개인정보보호 내부관리계획

2017. 5.

KCA 한국방송통신전파진흥원

[목 차]

개인정보보호 내부관리계획

제정 2011. 12. 07.

개정 2017. 5. 10.(개정이력 별첨)

제 1 장 총 칙

제1조(목적) 개인정보보호 내부관리계획(이하 ‘내부관리계획’이라 한다)은 「개인정보보호법」 제29조, 동법 시행령 제30조1항1호의 내부관리계획의 수립 및 시행 의무에 따라 한국방송통신전파진흥원(이하 ‘진흥원’이라 한다)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조 (정의) 본 계획에서 사용하는 용어의 정의는 다음과 같다.

1. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
2. “접속기록”이라 함은 개인정보 취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 ID 등의 식별자, 접속일시, 접속자 IP(Inrernet Protocol)주소 등의 접속지정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
3. “보조저장매체”란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disc), DVD(Digital Versatile Disc), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 업무용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.

4. “접근권한” 이란 개인정보처리시스템에 접속하여 정보자원을 활용할 수 있는 권한과 정보를 생성·변경·열람·삭제 등 이용할 수 있는 권한을 말한다.

5. “개인정보 보호책임자” 란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 개인정보보호법 제31조(개인정보 보호책임자 지정)에 따른 지위에 해당하는 자를 말한다.

6. “개인정보 보호담당자” 란 개인정보 보호책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보 보호책임자가 일정 요건의 자격을 갖춘 이를 지정한다.

7. “개인정보처리자” 란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

8. “개인정보취급자” 란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.

9. “정보주체” 란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

10. “개인정보파일” 이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

11. “정보통신망” 이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

12. “내부망” 이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

13. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용기기를 말한다.

14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

15. 내부관리계획에서 정의하지 않은 사항은 「개인정보보호법」 및 관련 법령의 정의에 따른다.

제3조(적용 범위) 본 내부관리계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 오프라인(서면, 전화, 팩스 등)을 통해 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부직원(계약직 등 비정규직 포함) 및 외부업체 직원에 대해 적용한다.

제 2 장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 시행)

① 개인정보 보호책임자는 진흥원의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

③ 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.

④ 개인정보 보호담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 11월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.

⑤ 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제5조(내부관리계획의 공표)

① 개인정보 보호책임자는 제4조에 따라 승인된 내부관리계획을 매년 1월말까지 또는 개정 승인 후 진흥원의 전 임직원에게 공표한다.

② 개인정보 보호책임자는 내부관리계획을 임직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제 3 장 개인정보 보호책임자

제6조(개인정보 보호책임자의 지정) 개인정보 보호책임자는 개인정보보호법 시행령 제32조 제2항 1호에 따라 해당하는 지위에 있는 자를 개인정보 보호책임자로 임명한다.

1. 개인정보 보호책임자 : 경영기획본부장
2. 분야별 개인정보 보호책임자 : 본부별 개인정보처리부서의 장

제7조(개인정보 보호책임자의 역할 및 책임)

① 개인정보 보호책임자의 업무는 다음 각 호와 같다.

1. 개인정보보호 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 보호교육 계획의 수립 및 시행

6. 개인정보파일의 보호 및 관리·감독

7. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행

8. 개인정보보호 관련 자료의 관리

9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 진흥원 전체의 개인정보 처리에 관한 업무를 총괄하여 책임진다.

③ 분야별 개인정보 보호책임자는 제1항 업무의 효율적 수행을 위하여 필요 시 관련 진흥원에서 개인정보 보호담당자 및 취급자를 지정하고 수행할 수 있다.

제8조(개인정보 보호담당자 및 개인정보취급자의 범위, 역할 및 책임)

① 개인정보 보호담당자는 진흥원 내에서 고객의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 관리한다.

② 개인정보 보호담당자 및 개인정보 취급자는 각 해당 시스템별 개인정보에 대한 접근권한을 가지며 진흥원 업무상에서 개인정보와 관련한 업무를 수행하는 자로 정규직이외에 계약직, 임시직, 파견근로자, 시간제근로자 등 직원도 포함한다.

③ 개인정보 취급자는 개인정보보호와 관련하여 다음 각 호와 같은 역할과 책임을 이행한다.

1. 내부관리계획의 준수 및 이행

2. 개인정보의 기술적·관리적 보호조치 기준 이행

3. 개인정보 침해행위에 대한 점검 등

4. 기타 개인정보보호를 위해 필요한 사항의 이행

5. 개인정보 접근 권한의 무단 양도 및 대여 금지 [별지 6] 기록

6. 담당자 또는 취급자는 개인정보처리시스템의 현황을 [별지 1] 개인정보파일대장에 기록 및 현행화
7. 「개인정보보호법」 제59조에 따라 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위, 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위, 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위 등 금지행위와 동법 제60조에 따라 직무상 알게 된 비밀의 누설 및 직무상 목적 외 용도로의 이용 금지

제 4 장 개인정보의 처리 단계별 기술적·관리적 보호조치

제9조(접근 권한의 관리)

① 개인정보 보호책임자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 진흥원은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 해당 개인정보취급자의 개인정보처리시스템 접근권한을 변경 또는 말소하여야 한다.

③ 진흥원은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 [별지 2] 개인정보 접근권한 관리대장에 변경사항을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 진흥원은 개인정보시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보 취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제10조(접근통제)

① 진흥원은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한한다.
2. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선, 또는 SSL과 2채널 인증 등 안전한 접속 수단을 적용한다.

③ 진흥원은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터 및 모바일 기기에 조치를 취한다.

④ 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)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑤ 개인정보 처리자는 개인정보 처리에 이용되는 모바일 기기의 분실·도난 등으로 개인정보가 유출·변조·훼손 되지 않도록 해당 모바일 기기에 비밀번호 설정, 분실 시 단말기 잠금 기능 등의 조치를 하여야 한다.

