

문서번호	경영지원실-965
보존년한	준영구
보고일자	
공개여부	공개

차장	총무회계팀장	실장	문화관광본부장
박정영	이건훈	권오경	전결 02/13 이경수
협조	대리 이승환		

2020년 개인정보 내부관리 계획[개정]



安東市施設管理公團
Andong City Facilities Management Corporation

목 차

제1장 총 칙

제1조 목적	1
제2조 용어정의	1
제3조 적용범위	3

제2장 내부 관리계획의 수립 및 시행

제4조 내부 관리계획의 수립 및 승인	4
제5조 내부 관리계획의 공표 및 시행	4

제3장 개인정보보호책임자의 역할 및 책임

제6조 개인정보보호책임자의 지정	5
제7조 개인정보보호책임자의 역할 및 책임	5
제8조 개인정보취급자의 역할 및 책임	6

제4장 개인정보보호 교육

제9조 개인정보보호책임자의 교육	7
제10조 개인정보취급자의 교육	7

제5장 개인정보의 기술적 안전조치

제11조 접근권한 관리	8
제12조 접근통제	9
제13조 개인정보의 암호화	10
제14조 접속 기록 보관 및 점검	11
제15조 악성프로그램 등 방지	11
제16조 관리용 단말기의 안전조치	12

제6장 관리적 안전조치

제17조 개인정보 보호조직 구성 및 운영	13
------------------------------	----

제7장 개인정보 침해대응 계획 수립·시행

제18조 개인정보 유출사고 대응 계획 수립·시행	13
제19조 개인정보 위험도 분석 및 대응방안	14
제20조 위탁계약 및 위탁업무의 공개	14
제21조 수탁자에 대한 관리·감독	14

제8장 물리적 안전조치

제22조 물리적 안전조치	15
제23조 재해·재난 대비 안전조치	16
제24조 개인정보파일 등록 및 변경	16
제25조 개인정보의 파기	16
제26조 처리실태 조사	17

제9장 영상정보처리기기 관리계획

제27조 영상정보처리기기 설치 및 운영관리	18
제28조 영상정보처리기기 운영·관리 방침 수립 및 공개	20
제29조 개인영상정보의 보호조치	20
제30조 영상정보처리기기 설치 및 관리 등의 위탁 및 제3자 제공 ..	21
제31조 보관 및 파기	22

제10장 기타

제32조 법령과의 관계	22
--------------------	----

[별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준	23
--	----

개인정보 내부 관리계획 개정이력

개정 번호	변 경 내 용	개인정보 보호담당자	개인정보 보호책임자	작성일
1	개인정보보호법에 의거 최초작성	전산7급 박정영	본 부 장 김운현	2014. 2. 11.
2	제13조(접속, 기록보관, 점검 및 위변조 방지) ③항 추가 제16조 수탁자 관리·관리 추가	전산6급 권영성	본 부 장 김운현	2015. 6. 26.
3	○ 제4장 개인정보의 관리적·기술적·물리적 안전조치 보완 ○ 제8장 개인정보 처리 위탁, 제9장 영상 정보처리기기 관리계획 추가	전산6급 박정영	상임이사 이 경 수	2018. 6. 25.
4	○ 제2조 적용범위 내용 수정 ○ 제3조 용어정의 내용 수정 ○ 제4조 내부 관리계획의 수립의 내용 및 제목 수정 ○ 제5조 내부 관리계획의 시정 내용 및 제목 수정 ○ 제10조 접근권한 관리 내용 수정 ○ 제11조 비밀번호 설정 내용 수정 ○ 제20조 개인정보 유출사고 대응 계획 수립·시행 내용 수정	전산5급 박정영	경영본부장 (상임이사) 이 경 수	2019. 1. 14
5	○ <신설> 제17조 개인정보 보호조직 구성 및 운영	전산5급 박정영	상임이사 이 경 수	2020. 2. 12.
	이 하 여 백			

개인정보 내부 관리계획

제1장

총 칙

제1조(목적)

개인정보 내부 관리계획은 「개인정보 보호법」 제23조제2항, 제24조제3항 및 제29조와 같은법 시행령 제21조 및 제30조에 따라 안전조치의무에 따라 공단에서 처리하는 개인정보 및 개인영상정보를 체계적으로 관리하여 개인정보 및 개인영상정보가 분실·도난·유출·변조·훼손되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 세부적인 기준을 정하는 것을 목적으로 한다.

