC(Media Access Control) 주소 등으로 제한하여 인가받지 않은 접근을 제한하도록 한다(침입차단 기능).
 - 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소, 포트(Port), MAC(Media Access Control) 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지(침입탐지 기능)하고 접근 제한·차단 등 적절한 대응 조치를 하여야 한다.
- 불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 포함하는 안전조치를 실시해야 하며, 침입차단 및 침입탐지 정책 설정, 개인정보처리시스템에 접속한 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요하다.
 - 정책 설정 운영: 신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책(패턴, 임계치 등)을 설정하고 지속적인 업데이트 적용 및 운영·관리하여야 한다.
 - 이상 행위 대응: 모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응하여야 한다.
 - 로그 분석: 로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 및 차단하여야 한다.
 - ※ 로그는 개인정보처리시스템의 접속기록, 네트워크 장비의 로그기록, 보안장비소프트웨어의 기록 등을 포함한다.
- IP 주소 등에는 IP 주소, 포트 그 자체뿐만 아니라, 이상행위(과도한 접속성공 및 실패, 부적절한 명령어 등 패킷)를 포함한다.
- 안전조치의 적용을 위해 상용 시스템을 도입하거나, 공개용 소프트웨어를 사용하거나, 클라우드컴퓨팅서비스 제공자가 제공하는 보안기능 또는 보안서비스를 활용할 수 있다. 다만, 어떠한 안전조치를 선택하더라도 침입 차단 및 탐지 기능이 모두 적용되어야 하며, 적절한 정책 설정 및 운영·관리가 이행되어야 한다.

참고

- ▶ 불법적인 접근: 인가되지 않은 자(내·외부자 모두 포함)가 사용자 계정 탈취, 개인정보 유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말한다.
- ▶ 침해사고: 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다(「정보통신망법」 제2조제1항제7호).



침입차단 및 침입탐지를 위한 안전조치 예시

- ▶ 관련 시스템으로는 침입차단시스템(방화벽), 침입방지시스템(IPS), 침입탐지시스템(IDS), 웹방화벽(WAF), 보안운영체제(Secure OS), 서버접근제어시스템, 데이터베이스 접근제어시스템, 로그분석시스템(ESM, SIEM) 등이 있다.
- ▶ 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List : 접근제어목록) 등 기능을 이용하여 IP 주소 등을 제한함으로써 침입차단 기능을 구현할 수 있다.
- ▶ 인터넷데이터센터(IDC), 클라우드컴퓨팅 서비스, 보안업체 등에서 제공하는 보안서비스, 보안기능 등도 활용할 수 있다.
- ▶ 공개용(무료) 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영할 수 있다. 다만, 공개용(무료) 소프트웨어를 사용하는 경우에는 접근 제한 기능 및 유출 탐지 기능이 모두 충족되는지, 해당 소프트웨어 및 보안정책이 정기적으로 업데이트되는지 등을 사전에 점검하고 설치·운영하여야 한다.

참고

- ▶ 보안제품 등을 도입할 때에는 IT보안인증사무국(<https://www.itscc.kr>)에서 제공하는 인증제품 목록(제품유형: 개인정보보호, 데이터베이스 접근통제, 통합로그관리 등) 등을 활용할 수도 있다.



정책설정 운영 및 이상행위 대응 예시

- ▶ (정책설정) 신규 취약점 또는 침해사고 발생 시 탐지 및 차단 정책(룰) 업데이트를 적용한다.
- ▶ (정책검토) 과도하게 허용되거나 사용되지 않는 정책 등에 대하여 주기적으로 검토 및 조치한다.
- ▶ (이상행위 대응) 비인가 IP 주소, 해외 IP 주소에서의 과도한 또는 비정상적인 접속시도 탐지 및 차단 조치, 개인정보처리시스템에서 과도한 또는 비정상적인 트래픽 발생 시 탐지 및 차단 조치, 크리덴셜 스테핑 공격 등에 따라 로그인 실패 로그가 과도하게 발생할 경우 이에 대한 탐지·분석 및 대응을 한다.

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.

- 인터넷구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 따라 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속해야 하는 경우 안전한 인증수단을 적용하여야 한다.
- 안전한 인증수단: 개인정보처리시스템에 접속한 자에게 부여된 계정 정보와 비밀번호 등을 입력하여 정당한 권한을 부여받은 개인정보취급자인지를 식별·인증하는 절차 이외에 추가적인 인증수단을 적용하는 것을 말한다.



안전한 인증수단의 예시

- ▶ 인증서(PKI, Public Key Infrastructure): 전자상거래 등에서 상대방과의 신원확인, 거래사실 증명, 문서의 위·변조 여부 검증 등을 위해 사용하는 전자서명으로서 해당 전자서명을 생성한 자의 신원을 확인하는 수단을 말한다.
- ▶ 보안토큰: 암호 연산장치 등으로 내부에 저장된 정보가 외부로 복사, 재생성 되지 않도록 인증서 등을 안전하게 보호할 수 있는 수단으로 스마트카드, USB 토큰 등이 해당된다.
- ▶ 일회용 비밀번호(OTP, One Time Password): 무작위로 생성되는 난수를 일회용 비밀번호로 한 번 생성하고, 그 값을 한 번만 사용할 수 있도록 하는 방식을 말한다.

- 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.
- 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 안전한 접속수단 또는 안전한 인증수단 중 하나를 선택하여 적용할 수 있으며, 어떤 수단을 선택하더라도 두 가지 중 한 가지 이상은 반드시 적용하여야 한다.



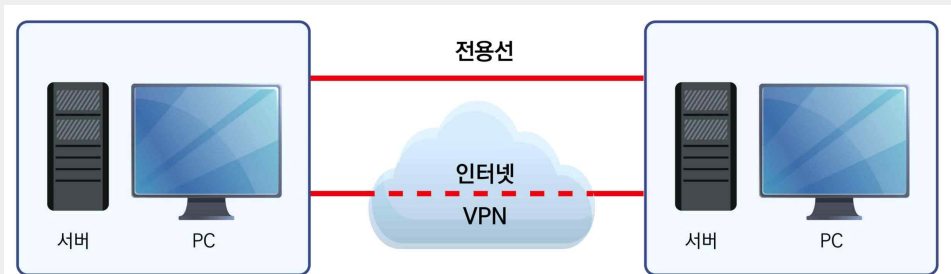
안전한 접속수단의 예시

- ▶ 가상사설망(VPN: Virtual Private Network): 개인정보취급자가 인터넷망 등을 거쳐 개인정보처리 시스템에 원격으로 접속할 때 IPsec이나 SSL 기반의 암호 프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있게 하는 보안 시스템 등을 말한다.

※ IPsec, SSL 등의 기술이 사용된 가상사설망을 안전하게 사용하기 위해서는, 잘 알려진 취약점들을 조치하고 사용해야 하며, 가상사설망을 통해 접속하는 자가 정당한 권한이 있는지를 확인하여야 한다.



가상 사설망 및 전용선 구성 예시



- ③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

- 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 접근통제 등의 안전조치를 하여야 한다.



인터넷 홈페이지 등을 통한 개인정보 유·노출 유형

- ▶ 검색엔진(구글링 등) 등을 통한 개인정보 유·노출
- ▶ 웹 취약점을 통한 개인정보 유·노출

- ▶ 인터넷 게시판을 통한 개인정보 유·노출
- ▶ 홈페이지 또는 모바일앱 등의 설계·구현 오류로 인한 개인정보 유·노출
- ▶ 크리덴셜 스테핑 공격 등으로 인한 개인정보 유출
- ▶ 클라우드 보안설정 미흡으로 인한 개인정보 유·노출
- ▶ 기타 방법을 통한 개인정보 유·노출

- 개인정보처리자는 개인정보의 보유 수, 처리 환경, 정보주체에 미치는 영향 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되 보안대책 마련, 보안 기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 한다.
- 개인정보처리자는 인터넷 홈페이지 운영·관리 시 개인정보 유·노출 방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선 조치를 하여야 한다.



운영 및 관리의 예시

- ▶ 인터넷 홈페이지 등에 보안대책을 정기적으로 검토
- ▶ 홈페이지 게시글, 첨부파일 등에 개인정보 포함 금지, 정기적 점검 및 삭제 등의 조치
- ▶ 서비스 중단 또는 관리되지 않는 홈페이지는 전체 삭제 또는 차단 조치
- ▶ 공격패턴, 위험분석, 침투 테스트 등을 수행하고 발견되는 결함에 따른 개선 조치
- ▶ 취약점을 점검하고 그 결과에 따른 적절한 개선 조치
- ▶ 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL(Uniform Resource Locator)에 대한 점검 및 삭제·차단 조치 등

참고

- ▶ 취약점 점검 항목: Broken Access Control 취약점, Injection 취약점, Security misconfiguration 취약점, Identification and Authentication Failures 취약점, SSRF(Server Side Request Forgery) 취약점 등
- * 취약점 점검 항목은 국가정보원 국가사이버안보센터(NCSC), 행정안전부, 한국인터넷진흥원 보호나라 & KrCERT/CC, OWASP(오픈소스웹애플리케이션보안프로젝트) 등에서 발표하는 항목을 참조하도록 한다.



개인정보 유·노출 방지 조치 예시

- ▶ 홈페이지 주소(URL), 소스코드, 임시 저장 페이지 등에 개인정보 사용 금지
- ▶ 홈페이지에 관리자 페이지의 주소 링크 생성 금지, 관리자 페이지 주소는 쉽게 추측하기 어렵게 생성, 관리자 페이지 노출 금지
- ▶ 엑셀 파일 등 숨기기 기능에 의한 개인정보 유·노출 금지
- ▶ 시큐어 코딩(Secure coding) 도입
- ▶ 취약점을 점검하고 그 결과에 따른 적절한 개선 조치
- ▶ 인증 우회(Authentication bypass)에 대비하는 조치 등
- ▶ 로그인 시도 횟수 증가 시 캡차(CAPTCHA) 적용, 로그인 실패 비율에 대한 임계치 설정 모니터링, 개인정보 페이지 로그인 시 정당한 사용자인지를 확인할 수 있는 수단(SMS, 이메일 등) 활용 등

참고

- ▶ 시큐어 코딩 항목: 입력데이터 검증 및 표현(SQL 삽입 등), 보안기능(부적절한 인가 등), 시간 및 상태 (종료되지 않는 반복문 등), 에러처리(오류 상황 대응 부재 등), 코드오류(해제된 자원 사용), 캡슐화 (잘못된 세션에 의한 정보 노출), API 오용(취약한 API 사용 등), 파라미터 변조 등
- ※ 시큐어 코딩에 관한 세부 내용은 소프트웨어 개발보안 가이드(행정안전부) 등을 참고하도록 한다.

- 인터넷 홈페이지의 설계·개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 인터넷 서비스 검색엔진(구글링 등) 등을 통해 관리자 페이지와 취급 중인 개인정보가 노출되지 않도록 필요한 조치를 한다.



안전한 설계·개발 예시

- ▶ 입력 데이터의 유효성을 검증
- ▶ 인증, 접근통제 등의 보호조치 적용
- ▶ 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성
- ▶ 세션을 안전하게 관리하도록 구성 등

- 인터넷 홈페이지에서 개인정보가 유출될 수 있는 위험성을 줄이기 위하여 정기적으로 웹 취약점 점검을 권고한다.

- 개인정보처리자는 개인정보처리시스템, 개인정보취급자의 컴퓨터, 모바일 기기 등에 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요한 경우에는 권한 설정 등의 조치를 통해 정당한 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 안전조치를 하여야 한다.
 - 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공개 설정된 공유폴더에 개인정보 파일이 포함되지 않도록 정기적인 점검이 필요하다.
 - 원격접속 프로그램을 통해 개인정보취급자 컴퓨터 등에 접속하는 경우도 공유설정에 해당되므로, 정당한 권한이 있는 자만이 접근할 수 있도록 접근통제 조치를 적용하여야 한다.
 - 이 외에도 외부 웹메일, 웹하드, 메신저, 클라우드 저장소, SNS 서비스 등을 통하여 고의 혹은 부주의로 인한 개인정보의 유·노출이 발생하지 않도록 접근통제 등을 해야 한다.



P2P, 공유설정 관련 안전조치 예시

- ▶ 불가피하게 공유설정 등을 할 때에는 비인가자가 접근하지 못하도록 비밀번호 등 접근통제 설정을 하고, 사용이 완료된 후에는 공유설정을 제거
- ▶ 파일 전송이 주된 목적일 때에는 읽기 권한만을 주고 상대방이 쓰기를 할 때만 개별적으로 쓰기 권한을 설정
- ▶ 업무용 컴퓨터 등에 P2P 프로그램, 상용 웹메일, 웹하드, 메신저, SNS 서비스 등의 사용을 금지하여 고의·부주의로 인한 개인정보 유·노출 방지
- ▶ WPA3(Wi-Fi Protected Access 3) 등 보안 프로토콜이 적용된 무선망 이용 등

참 고

- ▶ P2P, 웹하드 등의 사용을 제한할 때에는 단순히 사용금지 조치를 취하는 것이 아니라 시스템상에서 해당 프로토콜이나 IP 주소, 포트 등을 차단하는 등 근본적인 보호조치를 취하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되게 하는 등 필요한 조치를 하여야 한다.

- 개인정보처리자는 개인정보처리시스템의 불법적인 접근 및 침해사고를 방지하기 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 시스템 접속이 차단되게 하는 등 접속 제한에 필요한 조치를 취하여야 한다.
 - 접속차단 조치란 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속을 차단하는 것을 의미하며, 개인정보처리시스템과 연결이 완전히 차단되어 정보의 송수신이 불가능한 상태가 되어야 한다. 업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않는다.
 - 개인정보처리자는 개인정보를 처리하는 방법 및 환경, 보안위험요인, 업무특성 (데이터베이스 운영·관리, 시스템 모니터링 및 유지보수 등) 등을 고려하여 스스로의 환경에 맞는 최대 접속가능 시간을 정하여 시행할 수 있다.
 - 최대 접속가능 시간은 통상적인 수준(10분~60분 이내)에서 정할 수 있으며, 개인정보처리시스템 정기 점검 등 특별한 상황에서 장시간 접속이 필요한 때에는 사유 및 접속기간 등 그 기록을 보관·관리하고, 작업 종료 등에 따라 장시간 접속이 불필요해진 경우에는 다시 원래의 시간으로 복원하여야 한다.
- 개인정보취급자가 일정시간 이상 업무처리를 하지 않아 개인정보처리시스템에 접속이 차단된 이후, 다시 접속하고자 할 때에는 그 방법·절차 등이 최초의 접속 방법·절차 등과 동일한 수준 이상이 되도록 조치를 취하여야 한다.



접속 차단 미조치 예시

- ▶ 개인정보처리시스템에 접속 차단 등의 조치 없이 업무용 컴퓨터에 화면보호기만을 설정한 때
- ▶ 개인정보처리시스템 등에 다시 접속 시 자동 로그인 기능을 사용한 때
- ▶ 서버접근제어 프로그램 등을 이용하여 개인정보처리시스템에 별도의 로그인 절차 없이 접속이 가능하도록 구성하면서 해당 프로그램에 접속 차단 조치를 하지 않은 때
- ▶ 개인정보처리시스템 개편 작업을 위해 예외적으로 접속차단 조치 적용대상 시간을 장시간으로(24시간 등) 연장한 후, 개편 작업이 종료되었음에도 불구하고 접속차단 조치 적용대상 시간을 장시간으로 유지하고 있을 때

⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

- 개인정보처리자의 업무용 모바일 기기는 성능 및 처리 속도가 향상되어 대량의 개인정보 처리에 활용되고 있으나, 이동성·휴대성 등으로 인하여 기기가 분실·도난된 경우에는 해당 기기를 통하여 개인정보처리시스템에 접속하지 못하도록 조치하거나 기기에 저장된 개인정보가 유출되지 않도록 비밀번호 설정 등의 안전조치를 하여야 한다.



화면 잠금설정 예시

- ▶ 비밀번호, 패턴, PIN, 지문, 홍채 등을 사용하여 화면 잠금 설정
 - ▶ 디바이스 암호화 기능을 사용하여 애플리케이션, 데이터 등 암호화
 - ▶ USIM 카드에 저장된 개인정보 보호를 위한 USIM 카드 잠금 설정
 - ▶ 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제
 - ▶ 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등
- ※ MDM은 무선망을 이용해 원격으로 스마트폰 등의 모바일 기기를 제어하는 솔루션으로서, 분실된 모바일 기기의 위치 추적, 잠금 설정, 정보 삭제, 특정 사이트 접속 제한 등의 기능 제공

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보 취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리 시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.

- 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상(제공하는 정보통신서비스가 다수일 때에는 전체를 합산하여 적용) 개인정보처리자는 인터넷망 차단 조치를 하여야 한다.

- ‘이용자’란 정보통신망법에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 뜻한다.
- 다만, 이 기준에 따른 인터넷망 차단 조치를 해야 하는 개인정보처리자가 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 클라우드컴퓨팅서비스에 대한 접속 외에 다른 인터넷의 접속을 차단하는 경우 이 기준에서 정하는 인터넷망 차단 조치를 이행한 것으로 본다.
- 클라우드 서버에 개인정보처리시스템을 설치·운영하는 경우(IaaS), 클라우드서비스가 제공하는 개인정보 처리 응용프로그램(고객관계관리, 인사회계 등)을 이용하는 경우(SaaS), 클라우드 사업자가 제공하는 DBMS 등을 이용하여 개인정보처리시스템을 구축·운영하는 경우(PaaS) 등이 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에 해당될 수 있다



클라우드컴퓨팅서비스 이용 시 인터넷망 차단 조치 예시

- ▶ 클라우드컴퓨팅서비스를 개인정보처리시스템으로 이용하는 경우 해당 시스템에 대한 접근 권한을 관리 콘솔에서 부여 또는 변경할 수 있거나 관리 콘솔에서 다운로드할 수 있다면, 관리 콘솔 및 관리 콘솔에 접근하는 컴퓨터 등도 인터넷망 차단 조치의 대상이 될 수 있다.

- 물리적 인터넷망 차단조치: 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리하는 방식이다.
- 논리적 인터넷망 차단조치: 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 인터넷 접속이 불가능한 내부 업무영역과 인터넷 접속영역을 분리하는 방식이다.

참 고

- ▶ 정보통신서비스 제공자들은 스스로의 환경에 맞는 인터넷망 차단 조치를 적용하여 개인정보를 처리하는 과정에서의 외부와의 접점을 최소화함으로써 외부로부터 들어오는 공격이나 내부에서 외부로의 개인정보 유출 등을 차단하여야 한다.

- 이 기준에 해당하는 개인정보처리자가 인터넷망 차단 조치를 적용해야 하는 대상은 다음과 같다.

- 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 개인정보취급자의 컴퓨터 등
- 개인정보처리시스템에서 개인정보를 파기할 수 있는 개인정보취급자의 컴퓨터 등
- 개인정보처리시스템에 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등

참 고

- ▶ 다운로드: 개인정보처리시스템에 직접 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일 형태로 저장하는 것을 말한다.
- ▶ 파기: 개인정보처리시스템에 저장된 개인정보, 레코드, 테이블 또는 데이터베이스를 삭제하는 것을 말한다.
- ▶ 접근 권한 설정: 개인정보처리시스템에 접근하는 개인정보취급자에게 다운로드, 파기 등의 접근 권한을 설정하는 것을 말한다.

제7조 개인정보의 암호화

제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)
 - 가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
 - 나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보 처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.



해설

① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

- 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 데이터베이스, 파일 등으로 저장하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
 - ‘인증정보’란 비밀번호, 생체인식정보 등 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는 데 사용하는 정보를 말한다.
- 개인정보처리자는 인증정보 중 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
 - 일방향 암호화는 개인정보취급자 및 정보주체 등이 입력한 비밀번호를 평문 형태가 아닌 해시함수 등을 통해 비가역적으로 암호화한 값으로 저장하는 것을 말한다.
 - ※ 개인정보처리자는 비밀번호 일방향 암호화 시 무작위 대입공격, 레인보우 테이블 공격 등에 대응하기 위한 수단으로 솔트값 추가 등을 고려할 수 있다.
- 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 정보통신망을 통하여 송수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
 - ‘정보통신망’은 내부망과 외부망(인터넷망 등)을 포함한 모든 통신망을 의미하므로, 내부망에서 인증정보를 송수신하는 경우에도 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
 - 송수신 시 암호화 방법으로는 통신구간 암호화 프로토콜(SSL/TLS 등), 응용프로그램을 통한 암호화 전송 등의 방법을 사용할 수 있다.

참고

- ▶ API Access Key 등 프로그램 방식 액세스 자격 증명에 이용되는 인증정보는 이 기준에서 언급하는 비밀번호로 간주하지는 않으나, 안전한 관리방안을 수립해 이용해야 한다.



사용을 권장하는 안전한 암호 알고리즘의 예시

구분	미국(NIST)	일본(CRYPTREC)	유럽(ECRYPT)	국내
일방향 암호 알고리즘	SHA-224/256 /384/512	SHA-256/384/512	SHA-224/256/384 /512 Whirlpool	SHA-224/256/384 /512
대칭키 암호 알고리즘	AES-128/192/256)	AES-128/192/256 Camellia-128/192/ 256	AES-128/192/256 Camellia-128/192/ 256 Serpent-128/192/ 256	SEED, HIGHT ARIA-128/192/256 LEA-128/192/256
공개키 암호 알고리즘 (메시지 암-복호화)	RSA (사용 권고하는 키길이 확인 필요)	RSAPES-OAEP	RSAPES-OAEP	RSAPES
(키 길이 2048bits 이상)				

- ▶ 국내외 암호 연구 관련 기관에서 대표적으로 다루어지는 권고 암호 알고리즘만 표시
※ TDEA(TDES), MD5, SHA-1 등 보안강도가 낮은 것으로 판명된 암호 알고리즘을 사용하여서는 안 됨
- ▶ 처리속도 등 기술발전에 따라 사용 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용 시 국내외 암호 관련 연구기관에서 제시하는 최신 정보 확인 필요
- ▶ 국내 암호 관련 기관은 본 안내서 부록 제4장 암호화 조치 관련 참고 웹사이트에서 확인 가능

② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

- 개인정보처리자는 이용자의 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보 등 개인정보에 대해서는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용을 권고하는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

- 따라서 이 기준에 따른 암호화 조치를 이행하여야 하는 자는 이용자의 개인정보를 처리하는 개인정보처리자에 해당된다.

- 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에 클라우드에 저장하는 개인정보에 대해서는 클라우드컴퓨팅서비스 제공자가 제공하는 암호화 기능을 이용하여 암호화 조치를 이행할 수 있다. 다만, 해당 클라우드컴퓨팅서비스 제공자가 제공하는 암호화 기능이 이 기준에 부합하는 조치인지에 대해서는 확인이 필요하다.

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

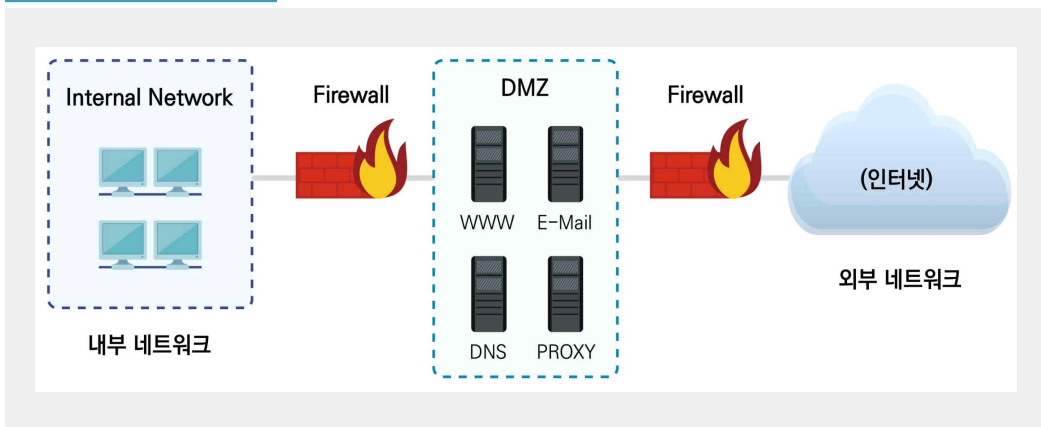
1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)
 - 가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
 - 나. 암호화 미적용시 위험도 분석에 따른 결과

- 인터넷망 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)은 외부에서 직접 접근이 가능하여 외부자의 침입을 받을 가능성이 있으므로 개인정보처리자가 이용자가 아닌 정보주체의 고유식별정보를 인터넷망 구간과 DMZ에 저장하는 경우, 암호화하여야 한다.
- 한편, 내부망에 이용자가 아닌 정보주체의 주민등록번호 외의 고유식별정보를 저장하는 경우에는 공공기관은 개인정보 영향평가의 결과, 그 외에는 암호화 미적용 시 위험도 분석에 따른 결과에 따라 암호화의 적용여부 및 적용범위를 정할 수 있다.

용 어	정 의
인터넷 영역	• 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간을 의미한다.
DMZ 영역	• 인터넷망 구간과 내부망 사이에 위치한 중간 지점 또는 인터넷망 구간 사이에 위치한 중간 지점으로서 인터넷망 구간에서 직접 접근이 가능한 영역을 말한다. (침입차단시스템 등으로 접근 제한 등을 수행하는 경우에도 해당)
내부망	• 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.



DMZ 구간의 예시



- 인터넷 구간이나 DMZ 구간은 외부에서 직접 접근이 가능하므로 외부자의 침입을 받을 가능성이 있다. 따라서 DMZ 구간에 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등의 고유식별정보를 저장하는 경우 암호화하여 저장해야 한다. 제1항에 따른 비밀번호 및 생체인식정보를 저장하는 경우에도 암호화하여 저장해야 한다.
- 주민등록번호는 법 제24조의2, 같은 법 시행령 제21조의2에 따라 암호화하여야 하는 대상으로, 내부망에 주민등록번호를 저장하는 경우에도 “개인정보 영향평가”나 암호화 미적용 시 “위험도 분석”의 결과에 관계없이 암호화하여야 한다.

「개인정보 보호법」

제24조의2(주민등록번호 처리의 제한) ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

「개인정보 보호법 시행령」

제21조의2(주민등록번호 암호화 적용 대상 등) ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

③ 보호위원회는 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

- 내부망에 주민등록번호를 제외한 고유식별정보를 저장하는 경우에는 다음에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
 - 법 제33조 및 시행령 제35조에 따라 영향평가의 대상이 되는 개인정보파일을 운용하는 공공기관은 해당 “개인정보 영향평가”의 결과
 - 공공기관 이외의 개인정보처리자는 암호화 미적용 시 “위험도 분석”에 따른 결과

「개인정보 보호법」

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다.

「개인정보 보호법 시행령」

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 “대통령령으로 정하는 기준에 해당하는 개인정보 파일”이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별 정보의 처리가 수반되는 개인정보파일

2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 “영향평가”라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.



