

## ICTworks 개인정보처리방침

### 제1장 총칙

인프라닉스주식회사(이하 “회사”)는 고객의 개인정보를 소중하게 생각하고 고객의 개인정보를 효과적으로 관리하고 안전하게 보호하기 위하여 최선의 노력을 다 하고 있습니다. 회사는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』과 개인정보보호 관련 각종 법규를 준수하고 있습니다. 또한 개인정보처리방침을 제정하여 이를 준수하고 있으며, 본 취급방침을 홈페이지에 공개하여 고객께서 언제나 쉽게 열람하실 수 있도록 하고 있습니다.

1. 개인정보란, 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향, 영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함)를 말합니다.
2. 회사는 고객의 개인정보를 중요시하며, "정보통신망 이용촉진 및 정보보호 등에 관한 법률"에 관한 법률을 준수하고 있습니다.
3. 회사는 개인정보처리방침을 통하여 고객께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며, 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다.
4. 회사의 개인정보처리방침은 관련 법령 및 내부 운영 방침의 변경에 따라 변경될 수 있습니다. 개인정보처리방침이 변경되는 경우에는 그 이유 및 변경된 내용을 지체없이 공지합니다.
5. 영업의 전부 또는 일부를 양도하거나 합병 상속 등으로 그 권리 의무를 이전하는 경우 서면, 전자우편 등을 통하여 고객께 개별적으로 통지하거나, 홈페이지(<http://www.ictworks.com>) 첫 화면에서 식별할 수 있도록 표기하여 30일 이상 그 사실을 공지합니다.
6. 회사는 개인정보처리방침을 개정하는 경우 웹사이트(<http://www.ictworks.com>) 또는 개별공지를 통하여 공지합니다.

### 제2장 개인정보 수집 및 이용 목적

ICTworks 매니지드 서비스는 수집한 개인정보를 다음의 목적을 위해 이용합니다.

1. 서비스 가입/변경/해지 처리, AS 서비스 문의등을 포함한 이용계약 관련 사항의 처리
2. 요금감면 제공대상 여부 판단 및 기타 서비스의 제공
3. 기타 개인정보처리방침(<http://www.ictworks.com>)에 고지된 수탁자에게 서비스 제공 등 계약의 이행에 필요한 업무의 위탁

### 제3장 수집하는 개인정보의 항목 및 수집방법

ICTworks 매니지드 서비스는 회원가입, 상담, 서비스 제공을 위하여 아래와 같이 필요한 최소한의 개인정보만을 수집하며, 인종 및 민족, 사상 및 신조, 출신지 및 본적지, 정치적 성향 및 범죄기록, 건강상태 등 고객의 인권을 현저하게 침해할 우려가 있는 개인 정보는 수집하지 않습니다. 다만, 고객께서 수집에 동의하시는 경우는 예외로 합니다.

1. 수집하는 개인정보의 항목

#### 가. 필수정보

- 신청인의 성명, 이메일주소, 연락처
- 요금납부자의 성명, 청구지 주소, 연락처

#### 나. 선택정보

- 이용요금의 할인을 위하여 국가공공자명, 복지할인 증명 등 제증명 사항
- 서비스 이용 또는 업무처리 과정에서 생성되어 수집될 수 있는 정보
  - 서비스 이용기록, 접속로그, 쿠키, 접속IP정보, 결제기록, 이용정지 기록

2. 회사는 다음과 같은 방법으로 개인정보를 수집합니다.

가. 가입신청서, 인터넷 홈페이지, 전화, Fax 등을 통한 회원가입, 전화나 인터넷을 통한 상담, 경품 행사 응모, 배송 요청 등을 위하여 고객께서 제시하신 개인정보 수집

나. 서비스 이용 또는 업무처리 과정에서 생성되거나 생성정보 수집 툴을 통해 정보를 수집 등

### 제4장 개인정보 수집 및 이용 등에 관한 동의방법

1. 고객의 개인정보 수집 시에는 관련 법령의 규정에 따라 개인정보의 수집 이용 목적과 제3자 제공 및 취급을 위탁하고 있는 내용을 고객께 알리고 동의를 얻거나 개인정보처리방침을 통해 고지하고 있습니다.
2. '웹 회원약관', '상품별 이용약관' 및 '개인정보처리방침'에 따른 고객의 개인정보 수집, 이용, 제3자 제공 및 취급 업무의 위탁 등에 대해 고객께서는 아래와 같은 방법 중 하나를 선택하여 동의하실 수 있습니다.
  - 가. '서비스 가입신청서', '명의변경 신청서' 등에 첨부된 '개인정보의 수집, 이용, 제공 동의서'의 세부내용을 숙지하시고 '동의서'에 서명하시는 방법