제11조(개인정보의 암호화)

① 진흥원은 고유 식별 정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 진흥원은 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화가 되지 않도록 일방향 암호화하여 저장하여야 한다.

③ 진흥원은 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

④ 진흥원은 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 진흥원은 업무용 컴퓨터 또는 모바일 기기에 고유 식별 정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

제12조(접속기록의 보관 및 점검)

① 진흥원은 개인정보 취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우에는 개인정보파일, ID 등의 식별자, 접속일시, 접속자 IP 등의 접속지 정보, 입력·출력·변경 등의 수행업무에 대한 접속기록을 남기고 최소한 6개월 동안 보관·관리하여야 한다.

② 진흥원은 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 [별지4] 개인정보처리시스템의 로그저장관리대장 양식 또는 그에 준하는 전자적 방식에 따라 개인정보처리시스템의 로그를 안전하게 보관하여야 한다.

③ 진흥원은 [별지 3] 개인정보 처리시스템의 접근기록대장 또는 그에 준하는 전자적 방식에 따라 개인정보처리시스템의 로그를 관리한다.

제13조(악성프로그램 등 방지)

진흥원은 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안

프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시
2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트 실시

제14조(물리적 접근 방지)

① 진흥원은 데이터센터, 보안실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

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

제15조(개인정보의 파기)

① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 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

③ 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제2항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구

및 재생되지 않도록 관리 및감독

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

④ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

제16조(출력 복사 시 보호조치)

① 개인정보 취급자는 소관 업무분야 내에서 개인정보가 기록된 출력자료와 기록매체가 유출되지 않도록 시건 장치가 된 캐비닛 등에 안전하게 보관하여야 하며, 활용이 종료된 출력자료 등은 즉시 파기하여야 한다.

② 개인정보 취급자는 개인정보를 인쇄하거나 보안 USB 메모리 등 이동 가능한 저장매체에 복사할 경우 개인정보가 기록된 입출력 자료를 [별지5] 개인정보 입출력 자료 관리대장에 기록하여야 한다. 출력, 복사물로부터 다시 복사하는 경우에도 그러하다.

③ 개인정보 취급자는 출력 자료의 파기날자를 기록, 관리하여야 하고 개인정보 보호책임자는 파기 여부를 확인하여야한다.

제17조(비밀번호 관리)

① 개인정보처리자는 개인정보취급자나 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템 등에 적용하여 운영 하여야 한다. 다만, 정보주체의 비밀번호는 정보주체의 편의성 등을 고려하여 개인정보처리자가 자율적으로 적절한 수준을 설정하는 것이 필요하다.

② 비밀번호는 산업스파이, 침입자, 비인가자가 추측하기 어려운 문자와 숫자를 포함하도록 하거나, 전에 사용된 비밀번

호를 다시 사용하지 않는 등의 다음과 같은 비밀번호 설정 원칙을 참고하여 생성하도록 한다.

- 비밀번호의 최소 길이 : 비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 하며, 이는 정보주체에 대한 비밀번호 작성규칙과는 달리 반드시 준수하여야 한다
  - · 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자 (32개)중 2종류 이상으로 구성한 경우
  - · 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자 (32개) 중 3종류 이상으로 구성한 경우
- 추측하기 어려운 비밀번호의 생성
  - · 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.
  - · love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.
- 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 6개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않는다.
- 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.

제18조(개인정보파일의 보유기간)

① 진흥원은 대상 개인정보파일에 대해 법령에 근거한 기한을 정하여 보유하고, 기한이 경과한 파일은 복구가 불가능하도록 완전삭제 조치를 하여야 한다.

② 고객센터 등 민원처리 개인정보 처리시 본인이 삭제를 요청했을시에는 즉시 삭제해야 한다.

제 5 장 개인정보 보호조직에 관한 구성 및 운영

제19조(구성) 개인정보보호 관리 전담조직은 현행 경영기획본부로 하고 개인정보보호 담당관, 개인정보보호 기관담당자 및 전담인력이 소속한 부서를 둔다. 개인정보보호 담당관과 개인정보보호 기관담당자의 역할은 다음과 같다.

① 개인정보보호 담당관의 역할 : 서비스 제공자 등의 소속 직원 또는 제3자에 의한 위법 부당한 개인정보 침해행위 점검 이용자로부터 제기되는 개인정보에 관한 불만이나 의견의 처리 및 감독 기타 이용자의 개인정보보호에 필요한 사항을 감독 개인정보 취급자에 관한 교육 총괄 및 업무처리지침 준수 여부 감독 개인정보의 기술적, 관리적 보호조치 기준 이행 임직원, 개인정보취급자 및 용역업체 직원 등에 대한 교육 등 인식 제고 이행

② 개인정보보호 기관담당자의 역할 : 이용자로부터 제기되는 개인정보에 관한 불만이나 의견의 처리 및 기타 이용자 개인정보보호에 필요한 사항, 수탁자의 합의사항을 성실하게 이행하는지 여부에 대하여 적절한 감독 수행 운영상의 시정을 요하는 사항이나 개인정보취급 직원이 이 지침을 위반한 사실을 발견 할 때에는 이를 개인정보보호 담당관에게 보고하고 필요한 조치를 취함 개인정보의 기술적 관리적 보호조치 기준 이행 임직원, 개인정보취급자, 수탁자, 대리점 등에 대한 교육 등 인식 제고 이행 개인정보 관리 책임자 및 관리자가 승인한 개인정보 처리에 관한 전반적인 사항의 실무처리

제 6 장 개인정보 유출사고 대응계획 수립·시행

제20조(침해・유출사고 분류) 개인정보의 침해 유출사고는 다음과 같이 분류된다.

① 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우

② 개인정보가 저장된 DB 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

③ 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이 문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

④ 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

제21조(대응방안) 개인정보 침해・유출사고 발생시 다음과 같이 대응팀을 구성하고 대처활동을 위한 조직을 운영한다.