참고자료

개인정보 영향평가 수행 안내서, 개인정보 위험도 분석 기준 해설

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

- 개인정보처리자는 정보주체의 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송수신하는 경우에는 안전한 암호 알고리즘으로 암호화하여야 한다.
 - 안전한 암호 알고리즘으로 암호화하기 위해 국내외 연구기관에서 권장하는 암호 알고리즘을 활용할 수 있다.
- 개인정보처리자의 보유한 개인정보의 수, 처리 환경 등을 고려하여 필요하다고 판단되는 경우에는 보안서버 구축 등의 조치를 할 수 있으며, SSL 인증서, 응용프로그램 등을 이용한 보안서버 등을 활용할 수 있다.
 - SSL 인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화하여 전송하는 방식이다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

- 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

- 이용자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자로, 서비스의 이용 관계에 있는 자로 한정된다. 따라서 이 기준에 따른 암호화 조치를 이행하여야 하는 자는 ‘이용자의 개인정보’를 처리하는 개인정보처리자에 해당된다.
- 또한, ‘이용자가 아닌 정보주체의 고유식별정보, 생체인식정보’를 처리하는 자는 이 기준에 따라 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.
- 개인정보처리자가 개인정보취급자의 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 컴퓨터, 모바일 기기에 내려받아 저장하는 경우에 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 통해 해당 파일을 암호화하여 불법적인 유·노출 및 접근 등을 막을 수 있다.
- 개인정보의 저장 형태가 오피스 파일 형태일 때에는 해당 프로그램에서 제공하는 암호 설정 기능을 활용할 수 있다.

참 고

▶ 암호화 적용 기준 요약

구분		「개인정보 보호법」에 따른 암호화 대상 개인정보	
		이용자가 아닌 정보주체	이용자
정보통신망을 통한 송·수신 시	인터넷망	개인정보	
	정보통신망	인증정보(비밀번호, 생체인식정보 등)	
저장 시	저장 위치 무관	주민등록번호	
		인증정보(비밀번호, 생체인식정보 등) ※ 단, 비밀번호는 일방향암호화	
		-	여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보
	인터넷망 구간, DMZ	고유식별정보	-
	내부망	고유식별정보 ※ 단, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 영향평가 또는 위험도 분석을 통해 암호화 적용여부 및 범위를 정할 수 있음	
개인정보취급자 컴퓨터, 모바일기기, 보조저장매체 등에 저장 시		고유식별정보, 생체인식정보	개인정보

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

- 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호 키를 안전하게 사용 및 관리하기 위한 키 관리 절차를 수립·시행하여야 한다.



TIP

- '대기업'이란 「독점규제 및 공정거래에 관한 법률」 제31조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
- '중견기업'이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
- '중소기업'이란 「중소기업기본법」 제2조에 해당하는 기업을 말한다.

- 암호 키는 암호화된 데이터를 복호화할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며, 라이프사이클 단계별 암호 키 관리 절차를 수립·시행하여야 한다.



암호키 관리 절차 예시

1. 준비 단계: 암호 키가 사용되기 이전의 단계

- 암호 키 생성
 - 암호 키 생성에 필요한 난수는 안전한 난수발생기(RNG)를 이용하여 생성
 - 비대칭키 알고리즘 키 생성 방식: 디지털 서명을 위한 키 쌍 생성, 키 설정을 위한 키 쌍 생성
 - 대칭키 알고리즘 방식: 미리 공유된 키, 비밀번호, 다수의 암호 키를 이용한 키 생성 등
- 암호 키 분배
 - 대칭키 알고리즘 키 분배 방식: 수동적 키 분배, 자동화된 키 전송 등
 - 비대칭키 알고리즘의 키 분배 방식
 - 기타 키 자료 생성 및 분배 방식: 영역 파라미터, 초기값, 공유된 비밀, RNG 시드, 다른 공개 및 비밀정보, 중간값, 난수, 비밀번호 등

2. 운영 단계: 암호 키가 암호 알고리즘 및 연산에 사용되는 단계

- 암호 키의 유효기간 동안 사용되는 키 자료들은 필요에 따라 장비 모듈에 보관하거나 별도의 저장 매체에 보관하여 저장해야 함
- 암호 키는 하드웨어 손상 또는 소프트웨어 오류 등의 사유로 손상될 가능성이 있으므로 가용성 보장을 위해서는 키 백업 및 키 복구 등이 가능해야 함
- 암호 키가 노출되거나 노출의 위험이 있는 경우 그리고 암호키 유효기간의 만료가 가까워지는 경우에는 암호 키를 다른 암호키로 안전하게 변경해야 함

3. 정지 단계: 암호 키가 더 이상 사용되지 않지만, 암호 키에 대한 접근은 가능한 단계

- 암호 키 보관 및 복구
 - 암호 키는 수정이 불가능한 상태이거나 새로운 보관 키를 이용하여 주기적으로 암호화
 - 운영 데이터와 분리되어 보관하며, 암호 정보의 사본들은 물리적으로 분리된 곳에 보관
 - 암호 키는 응용프로그램의 소스 프로그램 내에 평문으로 저장 금지
 - 암호화되는 중요한 정보에 대한 보관키는 백업되어야 하며, 사본은 다른 곳에 보관 등
- 모든 개인 키나 대칭 키의 복사본이 더 이상 필요하지 않다면 즉시 파기하여야 함
- 암호 키 손상 시 유효기간 내에 키 자료를 제거하고, 보안 도메인에 속해 있는 실체의 권한을 삭제하여 말소된 실체의 키 자료의 사용을 방지해야 함

4. 폐기 단계: 암호 키가 더 이상 사용될 수 없는 단계(폐기 또는 사고 상태)

- 일반적으로 폐기 단계의 키 자료에 대한 모든 기록은 삭제(다만, 일부기관에서는 감사를 목적으로 특정 키 속성 유지가 필요할 수도 있음)
- 폐기 상태의 암호 키와 사고 상태의 암호 키들의 특성에 대한 기록 유지 등

제8조 접속기록의 보관 및 점검

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.



해설

① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역 등의 접속기록을 1년 이상 보관·관리하여야 한다.
- 다만, 고유식별정보 또는 민감정보를 처리하거나 대량의 개인정보를 처리하는 경우 개인정보 유출 등으로 인한 피해 가능성이 매우 높으므로 다음의 개인정보취급자가

개인정보처리시스템에 접속하여 처리한 업무내역 등의 접속기록은 최소 2년 이상 보관·관리하여야 한다.

- 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
- 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
- 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우



- 민감정보란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 유전자검사 등의 결과로 얻어진 유전정보, 범죄경력자료, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보에 해당하는 정보를 말한다.
- 고유식별정보란 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다.

전기통신사업법

제5조(전기통신사업의 구분 등) ① 전기통신사업은 기간통신사업 및 부가통신사업으로 구분한다.

- ② 기간통신사업은 전기통신회선설비를 설치하거나 이용하여 기간통신역무를 제공하는 사업으로 한다.
- ③ 부가통신사업은 부가통신역무를 제공하는 사업으로 한다.

- 접속기록에는 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등의 사항을 모두 포함하여 기록하고, 처리한 정보주체 정보와 관련된 사항에는 민감하거나 과도한 개인정보가 저장되지 않게 하여야 하며, 필요시 이 기준에 따라 암호화해야 한다.

필수 기록 항목	설 명
① 식별자	• 개인정보처리시스템에서 접속한 자를 식별할 수 있도록 부여된 ID 등 식별자
② 접속 일시	• 개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점 (년-월-일, 시:분:초)
③ 접속지 정보	• 개인정보처리시스템에 접속한 자의 컴퓨터, 모바일기기 등 단말기 정보 또는 서버의 IP 주소 등 접속 주소

필수 기록 항목	설 명
④ 처리한 정보주체 정보	<ul style="list-style-type: none"> 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보(ID, 고객번호, 학번, 사번 등)
⑤ 수행 업무	<ul style="list-style-type: none"> 개인정보처리시스템에 접속하는 자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보(검색, 열람, 조회, 입력, 수정, 삭제, 출력, 다운로드 등)

- 가명정보를 처리하는 경우 추가 정보의 사용 없이는 정보주체를 식별할 수 없으므로 가명 처리된 데이터를 식별할 수 있는 가명정보ID, 일련번호 등이 있다면 ‘처리한 정보주체 정보’ 항목으로 해당 정보를 기록하여야 하며, 가명처리된 데이터를 구별할 수 있는 정보가 없는 경우는 ‘처리한 정보주체 정보’ 항목을 남기지 않을 수 있다.
- 검색조건문(쿼리)을 통해 대량의 개인정보를 처리했을 경우 해당 검색조건문을 정보주체 정보로 기록할 수 있으나, 이 경우 데이터베이스 테이블 변경 등으로 책임 추적성 확보가 어려울 수 있으므로 해당시점의 데이터베이스를 백업하는 등 책임 추적성 확보를 위해 필요한 조치를 취하여야 한다.



검색조건문(쿼리)의 예시

- ▶ ‘김’씨 성을 가진 회원을 조회하는 경우
 - 정보주체의 정보: `SELECT * FROM student WHERE name LIKE ‘김%’;`
 ※ name: 학생이름(컬럼), student: 학생정보(테이블)
- ▶ 영화를 연간 50회 이상 관람한 고객에게 VIP 등급부여
 - 정보주체의 정보: `UPDATE member SET membership=‘VIP’ WHERE movie_count_per_year=50;`
 ※ member: 회원정보(테이블), membership: 고객정보(컬럼), movie_count_per_year: 연간 영화관람 건수(컬럼)



접속기록 항목의 예시

- ▶ 식별자: A0001(개인정보취급자 식별정보)
- ▶ 접속일시: 2024-01-01, 15:00:00
- ▶ 접속지 정보: 192.168.10.9(접속한 자의 IP 주소)
- ▶ 처리한 정보주체 정보: CLI060719(정보주체를 특정하여 처리한 경우 정보주체의 식별정보)

▶ 수행업무: 연락처 조회 등

※ 위 정보는 반드시 기록하여야 하며 개인정보처리자의 업무환경에 따라 책임 추적성 확보에 필요한 항목은 추가로 기록할 필요가 있다.

- 개인정보처리자는 최소 보관기간 이후에도 접속기록을 즉시 삭제하지 않고 책임 추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부 관리계획에 보관기간을 정하고 이를 이행하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

- 개인정보처리자는 개인정보의 오남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록이 위·변조되지 않도록 접속기록을 월 1회 이상 정기적으로 점검하여야 한다. 점검 시 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제, 출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있다.
- 개인정보처리자는 개인정보처리시스템 운영 부서에서 접속기록 점검을 자체적으로 하게 하거나 특정부서가 여러 개의 개인정보 처리시스템을 통합하여 점검할 수 있다.



접속기록 내 비정상 행위 예시

- ▶ 식별자: 접근 권한이 부여되지 않은 계정 혹은 사용이 중지된 계정으로 접속한 행위 등
- ▶ 접속일시: 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외에 접속한 행위 등
- ▶ 접속지 정보: 인가되지 않은 단말기 또는 지역(IP 주소)에서 접속한 행위 등
- ▶ 처리한 정보주체 정보: 특정 정보주체에 대하여 과도하게 조회, 다운로드 등의 행위 등
- ▶ 수행업무: 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등
- ▶ 그 밖에 짧은 시간에 하나의 계정으로 여러 지역(IP 주소)에서 접속한 행위 등

- 특히, 개인정보처리시스템에 접근하여 개인정보를 다운로드한 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 확인하고, 개인정보취급자가 개인정보의 오남용이나 유출을 목적으로 다운로드한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다.
- 다운로드 사유의 확인이 필요한 기준은 개인정보처리자가 개인정보처리시스템의 운영 환경 등을 고려하여 자율적으로 수립할 수 있으며, 다운로드한 정보주체의 수, 일정기간 내 다운로드 횟수, 업무시간 외 다운로드 수행 사유 등을 포함할 수 있다.



- 다운로드란 개인정보처리시스템에 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일 형태로 저장하는 것을 말한다.

③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

- 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 접속기록을 안전하게 보관·관리하여야 한다. 접속기록을 보관·관리하기 위한 보호조치로 아래와 같은 방법을 활용할 수 있다.
 - 상시적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 저장장치에 보관 가능
 - 접속기록에 대한 위·변조를 방지하기 위해서는 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 정보를 별도의 장비에 보관·관리
 - ※ 접속기록에 대한 위·변조를 방지하기 위해서는 접속기록을 별도 저장매체에 보관하고, 위·변조 여부를 확인할 수 있는 정보(MAC 값, 전자서명 값 등)는 별도 저장매체 또는 관리대장에 보관하는 방법 등으로 관리할 수 있다.
 - 그 외 다양한 접속기록 위·변조 방지 기술 적용 가능
- 특히, 개인정보처리시스템의 접속기록은 임의적인 수정·삭제 등이 불가능하도록 접근 권한을 제한하는 등의 안전조치를 하여야 한다.

제9조 악성프로그램 등 방지

제9조(악성프로그램 등 방지) ① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
 2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
- ② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.



해설

① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

- 개인정보처리자는 악성프로그램(바이러스, 웜, 랜섬웨어, 스파이웨어, 웹셀 등) 등을 통해 개인정보가 위·변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 보안 프로그램을 설치·운영하여야 한다.
- 보안 프로그램은 그 목적과 기능에 따라 다양한 종류의 제품이 있으므로, 개인정보처리자는 스스로의 환경에 맞는 보안 프로그램을 설치하도록 한다.

참고

- ▶ 불법 또는 인가되지 않은 보안 프로그램 사용 시, 악성 프로그램 침투 경로로 이용되거나 보안 취약점 제거를 위한 업데이트 지원을 받지 못하여 개인정보 유출 사고가 발생할 수 있으므로 정품 소프트웨어만을 사용해야 한다.

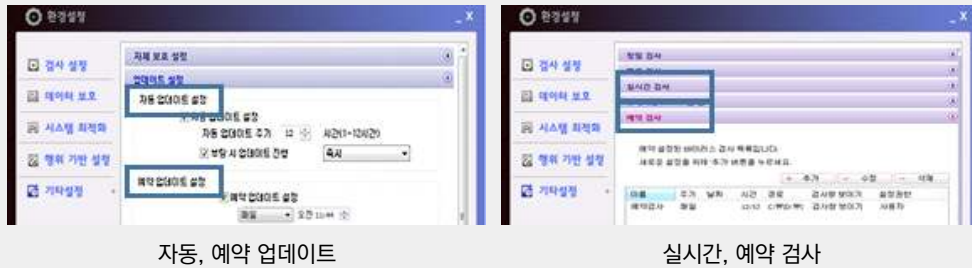
- 개인정보처리자는 설치한 보안 프로그램을 적절하게 운영하여야 한다.
 - 보안 프로그램 설치 후, 최신 상태의 보안 업데이트 적용
 - 보안 프로그램의 정책·환경 설정 등을 통해 사내의 보안정책을 적용
 - 보안 프로그램을 통해 발견되는 악성 프로그램 등 확산 방지 조치(삭제·치료, 물리적 차단·분리 등)
 - 웹서버나 파일서버 등 외부에서 파일 업로드 시 파일 내용을 검사하여 악성 코드가 포함되어있는지를 검사하고 감염을 예방할 수 있도록 개인정보처리시스템에 조치
- 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우 해당 클라우드컴퓨팅서비스제공자가 지원하는 기능을 이용하여 보안 프로그램에 필요한 조치를 할 수 있다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지

- 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램은 실시간 감시 등을 위해 항상 실행된 상태를 유지해야 한다.
- 보안 프로그램은 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지해야 한다.
 - 실시간으로 신종·변종 악성 프로그램이 유포됨에 따라 백신 상태를 최신의 업데이트 상태로 적용하여 유지해야 한다.
 - 특히 대량의 개인정보를 처리하거나 민감한 정보 등 중요도가 높은 개인정보를 처리하는 경우에는 키보드 해킹, 메모리해킹, 랜섬웨어 등 신종 악성 프로그램에 대해 대응할 수 있도록 보안 프로그램을 운영할 필요가 있으며, 항상 최신의 상태로 유지하여야 한다.

참고

▶ 백신 소프트웨어 설정 예시



- 다만, 보안 프로그램의 패치 오류 검증, 무결성 검증 등이 필요하여 보안 프로그램 업데이트를 즉시 적용하기 어려운 경우 등 ‘정당한 사유가 있는’ 경우에는 프로그램의 업데이트에 필요한 조치를 확인한 후 즉시 실시하여야 한다.

2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

- 개인정보처리자는 보안 프로그램을 설치·운영하여 발견된 바이러스, 웜, 랜섬웨어, 스파이웨어, 웹셀 등의 악성프로그램 등에 대해 삭제, 치료 등의 대응 조치를 하여야 한다.
- 발견된 악성프로그램에 대해 보안 프로그램에서 삭제, 치료 등의 기능을 지원하지 않는 경우에는 개인정보처리시스템, 개인정보취급자의 컴퓨터 등을 분리하는 등 악성프로그램의 확산 방지를 위한 적절한 안전조치를 취하여야 한다.

② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

- 운영체제(OS)·응용 프로그램의 보안 취약점을 악용하는 악성 프로그램 경보가 발령되었거나, 응용 프로그램, 운영체제 소프트웨어의 제작업체에서 보안 업데이트, 조치방안 등의

공지가 있는 경우에는 악성프로그램의 감염을 예방하고 감염된 경우 피해를 최소화하기 위해 정당한 사유가 없는 한 즉시 업데이트를 실시하여야 한다.

- ‘정당한 사유가 없는 한 즉시’란 현재 운영 중인 응용프로그램과의 업무연속성, 시스템에 미칠 영향 등을 고려하여 적용하기까지 소요되는 합리적인 시간을 의미한다.

참 고

- ▶ 한컴 오피스, MS 오피스 등 개인정보 처리에 자주 이용되는 응용 프로그램은 자동업데이트를 설정하면 보안 업데이트 공지에 따른 즉시 업데이트가 용이하다.

- 개인정보처리시스템 등에 대한 보안 업데이트 적용 사항, 적용 일자 등 설치·변경·제거 사항을 기록하는 등 형상관리를 통해 관리체계를 강화할 수 있다.
- 사이버위기 경보 단계 및 보안 업데이트 공지 여부를 지속적으로 확인하여 보안 업데이트 적용 시점 및 방법 등을 검토하고 적용하여야 한다.

참 고

- ▶ 응용 프로그램, 운영체제 소프트웨어의 제작업체에서 제공하는 보안 업데이트 공지를 우선 활용하되, 한국인터넷진흥원이 운영하는 인터넷 보호나라&KrCERT/CC(<https://www.boho.or.kr>)에서 제공하는 ‘보안공지’ 등도 활용할 수 있다.

제10조 물리적 안전조치

제10조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.



해설

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 비인가자의 출입 등으로 인한 개인정보의 유출 등을 방지하기 위해 출입통제 절차를 수립·운영하여야 한다.



출입통제 절차 예시

- ▶ 출입 요청 및 승인: 전산실, 자료보관실 등에 '출입 신청서'를 작성하여 개인정보 보호책임자 또는 전산실, 자료보관실 등 운영·관리책임자의 승인 등
- ▶ 출입 기록 작성: 출입에 관한 사항을 '출입 관리대장'에 기록하고 해당 업무 관계자가 이를 확인 등
- ▶ 출입 기록 관리: 정상·비정상적인 출입 여부, 장비 반입·반출의 적정성 등을 정기적으로 검토 등

- 출입을 통제하는 방법으로는 물리적 접근 방지를 위한 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하는 방법 등이 있다.

- 물리적 접근 방지를 위한 장치(예시): 비밀번호 기반 출입통제 장치, 스마트 카드 기반 출입 통제장치, 지문 등 바이오정보 기반 출입통제 장치 등
- 수기문서 대장 기록 방법(예시): 출입자, 출입일시, 출입목적, 소속 등



출입 신청서 및 관리대장 작성 예시

- ▶ 출입 신청서: 소속, 부서명, 신청자, 연락처, 출입일자, 입실·퇴실시간, 출입목적, 작업내역 등
- ▶ 출입 관리대장: 출입일자, 입실·퇴실시간, 출입자 정보(소속, 성명, 연락처), 출입목적, 승인부서, 입회자 정보(성명 등), 승인자 서명 등

참 고

- ▶ 전산실은 다량의 정보시스템을 운영하기 위한 별도의 물리적인 공간으로 전기시설(UPS, 발전기 등), 공조시설(항온항습기 등), 소방시설(소화설비 등)을 갖춘 시설을 말한다.
- ▶ 자료보관실은 가입신청서 등의 문서나 DAT(Digital Audio Tape), LTO(Linear Tape Open), DLT(Digital Linear Tape), 하드디스크, SSD(Solid State Drive) 등이 보관된 물리적 저장장소를 말한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

- 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체(이동형 하드디스크, USB메모리, 외장형 SSD 등) 등은 금고, 잠금장치가 있는 캐비닛 등 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

- 개인정보처리시스템을 운영하는 개인정보처리자는 이동형 하드디스크, USB메모리 등의 보조저장매체를 통해 개인정보가 유출되지 않도록 개인정보가 저장된 보조저장매체의 반출·입 통제를 위해 보안대책을 마련하여야 한다.

- 다만, 별도의 개인정보처리시스템을 운영하지 않고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 보조저장매체의 반출·입 통제 보안대책을 마련하지 않을 수 있다.



보조저장매체 반출·입 통제 시 고려사항 예시

- ▶ 보조저장매체 보유 현황 파악 및 반출·입 관리 계획
- ▶ 개인정보취급자 및 수탁자 등에 의한 개인정보 유출 가능성
- ▶ 보조저장매체의 안전한 사용 방법 및 인가되지 않은 사용의 대응조치
- ▶ USB를 컴퓨터에 연결 시 바이러스 점검을 디폴트로 설정하는 등 기술적 안전조치 방안 등

제11조 재해·재난 대비 안전조치

제11조(재해·재난 대비 안전조치) 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.

1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검
2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련



해설

10만명 이상의 정보주체에 관한 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관한 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.

- 10만명 이상의 정보주체에 관한 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관한 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템을 보호하기 위한 조치를 하여야 한다.
- 재난이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것을 말하며, 재해란 재난으로 인하여 발생하는 피해를 말한다.

재난 및 안전관리 기본법

제3조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “재난”이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것으로서 다음 각 목의 것을 말한다.
 - 가. 자연재난: 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 한파, 낙뢰, 가뭄, 폭염, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 소행성·유성체 등 자연우주물체의 추락·충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해

나. 사회재난: 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방사고·환경오염사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 국가핵심기반의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산, 「미세먼지 저감 및 관리에 관한 특별법」에 따른 미세먼지 등으로 인한 피해

자연재해 대책법

제2조(정의) 이 법에서 사용하는 뜻과 정의는 다음과 같다.

1. “재해”란 「재난 및 안전관리 기본법」(이하 “기본법”이라 한다) 제3조제1호에 따른 재난으로 인하여 발생하는 피해를 말한다.

1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검

- 개인정보처리자는 재해·재난 발생 시 개인정보의 손실 및 훼손 등을 방지하고 개인정보 유출사고 등을 예방하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 문서화하고 이에 따라 대처하여야 한다.
- 또한, 개인정보처리자는 대응절차의 적정성과 실효성을 보장하기 위하여 정기적으로 이를 점검하여야 한다.
 - 대응절차를 정기적으로 점검하여 대응절차에 변경이 있는 경우에는 변경사항을 반영하는 등 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후, 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다.
 - 대응절차의 실효성을 판단하기 위하여 개인정보처리시스템별로 시험계획을 수립·이행하고, 시험계획에 따라 정기적인 시험을 실시하여 대응절차가 효과적인지, 비상시 조직 구성원이 대응절차에 따라 신속하게 대응하는지에 대한 점검을 진행할 수 있다.
- 클라우드컴퓨팅 자원 등에 개인정보처리시스템을 구축한 개인정보처리자의 경우에도 책임 및 역할 등에 따라 이용기관 측면에서의 위기대응 매뉴얼 등 대응절차를 마련해야 한다.

2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련

- 재해·재난 발생에 따른 개인정보의 훼손·손실 등을 예방하고, 신속한 복구를 위한 백업 및 복구계획을 마련해야 한다.
- 개인정보처리자는 재해·재난 발생 시 혼란을 완화시키고 신속한 의사결정을 위한 개인정보 처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.
- 백업 및 복구를 위한 계획에는 개인정보처리시스템 등 백업 및 복구 대상, 방법 및 절차 등을 포함하여야 한다.



- 개인정보처리시스템 백업 및 복구 계획은 위기대응 매뉴얼 등에 포함할 수 있다.



개인정보침해시스템 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

제12조 출력·복사시 안전조치

제12조(출력·복사시 안전조치) ① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.



해설

① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

- 개인정보처리자는 개인정보처리시스템에서 개인정보를 출력(인쇄, 화면표시, 파일생성 등) 할 때에는 다음과 같은 사항 등을 고려하여 용도를 특정하고, 용도에 따라 출력 항목을 최소화하여야 한다.
 - 개인정보처리자는 출력 항목을 최소화하기 위해 용도에 따라 출력항목을 차등화하여 표시하거나, 개인정보를 마스킹 하는 등의 방법을 활용할 수 있다.
 - 다수의 개인정보처리시스템 등에서 개인정보를 각기 다른 방식으로 마스킹할 때에는 다수의 개인정보처리시스템을 이용하여 개인정보취급자가 이용자 개인정보 집합을 구성할 수 있으므로 동일한 방식의 표시제한 조치가 필요하다.
- 개인정보처리자의 업무 수행 형태 및 목적, 유형, 장소 등 여건 및 환경에 따라 개인정보 처리 시스템에 대한 접근 권한 범위 내에서 용도에 따른 최소한의 개인정보를 출력하여야 한다.

참고

▶ 출력 시 주의사항

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

- * 업무에 반드시 필요한 경우가 아니라면 개인정보 검색 시 like 검색이 되지 않도록 조치
- * 개인정보 검색 시에는 불필요하거나 과도한 정보가 조회되지 않도록 일치검색(equal 검색) 또는 두 가지 항목 이상의 검색조건 사용 등
- * 다수의 개인정보처리시스템 등에서 개인정보를 각기 다른 방식으로 마스킹 할 때에는 개인정보취급자가 개인정보 집합을 구성할 수 있으므로 동일한 기준으로 표시제한 조치

② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

- 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 외부 저장매체 등 출력·복사물을 통해 개인정보의 분실·도난·유출 등을 방지하고 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등에 필요한 안전조치를 갖추어야 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·운영
- ▶ 출력·복사물 외부반출 및 재생산 통제·신고·제한 등
- ▶ 인쇄자, 인쇄일시 등 출력복사물 기록 저장·관리
- ▶ 종이 인쇄물에 대한 파기 절차, 파기 여부 확인 등을 포함하는 파기계획 수립 및 주기적 점검
- ▶ 복합기 보안, 출력물 워터마크 등 출력·복사물 보안기술 적용 등

- 개인정보가 포함된 외부 저장매체 등의 복사물을 통한 개인정보의 분실·도난·유출 등 방지 및 복사물의 안전한 관리를 위해 문서보안(DRM), 보안 USB, DLP(Data Loss Prevention) 등의 보안솔루션을 적용할 수 있다.
 - 개인정보가 포함된 파일에 문서보안(DRM)을 적용하는 경우, 외부 저장매체에 복사한 이후에도 파일의 열람, 편집, 인쇄 등의 권한을 관리할 수 있다.
 - 개인정보취급자의 컴퓨터에 DLP(데이터 유출 방지), 매체 제어 등 보안프로그램을 설치하여 외부 저장매체에 개인정보가 포함된 파일을 복사할 수 없도록 통제하고, 업무상 복사가 필요한 경우 승인 절차를 거쳐 허용하거나 로그기록을 남기도록 하는 방법으로 관리할 수 있다.

