[참고 1] 비영리단체를 위한 개인정보 내부관리 계획(예시)

아래 예시는 내부관리 계획에 일반적으로 포함되는 내용을 정리한 것으로, 필요에 따라 수정해 활용하면 됩니다. 다만 공공기관이나 일반 기업 사례를 참고하여 작성한 것이기에, 비영리단체에 꼭 들어맞지 않는 내용도 포함되어 있을 수 있습니다. 비영리단체 맥락에 보다 적합한 개인정보 내부관리 계획 양식을 앞으로 발전시켜 나갈 필요가 있겠습니다.

[표지]

ㅇㅇㅇㅇㅇㅇ(단체명)

개인정보 내부 관리계획

20XX. XX. XX

[단체 직인]

[수정 이력]

[수정 이력]

순번	구분	시행 일자	주요내용
O	제정	OOOO. OO. OO.	
O	일부개정	OOOO. OO. OO.	[사유] OOOO. OO. OO. 개인정보보호법 개정 내용 반영 [수정사항] 1. OOOOO → 1. XXXXX
O	전부개정	OOOO. OO. OO.	1. OOOOO 2. OOOOO 3. OOOOO

제1장 총칙

제1조(목적)

ㅇㅇㅇㅇㅇ(단체명)(이하 '단체'라 한다) 개인정보 내부관리계획(이하 '본 계획' 또는 '내부관리계획'이라 한다)은 「개인정보 보호법」제29조(안전조치의무)와 '개인정보의 안전성 확보조치 기준'(제2023-6호)에 따라 제정된 것으로, ㅇㅇㅇㅇㅇ(단체명)가 개인정보를 처리함에 있어서 개인정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면, 전화, 팩스 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 ㅇㅇㅇㅇㅇ(단체명)의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 계획이 적용된다.

제3조(용어 정의)

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보"란 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. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
3. "개인정보보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말한다.
4. "개인정보보호담당자"란 개인정보보호책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보보호책임자가 일정 요건의 자격을 갖춘 이를 지정한다.
5. "개인정보취급자"란 사업장 내에서 고객의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
6. "개인정보처리시스템"란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

① 개인정보보호책임자는 ㅇㅇㅇㅇㅇ(단체명)의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.
② 개인정보보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.
③ 개인정보보호책임자는 개인정보보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.
④ 개인정보보호담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 11월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.
⑤ 개인정보보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보보호책임자에게 보고하고 개인정보보호책임자의 승인을 받아야 한다.

제5조(내부관리계획의 공표)

① 개인정보보호책임자는 제4조에 따라 승인한 내부관리계획을 매년 1월말까지 단체 전 임직원에게 공표한다.
② 내부관리계획은 임직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 지정)

단체는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자 중에서 1인 이상을 개인정보보호책임자로 임명한다.

1. 단체의 대표 또는 임원
2. 개인정보 처리 관련 업무를 담당하는 부서의 장

제7조(개인정보보호책임자의 역할과 책임)

① 개인정보보호책임자는 개인정보 보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보 보호관리자 및 취급자의 의무와 책임의 규정 및 총괄관리
2. 내부관리계획의 수립 및 승인
3. 개인정보의 안전성 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 계획에 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 개인정보보호담당자로 임명한다.

④ 개인정보보호담당자는 개인정보보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.

제8조(개인정보취급자의 범위 및 역할과 책임)

① 개인정보취급자의 범위는 단체 내에서 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.

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

1. 개인정보보호 활동 참여
2. 내부관리계획의 준수 및 이행
3. 개인정보의 안전성 보호조치 기준 이행
4. 임직원 또는 제3자에 의한 위법.부당한 개인정보 침해행위에 대한 점검 등

5. 기타 개인정보 보호를 위해 필요한 사항의 이행

제4장 개인정보의 안전성 확보조치

제9조(접근권한의 관리)

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.
② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.
⑥ 개인정보처리자는 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.

제10조(접근 통제)

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 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 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 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.
④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

⑤ 개인정보처리자는 업무용 모바일 기기의 분실・도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제11조(개인정보의 암호화)

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 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 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 개인정보처리자는 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 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제12조(접속 기록 보관 및 점검)

① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 2년 이상 보관・관리하여야 한다.

② 개인정보처리자는 개인정보의 오・남용, 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.
③ 개인정보처리자는 접속기록이 위・변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

제13조(악성프로그램 등 방지)

① 개인정보처리자는 악성프로그램 등을 방지・치료할 수 있는 보안 프로그램을 설치・운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

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 실시하여야 한다.

제14조(물리적 안전조치)

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립・운영하여야 한다.
② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출・입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제15조(출력 복사시 보호조치)

① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.
② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력・복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

제16조(개인정보의 파기)

① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각・파쇄 등)
2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제

③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 개인정보보호법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

제5장 개인정보보호 실태 점검

제17조(개인정보보호 실태 점검의 실시)

① 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 점검・관리 하여야 한다.
② 개인정보보호책임자는 개인정보보호 실태 점검의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.
③ 개인정보보호 실태 점검은 연1회 이상 실시한다.

제18조(점검 결과 반영)

① 개인정보보호책임자는 개인정보 보호를 위한 점검 실시 결과, 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 본 계획의 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

제19조(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.

제20조(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 연1회 이상의 개인정보보호 교육을 실시한다.

② 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.

③ 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 계획은 OOOO년 OO월 OO일부터 시행한다.