① 개인정보 침해・유출사고 상황의 전반적인 개인정보보호 통제 수행을 위한 침해・유출사고 대응팀 구성

- 체계화된 개인정보보호 정책 수립 등의 문서화 및 조직/인력에 대한 운영과 관리

② 개인정보 침해・유출사고 대처 활동을 위한 조직 운영

- 개인정보보호 통제사항을 관리하기 위하여 담당부서는 개인정보 보호업무를 전담 운영・관리

제22조(대응절차) 개인정보 침해・유출사고 발생시 다음과 같은 절차에 따라 처리한다.

① **개인정보 침해・유출사고 신고**

가. 1만명 이상의 고객에 관한 개인정보가 침해・유출된 경우에는 고객에 대한 통지 및 조치 결과를 5일 이내에 진흥

원장에게 보고

나. 고객에 관한 개인정보가 1만명 이상의 침해·유출된 경우에는 고객에 대한 통지 및 조치결과를 5일 이내에 진흥원장과 미래창조과학부장관을 경유하여 행정자치부장관 또는 한국인터넷진흥원 중 어느 하나에 신고

다. 개인정보 침해·유출사고 보고 또는 신고는 [별지 16] 서식의 '개인정보 침해·유출 신고서'를 활용

라. 전자우편, 팩스 또는 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 신고한 후, [별지 16] 서식의 '개인정보 침해·유출 신고서'를 제출 가능

마. 1만명 이상의 고객에 관한 개인정보가 유출된 경우에는 통지와 함께 진흥원 홈페이지에 고객이 알아보기 쉽도록 7일 이상 게재할 수 있도록 개인정보 보호책임자에게 요청

바. 개인정보 침해·유출사고 신고는 [별지 17] 서식의 '개인정보 침해·유출 신고 관리대장'에 기록·관리

② 개인정보 침해·유출사고 보고

가. 개인정보 침해·유출사고가 발생한 것으로 확인된 때에는 개인정보 보호담당자는 지체없이 개인정보 보호책임자에게 침해·유출 사고에 대한 보고

나. 사고 보고는 [별지 18] 서식 '개인정보 침해·유출사고 보고서' 활용

③ 개인정보 침해·유출사고 통지

가. 실제로 침해·유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 5일 이내에 해당 고객에게 아래사항 공지

- 침해·유출된 개인정보의 항목
- 침해·유출된 시점과 그 경위
- 침해·유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 고객이 할 수 있는 방법 등에 관한 정보
- 진흥원의 대응조치 및 피해 구제 절차
- 고객에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- [별지 12] '개인정보 침해·유출 통지 절차'
- [별지 13] '개인정보 침해·유출 통지문(안)'
- [별지 14] '개인정보의 침해·유출 통지내용(예시)'

나. 침해·유출된 시점과 그 경위의 경우, 개인정보 침해·유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증 필요

다. 침해·유출 사고의 조치를 취한 이후에는 고객에게 다음 아래의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있음
- 고객에게 유출이 발생한 사실
- 통지항목 중 확인된 사항

라. 고객에게 통지할 때에는 서면, 전자우편, 팩스, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일 이내에 고객에게 알려야 함과 동시에, 홈페이지 등을 통하여 공개 가능
- [별지 15] '고객의 대응방안 안내(예시)'

④ 개인정보 침해·유출사고 처리 및 종결

가. 진흥원에서는 개인정보 침해·유출사고 종결처리는 문서로 기록·관리
- [별지 17] 서식의 '개인정보 침해·유출 사고 관리대장'
- [별지 19] 서식의 '개인정보 침해·유출 사고 처리 보고서'

나. 개인정보 침해·유출사고에 대한 종결 처리되었음을 각 관련 기관에 통지

- 미래창조과학부
- 행정자치부장관 또는 한국정보화진흥원 또는 한국인터넷진흥원 중 어느 하나에 통지 (1만명 이상의 고객에 관한 개인정보가 유출된 경우)

제23조(권익침해 구제방법) 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다. 이 밖에 기타 개인정보침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

1. 개인정보분쟁조정위원회 : (국번없이)118
2. 대검찰청 사이버범죄수사단 : 02-3480-3571
3. 경찰청 사이버테러대응센터 : 02-1566-0112
4. 한국인터넷진흥원 개인정보침해신고센터 : privacy.kisa.or.kr

제 7 장 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치

제24조(재해 및 재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

제 8 장 개인정보처리 자체감사 및 관리

제25조(개인정보보호의 날 지정 및 운영)

① 개인정보 보호책임자는 매월 하루(매월 세 번째주 수요일)를 “개인정보 보호의 날”로 지정하여 내부관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 점검하고 관련 정책을 홍보하여 개인정보보호의 중요성을 인지시킨다.

② 웹사이트 및 내부 업무관리시스템 초기화면에 플래시나 관련 지침을 게재하는 등의 방법을 이용한다.

③ 해당 일이 휴일인 경우 전일 또는 다음 날 평일에 시행한다.

제26조(개인정보처리 자체감사 결과의 반영)

① 개인정보 보호책임자는 개인정보 보호를 위한 개인정보처리 자체감사 결과 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 내부관리계획의 내용을 위반할 때에는 시정·개선 등 필요한 조치를 취하여야 한다.

② 개인정보 보호책임자는 차년도 개인정보보호 계획수립 전에 개인정보처리 자체감사 결과를 검토하고 차년도 개인정보보호 계획 수립 시 반영한다.

제 9 장 개인정보보호 교육

제27조(개인정보 보호교육 계획의 수립)

① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보 보호교육 계획을 매년 12월말까지 또는 교육이 필요하다고 인정하는 경우 수립한다.

② 개인정보 보호책임자는 수립한 개인정보보호 교육 계획을

실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육 계획 수립에 반영하여야 한다.

제28조(개인정보보호 교육 계획의 실시)

① 개인정보 보호책임자는 개인정보 보호에 대한 직원들의 인식제고를 위해 노력해야 한다.

② 개인정보 보호책임자는 관련 시책에 따라 개인정보 보호 교육을 실시한다.

③ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.

④ 개인정보 보호에 대한 중요한 전파 사례가 있거나 개인정보 보호 업무와 관련하여 변경된 사항이 있는 경우, 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

제 10 장 수탁자에 대한 관리 및 감독

제29조(업무 위탁에 따른 개인정보 보호 세칙 수립)

① 진흥원의 업무를 위탁받아 수행하는 수탁자 중 개인정보 취급 또는 관리업무를 수행하는 기관, 단체 또는 개인에 대하여 법 제26조(업무위탁에 따른 개인정보의 처리 제한)애 따라 별도의 세칙을 제정하여 적용하여야 한다.

② 세칙에는 아래와 같은 사항을 마련하여야 한다.

1. 업무 위탁 계약 체결 : 수탁자명, 수탁업무내용 등
2. 개인정보 기술적·관리적 보호조치 : 접근권한, 기록, 파기 등
3. 관리감독 및 교육 : 처리현황, 수탁자 정기 교육 등
4. 자료 이관 및 손해 배상 : 사업종료 후, 위반사항 등

③ 개인정보처리위탁계약서는 [별지 10] 양식을 활용하여 작성한다.

[별지 1] 개인정보파일대장

개인정보파일대장

①번 호		
②기 관 명		
③등록부서		
④취급자담당자		
⑤업무분야		
⑥개인정보파일의 명칭		
⑦개인정보파일의 운영 근거		
⑧개인정보파일의 운영 목적		
⑨개인정보파일에 기록되는 개인정보의 항목	정보주체(개인정보를 수집하는 본인 등)	□이름 □집주소 □E-MAIL □집연락처 □직정연락처 □핸드폰 □생년월일 고유식별번호(□주민번호 □운전면허번호 □여권번호 □외국인등록번호), 민감정보(□사상·신념 □노동조합·정당의 가입·탈퇴 □정치적 견해 □건강 □성생활 □유전정보 □범죄경력자료) □기타( )
	법정대리인(14세 미만 보호자 등)	□이름 □집주소 □E-MAIL □집연락처 □직정연락처 □핸드폰 □생년월일 고유식별번호(□주민번호 □운전면허번호 □여권번호 □외국인등록번호), 민감정보(□사상·신념 □노동조합·정당의 가입·탈퇴 □정치적 견해 □건강 □성생활 □유전정보 □범죄경력자료) □기타( )
⑩개인정보의 처리방법		□오프라인 수집(개인이 신청서 등을 통한 서면 수집) □온라인 수집(홈페이지 회원신청, 전자접수 등) □시스템 연계를 통한 수집 □기타( )
⑪개인정보의 보유기간		○1년 ○3년 ○5년 ○10년 ○30변 ○준영구 ○영구 ○별도 규종이 있어 해당 규정에서 지정한 기간 [년, 월] ○기타( )
⑫개인정보를 통상적·반복적 제공하는 경우	제공 받는자	
	근거	
	개인정보의 범위	
⑬개인정보파일로 보유중인 개인 정보주체 수		( )건
⑭타 정보시스템과의 연계 여부		○예(정보주체수 ※[ ]건) ※등록하려는 개인정보파일(A)을 탑재한 정보시스템(B)이 다른 개인정보파일(C)를 탑재한 정보시스템(D)과 연계되어 개인정보파일 관련 업무를 처리하는 경우 A와 C에 포함된 개인정보 주체(중복제외) ○아니오
⑮개인정보처리 업무 담당부서	범위	○해당 업무부서의 담당자만 접근하여 활용할 수 있다. ○해당 업무부서의 담당자와 시스템 관리자만이 접근하여 활용할 수 있다. ○해당 업무부서 구성원이 모두 접근하여 활용할 수 있다. ○해당 업무부서와 시스템관리자가 접근하여 활용 가능하다. ○전 부서에서 접근하여 활용 가능하다. ○일부 관련부서에서 공동으로 활용하고 있다. ○기타( )
	공동사용부서	
⑯개인정보의 열람 요구를 접수, 처리하는 부서		
⑰개인정보파일에서 열람제한·거절하는 개인정보의 범위 및 그 사유	개인정보의 범위	
	사유	

개인정보파일대장 작성 요령

① **번호** - 생략

② **기관명** **(필수)** - 한국방송통신전파진흥원

③ **등록부서** **(필수)** - 담당자의 **소속 부서**

④ **취급담당자** **(필수)** - 해당 파일에 대한 담당자

⑤ **업무분야** **(필수)** - 등록하려는 개인정보파일의 업무기재 (홈페이지, 등록관리, 세입 등)

⑥ **개인정보파일의 명칭** **(필수)** - 해당 파일에 대한 시스템 화일명

⑦ **개인정보파일의 운영 근거** **(필수)** - 개인정보파일의 보유근거(관련 법령 및 규정)를 입력
* ⑪번 '개인정보의 보유기간'에 대한 근거도 포함하여 입력

⑧ **개인정보파일의 운영 목적** **(필수)** - 개인정보파일의 보유 목적

⑨ **개인정보파일에 기록되는 개인정보의 항목** **(필수)**
- 개인정보파일에서 수집하는 개인정보 항목을 **모두 ☑ 선택**
* 해당 항목이 없으면 **'기타'란 ☑ 후 항목 입력**

⑩ **개인정보의 처리방법** **(필수)** - 개인정보를 수집하는 방법을 선택
* 개인정보 처리방법 중복 ☑가 가능

⑪ **개인정보의 보유기간** **(필수)** - 해당 개인정보파일의 보유기간을 선택
* 별도 규정 및 기타를 선택하시면 년/월/일 중 선택 후 기재

⑫ **개인정보를 통상적 또는 반복적으로 제공하는 경우**
- 제공받는자 : 개인정보파일을 이용·제공 받는 기관명 입력 (필수)
- 기관명 입력 후 근거와 개인정보의 범위를 입력

