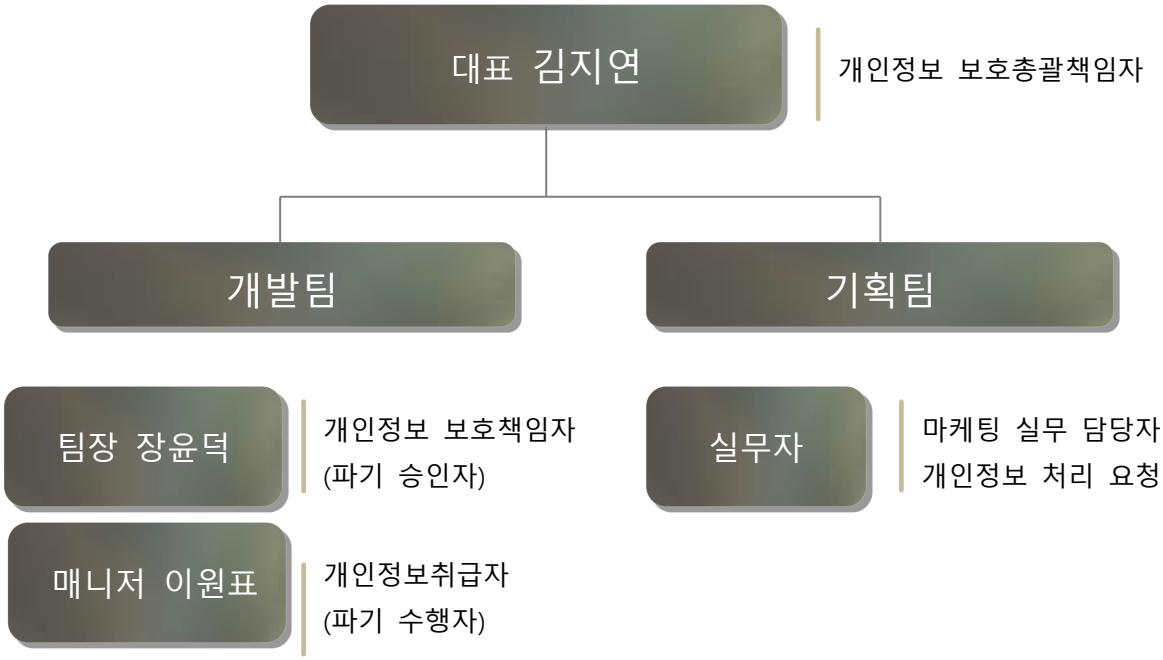
개인정보보호

내부 관리계획서

2019.04.25

Index

① 개인정보처리 관련 조직구성도



2019년 04월 25일부터 개인정보보호를 위해 위와 같은 조직 구성으로 수행 중임을 명시합니다.

② 개인정보 내부관리계획 방침

제 1 장 총칙

제 1 조 (목적)

본 계획은「개인정보보호법」(이하 "개인정보법") 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정통망법") 등에 따라 개인정보취급자가 처리하는 개인정보가 분실, 도난, 누출, 변조, 훼손되지 않도록 회사가 취하여야 하는 기술적, 관리적, 물리적 보호조치의 구체적인 내용을 정하는 것을 목적으로 한다.

제 2 조 (적용범위)

① 본 계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보에 대해 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 외부업체 직원에 대해 적용된다.

② 본 계획에서 언급되지 않는 사항은 관련 법규 및 회사의 사규에 따른다.

제 3 조 (용어 정의)

① '개인정보'라 함은 살아 있는 개인에 관한 정보로서 성명, 연락처, 주소 등의 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, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말한다.

③ '정보주체'란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

④ '개인정보 보호책임자'란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말한다.

⑤ '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.

⑥ '개인정보 파기감찰자'란 개인정보처리자의 개인정보 처리에 관한 업무 중 파기 업무 수행 과정에서 내부관리기준에 맞춰 수행되는지 감독하는 자를 말한다.

제 2 장 내부관리계획 수립 및 시행

제 4 조 (내부관리계획의 수립 및 변경)

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

② 개인정보 보호책임자는 내부관리계획의 변경이 필요한 경우 타당성을 검토한 후 내부관리계

획을 변경할 수 있다.

제 5 조 (내부관리계획의 공표)

개인정보 보호책임자는 내부관리계획을 회사 내 서버에 게시하는 등의 방법으로 공표하여 임직원이 쉽게 확인할 수 있도록 한다.

제 3 장 개인정보보호책임자의 의무와 책임

제 6 조 (개인정보보호책임자 지정)

① 회사는 고객, 임직원 기타 개인의 정보가 분실・도난・누출・변조・훼손되는 것을 방지하기 위하여 개인정보의 처리에 관한 업무를 총괄해서 책임지는 개인정보 보호책임자를 지정한다.

② 개인정보 보호책임자는 개인정보 처리 관련 업무를 담당하는 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)으로 한다.

제 7 조 (개인정보 보호책임자의 의무와 책임)

① 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

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 오용・남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리・감독
7. 개인정보처리방침의 수립・변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기

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

③ 개인정보보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 조직의 장에게 개선조치를 보고하여야 한다.

