2024
-08

내/외부 정책자료

분석 보고서

대표이사: 선영주

한라 KPC 漢拏

목차

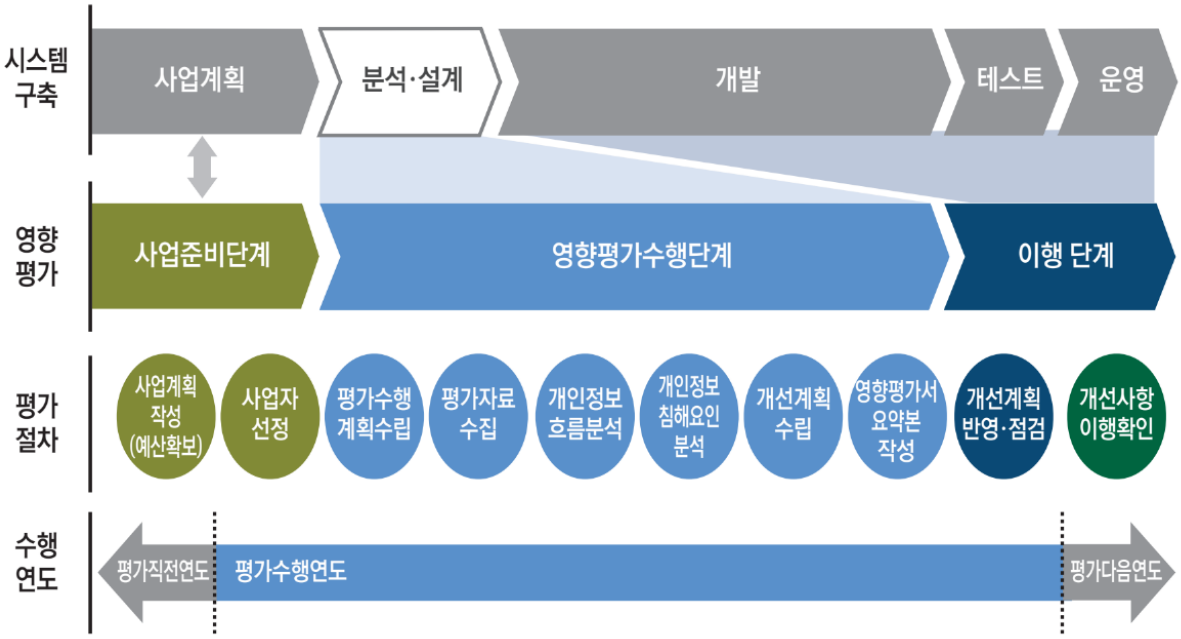
1 서론

1.1. 분석 배경 및 목적

본 보고서는 컨설팅 요구사항 2번(개인정보 영향평가)에 대해 '평가자료 수집' 절차를 진행하는 과정에서, 도로교통혁신안전센터(이하 '기관') 내부의 개인정보 보호 체계 및 관련 규정의 적절한 마련과 이행 여부를 평가하기 위한 기반으로서 작성되었다. 개인정보 보호는 법적 준수의 측면뿐만 아니라, 기관의 신뢰성과 정보 보안의 핵심 요소로서 개인정보 유출 및 오남용과 같은 잠재적 위험을 사전에 방지하는 데 매우 중요하다.

따라서, 본 분석과 분석 보고서 산출의 주요 목적은 기관 내부의 개인정보보호 정책과 정보보안 규정, 그리고 개인정보 취급자 및 관련자에 대한 관리 체계를 종합적으로 검토하여, 개인정보 보호 수준을 객관적으로 평가하는 것에 있다. 이 과정에서 기관이 개인정보를 안전하게 관리하고 보호할 수 있는 체계를 충분히 갖추고 있는지 확인하고, 법적 준수 여부와 보안 강화 필요성을 평가하여 필요한 개선 방안을 제시하는 업무의 초석을 다지고자 한다.