제2조(용어정의)

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상(사진, 그림, 이미지 포함) 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. “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.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

6. “개인정보 보호책임자”란 공단의 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
7. “개인정보보호담당자”란 “개인정보보호책임자”의 지시를 받아 실무를 처리하고 다수의 “개인정보취급자”를 대표 할 수 있는 자를 말한다.
8. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
9. “개인영상정보보호담당자”란 “개인정보보호책임자”의 지시를 받아 실무를 처리하고 다수의 “개인영상정보취급자”를 대표할 수 있는 자를 말한다.
10. “개인영상정보”란 영상정보처리기기에 의하여 촬영·처리·저장되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
11. “개인정보취급자”란 공단에서 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 담당하는 자를 말한다.
12. “개인영상정보취급자”란 영상정보처리기기를 운영하는 자를 말한다.
13. “영상정보처리기기”란 폐쇄회로 텔레비전(CCTV), 네트워크 카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망으로 통하여 전송하는 일체의 장치를 말한다.
14. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
15. “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.
16. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 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.
17. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를

이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

18. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
19. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
20. “고유식별정보”란 개인을 고유하게 구별하기 위하여 부여된 식별 정보를 말하는 것으로 개인정보 보호법에서는 법령에 따라 규정된 정보로 한정하고 있으며 주민등록번호, 여권 번호, 운전 면허 번호, 외국인등록번호를 고유 식별 정보로 규정하고 있다.
21. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
22. “보조저장매체”란 이동형 하드디스크, USB메모리, CD (Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리 시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
23. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
24. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
25. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(적용범위)

본 계획은 공단에서 전자적 처리를 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 전자적 처리 이외의 수단을 통해서 수집, 이용,

제공 또는 관리되는 개인정보와 공개된 장소에 설치·운영하는 영상정보처리 기기를 통하여 처리되는 개인영상정보에 대해서도 적용되며, 개인정보를 처리하거나 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게도 본 개인정보 내부 관리계획이 적용된다.

제2장 내부 관리계획의 수립 및 시행

제4조(내부 관리계획의 수립 및 승인)

- ① 개인정보보호책임자는 공단에서 처리하는 개인정보 및 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부의사결정 절차를 통하여 내부 관리계획을 수립 또는 개정하여야 하며, 개인영상정보담당자는 필요한 경우 개인정보처리시스템 또는 영상정보처리기기별로 자체실정에 맞게 내부 관리계획을 수립하여 시행하여야 한다.
- ② 개인정보보호책임자는 개인정보 및 개인영상정보 보호를 위한 내부 관리계획의 수립 또는 개정 시 관계 법령 및 규정을 준수할 수 있도록 내부의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.
- ③ 개인정보 보호책임자는 제1항, 제2항, 제3항에 따라 내부 관리계획을 수립하거나 수정하는 경우에는 최고경영자로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관·관리하여야 한다.
- ④ 개인정보보호담당자 및 처리자는 개인정보보호 내부관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 세부추진계획을 수립·시행할 수 있다.
- ⑤ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제5조(내부 관리계획의 공표 및 시행)

- ① 개인정보보호책임자는 제4조제3항에 따라 승인된 내부 관리계획을 모든 임직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.
- ② 내부 관리계획은 각 부서에 공문으로 발송하고 전 직원들이 언제든지

열람할 수 있도록 내부 행정업무시스템의 게시판에 게시 또는 비치하여 제동하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 역할 및 책임

제6조(개인정보 보호책임자의 지정)

공단의 개인정보 보호책임자(CPO : Chief Privacy Officer)는 『개인정보 보호법』 제31조와 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 문화관광본부장(상임이사)으로 정한다.

