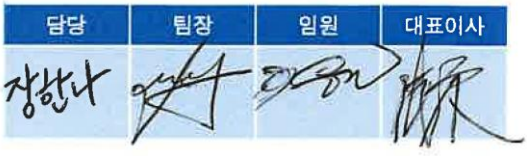
개인정보보호 내부관리계획

2025. 1. 1

(주)휴넥트



Revision History				
Revision	Reason for change	Date	작성자	비고
Ver.01	신규 제정	2012-01-02	이용신	
Ver.01.1	내부점검에 따른 항목보완/추가	2012-07-03	이인영	15,21,22조
Ver.01.2	장애대응 등 보완	2012-09-12	이인영	22조
Ver.01.3	2013년 내부관리계획	2012-12-30	이인영	
Ver.01.4	2015년 내부관리계획	2014-12-30	이인영	
Ver.01.5	2016년 내부관리계획	2015-12-30	강윤희	
Ver.01.6	2017년 내부관리계획	2017-01-01	이인영	6조
Ver.01.7	2018년 내부관리계획	2018-01-01	이인영	
Ver.01.8	2019년 내부관리계획	2019-01-01	이인영	개인정보책임자 변경
Ver.01.9	2020년 내부관리계획	2020-01-01	이인영	개인정보책임자 변경
Ver.01.10	2021년 내부관리계획	2021-01-01	이인영	사명 변경
Ver.01.11	2022년 내부관리계획	2021-12-21	장한나	제 8 장
Ver.01.12	2023년 내부관리계획	2022-12-29	장한나	
Ver.01.13	2024년 내부관리계획	2024-12-13	장한나	
Ver.01.14	2025년 내부관리계획	2025-01-10	장한나	개인정보책임자 변경 및 제9장 추가

2025년 정기적 자체검사실시 및 개인정보보호교육 일정

구분	대상	일시
개인정보보호 내부점검	개인정보담당자 및 취급자	2025년 6월 20~28일
개인정보시스템 설비점검	위탁관리업체	2025년 6월 21~25일
개인정보보호교육	개인정보취급자	2025년 6월~10월 (2주에 한번 1시간씩)
수탁자 정보보호교육	위탁업체 관리직원	2025년 10월

제 1 장 총 칙

제1조(목적)

개인정보보호 내부관리계획(이하 '본 계획' 또는 '내부관리계획'이라 한다)은 개인정보보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 ㈜휴넥트 (이하 '회사'이라 한다)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오.남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보 및 개인영상정보기기(CCTV)에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 직원 및 외부위탁업체 그리고 회사 관할 기관에 대해 적용된다.

제3조(용어 정의)

본 계획에서 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. "개인정보 보호책임자"라 함은 회사 및 관할기관의 개인정보보호 업무 및 조직을 총괄하여 지휘·감독하는 자를 말한다.
3. "개인정보 보호담당자"라 함은 개인정보 보호책임자를 보좌하여 개인정보보호업무에

대한 실무를 총괄하고 관리하는 자를 말한다.

4. "개인정보 분야별 책임자"라 함은 회사 및 관할기관 각 부서의 개인정보 업무를 지휘·감독하는 자를 말한다.
5. "개인정보취급자"라 함은 회사 및 관할기관 내에서 정보주체의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
6. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

제 2 장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

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

② 개인정보 보호담당자는 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.

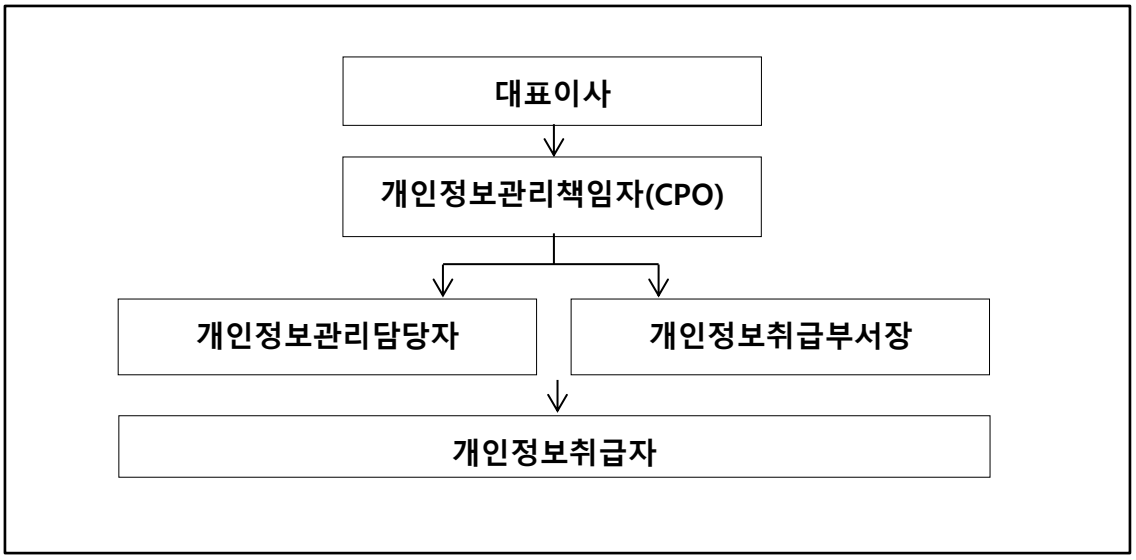
⑤ 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제5조(내부관리계획의 공표)

① 개인정보 보호책임자는 제4조에 따라 승인한 내부관리계획을 매년 1월말까지 회사 전 직원 및 관할기관에 공표한다.(2016년 12월 공표에 따라, 본항은 2017년부터 적용)

② 내부관리계획은 직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제 3 장 개인정보 보호책임자의 의무와 책임



[구성조직도]

제6조(개인정보 보호책임자의 지정)

① 회사는 "개인정보보호법시행령 제32조 제2항에 의하여 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람을 개인정보 보호책임자로 임명하며, 개인정보를 처리하는 부서의 장을 개인정보 분야별책임자로 임명한다.

