HEESUNG CATALYSTS CORP.

문서관리번호	HPJ-A-022
최초 제정일	2012.04.01
최신 개정일	2025.01.22
문서 관리자	인사총무팀

희성촉매 개인정보보호규정

제1장 총칙

제 1조(목적)

이 규정은「개인정보 보호법」제24조제3항 및 제29조와 같은 법 시행령 제21조 및 제30조에 따라 희성촉매주식회사(이하 "회사")의 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

제 2조(적용범위)

1. "개인정보"란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라고 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

※ 개인정보관리대상 : 업무상 개인정보를 수집하여 관리하고 있는 파일 또는 종이 형태와 업무처리를 위한 각종 신청 서식에 요청 받는 개인 정보도 해당

제 3조(용어 정의)

이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.
3. "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항 제1호 및 제2호에 해당하는 자를 말한다.
4. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
5. "정보통신망"이란「전기통신기본법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
6. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.
7. "내부망"이라 함은 물리적 망 분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
8. "비밀번호"라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

9. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
10. "공유설정"이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
11. "보조저장매체"라 함은 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.
12. "위험도 분석"이란 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출 시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

제 4조 개인정보 수집 시 동의

1. 개인정보를 수집하는 경우 정보주체에게 동의를 반드시 얻어야 한다.

- 개인정보의 수집, 이용목적 및 보유기간
- 개인정보를 제3자에게 제공하는 경우 개인정보를 제공 받는 자, 제공받는 자의 개인정보 이용목적, 제공하는 개인정보 항목, 보유 및 이용기간
- 민감정보 및 고유식별 정보의 수집, 이용

제 5조 개인정보의 폐기

1. 개인정보의 수집목적 또는 제공받은 목적을 달성한 경우, 개인정보를 폐기해야 한다. 단, 법령 등 규정 규정에 의하여 보존할 필요성이 있는 경우는 제외한다.
2. 개인정보의 폐기는 개인의 동의 철회 시 개인식별이 불가능하도록 폐기되어야 한다.
3. 시스템 상에서의 개인정보 폐기 시는 기록을 재생할 수 없게 삭제한다.
4. 문서의 폐기 시는 파쇄기를 이용하거나 완전 소각하여 폐기한다.

제 6조 내부감사

개인정보보호 체계에 대한 재평가 및 개선사항 이행을 위해 관리적, 기술적 보안점검 및 위험평가 등을 정기적으로 실시한다.

1. 개인정보 보안점검 및 감사결과에 따른 지적사항은 즉시 해결될 수 있도록 한다.
2. 차후 개인정보 보안점검 및 감사 시 기존 이행 점검결과에 따른 조치상황을 우선적으로 검토한다.

제2장 내부관리계획의 수립 및 시행

제 7조(내부관리계획의 수립 및 승인)

이 기준은 인사팀에서 수립하여 대표이사의 승인을 받아 시행한다. (세부내용은 별도의 내부관리계획 참조)

제 8조(내부관리계획의 공표)

이 기준의 시행일은 2012년 04월 01일로 한다.

제3장 개인정보보호책임자의 의무와 책임

제 9조(개인정보보호책임자의 지정)

개인정보 보호책임자의 자격요건에 부합하는 사람을 개인정보 보호책임자로 지정하며, 개인정보 보호책임자의 지정 시에는 공식적으로 책임과 역할을 부여한다.

제 10조(개인정보보호책임자의 의무와 책임)

1. 개인정보 보호책임자의 역할
   - 개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임지는 역할을 수행하는 사람으로, 개인정보 보호를 위해 개인정보와 관련된 내부지침을 준수하도록 기술적.관리적 보호조치를 실시하고 관리.감독하는 책임을 진다.
   - 또한, 정보주체의 불만사항 접수 및 처리에 대한 책임을 지며, 개인정보를 취급하는 직원에 대해 교육훈련을 실시하여야 한다. 개인정보를 취급하는 업무를 외부에 위탁한 경우, 개인정보 보호책임자는 해당 위탁자의 개인정보 관리현황을 지속적으로 확인해야 한다

제 11조(개인정보취급자의 범위 및 의무와 책임)

1. 개인정보취급자의 역할 및 책임
   - 개인정보취급자는 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자로서 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 해야 한다.

   ① 개인정보보호 활동 참여
   ② 내부관리계획의 준수 및 이행
   ③ 개인정보의 기술적.관리적 보호조치 기준 이행
   ④ 소속 직원 또는 제3자에 의한 위법.부당한 개인정보 침해행위에 대한 점검 등
   ⑤ 보안서약서 작성

제4장 개인정보의 처리단계별 기술적·관리적 안전조치

제 12조(개인정보취급자 접근 권한 관리 및 인증)

1. 개인정보처리시스템에 대한 접근권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여한다.
2. 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
3. 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.
4. 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 한다.