제7조(개인정보보호책임자의 역할 및 책임)

① 개인정보 보호책임자는 다음 각 호의 임무를 수행하여야 한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오·남용을 방지하기 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립과 시행
6. 개인정보파일의 보호 및 관리·감독
7. 「개인정보 보호법」 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보보호책임자는 담당자 및 취급자로부터 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고 받을 수 있으며, 이를 수시로 관리·감독하여야 한다.

제8조(개인정보취급자의 역할 및 책임)

- ① 개인정보보호분야별책임자는 개인정보 파일을 수집·보유하는 업무를 수행하는 부서의 장 또는 영상정보처리기기의 설치·운영업무를 수행하는 부서의 장으로 한다.
- ② 개인정보보호분야별책임자는 다음 각 호의 업무를 수행한다.
 1. 개인정보취급자 및 개인영상정보취급자 지정 및 관리·감독·교육
 2. 개인정보 및 개인영상정보 처리 실태 관리
 3. 개인정보 및 개인영상정보 파일의 지정·보호 및 관리·감독
 4. 처리목적이 달성되거나 보유기간이 지난 개인정보 및 개인영상정보의 파기
 5. 개인정보처리방침 및 영상정보처리기기 운영·관리 방침의 홈페이지 공개
 6. 개인정보 및 개인영상정보와 관련한 열람청구, 정정·삭제, 처리 정지 등 정보주체의 권리 보장
 7. 개인정보 및 개인영상정보 보호 관련 자료 관리 및 제출
 8. 개인정보 및 개인영상정보 유출 시 통지 및 피해확산 방지
 9. 개인정보 및 개인영상정보 관련 개선 권고사항 시정 조치 이행
 10. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리·감독
- ③ 개인정보보호분야별책임자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.
- ④ 개인정보취급자 및 개인영상정보취급자의 범위는 개인정보보호 분야별 책임자의 지휘·감독을 받아 개인정보 및 개인영상정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말한다. 직원 이외에 공무원직근로자, 기간제근로자, 공익근무요원, 공공근로자, 아르바이트생, 봉사활동 참가자, 각종 강좌 진행 강사, 외부 용역업체 직원 및 공단에서 제공하는 서비스 이용자에게도 적용될 수 있다.
- ⑤ 개인정보취급자는 개인정보 보호와 관련하여 다음과 같은 역할 및 책임을 이행하여야 한다.
 1. 개인정보 보호 활동 참여와 내부 관리계획의 준수 및 이행

2. 개인정보의 관리적·기술적·물리적 보호조치 기준 이행
 3. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검
 4. 기타 개인정보 보호를 위해 필요한 사항의 이행 등
- ⑥ 개인영상정보취급자는 개인영상정보 보호와 관련하여 다음과 같은 역할 및 책임을 이행하여야 한다.
1. 개인영상정보 보호 활동 참여와 내부 관리계획의 준수 및 이행
 2. 개인영상정보의 보호조치 기준 이행
 3. 직원 또는 제3자에 의한 위법·부당한 개인영상정보 침해행위에 대한 점검
 4. 기타 개인영상정보 보호를 위해 필요한 사항의 이행

제4장 개인정보보호 교육

제9조(개인정보 보호책임자의 교육)

- ① 개인정보보호책임자는 개인정보보호취급자예를 대상으로 연1회 이상 개인정보 보호와 관련된 교육을 실시한다.
- ② 개인정보보호책임자는 개인정보 보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 직원을 대상으로 매년 정기적으로 개인정보 보호교육을 실시할 수 있다.
- ③ 교육 방법은 집체 교육뿐만 아니라, 사이버 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문 강사에 위탁하여 교육을 실시할 수 있다.

