개인정보 내부관리 계획 신·구조문대비표

현 행	개 정 안
제2조 용어 정의 ①. ~ ㉟. (생 략) <신 설>	**제2조 용어 정의** - 연계정보 관련 정의 신설 ①. ~ ㉟. (현행과 같음) ㊱ "연계정보"란 본인확인기관이 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화하여 생성한 정보(CI : Connecting Information)를 말하며, 공단은 연계정보를 개인정보에 포함하여 관리한다. ㊲ "본인확인기관"이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제23조의3에 따라 본인확인기관으로 지정받은 자를 말한다. ㊳ "연계정보 처리시스템"이란 본인확인기관으로부터 연계정보를 제공받아 처리하는 홈페이지 회원가입 본인인증 연동 기능 등 정보시스템을 말한다. ㊴ "연계정보취급자"란 연계정보 처리시스템의 운영·관리 업무를 수행하는 개인정보취급자(수탁자의 직원을 포함한다)를 말한다.
제3조 적용 범위 ① (생 략) <신 설>	**제3조 적용 범위** - 연계정보 적용 명시 ① (현행과 같음) ② 본 계획은 공단이 본인확인기관으로부터 제공받아 처리하는 연계정보에 대해서도 적용한다.
제25조 개인정보 유출사고 대응 계획 수립·시행 ① 1. 개인정보 침해 분류 1등급 개인정보 항목 : 주민등록, 여권번호, 외국인등록번호, 운전면허번호, 계좌번호, 아이디, 비밀번호	**제25조 개인정보 유출사고 대응 계획 수립·시행** - 영향도 등급 보완 ① 1. 개인정보 침해 분류 1등급 개인정보 항목 : 주민등록, 여권번호, 외국인등록번호, 운전면허번호, 계좌번호, 아이디, 비밀번호, **연계정보(CI)**
<신 설>	**[제10장 신설 - 연계정보의 안전조치]** **제10장 연계정보의 안전조치** **제42조 연계정보 보호책임자 지정 등** ① 공단은 정보통신망법 제23조의6 및 「연계정보 생성·처리 등에 관한 기준」 제11조에 따라 연계정보의 안전조치를 총괄하는 연계정보 보호책임자로 제9조에 따른 개인정보 보호책임자(본부장)를 지정한다.

현 행	개 정 안
	② 연계정보 보호책임자를 보좌하여 연계정보 안전조치 실무를 담당하는 연계정보 보호담당자는 개인정보 보호담당자로 한다. ③ 연계정보 보호책임자는 다음 각 호의 업무를 수행한다. 1. 연계정보 안전조치에 관한 내부 규정의 수립·시행 및 개정 2. 연계정보취급자의 지정·관리 및 교육 3. 연계정보 처리 실태의 정기 점검(연 1회 이상) 및 개선 4. 연계정보 침해사고 대응 계획의 수립·시행 5. 연계정보 수집 근거 및 현황의 기록·보관 관리 6. 그 밖에 연계정보의 안전한 처리를 위하여 필요한 사항 **제43조 연계정보의 취급·관리 절차** ① 공단은 홈페이지 회원가입 시 휴대폰 본인인증 과정에서 본인확인기관으로부터 연계정보를 제공받을 수 있으며, 연계정보를 목적 외로 이용하거나 제3자에게 제공하지 아니한다. ② 공단은 본인인증 과정에서 연계정보가 제공되는 경우에도 이를 이용하지 아니하며, 데이터베이스·로그·파일 등에 저장하지 아니한다. ③ 연계정보 처리시스템을 변경하여 연계정보를 저장하려는 경우에는 사전에 연계정보 보호책임자의 승인을 받아야 하며, 저장 전에 제44조 및 제45조에 따른 안전조치를 적용하여야 한다. ④ 연계정보 보호책임자는 연계정보 처리시스템을 운영·관리하는 연계정보취급자를 업무상 필요한 최소한의 인원으로 지정하고, 「연계정보취급자 지정 현황」(붙임 23)으로 관리하여야 한다. ⑤ 연계정보 처리시스템에 대한 접근권한의 신청·승인·변경·말소는 제16조 및 「개인정보처리시스템 접근권한 관리 지침」에 따르며, 퇴직·전보 등으로 업무가 변경된 경우 지체 없이 권한을 말소하고 그 내역을 기록하여야 한다. ⑥ 연계정보 보호담당자는 분기 1회 이상 연계정보취급자 목록과 담당업무의 적정성을 검토하고 그 결과를 기록하여야 한다. ⑦ 연계정보 보호책임자는 연계정보취급자를 대상으로 연 1회 이상 연계정보의 안전한 처리에 관한 교육을 실시하여야 하며, 제4장에 따른 개인정보 보호교육에 연계정보 관련 내용을 포함하여 실시할 수 있다. **제44조 주민등록번호와 연계정보의 분리 보관** ① 공단은 법령에 근거가 있는 경우를 제외하고는 정보주체의 주민등록번호