② 회사는 다음 각호에 해당하는 자를 개인정보 보호책임자로 지정하며, 개인정보 분야 별책임자는 자체계획으로 임명하거나 임명하지 아니할 수 있다.

1. 개인정보 처리 관련 업무를 담당하는 부서의 장 (임원)

구 분	부서/직위	성 명
개인정보보호책임자	전무	이용신

제7조(개인정보 보호책임자의 의무와 책임)

① 개인정보 보호책임자는 정보주체의 개인정보보호하고 개인정보와 관련한 정보주체의 불만을 처리하기 위하여 다음 각 호의 임무를 수행한다.

1. 정보주체 개인정보의 수집·이용·제공 및 관리에 관한 업무의 총괄
2. 개인정보보호 관리 책임자 및 취급자의 의무와 책임의 규정 및 총괄관리
3. 내부관리계획의 수립 및 승인
4. 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
5. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검, 대응, 사후 조치 총괄
6. 정보주체로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄
7. 직원 및 개인정보취급업무 수탁자 등에 대한 교육 총괄
8. 본 계획에 규정된 개인정보보호와 관련된 제반 조치의 시행 총괄
9. 기타 정보주체의 개인정보보호에 필요한 사항

② 개인정보 보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리·감독하여야 하며, 직원에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.

③ 개인정보 보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리

전담부서의 직원 중 1인 이상을 개인정보 보호담당자로 임명한다.

④ 개인정보 보호담당자는 개인정보 보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.

⑤ 개인정보 보호책임자는 개인정보관리에 대하여 개인정보 분야별책임자를 지정하여 관리할 수 있다.

제8조(개인정보 부서장/담당자/취급자의 범위 및 의무와 책임)

① 개인정보관리 부서장은 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 취급자 중 부서의 장을 정하여 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보관리책임자 위임한 개인정보보호와 관련된 업무
2. 개인정보보호 계획 운영 및 소속직원에 대한 교육실시
3. 각 사업장 별 개인정보취급에 관한 실태 점검

② 개인정보 담당자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보 보호책임자가 임명하여 정보주체의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보관리책임자 위임한 개인정보보호와 관련된 업무
2. 정보보호마크(ePRIVACY)담당
3. 업무를 수행함에 있어서 취급하는 개인정보에 대한 보호관리
4. 웹사이트상의 개인정보에 대한 보호관리
5. 개인정보보호 계획 운영 및 소속직원에 대한 교육실시

③ 개인정보취급자의 범위는 회사 내에서 정보주체들의 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.

개인정보취급자는 정보주체의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

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

제 4 장 개인정보의 수집·이용

제9조(개인정보의 수집 및 수집 제한)

① 정보주체로부터 개인정보를 수집하는 경우에는 정보주체의 동의를 얻어야 하며, 그 수집 목적의 범위에서 이용할 수 있다. 정보주체의 개인정보를 수집하는 경우는 다음과 같다.

1. 온라인 홈페이지의 온라인 입사지원을 통한 정보 수집
2. 개인정보 수집·활용 동의서(서면)를 통한 정보 수집
3. 교육 또는 세미나 참석자에 대한 방명록을 통한 정보 수집

② 제1항의 규정에 의한 동의는 서면 또는 홈페이지상의 동의란에 대한 표시 등의 방법에 의한다

③ 제1항의 규정에도 불구하고 다음에 해당하는 경우 개인정보를 수집할 수 있다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

3. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
4. 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
5. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

④ 기본적인 인권에 관한 민감한 개인정보의 수집을 금지한다. 다만, 정보주체의 자발적·명시적 동의 또는 수집 대상 개인정보가 명시되어 있는 법률에 근거한 경우에는 수집을 허용한다.

⑤ 정보주체의 개인정보를 수집하는 경우, 적법하고 공정한 수단에 의하여 서비스 제공에 직접적으로 관련되어 필요한 최소한의 정보를 수집하여야 한다.

제10조(개인정보의 수집에 대한 고지)

① 정보주체로부터 제9조1항의 규정에 의한 동의를 받고자 하는 경우 또는 개인정보를 제3자로부터 제공받은 경우에는 미리 다음 각 호의 사항을 서면 또는 인터넷 홈페이지 등을 통하여 내용을 쉽게 확인할 수 있도록 정보주체에게 고지하거나 서비스 이용약관에 명시하여야 한다.

1. 개인정보보호책임자의 성명, 소속, 전화번호, 전자우편주소
2. 개인정보의 구체적인 수집목적 및 이용목적
3. 동의 철회, 열람 또는 정정 요구 등 정보주체 및 법정대리인의 권리와 그 행사방법
4. 정보주체로부터 수집하고자 하는 개인정보 항목
5. 수집하는 개인정보의 보유·이용기간 및 법적 근거 등 보유 근거

6. 기타 개인정보에 대한 처리 또는 관리 방식

제11조(개인정보의 이용 및 제공의 제한)

① 개인정보를 제10조의 규정에 의한 고지의 범위 또는 서비스 이용약관에 명시한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니 된다. 다만, 정보주체의 별도 동의가 있거나 다음 각 호의 1에 해당하는 경우에는 예외로 한다.

1. 다른 법률에 특별한 규정이 있는 경우
2. 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
3. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
4. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
5. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
6. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
7. 법원의 재판업무 수행을 위하여 필요한 경우
8. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

② 다른 개인정보처리자로부터 정보주체의 개인정보를 제공받은 자는 정보주체의 별도 동의가 있거나 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 제3자에게 제공하여서는 아니 된다.

③ 제1항 및 제2항의 규정에 의한 정보주체의 동의를 얻고자 하는 때에는 미리 정보주

체에게 개별적으로 서면, 전자우편, 전화 등으로 제10조 1항 각호의 사항을 고지하여야 한다.

제12조(개인정보 취급자의 제한)

① 개인정보 분야별책임자는 개인정보를 취급할 수 있는 자를 다음 각 호의 1에 해당하는 자로 정하여 최소한으로 제한하여야 한다.