제10조(개인정보취급자의 교육)

- ① 개인정보보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보 보호 교육계획을 매년 수립하여야 한다.
 1. 교육목적 및 대상
 2. 교육내용
 3. 교육 일정 및 방법

- ② 개인정보보호책임자는 제4당에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.
- ③ 개인정보보호책임자는 개인정보 보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우 부서 회의 등을 통해 수시로 교육을 실시할 수 있다.
- ④ 개인정보보호책임자는 개인정보보호교육 계획에 의해 자체적인 교육을 실시할 수 있다.

제5장 개인정보의 기술적 안전조치

제11조(접근권한 관리)

- ① 개인정보보호책임자는 개인정보처리시스템에 대한 접근 권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하여야 한다.
- ② 개인정보보호책임자는 개인정보취급자가 전보, 퇴직 등 인사이동으로 변경 되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 부여, 변경 또는 말소하여야 한다.
- ③ 개인정보보호책임자는 제1항 내지 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관하여야 한다.
- ④ 개인정보보호책임자는 개인정보취급자별로 한 개의 사용자 계정을 발급 하여야 하며, 다른 개인정보취급자와 공유하지 않도록 하여야 한다.
- ⑤ 개인정보보호책임자는 개인정보처리시스템, 인터넷 홈페이지 등에 개인 정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용하여야 한다.
- ⑥ 사용자 계정(ID)과 동일하지 않은 비밀번호 설정 사용
- ⑦ 숫자와 영문 대·소문자, 특수문자 중 2종류 이상을 조합하여 최소 12자리 이상 또는 3종류 이상을 조합하여 최소 12자리 이상의 길이로 구성 사용
- ⑧ 개인의 신상 및 부서 명칭 등과 관계가 없는 비밀번호 설정 사용
- ⑨ 일반 사전에 등록된 단어 설정 금지

- ⑩ 동일 단어 또는 숫자 반복 설정 금지
- ⑪ 한 번 이상 사용한 비밀번호 재사용 금지
- ⑫ 비밀번호 공유 사용 금지
- ⑬ 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
- ⑭ 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않음
- ⑮ 초기 할당된 임시 비밀번호는 로그인 후 즉시 변경 설정
- ⑯ 비밀번호에 유효기간을 설정하여 분기별 1회 이상 변경 설정
- ⑰ 개인정보보호책임자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

제12조(접근통제)

- ① 개인정보보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 침입차단시스템(Firewall 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 개인정보보호책임자는 외부망으로 부터 개인정보처리시스템에 대한 접속을 원칙적으로 차단하여야 한다. 다만, 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.
- ③ 개인정보보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P (Peer to Peer), 공유설정, 공개된 무선망 이용 등을 통해 열람권한이 없는

자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 개인정보취급자의 업무용 컴퓨터 및 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 취하여야 한다.

- ④ 고유식별정보를 처리하는 개인정보보호책임자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연1회 이상 취약점을 점검하고 필요한 보완 조치하여야 한다.
- ⑤ 개인정보보호책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.
- ⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.
- ⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
- ⑧ [별표]의 유형1에 해당하는 개인정보보호분야별책임자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

제13조(개인정보의 암호화)

- ① 개인정보보호책임자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
- ② 개인정보보호책임자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
- ③ 개인정보보호책임자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

- ④ 개인정보보호책임자가 내부망에 고유식별정보를 저장하는 경우에는 다음 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 개인정보보호책임자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
- ⑥ 개인정보보호책임자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
- ⑦ 개인정보보호책임자는 개인정보취급자가 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
- ⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보보호책임자는 제6항을 아니할 수 있다.