제 8 조 (개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급자는 회사 내에서 정보주체의 개인정보를 처리하는 업무를 수행하는 자를 말한다.

② 개인정보취급자는 다음 각 호의 의무와 책임을 이행한다.

1. 내부관리계획의 준수 및 이행
2. 개인정보의 기술적, 관리적 보호조치 기준 이행
3. 업무상 알게 된 개인정보를 제3자에게 제공하지 않음

제 9 조 (개인정보 파기감찰자의 범위 및 의무와 책임)

① 개인정보 파기감찰자는 회사 내에서 정보주체의 개인정보 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 수행 업무 시 현장 참관하여 내부관리계획 기준에 맞춰 파기가 진행되고 있는지를 감독하는 업무를 수행하는 자를 말한다.

② 개인정보취급자는 다음 각 호의 의무와 책임을 이행한다.

1. 내부관리계획의 준수 및 감독 이행
2. 개인정보의 기술적, 관리적 보호조치 기준 이행
3. 업무상 알게 된 개인정보를 제3자에게 제공하지 않음

제 4 장 개인정보의 기술적・관리적・물리적 안전조치

제 10 조 (개인정보취급자 접근권한 관리 및 인증)

① 회사는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 회사는 개인정보취급자의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 서약서를 받아야 한다.

③ 회사는 제1항, 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 회사는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 회사는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

제 11 조 (비밀번호 관리 및 개인정보 암호화)

① 회사는 개인정보취급자 또는 정보주체가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다.

② 회사는 비밀번호에 적정한 기간의 유효기간(반기별 1회 이상)을 설정하여야 한다.

③ 패스워드 작성 규칙: 영문 대/소문자, 숫자, 특수문자 등의 3조합 8자리이상 또는 2조합 10자리 이상

제 12 조 (접근통제)

① 회사는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 대하여 접근 통제 등에 관한 조치를 하여야 한다.

② 회사는 인터넷 홈페이지를 통해 고유식별정보가 유출・변조・훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

③ 회사는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

④ 회사는 업무용 모바일 기기의 분실・도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제 13 조 (접속기록의 위・변조 방지)

① 회사는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관하여야 한다.

② 회사는 개인정보취급자의 접속기록이 위・변조 및 도난, 분실되지 않도록 해당 접속기록을 별도 저장장치 등에 정기적으로 백업하여 안전하게 보관하여야 한다.

③ 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

제 14 조 (보안프로그램의 설치 및 운영)

① 회사는 개인정보처리시스템 또는 업무용 컴퓨터 등에 악성 프로그램 등을 방지・치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치・운영하여야 한다.

② 회사는 보안프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 적용하여야 한다.

③ 회사는 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시해야 한다.

④ 회사는 악성프로그램 등이 발견되는 경우 삭제 등의 대응조치를 하여야 한다.

제 15 조 (물리적 접근제한)

① 회사는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립・운영하여야 한다.

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

③ 회사는 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.

제 16 조 (개인정보 파기)

① 회사는 개인정보의 수집목적 또는 제공 받은 목적을 달성한 경우 개인정보를 지체없이 파기하여야 한다. 단, 법령의 규정에 따라 보존할 필요가 있는 경우에는 그러하지 아니하다.

② 개인정보의 파기는 고객의 동의 철회 시 개인 식별이 불가능하도록 조치된 형태로 파기되어야 한다.

③ 시스템 상에서 개인정보 파기시는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제하여야 한다.

④ PC 상에서의 개인정보 파기시 해당 개인정보가 완전히 삭제될 수 있도록 조치하여야 한다.

⑤ 개인정보가 포함된 문서의 파기시 쇄절기를 통한 완전한 파기를 수행하여야 한다.

⑥ 개인정보가 저장된 매체의 파기시 포맷 등의 조치를 통해 완전한 파기를 수행하여야 한다.

⑦ 외부업체에 제공된 개인정보에 대해서는 주기적으로 파기여부를 점검하고, 업체로부터 파기 확인서를 요청하여야 한다.

제 17 조 (출력 및 복사 시 보호조치)

① 개인정보취급자는 개인정보처리시스템에서 개인정보의 출력 시(인쇄, 화면표시, 파일생성 등) 개인정보보호책임자의 승인 하에 출력 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

② 회사는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

제 5 장 개인정보보호 교육

제 18 조(개인정보보호 교육)

① 회사는 개인정보보호 및 침해사고 예방을 위하여 임직원을 대상으로 개인정보보호 교육을 실시한다.

1. 교육횟수 : 반기별 1회 이상 (연 2회 이상)
2. 교육대상 : 개인정보 보호책임자, 개인정보취급자, 개인정보 파기감찰자 및 임직원
3. 교육내용 및 방법 : 개인정보의 안전한 처리 및 침해사고 예방을 위한 교육을 실시하며, 집체 교육, 인터넷 교육, 그룹웨어 교육 등 구체적 상황에 맞는 방법을 통해 실시한다.

② 개인정보 보호책임자는 교육실시 내역에 대한 근거자료를 최소 3년간 보관해야 한다.

제 6 장 개인정보 침해대응 및 피해구제

제 22 조(권익침해 구제방법)

개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다.

부 칙

본 계획은 2019년 04월 25일부터 시행한다.