1. 정보주체를 직접 상대로 하여 업무를 수행하는 자
2. 개인정보 보호책임자 등 개인정보관리 업무를 수행하는 자
3. 데이터베이스를 포함한 전산 관련 업무를 수행하는 자
4. 기타 업무상 개인정보의 취급이 불가피한 자

제13조(개인정보처리의 위탁)

① 업무상 타인에게 개인정보의 수집·취급·관리 등을 위탁하는 경우에는 서면, 전자우편, 전화 또는 홈페이지를 통하여 미리 그 사실을 정보주체에게 고지 또는 공개하여야 한다.

② 제1항의 규정에 의한 위탁계약을 체결하는 때에는 수탁자와 다음 각 호의 사항을 합의하여 서면 또는 전자적 기록으로 보존하여야 한다.

1. 기술적·관리적 보호 의무
2. 개인정보에 관한 비밀 유지 의무
3. 처리하는 개인정보의 제3자 제공 금지
4. 내부 규정에 의한 손해배상 책임
5. 기타 개인정보를 안전하게 처리하기 위하여 필요한 사항

③ 위탁 처리되는 개인정보가 안전하게 관리 될 수 있도록 수탁자가 제2항 각호의 내용을 성실하게 이행하는지 여부에 대하여 위탁한 업무의 범위 내에서 적절한 감독을 행

하여야 한다.

④ 제1항의 규정에 의하여 개인정보의 수집을 위탁 받은 자가 개인정보를 수집하는 때에는 미리 위탁 받은 사실을 정보주체에게 고지하여야 한다.

⑤ 제1항의 규정에 의하여 개인정보 수집·취급·관리 등을 위탁 받은 자는 개인정보를 위탁 받은 목적 외의 용도로 이를 이용하거나 제3자에게 제공하여서는 아니 된다.

제 5 장 개인정보의 기술적.관리적 보호조치

제14조(물리적 접근제한)

① 개인정보 분야별책임자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.

② 개인정보 분야별책임자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

③ 개인정보 보호책임자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

제15조(출력 복사시 보호조치)

- 개인정보 분야별책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.

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

개인정보 취급자 등 임직원이 고객의 개인정보에 대한 종이 인쇄 및 외부 저장매체 저장 등 출력.복사가 필요한 경우 및 출력•복사물로부터 다시 출력•복사하는 경우에는 출력.복사의 목적 및 용도, 소속, 이름, 요청일, 사용일 등을 명시하여 개인정보관리책임자에게 사전 승인을 받아야 한다.

① 출력.복사 관리 대장의 기록

개인정보를 종이로 인쇄하거나, 디스켓, USB, 콤팩트디스크 등 이동 가능한 저장매체에 보사할 경우 다음 각 호의 사항을 출력.복사 관리 대장에 기록하거나 별도의 기록을 남기고 개인정보관리책임자의 사전 승인을 득해야 한다.

- 출력•복사물 일련번호
- 출력•복사물의 형태
- 출력•복사 일시
- 출력•복사의 목적
- 출력•복사를 한 자의 소속 및 성명
- 출력•복사물을 전달 받을 자
- 출력•복사물의 파기일자
- 출력•복사물의 파기책임자

② 출력.복사 관리 대장의 양식

출력•복사시 기록양식은 아래와 같다.

출력•복사물 관리 대장

출력,복사물 관리 대장								
일련 번호	형태	일시	목적	출력물 복사를 한자	전달 받을자	파기 일자	파기 책임자	사전 승인자
				소속 성명	소속 성명			

※ 출력•복사물 관리 대장 표지 기재사항 : 상단에 표지 제목으로 "개인정보 출력•복사물 관리 대장"을 기재하고 하단에 "개인정보를 불법 유출할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있습니다" 는 경고 문구 기재

※ 양식 사이즈 : A4

※ 관리 대장 보존기한 : 최소한 1년간 보관한다.

※ 일련번호 : 출력•복사물에 일련번호가 자동으로 출력되지 않는 경우 "연도-팀(또는 그룹)코드-연도내 발생순서" 형식으로 한다.

※ 형태 : "프린트물", "복사물", "디스켓", "콤팩트디스크", "USB 메모리"등으로 기재한다.

※ 일시 : 출력•복사 일시

※ 소속 : 팀명

※ 파기일자 : 승인받은 파기일자를 기재하며, 목적이 달성되면 파기일자 이전이라도 파기

※ 파기책임자 : 책임지고 출력•복사물을 파기할 자를 기재

※ 파기일자, 파기책임자 기재 예외

파기일자 및 파기책임자를 사전에 알 수 없는 경우에는 "미정"이라고 기재한다.

※ 사전승인자 : 사전승인한 자의 서명 또는 날인

③ 이용자 발송 용도

우편발송, 고지서 발급, 이메일 발송 등 개인정보 처리시스템에 저장된 내역을 수령권한이 있는 이용자에게 필수적, 반복적, 정형화된 서비스의 일환으로 제공하는 경우에는 건별로 기록하지 아니하고 총 개수를 기록하며 파기 여부 확인은 예외로 한다.

④ 권한의 위임

개인정보관리 책임자는 사안에 따라 출력.복사의 승인 권한을 개인정보관리자 및 기타 실무자에게 위임할 수 있으며 개인정보관리책임자가 승인한 위임자가 서명 날인한 것은 개인정보관리책임자가 서명.날인 한 것으로 간주한다.

1. 이용자의 개인정보 관련 된 불만 사항 및 민원을 처리하는 경우 해당 실무자

2. 본인만에 관한 개인정보로서 본인 확인 후 본인에게 제공하는 경우 해당 실무자

3. 개인정보관리책임자가 승인한 바 있는 정기적 뉴스레터의 발송을 위한 경우 해당 실무자

⑤ 사후 승인

아래 각 항의 경우에는 사전 기록 및 개인정보 관리책임자의 승인을 받지 아니하고 우선 출력•복사 후 관리 대장에 기록하고 사후에 개인정보 관리책임자가 이를 확인하여도 무방하다.