제14조(접속 기록 보관 및 점검)

- ① 개인정보보호책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하여야 한다.
- ② 개인정보보호책임자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.
- ③ 개인정보보호책임자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제15조(악성프로그램 등 방지)

- ① 개인정보취급자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 백신 소프트웨어 등의 보안 프로그램은 실시간 감시 및 업데이트 등을 위해 항상 실행 상태를 유지하여야 한다.
2. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
3. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
4. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제16조(관리용 단말기의 안전조치) 개인정보보호분야별책임자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

- ① 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
- ② 본래 목적 외로 사용되지 않도록 조치
- ③ 악성프로그램 감염 방지 등을 위한 보안조치 적용
- ④ 개인정보보호분야별책임자는 개인정보가 포함된 정보를 출력 또는 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치 취하여야 한다.
- ⑤ 개인정보보호분야별책임자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사할 경우 출력, 복사자의 성명, 일시 등을 기재하여 개인정보 유출 등에 대한 책임소재를 확인할 수 있는 강화된 보호조치를 추가로 적용할 수 있다.
- ⑥ 개인정보취급자는 개인정보의 이용을 위하여 출력 또는 복사한 자료는 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제6장 **관리적 안전조치**

제17조(개인정보 보호조직 구성 및 운영)

- ① 개인정보책임자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보보호조직을 구성하고 운영하여야 한다.
 1. 개인정보 보호책임자의 지정
 2. 개인정보 보호책임자의 지휘·감독 하에 개인정보 보호책임자의 업무를 지원하는 담당자의 지정
 3. 개인정보를 처리하는 개인정보취급부서의 지정
- ② 개인정보 보호조직의 설치, 변경 및 폐지는 이사장으로부터 승인을 받아 정한다.
- ③ 개인정보취급부서에서는 개인정보보호조직과 충분히 협의, 조정하여 개인정보를 처리하여야 한다.
- ④ 개인정보보호조직은 제7조에 따른 업무를 수행하여야 하며, 그 밖에 개인정보의 안전성 확보를 위하여 개인정보책임자가 필요하다고 판단되는 사항을 수행할 수 있다.

제7장 **개인정보 침해대응 계획 수립·시행**

제18조(개인정보 유출사고 대응 계획 수립·시행)

- ① 개인정보 보호책임자는 개인정보취급자의 과실 및 오·남용 또는 개인정보 처리시스템의 외부 해킹 등으로 개인정보에 대한 침해·유출 사고가 발생할 경우를 대비하여 체계적이고 신속한 대응으로 피해를 최소화 할 수 있도록 대응 계획을 수립하여야 한다.
- ② 제1항에 따른 개인정보 유출 사고 대응 계획에는 긴급조치, 유출통지·조회 및 신고 절차, 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

또한 개인정보 보호책임자는 개인정보 유출사고 대응 계획을 각 부서에 공문으로 발송하고 전 직원이 언제든지 열람할 수 있도록 내부 행정업무

시스템의 게시판에 게시하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

- ③ 개인정보보호책임자는 개인정보 유출에 따른 피해복고 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제19조(개인정보 위험도 분석 및 대응방안) 개인정보의 위험도 분석 및 대응 관한 사항은 행정안전부·한국인터넷진흥원의 「개인정보 위험도 분석 기준」에 따른다.

제20조(위탁계약 및 위탁업무의 공개)

- ① 개인정보보호관리책임자(이하 “위탁자”라 한다)가 개인정보의 처리업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.
1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
 2. 개인정보의 관리적·기술적·물리적 조치에 관한 사항
 3. 위탁업무의 목적 및 범위
 4. 재위탁 제한에 관한 사항
 5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
 6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
 7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항
- ② 위탁자가 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지 등을 통해 지속적으로 공개하여야 한다.

제21조(수탁자에 대한 관리·감독)

- ① 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 위탁자가 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
1. 수탁자의 개인정보 처리현황 및 실태, 목적 외 이용제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하여야 한다.