⑬ **개인정보파일로 보유하고 있는 개인정보의 정보주체 수** **(필수)**
- 개인정보파일에 저장되어있는 인원수(레코드수)의 정확한 수치를 숫자로 기재

⑭ **타 정보시스템과의 연계 여부** - 등록하려는 개인정보파일(A)을 탑재한 정보시스템(B)이 다른 개인정보파일(C)를 탑재한 정보시스템(D)과 연계되어 개인정보파일 관련 업무를 처리하는 경우 A와 C에 포함된 개인정보 주체(중복제외)

⑮ **해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서의 범위**
- 개인정보파일에 접근하는 범위 선택 (필수)
- 해당 파일을 공동으로 사용하는 부서를 입력

⑯ **개인정보의 열람 요구를 접수, 처리하는 부서** **(필수)**
- 개인정보파일을 열람할 수 있는 기관 주소 및 부서 입력

⑰ **개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유**
- 개인정보파일에 열람제한이 있는 항목 입력 (필수)
* 제한 항목이 있을 경우, 그에 대한 사유를 입력

[별지 2] 개인정보 접근권한 관리대장

개인정보 접근권한 관리대장

번호	소속(부서)	사용자명	사용자IP	개인정보 관련 업무현황	개인정보 접근권한 내용	변경사항	변경사유	비고

[별지 3] 개인정보 처리시스템의 접근기록대장

개인정보 처리시스템의 접근기록대장

시스템 : [ ] 의 접근 기록							
번호	자료의 종류	주요항목	사용목적	접근발생일시	접근중지일시	처리담당자	처리부서장

[별지 4] 개인정보 처리시스템의 로그관리 저장 대장

개인정보 처리시스템의 로그저장관리 대장

(　　)월

시스템 담당자	시스템 관리자

작성일:　　년　　월　　일

(　　)월 로그관리 일정에 따라 아래의 시스템에 대한 백업을 실시하였음

시스템명	백업종류	보관장소	담당자	비고
참고 사항				

[별지 5] 개인정보 입출력 자료 관리대장

개인정보 입출력 자료 관리대장

번호	개인정보 파일명	자료의 종류	주요 기록항목	사용 목적	자 료 발생일	폐기일	처리담당자 성 명	처 리 부서장

[별지 6] 개인정보 목적 외 이용 및 제3자 제공 대장

■ 개인정보 보호법 시행규칙 [별지 제1호서식]

개인정보 목적 외 이용 및 제3자 제공 대장

<table>
<tr><td>개인정보 또는
개인정보파일 명칭</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공 구분</td><td colspan="3">[ ] 목적외 이용 [ ] 제3자 제공</td></tr>
<tr><td>목적 외 이용기관의 명칭
(목적 외 이용의 경우)</td><td></td><td rowspan="3">담당자</td><td>소 속 :
성 명 :
전화번호 :</td></tr>
<tr><td>제공받는 기관의 명칭
(제3자 제공의 경우)</td><td></td><td rowspan="3">담당자</td><td>성 명 :
소 속 :
전화번호 :</td></tr>
<tr><td>이용하거나 제공한 날짜,
주기 또는 기간</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한 형태</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공의 법적 근거</td><td colspan="3"></td></tr>
<tr><td>이용 목적 또는
제공받는 목적</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한
개인정보의 항목</td><td colspan="3"></td></tr>
<tr><td>「개인정보 보호법」
제18조제5항에 따라 제한을
하거나 필요한 조치를
마련할 것을 요청한
경우에는 그 내용</td><td colspan="3"></td></tr>
</table>

목적 외 이용 및 제3자 제공의 기록 관리

「개인정보보호법」 제18조(개인정보의 이용 · 제공 제한)와 시행령 제15조(개인정보의 목적외 이용 또는 제3자 제공의 관리)에 따라 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우를 기록하여야 하며, 다음의 경우에만 목적 외의 용도로 이용 · 제공이 가능하다.

1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
3. 통계작성, 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우
4. 민원만족도 조사용역을 위하여 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우

[별지 7] 개인정보 파일 파기 관리대장

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[별지 8] 개인정보(정정·삭제, 처리정지) 요구에 대한 결과 통지서

■ 개인정보 보호법 시행규칙 [별지 제10호서식]

개인정보 ([ ] 정정·삭제, [ ] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정·삭제 □ 처리정지 조치 내용	
□ 정정·삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

[별지 9] 위임장

■ 개인정보 보호법 시행규칙 [별지 제11호서식]

위 임 장

위임받는 자	성명	전 화 번 호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (□ 열람, □ 정정·삭제, □ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

ㅇㅇㅇㅇ 귀하

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

[별지 10] 표준 개인정보처리위탁 계약서(양식)

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

OOO(이하 "갑"이라 한다)과 △△△(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」 시행령 및 시행규칙,「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호) 및「표준 개인정보 보호지침」(행정안전부 고시 제2011-45호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "을"이 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 그 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은「개인정보 보호법」 제24조제3항 및 제29조, 동법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

---

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」 시행령 제16조 및 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호)에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.

③ 제2항에 따라 “을”이 개인정보를 파기한 경우 지체없이 “갑”에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① “갑”은 “을”에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “갑”은 “을”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이행하여야 한다.

③ “갑”은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 “을”을 교육할 수 있으며, “을”은 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “갑”은 “을”과 협의하여 시행한다.

제8조 (손해배상) ① “을” 또는 “을”의 임직원 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “을” 또는 “을”의 임직원 기타 “을”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “갑” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “을”은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “갑”이 전부 또는 일부를 배상한 때에는 “갑”은 이를 “을”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “갑”과 “을”이 서명 또는 날인한 후 각 1부씩 보관한다.