1. 회원 가입 신청서 등과 같이 개인정보가 기재된 사항을 회사가 제공하는 것이 아니고 회사가 고객 등으로부터 접수받는 경우

2. 긴급한 상황에 의해 개인정보취급 권한을 가진 내부 직원에게만 전달하는 경우

(개인 정보 도용 등 긴급 상황 발생시)

3. 개인정보 취급자가 개별 건별로 상위 결제권자에게 결제 득후 개인정보 취급자와

상위결제권자만 접근 가능토록 별도의 시건장치가 된 장소에 보관하는 경우

단, 이 경우에도 고객명부와 같은 대량의 고객정보를 출력•복사하는 경우에는 기록을 하여야 한다.

4. 약관 및 정책의 변경 등 이용자와의 주요 계약관계를 유지하기 위해 법률에서 규정한 신속한 정보 전달이 필요한 경우

5. 법원 등 국가기관에 소송 자료로써 제출을 하여야 하는 경우

제16조(개인정보취급자 접근권한 관리 및 인증)

① 개인정보 분야별책임자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.

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

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

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

⑤ 개인정보 분야별책임자는 제1항 내지 제4항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

제17조(개인정보의 암호화)

① 개인정보 분야별책임자는 주민등록번호 등 개인정보보호법에서 규정한 고유식별번호

및 민감정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

생년월일	암호화 없음
비밀번호	sql_password로 암호화
주민번호	수집안함

② 개인정보취급자는 비밀번호를 사용하는 경우 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.

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

④ 개인정보취급자는 정보주체의 개인정보를 개인용 컴퓨터(PC) 및 보조저장매체에 저장할 때에는 이를 암호화해야 한다.

제18조(접근통제)

① 개인정보 보호책임자는 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 개인정보 보호책임자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다. 개인정보취급자는 개인정보 보호책임자가 수립한 비밀번호 작성규칙을 준수하여야 한다.

③ 개인정보 보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통

해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

제19조(접속 기록의 위변조 방지)

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

② 개인정보 보호책임자는 제1항의 접속기록에 대해 년1회 이상 정기적으로 확인.감독한다.

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

제20조(보안프로그램의 설치 및 운영)

① 개인정보 보호책임자는 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프로그램 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.

제21조(장애 및 침해대응)

① 개인정보 백업

1. 모든 개인정보는 해킹, 컴퓨터 바이러스 감염, 전원공급 중단, 재해발생 등의 정보

시스템 장애로 인한 분실, 도난, 변조 또는 멸살된 경우에 대비한 신속한 복구를 위하여 별도의 미디어를 이용한 백업을 하여야 한다.

- 필요시 결제정보, 거래정보 등 중요한 정보에 대해서는 실시간(Real-time) 백업시스템이나 이중처리 시스템(Dual-system)을 운영할 수 있다.

2. 개인정보가 저장된 백업미디어는 온•습도 유지, 화재방지, 감시, 시건장치 등 필요한 조치가 취해진 용기 또는 장소에 보관, 유지한다.

② 개인정보 취급 시스템 취약성 점검 및 분석

1. 시스템의 정상적인 통신이 이루어지도록 온라인 회선 및 설비에 대해 정기적으로 점검하고 그 결과를 기록, 유지한다.

2. 개인정보를 취급하는 정보시스템의 취약점으로 인해 시스템 장애나 개인정보에 대한 침해가 일어나지 않도록 년1회 이상 취약성 진단을 실시하며 취약점에 대한 적절한 조치를 취하도록 한다.

- 취약성 진단은 전문지식이 있는 내부 전담직원 또는 외부의 취약성 진단 전문 기관, 인력을 활용하여 실시한다.

③ 개인정보 장애 및 침해 사고 시 대응 및 복구

1. 개인정보 침해사고의 징후

- 개인정보가 외부 또는 허가되지 않은 자에게 노출되거나 외부에서 언급되는 것을 발견한 경우

- 개인정보에 대해 불필요한 잦은 조회와 다운로드를 발견한 경우

- 다량의 개인정보들이 허가 없이 전송되거나 출력되고 있는 것을 발견한 경우

- 자신이 관리하는 개인정보 데이터 또는 문서파일이 삭제되거나, 변조, 손상된 것을 발견한 경우

- 개인정보 처리시스템에 대한 최종 로그인•로그아웃 시간이 자신의 실제 최종 로그인•로그아웃 시간과 다르게 표시된 경우

- 개인정보 처리시스템의 로그인 계정에 대한 시도의 실패 흔적을 발견한 경우

- 개인정보 처리시스템이나 소프트웨어에 오류가 발생하거나 비정상적으로 종료하거나 재부팅되는 경우

- 일반 사용자가 관리자 권한으로 작업을 시도하는 경우

- 침입탐지시스템, E-Mail 모니터링 시스템 등의 정보보호 시스템에서 경고가 발생한 경우

- 퇴직자, 휴직자의 계정으로의 접근이 시도된 것을 발견하는 경우

- 기타 침입이나 사고 징후를 발견한 경우

2. 개인정보 시스템 장애 유형

- 정전으로 인한 장애

이는 장애로 판정이 되며 재해에 의한 장애는 재해의 원인이 복구 후에 테스트 후 장비의 이상 유무를 확인하는 것이 중요

- 네트워크 과부하로 인한 장애

네트워크 회선은 그 대역폭이 한계가 있어서 여러명의 사람이 동시에 높은 대역폭을 가지는 작업을 수행하면 혹은 바이러스에 의한 높은 대역폭이 생겨버리면 전체 네트워크의 다운이 발생한다. 이는 간헐적으로 발생되는 사항이기 때문에 발견하기도 어렵고, 전례가 있기 때문에 전산 담당자에게 연락을 취해 네트워크 사용량을 분석하여 원인이 되는 지점을 빠르게 파악하여 대처 해야 한다.

- 장비(방화벽)의 문제에 의한 장애

잦은 환경적 요인에 의한 물리적 장애가 발생 되었을 경우엔 신속히 장비를 공수

하여 대체 장비를 설정해야 한다.

- 케이블 문제

대다수의 네트워크 장애는 케이블에서 문제가 발생한다. 케이블의 접지 상태가 좋지 않을 수도 있고, 케이블 선로 구성 시 작업자의 실수로 인해 배열이 다를 수 도 있다.