② 개인정보처리 업무를 위탁하는 경우에 위탁자는 아래의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

제8장 **물리적 안전조치**

제22조(물리적 안전조치)

- ① 개인정보보호책임자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 하며 물리적 접근제한을 위한 잠금장치, 지문인식장치, CCTV 등을 설치하고 출입자 관리대장을 비치하여야 한다.
- ② 개인정보보호책임자는 개인정보취급자 또는 정보시스템의 유지관리 수행을 위한 용역업체 직원 등 상시출입자로 지정되지 않은 자가 제1항의 장소에 출입하거나 그곳에 보관하고 있는 개인정보를 열람할 경우 출입 사실 및 열람 내용을 출입자 관리대장에 기록하고 관리하여야 한다.
- ③ 개인정보보호책임자는 제2항의 출입자 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검·확인하여야 한다.
- ④ 개인정보취급자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사하여 보관할 경우 시건장치가 되어 있는 안전한 곳에 보관하여야 한다.

- ⑤ 개인정보취급자는 개인정보가 포함된 보조저장매체 사용 시 휴대용 저장매체관리시스템(<http://172.168.1.25>)에 등록된 저장매체를 이용하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제23조(재해·재난 대비 안전조치)

- ① 개인정보보호책임자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보 처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.
- ② 개인정보보호책임자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.
- ③ [별표]의 유형1 및 유형2에 해당하는 개인정보보호책임자는 제1항부터 제2항 까지 조치를 이행하지 아니할 수 있다.

제24조(개인정보파일 등록 및 변경)

개인정보취급자는 개인정보파일을 보유할 경우 보유를 시작(변경)한 날로부터 60일 이내에 개인정보파일명, 수집근거, 보유목적, 보유기간 등을 행정안전부에서 운영하는 개인정보보호종합지원시스템(<http://intra.privacy.go.kr>)에 등록(변경)하여야 하며, 개인정보보호책임자는 개인정보취급자가 등록(변경) 신청한 개인정보파일에 대하여 검토하고 승인 또는 반려처리 하여야 한다.

☞ 등록된 항목 중 하나라도 변경된 경우에도 60일 이내에 재등록하여야 함.
단, 개인정보파일이 상시적으로 변경되는 경우, 1년 1회 변경 등록 가능.

제25조(개인정보의 파기)

- ① 개인정보취급자는 보유기간 종료일 또는 개인정보처리가 불필요한 것으로 인정되는 날로부터 5일 이내에 개인정보를 파기하여야 하며, 개인 정보 파일을 파기하기 전에 개인정보파일 파기 요청서 작성하여 개인정보보호 담당자에게 제출하여야 한다.

- ② 개인정보보호담당자는 개인정보파일 파기 요청 시 파기 결과를 확인한 후, 개인정보파일 파기 관리대장을 작성하고 행정안전부에서 운영하는 개인정보 보호종합지원시스템에 등록된 개인정보파일 현황을 삭제하여야 한다.
- ③ 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
 - 1. 완전파괴(소각·파쇄 등)
 - 2. 전용 소자장비를 이용하여 삭제
 - 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
- ④ 개인정보처리자가 개인정보의 일부만을 파기하는 경우 “완전파괴, 전용 소자 장비를 이용하여 삭제, 데이터가 복원되지 않도록 초기화 또는 덮어쓰기” 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.
 - 1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
 - 2. 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

제26조(처리실태 조사)

- ① 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지에 대한 실태 조사를 할 수 있다.
- ② 개인정보보호책임자는 개인정보의 처리에 대한 실태조사를 위해 조사 대상, 일정, 절차 및 방법 등을 포함하는 실태조사 계획을 별도로 수립·시행할 수 있다.
- ③ 개인정보보호분야별책임자는 수시로 개인정보취급자 및 개인정보처리 시스템에 대해 개인정보처리실태 점검, 관리·감독을 통하여 개선 조치하고, 개인정보의 처리 실태조사에 적극 협조하여야 한다.

