개인정보 내부관리 계획 신·구조문대비표

현 행	개 정 안
제1조 목적 양천구시설관리공단 개인정보 내부 관리계획은 「개인정보 보호법」 제29조와 같은 법 시행령 제30조 및 '개인정보의 안전성 확보 조치 기준'(제2016-35호)에 따라 공단에서 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.	**제1조 목적** - 관련 법령 수정 양천구시설관리공단 개인정보 내부 관리계획은 「개인정보 보호법」 제29조와 같은 법 시행령 제16조제2항, 제30조 및 제30조2에 따라 공단에서 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.
제4조 내부 관리계획의 수립·변경 및 승인 ① 개인정보 보호책임자는 공단에서 처리하는 개인정보 및 개인영상 정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부의사결정 절차를 통하여 내부관리계획을 수립 또는 개정하여야 하며, 영상정보 담당자는 필요한 경우 개인정보처리시스템 또는 영상정보처리기기별로 자체 실정에 맞게 내부관리계획을 수립하여 시행하여야 한다.	**제4조 내부 관리계획의 수립·변경 및 승인** - 최신 법령 적용 ① 개인정보 보호책임자는 공단에서 처리하는 개인정보 및 영상정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 내부관리계획을 수립 또는 개정하여야 하며, 영상정보 담당자는 필요한 경우 개인정보처리시스템 또는 영상정보처리기기별로 자체 실정에 맞게 내부관리계획을 수립하여 시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다. ⑤ 개인정보처리자는 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.
제7조 개인정보 관리조직의 구성	**제7조 개인정보 관리조직의 구성** - 신규 부서 추가
제16조 접근 권한 관리 ⑥ 개인정보 보호책임자는 권한 있는 개인정보취급자만 개인정보처리 시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.	**제16조 접근 권한 관리** - 최신 법령 적용 ⑥ 개인정보 보호책임자는 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.
제17조 접근 통제 ① 개인정보 보호책임자는 정보통신망을 통한 불법적인 접근 및 침해 사고 방지를 위해 다음 각 호의 기능을 포함한 침입차단시스템 (Firewall	**제17조 접근 통제** - 최신 법령 적용 ① 개인정보 보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

현 행	개 정 안
System) 또는 침입방지시스템(Intrusion Prevention System)을 설치·운영하여야 한다. 1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한할 수 있는 시스템 2. 개인정보처리시스템에 접속한 IP(Internet Protocol) 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지 및 대응할 수 있는 시스템 ② 개인정보 보호책임자는 외부망으로 부터 개인정보처리시스템에 대한 접속을 원칙적으로 차단하여야 한다. 다만, 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요 한 경우 가상사설망(VPN : Virtual Private Network) 또는 전용 선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여 야 한다. ③ 개인정보 보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P (Peer to Peer), 공유설정, 공개된 무선망 이용 등을 통해 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리 시스템, 업무용 개인정보취급자의 업무용 컴퓨터 및 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 취하여야 한다. ⑤ 개인정보 보호책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 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 개인정보 보호책임자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상 사설망 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. ⑤ 개인정보 보호책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.
제18조 개인정보의 암호화 ① 개인정보 보호책임자는 고유식별정보, 비밀번호, 바이오정보를 정보 통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. ② 개인정보 보호책임자는 비밀번호 및 바이오정보(지문, 홍채 등)는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향(해쉬함수) 암호화하여 저장하여야 한다. ③ 개인정보 보호책임자는 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다. ④ 개인정보 보호책임자가 내부망에 고유식별정보를 저장하는 경우에는 다	**제18조 개인정보의 암호화** - 최신 법령 적용 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 개인정보 보호책임자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호

현 행	개 정 안
음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다. 1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 정보시스템의 경우에는 해당 개인정보 영향평가의 결과 2. 암호화 미적용시 위험도 분석에 따른 결과 ⑤ 개인정보 보호책임자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다. ⑥ 개인정보 보호책임자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다. ⑦ 개인정보 보호책임자는 개인정보취급자가 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다. ⑧ 이메일을 통해 개인정보를 전송하는 경우 이메일 첨부 문서를 암호화하여 전송하여야 한다.	5. 신용카드번호 6. 계좌번호 7. 생체인식정보 ③ 개인정보 보호책임자는 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 개인정보 보호책임자는 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 보조 저장매체 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 보호책임자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다. ⑦ 이메일을 통해 개인정보를 전송하는 경우 이메일 첨부 문서를 암호화하여 전송하여야 한다.
제19조 접속기록의 보관 및 점검 ① 개인정보 보호책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상(5만명 이상 정보주체의 개인정보 또는 고유식별정보, 민감정보 처리 시 2년 이상) 보관·관리하여야 한다. ② 개인정보 보호책임자는 개인정보의 분실·도난·유출·위조·변조 또는	**제19조 접속기록의 보관 및 점검** - 최신 법령 적용 ① 개인정보 보호책임자는 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 개인정보처리

현 행	개 정 안
훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.	시스템에 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 개인정보 보호책임자는 개인정보의 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.
제29조 재해·재난 대비 안전조치 ① 개인정보 보호책임자 및 분야별 책임자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검하여야 한다. ② 개인정보 보호책임자 및 분야별 책임자는 재해·재난 발생 시 개인정보처리시스템의 백업 및 복구를 위한 계획을 마련하여야 한다. ※ 세부사항은 「재해·재난 대비 개인정보처리시스템 위기대응 지침」참고	**제29조 재해·재난 대비 안전조치** - 최신 법령 적용 ① 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 ※ 세부사항은 「재해·재난 대비 개인정보처리시스템 위기대응 지침」참고
제34조 영상정보처리기기 운영·관리 방침 수립 및 공개	**제34조 고정형 영상정보처리기기 운영·관리 방침 수립 및 공개** - 명칭 변경