제 13조(비밀번호 관리)

개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 한다.
세부 비밀번호 작성규칙은 다음과 같다.

1. 8자리 이상 문자 숫자 조합 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 중 2종류 이상으로 구성
2. 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.
3. love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.
4. 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 6개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않는다.
5. 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.

제 14조(접근통제)

1. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치.운영한다.
   1) 개인정보처리시스템에 대한 접속 권한을 ID와 PW 그리고 IP(Internet Protocol)주소 등으로 제한하여 인가 받지 않은 접근을 제한한다.
   2) 외부에서 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지한다.
2. 취급중인 개인정보가 인터넷 홈페이지, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 다음과 같은 조치를 한다.
   1) 개인정보취급자의 컴퓨터는 원칙적으로 P2P 프로그램.공유 폴더 사용을 금지한다. 하지만 반드시 사용해야 할 경우 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하

도록 한다.

2) 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

※ Windows XP 접근통제 사용방법 : [설정] → [제어판] → [Windows 방화벽]에서 '사용(권장)' 클릭

제 14조(개인정보의 암호화)

1. 법 시행령 제25조 및 제33조에 따라 암호화하여야 하는 개인정보는 고유식별정보, 등을 말한다.
2. 제1항에 따른 개인정보를 정보통신망을 통하여 송.수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
3. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
4. 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 위험도 분석에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
5. 제1항에 따른 개인정보를 암호화하는 경우 안전하게 저장하여야 한다.
6. 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 기타 소프트웨어를 사용하여 암호화 저장하여야 한다.

제13조(접근기록의 보관 및 위·변조 방지)

1. 개인정보취급자가 개인정보처리시스템에 접속한 기록은 6개월간 보관·관리한다.
2. 개인정보취급자의 접속기록은 위·변조 및 도난, 분실되지 않도록 하며 수시로 백업을 한다.

제14조(보안프로그램의 설치 및 운영)

1. 악성 프로그램 등을 방지.치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치, 운영하며, 다음 각 호의 사항을 준수한다.
   1) 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시
   2) 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제15조(물리적 접근제한)

1. 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는

경우 이에 대한 출입통제 절차를 수립.운영한다.

2. 개인정보가 포함된 서류, 보조저장매체 등은 잠금 장치가 있는 안전한 장소에 보관하여야 한다.

제5장 개인정보보호 교육

제16조(개인정보보호 교육의 목적)

안전하게 개인정보가 관리될 수 있도록 개인정보취급자의 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키고자 함을 위해 개인정보보호 교육을 시행한다.

제17조(개인정보보호 교육의 세부 사항)

개인정보보호 교육 계획에는 교육을 하는 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함하고, 내부관리계획 또는 임직원의 결재를 얻어 관리한다.

교육방법은 집체교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수도 있다.

개인정보보호 교육내용 예시

- 개인정보보호의 중요성 설명
- 내부관리계획의 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법
- 개인정보의 기술적.관리적 보호조치 기준 이행
- 개인정보보호 위반을 보고해야 할 필요성
- 개인정보보호업무의 절차, 책임, 작업 설명
- 개인정보보호 관련자들의 금지 항목들
- 개인정보보호 준수사항 이행 관련 절차 등

제6장 개인정보 침해사고 발생시 조치

개인정보 유출 시 지체 없이(5일 이내) 정보주체에게 유출사실을 통지해야 하며, 1만명 이상 개인정보 유출 시에는 지체 없이(5일이내) 행정안전부 또는 한국정보화진흥원, 한국인터넷진흥원에 신고한다.

1. 통지방법

- 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법

· 1만명 이상 개인정보 유출 시, 통지와 동시에 인터넷 홈페이지에 7일 이상 게재

2. 조치방법

· 유출된 개인정보 확산 및 추가유출 방지를 위하여 접속경로 차단, 취약점 점검, 보완.

· 유출된 개인정보 삭제 등 긴급한 조치 필요 시 해당 조치를 먼저 취한 후 정보주체에게 통지 가능

· 개인정보에 관한 권리, 이익을 침해 받은 사람은 행정안전부장관에게 침해사실을 신고할 수 있으며 해당

침해 신고가 접수된 경우 처리대장을 작성하여 관리한다.

이 규정은 2012년 4월 1일부터 적용한다.