제13조 개인정보의 파기

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
 2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
- ② 개인정보처리자가 개인정보의 일부를 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제
- ③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.



해설

① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

- 개인정보처리자는 보유 기간의 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때는 지체 없이 그 개인정보를 파기하여야 한다. 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 조치하여야 한다.
 - ‘복원이 불가능한 방법’이란 현재의 기술 수준에서 사회통념상 적절한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다(표준 개인정보 보호지침 제10조).
 - 메모리 저장장치의 경우에는, 1호(완전파괴(소각·파쇄 등)), 3호(데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행) 내용을 적용하여야 한다.

구분	파기 방법
저장매체	• 하드디스크, USB 등의 저장매체는 장비(디가우저 등)를 활용하여 파기
종이문서	• 소량의 종이문서는 쇄절기를 이용하여 파기하며, 대량의 종이문서는 소각, 용해 등의 방법으로 파기
전자적 데이터	• 전자적 데이터는 완전 삭제 프로그램 등을 이용하여 복구할 수 없는 방법으로 파기

- 개인정보처리자는 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 다음 중 어느 하나의 조치를 하여야 한다.

- 완전파괴(소각·파쇄 등)

※ 예시: 개인정보가 저장된 회원가입신청서 등의 종이문서, 하드디스크나 자기테이프를 파쇄기로 파기 또는 용해하거나 소각장, 소각로에서 태워서 파기 등

- 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제

※ 예시: 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제 등

- 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

※ 예시: 개인정보가 저장된 하드디스크에 대해 완전포맷(3회 이상 권고), 데이터 영역에 무작위 값(0, 1 등)으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등



- 개인정보 파기 시 파기를 전문으로 수행하는 업체를 활용할 수 있다.
- 개인정보 파기의 시행 및 파기 결과의 확인은 개인정보 보호책임자의 책임하에 수행되어야 하며, 파기에 관한 사항을 기록·관리하여야 한다.

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우: 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제

- ‘개인정보의 일부만 파기하는 경우’는 저장 중인 개인정보 중 보유기간이 경과한 일부 개인정보를 파기하는 경우로 구체적인 사례는 다음과 같다.
 - 운영 중인 개인정보가 포함된 여러 파일 중 특정 파일을 파기하는 경우
 - 개인정보가 저장된 백업용 디스크나 테이프에서 보유기간이 만료된 특정 파일이나 특정 정보주체의 개인정보만 파기하는 경우
 - 운영 중인 데이터베이스에서 탈퇴한 특정 회원의 개인정보를 파기하는 경우
 - 회원가입신청서 종이문서에 기록된 정보 중 특정 필드의 정보를 파기하는 경우 등
- 개인정보처리자가 개인정보의 일부만 파기하는 경우 복구 또는 재생되지 아니하도록 개인정보가 저장된 매체 형태에 따라 다음 중 어느 하나의 조치를 하여야 한다.
 - 전자적 파일 형태인 경우: 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리·감독
 - ※ 개인정보를 삭제하는 방법 예시: 운영체제, 응용프로그램, 상용 도구 등에서 제공하는 삭제 기능을 사용하여 삭제, 백업 시 파기 대상 정보주체의 개인정보를 제외한 백업 등
(운영체제, 응용프로그램, 상용 도구 등에서 제공하는 삭제 기능을 사용하는 경우에도 가능한 복구 불가능한 방법을 사용해야 복구 및 재생의 위험을 줄일 수 있다.)
 - ※ 복구 및 재생되지 않도록 관리 및 감독하는 방법 예시: 복구 관련 기록·활동에 대해 모니터링하거나 주기적 점검을 통해 비인가된 복구에 대해 조치
 - 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록 매체인 경우: 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제
 - ※ 예시: 회원가입 신청서에 기재된 주민등록번호 삭제 시 해당 신청서에서 주민등록번호가 제거되도록 절삭, 구멍 뚫기 또는 펜 등으로 마스킹

③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

- 블록체인 등과 같이 기술적인 특성으로 인하여 이 기준의 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 따른 익명정보로 처리하는 등 개인정보가 복원이 불가능하도록 조치하여야 한다.
- 블록체인은 기술적 특성상 데이터가 기록된 이후에는 수정 또는 변경이 불가능하므로 개인정보는 별도저장소(오프체인)에 기록하고, 블록체인상에는 개인을 알아볼 수 없도록 처리한 익명정보(해시값 등)만 저장할 수 있다.
 - 특히 블록체인상에 익명정보(해시값 등)를 저장하려는 경우에는 해시값이 대입공격 등을 통해 복원되더라도 특정 개인을 알아볼 수 없도록 개인 솔트값(또는 키값)을 적용하여야 한다.
- 또한, 개인정보의 보유기간이 경과, 처리 목적이 달성되는 등 개인정보가 불필요하게 되었을 때에는 지체 없이 오프체인에 저장된 개인정보를 복원 불가능한 방법으로 파기하여야 하며, 개인정보 파기 시에는 개인 솔트값(또는 키값)을 함께 삭제하여야 한다.

제3장 공공시스템운영기관 등의 개인정보 안전성 확보조치

제14조 공공시스템운영기관의 안전조치 기준 적용

제14조(공공시스템운영기관의 안전조치 기준 적용) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 “보호위원회”라 한다)가 지정하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템 운영기관”이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.

1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우

가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템

나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템

다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템

2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우

3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우

가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템

나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템

다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템

라. 총 사업비가 100억원 이상인 시스템

- ② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리 시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.

1. 체계적인 개인정보 검색이 어려운 경우

2. 내부적 업무처리만을 위하여 사용되는 경우

3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우



해설

① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 “보호위원회”라 한다)가 지정하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.

1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우

가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템

나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템

다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템

2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우

3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우

가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템

나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템

다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템

라. 총 사업비가 100억원 이상인 시스템

- 국민의 개인정보를 대량으로 처리하는 공공시스템을 운영하는 기관은 시행령 제30조에 따른 개인정보의 안전성 확보조치 외에 시행령 제30조의2 및 이 기준의 제14조부터 제17조에 해당하는 안전성 확보조치를 추가로 이행하여야 한다.

- 제14조부터 제17조까지는 사전 준비를 위해 1년간 유예기간을 부여하여, 2024년 9월 15일부터 시행되었다.

- 공공부문의 개인정보처리시스템은 운영 형태에 따라 단일접속시스템, 표준 배포시스템, 개별시스템 등으로 구분되며, 위원회는 처리되는 개인정보의 규모나 성격, 취급자의 수 등이 이 기준 제14조에서 정하는 기준에 부합할 경우 공공시스템으로 지정할 수 있다.

- 단일접속 시스템: 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 하는 시스템

참 고

▶ 단일접속 시스템 기준

- 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
- 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
- 다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템

- 표준배포 시스템: 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 시스템
- 개별 시스템: 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 시스템

참 고

▶ 개별 시스템 기준

- 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
- 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
- 다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템
- 라. 총사업비가 100억 원 이상인 시스템

② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리 시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.

1. 체계적인 개인정보 검색이 어려운 경우
2. 내부적 업무처리만을 위하여 사용되는 경우
3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우

- 보호위원회는 공공시스템의 운영 목적, 개인정보 처리 현황, 정보주체에 미치는 영향 등을 평가하여 다음 각 호에 해당하는 경우에는 이 기준에 따른 안전조치를 이행하여야 하는 공공시스템에서 제외할 수 있다.

- 체계적인 개인정보 검색이 어려운 경우: 개인정보가 데이터베이스에 테이블 형태로 저장되지 않고, 문서(PDF)나 이미지(JPG, PNG 등) 내에 텍스트로 포함되어 있는 경우
 - 내부적 업무처리만을 위하여 사용되는 경우: 인사·회계·예산이나 전자문서결재 등 기관 내부 직원들이 업무처리를 위해 사용하는 ERP시스템 등
 - 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우: 개인정보취급자 수가 적거나 개인정보의 수가 적은 경우 등 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우
- 다만, 이 기준에서 규정하는 안전조치를 이행해야 하는 공공시스템에서 제외되는 경우라도, 이 기준에 따른 개인정보의 안전성 확보를 위하여 필요한 추가적인 조치를 할 수 있다. (권장사항)

제15조 공공시스템운영기관의 내부 관리계획의 수립·시행

제15조(공공시스템운영기관의 내부 관리계획의 수립·시행) 공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.

1. 영 제30조의제4항에 따른 관리책임자(이하 “관리책임자”라 한다)의 지정에 관한 사항
2. 관리책임자의 역할 및 책임에 관한 사항
3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항
4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항
5. 제16조 및 제17조에 관한 사항



해설

공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.

- 공공시스템운영기관은 공공시스템의 운영 및 안전성 확보에 필요한 영 제30조의제1항 제1호에 따른 사항(이하 ‘안전조치 방안’)을 공공시스템별로 내부 관리계획을 수립·시행하여야 한다.
 - 공공시스템별로 내부 관리계획을 수립하여야 하므로, 영 30조에 따른 기관 내부 관리계획과 별도로 구분하여 공공시스템 각각 내부 관리계획을 수립할 수 있고, 기관 내부관리계획 내 별지 형식으로 ‘안전조치 방안’을 수립할 수 있다.
 - 또한, 하나의 기관이 여러 개의 공공시스템을 운영하는 경우 시스템을 비슷한 유형으로 묶어 ‘유형별 안전조치 방안’을 수립할 수 있다.
- 공공시스템별로 수립해야 하는 내부 관리계획에는 이 기준 제15조 제1호부터 제5호에 해당하는 사항이 포함되어야 한다.
- 또한 공공시스템 관리책임자는 이 기준 제4조제4항에 따라 공공시스템별 내부관리계획의 이행실태를 연 1회 이상 점검하여야 한다.

- 영 제30조의2제1항의 공공시스템운영기관은 제4조제1항제1호에 따른 ‘개인정보 보호 조직의 구성 및 운영에 관한 사항’에 영 제30조의2제3항에 따른 개인정보 보호 전담부서 지정 또는 전담인력 배치와 같은 조 제5항에 따른 공공시스템운영협의회 설치·운영에 관한 내용을 포함하여야 한다.

「개인정보 보호법 시행령」

제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) ① 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은 법 제29조에 따라 이 영 제30조의 안전성 확보 조치 외에 다음 각 호의 조치를 추가로 해야 한다.

1. 제30조제1항제1호에 따른 내부 관리계획에 공공시스템별로 작성한 안전성 확보 조치를 포함할 것
2. 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 “공공시스템이용기관”이라 한다)이 상당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치
3. 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치

② 공공시스템운영기관 및 공공시스템이용기관은 상당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우에는 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지해야 한다. 이 경우 다음 각 호의 어느 하나에 해당하는 경우에는 통지를 한 것으로 본다.

1. 법 제34조제1항에 따라 정보주체에게 개인정보의 분실·도난·유출에 대하여 통지한 경우
2. 다른 법령에 따라 정보주체에게 개인정보에 접근한 사실과 피해 예방 등을 위해 필요한 사항을 통지한 경우

③ 공공시스템운영기관(공공시스템을 개발하여 배포하는 공공기관이 따로 있는 경우에는 그 공공기관을 포함한다. 이하 이 조에서 같다)은 해당 공공시스템의 규모와 특성, 해당 공공시스템이용기관의 수 등을 고려하여 개인정보의 안전한 관리에 관련된 업무를 전담하는 부서를 지정하여 운영하거나 전담인력을 배치해야 한다.

④ 공공시스템운영기관은 공공시스템별로 해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정해야 한다. 다만, 해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 업무 관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 관리책임자를 지정해야 한다.

⑤ 공공시스템운영기관은 공공시스템의 안전성 확보 조치 이행상황 점검 및 개선에 관한 사항을 협의하기 위하여 다음 각 호의 기관으로 구성되는 공공시스템운영협의회를 공공시스템별로 설치·운영해야 한다. 다만, 하나의 공공기관이 2개 이상의 공공시스템을 운영하는 경우에는 공공시스템운영협의회를 통합하여 설치·운영할 수 있다.

1. 공공시스템운영기관
2. 공공시스템의 운영을 위탁하는 경우 해당 수탁자
3. 공공시스템운영기관이 필요하다고 인정하는 공공시스템이용기관

⑥ 보호위원회는 공공시스템운영기관이 개인정보의 안전성 확보 조치를 이행 하는데 필요한 지원을 할 수 있다.

⑦ 제1항부터 제6항까지에서 규정한 사항 외에 공공시스템운영기관 등의 개인정보의 안전성 확보 조치에 필요한 사항은 보호위원회가 정하여 고시한다.

1. 영 제30조의2제4항에 따른 관리책임자(이하 “관리책임자”라 한다)의 지정에 관한 사항

- 공공시스템운영기관은 영 제30조의2제4항에 따른 관리책임자를 공공시스템 각각에 대하여 지정하여야 하며, 이 기준 제15조제1호에 따른 관리책임자는 해당 공공시스템을 총괄하여 관리하는 부서의 장으로 지정하여야 한다.
 - 다만, 해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 개인정보 안전조치 업무와의 관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 관리책임자를 지정하여야 한다.

2. 관리책임자의 역할 및 책임에 관한 사항

- 공공시스템 관리책임자가 공공시스템을 총괄하여 관리할 수 있도록 공공시스템운영기관은 관리책임자의 역할 및 책임에 관한 사항을 내부 관리계획에 포함하여 수립하여야 한다.
- 공공시스템 관리책임자는 공공시스템운영기관에 부여된 의무의 대부분을 이행할 책임을 진다. 또한 공공시스템이용기관의 접근 권한 부여·변경·말소 신청이나 접속기록 점검, 이상행위 탐지, 사전승인·사후소명 등 절차 이행 등에 대한 규정을 준수하도록 지도·점검하여야 한다.



공공시스템 관리책임자의 역할 및 책임(예시)

- ▶ 영 제30조의2제5항에 따른 공공시스템운영협의회 참석
 - ▶ 영 제30조의2제2항에 따른 정보주체에 대한 사후통지
 - ▶ 이 기준 제15조에 따른 공공시스템별 내부관리계획 수립·시행 및 점검(연 1회 이상)
 - ▶ 접근 권한 부여·변경·말소 내역에 대해 반기별 1회 이상 점검
 - ▶ 공공시스템이용기관에 접근 권한 부여·변경·말소 관련 이행 교육 및 실태 관리
 - ▶ 공공시스템이용기관이 소관 접속기록에 대해 월 1회 이상 점검·관리토록 교육 및 실태 관리
- 공공시스템운영기관은 영 제30조의2제5항에 따라 시스템 운영 수탁자, 이용기관 등이 참여하는 공공시스템운영협의회를 설치·운영하여야 한다. 산하 공공기관이 운영하는

공공시스템의 경우, 협의회를 주관부처가 아닌 산하기관에 설치할 수도 있으나 가급적 주관부처도 협의회에 참여해야 한다.

- 협의회는 운영기관의 개인정보 보호책임자와 공공시스템 관리책임자, 운영 수탁기관 및 주요 이용기관으로 구성하고,
- 「공공부문 집중관리시스템 개인정보 안전조치 강화계획」에 따라 10대 과제 이행실태 점검, 시스템 운영상 애로사항이나 우수사례 공유 및 발전방향 모색 등을 위해 연 1회 이상 개최하여야 한다.

※ 협의회 구성 예시

시스템 유형	주관기관	협의회 참여기관
단일접속	주관부처	기관 CPO, 시스템별 관리책임자, 주요 수탁기관 및 이용부서 등
표준배포	개발·배포부처	17개 시·도(교육청) CPO, 시스템별 관리책임자로 구성 (시·도는 산하기관에 협의회 논의 결과 전파 및 지도·감독)
개별	주관부처	기관 CPO, 시스템별 관리책임자, 주요 수탁기관 및 이용부서 등

- 개발·배포부처는 시·도(교육청)에서 산하 시·군·구 또는 지청을 포함하여 협의회를 구성하도록 지도하고, 협의회 결과를 시스템 운영에 반영하여야 한다(시·도는 ‘표준 개인정보 보호조례’를 제정하고, 이에 근거하여 ‘시·도 개인정보 보호 관계기관 협의회’ 설치·운영 가능).



공공시스템운영협의회 구성원(영 제30조의2제5항 각 호)

- ▶ 공공시스템운영기관
- ▶ 공공시스템의 운영을 위탁하는 경우 해당 수탁자
- ▶ 공공시스템운영기관이 필요하다고 인정하는 공공시스템이용기관

- 또한, 2개 이상의 공공시스템을 운영하는 기관은 기관별 또는 유형별로 통합 설치도 가능하다. 추가로 운영기관의 개인정보 보호책임자와 공공시스템 관리책임자들을 중심으로 운영협의회를 설치하고, 그 아래 여러 개의 유형별 소협의회를 구성하는 방식으로 운영할 수 있다.

3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항

- 개인정보처리자는 이 기준 제4조제1항제3호에 따라 '3. 개인정보 보호책임자와 개인정보 취급자의 역할 및 책임에 관한 사항'을 수립하여야 하며, 공공시스템운영기관의 경우 공공시스템에 대한 개인정보취급자의 역할 및 책임에 관한 사항을 별도로 내부 관리계획에 포함하여 수립하여야 한다.



공공시스템 개인정보취급자의 역할 및 책임(예시)

- ▶ 인사정보 미등록자(비공무원)가 공공시스템에 대한 접근 권한을 부여받을 경우 개인정보 보안서약서 제출 및 개인정보 보호 교육 이수
- ▶ 인사이동 등으로 공공시스템에 접근이 필요하거나, 필요 없어진 경우 지체 없이 접근 권한 부여·변경·말소 신청
- ▶ 주어진 접근 권한 내에서 공공시스템을 통한 개인정보 처리
- ▶ 공공시스템운영기관이 정하는 이상행위 기준에 해당하는 개인정보 처리를 한 경우 공공시스템 관리책임자 또는 부서장에게 사전승인을 받거나 정당한 업무였음을 사후소명

4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항

- 개인정보처리자는 이 기준 제4조제1항제4호부터 제6호까지 및 제8호에 해당하는 사항을 포함하여 내부 관리계획을 수립하여야 한다.
- 내부 관리계획은 개인정보 안전조치와 관련된 보호법령 및 이 기준의 내용을 그대로 기술하는 것을 넘어 공공시스템별로 안전조치 의무 이행에 필요한 세부적인 절차나 방법 및 기준을 제시하여, 누구든지 내부관리계획만 참고하면 필요한 안전조치를 이행할 수 있어야 한다.



제4조제1항제4호, 제5호, 제6호 및 제8호 등

4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
8. 접속기록 보관 및 점검

참고

- ▶ 공공시스템운영기관은 영 제30조의2제1항제2호에 따라 공공시스템이용기관이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치를 지원하여야 한다.

5. 제16조 및 제17조에 관한 사항

- 공공시스템운영기관은 이 기준에 따라 공공시스템에 대한 접근 권한을 관리, 접속기록의 보관 및 점검에 관한 사항을 내부 관리계획에 포함하여 수립하여 이행하여야 한다.
- 특히 공공시스템이용기관도 자체적인 접근 권한의 부여·관리 및 접속기록 점검·관리 등의 역할과 책임을 수행할 수 있도록 실행 방법, 기준 및 절차를 구체적으로 기술하여야 한다.



제16조 및 제17조

제16조 공공시스템운영기관의 접근 권한 관리에 관한 사항
제17조 공공시스템운영기관의 접속기록의 보관 및 점검에 관한 사항

제16조 공공시스템운영기관의 접근 권한의 관리

제16조(공공시스템운영기관의 접근 권한의 관리) ① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.

② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조제3항에 따른 내역에 포함하여야 한다.

③ 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.

④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.

⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 “공공시스템이용기관”이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.



해설

① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.

- 공공시스템운영기관은 영 제30조의2 제1항제2호에 따라 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 이 조에서 “공공시스템이용기관”이라 한다)이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치를 하여야 한다.
- 특히, 개인정보취급자가 수백 명부터 수만명에 이르는 대규모 공공시스템은 주로 상위 기관에서 하위기관의 접근 권한 총괄관리자를 지정하고, 그로 하여금 하위 기관에 대해 접근 권한 부여 등 관리·감독 권한을 부여하고 있다. 이러한 경우 접근 권한이 올바르게 부여, 변경 또는 말소 등 관리되고 있는지 확인하기 어려우므로 제16조는 공공시스템의 경우 인사정보와 연계하여 시스템에 대한 접근 권한이 보다 엄격하게 관리되도록 하려는 목적을 가지고 있다.

- 공공시스템운영기관은 접근 권한을 안전하게 관리하기 위한 조치로서 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 경우 정당한 권한을 가진 자만 공공시스템에 접근할 수 있도록 인사정보와 자동으로 연계하는 등의 조치를 하여 접근 권한의 변경 사항이 지체 없이 반영될 수 있도록 하여야 한다.
 - 인사정보는 전자인사관리시스템(e인사, 인사혁신처), 표준지방인사정보시스템(행정안전부), 정부디렉토리시스템(행정안전부)과 연계하여야 한다.
- 다만, 공공시스템에 대한 접근 권한을 인사정보와 자동으로 연계가 곤란한 경우에는 제16조 제2항 및 제3항에서 절하는 절차와 방법에 따라 접근 권한(계정)을 발급하여야 한다.
- 인사정보 연계란 인사시스템과 인사정보를 공유하여 성명, 소속기관 및 부서 관련 정보(업무분장 미포함)를 통해 정당한 업무 권한을 가진 공무원인지를 확인하고 공공시스템에 접근할 수 있는 계정과 권한을 부여하는 것을 말한다.
- 또한, 인사정보 연계를 통해 공공시스템에 접근 권한을 가진 자(개인정보취급자)가 퇴직, 휴직, 징계, 부서이동 등을 이유로 해당 공공시스템에 접근할 권한이 없어진 경우 접근 권한(계정)이 자동으로 말소되어야 한다.
 - 부서 내 팀배치 변경 등으로 업무만 변경되는 경우에는 공공시스템에 정당한 접근 권한이 유지되는지를 판단할 수 없으므로 이 경우에는 인사정보 연계로 자동 말소되지 않고, 공공시스템 관리책임자가 이 기준 제5조제2항에 따라 권한을 지체 없이 현행화할 수 있도록 필요한 조치를 하여야 한다.
- 이 기준 제16조제5항에 따라 공공시스템이용기관도 접근 권한의 부여·변경·말소와 관련하여 필요한 절차를 이행하여야 하며, 특히 업무나 시설을 위탁과 관련하여 비영리민간단체 등이 공공시스템을 이용하는 경우 해당 단체 등의 소속직원에게 접근 권한이 적법하게 부여·변경·말소될 수 있도록 지도·점검, 교육 등 필요한 조치를 하여야 한다.

「개인정보 보호법 시행령」

제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) ① 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은 법 제29조에 따라 이 영 제30조의 안전성 확보 조치 외에 다음 각 호의 조치를 추가로 해야 한다.

2. 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 이 조에서 “공공시스템이용기관”이라 한다)이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치



인사정보 연계 예시

- ▶ 인사발령, 전보 등 인사정보시스템에 등록된 사항에 따른 지체 없이 접근 권한을 부여, 변경, 말소하도록 시스템을 구축 운영함
- ▶ 인사정보에 변동이 발생하는 경우 지체 없이 해당 내용을 공공시스템에 반영하여 접근 권한을 부여, 변경, 말소하는 조치를 함
- ▶ 조직 변경, 인사 이동 시 시스템 변경 매뉴얼에 접근 권한의 부여, 변경, 말소에 대한 사항을 반영하고 이행함

② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조제3항에 따른 내역에 포함하여야 한다.

- 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 공공 시스템에 접근할 수 있는 권한을 원칙적으로 발급하여서는 안 된다.
- 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 인사정보에 등록되지 않은 자에게 공공시스템에 대한 접근 권한을 필요한 최소한의 범위 내에서 부여할 수 있다.
 - 긴급상황 등 불가피한 사유로 계정을 발급하는 경우라도 이 기준 제5조제3항에 따라 접근 권한을 부여, 변경, 말소한 내역을 기록하고 그 기록을 최소 3년간 보관하여야 하며, 공공시스템에 대한 접근 권한을 발급한 경우 목적이 달성되는 등 권한을 유지할 사유가 없는 경우에는 지체 없이 접근 권한을 말소하는 조치를 하여야 한다.

- 공공기관(출연기관, 공기업, 공단 등) 소속 직원이 공공시스템을 운영하는 경우 제2항과 제3항에서 정하는 계정 발급 절차와 방법을 따라야 하나, 공공시스템을 이용하는 공공기관이 자체적인 인사정보를 보유하고 있고 이를 접근 권한 관리 기능과 연계할 수 있는 경우에는 제1항에 따른 방법과 절차에 따라 접근 권한을 부여, 변경, 말소할 수 있다.



불가피한 사유 예시

- ▶ 중앙행정기관으로부터 공공시스템 개발·운영 업무를 위탁받은 공공기관이 해당 공공시스템을 운영해야 하는데, 자체적인 인사정보가 없거나 인사정보가 있음에도 접근 권한 관리기능과 연계가 곤란한 경우
- ▶ 공공시스템에 대한 유지보수를 수행하는 업체 직원의 경우
- ▶ 사무·시설 수탁자인 기업·비영리민간단체 등의 직원이 공공시스템을 이용해야 하는 경우

③ 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.

- 공공시스템에는 국민에 관한 개인정보가 대량으로 저장 및 관리되고 있으므로 공공시스템에 접근하는 개인정보취급자가 개인정보 보호에 필요한 인식을 갖출 수 있도록 개인정보 보호에 필요한 교육을 실시하고, 개인정보 보호에 필요한 보안 서약을 받아야 한다.
 - 개인정보 보호에 관한 교육을 모두 이수한 뒤 계정을 발급하는 것은 바로 필요한 업무를 수행하는 데 지장을 초래할 수 있으므로 기관별·시스템별 개인정보취급자 행동수칙을 정하여 이를 알려주는 것으로 교육을 대체할 수 있다.

개인정보취급자 표준행동수칙(안)

1. 정당한 사유 없이 다른 사람의 개인정보를 열람하거나 처리하지 않는다.
2. 업무상 알게 된 개인정보를 누설하거나 다른 사람에게 제공하지 않는다.
3. 개인정보가 포함된 자료를 외부에 전송할 때는 반드시 안전한 비밀번호를 설정하고, 설정한 비밀번호는 다른 연락수단을 활용하여 수신자에게 알려 준다.
4. 개인정보가 포함된 자료를 가급적 개인용 컴퓨터에 저장하지 않는다. 업무상 불가피하게 저장하는 경우에는 문서를 암호화하여 저장한다.

