개인정보보호법고시
개인정보의 안전성 확보조치 현행 고시 및 안내서 변동사항 (24.10.31 공개)

2024.10.31 발행
개인정보의 안전성 확보조치 기준 안내서

2023.09.22 시행
개인정보의 안전성 확보조치 기준

2020.12.02 발행
개인정보 보호법령 및 지침·고시 해설서

조항	키워드	2023.09 시행 현행 고시	기존 고시 대비 변경내용	안내서 신설 변경 내용	기술적 보호조치
1조 목적	고시목적	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	변동사항 없음	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.** **(2년 이하 징역, 2천만원 이하 벌금 삭제)**	
2조 정의	용어정의	1. 개인정보처리시스템 2. 이용자 3. 접속기록 4. 정보통신망 5. P2P 6. 공유설정 7. 모바일기기 8. 비밀번호 9. 생체정보 10. 생체인식정보 11. 인증정보 12. 내부망 13. 위험도분석 14. 보조저장매체	(추가) 이용자, P2P, 공유설정, 모바일기기, 생체정보, 생체인식정보, 인증정보, 내부망, 보조저장매체 (삭제) 정보주체, 개인정보파일, 대기업, 중견기업, 중소기업, 소상공인, 개인정보보호책임자, 개인정보취급자, 정보통신망, 공개된 무선망	1. 개인정보 처리시스템이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템 · 데이터베이스를 구성 운영하는 시스템 그 자체 · 웹서버, WAS서버 등 응용시스템 **· FTP서버, 백업서버 등 파일처리시스템** **· 클라우드 컴퓨팅 환경에 구축한 시스템 또는 서비스**	
				5. P2P(Peer to Peer)이란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것 · 정보 제공자(개인)와 정보 수신자(개인)가 직접 연결되어 각 개인이 가지고 있는 파일 등을 공유하는 것을 말한다(개인↔개인).	
				6. 공유설정이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것 **· 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 해당**	
				14. 보조저장매체란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장매체를 지칭 · 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 포함됨 **(CD, DVD 삭제)** **· 경우에 따라서는 스마트폰도 보조저장매체에 해당됨**	
3조 안전조치 적용원칙	적용원칙	개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용	개인정보 처리자유형 및 보유량에 따른 기준 폐지 (대기업, 중견, 소상공인)	· 개인정보처리자가 개인정보를 처리할 때 개인정보가 분실·도난·유출·위조·변조 또는 훼손 등이 되지 않도록 기술적·관리적·물리적 안전조치에 관한 최소한의 기준을 정한 것이며 개인정보 처리자는 해당 기준 외 필요한 추가적 기준을 수립, 적용, 점검해야 함.	
4조 내부관리 계획의 수립시행 및 점검	관리적 조치	① 개인정보처리자는 개인정보 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립·시행 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있음.	소상공인 예외규정 단서 신설	· 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체도 내부 관리계획 외에 개인정보 보호를 위하여 필요한 계획(예: 체크리스트)을 자율적으로 수립하여 시행할 수 있음. 해당 기준에서 정한 해당되는 다른 안전조치 의무사항은 이행되어야 함.	개인정보보호 컨설팅
5조 접근권한의 관리	권한 최소화	① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 함.	변동사항 없음	· 업무 수행에 필요한 최소한의 범위란 개인정보취급자가 각자의 업무를 수행하기 위해 필요한 최소한의 단위로 접근 권한을 구분하는 것 · 이를 위해 업무별로 접근 가능한 메뉴 및 상세 권한(열람, 입력, 삭제, 수정, 다운로드, 인쇄 등)을 세분화하여 관리	DB DLP DB 접근제어
		④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 함	변동사항 없음	· '정당한 사유'란 개인정보취급자의 계정은 원칙적으로 개별로 발급되어야 하나, 시스템이 제공하는 고정된 계정(root 등)과 같이 기술적으로 개별 발급이 불가능한 경우 · '계정 관리 대장, 접근제어 시스템 도입 등 관리적 또는 기술적 보완통제로써 실제 개인정보처리시스템에 접속한 자를 식별할 수 있도록 하여야 함	DB접근제어