현 행	개 정 안
	를 수집·보관하지 아니한다. ② 제43조제3항에 따라 연계정보를 저장하는 경우로서 법령에 따라 주민등록번호를 보관하는 경우에는 비인가자의 접근 등에 의해 연계정보와 주민등록번호가 함께 유출되지 않도록 다음 각 호의 어느 하나의 방법으로 분리하여 보관·관리하여야 한다. 1. 물리적 분리 : 서버 또는 DBMS를 달리하여 보관 2. 논리적 분리 : DBMS의 인스턴스 또는 테이블을 달리하여 보관하고, 각각에 대한 접근권한을 업무 특성에 따라 최소한으로 차등 부여 **제45조 연계정보의 안전한 저장·전송** ① 연계정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 SSL/TLS 등 안전한 암호 알고리즘을 적용한 보안 기술을 사용하여 암호화하여야 한다. ② 제43조제3항에 따라 연계정보를 저장하는 경우에는 안전한 암호 알고리즘으로 암호화하여 저장하여야 하며, 연계정보 처리 과정에서 로그 형태로 저장되는 연계정보도 또한 같다. ③ 제2항에 따른 암호화에 사용하는 암호 키의 생성·이용·보관·배포 및 파기는 제18조제6항에 따른 절차를 준용한다. ④ 연계정보는 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장하여서는 아니 된다. **제46조 연계정보 유출·도난 방지를 위한 취약점 점검** ① 연계정보 보호책임자는 연계정보의 유출·도난을 방지하기 위하여 연 1회 이상 연계정보 처리시스템(홈페이지 본인인증 연동 기능 등)에 대한 보안 취약점 점검을 실시하여야 한다. ② 제1항의 취약점 점검은 제23조에 따른 취약점 점검 및 웹 취약점 진단과 병행하여 실시할 수 있으며, 점검 결과 발견된 취약점은 지체 없이 조치하고 그 결과를 기록·보관하여야 한다. **제47조 연계정보 침해사고 대응** ① 공단은 연계정보의 수집 출처, 처리 목적, 처리 방법, 이용·보유 여부(이용·저장하지 않음) 및 안전조치 등 연계정보 처리에 관한 사항을 개인정보 처리방침에 포함하여 인터넷 홈페이지에 공개하여야 한다. ② 연계정보 침해사고의 접수 및 처리는 다음 각 호에 따른다. 1. 접수 창구 : 개인정보 고충처리부서(혁신성과팀) 유선·방문, 공단 홈페

현 행	개 정 안
	이지 민원 센터, 전자우편 2. 대응 절차 : 사고 접수·인지 → 연계정보 보호책임자 보고 → 피해 확산 방지(접근 차단, 계정 잠금 등) → 원인 분석 및 증거 보존 → 정보주체 통지 및 관계 법령에 따른 신고 → 피해 복구 및 재발방지 대책 수립 3. 대응 담당 : 연계정보 보호책임자(총괄), 연계정보 보호담당자(실무), 분야별 책임자 및 수탁자(협조) 4. 그 밖의 세부 절차는 제25조 및 「개인정보 침해·유출사고 대응 지침」을 준용한다. ③ 정보주체는 연계정보 이용내역 등 연계정보 처리에 관한 사항의 열람, 정정·삭제, 처리정지, 동의 철회를 요구할 수 있으며, 공단은 개인정보 처리 방침 제11조 및 「개인정보 정보주체 권리행사 절차서」에 따라 지체 없이 처리한다. 이 경우 요구 방법과 절차는 연계정보 수집 방법과 절차보다 어렵지 않도록 하여야 한다. **제48조 연계정보 수집 현황의 기록·보관 및 실태점검** ① 연계정보 보호담당자는 연계정보 수집의 근거 및 현황을 확인할 수 있도록 다음 각 호의 사항을 분기별로 「연계정보 수집 현황 기록대장」에 기록하여야 한다. 이 경우 연계정보 값 자체는 기록하지 아니한다. 1. 수집 출처(연계정보를 제공한 본인확인기관의 명칭) 2. 수집 시기(본인인증 기간 및 건수) 3. 수집 목적 4. 수집 대상(본인인증을 거쳐 가입한 회원) 및 건별 세부 기록 위치 ② 건별 세부 기록은 홈페이지 회원 데이터베이스의 본인인증 이력(본인인증 일시·회원번호)으로 갈음하며, 제1항의 기록대장은 1년 이상 보관하여야 한다. 이 경우 해당 기록은 제30조 및 「재해·재난 대비 개인정보처리 시스템 위기 대응 지침」에 따른 정기 백업 대상에 포함하여 관리한다. ③ 연계정보 보호책임자는 연계정보가 이 장에 따라 안전하게 처리되고 있는지 연 1회 이상 실태점검을 실시하고, 점검 결과 미흡사항은 개선 조치하여야 한다.

현 행	개 정 안
제10장 그 밖에 개인정보 보호를 위하여 필요한 사항 제42조 개인정보보호 자체점검 주기 및 절차 제43조 자체점검 결과 관리 제44조 타 법령과의 관계	**제11장 그 밖에 개인정보 보호를 위하여 필요한 사항** - 조문 이동 **제49조** 개인정보보호 자체점검 주기 및 절차 **제50조** 자체점검 결과 관리 **제51조** 타 법령과의 관계
제42조 개인정보보호 자체점검 주기 및 절차 ① (점검 분류표) … 영상정보처리시스템 / 운영부서 주관으로 점검 실시 / 연1회 <신 설>	**제49조 개인정보보호 자체점검 주기 및 절차** - 점검항목 추가 ① (현행과 같음) 연계정보 처리실태 점검 / 「연계정보 생성·처리 등에 관한 기준」 [별표4]에 따른 연계정보 안전조치 이행 여부 점검 / 연1회
제44조 타 법령과의 관계 ① 1. ~ 4. (생 략) <신 설>	**제51조 타 법령과의 관계** - 관계 법령 추가 ① 1. ~ 4. (현행과 같음) 5. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 같은 법 시행령 6. 「연계정보 생성·처리 등에 관한 기준」
[붙임 21] 개인정보 침해신고 처리대장 <신 설>	[붙임 21] (현행과 같음) **[붙임 22] 연계정보 수집 현황 기록대장** **[붙임 23] 연계정보취급자 지정 현황**