이를 통해, 기관은 개인정보보호 관련 법규를 철저히 준수할 수 있을 뿐만 아니라, 정보보안 강화를 통해 보다 안전한 개인정보 관리 환경을 구축할 수 있을 것으로 기대된다.



[그림 1] 개인정보영향평가 시기 및 절차 (출처: KISA 개인정보 영향평가 수행안내서)

1.2. 분석 범위 및 대상

본 보고서에서 다르는 분석 범위 및 대상의 경우 기관 내 개인정보보호 규정 및 직제표 등이 있으며, 그 상세는 아래 표와 같다.

개인정보보호	개인정보보안 및 정보보안 자체교육 계획
	개인정보 사고대응 메뉴얼
	개인정보 제3자 제공 동의서
	개인정보 제공 및 고유식별정보 처리 동의서
	개인정보 관리방침
	개인정보시스템 보안 지침
	개인정보 열람/정정/삭제 처리요구서
	개인정보 흐름도
	개인정보 흐름표
	개인정보 파기 지침
	개인정보처리시스템 위기대응 절차 및 백업 복구 계획

관리보안	외부 용역 보안서약서
	입사자 비밀유지 서약서
	재직자 비밀유지 서약서
	퇴사자 비밀유지 서약서
	외부 용역 채용공고 및 응시원서
내부 및 물리보안	USB 메모리 등 휴대용 저장매체 보안관리지침
	기록물 관리지침
	보안 내부감사 시행계획 기술서
	실시간 보안 모니터링 절차 기술서
	영상정보처리기기 운영 및 관리 방침
	전산장비 및 휴대용 저장매체 반출입 대장
	정보보호조치에 관한 지침
	CCTV 안내문 및 사내 설계도면
	문서생명주기 기술서
	영상물 요청서
	교통신호제어기 이력카드
	영상정보 관리대장
	외부 방문자 출입관리대장
	출입카드 발급대장
기술보안	네트워크 보안지침
	데이터베이스 보안관리지침
	데이터베이스 운전 및 교육 구조도

[표 1] 내부 정책자료 분석 범위 및 대상

(참고: 도로교통혁신안전센터 증적자료)

2 기관 내부 정책 및 규정 현황 분석

2.1. 개인정보보호 체계 및 규정 분석

본 목차에서는 개인정보보호와 관련된 체계에 대한 상세 규정 분석에 대한 내용을 다룬다. 분석 내역 중 핵심적인 내용의 경우 다음과 같다.

2.1.1. 개인정보 및 정보보안 관련 자체교육

도로교통혁신안전센터의 경우, 정보보호 중요성에 대한 인식 제고 및 보안사고 예방을 목적으로 하는 교육 추진 계획에 대한 문서를 관리하고 있다. 해당 체계는 개인정보보호법 제28조(개인정보취급자에 대한 감독) 중 '개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.'라는 조항에 근거를 두고 있으며, 하단의 방침을 따른다.

◦ (맞춤형 교육) 교육대상자별 교육 운영으로 효과성 제고

* 개인정보 보호담당자, 취급자/직원, 수탁자 등

◦ (교육자료 공유) 콘텐츠 최신화 및 실시간 공유로 교육 내실화

* 법령·지침 등 개정사항, 유·노출 사례 등 최신화·공유

◦(지정강사* 운영) 개인정보보호 교육인프라 강화로 전문성 향상

* 지정강사: 기관 내 상시 교육기반 운영, 개인정보보호 분야 상담자 역할수행

교육 현황 및 주요 성과 결과는 다음과 같으며, 올해 교육 의무기준 대비 목표를 달성한 상태이다. 본 기관에서는 직급 및 역할에 따라 교육 횟수를 달리 지정하고 있으며, 이를 통한 전 이해관계 직원들의 정보보호 의식제고 문화 확산을 기대하고 있다.