④ 개인정보 침해사고의 징후 또는 장애로 보안사고가 발견되는 즉시 발견자는 개인정보보호 담당자와 상위관리자에게 보고한다.

⑤ 개인정보보호 관리자와 개인정보보호 담당자는 그 문제의 유형에 따라 관련 대상자들과 상의하여 대응을 결정한다.

⑥ 개인정보 보안사고의 대응 시 전문적인 기술이 필요할 경우 외부전문가에 대한 비상연락망을 유지하여 외부전문가를 활용한다.

⑦ 개인정보 보안사고에 대한 내용을 지정된 보고자 외에 다른 사람에게 유출하지 않는다.

⑧ 개인정보 보안사고 해당 부서 및 개인정보보호 담당자는 보안사고로 인한 패해 상황 및 증거, 그리고 이에 따른 대책을 수립하여 개인정보보호 관리자에게 보고한다.

⑨ 필요 시 교육과 훈련을 통해 동일 문제가 재발하지 않도록 한다.

제22조(개인정보 파기)

① 개인정보 폐기 절차

1. 개인정보의 수집목적 또는 제공 받은 목적을 달성한 경우 개인정보를 지체 없이 파기하여야 한다. 단, 다음의 경우에는 예외로 한다.

- 상법 등 법령의 규정에 의하여 보존할 필요성이 있는 경우

- 보유기간을 미리 고객에게 고지하거나 명시한 경우

- 개별적으로 고객의 동의를 받은 경우

2. 개인정보의 파기는 고객의 동의 철회 시 개인 식별이 불가능하도록 조치된 형태로 파기되어야 한다. 단, 사후 문제 발생 시 대응을 위하여 별도 개인정보 List를 유지하고 이는 개인정보보호 담당자에 의해 직접 관리한다.

② 데이터 폐기 절차

1. 운영계 시스템 상에서 개인정보 폐기시는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제하여야 한다.

2. PC 상에서의 개인정보 폐기시 해당 개인정보가 완전히 삭제될 수 있도록 조치하여야 한다.

3. PC 상에서의 개인정보 폐기 조치결과를 개인정보보호 담당자에게 보고하여 개인정보보호 담당자가 폐기목록에 반영할 수 있도록 한다.

③ 문서 폐기 절차

1. 개인정보가 포함된 문서의 폐기시 쇄절기를 통한 완전한 폐기를 수행하여야 한다.

2. 해당 개인정보 문서 폐기 조치결과를 개인정보보호 담당자에게 보고하여 개인정보보호 담당자가 폐기목록에 반영할 수 있도록 한다.

④ 매체 폐기 절차

1. 개인정보가 저장된 매체의 폐기시 로우포맷 등의 조치와 더불어 물리적 파괴를 통하여 완전한 폐기를 수행하여야 한다.

2. 해당 개인정보 매체 폐기 조치결과를 개인정보보호 담당자에게 보고하여 개인정보보호 담당자가 폐기목록에 반영할 수 있도록 한다.

⑤ 외부 전송 데이터 폐기 확인 절차

1. 외부업체에 전송된 개인정보에 대해서는 별도 폐기목록을 유지하도록 강제하고 주기적으로 해당 폐기목록을 점검하여야 한다.

2. 해당 개인정보 폐기 조치결과를 개인정보보호 담당자에게 보고하여 개인정보보호 담당자가 폐기목록에 반영할 수 있도록 한다.

제 6 장 정기적인 자체감사

제23조(자체감사 주기 및 절차)

① 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 감사 또는 점검하여야 한다.

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

③ 개인정보보호 자체감사는 최소 년 1회 이상 실시하며, 관할기관을 포함하여 실시한다.

제24조(자체검사 결과 반영)

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

② 개인정보 보호책임자는 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.

제 7 장 개인정보보호 교육

제25조(개인정보보호 교육 계획의 수립)

① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 3월말까지 수립한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

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

제26조(개인정보보호 교육의 실시)

① 개인정보 보호책임자는 정보주체정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 회사 직원 및 관할기관을 대상으로 매년 정기적으로 년2회 이상의 개인정보보호 교육을 실시한다.

② 년2회의 정기 교육은 상반기에 1회, 하반기에 1회 실시한다.

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

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

제 8 장 영상정보처리기기(CCTV) 설치·운영 제한

제27조(영상정보처리기기의 개념)

① "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 다음의 장치를 말한다.

1. 폐쇄회로 텔레비전 : 다음의 어느 하나에 해당하는 장치
   I. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
   II. 위 I.에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
2. 네트워크 카메라 : 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

제28조(공개된 장소에서의 설치·운영 금지)

① 누구든지 다음의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영해서는 안 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 함)는 정보주

체가 쉽게 인식할 수 있도록 다음의 사항이 포함된 안내판을 설치해야 한다. 다만, 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 성명 및 연락처
4. 그 밖에 「개인정보 보호법 시행령」으로 정하는 사항

③ 이 경우에는 안내판 설치, 인터넷 홈페이지 게재 및 사업장 등에 공개할 때 위탁받는 자의 명칭 및 연락처를 포함시켜야 한다. 영상정보처리기기운영자가 설치·운영하는 영상정보처리기기가 다음의 어느 하나에 해당하는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 위의 안내사항을 게재할 수 있다.

1. 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우
2. 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우

④ 인터넷 홈페이지에 위의 안내 사항을 게재할 수 없으면 영상정보처리기기운영자는 다음 의 어느 하나 이상의 방법으로 안내사항을 공개해야 한다.

1. 영상정보처리기기운영자의 사업장·영업소·사무소·점포 등(이하 "사업장 등"이라 함)의 보기 쉬운 장소에 게시하는 방법
2. 관보(영상정보처리기기운영자가 공공기관인 경우만 해당함)나 영상정보처리기기운영자의 사업장 등이 있는 특별시·광역시·도 또는 특별자치도 이상의 지역을 주된 보급지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법

제29조(사생활 침해 우려가 있는 장소에서의 설치·운영 금지)

① 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영해서는 안 된다.