제27조(영상정보처리기기 설치 및 운영관리)

- ① 누구든지 공개된 장소에 영상정보처리기기를 설치·운영하는 것은 원칙적으로 금지되어야 하나 다른 법익의 보호를 위하여 필요한 경우 다음의 같이 예외적으로 설치·운영을 허용할 수 있다.
 1. 법령에서 구체적으로 허용하고 있는 경우
 2. 범죄의 예방 및 수사를 위하여 필요한 경우
 3. 시설 안전 및 화재 예방을 위하여 필요한 경우
- ② 불특정 다수가 이용하는 공개된 장소라도 현저히 사생활 침해 우려가 있는 목욕실, 화장실, 발한실, 탈의실 등의 장소는 영상정보처리기기의 설치·운영을 금지하여야 한다.
- ③ 영상정보처리기기에는 녹음 기능을 사용할 수 없고 설치 목적과 다른 목적을 위하여 임의 조작할 수 없어야 한다.
- ④ 개인정보보호책임자는 영상정보처리기기 설치·운영 시 정보주체가 쉽게 알아 볼 수 있도록 안내판을 설치하여야 한다.
 1. 설치 목적 및 장소
 2. 촬영 범위 및 시간
 3. 관리책임자의 성명 또는 직책 및 연락처
 4. 위탁받는 자의 명칭 및 연락처(영상정보처리기기의 설치·운영을 위탁한 경우)
- ⑤ 개인정보보호책임자는 법률에서 정하는 등 특별한 경우를 제외하고 개인영상 정보를 수집 목적 이외로 이용하거나 제3자에게 제공할 수 없으며, 개인영상정보 이용 및 제3자 제공 제한의 예외사항은 다음 각 호와 같다.
 1. 정보주체의 별도의 동의를 얻은 경우
 2. 다른 법률에 특별한 규정이 있는 경우
 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체

또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우

⑥ 개인정보보호책임자는 영상정보처리기기에 의하여 수집된 영상정보는 보유 기간이 만료한 후, 지체 없이 삭제하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러지 아니할 수 있다.

⑦ 개인정보보호책임자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있으며, 위탁을 하는 경우 다음 각 호와 같이 위탁업무 수행 목적 외 개인영상정보 처리금지에 관한 사항 등이 포함된 문서로 해야 하며, 위탁자인 개인정보보호분야별책임자는 수탁자가 개인영상정보를 안전하게 처리하는지 관리·감독하여야 한다.

1. 위탁업무 수행 목적 외 개인영상정보의 처리 금지에 관한 사항

2. 개인영상정보의 기술적·관리적 보호조치에 관한 사항

3. 위탁하는 사무의 목적과 범위 및 재위탁 제한에 관한 사항

4. 개인영상정보 관리현황점검 및 수탁자 소속 직원의 교육에 관한 사항

5. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

⑧ 정보주체는 해당 개인정보보호책임자에게 개인영상정보에 대하여 열람 또는 존재확인을 요구할 수 있으며, 개인정보보호책임자는 이에 대하여 지체 없이 필요한 조치를 취하여야 한다. 다만, 다음 각 호의 사항에 해당하는 경우 요구를 거부할 수 있으며, 이때에는 거부사유를 10일 이내에 서면으로 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우

2. 특정 정보주체의 영상정보만 선택하여 삭제하는 것이 기술적으로 현저히 곤란한 경우

3. 제1항에 따른 요청에 필요한 조치를 취함으로써 타인의 사생활권이 침해될 우려가 큰 경우

4. 기타 열람 등의 요청을 거절할 만한 정당한 공익적 사유가 존재하는 경우

- ⑨ 개인정보보호책임자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 취하여야 한다.
- ⑩ 개인정보보호책임자는 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보 침해가 우려되는 경우에는 자체점검 등 개인영상 정보의 침해 방지를 위해 적극 노력하여야 한다.
- ⑪ 개인정보보호책임자는 영상정보처리기기를 신규로 설치하거나 또는 변경설치 할 때는 CCTV 설치현황을 작성하여 개인정보보호책임자에게 보고하여야 한다.

제28조(영상정보처리기기 운영·관리 방침 수립 및 공개)

개인정보보호책임자는 다음 각 호의 사항을 모두 포함한 영상정보처리기기 운영·관리 방침을 수립하여 공단 대표 홈페이지를 통하여 공개하여야 한다.