나. 고객센터 등을 통한 전화상담의 경우 상담원으로부터 직접 동의 내용을 안내 받으시거나, 상담원의 안내에 따라 홈페이지(<http://www.ictworks.com>)에 게시된 ‘개인정보처리방침’을 확인하신 후 전화상으로 본인이 동의 의사를 표명하는 방법  
 다. 우편 또는 팩스를 통해 동의서에 서명, 날인 후 제출하는 방법 등

### 제5장 개인정보의 보유, 이용기간, 보관장소

1. 회사는 고객의 개인정보를 고객께 서비스를 제공하는 기간(이용기간) 또는 분쟁처리기간(보유기간) 동안에 한하여 보유하고 이를 활용합니다. 다만, 법률에 특별한 규정이 있는 경우에는 관계 법령에 따라 보관됩니다.
  - 가. 이용기간 : 서비스 가입기간(가입일~해지일) 또는 분쟁기간 동안
  - 나. 보유기간 : 요금정산, 요금 과오납 등 분쟁 대비를 위해 해지 후 6개월까지, 요금 미/과납이 있을 경우와 요금관련 분쟁이 계속될 경우에는 해결 시까지 보유 (단, 법령에 특별한 규정이 있을 경우 관련 법령에 따라 보관)
  - 다. 보관장소 : 개인정보 데이터는 국내에 보관하는 것이 원칙이며, 해외이전 불가 원칙이 적용됩니다.
2. 해지 고객의 개인정보는 국세기본법 제 85조의 3규정에 따라 다음 항목의 정보를 보관합니다.
  - 가. 보관항목 : 고객명, 고객식별번호, 전화번호, 요금내역(청구액, 부가세액, 수납액, 청구년월일, 수납년월일), 요금납부자명, 이용서비스, 감액 금액 및 사유, 요금 청구지 주소 등
  - 나. 보관기간 : 5년
3. 기타
  - 가. 표시/광고에 관한 기록 : 6개월(전자상거래 등에서의 소비자보호에 관한 법률)
  - 나. 계약 또는 청약 철회 등에 관한 기록 : 5년(전자상거래 등에서의 소비자보호에 관한 법률)
  - 다. 대금결제 및 재회 등의 공급에 관한 기록 : 5년(전자상거래 등에서의 소비자보호에 관한 법률)
  - 라. 소비자 불만 또는 분쟁처리에 관한 기록 : 3년(전자상거래 등에서의 소비자보호에 관한 법률)
  - 마. 신용정보의 수집/처리 및 이용 등에 관한 기록 : 3년(신용정보의 이용 및 보호에 관한 법률)

### 제6장 암호화 정책 수립

1. 클라우드 시스템에서 이용자 및 사용자의 개인정보, 인증정보, 의료정보 등 중요정보 저장 및 전송 시 안전한 보호를 위한 암호 정책을 수립·이행합니다.
2. 암호 정책은 관련 법령 요구사항을 준수하여야 하며 다음 각 호와 같이 데이터 처리 유형에 따른 암호화 대상 식별, 암호화 방식, 강도, 암호키의 관리 방안을 포함합니다.
  - 가. 데이터 저장 시 암호화 적용 대상
    - 1) 주민등록번호를 포함한 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)
    - 2) 비밀번호
    - 3) 신용카드번호, 계좌번호 등 주요 금융정보
    - 4) 지문, 홍채 등 바이오정보
  - 나. 데이터 전송 시 암호화 적용 대상
    - 1) 제2항 제1호에서 명시한 저장 시 암호화하여야 하는 대상
    - 2) 그 외 송·수신되는 모든 개인정보
  - 다. 암호화 대상별 암호화 방식과 알고리즘 강도 정의
    - 1) 비밀번호 저장 시 256bit 이상의 일방향 암호화 알고리즘 필수 적용
    - 2) 비밀번호 외 암호화 대상은 한국인터넷진흥원의 권고 방식으로 암호화
    - 3) 통신구간 암호화는 SSL 보안서버 구축 또는 별도 암호화 프로그램 적용
    - 4) PC 또는 모바일 저장 시 문서 암호 설정 또는 별도 암호화 프로그램 적용
  - 라. 암호키 관리 대책 인프라리스 클라우드 정보보안 지침
  - 마. 암호화 관련 시스템 운영 담당자 역할 및 책임 정의
  - 바. 그 외 암호화 관련 법적 요구사항 반영
3. 이용자(고객 등) 및 사용자(임직원 등)의 비밀번호 저장 시 암호 정책을 수립·이행한다. 그 외 기타 세부사항은 “암호키관리지침”에서 정함이다.