제30조(설치 목적 외 임의조작과 녹음의 금지)

① 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 안 되며, 녹음기능은 사용할 수 없다.

② 사생활 침해 우려가 있는 장소에서의 설치·운영 금지영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 조치를 해야 한다.

제31조(영상정보처리기기 운영·관리방침)

① 영상정보처리기기운영자는 다음의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련해야 한다.

1. 영상정보처리기기의 설치 근거 및 설치 목적
   I. 법령에서 구체적으로 허용하고 있는 경우
   II. 범죄의 예방 및 수사를 위하여 필요한 경우
   III. 시설안전 및 화재 예방을 위하여 필요한 경우
   IV. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람

I. 관리책임자 : 영상정보보유 관리자

II. 접근권한자 : 영상정보보유 부서의 담당자

4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

I. 촬영시간 : 24시간

II. 보관기간 : 30일(그리고 법이 허용하는 보관기간)

III. 보관장소 : 녹화영상(CCTV) 설치 해당 기관

IV. 처리방법 : 보관기간 만료 시 복원이 불가능한 방법으로 영구 삭제

5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소

I. 확인 방법 : 영상정보 관리책임자 및 담당자에게 미리 연락 후 방문

II. 확인 범위 : 정보주체 본인이 촬영된 최소한의 영상정보만 확인 가능

III. 확인 장소 : 녹화영상(CCTV) 설치 해당 기관

6. 정보주체의 영상정보 열람 등 요구에 대한 조치

I. 개인영상정보에 관하여 열람 또는 존재 확인. 삭제를 원하는 경우, 언제든지 영상정보처리기기 운영자에게 요구 가능하나, 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한정한다.

II. 개인영상정보에 관하여 열람 또는 존재 확인. 삭제를 요구한 경우 지체없이 필요한 조치를 취한다.

III. 정보주체의 개인영상정보 열람 등 요구 시 기록사항

① 개인영상정보 열람 등을 요구한 정보주체의 성명 및 연락처

② 정보주체가 열람 등을 요구한 개인영상정보 파일의 명칭 및 내용

③ 개인영상정보 열람 등의 목적

④ 개인영상정보 열람 등을 거부한 경우 그 거부의 구체적 사유

⑤ 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

I. 영상정보 요청 및 제공 절차

① 신　　청 : 정보주체 또는 수사관서에서 신청서 또는 공문으로 요청

② 접수·확인 : 본인 여부, 신청서 내용 확인 및 해당 영상 유무 파악

③ 내용 검토 : 제3자 영상 포함 및 타인의 사생활 침해 등 검토

④ 열람·제공 : 영상화면의 현장 열람 또는 영상파일/출력물 등 제공, 필요시 제3자의 영상 모자이크 또는 마스킹 처리후 제공

⑤ 안전 관리 : 제공받은 자는 제공받은 목적 범위 내 이용 및 안전한 관리

⑥ 파　　기 : 제공받은 자는 제공목적 달성한 후 즉시 파기 및 통보

II. 영상정보 열람 등의 청구를 거부할 수 있는 사유

① 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우

② 영상정보의 보관기간이 경과하여 파기한 경우

③ 기타 정보주체의 열람 등 요구를 거부할 만한 정당한 사유가 존재하는 경우(ex. 영상정보 열람으로 인하여 다른 사람의 사생활이나 정당한 이익을 침해할 우려가 큰 경우)

7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치

I. 개인정보에 대한 접근 권한을 차등화하고 열람시 열람 목적 열람자 열람 일시 등의 관리를 위해 열람신청서를 작성한다.

II. 개인영상 정보의 안전한 물리적 보관을 위하여 잠금장치를 설치한다.

III. 개인정보처리자는 영상정보 보호를 위한 기술적, 관리적 및 물리적 조치를 제3자에게 위탁할 수 있다.

- 개인영상정보의 보관기간이 경과하여 파기한 경우
- 기타 정보주체의 열람 등 요구를 거부할 만한 정당한 사유가 존재하는 경

우

8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

I. 영상정보처리기기 운영/관리 방침 안내문

- (주)휴넥트는 영상정보처리기기 운영·관리 방침을 통해 처리하는 영상정보가 어떠한 용도와 방식으로 이용 관리되고 있는지 알려드립니다. 다만 각 사업장 또는 소속기관에서 소관업무의 특성상 별도의 영상정보처리기기 운영·관리 방침을 마련하여 공개하는 경우에는 그에 따릅니다.

② 공개된 장소에서 영상정보처리기기를 설치·운영하려고 하거나 교도소·정신보건 시설 등에서 내부가 보이도록 영상정보처리기기를 설치·운영하려는 공공기관의 장은 다음의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴해야 한다.

1. 행정예고의 실시 또는 의견청취
2. 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

제32조(영상정보처리기기의 설치·운영 사무의 위탁)

① 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다.

② 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음의 내용이 포함된 문서로 해야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항

4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

③ 이 경우에는 안내판 설치, 인터넷 홈페이지 게재 및 사업장 등에 공개할 때 위탁받는 자의 명칭 및 연락처를 포함시켜야 한다.

제 9 장 개인정보 침해대응 및 피해구제

제33조(개인정보 침해사고 정의 및 유형)

① 개인정보 유출이란 정보주체의 동의 없이 개인정보가 외부로 유출되거나 접근이 허용된 상태를 의미하며, 다음 각 호의 사례를 포함한다.

1. 개인정보가 포함된 서류, 저장장치, 전자기기 등의 분실 또는 도난
2. 개인정보처리시스템에 비인가된 접근 발생
3. 개인정보 파일, 문서 등이 권한 없는 자에게 전달된 경우
4. 기타 개인정보가 외부로 유출된 모든 상황

② 개인정보 노출은 인터넷 상에서 별도의 해킹 방법 없이 개인정보가 접근 가능한 상태로 방치된 상황을 의미한다.

제34조(개인정보 침해사고 대응절차)

① 개인정보취급자는 개인정보 침해(유출·노출)가 발생했거나 의심되는 경우 즉시 업무 부서의 개인정보관리담당자 또는 분야별 책임자에게 보고해야 한다.