- ① 영상정보처리기기의 설치 근거 및 설치 목적
- ② 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
- ③ 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
- ④ 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
- ⑤ 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
- ⑥ 정보주체의 영상정보 열람 등 요구에 대한 조치
- ⑦ 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
- ⑧ 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

제29조(개인영상정보의 보호조치)

- ① 개인정보보호분야별책임자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.
 1. 개인영상정보의 안전한 처리를 위한 보호계획의 수립·시행
 2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
 3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용(네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장 시 비밀번호 설정 등)
 4. 처리기록의 보관 및 위조·변조 방지를 위한 조치(개인영상정보의 생성

일시 및 열람할 경우에 열람 목적, 열람자, 열람 일시 등 기록관리 조치 등)

5. 개인영상정보의 물리적 보관시설 마련 또는 잠금장치 설치

② 개인영상정보보호담당자는 “표준 개인정보 보호지침”의 준수 여부에 대한 다음 각 호의 사항에 대해 자체점검을 년 1회 실시하여 다음 해 3월 31일까지 그 결과를 행정안전부장관에게 통보하고, 개인정보보호종합지원시스템에 등록하여야 하며, 공단 홈페이지에 공개하여야 한다.

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기기 설치·운영의 필요성 지속 여부

제30조(영상정보처리기기 설치 및 관리 등의 위탁 및 제3자 제공)

① 개인정보보호분야별책임자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 수탁자의 명칭을 안내판과 영상정보처리기기 운영·관리 방침에 공개하여야 한다.

② 개인정보보호분야별책임자는 위탁 문서 작성 시 다음과 같은 내용이 포함되어야 한다.

1. 위탁업무 수행 목적 외 개인영상정보의 처리 금지에 관한 사항
2. 개인영상정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁하는 사무의 목적과 범위 및 재위탁 제한에 관한 사항
4. 개인영상정보 관리현황점검 및 수탁자 소속 직원의 교육에 관한 사항
5. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

③ 개인정보보호분야별책임자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 시 수탁자가 개인영상정보를 안전하게 처리하는지 관리·감독하여야 한다.

- ④ 개인정보보호분야별책임자는 개인영상정보를 관련 근거에 의해 제3자에게 제공할 경우나 수집 목적 이외로 이용할 경우 개인정보의 목적 외 이용 및 제3자 제공대장을 작성하여 관리하여야 한다.

제31조(보관 및 파기)

- ① 개인정보보호분야별책임자는 수집한 개인영상정보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 다른 법령에 특별한 규정이 없는 한 지체 없이 파기하고 개인영상정보 관리대장을 작성하여 관리하여야 한다.
- ② 개인정보보호분야별책임자가 그 사정에 따라 보유 목적의 달성을 한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보수집 후 30일 이내로 한다.
- ③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.
1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
 2. 전자기적 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제10장 기타

제32조(법령과의 관계) 이 내부 관리계획에 명시되지 않은 사항은 다음 각 호에 따른다.

- ① 「개인정보 보호법」 및 같은 법 시행령 및 시행규칙
- ② 「표준 개인정보 보호지침」(행정안전부 고시)
- ③ 「개인정보의 안전성 확보조치 기준」(행정안전부 고시)
- ④ 「개인정보 영향평가에 관한 고시」(행정안전부 고시)

부칙

본 계획은 2020년 2월 12일부터 시행한다.

[별표]

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전조치 기준
유형1 (완화)	· 1만명 미만의 정보주체에 관한 개인정보를 보유한 정보처리시스템	· 제5조 : 제2항부터 제5항까지 · 제6조 : 제1항, 제3항, 제6항 및 제7항 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형2 (표준)	· 5만명 미만의 정보주체에 관한 개인정보를 보유한 정보처리시스템	· 제4조 : 제1항제1호부터 제11호까지 및 제 15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형3 (강화)	· 5만명 이상의 정보주체에 관한 개인정보를 보유한 정보처리시스템	· 제4조부터 제13조까지