갑	을
○○시 ○○구 ○○동 ○○번지	○○시 ○○구 ○○동 ○○번지
성 명 : (인)	성 명 : (인)

2) 「개인정보 안전성 확보조치 기준 고시」(행정자치부 고시 제2014-7호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

[별지 11] 개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

※ 상기 내용은 인사혁신처 개인정보보호지침 제35호, 2015.12.31.을 적용함

[별지 12]

개인정보 침해·유출 통지 절차

구분	세 부 내 용	법적근거
침해·유출통지방법	진흥원은 개인정보 유출이 발생했을 경우 지체 없이 정보주체에게 개인정보 유출 관련 사항을 통지	법 제34조 시행령 제40조 보호지침 제26조
통지방법	1. 서면, 전자우편, 팩스, 전화, 휴대전화 문자전송 또는 이와 유사한 방법 2. 1번의 통지방법과 동시에 홈페이지 등을 통하여도 공개 - 단, 통지 및 조치 후에도 1만명 이상의 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알기 쉽도록 7일 이상 통지내용을 게재 - 인터넷 홈페이지를 운영하지 않는 부서의 경우 사업장 등의 보기 쉬운 장소에 통지내용을 게시	시행령 제40조 보호지침 제28조, 제29조
통지내용	① 유출된 개인정보의 항목 ② 유출된 시점과 그 경위 ③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 ④ 진흥원의 대응조치 및 피해구제절차 ⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	법 제34조 제1항 보호지침 제27조 제1항
통지시기	5일 이내(유출사고 최초발생 시점과 확인된 시점 사이에 시간적 차이가 있는 경우 이에 대한 과실유무를 입증해야 함)	보호지침 제27조
통지연기	1. 개인정보 유출확산방지를 위해 조치가 필요한 경우 유출통지를 연기 ① 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제•변경 또는 폐쇄 조치 ② 네트워크, 방화벽 등 대•내외 시스템 보안점검 및 취약점 보완 조치 ③ 향후 수사에 필요한 외부의 접속기록 등 증거 보존 조치 ④ 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치 ⑤ 기타 개인정보의 유출확산 방지를 위해 필요한 기술적•관리적 조치 2. 진흥원은 1번 각 항목의 조치를 취한 이후, 정보주체에게 다음 각 항목의 사실만 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있음 ① 정보주체에게 유출이 발생한 사실 ② 통지내용 중 확인된 사항	시행령 제40조

구분	세 부 내 용	법적근거
침해·유출통지 신고방법		
신고대상	1만명 이상의 정보주체에 관한 개인정보가 유출된 경우	법 제34조 제3항 보호지침 제29조
신고기관	http://www.privacy.go.kr	시행령 제39조 제2항 보호지침 제29조
신고시기	5일 이내(정보주체에 대한 통지 및 조치결과 신고)	
신고방법	① 전자우편, 팩스, 인터넷 사이트를 통해 유출사고 신고 및 신고서 제출 ② 시간적 여유가 없거나 특별한 사정이 있는 경우 : 전화를 통하여 통지내용을 신고한 후, 유출신고서를 제출할 수 있음	
신고내용	기관명, 통지여부, 유출된 개인정보 항목 • 규모, 유출 시점 • 경위, 유출피해 최소화 대책 • 조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서 • 담당자 연락처 등	
신고접수 기록	행정자치부장관 또는 한국정보화진흥원장 또는 한국인터넷진흥원장은 신고접수사실 확인(신고자 전자우편, 팩스)	

기술지원		
지원요청	피해 확산방지, 피해복구 등을 위한 기술지원 - 행정자치부 또는 한국인터넷진흥원과 공동으로 조사 • 지원팀 구성	법 제34조 제3항
결과보고	유출신고 처리결과 보고서를 유출신고 업무종결한 날로부터 10일 이내 행정자치부장관에게 제출	

벌칙		
벌칙조항	개인정보 유출신고(5일이내) 위반시 과태료 3천만원이하	제75조 제2항 제9호

[별지 13]

개인정보 침해·유출 표준 통지문(안)

※ 부가설명 란에 **필수사항은 < >, 참고사항은 ( )**로 표기

※ 필수사항이 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지

※ 아래 (안)을 참고하여 유출 상황에 적합하게 내용을 변경하여 활용

표준 통지문(안) 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	<제목> - '유출 통지' 문구 포함
귀하의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 귀하의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.	(사과문) - 유출 통지 사실 알림 - 사과문을 먼저 표현
귀하의 개인정보는 ○○○○년 ○○월 ○○일 ○○○시스템 장애 처리를 위한 데이터 분석 과정에서 유지관리업체로 전달되었고, 유지관리업체는 자체 서버에 저장·보관하다가 안전한 조치를 다하지 못해 ○○○○년 ○○월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 ○○○○○에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	<유출된 시점과 경위> - 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 - '귀하', '고객님' 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원정보의 일부 - 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 등 총 6개입니다.	<유출된 항목> - 유출된 항목을 누락 없이 모두 나열 ※ '등'으로 생략하거나, '회사 전화번호' 및 '집 전화번호'를 합쳐서 '전화번호'로 표시 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	<대응조치> - 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근 통제, 시스템 모니터링 강화 등 조치한 내용 설명
○○○○○이 발표한 수사 결과에 따르면 현재 해커는 검거되었고, 해커가 불법 수집한 개인정보는 2차 유출하거나 판매하지는 않은 것으로 확인되었습니다.	<피해 최소화를 위한 정보주체의 조치방법> - 유출 경위에 따라 정보주체가 할 수 있는 방

표준 통지문(안) 예시	부가 설명
따라서 현재로서는 이번 사고로 인한 2차 피해가 발생할 가능성이 높지 않아 보이나, 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. 그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고, 신속하게 대응하도록 하겠습니다.	법을 안내 - 사건에 따라 다양한 피해를 추정하여 예방 가능한 방법을 모두 안내 (보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등)
아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다. 한국인터넷진흥원의 개인정보 분쟁 조정이나 민사 상 손해배상 청구, 감독기관인 행정자치부 개인정보침해신고센터 등을 통해 피해를 구제받고자 하실 경우에도 연락주시면 그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.	<피해 구제절차> - 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재 - 보상이나 배상이 결정되지 않은 경우 계획과 절차를 안내 - 감독기관 등을 통한 구제절차도 안내
앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.	(향후 대응계획) - 추가적인 향후 대응계획을 포함
항상 믿고 사랑해 주시는 귀하께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.	(사과문)
▶ 피해 등 접수 담당부서 : OOO팀 ▶ 피해 등 접수 전화번호 : 061-338-OOOO ▶ 피해 등 접수 e-메일주소 : privacyOO@tp.or.kr	<피해 등 신고 접수 담당 부서 및 연락처> - 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내
<기관명> 직원 일동	(발신명의)

[별지 14]

개인정보 침해·유출 통지내용(예시)

고객 여러분의 개인정보가 유출되어
심려를 끼치게 된 점 진심으로 사과드립니다.

