개인정보보호 내부관리규칙

제정 2012. 02. 08.
개정 2014. 02. 13.

제1장 총칙

제1조(목적) 개인정보 내부관리규칙(이하 ‘본 규칙’ 또는 ‘내부관리규칙’이라 한다)은 개인정보보호법의 내부관리규칙의 수립 및 시행 의무에 따라 제정된 것으로 한국콘텐츠진흥원(이하 ‘진흥원’라 한다)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위) 본 규칙은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의) 본 규칙에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “개인정보”라 함은 생존하는 개인에 관한 정보로서 성명/주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호/문자/음성/음향 및 영상 등의 정보(해당 정보만으로 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
2. “개인정보보호책임자”라 함은 진흥원의 개인정보보호 업무 및 조직을

총괄하여 지휘하는 자로 부원장(콘텐츠진흥)을 말한다. <개정 2014.2.13.>

3. “개인정보관리실무자”라 함은 개인정보보호책임자를 보좌하여 개인정보보호업무에 대한 실무를 총괄하는 자로 정보보안 업무 담당자를 말한다.

4. “개인정보분야별책임자”라 함은 진흥원의 업무를 위해 개인정보파일을 보유·이용·제공하는 취급 부서의 장을 말한다.

5. “개인정보처리담당자”라 함은 개인정보분야별책임자를 보좌하여 해당 부서의 개인정보를 활용한 업무를 실제 수행하며 개인정보취급자를 관리·감독을 하는 자를 말한다.

6. “개인정보취급자”라 함은 진흥원 내에서 고객의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자로 개인정보를 취급하는 직원을 말한다.

7. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

제2장(내부관리규칙의 수립 및 시행)

제4조(내부관리규칙의 수립 및 승인) ① 개인정보관리실무자는 진흥원의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리규칙을 수립하여야 한다.

② 개인정보관리실무자는 개인정보보호를 위한 내부관리규칙의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리규칙을 수립하여야 한다.

③ 개인정보보호책임자는 개인정보관리실무자가 수립한 내부관리규칙의 타당성을 검토하여 개인정보보호를 위한 내부관리규칙을 승인하여야 한다.

④ 개인정보관리실무자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 11월말까지 내부관리규칙의 타당성과 개정 필요

성을 검토하여야 한다.

⑤ 개인정보관리실무자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리규칙의 개정안을 작성하여 개인정보보호책임자에게 보고하고 개인정보보호책임자의 승인을 받아야 한다.

제5조(내부관리규칙의 공표) ① 개인정보보호책임자는 前 조에 따라 승인한 내부관리규칙을 진흥원 전 임직원에게 공표하여야 한다.

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

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 의무와 책임) ① 개인정보보호책임자는 고객의 개인정보보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보보호 관리 책임자 및 취급자의 의무와 책임의 규정 및 총괄 관리
2. 내부관리규칙의 수립 및 승인
3. 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
4. 임직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검, 대응, 사후조치 총괄
5. 고객으로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄
6. 임직원 및 개인정보취급업무 수탁자 등에 대한 교육 총괄
7. 본 규칙에 규정된 개인정보보호와 관련된 제반 조치의 시행 총괄
8. 기타 고객의 개인정보보호에 필요한 사항

② 개인정보보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리·감독하여야 하며, 임직원에 대한 교육 및 보안서약 등을

통해 개인정보 침해사고를 사전에 예방한다.

③ 개인정보보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보관리실무자로 임명한다.

④ 개인정보관리실무자는 개인정보보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.

제7조(개인정보분야별책임자의 의무와 책임) ① 개인정보 분야별 책임자는 고객의 개인정보보호를 위하여 다음 각 호의 임무를 수행한다.

1. 부서의 개인정보 교육 및 관리·감독(부서 추진계획의 수립 및 시행)
2. 개인정보 접근권한 승인 및 단말기 설정 등 보호장치에 관한 사항 감독
3. 부서 내 개인정보 취급 내역과 취급자에 대한 기록 확보 및 점검 실시
4. 부서의 개인정보취급자 현황, 개인정보 취급 현황 등의 통계, 개인정보 침해 및 위법 사항 등을 개인정보보호책임자에게 주기적으로 보고
5. 부서 내 개인정보침해사고 발생 시 개인정보보호책임자에게 보고하고 협력하여 조사, 처리 및 재발 방지 방안 수립
6. 개인정보를 유관기관에 제공하거나 접근권한을 제공할 경우 관리·감독
7. 취급업무를 외부기관에 위탁한 경우 수탁기관의 개인정보보호 처리에 관한 업무 관리·감독
8. 개인정보 유출 시 개인정보 주체에 통지

② 분야별책임자는 부서 내 개인정보처리담당자를 지정하여 업무를 운영할 수 있다.