### 제7장 암호키 관리

1. 암호키 생성, 이용, 보관, 배포, 복구, 파기 등에 관한 절차를 다음 각 호의 내용을 포함하여 수립·이행합니다.
  - 가. 암호키 관리 담당자 지정
  - 나. 암호키 생성, 보관(소산 백업 등) 방법
  - 다. 암호키 배포 대상자 정의 및 배포방법(복호화 권한 부여 포함)
  - 라. 암호키 사용 유효기간(변경주기)
  - 마. 복구, 변경, 폐기 절차 및 방법 등
2. 암호키 생성 후 암호키는 다음 각 호의 사항을 고려하여 별도의 안전한 장소에 소산 보관하고, 암호키 사용에 관한 접근권한 부여를 최소화 합니다.

- 가. 암호키 DB와 분리하여 소산보관
  - 나. 보안USB 등 별도 지정된 장소 또는 방법으로 암호키 백업
  - 다. 백업 암호키 소산보관
  - 라. 암호키 접근권한 부여 최소화
    - 1) 저장공간 접근통제 적용
3. 암호키 변경에 관한 정책을 다음 각 호의 사항을 참고하여 수립·이행합니다.
- 가. 암호키 유효기간(변경주기)에 따라 암호키 변경
  - 나. 암호키 유출, 해킹 등이 의심되는 경우 암호키 즉시 변경

**제8장 개인정보 암호화**

개발자는 응용프로그램 개발 시 법률상 암호화를 요구하는 중요 개인정보 등을 포함하는 비밀정보에 대하여 다음과 같은 내용에 따라 기밀성 유지를 위한 보안대책을 마련·적용하여야 합니다.

구분		사용처	요구기준 (최소사양)
해쉬		패스워드 저장 시	SHA-256
암호화	대칭	비밀의 전송 시	3DES(168 비트) / AES 192 비트*
		비밀의 저장 시 개인정보 저장 시	3DES(168 비트) / AES 128 비트
	비대칭	SSL 사용 시	RSA 2048 비트
* 이와 동급 이상의 안정성을 가진 알고리즘으로 정보보호 최고책임자가 승인한 알고리즘도 사용 가능함			

**제9장 중요 정보 노출 방지**

개발자는 법률상 노출 제한이 요구되는 개인정보 등을 포함하는 비밀정보가 사용자에게 노출되지 않도록 응용프로그램 설계 시 다음의 사항을 준수하여야 합니다.

1. 권한이 없는 사용자가 중요정보에 접근 할 수 없도록 설계되어야 하며, 권한이 있는 경우에도 업무성격에 맞는 정보만 표시될 수 있도록 설계하여야 합니다.
2. 응용프로그램에서 리스트 형식의 상세 개인정보(주민등록번호, 비밀번호, 전화번호 등)를 화면에 출력할 때에는 정보의 일부가 음영 또는 별표(\*)처리되도록 설계하여야 합니다.
3. 응용프로그램에서 사용자의 정보가 노출되지 않도록 암호화하여 처리하고 웹 응용프로그램에서 웹 소스 보기등을 통해 사용자의 인증 정보가 노출되지 않도록 설계하여야 합니다.

**제10장 개인정보의 파기절차 및 방법**

회사는 원칙적으로 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체없이 파기합니다.

파기 절차 및 방법은 다음과 같습니다.