5. 개인정보가 담긴 서류 또는 보조저장매체는 안전한 장소에 보관한다.
6. 개인정보처리시스템 계정 로그인 정보를 다른 취급자와 공유하지 않는다. 특히 권한 없는 제3자가 나의 계정을 사용하게 하지 않는다.
7. 전보나 휴직 등으로 사용하던 개인정보처리시스템과 관련한 업무처리권한이 없어진 경우 해당 시스템을 사용하지 않는다.
8. 비밀번호는 알파벳 대문자·소문자, 숫자, 특수기호 등을 활용하여 최소 8자리 이상으로 안전하게 설정하고, 주기적으로 변경한다.
9. 개인용 컴퓨터에 백신 소프트웨어를 설치하고 수시로 업데이트하여 최신 버전으로 관리한다.
10. 개인정보 열람 요구 등 국민의 정당한 개인정보 관련 권리를 보장하기 위해 노력한다.

※ 이 외에 시스템별 특성을 담은 행동수칙을 추가하여 활용

- **非공무원 소속 부서장은 계정발급 신청서, 개인정보 보안서약서, 행동강령 교육실적을 공문으로 요청하고, 이를 보관하여야 한다.**
 - 非공무원 계정 발급 시 권한 부여·변경·말소 내역을 기록하고 최소 3년간 보관하여야 한다
- **행동수칙 교육 및 보안서약서 징구는 별도 문서에 의하여 오프라인으로 이행할 수도 있으나, 공공시스템 내에서 이뤄지는 계정발급(회원가입과 가입승인) 과정에서 팝업창으로 관련 내용을 보여주고 확인 및 동의 여부를 체크하게 하는 온라인방식으로 이행하도록 권장한다.**

④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.

- **공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.**
 - 특히, 공공시스템을 여러 기관이 이용하고 취급자가 많은 단일접속시스템이나 표준배포 시스템 개발·배포기관은 해당 시스템 이용기관에서 제5조제2항에 따른 접근 권한 현행화가 적절히 이행되고 있는지 정기적으로 점검하고, 이용기관을 관리·감독하여야 한다.
- **공공시스템 관리책임자는 접근 권한의 부여, 변경 또는 말소 내역 등에 대한 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는**

사안 등에 대해서는 사업주·대표·임원 등에게 점검결과를 보고하고, 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다.

⑤ 공공시스템을 이용하는 기관은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.

- 공공시스템운영기관이 제공하는 단일 배포시스템, 표준 배포시스템을 이용하는 공공시스템 이용기관 중 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접 하는 경우에는 이 기준 제16조제2항부터 제4항까지의 조치를 하여야 한다.

제17조 공공시스템운영기관의 접속기록의 보관 및 점검

제17조(공공시스템운영기관의 접속기록의 보관 및 점검) ① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.

② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.



① 공공시스템에 접속한 자의 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.

- 개인정보취급자가 수천수만명에 이르고, 개인정보 보유량이 매우 큰 대규모 공공시스템의 경우, 접속기록이 하루에만 수 GB에서 수 TB까지 생성되는 경우가 많으므로, 공공시스템 운영기관에서 접속기록을 엑셀파일 등으로 내려받아 이를 꼼꼼하게 점검하기는 매우 어려운 실정이다. 제17조는 자동화된 방식을 통해 이 기준 제8조에 따른 접속기록의 보관·점검이 보다 효율적으로 이행되게 하여 사후적인 책임자 특정을 넘어 유출 등 침해 사고를 사전에 예방하는 안전장치로서의 의의가 있다.
- 영 제30조의2제1항제3호 및 이 기준 제17조제1항에 따라 공공시스템운영기관은 공공시스템에 접속한 자의 접속기록 중 비인가자의 접속이나 이상행위 등을 탐지하여 개인정보 유출 사고 등을 방지하기 위하여 공공시스템에 접속한 자의 접속기록을 분석하여 탐지하는 조치를 하여야 한다.
 - 공공시스템운영기관은 공공시스템에 접속기록 점검·관리 기능을 위한 메뉴가 있고, 이 메뉴 안에서 개인정보취급자들의 접속기록을 다양한 검색 조건을 통해 검색할 수 있도록 관련 기능을 갖춰야 한다.
 - 또한, 일부 시스템은 접속기록을 보관할 때, 이 기준 제2조제3호에서 정한 식별자, 접속일시, 접속지 정보, 처리한 정보주체의 정보, 수행업무 등 5가지 항목이 모두 저장되어야 함에도 일부 항목이 누락되는 사례가 자주 발견되고 있으므로, 공공시스템운영기관은 보유한

공공시스템이 접속기록을 적정하게 생성·보관하고 있는지 확인하고, 필요한 조치를 하여야 한다.



접속기록 생성시 일부 누락하는 사례(예시)

- ▶ 시스템 개통 후 추가된 메뉴·기능에 대해 접속기록 생성 로직과 연계하지 않아, 해당 메뉴 또는 기능을 이용하는 접속기록이 전혀 생성되지 않는 경우
- ▶ 개인정보 항목을 정보주체별로 하나하나 열람하거나 내려받지 않고, 검색 조건을 통해 다량의 개인정보를 한꺼번에 열람하거나 내려받는 경우 처리한 정보주체의 정보가 공란으로 처리되는 경우
- ▶ 하나의 메뉴 또는 기능에 접속하면 보이는 첫 화면에서 미리 설정된 조건으로 개인정보가 검색되어 화면에 보이는데도, 이러한 접근이 접속기록에 반영되지 않는 경우(화면에서 개인정보를 일부 마스킹 처리하여 특정 개인을 식별하지 못하게 조치한 경우에는 접속기록이 생성되지 않아도 됨)

「개인정보 보호법 시행령」

제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) ① 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은 법 제29조에 따라 이 영 제30조의 안전성 확보 조치 외에 다음 각 호의 조치를 추가로 해야 한다.

3. 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치

- 불법적인 개인정보 유출 및 오용, 남용 시도를 신속하게 탐지하고 필요한 조치를 취하기 위하여 공공시스템에 접속한 자의 접속기록을 분석하여 이상행위를 탐지하는 기능을 직접 구축하거나 관련 상용 솔루션을 구매하여 시스템에 적용하여야 한다.
- 특히, 공공시스템운영기관은 소관 공공시스템에서 처리되는 업무나 취급자들의 업무 수행 행태를 분석하여 휴일·업무시간 외 개인정보 접근, 단기간에 다량의 개인정보 열람 및 내려받기 행위 등 비정상적인 업무라고 판단될 수 있는 기준을 설정하고 이상행위 탐지에 적용하여야 한다.
- 자동화된 방식이란 공공시스템에 접속하는 자가 공공시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 실시간으로 확인하거나 이에 준하는 방식으로 분석·점검하고, 이상행위 탐지 시 알림 및 별도의 확인이 가능한 방식을 말한다.

- 다만, 소요예산을 확보하여 자동점검 기능이 구현되기 전까지는 비정상적인 업무로 의심되는 접속기록은 없는지 수시로 점검하여야 한다.



이상행위 판단 기준 예시

- ▶ 공휴일, 업무 시간 외 개인정보 열람 또는 다운로드
 - ▶ 전 3개월 평균 개인정보 열람 또는 다운로드 횟수·정보량을 초과하는 개인정보 열람 또는 다운로드
 - ▶ 월별 개인정보 다운로드 건수 상위 개인정보취급자
 - ▶ 월별 접속지(IP 주소) 정보가 다수인 개인정보취급자
- 공공시스템운영기관은 공공시스템에 접속한 자가 부여된 권한을 초과하여 개인정보를 오용, 남용하는 것으로 의심되는 경우에는 그 사유를 소명하도록 하고, 공공시스템 관리책임자나 소속 부서장이 소명사항에 대하여 승인 및 정당한 권한이 부여되었는지를 검토(사후소명)하여야 한다.
 - 공공시스템운영기관은 사후소명 절차를 도입·운영하는 대신 이상행위로 규정된 기준에 해당하는 개인정보 접근을 하기 전에 영 제30조의2제4항에 따른 공공시스템 관리책임자나 소속 부서장 등에게 해당 접근의 목적 및 필요성, 처리할 정보주체의 정보 및 수행업무 내용 등을 적시하여 사전승인을 받을 수 있다. 또한 사전승인과 사후소명 절차를 모두 이행할 수도 있다.
 - 개인정보를 오용, 남용한 것으로 확인되는 경우에는 이 법 등 개인정보 보호와 관련된 법규의 위반, 내부 관리계획 또는 내부 규정에서 정하는 사항의 위반 정도에 따라 수사기관에 그 내용을 고발하거나 소속 기관·단체 등의 장에게 징계하도록 하는 등의 조치를 하여야 한다.
 - 또한, 공공시스템운영기관 및 이용기관은 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우 영 제30조의2제2항에 따라 해당 정보주체에게 해당 사실을 알리고 피해 예방 등을 위해 필요한 사항을 통지해야 한다.
 - 다만, 법 제34조제1항에 따라 정보주체에게 개인정보의 분실·도난·유출에 대하여 통지한 경우나 다른 법령에 따라 정보주체에게 개인정보에 접근한 사실과 피해 예방 등을 위해 필요한 사항을 통지한 경우는 영 제30조의2제2항에 따른 통지를 한 것으로 본다.

② 공공시스템운영기관은 공공시스템을 이용하는 기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

- 공공시스템운영기관은 공공시스템을 이용하는 공공시스템이용기관이 소관 개인정보 취급자의 접속기록을 직접 점검할 수 있도록 접속기록을 확인, 분석할 수 있는 기능을 제공하여야 한다.
 - 이는 하루에도 수 GB씩 생성되는 접속기록 전체를 공공시스템운영기관에서 효과적으로 점검하기에는 불가능하다는 점에서 책임과 역할을 분산하려는 조치이자, 공공시스템 이용기관에서도 이 기준에서 정하는 공공시스템에 대한 안전성 확보에 필요한 사항을 이행하도록 하는 조치이다.

제18조 재검토 기한

제18조(재검토 기한) 개인정보보호위원회는 「행정규제기본법」 제8조 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.



해설

- 개인정보보호위원회는 신규 침해위험 및 기술·서비스 발전 등을 고려하여 이 기준에 대하여 정기적으로 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙

부칙 <제2023-6호, 2023. 9. 22.>

이 고시는 발령한 날부터 시행한다. 다만, 다음 각 호의 개정규정은 각 호의 구분에 해당하는 개인정보 처리자에 대해서는 2024년 9월 15일부터 시행한다.

- 제5조제6항, 제7조제6항, 제8조제2항, 제11조의 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회고시 제2021-3호) 적용대상인 개인정보처리자
- 제7조제4항, 제12조제2항의 개정규정 및 제5조제6항 중 정보주체에 관한 개정규정 : 종전의 「(개인정보 보호위원회) 개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2021-2호) 적용대상인 개인정보처리자
- 제14조부터 제17조까지의 개정규정 : 공공시스템운영기관과 공공시스템이용기관

개인정보의 안전성
확보조치 기준 안내서



IV

부록

제1장 자주 묻는 질문과 답변

제2장 인터넷망 차단 조치 해설

제3장 개인정보 위험도 분석 기준 해설

제4장 암호화 조치 관련 참고 웹사이트

IV | 부록

제1장 자주 묻는 질문과 답변

1. 적용 대상 및 원칙



1

개인정보의 안전성 확보에 필요한 기술적·관리적·물리적 안전조치에 관한 최소한의 기준이란 무엇을 의미하는지요?

- 개인정보처리자가 개인정보를 처리할 때 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 의미합니다.
- 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.



2

「개인정보 보호법」에 따라 특례조항이 적용되던 정보통신서비스제공자등의 경우에도 이 기준을 준수해야 하나요?

- 네, 그렇습니다. 기존 개인정보처리자에 적용되던 ‘개인정보의 안전성 확보조치 기준’과 정보통신서비스제공자등에 적용되던 ‘개인정보의 기술적·관리적 보호조치 기준’이 ‘개인정보의 안전성 확보조치 기준’으로 일원화되었습니다.
- 따라서 기존 특례조항을 적용받던 정보통신서비스제공자등도 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.



3

개인정보처리자로부터 업무를 위탁받아 처리하는 수탁자도 이 기준을 준수하여야 합니까?

- “수탁자”는 개인정보처리자로부터 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위 등의 업무를 위탁받아 처리하는 자(법 제26조)를 말합니다. 따라서 “수탁자”도 법 제29조(안전조치의무) 등을 적용(법 제26조 제8항) 받으며, 이 기준에 따라 개인정보의 안전성 확보에 필요한 조치를 준용하여야 합니다.



4

부가통신사업자로 신고하였으나 해당 사업에서 개인정보를 수집하지는 않고, 오프라인으로 제품을 판매하는 과정에서 고객의 개인정보를 수집하고 있을 때에도 이 기준을 이행하여야 합니까?

- 기존 개인정보처리자에 적용되던 ‘개인정보의 안전성 확보조치 기준’과 정보통신서비스 제공자등에 적용되던 ‘개인정보의 기술적·관리적 보호조치 기준’이 통합되어 ‘개인정보의 안전성 확보조치 기준’으로 일원화되었습니다.
- 따라서 부가통신사업자로 신고하여 “정보통신서비스 제공자등”의 범위에 속하는 경우 온·오프라인에 관계없이 고객의 개인정보를 처리한다면 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치)제1항에 따른 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.



5

여행사입니다. 홈페이지를 운영하고 있지는 않지만 오프라인으로 여행상품의 계약 등을 하는 과정에서 고객의 개인정보를 수집하고 있을 때에도 이 기준을 이행하여야 합니까?

- 홈페이지 운영 여부와 관계없이 고객의 개인정보를 처리하는 경우 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치)제1항에 따른 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.



6

회사에서 내부 직원의 인사관리에 사용되는 시스템을 보유·운영할 때에도 이 기준을 이행하여야 합니까?

- 회사에서 내부 직원의 인사관리에 사용되는 시스템을 보유·운영하는 경우에도 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치)제1항에 따른 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.



7

자동차 판매회사입니다. 고객정보가 취득되는 경로를 보면 당사 차량구입고객정보, 오토카드, 정비고객, 영업사원 취득정보, 홈페이지 회원 정보, 이벤트 참여고객 등으로 나누어지는데 보호조치 기준을 이행하여야 하는 고객정보는 홈페이지 회원 정보만 해당되는 건가요?

- 기존 개인정보처리자에 적용되던 ‘개인정보의 안전성 확보조치 기준’과 정보통신서비스 제공자등에 적용되던 ‘개인정보의 기술적·관리적 보호조치 기준’이 통합되어 ‘개인정보의 안전성 확보조치 기준’으로 일원화되었습니다.
- 따라서 자동차 판매회사가 온라인과 오프라인을 통해 개인정보를 처리하는 모든 경우에는 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치) 제1항에 따른 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.



8

소상공인입니다. 현재 500명의 고객관리를 위해 업무용 컴퓨터를 운영하고 있습니다. ‘개인정보의 안전성 확보조치 기준’에 따른 조치를 수행해야 하는지요?

- 500명의 고객을 관리하는 소상공인의 경우에도 ‘개인정보의 안전성 확보조치 기준’에서 규정한 조치를 이행하여야 합니다.

2. 정의



1

개인정보처리시스템의 범위는 어디까지를 말하는지요?

- 일반적으로 데이터베이스와 데이터베이스 내 데이터에 접근할 수 있도록 해주는 응용 시스템을 의미하며, 이를 구축하거나 운영하는 데 필요한 시스템을 말합니다. 아울러, 네트워크 관리시스템 등에서 계정 관리, 알림 통지 등을 위해 개인정보를 처리하는 경우에는 해당 장비들도 해당되며, 업무용 컴퓨터, 노트북에 데이터베이스 관련 응용프로그램이 설치되어 개인정보취급자가 사용하거나, 웹서버라도 데이터베이스에 연결되어 개인정보를 처리하는 경우에는 개인정보처리시스템에 해당될 수 있습니다.



2

웹서버도 개인정보처리시스템에 해당합니까?

- 인터넷 홈페이지는 웹서버를 통해 데이터베이스와 연결되어 개인정보에 접근하여 조회, 수정, 삭제 등 개인정보를 처리할 수 있으므로 개인정보처리시스템에 해당됩니다. 따라서 개인정보처리자는 인터넷 홈페이지를 통해 개인정보가 유출되지 않도록 웹서버 등에 필요한 조치를 하여야 합니다.



3

회사 내부에서 사용하는 그룹웨어 등의 업무시스템도 개인정보처리시스템에 해당합니까?

- 개인정보처리시스템이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템을 말합니다(기준 제2조 제1호).
- 임직원의 부서, 사번, 성명, 연락처 정보는 개인정보에 해당하며, 그룹웨어 등 업무 시스템에서 결재·알림·검색 등을 위해 해당 정보를 처리하는 경우 개인정보처리시스템에 해당됩니다.



4

개인용 스마트폰에서 회사 e-mail 서버로부터 자료를 주고받아 개인정보 처리 업무를 수행하는 경우, 이 기준에 따라 안전조치를 해야 하는 모바일 기기에 포함되는지요?

- 개인용 스마트폰이나 태블릿 컴퓨터에 회사의 업무용 앱(App)을 설치하여 업무목적의 개인정보를 처리하는 경우나, 개인용 스마트폰이나 태블릿 컴퓨터에 설치된 메일 읽기 프로그램을 사용하여 회사 메일서버에 접속 후 업무목적의 개인정보를 처리하는 경우에는 안전조치를 해야 하는 모바일 기기에 해당됩니다.
- 다만, 개인용 스마트폰이 회사 e-mail 서버로부터 자료를 주고받더라도 개인정보가 포함되지 않거나, 회사 업무목적이 아닌 경우는 제외됩니다.

3. 내부 관리계획의 수립·시행 및 점검



1

내부 관리계획 수립 시, 문서 제목을 반드시 ‘내부 관리계획’으로 하여야 하나요?

- 내부 관리계획의 문서 제목에 가급적 ‘내부 관리계획’이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 방침에 따라 다른 용어를 사용할 수도 있습니다. 만약, 다른 용어를 사용하는 경우에도 이 기준 제4조(내부 관리계획의 수립·시행 및 점검)에 관한 사항을 이행하여야 합니다.



2

내부 관리계획에 출력·복사 시 보호조치에 관한 사항도 포함하여야 하나요?

- 제4조제1항에 따라 이 기준에서 정하는 기술적·관리적·물리적 안전조치에 관한 사항은 내부 관리계획에 모두 포함되어야 합니다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체는 이를 생략할 수 있습니다.
- 제13조 ‘출력·복사시 안전조치’에 대한 사항도 포함되어야 하며, 내부 관리계획을 수립하는 경우 별도의 목차를 구성하거나, ‘16. 그 밖에 개인정보 보호를 위하여 필요한 사항’에 포함하여 작성할 수도 있습니다.



3

내부 관리계획의 변경·업데이트 주기는 어떻게 되나요?

- 개인정보보호 관련 법·제도의 제·개정 여부를 정기적으로 확인하여 변경이 있을 때에는 변경 사항을 반영하고 개인정보 처리 방법, 처리 환경 및 보호조치 사항 등에 변경이 있을 때에도 변경 사항을 내부 관리계획에 즉시 반영하여 시행하여야 합니다. 또한, 내부 관리계획의 수정 이력을 관리하여야 합니다.
- 내부 관리계획은 기준 제4조제4항에 따라 연1회 이상 점검·관리하도록 하고 있으므로 최소한 연 1회 이상 점검·관리하여 변경 사항을 내부 관리계획에 반영하여야 합니다.



4 개인정보 보호책임자는 새로운 임원으로 별도 채용해야 하나요?

- 조직 전체에 임원이 없는 경우에는 신규 인력을 채용하거나 개인정보 처리 관련 업무를 담당하는 부서의 장 등을 지정할 수 있습니다. 개인정보 보호책임자는 「개인정보 보호법」 제31조(개인정보 보호책임자의 지정 등)에서 정하는 요건을 충족한 자여야 합니다.



5 개인정보보호 교육은 누구를 대상으로 해야 하는지요?

- 정보주체의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하는 ‘개인정보 보호책임자’ 그리고 고객 등 정보주체의 개인정보를 처리하는 ‘개인정보취급자’ 정규직, 비정규직, 파견직, 시간제 등 근로형태 불문) 등을 대상으로 개인정보보호 교육을 실시하여야 합니다.



6 정보보호 교육의 일부분으로 개인정보보호에 관한 사항이 포함되었다면 개인정보보호 교육을 실시한 것으로 볼 수 있나요?

- 교육과정명이 ‘정보보호 교육’이라 하더라도 회사 내부의 ‘개인정보보호 교육 계획’에 따라 실시되었다면 개인정보보호 교육으로 볼 수 있습니다.
- 다만, 이러한 때에는 교육 목적, 대상, 내용, 일정, 방법 등이 개인정보보호 교육 계획에 부합해야 합니다. 교육 실시 결과는 문서로 작성하여 보관하도록 합니다.



7 내부 관리계획 수립·시행을 생략할 수 있는 소상공인·개인·단체의 규모나 세부 기준을 알고 싶습니다.

- 기준 제4조 제1항에 따라 개인정보처리자 중 소상공인 또는 개인 또는 단체에 해당되면서 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 경우에는 내부 관리계획의 수립·시행을 생략할 수 있습니다.

- 다만, 소상공인, 개인, 단체에 해당된다고 하더라도 1만명 이상의 정보주체에 관하여 개인정보를 처리하는 경우에는 내부 관리계획을 수립·시행하여야 하며, 그 외 공공기관, 대기업, 중견기업, 중소기업 등에 해당하는 개인정보처리자는 처리하는 개인정보의 수량과 무관하게 내부 관리계획을 수립·시행하여야 합니다.
- 참고로 ‘소상공인’이란 「소상공인 보호 및 지원에 관한 법률」제2조에 해당하는 자로서 상시 근로자 수가 10명 미만인면서 업종별 상시 근로자 등이 「소상공인 보호 및 지원에 관한 법률」 시행령으로 정하는 기준에 해당하는 자를 말합니다(광업·제조업·건설업 및 운수업: 10명 미만, 그 밖의 업종: 5명 미만).

4. 접근 권한의 관리



1

개인정보취급자의 접근 권한 부여는 어떻게 해야 하나요?

- 개인정보처리자는 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 개인정보 처리시스템 접근 권한을 차등 부여 하여야 합니다.
- 특히, 개인정보처리시스템의 데이터베이스에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요성이 있습니다. 정보통신서비스 제공자들은 서비스 제공을 위해 개인정보처리시스템에 대한 열람, 수정, 다운로드 등 접근 권한을 필요한 범위에 따라 구체적으로 차등화하여 부여해야 합니다.



2

개인정보처리시스템에 접근 권한의 변경·말소는 어떻게 해야 하나요?

- 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 합니다. 여기서, '지체없이'란 정당한 사유가 없는 한 즉시 조치하여야 함을 의미합니다.
- 개인정보처리자는 접근권한의 변경 또는 말소 조치를 불완전하게 하여, 정당한 권한이 없는 자가 개인정보처리시스템에 접근하는 일이 없도록 해야 합니다.



3

일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한해야 하는 정보주체에는 웹사이트 등의 일반 이용자도 포함되나요?

- 우선 '정보주체'란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말합니다(「개인정보 보호법」 제2조제3호). 또한 '이용자'란 「정보통신망법」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말합니다. 결국 이용자 또한 처리되는 정보에 의해 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람에 해당되므로, '이용자'는 정보주체의 범위에 포함된다고 할 수 있습니다.

- 아울러, 이용자를 대상으로 하는 웹사이트는 회원서비스 등을 제공하기 위해 이용자의 개인정보를 수집, 저장, 이용, 파기 등을 처리할 수 있도록 체계적으로 구성한 시스템에 해당되므로, 개인정보처리시스템에 해당한다고 할 수 있습니다.
- 따라서, 이 기준 제5조제6항에 따라 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한해야 하는 정보주체에 웹사이트 등의 일반 이용자도 포함된다고 할 수 있습니다.



4

일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 조치에는 어떤 것들이 있나요?

- 일정 횟수 이상 인증에 실패한 경우 접근을 제한하는 조치로는 즉시 계정을 잠그거나, 인증 재시도 가능 시간을 지연하는 등의 방법을 적용할 수 있습니다. 또한, 봇의 접근을 제한하는 부수적인 수단으로 캡차(CAPTCHA)를 활용할 수 있습니다.
- 인증 재시도 가능시간 제한 등의 방법을 적용한 이후 무제한적인 인증 재시도가 발생하지 않도록, 일정 횟수 이상 인증에 실패한 경우에는 계정을 잠그는 등의 접근 제한 조치가 필요합니다.



5

과거 '개인정보의 기술적·관리적 보호조치 기준'의 비밀번호 구성 및 변경 기준은 더 이상 준수하지 않아도 되나요?

- 비밀번호 구성 및 변경 기준을 별도로 규정하고 있지 않습니다. 따라서, 개인정보처리자는 대상 시스템의 특성, 관련 위험요인 등을 종합적으로 고려하여 조직의 환경에 맞게 비밀번호 관련 내용을 정할 필요가 있습니다.
- 참고로 비밀번호를 너무 복잡하게 작성하도록 하거나 빈번하게 바꾸도록 요구하는 경우, 비밀번호 기억 및 관리의 어려움 때문에 오히려 보안성이 떨어질 수 있습니다. 또한, ID와 동일한 비밀번호, 연속된 숫자, 취약한 것으로 널리 알려진 비밀번호 등을 사용할 경우에는 비인가자가 이를 도용할 위험성이 있습니다.

5. 접근통제



1

침입 탐지 및 유출 탐지 기능을 갖춘 접근통제 장치만 설치한다면, 이 기준에서 정한 접근통제 요구사항을 충족하나요?

- 단순히 방화벽 등 정보보호 솔루션을 구매 및 설치하는 것만으로는 요구사항을 충족하지 않습니다.
- 신규 위협 대응 및 정책의 관리를 위하여 정책설정의 지속적인 업데이트 적용 및 운영·관리, 이상행위 대응, 로그분석 등의 방법으로 체계적으로 운영·관리를 하여야 합니다.



2

현재 설치·운영 중인 침입차단시스템, 침입탐지시스템을 교체·변경하려고 합니다. 시스템의 규격, 성능 등을 이 기준에서 정하고 있습니까?

- 이 기준에서는 침입차단시스템, 침입탐지시스템 등의 설치 규격, 성능 등을 정하고 있지 않습니다.
- 다만, 이 기준에서 정하는 사항을 이행하는 데 필요한 기능이 해당 시스템에서 제공되는지를 사전에 확인하기 바랍니다.



3

일정 시간 이상 업무처리를 하지 않을 때 자동으로 시스템 접속이 차단되도록 하는 최대 접속시간은 얼마로 설정해야 하나요?

- 개인정보처리자는 개인정보를 처리하는 방법 및 환경, 보안위험요인, 업무특성(데이터베이스 운영·관리, 시스템 모니터링 및 유지보수 등) 등을 고려하여 스스로의 환경에조직의 환경에 맞는 최대 접속시간을 각각 정하여 시행할 수 있습니다(예를 들어, 데이터베이스 운영·관리자인 경우 10분 등).
- 최대 접속시간은 최소한으로 정하여야 하며 불가피한 사유로 장시간 접속이 필요할 때에는 접속시간 등 그 기록을 보관·관리하여야 합니다.



4

개인정보취급자가 외부 인터넷망을 통해 개인정보처리시스템에 접속하려는 경우 안전한 인증수단이 적용되어 있습니다. 이 때에도 VPN과 같은 안전한 접속수단을 함께 적용해야 하나요?