고객 여러분께 알려드립니다.
저희 진흥원에서는 내부 모니터링을 통해 **고객의 일부 정보가 00월 00일 해킹에 의해 유출된 사실을 11월 11일 확인**하였으며 고객 여러분의 피해예방 및 조속한 범인검거를 위하여 **수사기관 및 관계기관에 즉시 조사를 의뢰**하였음을 알려드립니다.

현재까지 파악된 바는 유출된 개인정보는 **암호화된 비밀번호, 암호화된 주민등록번호** 등이며, **비밀번호, 주민등록번호는 최고 수준의 기술로 암호화되어 있어 안전합니다.**

이는 중국발 IP로부터의 악성코드를 통해 해킹된 것으로 추정하고 있으며 자세한 상황은 수사기관 및 관계기관의 사실 확인을 바탕으로 추가 공지해 드리겠습니다.
고객 여러분의 서비스 사용에는 아무런 문제가 없습니다만, 보이스 피싱 및 스팸 메일 예방을 위하여 고객 여러분의 세심한 주의를 부탁드립니다.

고객의 피해예방을 위한 안내 및 당 진흥원의 조치

1. 보이스 피싱 주의 : 공공기관 및 기타 기관의 직원을 사칭하여 전화 등으로 금융정보를 묻는 경우에는 전화를 일단 끊고 반드시 해당 기관에 확인해 주시기 바랍니다.
2. 스팸 메일 주의 : 광고, 홍보성 메일이 증가할 수 있으니 각 메일에서 제공하고 있는 스팸 설정, 수신거부 기능 등을 참고하여 차단해 주시면 스팸 수신을 줄일 수 있습니다.
   당 진흥원에서는 중국 등 위험 지역 특정 IP로부터의 대량 메일 발송에 대하여서는 자동 차단 기능 등 스팸에 대한 필터를 강화할 것입니다.
3. 비밀번호 변경 : 비밀번호는 암호화되어 있어 안전합니다만 생년월일, 휴대폰번호, 단순한 숫자의 나열 등 예측하기 쉬운 방식으로 설정하신 비밀번호는 만일의 경우를 대비해서 변경해 주시기 바랍니다.

아이디/비밀번호 찾기

우리 진흥원에서는 비밀번호 변경 캠페인을 정기적으로 진행하고 있으며 무작위 조합을 통한 비정상 로그인 시도를 차단하기 위하여 틀린 비밀번호 입력 시 인증을 강화하였습니다.

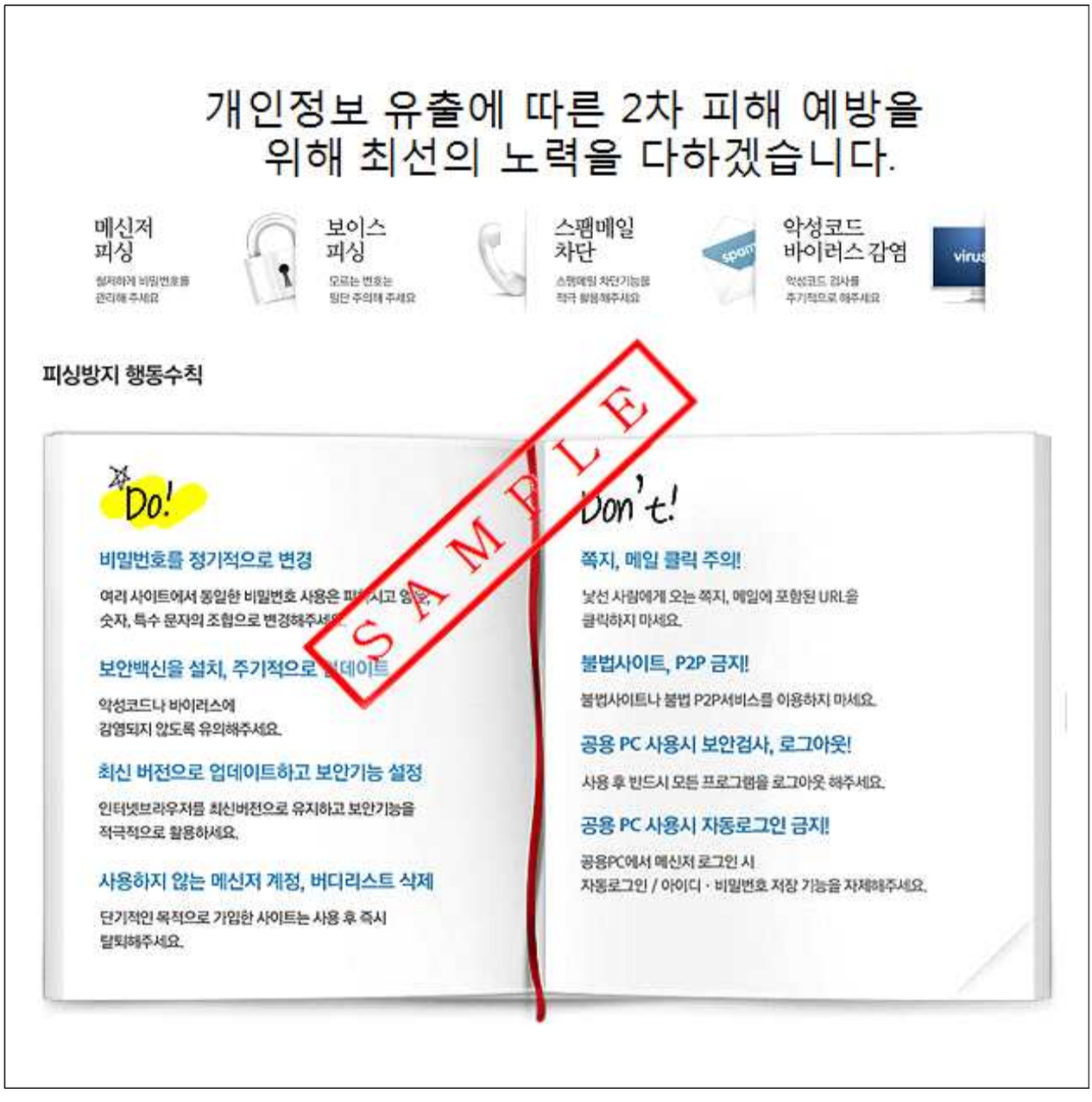
우리 진흥원은 조속한 범인 검거와 고객정보의 회수를 위하여 수사기관 및 관계기관에 적극 협조할 것이며, 업계 전문가 및 관련 정부 기관들과 함께 유출 정보의 유포 방지 및 2차 피해예방을 위하여 최선의 노력을 다할 것입니다. 관련하여 궁금한 점이 있으시면 아래 핫라인으로 연락주시기 바랍니다.
핫라인: 061-350-OOOO 메일주소: OOOO@kca.kr