1. 파기절차
  - 가. 원칙적으로 고객께서 서비스 가입 등을 위해 제공하신 정보는 수집 및 이용목적이 달성된 후 별도의 DB로 옮겨져 (종이의 경우 별도의 서류함) 내부방침 및 관련 법령에 의한 정보보호 사유 (보유 및 이용기간 참조)에 따라 일정 기간 저장된 후 파기됩니다.
  - 나. 별도 DB로 옮겨진 개인정보는 법률에 의한 경우와 재가입시 가입비 면제 대상 여부를 확인하는 경우가 아니고서는 보유되는 이외의 다른 목적으로 이용되지 않습니다.
  - 다. 파기대상 : 보유기간 및 관련법령에 따른 보존기간이 종료된 고객정보
2. 파기방법
  - 가. 종이(서면)에 작성 출력된 개인정보 : 분쇄하거나 소각 등의 방법으로 파기
  - 나. DB 등 전자적 파일 형태로 저장된 개인정보 : 재생할 수 없는 기술적 방법으로 삭제

**제11장 개인정보 처리의 위탁**

회사는 서비스 이용계약, A/S 제공 및 그 부대업무의 대행 등 고객 편의 제공, 관리 등을 위하여 개인정보 처리업무를 위탁하고 있으며, 수탁자에 대해서는 “위.수탁계약서” 등을 통하여 관련 법규 및 지침의 준수, 정보보호 및 기밀유지, 제3자 제공금지, 사고 시 책임부담, 위탁기간 종료 즉시 개인정보의 반납/파기 의무 등을 규정하여 관리하고 있습니다.

○ 개인정보 처리업무 수탁사 및 위탁내용

수탁사	위탁 업무 내용
(주)케이티	서비스 관련 상담업무, 장애처리 기술지원, uCloud Server 컨설팅 및 기술지원 업무
(주)원스테크넷	매니지드 Security 서비스 운영, IPS, F/W, 웹방화벽 등의 원격 보안관제 수행

**제12장 이용자 및 법정대리인의 권리와 그 행사 방법**

고객의 개인정보 열람 및 정정을 위해서는 ‘개인정보변경’을, 가입해지(동의철회)를 위해서는 ‘해지신청서’를 작성하여 회사에 제출하거나, 웹사이트 고객의 경우 ‘회원탈퇴’를 클릭하여 본인 확인 절차를 거치신 후 직접 열람, 정정 또는 탈퇴가 가능합니다.

1. 개인정보의 열람, 증명 또는 정정

- 가. 고객(법정대리인)께서는 회사를 직접 방문하시어 개인정보에 대한 열람 증명을 요구 할 수 있습니다.  
그러나 고객의 개인정보 보호를 위하여 전화, 우편, Fax 등의 신청방법에 의해서는 고객의 개인정보에 대한 열람, 증명이 제공되지 않습니다.
- 나. 고객께서 본인의 개인정보에 대한 열람, 증명을 요구하시는 경우 고객의 신분을 증명 할 수 있는 주민 등록증, 여권, 운전면허증(신형) 등의 신분증명(사본)을 제시 받아 본인 여부를 확인합니다.
- 다. 고객의 대리인이 열람증명을 요구하는 경우에는 대리 관계를 나타내는 위임장, 명의고객의 인감증명서와 대리인의 신분증명서 등의 증표를 제시 받아 대리인인지 여부를 확인합니다.
- 라. 고객의 개인정보는 오류에 대한 정정을 요청하신 경우에는 정정을 완료하기 전까지 당해 개인정보를 이용 또는 제공하지 않습니다. 또한 잘못된 개인정보를 제3자에게 이미 제공한 경우에는 정정 처리결과를 제3자에게 지체없이 통지하여 정정이 이루어지도록 하겠습니다.

2. 개인정보의 수집과 이용 또는 제공에 대한 동의 철회

- 가. 고객께서는 위 제 1항 '나'에 고지된 신분증을 지참하시고 회사를 직접 방문하여 개인정보의 수집과 이용, 위탁 또는 제공에 대해 동의 하시거나, 이에 대한 동의를 선택적으로 철회하실 수 있습니다.
- 나. 회사의 고객센터에 전화 또는 '온라인 문의' 및 'E-mail 상담'등으로 연락하시면 지체 없이 조치하겠습니다.  
※ 단, 서비스 제공에 필요한 필수정보의 수집과 이용에 관한 동의철회는 예외로 합니다.
- 다. 회사는 고객의 요청에 의해 해지 또는 삭제된 개인정보는 “회사가 수집하는 개인정보의 보유 및 이용기간”에 명시된 바에 따라 처리하고 그 외의 용도로 열람 또는 이용할 수 없도록 처리하고 있습니다.