- 외부에서 개인정보처리시스템에 접속하는 경우 안전한 인증수단(일회용 비밀번호, 인증서 등)을 적용하여야 합니다. 이 경우 VPN 등 안전한 접속수단과 안전한 인증수단을 모두 적용하는 것이 의무사항은 아닙니다.



5

인터넷망 차단 대상 사업자의 기준은?

- 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자를 대상으로 합니다.



6

온라인과 오프라인으로 서비스를 제공하고 있는 업체입니다. 오프라인으로만 수집한 고객의 개인정보가 100만명 이상이면 인터넷망 차단을 적용해야 합니까?

- 오프라인으로 수집한 고객의 개인정보가 온라인으로 서비스된다면 이 기준을 이행하여야 합니다. 따라서, 수집 경로와 상관없이 정보통신서비스 부문에서 수집한 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 고객 수가 일일평균 100만명 이상일 때에는 인터넷망 차단조치를 해야 합니다.



7

인터넷망 차단 대상인 100만명의 산정 기준을 알고 싶습니다.

- 기준 제6조제6항에서는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자수가 일일평균 100만명 이상인 경우 인터넷망 차단조치를 적용하도록 하고 있습니다.
- 이때 ‘이용자’는 정보통신망법 제2조제1항제4호에 따른 정보통신서비스제공자가 제공하는 정보통신서비스를 이용하는 자를 말합니다.
- 따라서, 정보통신서비스가 아닌 오프라인에서 처리하는 개인정보, 임직원의 개인정보 등 이용자가 아닌 정보주체의 개인정보를 제외한 이용자의 개인정보를 기준으로 산정하게 됩니다.
- 전년도 말 직전 3개월(10월, 11월, 12월)간 그 개인정보가 저장·관리되고 있는 이용자수를 일 단위로 합산한 후에 92일로 나누면 일일평균 이용자수를 산정할 수 있습니다.
- 만약 개인정보처리자가 다수의 정보통신서비스를 제공하는 경우, 개별 정보통신서비스 단위로 일일평균 이용자수를 계산한 후, 이를 개인정보처리자 단위로 합산하여 일일평균 이용자수를 산정하여야 합니다.



8

인터넷망 차단 대상인 개인정보취급자의 컴퓨터 등에 대해 알고 싶습니다.

- 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있는 컴퓨터 등은 인터넷망을 차단해야 하며, 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자(예시: 데이터베이스 운영관리자)의 컴퓨터 등에 대해 인터넷망 차단 조치를 적용하여야 합니다.



9

인터넷망 차단 방식의 세부 내용은 무엇인가요?

- 이 기준 [부록] ‘개인정보취급자를 위한 인터넷망 차단 해설’ 등을 참고하시기 바랍니다.



10

소량의 개인정보를 다운로드하는 개인정보취급자도 인터넷망 차단 대상인지요?

- 인터넷망 차단 적용 대상 여부는 개인정보를 다운로드하는 건수로 정하고 있지 않습니다. 따라서 인터넷망 차단 적용 대상 개인정보취급자에 해당하는 경우라면, 소량의 개인정보를 다운로드하더라도 인터넷망 차단조치를 해야 합니다.

6. 암호화



1 공공기관에서 암호화를 수행하는 경우, 이 기준에서 규정하는 사항과 다른 기관에서 규정하는 지침 등이 있을 때는 어느 규정을 준수해야 하는지요?

- 이 기준의 제7조(개인정보의 암호화)에서 규정하는 사항을 이행하면 「개인정보 보호법」상 암호화 의무는 준수한 것으로 볼 수 있습니다.
- 다만, 해당 분야에 관련된 다른 암호화 지침 등이 있는 경우에는 해당 규정도 준수하여야 할 것입니다.



2 내부망에 저장하는 주민등록번호는 영향평가나 위험도 분석을 통해 암호화하지 않고 보유할 수 있는지요?

- 내부망에 주민등록번호를 저장하는 경우, 법 제24조의2, 동법 시행령 제21조의2에 따라 ‘개인정보 영향평가’나 ‘위험도 분석’의 결과와 관계없이 암호화하여야 합니다.



3 암호화해야 하는 생체인식정보의 대상은 어디까지인지요?

- 생체인식정보를 식별 및 인증 등의 업무에 활용하기 위하여 수집·이용하는 경우 등에는 암호화 조치를 하여야 하며 복호화가 가능한 양방향 암호화 저장을 할 수 있습니다.



4 업무용 컴퓨터에서 고유식별정보나 생체인식정보를 처리하는 경우 개인정보 암호화는 어떻게 해야 하는지요?

- 개인정보취급자 컴퓨터에 고유식별정보, 생체인식정보를 저장하는 경우에는 안전한 암호알고리즘을 사용하여 암호화 하여야 합니다. 또한, 상용프로그램 비밀번호 설정기능이 안전한 암호알고리즘으로 암호화된다면 이를 활용할 수 있습니다.



5

개인정보 수집이 필요한 웹기반 시스템을 개발 중인데 일방향 암호화를 어떻게 적용하라는 의미인지요?

- 웹기반 시스템의 데이터베이스에 이용자의 비밀번호가 평문으로 저장되어 이용자가 입력한 비밀번호와 단순하게 비교하는 방식으로 인증 시스템 개발이 되지 않아야 한다는 의미입니다. 다시 말해, 개발 시 상용 암호 모듈을 이용하여 적용하는 방법, 자체 데이터베이스 시스템에서 제공하는 암호 모듈 활용 방법, 공개용 암호 라이브러리 등을 사용하여 프로그램을 직접 개발하는 방법이 있는데 이들 모두 일방향(해시함수) 암호화 기능이 제공되는 라이브러리를 이용하여 개발하여야 합니다.
- 다만, MD5, SHA-1 등 취약한 것으로 알려진 해시함수등은 사용해서는 안 됩니다.



6

인증정보를 안전한 암호 알고리즘으로 암호화한 경우, 송수신 구간의 암호화 적용이 필수인가요?

- 정보통신망을 통해 송수신하기 전에 인증정보가 이미 안전한 암호 알고리즘으로 암호화되어 있어 인증정보 유·노출에 따른 인증정보 도용 및 재사용 등의 위험이 없다면, 송수신 시 추가적으로 암호화(송수신구간 암호화)할 필요는 없습니다.
- 참고로 토큰 등에서 일방향 암호화 한 값을 인증정보로 사용하는 경우에는 일방향 암호화 된 값 자체가 인증정보에 해당할 수 있으므로, 이때는 송수신 시 추가적으로 암호화할 필요가 있습니다.

7. 접속기록의 보관 및 점검



1

접속기록에는 어떠한 정보를 보관·관리하여야 하는지요?

- 접속기록에는 식별자(개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정정보), 접속일시(접속한 시간 또는 업무를 수행한 시간), 접속지 정보(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소), 처리한 정보주체의 정보(개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보), 수행업무(개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보)가 포함됩니다.



2

월 1회 이상 접속기록을 점검할 때 보관하고 있는 모든 접속기록에 대하여 점검해야 하는지요?

- 월 1회 이상 접속기록을 점검할 때 보관하고 있는 모든 접속기록을 점검할 필요는 없습니다. 개인정보처리자가 기존에 점검을 완료한 접속기록임을 확인하였을 경우, 해당 접속기록에 대하여 별도의 점검을 하지 않을 수 있습니다. 또한, 내부 관리 계획에서 정하는 점검 기준 및 점검 범위는 실질적인 개인정보 유출 및 오남용을 확인할 수 있도록 타당하고 합리적으로 수립·이행하여야 합니다.



3

개인정보취급자가 아닌 이용자의 접속기록은 보관하지 않아도 되나요?

- 이용자의 접속기록 보관에 관한 사항은 이 기준에서 규정하고 있지는 않습니다.
- 다만, 이용자의 접속기록은 「통신비밀보호법」 제2조제11호 마목 및 사목, 같은 법 시행령 제41조제2항제2호에 따라 3개월 이상 보관하여야 합니다.



4

개인정보 보호책임자에게 접속기록을 주기적으로 보고해야 하나요?

- 기준 제8조제2항에서는 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검해야 할 주체를 개인정보처리자로 규정하면서, 개인정보 보호책임자에게 보고해야 하는 주기 등에 대해서는 별도로 규정하고 있지 않습니다.
- 다만, 개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 위치에 있으면서 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선, 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축, 개인정보파일의 보호 및 관리·감독 등의 업무를 수행하며, 이러한 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있습니다(법 제31조제1항 내지 제4항).
- 또한, 기준 제4조 4항에 따라, 개인정보 보호책임자는 접속기록 보관 및 점검, 접근 권한 관리, 암호화 조치 등 개인정보의 내부 관리계획 이행 실태를 연 1회 이상 점검·관리하여야 합니다.
- 결국 개인정보처리시스템의 접속기록을 점검하여야 하는 최종 책임은 개인정보 보호책임자에게 있습니다. 따라서 개인정보의 오남용, 분실·도난·유출·위조·변조 또는 훼손 등에 효과적으로 대응할 수 있도록 조직의 환경, 개인정보 처리에 따른 위험요인 등을 고려하여 자체적으로 점검 방법 및 점검 결과에 대한 개인정보 보호책임자 보고 주기를 결정해야 합니다.

8. 물리적 안전조치



1

전산실 또는 자료보관실이 없는 중소기업입니다. ‘개인정보의 안전성 확보조치 기준’ 제10조(물리적 안전조치) 조항을 준수해야 하는지요?

- 개인정보가 포함된 서류나 보조저장매체 등을 운영하는 경우에는 잠금장치가 있는 캐비닛 등 안전한 장소에 보관하여야 하며, 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여 운영해야 합니다.
- 다만, 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있지 않은 경우에는 이에 대한 출입통제 절차를 수립·운영하지 않을 수 있습니다.



2

재해·재난 대비 안전조치는 반드시 필요한가요?

- 10만명 이상의 정보주체에 관한 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관한 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템에 보관된 개인정보의 손실, 훼손 등을 방지하고 개인정보 유출 사고 등을 예방하기 위한 안전조치가 필요합니다.
- 개인정보처리자는 재해·재난 발생 시 혼란을 완화하고 신속하게 의사결정을 하기 위하여 대응절차 마련 및 점검, 백업 및 복구 계획 수립 등을 이행하여야 합니다.

9. 출력·복사 시 안전조치



1

개인정보처리시스템에서 개인정보의 출력 시(인쇄, 화면표시, 파일생성 등) 용도에 따른 출력항목의 최소화가 무엇을 의미하는지요?

- 개인정보처리자는 업무 수행 형태 및 목적, 유형, 장소 등 여건 및 환경에 따라 개인정보 처리시스템에 대한 접근 권한 범위 내에서 최소한의 개인정보를 출력하도록 조치해야 합니다.



2

개인정보처리자는 개인정보를 의무적으로 마스킹 처리를 하여야 하나?

- 이 기준 제12조 제1항에서는 개인정보의 출력항목을 최소화하도록 규정하고 있습니다. 마스킹 조치는 출력항목을 최소화하기 위한 조치 중 하나에 해당될 수 있습니다.
- 개인정보 출력항목을 최소화하는 방법으로서 마스킹을 적용하는 경우, 개인정보 처리 화면별로 마스킹이 상이하게 적용되어 여러 화면을 통해 개인정보가 조합되는 위험을 줄일 수 있도록 마스킹 방식에 관한 일관된 기준을 수립·적용하는 것이 바람직합니다.

10. 공공시스템 지정



1 제14조부터 제17조는 모든 공공시스템에 적용되는지요?

- 아닙니다. 개인정보 보유량, 취급자 수 등을 고려하여 보호위원회가 지정하는 공공시스템의 운영기관 및 이용기관만 안전조치 특례를 준수하여야 합니다.



2 공공시스템 지정은 누가, 어떤 방식으로 하나요?

- 제14조에서 정한 기준을 고려하여 보호위원회가 지정합니다. 2024년을 기준으로 382개, 123종의 공공시스템을 지정하였으며, 이는 보호위원회 홈페이지(www.pipc.go.kr)에 공지하였습니다. 향후 단계적으로 공공시스템 지정을 확대해 나갈 것입니다.



3 제14조부터 제17조를 위반하면 어떻게 되나요?

- 법 제29조 및 영 제30조의2에 따른 안전조치 의무 위반이 되며, 같은 법 제75조제2항 제5호에 따라 3,000만 원 이하의 과태료 부과 대상입니다.
- 만약, 개인정보 유출 등이 발생한 경우에는 법 제64조의2에 따라 과징금 부과 대상이 될 수 있습니다.



4 공공시스템은 유형별로 어떻게 안전조치를 준수해야 하는지 궁금합니다.

- 시스템 운영기관은 기능 구현을 위해 시스템을 개선하거나 필요한 절차·기준을 마련·시행해야 하고, 이용기관은 기능을 활용하거나 절차를 이행해야 합니다. 구체적인 구분 기준은 아래 표를 참고하시기 바랍니다.

(단) 단일접속시스템 / (표) 표준배포시스템 / (개) 개별시스템

분야	과제	(단) 운영기관 (표) 배포-운영기관 (개) 운영기관	(단) 이용기관	(표) 이용 지자체 및 지방교육청
1. 시스템 관리체계	① 협의회 설치	필요	불필요	필요
	② 시스템 책임자 지정	필요	불필요	필요
	③ 안전조치 방안 수립	필요	불필요	필요
2. 엄격한 접근 권한 관리	④ 인사정보 연계	기능 구현	구현된 기능 활용	구현된 기능 활용
	⑤ 접근 권한 현행화	필요	필요	필요
	⑥ 비공무원 계정발급 절차 도입	필요 (기능구현 권고)	절차 이행 필요	절차 이행 필요
3. 접속기록 점검 강화	⑦ 접속기록 점검	접속기록 생성 및 이용기관 다운로드 기능 구현 및 월 1회 점검 필요	월 1회 점검 필요	월 1회 점검 필요
	이상행위 탐지	이상행위 기준 마련 및 자동탐지 기능 구현 필요	이상행위 탐지 필요	이상행위 탐지 필요
	⑧ 사전·사후 절차	절차 도입 및 이행 필요	이행 필요	이행 필요
4. 담당인력 및 시스템 확충	⑨ 전담인력 확충	필요	불필요	필요
	⑩ 시스템 개선	필요	불필요	필요



5

영리를 목적으로 하지 않는 공공기관, 지방자치단체 등도 인터넷망 차단 정책 적용 대상에 포함되나요?

- 인터넷망 차단조치는 「개인정보 보호법 시행령」 제30조제1항제3호나목 및 기준 제6조6항에 따라 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당합니다.
- 이 경우 ‘이용자’란 정보통신망법 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말합니다. 결국 인터넷망 차단조치 적용 대상이 되려면 정보통신서비스 제공자에 해당되면서, 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되는 이용자 수가 일일평균 100만명 이상이 되어야 합니다.
- 이때, 정보통신서비스 제공자란 전기통신사업법 규정에 따른 ①전기통신사업자와 ②영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말합니다.

- 따라서, 중앙행정기관, 지방자치단체, 준정부기관의 경우에는 영리를 목적으로 정보통신서비스 등을 제공하지 않으므로 인터넷망 차단조치 적용대상에서 제외됩니다. 다만 그 외 공공기관의 경우에는 영리를 목적의 정보통신서비스 제공 여부를 개별적으로 판단하여 인터넷망 차단조치 적용대상 여부를 확인할 필요가 있습니다.
- 예를 들어, 공기업이 영리 목적의 정보통신서비스를 제공하면서 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되는 이용자 수가 일일평균 100만명이 넘는 경우 인터넷망 차단조치 적용대상이 될 수 있습니다.

11. 공공시스템 내부 관리계획



1 시스템별 내부 관리계획을 산하기관에서 수립해도 되는지요?

- 산하기관이 해당 시스템을 실제로 운영한다면 해당 산하기관이 내부 관리계획을 수립해도 됩니다. 다만, 소관부처가 산하 공공기관에 시스템 운영을 위탁했다면, 해당 시스템 관련 개인정보 처리 업무 위탁에 대한 내용을 자신의 내부 관리계획 및 개인정보처리방침에 담아야 합니다.



2 시스템별 안전조치방안 수립 중 내부 관리계획 명칭을 기재하라고 되어있는데, 시스템별 내부 관리계획을 세워야 하는 건가요? 아니면 시스템별 안전성 확보조치 계획을 세우면 되나요?

- 내부 관리계획 수립방법은 다양합니다. 기관 내부 관리계획과 별도로 공공시스템별 내부 관리계획을 수립할 수 있고, 기관 내부 관리계획 내 접근 권한, 접속기록 등 해당 항목 아래에 시스템별 안전조치 방안을 수립해도 되며, 기관 내부 관리계획의 별지 형태로 공공시스템별 내부 관리계획을 수립해도 됩니다.
- 또한 운영하고 있는 공공시스템이 여러 개라면 비슷한 유형별로 묶어 내부 관리계획을 수립할 수도 있습니다.



3 개인정보협의회에 참여하는 수탁기관의 범위를 알고 싶습니다.

- 시스템 개발·운영을 위탁받은 기관(주로 부처 산하 공공기관)을 말하며, 유지보수 업체는 포함되지 않습니다.



4 관련자가 참여하는 다른 협의회를 구성·운영하고 있음에도, 개인정보협의회를 따로 구성해야 하는지요?

- 개인정보 보호 관점에서 이해관계자가 모여 시스템 운영에 대한 논의가 필요하므로 가급적 별도로 구성할 것을 권장합니다. 다만 기관의 판단에 따라 다른 협의회와 통합하여 운영할 수 있습니다.

12. 공공시스템 접근 권한 관리

1 주관부처 소속 직원에게 공공기관 운영하는 개별시스템에 대한 사용자 계정을 부여하는 경우 인사시스템 연계가 필요한지요?

- 소관부처 직원은 공무원이므로 e-인사시스템 또는 정부디렉토리 등의 인사시스템(인사정보)과 연계하여 계정 발급·변경·말소를 연계 하여야 합니다.

2 인사정보 연계를 위해, 인사이동 시 업무분장까지도 파악해야 하는지요?

- 인사정보에 기록되는 소속부서까지만 연계하면 됩니다.

3 공단이 개인정보처리자인 시스템인 경우 비공무원, 부처직원에 대한 이상패턴도 점검 대상이 되는지요? 사전승인 또는 사후보고 내역이 기록되어야 하나요?

- 공무원, 비공무원 구분하지 않고 개인정보처리시스템에 접근한 자의 접속기록은 모두 저장 및 점검·관리되어야 합니다. 아울러 소관부처 직원은 공무원입니다.

4 공무원의 인사시스템이면 인사혁신처에서 연계 모듈을 제공해 주는건가요?

- 안전조치 강화계획에서 말하는 인사시스템은 인사정보로 해석할 수 있습니다. 각 부처에서 별도로 인사정보를 관리하고 있다면 그 정보를 연계하고, 별도 인사정보가 없을 시 인사혁신처나 행안부 인사정보를 연계하는 방법이 있습니다. 연계 방법은 인사혁신처(e-인사) 또는 행안부(정부디렉토리 또는 표준지방인사시스템)와 시스템별로 협의가 필요한 사항입니다.



5 인사정보 연계가 안 되는 기관의 공무원이 이 기준 제16조제3항처럼 접근 권한을 관리하면 되나요?

- 공무원이 인사정보 연계가 되지 않는 경우 e-인사시스템(인사혁신처) 또는 정부 디렉토리시스템(행정안전부) 등과 협의하여 연계방법을 찾아 연계를 추진해야 합니다. 공공기관은 자체적인 인사시스템(인사정보)이 있는 경우 이와 연계하여 계정의 발급·변경·말소 등을 관리할 수 있습니다.



6 민간인도 시스템 사용자인데 민간인에게도 교육과 보안서약서를 징구해야 하나요

- 민간인은 인사정보 미등록자이므로 이 기준 제16조제3항에 따라 발급절차를 마련하여 시행하여야 하며, 발급절차에 개인정보 교육과 보안서약서 징구가 포함되어야 합니다.



7 우리 시스템은 모든 사용자가 공무원입니다. 해당되는 모든 기관과 연계해야 하나요?

- 인사혁신처의 전자인사관리시스템, 행정안전부의 정부디렉토리시스템 또는 표준지방 인사시스템과 연계하면 됩니다. 그 외 인사정보는 해당 인사정보를 보유한 기관과 별도로 협의하여 연계하는 방법이 있습니다.



8 현재 코러스는 인사데이터에 공무원 및 비공무원(교직원)의 데이터가 함께 관리되고 있습니다. 이런 경우 비공무원은 미등록자에 해당되는지요?

- 교직원은 교직원들의 인사이동 상황(부서변경, 휴직, 면직 등)이 기록되는 인사정보 시스템이 있다면 이와 연계하여 계정 발급 등 관리업무를 추진하면 됩니다. 그러나 이러한 시스템이 없다면 인사정보 미등록자에 준하는 계정발급 절차가 필요합니다.



9

아이돌봄 경우 시군센터 종사자(인사정보 미등록자)에게 개인정보보호교육을 실시하고, 보안서약서를 징구하는 주체는 누구(시군, 부처 등) 인가요?

- 미등록자의 소속기관을 관리하는 지자체의 관련 부서장이 개인정보 교육 및 보안서약서 징구 등 비공무원에 대한 계정 발급절차를 진행하여야 합니다.



10

비공무원의 보안서약서 등 징구 방법은 내부결재(공문)나 시스템 내 해당 기능 구현 모두 가능한가요?

- 발급절차를 마련·시행하라는 뜻으로 반드시 시스템적으로 처리할 필요는 없습니다. 다만 내부결재(공문)으로 절차를 이행하는 경우 향후 현장점검 등에 대비하여 증빙 자료를 보관할 필요가 있습니다.
- 또한, 업무의 효율성 등을 고려하여 장기적으로는 발급절차를 공공시스템 내에서 처리할 수 있도록 시스템 고도화를 장려합니다.



11

데이터베이스 접근통제 상용 솔루션을 대상으로 접속자에 대한 권한을 부여, 변경 또는 말소하는 경우에 인사정보와 연계하여야 하나요?

- 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 합니다(기준 제16조제1항).
- 이에 따라, 공공시스템 데이터베이스에 대한 접근 권한을 데이터베이스 접근통제 상용 솔루션에서 관리하는 경우에는 해당 데이터베이스 접근통제 상용 솔루션을 인사 정보와 연계하여 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소할 필요가 있습니다.



12

인사정보 연계에서 ‘인사정보와 연계’는 무엇을 의미하나요?

- ‘인사정보와 연계’는 인사정보(전자인사관리시스템(e 인사, 인사혁신처), 표준지방인사정보시스템(행정안전부), 정부디렉토리시스템(행정안전부) 등)과 시스템적으로 연계하여 공공시스템의 접근 권한을 자동으로 부여, 변경, 말소하는 것을 의미합니다.
- 예를 들어, 공공시스템의 접근 권한을 보유한 개인정보취급자의 퇴직, 휴직, 부서이동 등으로 인사이동이 발생할 경우 인사정보 연동을 통해 공공시스템의 접근 권한이 자동으로 말소 또는 변경될 수 있어야 합니다.
- 다만, 불가피한 사유로 인사정보와 자동으로 연계가 곤란한 경우 인사정보 변동 시 공공시스템의 접근 권한을 지체 없이 변경하는 절차를 마련·시행할 수 있습니다.

13. 공공시스템 접속기록 보관 및 점검



1

중앙(공단 본사)에서 관리하는 시스템을 지방소속에서 사용하는 경우, 지방소속 사용자의 시스템 사전승인 또는 사후보고는 지방소속의 부서장이 되어야 하나요?

- 전체적인 업무량을 고려할 때, 지방소속 부서장 단위로 분산하는 것이 효율적입니다.



2

이상행위를 차단할 수 있는 특정 솔루션을 도입해야 하나요?

- 이상행위 탐지·차단 기능을 도입하기 위해 특정 솔루션을 구입하라는 의미가 아닙니다. 솔루션을 구입하더라도 커스터마이징이 필요할 것이고, 해당 기능을 새로 개발하는 방법도 가능합니다.



3

사전승인 또는 사후보고 결재프로세스를 거칠 때 공무원이 사용하는 전자문서시스템과 다운로드하는 시스템이 다르다면 부서장이 일일이 다운로드할 때마다 시스템에 접근해서 승인처리를 해야 하나요?

- 사후보고(소명) 절차를 선택한 경우 다운로드할 때마다 일일이 승인할 필요는 없습니다. 시스템별로 사후보고 대상이 되는 접근행위에 대한 기준을 설정하고, 이에 해당하는 접근행위를 별도로 보관한 뒤 부서장이 정기적으로 점검하고 의심되는 접근행위에 대해 해당 취급자로부터 사후 해당 접근에 대한 사유를 보고(해명)받으면 됩니다.

제2장 | 인터넷망 차단 조치 해설

1. 인터넷망 차단 개요

1 법적 근거 및 취지

- 개인정보취급자의 컴퓨터 등이 정보통신망을 통하여 악성코드에 감염되는 등 불법적인 접근을 차단하고 침해사고를 방지하기 위하여 인터넷망 차단 조치 제도가 시행되었다. 법에서는 대규모 개인정보 유출사고를 방지하기 위하여 다음과 같이 인터넷망 차단 조치에 관한 사항을 규정하고 있다.

「개인정보 보호법 시행령」

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

3. 개인정보에 대한 접근 통제를 위한 다음 각 목의 조치

나. 보호위원회가 정하여 고시하는 기준에 해당하는 개인정보취급자의 컴퓨터 등에 대한 인터넷망의 차단 (전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호의 이용자 수가 일일평균 100만명 이상인 경우만 해당한다)

개인정보의 안전성 확보 조치 기준

제6조(접근통제) ⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.

2 용어 정의

- ‘인터넷망 차단 조치’란 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해, 개인정보취급자의 컴퓨터 등에 대해 인터넷망을 차단하는 조치를 말한다.
- ‘다운로드’란 개인정보처리시스템에 접근하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드 등의 파일형태로 저장하는 것을 말한다.
- ‘파기’란 개인정보처리시스템에 저장된 개인정보 파일, 테이블 또는 데이터베이스를 삭제하는 것을 말한다.
- ‘접근 권한 설정’이란 개인정보처리시스템에 접근하는 개인정보취급자에게 다운로드, 파기 등 접근 권한을 설정하는 것을 말한다.

3 적용 대상 및 범위

- 인터넷망 차단 조치를 적용하여야 하는 개인정보처리자는 다음과 같다.

적용 대상

전년도 말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상

$$\text{※ 일일평균 이용자 수} = \frac{\text{일일 보유량(10, 11, 12월)의 총합}}{92(\text{일수})}$$

- 위에 해당하는 개인정보처리자는 다음에 대하여 인터넷망 차단 조치를 적용하여야 한다.