대상	교육 횟수	비고
개인정보보호 책임자	2	연 1회 이상
개인정보보호 취급자, 신규 직원	12	-

개인정보보호 총괄 담당자	4	연 2회 이상
수탁자	4	반기 1회 이상

[표 2] 대상별 정보보안 교육 현황

(출처: 도로교통혁신안전센터_개인정보 및 정보보안 자체교육 계획서)

교육은 부분 실시간 온라인 형식(온라인 강의, PC 영상회의)으로 진행되었으며, 신규 임용직원 19명을 대상으로 총 6회의 개인정보 및 정보보안 교육이 진행된 상태임이 확인되었다.

또한 매 교육에서의 미흡 및 보완사항에 대한 검토도 이루어지고 있으며, 이에 대한 개선 방침에 대한 논의도 진행되고 있다. 기존 개인정보보호 교육 이수시간 및 횟수 달성 등 형식적인 면모에 치중했던 측면을 개선하고자 하고 있으며, 정보보호 인식 제고를 위해 보다 더 다양화된 교육 훈련(세미나 참석 등)의 필요성을 인지하고 있는 상태로 파악된다.

교육 대상별 맞춤형 교육의 세부 추진 계획 및 상세 내역은 다음과 같다.

구분	대상	교육 과정 및 내용	교육 이수 횟수
개인정보보호 책임자	CPO	고급과정	연 1회 이상
	분야별 부서장	온라인 또는 직장교육	연 1회 이상
개인정보보호 담당자	총괄 담당자	공공기관 및 초/중급과정	연 2회 이상
	부서 담당자	온라인 또는 직장교육	연 1회 이상
개인정보 취급자	전 직원	외부강사, 온라인, 직장교육	연 1회 이상
	신규 직원	직장교육	수시
개인정보 수탁자	용역업체 직원	직장교육 또는 관련기관 방문	반기 1회

[표 3] 교육 대상별 교육 상세 현황

(출처: 도로교통혁신안전센터_개인정보 및 정보보안 자체교육 계획서)

◦ (책임자 교육) 관리자의 관심·역량 강화

- 개인정보보호책임자(CPO) : 책임자 대상 고급과정 이수(연 1회 이상)

- 분야별 책임자(부서장) : 온라인 또는 직장교육 이수(연 1회 이상)

◦ (담당자 교육) 개인정보 보호담당자의 역량 및 전문성 향상

- 총괄 담당자 : 외부 전문교육, 본청 주관 직장교육 이수(연 2회 이상)

- 부서 담당자 : 온라인 또는 직장교육 이수(연 1회 이상)

◦ (취급자 교육) 개인정보 취급 기본 규정 숙지

- 외부강사(본청 포함) 초청 개인정보 및 정보보안 집합 교육(5~6월 중)

- 개인정보보호 및 정보보안 교육 이수(연 1회 이상)

- 신규 임용·복직·타 부처 전입직원 등 수시·집중 교육

◦ (수탁자) 용역사업 참여직원에 대한 정기 교육

- 자체 교육실시 또는 외부 전문기관 교육수료 독려(반기 1회 이상)

* 업체직원이 교체되는 경우 업무 투입 전 정보보호 교육(수시)

2024년 기관이 따르는 개인정보보호위원회 주관 개인정보보호 교육 일정과 지정강사 등 체계 전반에 대한 사항은 다음 표와 같다. 단, 1-1 등과 같은 주요 추진 과제에 대한 개괄은 도로교통혁신안전센터의 '개인정보 및 정보보안 자체교육 계획' 문서에 첨부된 붙임에 따른다.