조항	키워드	2023.09 시행 현행 고시	기존 고시 대비 변경내용	해설서 신설 변경 내용	기술적 보호조치
6조 접근통제	접근제한	① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 안전조치를 하여야 함. 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	일부용어 변경 IP(Internet Protocol) → 인터넷 프로토콜 (IP)	· 로그 분석: 로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 및 차단하여야 함. **※ 로그는 개인정보처리시스템의 접속기록, 네트워크 장비의 로그기록, 보안장비소프트웨어의 기록 등을 포함** **· IP 주소 등에는 IP 주소, 포트 그 자체뿐만 아니라,** **이상행위(과도한 접속성공 및 실패, 부적절한 명령어 등 패킷)를 포함하여야 함.**	DB접근통제 Network DLP 방화벽 IPS
	유출차단	③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 함	일부 변경 업무용 컴퓨터, 모바일기기, 관리용단말기 등 접근통제 등에 관한 조치 → 개인정보 취급자의 컴퓨터 및 모바일기기에 조치	**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 등 설계구현 오류로 인한 개인정보 유·노출 **· 크리덴셜 스터핑 공격 등으로 인한 개인정보 유출** **· 클라우드 보안설정 미흡으로 인한 개인정보 유·노출** · 기타 방법을 통한 개인정보 유·노출 **P2P, 공유설정 관련 안전조치 예시** · 불가피한 공유설정 시 비인가자가 접근하지 못하도록 비밀번호 등 접근통제 설정, 사용 완료 후 공유설정 제거 **· 파일 전송이 주된 목적일 때에는 읽기 권한만을 주고 상대방이 쓰기를 할 때만 개별적으로 쓰기 권한을 설정** **· P2P, 상용 웹메일, 웹하드, 메신저, SNS 서비스 사용을 금지하여** **고의·부주의로 인한 개인정보 유·노출 방지 (DLP, DRM, 매체제어)** · WPA3(Wi-Fi Protected Access 3) 등 보안 프로토콜이 적용된 무선망 이용 등	Network DLP Endpoint DLP 비업무/유해차단 솔루션 (읽기권한 설정)
	망분리	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 함.	**기존** **개인정보의 기술적 관리적** **보호조치 기준** **4조 (접근통제) ⑥항 규정 이관**	· 물리적 인터넷망 차단조치 정의 : 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리 **· 논리적 인터넷망 차단조치 정의 :** **물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등 방법으로** **인터넷 접속이 불가능한 내부 업무영역과 인터넷 접속영역을 분리하는 방식** · 개인정보처리시스템에서 개인정보를 다운로드, 파기, 권한설정할 수 있는 컴퓨터는 인터넷망 차단조치 필수	논리적 망분리 (클라우드 PC) 물리적 망분리
7조 개인정보의 암호화	암호화저장 개인정보	② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장 1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 생체인식정보	**신용카드, 계좌번호** 암호화대상 추가	-	Endpoint DLP Server DLP 파일암호화 DB암호화
8조 접속기록의 보관 및 점검	접속기록 관리	① 개인정보처리자는 개인정보처리시스템 접속기록을 1년 이상 보관·관리함. 다만, 다음 각 호의 어느 하나에 해당하는 경우 2년 이상 보관·관리. 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템 3. 개인정보처리자로서 「전기통신사업법」에 따라 등록, 신고한 기간통신사업자	변동사항 없음	· 가명정보는 추가 정보의 사용 없이는 정보주체를 식별할 수 없으므로 해당 데이터를 식별할 수 있는 가명정보ID, 일련번호 등이 있다면 '처리한 정보주체 정보' 항목으로 해당 정보를 기록하여야 하며, 가명처리된 데이터를 구별할 수 있는 정보가 없는경우는 '처리한 정보주체 정보' 항목을 남기지 않을 수 있음.	DB접근제어 (개인정보 접속기록관리) APP서버 로그관리