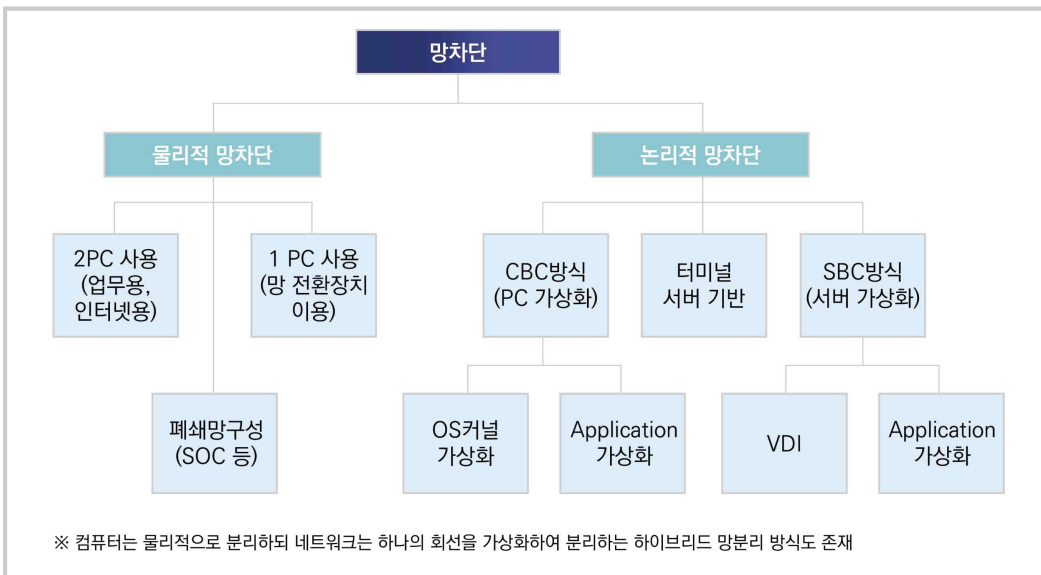
적용 범위

- ① 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 개인정보취급자의 컴퓨터 등
- ② 개인정보처리시스템에서 개인정보를 파기할 수 있는 개인정보취급자의 컴퓨터 등
- ③ 개인정보처리시스템에 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등

2. 주요 인터넷망 차단 조치 방식

1 인터넷망 차단 조치 방식 비교

- 업무망과 인터넷망을 분리하는 방식은 물리적 인터넷망 차단과 논리적 인터넷망 차단 등으로 구분할 수 있으며, 다음에서 제시된 방식 이외에도 다양한 방식이 존재할 수 있다. 다만, 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단할 수 있도록, 개인정보취급자의 컴퓨터 등에 대해 인터넷망을 차단하여야 한다.



- 물리적 인터넷망 차단과 논리적 인터넷망 차단은 다음과 같은 장단점이 있다. 이러한 장단점은 일반적인 상황을 가정한 것으로서 구성 방식과 설정 등에 따라 달라질 수 있다.

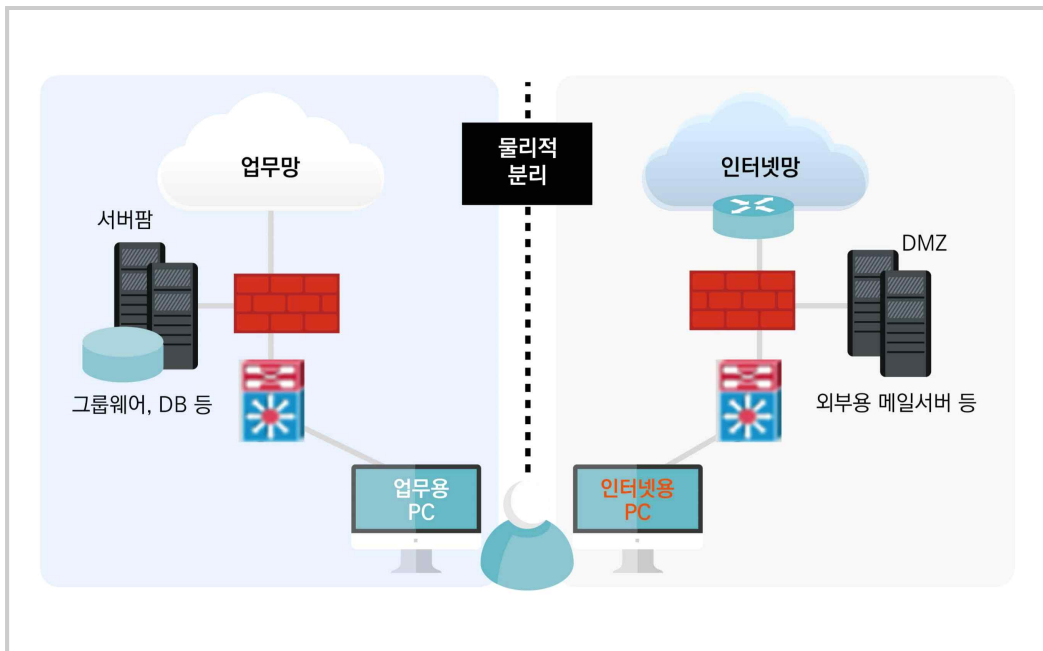
구 분	물리적 인터넷망 차단	논리적 인터넷망 차단
운영 방법	- 업무용 망과 인터넷용 망을 물리적으로 분리	- 가상화 등의 기술을 이용하여 논리적으로 분리
도입 비용	- 높음(추가 컴퓨터, 별도 망 구축 등)	- 구축환경에 따라 상이함
보안성	- 높은 보안성(근본적 분리)	- 상대적으로 낮은 보안성(구성 방식에 따라 취약점 발생 가능)
효율성	- 업무 환경의 효율성 저하	- 상대적으로 관리 용이

2 물리적 인터넷망 차단

- 물리적 인터넷망 차단은 업무망과 인터넷망을 물리적으로 분리할 뿐만 아니라 각 망에 접속하는 컴퓨터도 물리적으로 분리하여 망간 접근경로를 차단하는 방식을 말한다.
 - 어떠한 때에도 동일한 시점에 한 컴퓨터에서 업무망과 인터넷망을 동시에 접속할 수 없도록 하는 방식
 - 업무망 컴퓨터에서 인터넷망과의 연결점을 제거하여 인터넷으로부터의 악성코드 감염, 해킹, 개인정보 유출 등의 경로를 원천적으로 차단하는 방법
- 물리적 인터넷망 차단을 적용하기 위해서는 ① [방식1] 2대 컴퓨터 이용 인터넷망 차단, ② [방식2] 망전환장치 이용 인터넷망 차단, ③ [방식3] 물리적 폐쇄망 구축 등의 방식을 선택할 수 있다.
 - 이 외에도 물리적 인터넷망 차단과 논리적 인터넷망 차단을 혼용하거나 컴퓨터는 2대로 분리하되 네트워크는 하나의 망을 가상화하는 등의 하이브리드 형태의 인터넷망 차단도 적용 가능
- 물리적 인터넷망 차단 적용 시, 업무망 컴퓨터에서 인터넷이 접속되거나 악성코드가 감염되지 않도록 하는 등의 보안정책을 수립하고 안전하게 관리하는 것이 매우 중요하며 다음과 같은 방법 등이 활용될 수 있다.
 - 비인가된 디바이스(컴퓨터, 스마트폰 등)의 업무망(폐쇄망) 연결 통제
 - 업무망 컴퓨터의 IP 주소 변경, 인터넷용 랜케이블 연결 등을 통한 인터넷망 연결 차단
 - 업무망 컴퓨터에서의 테더링 등 인터넷망 차단 우회 등을 통한 인터넷 사용 차단
 - 2개의 랜카드를 사용하여 업무망과 인터넷망 동시 연결 차단
 - 업무망과 인터넷망 간의 자료 전송이 반드시 필요할 때에는 안전한 방식 적용(망연계 시스템, 보안 USB 등)
 - 외부 이메일을 통한 악성코드 유입 및 개인정보 유출 차단(인터넷용 메일시스템 도입 등)
 - USB 연결을 통한 악성코드 유입 및 개인정보 유출 차단
 - 프린터 등 주변기기에 대하여도 업무용, 인터넷용 분리 운영

① [방식1] 2대 컴퓨터 이용 인터넷망 차단

- ‘2대 컴퓨터 이용 인터넷망 차단’이란 인터넷망에 접근하는 컴퓨터와 업무망에 접근하는 컴퓨터를 별도로 사용하는 방식을 말한다.
- 인터넷용 컴퓨터와 업무용 컴퓨터를 구분하고, 인터넷용 컴퓨터는 인터넷망에 그리고 업무용 컴퓨터는 업무망에 연결하여 사용한다.

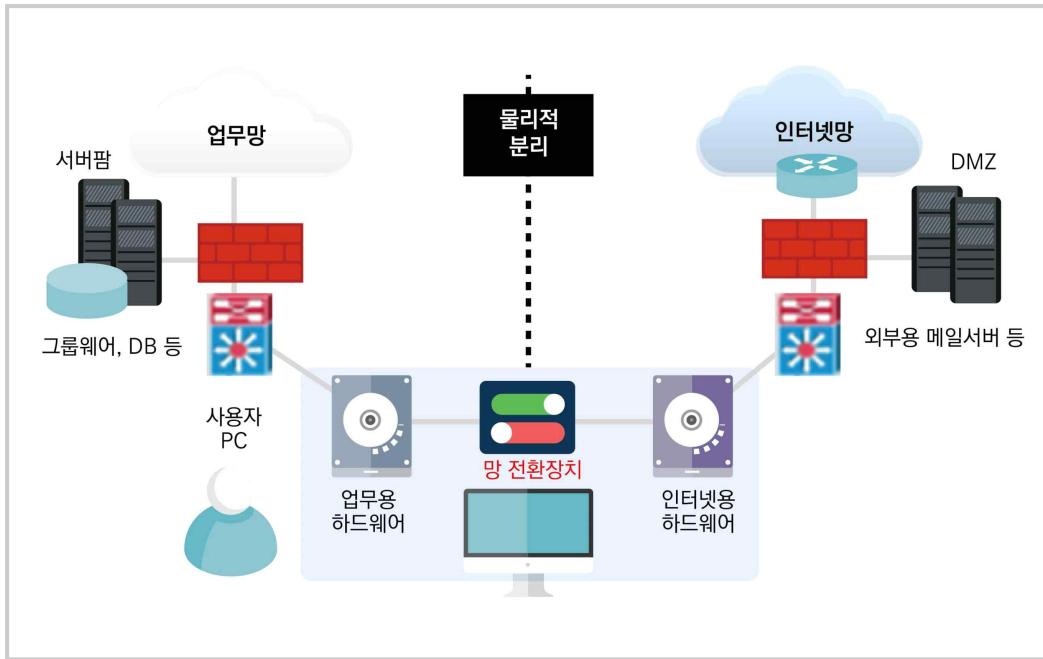


- 이 방식은 업무망과 인터넷망 간의 접근경로가 물리적으로 차단되어 보안성이 높다는 장점이 있으나 별도 네트워크 구축, 컴퓨터 추가 구매 등에 따른 비용 증가 및 관리의 어려움 등의 단점이 있다.

구분	설 명
장 점	- 인터넷망과 업무망 간 접근경로가 물리적으로 차단되어 보안성 높음
단 점	- 별도 네트워크 구축, 컴퓨터 등 추가 장비에 비용 소요 - 추가 장비로 인한 공간 및 에너지 소비 증가 - 추가 장비에 보안 관리의 부담 증가 등

② [방식2] 1대 컴퓨터 이용 인터넷망 차단

- ‘1대 컴퓨터 이용 인터넷망 차단’이란 하드디스크, IP 주소 등 정보처리 및 네트워크 연결자원을 분할한 컴퓨터에 망 전환장치를 사용하여 인터넷망과 업무망에 선택적으로 접속하는 방식을 말한다.

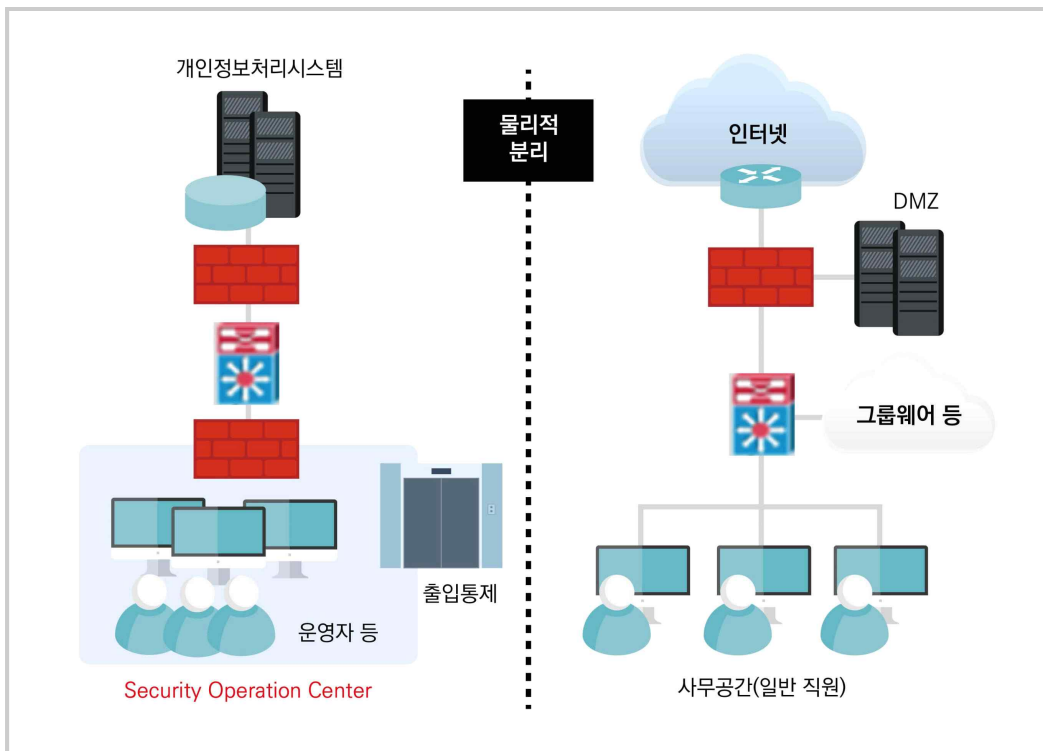


- 이 방식은 사무 공간이 협소할 때 적합할 수 있으나 망 전환 시 재부팅을 해야하는 등의 이용자 불편을 초래하는 단점이 있을 수 있다.
 - 하나의 컴퓨터 케이스에 2개의 메인보드, 하드드라이브가 각각 설치되어 동시에 부팅 및 사용이 가능한 듀얼 컴퓨터 등 다양한 하드웨어 장치가 있다.

구 분	설 명
장 점	- 인터넷망과 업무망 간 접근경로가 물리적으로 차단되어 보안성 향상 - 협소한 사무 공간에 적합
단 점	- 별도 네트워크 구축, 망 전환장치 설치 등 추가 장비에 비용 소요 - 망 전환 시 재부팅이 필요할 수 있으며, 이에 따라 업무 수행시간이 지연될 수 있음

③ [방식2] 물리적 폐쇄망 구성(SOC 등)

- 업무적으로 인터넷 사용이 반드시 필요할 때가 아니라면, 업무망 컴퓨터에 인터넷망과의 연결점을 제거하여 특정 물리적 공간을 폐쇄망으로 구성하는 방식을 고려할 수 있다.
 - SOC(Security Operation Center): 물리적으로 접근이 통제된 공간을 폐쇄망으로 구성하여, 개인정보처리시스템의 운영, 관리 목적의 접근은 SOC에서만 가능하도록 구성한다.
 - 데이터센터 운영실을 인터넷 접속이 불가능한 폐쇄망으로 구성하고 인터넷 접속이 필요할 때 별도의 인터넷 접속용 컴퓨터를 통해서 접속하도록 구성한다.



- 이 방식은 개인정보처리시스템의 직접 접속은 물리적으로 분리된 공간에서만 가능하게 함으로써 보안성을 향상할 수 있는 장점이 있는 반면에 물리적 공간 및 통제장치 마련에 따라 비용이 크게 소요될 수 있으며 업무 불편이 증가할 수 있다. 이는 폐쇄망 구성을 어떻게 하는지에 따라 매우 상이하므로 구축 방식에 따른 비용, 효과성 등을 사전에 충분히 검토 후 적용할 필요가 있다.

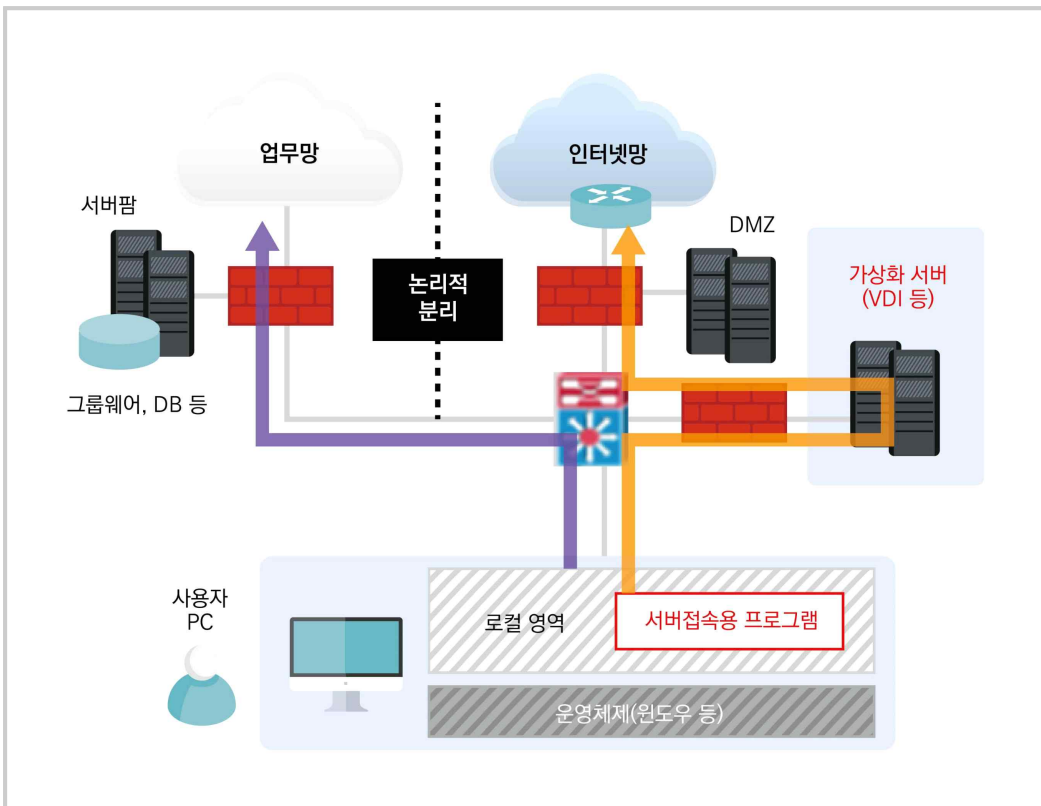
3 논리적 인터넷망 차단

- 논리적 망 분리는 가상화 기술을 이용하여 서버 또는 컴퓨터를 가상화함으로써 논리적으로 업무망과 인터넷망을 분리하는 방식을 말한다.
 - 일반적으로 1대의 컴퓨터에서 일반 영역과 가상 영역을 접속하여 업무를 수행
 - 가상환경 접속용 전용 장치(Zero Client 등)를 사용 등
- 논리적 인터넷망 차단 방식은 ① [방식1] 서버기반 논리적 인터넷망 차단(SBC, Server Based Computing), ② [방식2] 컴퓨터기반 논리적 인터넷망 차단(CBC, Client Based Computing) 등으로 구분할 수 있다.
 - 이 외에도 컴퓨터에 설치된 서버접속용 프로그램으로 인터넷망 터미널 서버에 접속하여 인터넷을 사용하는 터미널 서버기반 인터넷망 분리 방식이 있을 수 있다.
- 논리적 인터넷망 차단은 일반적으로 물리적 인터넷망 차단에 비해 상대적으로 보안성이 떨어질 수 있으므로, 논리적 인터넷망 차단 방식을 적용할 때에는 가상화 기술에 관한 보안 위협 등에 대해 충분히 검토하고 대책을 수립하여야 하며, 이를 위해 다음과 같은 방법 등이 활용될 수 있다.
 - 가상화 기술(하이퍼바이저 등)의 취약점 확인 및 조치
 - 업무망과 인터넷망 간의 자료 전송이 필요할 때에는 안전한 방식 적용(망연계 시스템 등)
 - 외부 이메일 통한 악성코드 유입 및 개인정보 유출 차단(인터넷용 메일시스템 도입 등)
 - 논리적 인터넷망 차단 설정 오류 등에 따른 업무망과 인터넷망 간의 접점 또는 우회접속 경로 차단
 - 동일한 네트워크 구간에 위치한 인터넷망 차단 미적용 컴퓨터에 의한 침해 대책 마련
 - 가상화되지 않은 영역(로컬 컴퓨터 등)에 대한 침해로 인해 가상화 영역이 동시에 침해받을 수 있는 가능성 검토 및 대책 마련 등

① [방식1] 서버기반 논리적 인터넷망 차단

- 서버기반 논리적 인터넷망 차단은 인터넷 접속, 업무 수행 등 기존에 수행하던 작업을 가상화 서버, 터미널 서버 등에 접속하여 수행함으로써, 논리적으로 인터넷망과 업무망을 분리한다.

- 세부적으로는 윈도우즈, 리눅스 등 운영체제(OS) 레벨에서 가상환경을 제공하는 VDI(Virtual Desktop Infrastructure, 데스크톱 가상화)와 특정 애플리케이션에 가상환경을 제공하는 애플리케이션 가상화 방식으로 구분될 수 있다.



- 서버기반 논리적 인터넷망 차단을 할 때 개인정보처리시스템의 운영·개발·보안을 목적으로 데이터베이스 서버 등에 접속하는 개인정보취급자(예시: 데이터베이스 운영관리자)의 컴퓨터는 인터넷망 영역을 가상화 하는 방식을 적용하는 것이 권장된다. 한편, 업무망 영역을 가상화할 때는 사용자 컴퓨터(로컬영역)가 악성코드에 감염되거나 해킹을 당할

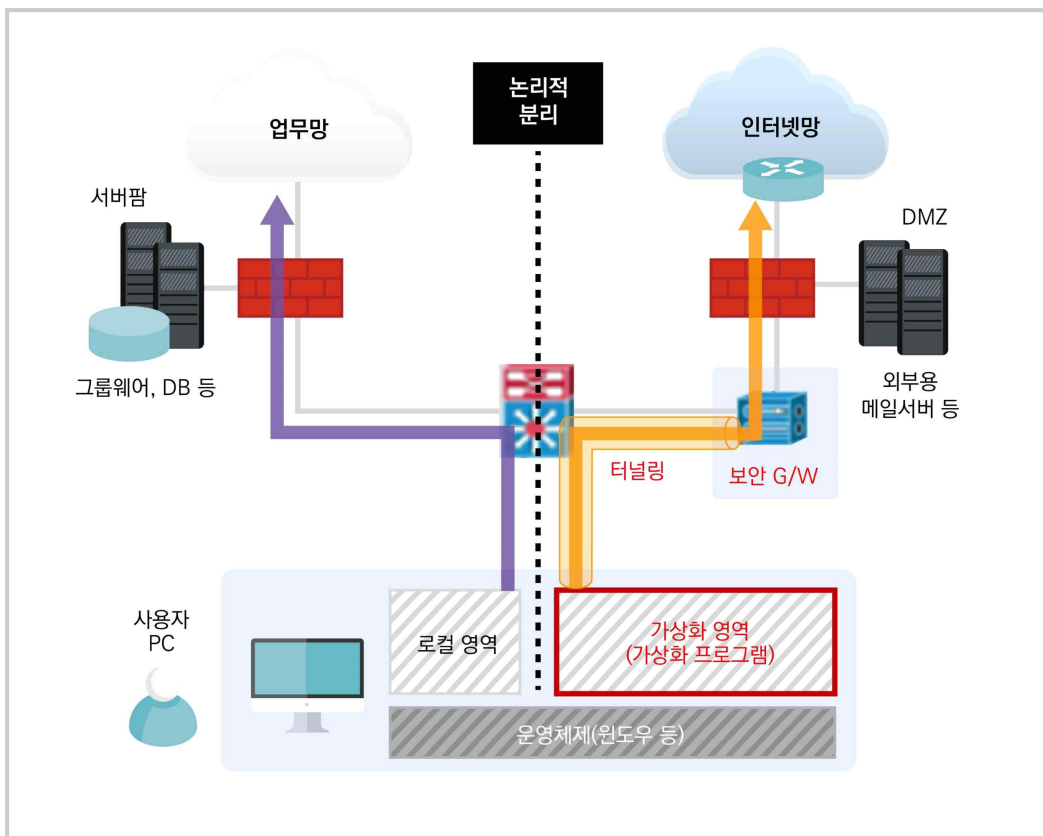
때, 업무망으로의 악성코드 유입 및 불법적인 침해 발생이 가능하다는 점을 고려하여, 그러한 침입을 차단하거나 모니터링할 수 있는 별도의 보안기술을 혼용하는 것이 보다 안전하다.

- 인터넷망 가상화 방식과 업무망 가상화 방식은 다음과 같이 비교할 수 있다.

구 분	인터넷망 가상화	업무망 가상화
특 징	<ul style="list-style-type: none"> - 업무는 사용자 컴퓨터에서 직접 수행 - 인터넷은 컴퓨터에 설치된 서버접속용 프로그램으로 인터넷망 가상화 서버에 접속하여 사용 	<ul style="list-style-type: none"> - 인터넷은 사용자 컴퓨터에서 직접 사용 - 업무는 컴퓨터에 설치된 서버접속용 프로그램으로 업무용 가상화 서버에 접속하여 수행
장 점	<ul style="list-style-type: none"> - 가상화 서버환경에 사용자 통제 및 관리정책 일괄적용 가능 - 가상화된 인터넷 환경 제공으로 인한 악성코드 감염 최소화 - 인터넷 환경이 악성코드에 감염되거나 해킹을 당해도 업무 환경은 안전하게 유지 가능 	<ul style="list-style-type: none"> - 가상화 서버 환경에 업무정보가 저장됨에 따라 업무 데이터에 중앙관리 및 백업 용이, 내부정보 유출 방지 효과 증가 - 사용자 통제 및 관리 정책 일괄 적용 가능
단 점	<ul style="list-style-type: none"> - 가상화 서버 구축을 위한 비용발생 - 가상화 서버를 다수의 사용자가 동시에 사용함에 따라 컴퓨터와 가상화 서버 간 네트워크 트래픽 증가로 인터넷망 트래픽 증가 및 속도 지연 가능 - 가상화 서버 환경에서 실행되는 보안프로그램 (인터넷 뱅킹 등)에 호환성 검토 필요 	<ul style="list-style-type: none"> - 가상화 서버 구축을 위한 비용발생 - 가상화 서버 성능 및 용량이 충분하지 못할 때 속도 저하, 업무 지연 등 발생 - 가상화 서버 장애 발생 시 업무 중단 - 가상화 서버 환경에서 실행되는 업무 프로그램, 보안프로그램 등에 호환성 검토 필요 - 사용자 컴퓨터(로컬영역)가 악성코드에 감염되거나 해킹당한 때, 업무망으로의 악성코드 유입 및 불법적인 침해 발생 가능

② [방식2] 컴퓨터기반 논리적 인터넷망 차단

- 컴퓨터기반 논리적 인터넷망 차단은 인터넷 접속 등의 작업을 컴퓨터기반 가상화 기술(CBC, Client Based Computing)이 적용된 영역에서 수행함으로써 인터넷망과 업무망을 논리적으로 분리한다.
 - 세부적으로는 윈도우즈, 리눅스 등 운영체제(OS) 레벨에서 가상환경을 제공하는 OS커널 가상화와 웹 브라우저 등 특정 애플리케이션에 가상환경을 제공하는 애플리케이션 가상화 방식으로 구분될 수 있다.