**제13장 개인정보 자동 수집장치의 설치운영 및 그 거부에 관한 사항**

회사는 홈페이지 운영에 있어 필요 시 정보를 찾아내고 저장하는 ‘쿠키(Cookie)’를 운용합니다. 쿠키는 회사의 웹사이트를 운영하는데 이용되는 서버가 고객의 브라우저에 보내는 아주 작은 텍스트 파일로서 고객의 컴퓨터 하드디스크에 저장됩니다. 고객께서는 웹브라우저의 보안 정책을 통해 쿠키에 의한 정보수집의 허용거부 여부를 결정하실 수 있습니다.

1. 쿠키에 의해 수집되는 정보 및 이용 목적

- 가. 수집 정보 : ID, 접속 IP, 접속로그, 이용 콘텐츠 등 서비스 이용정보
  - 나. 이용목적
    - 고객의 관심분야에 따라 차별화된 정보를 제공
    - 회원과 비회원의 접속 빈도나 방문시간 등을 분석하고 이용자의 취향과 관심분야를 파악하여 타겟(Target) 마케팅 및 서비스 개편 등의 척도로 활용합니다.
2. 고객은 쿠키 설치에 대한 선택권을 가지고 있습니다. 따라서 웹브라우저에서 옵션을 설정함으로써 쿠키에 의한 정보수집 수준의 선택을 조정하실 수 있습니다.
- 가. 웹브라우저의 [도구]메뉴에서 [인터넷옵션]->[보안]->[사용자 정의수준]을 선택하여 쿠키에 의한 정보 수집 수준을 정할 수 있습니다.
  - 나. 위에 제시된 메뉴를 통해 쿠키가 저장될 때마다 확인을 하거나, 아니면 모든 쿠키의 저장을 거부할 수도 있습니다.  
단, 고객께서 쿠키 설치를 거부하였을 경우 서비스 제공에 어려움이 있을 수 있습니다.

**제14장 개인정보의 기술적, 관리적 보호**

회사는 고객의 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 않도록 안전성 확보를 위하여 다음과 같은 기술적 관리적 대책을 마련하고 있습니다.

[기술적 보호대책]

- 1. 개인정보는 비밀번호에 의해 보호되며, 중요한 데이터는 파일 및 전송데이터를 암호화하거나 파일 잠금 기능(Lock)을 사용하는 등 별도 보안기능을 통해 보호되고 있습니다.
- 2. 백신 프로그램을 이용하여 컴퓨터 바이러스에 의한 피해를 방지하기 위한 조치를 취하고 있습니다. 백신 프로그램은 주기적으로

업데이트되며 갑작스런 바이러스가 출현할 경우 백신이 나오는 즉시 이를 도입, 적용함으로써 개인정보가 침해되는 것을 방지하고 있습니다.

3. 네트워크 상의 개인정보를 안전하게 전송할 수 있도록 보안장치(SSL)를 채택하고 있습니다.
4. 해킹 등에 의해 고객의 개인정보가 유출되는 것을 방지하기 위해, 외부로부터 접근이 통제된 구역에 시스템을 설치하고, 침입을 차단하는 장치를 이용하고 있으며, 아울러 침입방지시스템을 설치하여 24시간 침입을 감시하고 있습니다.