추진 과제	1/4 분기			2/4 분기			3/4 분기			4/4 분기		
	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
1. 개인정보처리자 실무 역량 제고												
1-1												
1-2												
1-3												
1-4												
1-5												
2. 정보취약계층 교육 확대												
2-1												
2-2												
2-3												

3. 개인정보 전문인력 양성 강화												
3-1												
3-1-1												
3-1-2												
3-2												
3-3												
4. 민관 협업형 개인정보 교육 강화												
4-1												
4-2												
4-3												
5. 개인정보보호 교육방식 전환												
5-1												
5-2												
5-3												

[표 4] 개인정보보호위원회 주관 개인정보보호 교육 일정

(참고: 개인정보보호위원회 & 개인정보배움터)

2.1.2. 개인정보 유출 대응 체계

본 기관에서는 개인정보처리자 등이 처리하고 있는 개인정보가 분실 도난 유출 사고가 발생할 경우, 이에 대한 신속한 대응 및 조치를 통한 피해확산 방지 및 정보주체에 대한 피해구제를 위한 매뉴얼을 수립하여 운용하고 있다.

관련 문서인 '개인정보 유출 대응 메뉴얼'에서의 개인정보의 분실·도난·유출(이하 "유출 등"이라 한다)이란, 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

해당 매뉴얼은 개인정보 유출 등 사고와 관련하여 신속한 대응과 그 피해를 최소화하기 위한 최소한의 사항을 안내하고 있으며, 특히 「개인정보 보호법」 제34조(개인정보 유출 등의 통지·신고)로 변경 및 「신용정보의 이용 촉진 및 보호에 관한 법률」(이하 「신용정보법」이라 한다) 제39조의4(개인신용정보 누설통지 등)에 따라 개인정보보호위원회 또는 한국인터넷진흥원(KISA)에 신고하여야 하는 개인정보 유출 등 사고에 대한 안내를 포함하고 있다.

해당 문서에서 규정된 용어와 그 설명은 다음과 같다.

구분	용어설명
개인정보	살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보 - 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 - 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려해야 함 - 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보
개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인
유출	법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것
유출사고 대응팀	개인정보 유출사고 발생에 따른 사고의 분석, 처리지원, 사후 복구, 사후 예방조치 등을 주요 업무로 하는 개인정보보호 담당부서
개인정보 보호책임자	개인정보 보호법 제31조에 근거하여 개인정보 처리 업무를 총괄하는 자로, 개인정보 보호담당자를 임명하여 유출사고 발생 시 본 절차에 따라 대응토록 함
개인정보 보호담당자	개인정보 보호책임자의 지정을 받아 개인정보 보호업무를 수행하는 자

[표 5] 개인정보 유출 대응 메뉴얼 용어 정리
(출처: 도로교통혁신안전센터 개인정보 유출 대응 메뉴얼)

또한 본 기관에서는 "개인정보 유출 등 사고 신속대응팀"(가칭)을 운영하여 개인정보 유출 사고 발생에 따른 사고 분석, 처리, 사후 복구 및 예방 조치 등을 수행하고 있다. 이어 개인정보 보호책임자를 중심으로 내부 조직 및 인력을 효율적으로 분배하여 유출 원인분석 및 대응, 유출 등 신고·통지, 이용자 피해구제 등 고객지원 등으로 세분화하여 신속히 대응하는 체계를 수립하여 운용 중이다.

개인정보 보호 책임자(CPO)는 개인정보보호 업무를 총괄하며, 개인정보파일의 등록, 파기, 관리 감독과 관련 지침의 제·개정을 담당한다. 신속대응팀장은 CPO를 보좌하고, 개인정보보호 계획의 작성 및 추진, 파일 등록·변경·파기, 교육, 보호 업무, 부서 점검을 담당한다. 개인정보 유출 부서장은 신속대응팀장을 보좌하며 교육, 기록 관리, 위탁 업무의 관리·감독을 수행한다. 개인정보 분야별 책임자는 보호 계획의 수립·시행, 실태 점검, 통계 자료 취합, 시스템 보호 장치 강화 및 CPO에게 보고한다. 개인정보 담당자/취급자는 파일 관리, 처리 절차 준수, 안전 조치와 관리 업무를 수행하는 체계로 구성되어 있음을 확인하였다.