- 이 방식은 사용자 컴퓨터의 영역을 분리하는 컴퓨터 가상화 전용프로그램을 설치하고, 분리된 가상영역에서 인터넷 등을 사용하도록 구성된다.
 - 서버가상화 기반 인터넷망 차단 방식에 비해 별도의 가상화 서버 구축이 불필요함에 따라

비용이 상대적으로 절감되는 장점이 있는 반면에, 사용자 컴퓨터에 설치된 운영체제, 응용프로그램과의 호환성 등에 대해 충분한 검토가 필요하다.

구분	설 명
장 점	<ul style="list-style-type: none"> - 가상화 영역에 사용자 통제 및 관리 정책 일괄 적용 가능 - 기존 업무용 단말기를 활용하여 상대적으로 도입 비용이 낮음
단 점	<ul style="list-style-type: none"> - 운영체제(OS) 및 다양한 컴퓨터 환경, 응용프로그램에 호환성 확인 필요 - 사용 중인 운영체제, 응용프로그램, 보안프로그램의 패치 등 변경 발생 시 영향도에 따른 지속적인 관리 및 지원 필요

3. 인터넷망 차단조치 적용 시 고려사항

- 인터넷망 차단조치 구성 및 설정상의 취약점을 이용한 업무망 침투, 대량의 개인정보 유출사고 등이 발생하고 있으므로 인터넷망 차단 조치 적용 시 충분한 보안성 검토 등을 통하여 안전하게 구성하여야 한다.
- 또한, 인터넷망 차단조치 적용자와 미적용자가 동일한 네트워크 구간에 존재하는 경우 인터넷망 차단조치 미적용자의 컴퓨터를 경유하여 개인정보처리시스템에 침투하는 사례도 발생하고 있으므로 이에 필요한 대책을 수립·적용할 필요가 있다.

구 분	주요 고려 사항	보안기술 (예시)
컴퓨터 보안관리	<ul style="list-style-type: none"> - 네트워크 설정 임의 변경 등 인터넷망 차단 우회경로 차단(업무용 컴퓨터의 인터넷 연결, 추가 랜카드 설치 및 각 망에 동시 연결, 비인가된 무선인터넷 연결 및 스마트폰 테더링, IP 주소 임의 변경 등) - 비인가자의 임의사용 금지를 위한 컴퓨터 보안 상태 유지·관리 (로그온 암호설정, 화면보호기, 공유폴더 제한 등) - USB메모리 등 보조저장매체를 통한 정보유출 및 악성코드 감염 대책 마련 등 	<ul style="list-style-type: none"> - 컴퓨터보안 - NAC(Network Access Control) - IP 주소 관리 등
망간 자료전송 통제	<ul style="list-style-type: none"> - 업무망 컴퓨터와 인터넷망 컴퓨터 간 안전한 데이터 전달방법 제공 - 인터넷망과 업무망, 전송통제서버 간 통신은 일반적인 형태의 TCP/IP 방식이 아닌 암호화된 전용프로토콜을 사용하고 일방향성을 유지(공유스토리지 연계방식, UTP기반 전용프로토콜 연계방식, IEEE1394 연계방식 등) - 망간 자료 전송 시 책임자 승인절차, 사용자 인증 및 권한관리, 전송 내역 보존, 악성코드 검사 등 수행 등 	<ul style="list-style-type: none"> - 망연계솔루션 - 보안USB 등
인터넷 메일사용	<ul style="list-style-type: none"> - 업무망 컴퓨터에서 외부 이메일 수신 차단 - 외부 이메일 송·수신을 위한 메일서버는 업무망과 분리하고 인터넷 컴퓨터에서만 접근 가능하도록 구성 등 	<ul style="list-style-type: none"> - 인터넷 전용 메일서버 등
패치 관리	<ul style="list-style-type: none"> - 인터넷 컴퓨터 및 업무용 컴퓨터에 신속하고 지속적인 보안패치 (보안업데이트) - 패치관리시스템 도입 시 외부 인터넷과 분리하여 운영 - 인터넷이 차단된 업무용 컴퓨터에 패치관리 절차 수립 및 이행(관리자가 수동으로 다운로드 후 무결성 검증 및 악성코드 감염여부 등을 확인하고 패치관리시스템에 적용 등) - 패치관리시스템에 보안관리 강화(인가된 관리자만 접속할 수 있도록 접근통제 등) 등 	<ul style="list-style-type: none"> - 패치관리 시스템 (인터넷망용, 업무망용) 등
네트워크 접근제어	<ul style="list-style-type: none"> - 비인가된 기기(PC, 노트북, 스마트폰 등)는 인터넷망과 업무망에 접속할 수 없도록 차단 등 	<ul style="list-style-type: none"> - NAC - IP 주소 관리 등

구 분	주요 고려 사항	보안기술 (예시)
보조저장 매체 관리	- 인가된 보조저장매체(USB메모리, 외장하드 등)만 사용하도록 제한 등	- 보안USB - 컴퓨터보안 - DLP 등
프린터 등 주변기기 운영	- 프린터 등 주변기기는 인터넷용 또는 업무용으로 분리·운영 - 프린터를 공유할 때, 공유프린터에서 서로 다른 연결 포트를 사용하고 프린터 서버 등을 이용하여 접근통제 등	- 복합기보안 등
기타 보안관리	- 인터넷망 차단 조치 대상자에 인식제고 교육 수행 - 동일한 네트워크 구간에 인터넷망 차단 조치 대상자와 미대상자가 혼재되어 있을 때, 이에 따른 위험평가 및 대책수립 - 가상환경 및 시스템 접속 시 강화된 인증 적용(OTP, 보안토큰 등) - 서버 및 데이터베이스 레벨에서의 접근제어 (인터넷망 차단 환경을 우회한 서버·데이터베이스 접근 및 정보유출 차단) - 서버에서의 불필요한 인터넷 접속 차단 - 인터넷망 차단 상태, 컴퓨터 보안 관리 현황, 규정 준수 여부, 보안 취약점 등 정기점검 수행 등	- NAC - OTP - 서버접근제어 - 데이터베이스 접근제어 등

제3장 | 개인정보 위험도 분석 기준 해설

1. 개요

1 추진근거

- 법 제24조제3항, 제29조, 같은 법 시행령 제21조제1항, 제30조 및 「개인정보의 안전성 확보조치 기준」 제7조제3항에 따라, 개인정보처리자가 내부망에 이용자가 아닌 정보주체의 주민등록번호 외의 고유식별정보를 저장하는 경우 ‘위험도 분석 기준’에 따른 위험도 분석 결과에 따라 암호화의 적용 여부 및 적용 범위를 정하여 시행할 수 있습니다.
- 다만, 주민등록번호는 법 제24조의2, 같은 법 시행령 제21조의2에 따라 법령에서 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하도록 규정하고 있으므로, ‘위험도 분석 기준’의 결과에 관계없이 암호화하여야 합니다.



■ 고유식별정보란?

- 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다.

- 개인정보처리자는 ‘개인정보 영향평가’ 또는 ‘위험도 분석’ 결과에 따라 암호화 기술의 적용 또는 이에 상응하는 조치를 이행하여야 합니다.

※ 개인정보 영향평가 : 법 제33조, 같은 법 시행령 제38조

제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우

2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파괴 등에 관한 절차를 수립·시행하여야 한다.

2 위험도 분석 기준이란

- ‘위험도 분석’은 개인정보처리시스템에 적용하고 있는 개인정보 보호조치 이행 여부와 개인정보 유출 시 정보주체의 권리를 침해할 위험의 정도를 ‘위험도 분석 기준’을 이용하여 분석하는 행위를 말합니다.
- ‘위험도 분석 기준’은 개인정보처리자가 내부망에 고유식별정보(단, 주민등록번호 제외)를 암호화하지 않고 저장하는 경우 이행하여야 할 최소한의 보호조치 기준을 말합니다.
- 위험도 분석 점검 결과, 어느 한 개의 항목이라도 ‘아니요’에 해당하는 경우라면 암호화하여야 합니다.
※ 해당사항이 없는 경우 ‘해당없음’ 항목에 체크하며 ‘해당없음’ 체크 항목도 ‘예’로 적용합니다.
- ‘위험도 분석’은 최초 분석 이후에도 해당 개인정보파일과 관련된 개인정보처리시스템의 증설, 내·외부망과 연계, 기타 운영환경 변화의 경우에 지속적으로 실시하여야 합니다.

3 위험도 분석 기준 구성

- 위험도 분석 기준은 ①현황 조사, ②위험도 분석 점검 항목, ③위험도 분석 결과보고서로 구성되어 있습니다.

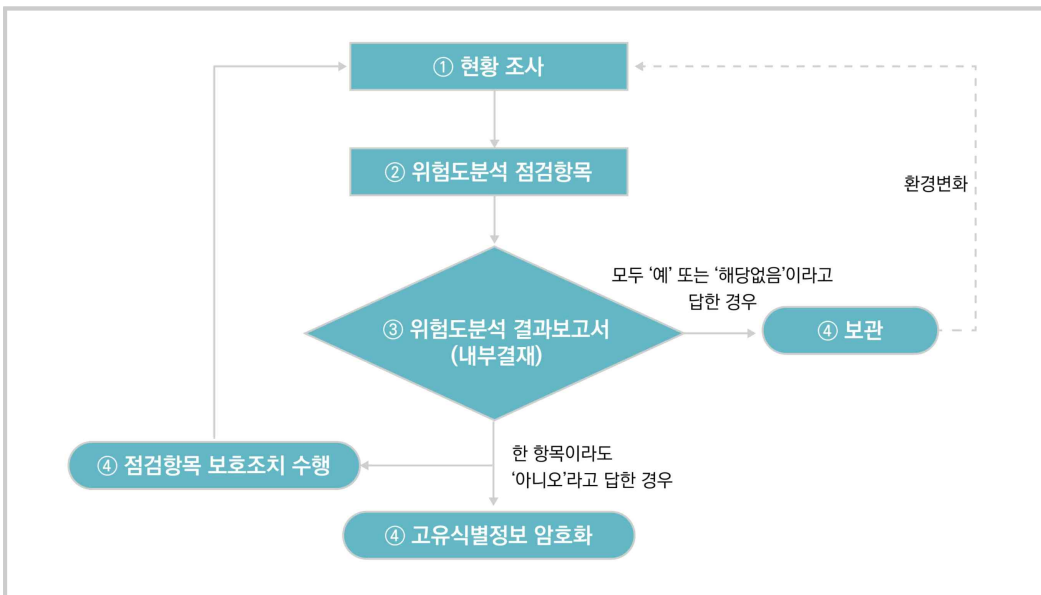
[그림 1] 위험도 분석 기준 구성



4 위험도 분석 절차

- 위험도 분석은 다음과 같은 4단계의 절차로 진행됩니다.
 - ① 위험도 분석을 위해 개인정보파일 및 고유식별정보 보유 여부 등 현황조사
 - ② 개인정보파일 단위로 위험도 분석 점검 항목별 점검을 수행
 - ③ ‘위험도 분석 결과보고서’를 작성하여 내부결재 후 보관
 - ④ 점검 결과에 따라 고유식별정보 암호화 등을 수행

[그림 2] 위험도 분석 절차



5 위험도 분석 결과보고서의 작성

- 개인정보처리자는 ‘위험도 분석 기준’에 따른 결과를 허위로 작성해서는 안 되며, ‘위험도 분석 결과보고서’는 개인정보 보호책임자 또는 해당 부서의 장의 결재를 받은 후 보관하여야 합니다.
- ‘위험도 분석’은 개인정보파일 단위로 분석하고 결과보고서를 작성하며, 개인정보파일을 위탁하여 관리하는 경우에도 위탁기관의 책임하에 작성합니다.
 - ※ 결과보고서는 기관의 문서관리 규정에 따라 ‘대외비’ 등으로 관리하시기 바랍니다.

2. 위험도 분석 기준 해설

1 현황 조사

① 개인정보파일 현황

개인정보 파일 명칭	취급개인정보	네트워크 연결여부 (개인정보파일 연동사용)	보유량 (단위: 만건)	개인정보 처리시스템명
개인정보파일 (예시)	이름, 전화번호, 이메일, 운전면허번호 등	OOO 업체와 개인정보파일 연동	500	운전면허번호 조회시스템
...				
개인정보파일_n				

- 개인정보파일 현황에는 개인정보처리시스템을 기준으로 해당 시스템이 보유하고 있는 개인정보 파일 목록을 기재합니다.
- 각 개인정보파일별로 취급하는 개인정보 항목, 네트워크 연결여부, 개인정보 보유량 등을 기재하고 해당 개인정보파일이 운영되고 있는 개인정보처리시스템 명칭을 기재합니다.
- 위험도 분석 점검의 단위인 ‘개인정보파일’이란 반드시 데이터베이스 테이블 단위로 구분되는 것은 아닙니다. 업무단위 또는 정보시스템의 기능 목록명 또는 프로세스명으로 분류하여 고유식별정보를 저장하는 데이터베이스 테이블을 통합하여 점검 가능합니다.



작성 예시

‘○○ e-러닝시스템’이란 시스템이 있다면, 강사목록 테이블, 수강생목록 테이블 등을 교육관리라는 업무로 분류하여 위험도 분석을 할 수 있습니다.



TIP

■ ‘개인정보파일’이란 ?

- 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

② 고유식별정보 현황

1. 저장하는 고유식별정보에 해당되는 항목을 모두 체크하여 주십시오.

① 여권번호 ② 운전면허번호 ③ 외국인등록번호

- 위험도 분석은 내부망에 주민등록번호 외의 고유식별정보를 저장할 경우, 암호화의 적용 여부 및 적용 범위를 결정하는 기준이므로 해당 개인정보파일에서 고유식별정보를 저장하고 있는지 점검하여 체크합니다.
- 다만, 내부망에 주민등록번호를 저장하는 경우 '위험도 분석 기준'의 결과와 관계없이 암호화하여야 합니다.
- 해당 사항이 없을 경우 고유식별정보 암호화 의무 대상이 아니므로 위험도 분석을 중단할 수 있습니다.

2. 1번 항목에서 체크한 개인정보를 어떻게 저장하고 있습니까?

① 모든 항목 암호화 저장 ② 일부 항목 암호화 저장 ③ 암호화 하지 않고 저장

- 개인정보를 저장하는 방법은 다음 중에서 선택하여 구성할 수 있습니다.

저장 방식	세부 내용
① 모든 항목 암호화 저장	해당 개인정보파일에서 저장하고 있는 모든 고유식별정보를 암호화하여 저장하는 경우 선택
② 일부 항목 암호화 저장	여러 고유식별정보 중 일부 항목만 암호화하여 저장하는 경우 선택
③ 암호화하지 않고 저장	모든 고유식별정보를 암호화하지 않고 저장하는 경우 선택

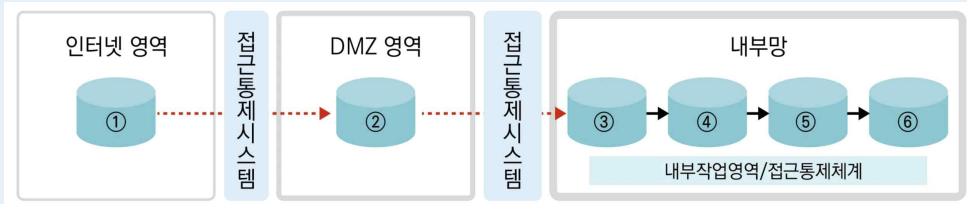
- ①번 항목을 선택하는 경우 모두 암호화를 하고 있으므로 위험도 분석을 수행할 필요가 없습니다. 단, 고유식별정보를 암호화하는 경우 국내 및 미국, 일본, 유럽 등 국내외 암호 연구 관련 기관에서 권고하는 안전한 암호 알고리즘으로 암호화하여야 합니다.
- 안전한 암호 알고리즘을 사용하더라도 암호화 키가 잘못 관리되는 경우에는 암호화된 정보들이 유·노출될 수 있으므로 이를 안전하게 관리하여야 합니다.

3. 개인정보파일의 저장위치는 어디 입니까?

① 인터넷 영역 ② DMZ 영역 ③ 내부망

※ 아래 그림을 참고하여 해당 개인정보의 저장·검색·편집·정정 등을 위한 개인정보처리시스템 (데이터베이스 등)이 위치하고 있는 번호에 체크하십시오.

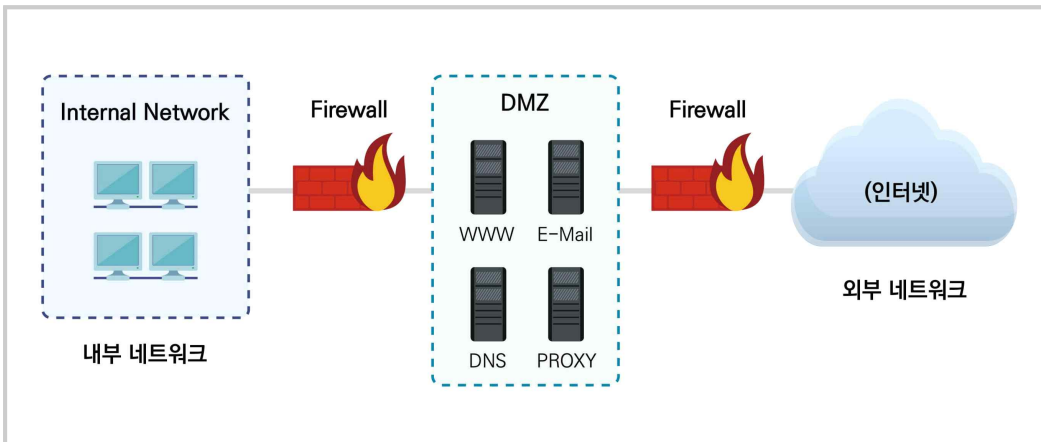
[내부망 구성도 예시]



● 용어 정의

용어	정의
인터넷 영역	개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간입니다.
DMZ 영역	인터넷 구간과 내부망 구간 사이에 위치한 중간 지점으로 침입차단 시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말합니다.
내부망	인터넷 구간과 물리적으로 망이 분리되어 있거나, 비인가된 불법적인 접근을 차단하는 기능 등을 가진 접근통제시스템에 의하여 인터넷 구간에서의 직접 접근이 불가능하도록 통제·차단되어 있는 구간을 말합니다.

[네트워크 구성도 예시]



- ①번 또는 ②번 항목 선택 시, 위험도 분석과 상관없이 무조건 암호화 대상입니다.
- 인터넷 영역이나 DMZ 영역은 외부에서 직접 접근이 가능하므로 외부 침입의 위험성이 크기 때문에 이 영역에 고유식별정보를 저장하려는 경우 반드시 암호화해야 합니다.

2 위험도 분석 점검 항목

① (기관 기준) 점검 항목

- 개인정보파일이 포함되어 있는 개인정보처리시스템 환경에 관한 내용으로 기관 전체를 대상으로 항목별로 점검하여야 합니다.

구 분	점 검 항 목	예	아니요	해당 없음
정책기반	1. 개인정보 보호책임자를 지정하여 운영하고 있습니까?			
	2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?			
	3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?			
	4. 데이터베이스 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 소프트웨어 사용을 방지하고 정품 소프트웨어만 사용하도록 하는 정책을 수립·운영하고 있습니까?			
	5. 데이터베이스 서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등)를 대상으로 개인정보보호 관련 교육을 연 2회 이상 실시하고 있습니까?			
네트워크 기반	6. 상시적으로 비인가 인터넷 프로토콜(IP) 주소의 접근을 통제하고 있습니까?			
	7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?			
	8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?			
	9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?			
	10. 주기적으로 네트워크 접속에 대한 로그를 기록 및 분석하고, 안전하게 보관하고 있습니까?			
	11. 네트워크 장비 및 정보보호시스템의 보안패치 발생 시 정당한 사유가 없는 한 즉시 업데이트를 수행하고 있습니까?			

② (개인정보처리시스템 기준) 점검 항목

• 개인정보파일이 운용되는 개인정보처리시스템의 보호조치에 관한 내용입니다.

구 분	점 검 항 목	예	아니요	해당 없음
데이터베이스 및 애플리케이션 기반	12. 상시적으로 네트워크를 통한 비인가자의 데이터베이스 접근을 통제하고 있습니까?			
	13. 데이터베이스 서버 내에 불필요한 서비스 포트를 차단하고 있습니까?			
	14. 상시적으로 데이터베이스 접속자 및 개인정보취급자의 접속 기록을 남기고 있습니까?			
	15. 데이터베이스 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?			
	16. 데이터베이스 서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?			
	17. 개인정보취급자의 역할에 따라 데이터베이스 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있습니까?			
	18. 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 데이터베이스 접근 권한을 변경하고 있습니까?			
	19. 데이터베이스 접속자 및 개인정보취급자의 데이터베이스 로그인을 위한 인증수단을 안전하게 적용하고 관리하고 있습니까?			
	20. 데이터베이스 접속자 및 개인정보취급자가 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하고 있습니까?			
	21. 데이터베이스 및 데이터베이스 접속 애플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?			
	22. 데이터베이스 및 데이터베이스 접속 애플리케이션 서버에서 보조저장 매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?			
	23. 데이터베이스 서버 및 데이터베이스 접속 애플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 정당한 사유가 없는 한 즉시 수행하고 있습니까?			
웹(Web) 기반 ※ 웹사이트를 운영하는 경우에만 해당	24. 하드디스크(HDD)등 데이터베이스 저장매체의 불용처리 시 (폐기, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?			
	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단·보완을 연 1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호조치를 하고 있습니까?			
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 정당한 사유가 없는 한 즉시 수행하고 있습니까?			

① (기관 기준) 점검 항목 해설

①-1. 정책기반

1. 개인정보 보호책임자를 지정하여 운영하고 있습니까?

- 개인정보처리자는 법 제31조제1항 및 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자(CPO : Chief Privacy Officer)를 지정해야 합니다.

참고

▶ 개인정보 보호책임자는 개인정보 관련 업무경력과 개인정보 관련 전문지식을 모두 보유한 사람으로 개인정보 처리업무를 자신의 책임 하에 관리할 수 있는 직위를 가져야 합니다(자세한 자격요건은 시행령 제32조 참조).

- 개인정보 보호책임자는 개인정보처리에 관한 전반적인 사항을 결정하고 이로 인한 제반 결과에 대하여 책임을 지는 자이므로 개인정보 수집·이용·제공 등에 대하여 실질적인 권한을 가지고 있어야 합니다.
- 개인정보 처리업무 경험이 있는 자로서, 개인정보보호를 위한 관리적·기술적·물리적 보호조치를 할 수 있는 사람이어야 합니다.

- 개인정보 보호책임자를 지정하는 것은 형식적인 절차가 아닌 내부 개인정보보호 관리체계를 강화하고, 개인정보를 안전하게 보호하도록 책임과 의무를 부여하려는 취지입니다. 이를 위해 전문지식을 보유하고 보호조치 수행이 가능한 개인정보 보호책임자를 지정하여 운영합니다.
- 만약, 개인정보 보호책임자가 실무를 담당하지 않는 경우, 개인정보의 기술적·관리적·물리적 조치를 실행할 수 있는 개인정보 보호담당자를 지정하여 업무를 수행합니다.
- 개인정보 보호책임자의 지정, 역할, 책임에 관한 내용은 내부 관리계획 등에 명시하여 최고 경영층으로부터 승인받습니다.
- 조직도, 책임자, 역할 및 책임 등이 명시된 증적자료를 '위험도 분석 결과보고서'에 첨부합니다.

2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?

- 개인정보보호를 위한 정책 또는 관리계획이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립·시행하는 내부 기준으로 내부 관리계획, 개인정보보호 추진계획 등 개인정보보호 관련 각종 내부 계획, 지침, 규정 등을 의미합니다.
- 개인정보 보호를 위한 정책 또는 관리계획을 수립·운영하도록 하는 것은 개인정보보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행되도록 하는 데 목적이 있습니다. 따라서 당해 조직의 구성원 전체에 통용되는 내부 규정을 마련합니다.
- 특히, 개인정보 침해사고에 대비하여 침해사고 시 대응 절차, 담당자, 피해복구 조치 등 침해 대응계획이 포함되어야 합니다.
- 개인정보보호 정책 및 침해사고 대응계획 수립현황 등 증적자료를 ‘위험도 분석 결과 보고서’에 첨부합니다.

3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?

- 조직에서 구성원들의 개인정보 유출 위험을 최소화하고, 구성원에게 개인정보보호에 대한 책임을 명확히 주지시키기 위해 문서화한 보안서약서에 서명하도록 해야 하며, 개인정보를 취급하는 외주 인력도 보안관리 대상에서 제외되지 않도록 합니다.
- 최근의 개인정보 유출사례를 보면 개인정보취급자에 대한 관리 소홀, 특히 외주 인력에 대한 보안관리 소홀이 그 원인이 되는 경우가 많으므로 보안서약서 집행, 비밀번호 노출 예방 등 외주 인력의 보안관리 조치를 수행하여 개인정보 유출을 방지합니다.
※ 개인정보취급자는 기업·단체·공공기관의 임직원, 계약직원, 아르바이트 직원 등의 시간제 근로자뿐만 아니라 외부기관에서 또는 외부기관으로 파견된 근로자 등도 해당됩니다.
- 외주 보안관리 현황 등 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

4. 데이터베이스 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 소프트웨어 사용을 방지하고 정품 소프트웨어만 사용하도록 하는 정책을 수립·운영하고 있습니까?

- 운영체제 소프트웨어의 경우, 불법복제 소프트웨어는 정품 인증을 받지 못함에 따라 신규 보안위협을 제거하기 위한 업데이트를 지원받지 못하게 되어 운영체제 취약점을 이용한 악성코드 감염으로 대량의 개인정보 유출 피해가 발생할 수 있습니다.
- 따라서, 개인정보의 안전한 관리를 위하여 데이터베이스 서버에 접속하는 장비 또는 개인정보취급자의 PC에는 정품 소프트웨어만을 사용하도록 하는 정책을 수립합니다.
- 소프트웨어 사용정책 및 현황 등 증적자료를 '위험도 분석 결과보고서'에 첨부합니다.

5. 데이터베이스 서버에 접근 가능한 자(내부직원, 수탁자, 개발자 등) 대상으로 개인정보보호 관련 교육을 연 2회 이상 실시하고 있습니까?

- 개인정보처리자는 개인정보취급자의 개인정보보호에 대한 인식을 제고하기 위해 매년 정기적으로 개인정보보호 교육을 실시합니다.
- 최근의 유출 사례에서 볼 수 있듯이 개인정보 유출은 내부직원의 보안인식 부족으로 발생하는 경우가 많으므로 개인정보취급자에 대한 연 1회 이상의 교육을 실시합니다.
※ 예시: 내부 직원이 고객정보를 출력물로 유출, 직원 실수로 고객정보가 포함된 이메일 발송
- 특히, 고유식별정보가 저장된 데이터베이스 서버에 접근 가능한 자(내부직원, 수탁자, 개발자 등)에 대해서는 내부 관리계획에 별도의 교육방법 및 횟수(예시: 연 2회) 등을 명기하여 교육을 실시하여야 한다.