제8조(개인정보취급자의 범위 및 의무와 책임) ① 개인정보취급자의 범위는 진흥원 내에서 고객들의 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직, 외부업체 직원도 포함될 수 있다.

② 개인정보취급자는 고객의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보보호 활동 참여
2. 내부관리규칙의 준수 및 이행
3. 개인정보의 기술적·관리적 보호조치 기준 이행
4. 임직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등
5. 기타 고객의 개인정보보호를 위해 필요한 사항의 이행

제4장 개인정보의 기술적·관리적 보호조치

제9조(물리적 접근제한) ① 개인정보보호책임자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.

② 개인정보보호책임자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람내용에 관한 관리대장을 작성하도록 하여야 한다.

③ 개인정보보호책임자는 물리적 접근제한 관리대장의 출입 및 열람내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

제10조(출력 복사 시 보호조치) ① 개인정보보호책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.

② 개인정보보호책임자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사할 경우 출력·복사자의 성명, 일시 등을 기재하여 개인정보 유출 등에 대한 책임 소재를 확인할 수 있는 강화된 보호조치를 추가로 적용할 수 있다.

③ 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제11조(개인정보취급자 접근권한 관리 및 인증) ① 개인정보보호책임자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.

② 개인정보보호책임자는 개인정보취급 업무를 담당하는 임직원의 담당업무에 따라 개인정보 취급권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정 및 삭제 권한)을 차등 부여한다.

③ 개인정보보호책임자는 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

④ 개인정보보호책임자는 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.

⑤ 개인정보보호책임자는 제1항 내지 제4항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.

제12조(개인정보의 암호화) ① 개인정보보호책임자는 주민등록번호, 신용카드 번호 및 계좌번호에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

② 개인정보보호책임자는 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화 하여 저장하는 방식을 고려할 수 있다.

③ 개인정보보호책임자는 정보통신망을 통해 고객의 개인정보 및 인증정보를 송수신 할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다.

④ 개인정보취급자는 고객의 개인정보를 개인용 컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

제13조(접근통제) ① 개인정보보호책임자는 정보통신망을 통한 불법적인

접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 및 운영한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보보호책임자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다. 개인정보취급자는 개인정보보호책임자가 수립한 비밀번호 작성규칙을 준수하여야 한다.

③ 개인정보보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

제14조(접속 기록의 위변조 방지) ① 개인정보보호책임자는 접속 기록의 위변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입/출력, 수정, 등 DB접근)하는 경우에는 처리일시, 처리내역 등 접속기록을 저장한다.

② 개인정보보호책임자는 제1항의 접속기록에 대해 분기1회 이상 정기적으로 확인·감독한다.

③ 개인정보보호책임자는 제1항의 접속기록에 대해 위·변조 방지를 위해 별도의 저장매체에 백업 보관하며, 보관기간은 최소 6개월 이상으로 한다.

제15조(보안프로그램의 설치 및 운영) ① 개인정보보호책임자는 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프

로그램 등의 보안 프로그램을 설치·운영하여야 한다.

② 보안 프로그램은 항상 최신의 버전으로 업데이트를 적용하여야 한다.

③ 보안 프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시간 감시 기능을 적용하여야 한다.

제5장 정기적인 자체감사

제16조(자체감사 주기 및 절차) ① 개인정보보호책임자는 개인정보보호를 위한 내부관리 규칙 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 감사 또는 점검하여야 한다.

② 개인정보보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.

③ 개인정보보호 자체감사는 최소 반기 1회 이상 실시한다.

제17조(자체검사 결과 반영) ① 개인정보보호책임자는 개인정보 보호를 위한 자체감사 실시 결과, 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 본 규칙의 내용을 위반할 때에는 시정·개선 또는 인사발령 등 필요한 조치를 취하여야 한다.

② 개인정보보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 개인정보 취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

제6장 개인정보보호 교육

제18조(개인정보보호 교육 계획의 수립) ① 개인정보보호책임자는 다음 각

호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 12월말까지 수립한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

② 개인정보보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제19조(개인정보보호 교육의 실시) ① 개인정보보호책임자는 고객정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 연2회 이상의 개인정보보호 교육을 실시한다.

② 연2회의 정기 교육은 상반기에 1회, 하반기에 1회 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 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

부칙

본 규칙은 2012년 2월 8일부터 시행한다.