#### [관리적 보호대책]

1. 회사는 고객의 개인정보에 대한 관리와 접근에 필요한 절차를 마련하여 임직원이 이를 숙지하고 준수 하도록 하고있으며 준수 여부를 주기적으로 점검하고 있습니다.
2. 회사는 고객의 개인정보를 취급할 수 있는 자를 최소한으로 제한하고 접근 권한을 관리하며, 교육을 통하여 법규 및 정책을 준수할 수 있도록 하고있습니다. 고객의 개인정보를 취급하는 자는 다음과 같습니다.
  - 가. 고객을 직,간접적으로 상대하여 마케팅 업무를 수행하는 자
  - 나. 개인정보관리책임자 및 개인정보관리담당자 등 개인정보 관리 및 개인정보보호 업무를 담당하는 자
  - 다. 기타 업무상 개인정보의 취급이 불가피한 자
3. 신규직원 채용 시 정보보호서약서에 서명하게 함으로써 직원에 의한 정보(개인정보 포함) 유출을 사전에 방지 하고, 수시로 개인정보보호 의무를 상기시키며 준수 여부를 감시하기 위한 내부 절차를 마련하여 시행하고 있습니다.
4. 개인정보 처리자의 업무 인수인계는 보안이 유지된 상태에서 철저하게 이뤄지고 있으며, 입사 및 퇴사 후 개인정보 침해사고에 대한 책임을 명확하게 규정하고 있습니다.
5. 회사는 전산실 및 자료보관실 등을 통제구역으로 설정하여 출입을 통제합니다.
6. 서비스 이용계약 체결 또는 서비스 제공을 위하여 고객의 은행결제계좌, 신용카드번호 등 대금결제에 관한 정보를 수집하거나 고객에게 제공하는 경우 당해 고객이 본인임을 확인하기 위하여 필요한 조치를 취하고 있습니다.
7. 회사는 고객 개인의 실수나 기본적인 인터넷의 위험성 때문에 일어나는 일들에 대해 책임을 지지 않습니다. 고객의 개인정보를 보호하기 위해서 자신의 ID와 비밀번호를 철저히 관리하고 책임을 져야 합니다.

#### 제15장 개인정보 관리책임자 및 담당자의 소속, 성명 및 연락처

회사는 고객의 개인정보를 보호하고 개인정보와 관련한 불만 및 문의사항을 처리하기 위하여 아래와 같이 관련 부서를 지정하여 운영하고 있습니다. 또한 고객의 의견을 매우 소중하게 생각합니다. 고객께서 문의사항이 있을 경우 회사의 지사를 방문하시거나 또는 개인정보담당부서로 문의하시면 신속,정확한 답변을 드리겠습니다.

1. 개인정보 보호책임 부서 및 연락처
  - 가. 개인정보 보호책임자 : MCS사업부 신동경 사업부장
    - 전화번호 : 02-2642-3131
    - 이메일 : [systeer\\_eng@infranicsmail.com](mailto:systeer_eng@infranicsmail.com)
  - 나. 개인정보 보호담당자 : MCS기술팀 류상훈 마스터
    - 전화번호 : 02-2642-3131
    - 이메일 : [systeer\\_eng@infranicsmail.com](mailto:systeer_eng@infranicsmail.com)
2. 개인정보 관리책임자 역할
  - 가. 개인정보보호 관련 주요 지침/정책/제도 수립 시행
  - 나. 개인정보 유출, 오남용 방지를 위한 내부통제시스템 구축
  - 다. 개인정보보호 분야 관리실태 감사 및 지도점검
  - 라. 개인정보보호 교육 계획 수립 시행
  - 마. 개인정보처리방침 수립 개정
  - 바. 개인정보 침해사고 예방 대응
  - 사. 기타 기타정보보호를 위하여 필요한 업무
3. 기타 개인정보침해에 대한 신고나 상담이 필요하신 경우에는 아래 기관에 문의하시기 바랍니다.
  - 가. 개인정보 분쟁조정위원회 : [www.kopico.go.kr](http://www.kopico.go.kr) / 국번없이 1833-6972
  - 나. 대검찰청 사이버수사과 : [www.spo.go.kr](http://www.spo.go.kr) / 02-3480-3570 또는 국번없이 1301
  - 다. 경찰청 사이버안전국 : [cyberbureau.police.go.kr](http://cyberbureau.police.go.kr) / 국번없이 182
  - 라. 개인정보침해신고센터 : [privacy.kisa.or.kr](http://privacy.kisa.or.kr) / 국번없이 118

#### 제16장 개인정보처리방침 고지

현 개인정보 처리방침 내용 추가, 삭제 및 수정이 있을 시에는 개정 최소 7일전부터 홈페이지의 '공지 사항'을 통해 고지할 것입니다. 개인정보의 수집 및 활용, 제3자 제공 등과 같이 이용자 권리의 중요한 변경이 있을 경우에는 최소 30일전에 고지합니다.

- 개인정보처리방침 공고일자 : 2020년 7월 01일
- 개인정보처리방침 시행일자 : 2019년 11월 01일