조항	키워드	2023.09 시행 현행 고시	기존 고시 대비 변경내용	해설서 신설 변경 내용	기술적 보호조치
9조 악성 프로그램 등 방지	**악성 프로그램**	① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며 다음 사항을 준수해야 함. 1. 프로그램의 자동 업데이트 기능 사용 또는 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치	변동사항 없음	· 개인정보처리자는 악성프로그램(바이러스, 웜, **랜섬웨어,** 스파이웨어, 웹셸 등) 등을 통해 개인정보가 위·변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 보안 프로그램을 설치·운영 · 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우 해당 클라우드컴퓨팅서비스제공자가 지원하는 기능을 이용하여 보안 프로그램에 필요한 조치 수행	Endpoint DLP 안티바이러스 EDR
		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 실시	기존 1항 3호를 2항으로 이동	· 악성프로그램의 감염을 예방하고 감염된 경우 피해를 최소화하기 위해 정당한 사유가 없는 한 즉시 업데이트를 실시	Endpoint DLP EDR 안티바이러스
10조 물리적 안전조치	**출입통제 절차**	① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우 출입통제 절차 수립·운영	변동사항 없음	-	개인정보보호 컨설팅
	잠금장치	② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관			시건장치 캐비닛
	반출입 보안대책	③ 개인정보처리자는 개인정보 포함 보조저장매체 반출·입 통제를 위한 보안대책을 마련해야 함. 다만, 별도 개인정보처리시스템을 운영하지 않고 업무용 컴퓨터 또는 모바일기기를 이용하여 개인정보를 처리하는 경우 예외.			매체제어 Endpoint DLP
제11조 재해·재난 대비 안전조치	**위기대응**	10만명 이상 정보주체 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 개인정보를 처리하는 중소기업·단체는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 조치를 하여야 함 1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검 2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련	10만명 이상 개인정보 처리 대기업·중견기업·공공기관 또는 100만명 이상 개인정보 처리 중소기업·단체 해당 규정 적용대상 명시	· 클라우드컴퓨팅 자원 등에 개인정보처리시스템을 구축한 개인정보처리자도 책임 및 역할 등에 따라 이용기관 측면에서의 위기대응 매뉴얼 등 대응절차를 마련해야 함	
12조 출력복사시 안전조치	**출력물**	① 출력(인쇄, 표시, 생성) 용도 특정 및 출력항목 최소화	**기존 개인정보의 기술적 관리적 보호조치 기준 9조 (출력 복사시 보호조치) 규정 이관**	개인정보처리자는 개인정보처리시스템에서 **개인정보를 출력(인쇄, 화면표시, 파일생성 등)** 할 때에는 다음사항 등을 고려하여 용도를 특정하고, 용도에 따라 출력 항목을 최소화하여야 함 · 개인정보처리자는 출력 항목을 최소화하기 위해 용도에 따라 출력항목을 차등화하여 표시 또는 개인정보를 마스킹 하는 등의 방법을 활용 · 다수 개인정보처리시스템 등에서 개인정보를 각기 다른 방식으로 마스킹시 해당 방법을 악용하여 개인정보취급자가 이용자 개인정보 집합을 구성할 수 있으므로 일관된 동일한 방식의 표시제한 조치가 필요	DB접근제어 Endpoint DLP Server DLP
		② 종이인쇄물, 개인정보파일이 포함된 외부저장매체 관리조치 구축		**개인정보 포함 외부저장매체 등의 복사물을 통한 개인정보의 분실·도난·유출 방지 및 복사물의 안전한 관리를 위해 DLP(Data LossPrevention), 문서보안(DRM), 보안 USB 등의 보안솔루션을 적용할 수 있음** **· 개인정보취급자 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 관리**	Endpint DLP 매체제어 DRM
13조 개인정보의 파기	**파기**	① 개인정보를 파기할 경우 다음 하나의 조치를 하여야 함 1. 완전파괴(소각·파쇄 등) 2. 전용 소자장비 이용 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 ② 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 조치를 수행. 1. 전자적 파일 : 개인정 삭제 후 복구 및 재생되지 않도록 관리 및 감독	변동사항 없음	· 전자적 데이터는 완전 삭제 프로그램 등을 이용하여 복구할 수 없는 방법으로 파기	Endpoint DLP Server DLP 외 전문삭제 프로그램

*공공시스템 운영기관 등의 개인정보 안전성 확보조치는 본 리포트에 포함하지 않았음