② 분야별 책임자는 개인정보 유출 사고가 발생한 경우, [별지서식 4] "개인정보 유출신고서"를 작성하여 개인정보관리담당자에게 제출해야 한다.

1. 관리담당자는 유출 내용 및 조치 결과를 5일 이내에 관계 기관(예: 행정안전부 또

는 한국인터넷진흥원)에 보고한다.

2. 1,000명 이상의 개인정보가 유출된 경우, 홈페이지에 통지 사항을 7일 이상 게재해야 한다.

③ 유출 보고 또는 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 경우, 전화로 사전 신고 후 [별지서식 4]"개인정보 유출신고(보고)서"를 제출할 수 있다.

④ 유출된 개인정보가 정보주체에게 직접적인 영향을 미칠 경우, 회사는 정당한 사유가 없는 한 5일 이내에 정보주체에게 다음 사항을 통지한다.

1. 유출된 개인정보 항목
2. 유출 사고의 발생 시점 및 경위
3. 정보주체가 취할 수 있는 보호조치 및 예방 방법
4. 유출로 인한 피해를 최소화하기 위한 회사의 대응 조치
5. 정보주체가 신고를 접수할 수 있는 담당부서 및 연락처

⑤ 통지 시 모든 항목을 확인하기 어려운 경우, 우선 유출 사실과 확인된 항목만 통지하고 추가 사항은 확인 즉시 통지한다.

⑥ 정보주체 통보는 서면, 이메일, 휴대전화 문자 등 가능한 방법을 통해 진행한다.

⑦ 정보 유출 사고 발생 시, 회사는 다음과 같은 절차를 통해 사고를 처리한다.

1. **인지 및 보고**

I. 개인정보취급자는 침해사고 발생 사실을 인지한 즉시 개인정보관리담당자 또는 개인정보관리책임자에게 보고한다.

II. 침해사고는 즉시 최고경영진 및 관련 부서에 공유되어 초기 대응이 준비된다.

2. **초기 대응**

I. 개인정보 유출 확산을 방지하기 위해 시스템 접속 차단, 계정 비활성화, 권한 제한 등의 긴급조치를 수행한다.

II. 유출된 개인정보에 접근 가능한 경로를 차단하고, 취약점 점검 및 긴급 복구를

실시한다.

3. **원인 분석**

I. 사고 원인을 파악하기 위해 관련 시스템의 로그를 분석하고, 취약점을 점검하며, 사고 경로를 조사한다.

II. 사고 발생 환경 및 유출 경로를 상세히 기록하여 추가적인 유사 사고를 예방한다.

4. **복구 및 개선**

I. 유출된 개인정보를 복구하고 추가 피해를 방지하기 위한 기술적 및 관리적 조치를 취한다.

II. 사고의 재발 방지를 위한 구체적인 개선 대책을 수립하고, 관련 부서와 협력하여 이행한다.

III. 모든 조치 과정 및 결과를 문서화하여 기록으로 유지한다.

5. **결과 보고**

I. 사고 대응 과정과 결과를 상세히 문서화하여 최고경영진에 보고한다.

II. 관계 기관(예: 행정안전부, 한국인터넷진흥원)에 사고 내용을 5일 이내에 보고하고 필요한 지원을 요청한다.

III. 정보주체에게 사고 발생 사실과 대응 내용을 알리고, 피해구제 방안을 안내한다.

제 35조(침해사고 재발 방지)

① 회사는 침해사고 발생 시 원인을 분석하여 재발 방지 대책을 수립한다.

② 개인정보 보호 관련 교육을 강화하며, 취약점 점검 및 시스템 보안 조치를 시행한다.

제 36조(개인정보 보호조직 구성 및 운영)

① 개인정보 침해사고 발생시 신속한 대응, 공격탐지, 피해복구, 예방 등 종합적이고 체계적인 공동대응 체제구축을 위해 교육정보담당관(정보기획담당) 주관 하에"개인정보보호조직(침해사고 대응반)"을 편성하고, 침해사고에 신속히 대처한다.

② 중요 정보시스템에 대한 백업(시스템, DB 등)을 실시하고, 백업된 자료는 원격지로 소산하여 중요 정보 유실을 방지한다.

③ 개인정보 보호조직(개인정보 침해사고 대응 조직)별 역할은 아래와 같다.

구 분	내용
개인정보보호책임자 (CPO)	- 개인정보 침해사고 예방, 처리 및 재발방지 총괄 관리 - 개인정보 침해사고 발생 시 침해사고 처리책임자를 지정 - 침해사고 대응조직 구성 및 운영
개인정보취급부서장 (침해사고 처리책임자)	- 해당 침해사고 발생 부서의 장으로 지정 - 처리 및 재발방지에 대한 책임을 지고 개인정보 침해사고 대응반과 협력하여 사고 해결
개인정보관리담당자	- 개인정보 침해사고를 접수하고 침해사고 대응 절차를 개시 - 대내(부서·팀 내)·외 비상연락 및 절차별 업무추진 - 개인정보 침해기록을 관리하고 필요시 관련자 및 기관에 보고
개인정보취급자 (전 직원)	- 모든 직원은 개인정보에 대한 침해사고가 발생한 것을 인지할 경우 개인정보보호 분야별 책임자를 경유하여 개인정보관리 담당자에게 신고

제 37조(권익침해 구제방법)

① 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다.

② 이 밖에 기타 개인정보침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

1. 개인정보 분쟁조정위원회 : 1833-6972(www.kopico.go.kr)

2. 개인정보 침해신고센터 : (국번없이) 118 (내선2번)(privacy.kisa.or.kr)
3. 대검찰청 사이버수사과 : (국번없이) 1301, privacy@spo.go.kr, (www.spo.go.kr)
4. 경찰청 사이버안전국 : (국번없이) 182, (cyberbureau.police.go.kr)

[별지서식 1]

개인정보 취급자 서약서

㈜휴넥트(이하 "회사")의 개인정보 취급자는 본 서약서가 근무기간뿐 아니라 퇴직 후에도 적용될 수 있음을 인식하고 숙독하신 후 서명하여 주시기 바랍니다.