해킹으로 인해 고객 여러분께 불편을 끼쳐드린 점 다시 한번 고개 숙여 사과드리며, 이번 일을 계기로 최고 수준의 보안으로 한층 강화하여 신뢰를 줄 수 있는 진흥원이 되도록 노력하겠습니다.

개인정보 유출여부 확인을 위한 기능은 빠른 시간 내에 제공하겠습니다.

[별지 15]

고객의 대응방안 안내(예시)



[별지 16]

표준 개인정보 보호지침 [별지 제1호 서식]

개인정보 침해·유출 신고서

<table>
<tr><td>기 관 명</td><td colspan="5"></td></tr>
<tr><td>고객에의 통지 여부</td><td colspan="5"></td></tr>
<tr><td>유출된 개인정보의 항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출된 시점과 그 경위</td><td colspan="5"></td></tr>
<tr><td>유출피해 최소화 대책·조치 및 결과</td><td colspan="5"></td></tr>
<tr><td>고객이 할 수 있는 피해 최소화 방법 및 구제절차</td><td colspan="5"></td></tr>
<tr><td rowspan="3">담당부서·담당자 및 연락처</td><td>구분</td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보 보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>개인정보 보호담당자</td><td></td><td></td><td></td><td></td></tr>
</table>

유출신고 접수기관	기관명	담당자명	연락처

[별지 17]

개인정보 침해·유출 신고 관리대장

신고 접수		신 고 내 용	처리결과	결 재		
일시	신고인 인적사항			개인정보 취급자	개인정보 보호담당자	개인정보 보호책임자

[별지 18]

개인정보 침해·유출 사고 보고서

개인정보 보호담당자	개인정보 보호책임자

침해·유출사고 처리 담당자	침해·유출사고 번호

신고자 정보	
소 속	
신고자 이름	
전화번호	
E-mail	

피해 시스템 정보	
IP 주소	
호스트 명	
운영체제	
추정 피해 시간	
시스템 운영 환경	

공격 시스템 정보	
IP 주소	
호스트 명	

사고에 대한 설명(간단히 작성)	
사고발견 경위, 피해현황 등	

관련 기관(부서) 통지	
기관(부서)명	통지 내용

[별지 19]

개인정보 침해·유출 사고 처리 보고서

<table>
<tr><td>보고일자</td><td>201 년 월 일</td><td>문서번호</td><td></td></tr>
<tr><td colspan="4">침해·유출 신고/접수번호</td></tr>
<tr><td>침해·유출
대상정보</td><td colspan="3">☐ 일반 개인정보 ☐ 주민등록번호 ☐ 외국인등록번호
☐ 민감정보 ☐ 계좌번호 ☐ 신용카드번호</td></tr>
<tr><td>접수일시</td><td></td><td>신고자</td><td></td></tr>
<tr><td>침해·유출사고
처리책임자</td><td></td><td>신고자
연락처</td><td></td></tr>
<tr><td>신고내용</td><td colspan="3"></td></tr>
<tr><td rowspan="2">대응과정</td><td>일시</td><td colspan="2">대응활동</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>침해·유출
내용</td><td colspan="3">※ 확인된 침해 정보의 세부사항, 규모 및 유출방법
- 침해·유출방법 : 유출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안전한 저장, 파기, 비파기 등 세부사항</td></tr>
<tr><td>침해·유출
발생 경위</td><td colspan="3"></td></tr>
<tr><td>관련자</td><td colspan="3"></td></tr>
<tr><td>침해·유출
발생 원인</td><td colspan="3"></td></tr>
<tr><td>증거자료</td><td colspan="3"></td></tr>
<tr><td>복구 및 재발
방지 조치</td><td colspan="3"></td></tr>
<tr><td>처분</td><td colspan="3"></td></tr>
</table>

제 · 개정 이력

순번	제 · 개정일	변경내용	관리부서	비고
1	2011. 12. 7.	- 개인정보 내부관리계획	기획조정실	제정
2	2012. 2. 29.	- 별지6 신설, 용어의 명확화	기획조정실	개정
3	2014. 7. 31.	- 용어 재정의, 별지 변경 등	기획조정실	개정
4	2016. 3. 18.	- 개인정보처리위탁계약서 양식 등	기획조정실	개정
5	2017. 5. 10.	- 개인정보의 파기 등	기획조정실	개정
6	.			
7				