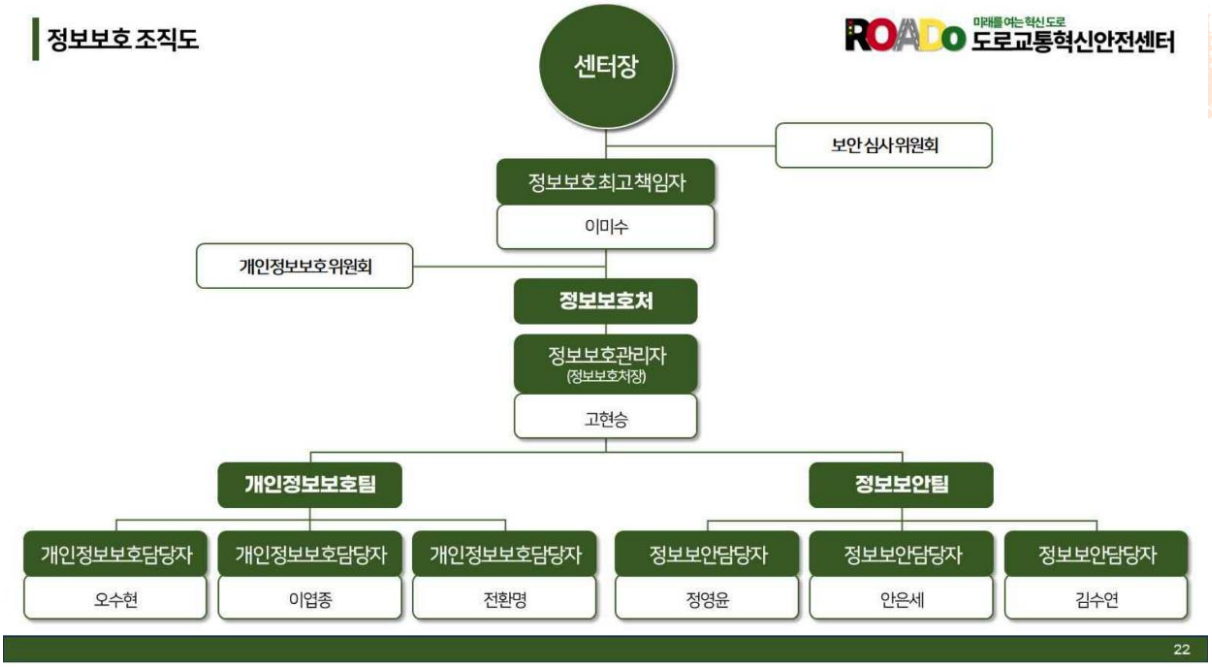
단계별 절차의 경우, '사고 인지 긴급 조치'를 시작으로 '정보주체 유출 통지', '개인정보 유출 신고', '사고분석', '민원대응', '유출사고 결과보고', '개선 및 이행점검'으로 이루어진다. 각 절차별 상세 수행 내역과 담당자를 명시하였으며, 주요 내용은 다음 자료와 같다.

단계	주요 내용	담당자
사고 인지 긴급 조치	• 개인정보 유출 사고 인지 및 신고 접수 • 개인정보 보호담당자는 사고 내용 등에 대해 개인정보 보호책임자에게 보고 • 개인정보 유출 신고 등 사고 신속 대응팀 구성 • 피해 최소화를 위한 긴급 조치 수행	개인정보담당자, 정보보호담당자
정보주체 유출 통지	• 1건이라도 개인정보 유출 시, 정보주체에게 유출사실 통지 (72시간 이내)	정보보호관리자, 개인정보보호 담당자

개인정보 유출신고	• 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우, 민감정보 또는 고유식별정보가 유출된 경우 • 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우	정보보호관리자, 개인정보보호 담당자
사고분석	• 개인정보 유출 신고 등 사고 신속 대응팀의 조사 및 분석	정보보호관리자, 개인정보보호 담당자
민원대응	• 민원대응을 위한 별도의 온/오프라인 창구를 개설 및 운영	정보보호관리자, 개인정보보호 담당자
유출사고 결과보고	• 개인정보 유출사고 결과보고서 작성 및 보고	개인정보보호 담당자
개선 및 이행점검	• 개인정보 유출사고 사례 전파 교육 및 개선대책 시행 (재발방지)	개인정보보호 위원회