1. 나는 회사로부터 취득한 모든 개인정보를 업무에 한해 이용할 것이며, 타기업의 보호대상 정보를 회사 내 보관치 않겠다.
2. 나는 상대가 누구이건 간에(회사직원, 고객 혹은 계약직 사원 등) 알 필요가 없는 자에게 직무상 알게 된 회사 혹은 제3자의 개인정보를 누설하지 않을 것이다.
3. 나는 명백히 허가 받지 않은 정보나 시설에 접근하지 않으며, 회사관련 업무를 수행할 때에는 사내에서 지정된 데이터 처리시설 및 설비만을 이용할 것이다.
4. 나는 업무와 관련한 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위에 대하여 회사의 규정과 통제절차를 준수할 것이다.
5. 나는 나에게 할당된 사용자 ID, 패스워드, 출입증, 개인정보 처리시스템을 타인과 공동 사용하거나 관련정보를 누설하지 않겠다.
6. 나는 회사로부터 제공받은 개인정보자산(서류, 사진, 영상, 전자파일, 저장매체 등)을 무단변조, 복사, 훼손, 분실 등으로부터 안전하게 관리하겠으며 승인 받지 않은 프로그램, 정보저장 매체(외장 Drive, CD.ROM, 외장 HDD 등)을 회사 내에서 사용하지 않겠다.
7. 나는 퇴직 시 회사에서 제공받은 회사 소유 모든 정보자산을 반드시 반납할 것이며, 퇴직 후에도 퇴직전의 모든 고객정보는 물론이고 영업비밀 등 기타 누설됨으로 인하여 회사에 손해가 될 수 있는 각종 정보에 대하여는 일체 누설하지 않겠다.

상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며 서약서의 보안 사항을 위반하였을 경우에는 "개인정보보호법률", "정보통신망이용촉진 및 정보보호 등에 관한 법률", "부정경쟁 방지 및 영업비밀보호에 관한 법률" 등 관련법령에 의한 민/형사상의 책임 이외에도, 회사의 사규나 관련 규정에 따른 징계조치 등 어떠한 불이익도 감수할 것이며 회사에 끼친 손해에 대해 지체 없이 변상/복구할 것을 서약합니다.

2025년 월 일

소 속 :

직 위 :

성 명 : (인)

[별지서식 2]

퇴직자 보안서약서

본인 _____은(는) 휴넥트 주식회사의 소속으로 _____년 __월 __일부터 _____년 __월 __일까지 근무기간 중 업무를 처리하는 과정에서 취득한 고객정보에 관하여 퇴직 후에도 관련 법률을 준수하고, 어떠한 경우에도 대외 유출하지 않을 것을 확약하며 만약 이를 위반할 경우 관련 법률과 규정에 의거 민사/형사상의 책임을 질 것을 서약합니다.

2025년 월 일

성 명 : (인)

[별지서식 3]

개인정보 위탁사업자 서약서

본인은 ㈜휴넥트(이하 "회사")의 협력사(외주용역, 프리랜서, 파트타이머 등) 직원으로 개인정보취급자로써, 금번 _____사업(용역, 프로젝트 등)을 수행함에 있어, 본 서약서가 근무기간 뿐 아니라 퇴직 후에도 적용될 수 있음을 인식하고 있으며 회사규정을 준수하고 업무와 관련하여 지득한 모든 사항에 대하여 일체 누설하지 않을 것이며, 이로 인한 문제 발생 시 법적 책임을 다할 것임을 서약합니다.

1. 나는 회사로부터 취득한 모든 개인정보를 위탁업무에 한해 이용할 것이며, 타기업의 보호대상 정보를 회사 내 보관치 않겠다.
2. 나는 상대가 누구이건 간에 알 필요가 없는 자에게 직무상 알게 된 회사 혹은 제3자의 개인정보를 누설하지 않을 것이다.
3. 나는 명백히 허가 받지 않은 정보나 시설에 접근하지 않으며, 회사관련 업무를 수행할 때에는 사내에서 지정되고 허가된 데이터 처리시설 및 설비만을 이용할 것이다.
4. 나는 업무와 관련한 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위에 대하여 회사의 규정과 통제절차를 준수할 것이다.
5. 나는 나에게 할당된 사용자 ID, 패스워드, 출입증, 개인정보 처리시스템을 타인과 공동 사용하거나 관련정보를 누설하지 않겠다.
6. 나는 회사로부터 제공받은 개인정보자산(서류, 사진, 영상, 전자파일, 저장매체 등)을 무단변조, 복사, 훼손, 분실 등으로부터 안전하게 관리하겠으며 승인 받지 않은 프로그램, 정보저장 매체를 회사 내에서 사용하지 않겠다.
7. 나는 퇴직 시 회사에서 제공받은 회사소유 모든 정보자산을 반드시 반납할 것이며, 퇴직 후에도 퇴직전의 모든 고객정보는 물론이고 영업비밀 등 기타 누설됨으로 인하여 회사에 손해가 될 수 있는 각종 정보에 대하여는 일체 누설하지 않겠다.

상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며 서약서의 보안사항을 위반하였을 경우에는 "개인정보보호 법률", "정보통신망이용촉진 및 정보보호 등에 관한 법률", "부정경쟁 방지 및 영업비밀보호에 관한 법률" 등 관련법령에 의한 민/형사상의 책임 이외에도, 회사의 사규나 관련 규정에 따른 징계조치 등 어떠한 불이익도 감수할 것이며 회사에 끼친 손해에 대해 지체 없이 변상/복구할 것을 서약합니다.

2025년 월 일

회사명 :

직 위 :

성 명 : (인)

[별지서식 4]

개인정보 유출신고(보고)서

사업장명	
정보주체에의 통지 여부	
유출된 개인정보의 항목 및 규모	
유출된 시점과 그 경위	
유출피해 최소화 대책·조치 및 결과	
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	
담당부서·담당자 및 연락처	

유출신고(보고) 접수자	사업장명	담당자명	연락처

2025년 월 일