■ 개인정보취급자

- 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다(표준개인정보처리지침 제2조제6호).
- 개인정보취급자는 개인정보 처리 업무를 담당하고 있는 자라면, 정규직, 비정규직, 하도급, 시간제 등 모든 근로 형태를 불문한다. 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함된다(개인정보 보호법령 및 지침·고시 해설서).

- 정기적인 개인정보취급자 교육을 통해 개인정보가 안전하게 관리될 수 있도록 개인정보 취급자의 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시킵니다.
- 교육 방법은 집체 교육 뿐만 아니라 조직의 환경을 고려하여 온라인 교육, 사내교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문 인력에게 위탁하여 교육을 실시할 수 있습니다.
- 교육내용에는 업무를 수행하는 데 필요한 개인정보 관련 기술교육뿐만 아니라 개인정보 보호 관련 법률 및 제도, 사내규정 등 반드시 알고 있어야 하는 기본적인 내용을 포함하는 등 목적에 부합하도록 교육을 실시합니다.



교육 내용 예시

- ▶ 개인정보보호의 중요성
- ▶ 개인정보 내부 관리계획 등 규정, 지침의 제·개정에 따른 사항
- ▶ 개인정보처리시스템의 안전한 운영·사용법(하드웨어, 소프트웨어 등)
- ▶ 개인정보의 기술적·관리적·물리적 안전조치 기준
- ▶ 개인정보 처리업무 위·수탁 시 보호조치
- ▶ 개인정보 보호업무의 절차, 책임, 방법
- ▶ 개인정보 처리 절차별 준수사항 및 금지사항
- ▶ 개인정보 유·노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 절차 등

- 교육 목적, 대상, 내용, 일정 및 방법 등을 포함하는 ‘00년 개인정보보호 교육계획’, 교육결과 보고 등 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

①-2. 네트워크(N/W) 기반

6. 상시적으로 비인가 IP 주소의 접근을 통제하고 있습니까?

- IP 주소의 접근통제의 목적은 개인정보처리시스템에 대해 인가되지 않는 접근을 차단하여 개인정보의 불법사용, 누출, 변조, 훼손 등의 위험을 적절히 차단하는 것입니다.

- 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위해, 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한하거나, 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도를 탐지할 수 있습니다.
 - 이를 위해 침입차단시스템 또는 침입방지시스템(IPS: Intrusion Prevention System) 등을 설치·운영하는 것도 가능합니다.
- IP 접근통제 현황을 '위험도 분석 결과보고서'에 첨부합니다.

7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?

- 서비스와 상관없는 포트가 불필요하게 개방되어 있는 경우 불법 침입의 경로로 이용될 수 있으므로 침입차단시스템, 서버 설정 등으로 차단하고, 서비스에 꼭 필요한 포트만 사용하도록 통제합니다.
- 서비스 포트 제한 현황 등을 '위험도 분석 결과보고서'에 첨부합니다.

8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?

- 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위해 IP 주소의 접근을 제한하거나, 비인가된 접근이 있는지를 분석하는 등 이에 대한 상시 모니터링을 합니다.
- 침입차단 및 침입탐지 기능을 갖춘 설비를 설치·운영하는 경우에는 이에 대한 상시 모니터링이 함께 이루어져야 불법적인 해킹시도에 대한 상시 대응이 가능합니다.
- 침입차단 및 침입탐지를 위한 접근통제 조치의 운영, 모니터링 현황을 '위험도 분석 결과보고서'에 첨부합니다.

9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?

- 바이러스, 웜 등 악성 프로그램들이 네트워크를 통해 유입되어 감염될 경우 해킹에 의한 개인정보 유출의 통로로 이용될 수 있으므로 네트워크상에서 상시적으로 악성 프로그램 검사를 수행하여 유입을 차단합니다.
- 네트워크를 통해 유입되는 콘텐츠의 바이러스 감염 여부를 검사하고 차단 및 치료할 수 있는 보안 프로그램을 설치·운영하여야 합니다.
- 네트워크 바이러스 차단 현황 등을 ‘위험도 분석 결과보고서’에 첨부합니다.

10. 주기적으로 네트워크 접속에 대한 로그를 기록 및 분석하고, 안전하게 보관하고 있습니까?

- 네트워크 접속 로그 파일을 생성함으로써 불법적인 접근 및 행위를 확인할 수 있고 유출사고 발생 시 책임 추적성을 확보할 수 있습니다.
- Access log 등을 기록하고, 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하기 위한 조치를 합니다.
- 접속기록을 월 1회 이상 점검하는 등 주기적으로 분석하여 이상 징후를 파악하고 대응합니다.
- 네트워크 접속기록 관리 및 분석 현황 등을 ‘위험도 분석 결과보고서’에 첨부합니다.

11. 네트워크 장비 및 정보보호시스템의 보안패치 발생 시 정당한 사유가 없는 한 즉시 업데이트를 수행하고 있습니까?

- 라우터, 스위치 등 네트워크 장비 및 침입차단시스템, 가상사설망(VPN), 침입방지 시스템(IPS) 등 정보보호시스템 운영 시 환경설정, 보안정책 설정, 침입패턴 등을 최신으로 유지할 수 있도록 업데이트를 수행하고 취약점 발견 등으로 인한 보안패치 발생 시 즉시 업데이트를 수행하여 신규로 발생하는 보안 위협에 대응합니다.

- ‘정당한 사유’란 보안패치 등 최신 업데이트의 무결성 검토, 시스템 적용 시 운영 연속성 테스트 등 개인정보처리시스템의 안정적인 운영을 위해 필요한 경우를 의미합니다.
- 네트워크 장비 및 정보보호시스템 업데이트 현황을 ‘위험도 분석 결과보고서’에 첨부합니다.

② (개인정보처리시스템 기준) 점검 항목 해설

②-1. 데이터베이스 및 애플리케이션 기반

12. 상시적으로 네트워크를 통한 비인가자의 데이터베이스 접근을 통제하고 있습니까?

- 방화벽 등 네트워크 단의 침입차단시스템이 잘 운용되고 있는 상황이라도 데이터베이스에 대한 비인가자의 접근통제는 별도로 실시합니다.
- 상시적으로 비인가자에 대한 데이터베이스 접근을 통제하기 위하여 데이터베이스 접근제어 솔루션 등을 이용할 수 있습니다.
- 사용자가 DBMS에 로그인하거나 SQL을 수행하려고 할 때 미리 정의된 규칙에 따라 권한 여부를 판단하여 통제합니다.
- 데이터베이스 접근통제 현황을 위험도 분석 보고서에 첨부합니다.

13. 데이터베이스 서버 내에 불필요한 서비스 포트를 차단하고 있습니까?

- 서비스와 상관없는 포트가 불필요하게 개방되어 있는 경우 불법 침입의 경로로 이용될 수 있으므로 관리자가 데이터베이스 관리를 위해 사용해야 하는 포트, 애플리케이션 서버에서 데이터베이스 연결을 위해 반드시 필요한 포트 이외는 차단하여 악성코드 유입 및 불법 침입 경로를 차단합니다.
- 서비스 포트 제한 현황 등을 ‘위험도 분석 결과보고서’에 첨부합니다.

14. 상시적으로 데이터베이스 관리자 및 개인정보취급자의 접속기록을 남기고 있습니까?

- 내부관리자가 데이터베이스 관리 툴, Telnet등을 이용해 데이터베이스에 직접 접속하는 경우와 개인정보취급자가 웹 또는 응용프로그램을 통해 접속하는 경우 모두 접속기록을 남김으로써, 불법적인 접근 및 행위를 확인하고 유출사고 발생 시 책임 추적성을 확보합니다.
- 데이터베이스 접속기록 관리 현황을 '위험도 분석 결과보고서'에 첨부합니다.

15. 데이터베이스 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?

- 데이터베이스 접속기록에 대한 모니터링 과정 없이 단순히 데이터베이스 접속기록을 남기는 것만으로는 데이터베이스 접속자의 행위에 대한 효과적인 통제가 이루어진다고 할 수 없습니다.
- 매주 데이터베이스 접속에 대한 이상 징후가 있는지 데이터베이스 접속기록에 대해 최소 주 1회 이상 주기적으로 모니터링을 실시하면 데이터베이스 접속에 대한 이상 징후를 파악하여 조치가 가능하고, 데이터베이스에 접속하는 모든 사람에게 모니터링이 이루어지고 있음을 인지시킴으로써 불법적인 시도 자체를 줄일 수 있습니다.
※ 데이터베이스에 접속한 개인정보취급자의 최대 접속시간 제한, 일정 시간 동안 업로드·다운로드 양 제한 등 비정상 처리 통제 정책이 준수되고 있는지 여부 모니터링 포함
- 데이터베이스 접속기록 모니터링 현황을 '위험도 분석 결과보고서'에 첨부합니다.

16. 데이터베이스 서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?

- 데이터베이스 관리자의 PC에 악성코드가 삽입되면 데이터베이스 관리자 계정이 탈취되어 대규모 개인정보 유출사고가 발생할 수 있습니다.

- 데이터베이스 관리자 PC가 인터넷 접속으로 악성코드에 감염된 채 데이터베이스 서버에 접속할 수 없도록 데이터베이스에 접속하는 데이터베이스 관리자 PC는 인터넷 접속이 불가능하도록 접속을 차단합니다.
- 데이터베이스 관리자 PC의 인터넷망 차단 조치는 네트워크를 별도로 구축하는 물리적 방식 외에 가상화를 이용한 논리적 방식도 가능합니다.
- 데이터베이스 관리자 PC의 네트워크 분리 현황 등을 ‘위험도 분석 결과보고서’에 첨부합니다.

17. 개인정보취급자의 역할에 따라 데이터베이스 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있습니까?

- 접근 권한 관리의 목적은 개인정보처리시스템에 대하여 업무 목적 외 불필요한 접근을 차단하여 개인정보의 도난, 유출, 변조, 훼손을 방지하기 위한 것입니다.
- 따라서 개인정보취급자의 역할에 따라 조회, 등록, 수정, 삭제 등의 권한을 업무 수행 목적에 따라 최소한의 범위로 차등 부여합니다.
- ‘업무 수행에 필요한 최소한 범위의 차등 부여’란, ‘최소 업무 단위 수준에서 차등 부여하여야 한다’는 의미입니다.

※ 예시: 회계부서는 영업부서 화면에 접근하지 못하도록 권한 부여

- 개인정보취급자 계정 관리 정책, 권한부여·변경 내역을 ‘위험도 분석 결과보고서’에 첨부합니다.

18. 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 데이터베이스 접근 권한을 변경하고 있습니까?

- 개인정보취급자가 아닌 사람이 계속 개인정보처리시스템에 접근 가능한 경우, 업무목적 외 불필요한 접근으로 인해 악의적 사용 및 유출 등의 문제가 발생할 수 있습니다.

개인정보취급자 또는 개인정보취급자의 업무가 변경되는 경우 철저한 접근 권한 통제가 이루어지도록 합니다.

- 조직 내의 임직원 전보 또는 퇴직, 휴직 등 인사이동 발생, 조직의 변경 또는 조직 내의 업무 조정을 통해 개인정보취급자의 업무가 변경되는 등 계정의 변경·삭제가 필요한 경우 즉시 계정 변경·삭제 및 비밀번호 변경 등 데이터베이스 접근 권한을 변경합니다.
- 접근 권한 변경 시, 일회성 조치로 제외되는 경우가 생기지 않도록 공식적인 사용자 계정 관리 절차에 따라 통제될 수 있도록 합니다.
- ‘지체 없이’란 조직원의 전보, 휴직, 퇴사, 인사이동 등의 사유로 접근 권한을 변경하기까지 소요되는 합리적인 최소한의 시간을 의미합니다.
※ 원칙적으로는 데이터베이스 접근 권한의 변경, 삭제 등을 즉시 수행하여야 하나, 업무인수인계(전보) 등으로 인하여 불가피한 경우에는 지체 없이 변경, 삭제 등을 수행합니다.
- 개인정보취급자 계정 관리 정책, 권한부여·변경 내역을 ‘위험도 분석 결과보고서’에 첨부합니다.

19. 데이터베이스 접속자 및 개인정보취급자의 데이터베이스 로그인을 위한 인증수단을 안전하게 적용하고 관리하고 있습니까?

- 정당한 권한을 가진 자인지를 인증하기 위하여 데이터베이스 접속자 및 개인정보취급자의 인증수단을 안전하게 적용하고 관리하여야 합니다.
- 비밀번호, 생체인식 등 다양한 인증수단을 활용할 수 있으며, 개인정보처리자의 환경, 개인정보 처리 현황, 침해 위험 등을 고려하여 필요하다고 인정되는 인증수단을 적용합니다.
- 인증수단을 안전하게 관리하기 위한 기준 및 방법 등은 개인정보처리자가 자율적으로 정하여 이행합니다.
※ 비밀번호를 이용하는 경우 추가적인 인증수단을 적용하고, 장기간 동일한 비밀번호를 사용하는 경우 해킹의 가능성도 높아지므로 변경 주기 등을 정하여 적용할 수 있습니다.
- 인증수단의 관리 정책 및 현황을 증적자료로 ‘위험도 분석 결과보고서’에 첨부합니다.

20. 데이터베이스 접속자 및 개인정보취급자가 인증정보를 일정 횟수 이상 인증에 실패한 경우 개인정보 처리시스템에 대한 접근을 제한하고 있습니까?

- 계정 잠금 기능이 제공되지 않는 경우, 공격자는 해당 계정의 비밀번호 등 인증정보를 파악할 때까지 지속적인 무차별 대입 공격(Brute force attack)을 수행할 수 있으므로 일정 횟수 이상 인증에 실패한 경우 개인정보 처리시스템에 대한 접근을 제한하여야 합니다.
- 접근을 제한하는 조치로 데이터베이스 관리자 등 데이터베이스에 직접 접속하는 경우, DBMS의 비밀번호 입력횟수 제한 기능을 사용합니다. 기능을 제공하지 않는 DBMS를 사용하는 경우에 한하여 데이터베이스 서버의 입력횟수 제한 기능을 사용할 수 있습니다.
- 계정 잠금에 따라 서비스가 신속히 이루어 질 수 있도록 잠금 해제 절차를 수립합니다.
- 비밀번호 관리정책 및 현황 등을 증적자료로 '위험도 분석 결과보고서'에 첨부합니다.

21. 데이터베이스 및 데이터베이스 접속 애플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?

- 개인정보처리시스템의 서버에 비인가자의 물리적 접근이 가능한 경우 개인정보 유출, 파괴 등의 위험이 발생할 수 있으므로 물리적 접근통제를 실시합니다.
- 전산실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우, 출입을 통제하는 방법으로 물리적 접근통제 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하는 방법 등이 있습니다.
 - 전자적 매체 기록방법: 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입 통제장치, 지문 등 바이오정보 기반 출입통제 장치 등
 - 수기문서 대장 기록방법: '출입자', '출입일시', '출입목적' 등을 출입관리 대장에 기록
- 데이터베이스 서버 및 데이터베이스 접속 애플리케이션 서버에 대한 비인가자 접근을 차단하기 위해 접근 통제 절차를 수립·운영하여야 하며, 접근기록을 보관합니다.
 - ※ 접근통제 절차에는 출입증·출입카드 발급절차, 회수절차 등이 포함됨

- 데이터베이스 서버 및 데이터베이스 접속 애플리케이션 서버를 별도의 전산실에서 운영하지 않는 경우 비인가자가 무단접근하지 못하도록 통제선, 칸막이 등을 이용하여 비인가자 접근을 차단하여야 합니다.
- 개인정보처리시스템에 대한 물리적 접근통제 현황 등 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

22. 데이터베이스 및 데이터베이스 접속 애플리케이션 서버에서 보조저장매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?

- 방화벽, 침입탐지 등 네트워크 접근제한 솔루션을 운용하더라도 데이터베이스 서버 등에 보조저장매체를 사용해 직접 접근으로 해킹 프로그램을 구동하거나 개인정보의 유출이 가능할 수 있으므로 이를 방지하여야 합니다.
- 데이터베이스 서버나 데이터베이스 접속 애플리케이션 서버에 직접 보조저장매체 삽입을 차단하고 불가피하게 업무 목적으로 쓸 경우 관리자 허가를 받는 절차를 거쳐야 합니다.
- 관리자는 보조저장매체의 사용 및 회수를 통제하여야 하며, 최신 보안 프로그램으로 악성코드 감염여부를 확인하는 등 보안조치를 확인한 후 사용을 허가하고 관리자의 승인 내역을 전자적인 매체 또는 수기문서 대장에 기록하여야 합니다.
- 보조저장매체 이용관리 현황 등 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

23. 데이터베이스 서버 및 데이터베이스 접속 애플리케이션 서버에 접속하는 모든 개인정보 취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 정당한 사유가 없는 한 즉시 수행하고 있습니까?

- 보안패치는 운영체제나 응용프로그램에 내재된 보안 취약점을 보완하는 소프트웨어로서 보안패치를 할 경우 취약점을 악용하는 악성코드 감염을 방지합니다.

- 운영체제나 응용프로그램의 보안 취약점은 해커에 의한 공격 경로를 제공할 수 있으므로, 운영체제 제조사 등에서 업데이트 공지가 있는 경우 최신 보안패치를 즉시 적용합니다.
- ‘정당한 사유가 없는 한 즉시’란 개인정보취급자 단말기(PC, 노트북 등)의 운영체제 보안패치에 대한 제조사 공지 후 적용하기까지 소요되는 합리적인 최소한의 시간을 의미합니다.
- 데이터베이스 접속 단말기의 운영체제 보안패치 현황 등 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

24. 하드디스크(HDD)등 데이터베이스 저장매체의 불용처리 시(폐기, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?

- 저장매체의 폐기, 교체 등 불용처리로 저장매체에 저장된 개인정보는 모두 파기해서 외부에 노출되지 않도록 해야 하며, 복구될 수 없도록 완전히 삭제해야 합니다. 암호화되지 않은 개인정보는 저장매체의 불용처리로 인해 외부에 반출되거나 복구될 경우 개인정보 유출 위험이 있습니다.
- 파일을 삭제하거나 하드디스크를 포맷한 후 중고로 매매하는 경우가 종종 있으나 파일 삭제 또는 하드디스크 포맷만으로는 데이터 영역이 완전하게 삭제되지 않아 복구될 수 있습니다. 중고 하드디스크에 개인정보가 남아있을 경우 개인정보 오남용의 위험성이 있으므로 이를 방지하기 위하여 다음 중 어느 하나의 조치가 필요합니다.

- 완전파괴(소각·파쇄 등)

※ 예시: 개인정보가 저장된 회원가입신청서 등의 종이문서, 하드디스크나 자기테이프를 파쇄기로 파기 또는 용해하거나 소각장, 소각로에서 태워서 파기 등

- 전용 소자장비를 이용하여 삭제

※ 예시: 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제 등

- 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

※ 예시: 개인정보가 저장된 하드디스크에 대해 완전포맷(3회 이상 권고), 데이터 영역에 무작위 값(0, 1 등)으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등

- 데이터베이스 저장매체 불용처리 절차 및 현황 등 관련 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

②-2. 웹(Web) 기반

25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단 또는 보안을 연 1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호조치를 하고 있습니까?

- 개인정보가 내부망에 존재할 때 외부에서의 접근은 불가능하지만 외부에 의해 해킹이 일어나는 경우는, 주로 다른 시스템을 경유하여 일어나며 대표적으로는 외부에 오픈되어 있는 웹서버를 통하여 발생할 수 있습니다.
- 웹서버를 통한 해킹 방지를 위해 웹 취약점 진단을 정기적으로 실시하여 보완하거나 웹 방화벽을 통해 웹서버 자체에 대한 공격을 방지하기 위한 조치가 필요합니다.
- 웹 취약점 진단
 - 해커는 웹서버 자체의 취약점을 직접 공격하거나 웹 애플리케이션의 취약점을 공격하여 개인정보를 유출합니다. 데이터베이스에 외부로부터 접근할 수 있는 거의 유일한 통로이므로 웹 취약점에 대한 공격이 집중적으로 이루어져 대부분의 개인정보 유출사고의 경로가 됩니다.
 - 데이터베이스 접근제어 솔루션을 적용하더라도 SQL Injection 등의 취약점 공격을 완전히 막기는 어려우므로 웹 애플리케이션의 취약점을 제거하여 이를 사전에 방지해야 합니다.
 - 해킹기술이 발달하고 서비스 환경이 변화함에 따라 계속 새로운 취약점이 발생하므로 연 1회 이상 정기적으로 웹 취약점을 점검해야 하며, 긴급한 취약점 발생 시에도 추가적인 취약점 점검을 통한 보완조치가 필요합니다.
- 웹 방화벽
 - 웹서버를 통해 데이터베이스 정보를 유출하고자 하는 SQL Injection, 웹서버 자체를 해킹하고자 하는 웹셸 등의 공격을 효과적으로 방어하여 웹 해킹을 방지합니다.
- 웹 취약점 점검 현황, 점검 조치 결과, 주기적 점검계획 등이 포함된 증적자료나 웹 방화벽 운영현황 등 웹서버 보호조치 현황을 ‘위험도 분석 결과보고서’에 첨부합니다.

26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 정당한 사유가 없는 한 즉시 수행하고 있습니까?

- 보안패치는 운영체제나 응용프로그램에 내재된 보안 취약점을 보완하는 소프트웨어로 보안패치를 할 경우 취약점을 이용하는 악성코드 감염을 방지합니다.
- 운영체제나 응용프로그램의 보안 취약점은 해커에 의한 공격 경로를 제공할 수 있으므로 운영체제 제조사 등에서 업데이트 공지가 있는 경우 최신 보안패치를 즉시 적용합니다.
- ‘정당한 사유’란 보안패치 등 최신 업데이트의 무결성 검토, 시스템 적용 시 운영 연속성 테스트 등 개인정보처리시스템의 안정적 운영을 위해 필요한 최소한의 경우를 의미합니다.
- 웹서버의 보안패치 현황 등 증적자료를 ‘위험도 분석 결과보고서’에 첨부합니다.

3 위험도 분석 결과보고서

작성일	년 월 일	작성자	(소속)	(성명)
개인정보파일명				



작성 예시

[목차]

I. 현황 조사

1. 개인정보파일 현황 (※ 고유식별정보 항목 및 암호화 현황 포함)
2. 고유식별정보 현황
3. 네트워크 및 시스템 구성도

II. 기관 기준 보호조치 현황

1. 정책 기반 보호조치
 - 조직도, 책임자, 역할 및 책임
 - 내부 관리계획 및 침해사고 대응계획 수립 현황
 - 외주 보안관리 현황
 - 소프트웨어 사용 정책
 - 개인정보취급자 교육 현황
2. 네트워크 기반 보호조치
 - IP 접근통제 및 서비스 포트 제한 현황
 - 정보보호시스템 운영 및 모니터링 현황
 - 네트워크 바이러스 차단 현황
 - 네트워크 접속기록 관리 및 분석 현황
 - 네트워크 장비 및 정보보호시스템 업데이트 현황 (※ 보안패치 및 패턴갱신 등 포함)

III. 개인정보처리시스템 기준 보호조치 현황

1. 데이터베이스 및 애플리케이션 기반 보호조치
 - 데이터베이스 접근통제 현황
 - 데이터베이스 서버 서비스 포트 제한 현황
 - 데이터베이스 접속기록 관리 및 모니터링 현황
 - 관리자 PC 네트워크 분리 현황
 - 데이터베이스 접근 권한 부여 현황 및 변경·말소 내역
 - 비밀번호 관리 정책 및 현황
 - 물리적 접근통제 현황
 - 보조저장매체 이용 관리 현황
 - 운영체제 보안패치 현황 (※ 데이터베이스 서버 및 데이터베이스 서버 접속 단말기 포함)
 - 데이터베이스 저장매체 불용처리 절차 및 현황
2. 웹 기반 보호조치
 - 웹 취약점 점검 현황 및 결과 (※ 조치결과, 주기적 점검계획 등 포함)
 - 웹서버 보호조치 현황 (※ 웹방화벽 운영현황 등)

IV. 위험도 분석 결과

- 위험도 분석 점검에 의한 암호화 여부 판정 결과 등

- ‘위험도 분석 결과보고서’에는 위험도 분석 기준 작성에 대한 증적과 위험도 분석 점검에 따른 암호화 여부 등 위험도 분석 결과를 작성합니다.
- 개인정보처리자는 위험도 분석 점검 내용에 대한 입증 책임이 있으며, 위험도 분석 결과의 허위 작성을 방지하기 위하여 ‘위험도 분석 점검 항목’에 ‘예’로 체크했다면 그에 대한 증적을 명시하여야 합니다.
- ‘위험도 분석 점검 항목’에서 어느 하나의 점검항목이라도 ‘아니요’에 해당하는 경우, 암호화에 상응할만한 충분한 보호조치가 이루어지고 있다고 볼 수 없으므로 암호화에 상응하는 조치를 이행하거나 해당 개인정보파일에 대해 암호화 조치를 수행합니다.
- ‘위험도 분석 점검 항목’과 ‘위험도 분석 결과보고서’는 개인정보 보호책임자 또는 해당부서장의 결재를 받은 후 보관합니다.
- ‘위험도 분석’은 개인정보파일 단위로 분석하고 결과보고서를 작성하여야 하며, 개인정보 파일을 위탁하여 관리하는 경우에도 위탁기관의 책임하에 작성합니다.
※ 결과보고서는 기관의 문서관리 규정에 따라 ‘대외비’ 등으로 관리하시기 바랍니다.
- 개인정보처리시스템 증설, 내·외부망 연계 등 기타 운영환경이 변경된 경우, 위험도가 새롭게 발생될 수 있으므로 위험도 분석을 지속적으로 실시하여 개인정보의 안전한 관리가 가능하도록 조치합니다.

제4장 암호화 조치 관련 참고 웹사이트

사이트명	URL	주요 내용	운영기관
암호모듈 검증	nis.go.kr/AF/1_7_3_1.do	<ul style="list-style-type: none"> • 암호모듈 검증 제도 소개 • 검증대상 암호알고리즘 • 검증필 암호모듈 목록 	국가정보원
암호이용 활성화	seed.kisa.or.kr	<ul style="list-style-type: none"> • 국내 암호기술 • 차세대 암호기술 • 암호모듈 검증제도 • 암호 관련 자료 등 	한국인터넷 진흥원

개인정보의 안전성 확보조치 기준 안내서

발 행 일 2024년 10월
발 행 처 개인정보보호위원회
지원기관 한국인터넷진흥원
디 자 인 호정씨앤피(☎02-2277-4718)



여성기업

※ 최신자료는 “개인정보보호위원회 누리집(pipc.go.kr)”, “개인정보 포털(privacy.go.kr)”에서 확인할 수 있습니다.

개인정보의 안전성 확보조치 기준 안내서



개인정보보호위원회

personal Information Protection Commission