[표 6] 개인정보 유출 대응 단계별 절차

(출처: 도로교통혁신안전센터 개인정보 유출 대응 메뉴얼)



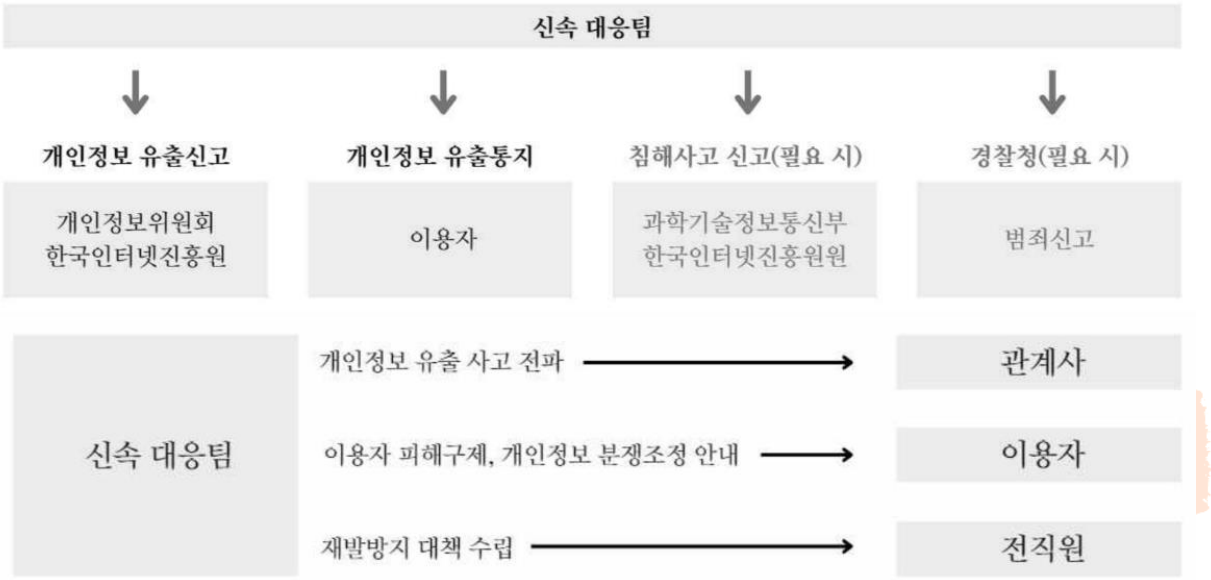
[그림 2] 도로교통혁신안전센터 정보보호 조직도 및 신속대응 체계 모식도

(출처: 도로교통혁신안전센터)

또 피해에 대해 해킹, 내부자 유출 등의 문제 원인별 목차를 나누어 체계적인 긴급 조치가 가능하도록 구상하였다. 이에 대해 피해 최소화 방안 및 피해자 구제절차 등에 대한 내용을 기재하는 '개인정보 유출 신고서' 양식을 활용하고 있다.

2.1.3. 개인정보 관리 체계

본 기관에서는 '개인정보 제3자 제공 동의서', '개인정보 제공 및 고유식별정보처리 동의서', '개인정보 열람/정정/삭제/처리 요구서' 양식을 통해 정보주체의 권리를 보장하고 있다. 개인정보 제3자 제공 동의서의 경우 개인정보가 전달되는 조직명과 활용되는 서비스명, 이용 목적 및 제공되는 정보에 대한 목록을 기재하고 있다. 추가적으로 전달된



개인정보의 보유 및 이용기간과 제공 미동의 시 얻을 수 있는 불이익에 대한 내용도 기재되어 있는 상태이다. 이를 포함, 개인정보 관련 동의서 양식에 포함된 내용 여부는 다음 표와 같다.

기재 정보	문서	
	개인정보 제3자제공 동의서	개인정보 제공 및 고유식별정보 처리 동의서
정보 수집 및 이용 목적	O	O

수집/제공하고자 하는 개인정보 항목	O	O
개인정보 보유 및 이용 기간	O	O
제공 & 처리자 및 조직명	O	X
비동의 시 불이익 사항	O	O
수집 및 제공 근거	O	O

[표 7] 개인정보 연관 동의서 양식별 기재 내용

(출처: 도로교통혁신안전센터 개인정보의 제3자 제공 동의서 외 1)

개인정보의 제3자 제공에 대해 제공 조직은 모두 도로교통혁신안전센터 내 교육 운영처이며, 총 2가지 서비스에 대한 제3자 제공이 이루어지고 있다. 먼저 특별교통안전교육 서비스의 경우, 특별교통안전 교육이수처리를 목적으로 이용된다. 주민등록번호와 성명이 제공되고, 이는 제공받는 측인 경찰청에 영구적으로 보관/이용된다. 만일 제공을 거부할 경우, 교육 이수에 따른 행정처리가 불가함도 함께 안내하고 있다. 반면 고령운전자 안전교육 서비스의 경우, 고령운전자의 교육이수정보를 확인하기 위한 목적으로 경찰청에게 성명과 운전면허번호가 제공된다. 이는 3년간 보관 및 이용되고, 제공을 거부할 경우 교육 이수 및 그에 따른 혜택 수령이 불가함을 안내하고 있다.

도로교통혁신안전센터는 원활한 개인정보 업무처리를 위하여 [표 8]과 같이 개인정보 처리업무를 위탁하고 있으며, 위탁계약 체결 시 「개인정보 보호법」 제26조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 안전성 확보조치, 재위탁 제한, 수탁자에 대한 관리·감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있다. 또 위탁업무 내용이나 수탁자가 변경되었을 경우에는 지체 없이 본 개인정보 처리방침을 통하여 공개하는 것을 원칙으로 하고 있다.

연번	개인정보 처리업무 위탁명	위탁부서	수탁기관	위탁기간
1	본인인증 SMS 서비스	미래교육처	㈜코리아 크레딧뷰로	2023. 9. 2.~ 2024. 9. 1.
2	2023년 도로교통혁신안전센터 온라인 교육	인재개발처	㈜휴넷	2024. 1. 1.~ 2024.12.31.

3	홈페이지 본인인증	ICT 운영처	한국모바일인증㈜	2024. 6. 1.~ 2025. 5.31.
4	2024년 고령운전자 교통안전교육 우편통지 발송 대행	교육운영처	(사)우리들행복나눔 인쇄사업단	2024. 3.26.~ 2024.12.31.

[표 8] 개인정보 처리업무 위수탁 사항

(출처: 도로교통혁신안전센터)

또 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 대해 정보주체는 공단에 대해 언제든지 개인정보 열람·정정·삭제·처리정지 요구 등의 권리를 행사할 수 있으며, 만 14세 미만 아동에 관한 개인정보의 열람등 요구는 법정대리인이 직접 해야 함을 규정하고 있다. 단, 만 14세 이상의 미성년자인 정보주체는 정보주체의 개인정보에 관하여 미성년자 본인이 권리를 행사하거나 법정대리인을 통하여 권리를 행사할 수도 있음을 별도로 기재하고 있다.

권리 행사는 공단에 대해 「개인정보 보호법」 시행령 제41조 제1항에 따라 서면, 전자우편, 모사전송(FAX) 등을 통하여 할 수 있으며, 도로교통혁신안전센터는 이에 대해 지체 없이 조치하고 있다. 또 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 이루어질 수 있으며, 이 경우 "개인정보 처리 방법에 관한 고시(제2020-7호)" 별지 제11호 서식에 따른 위임장을 제출해야 한다. 개인정보 열람 및 처리정지 요구는 「개인정보 보호법」 제35조 제4항, 제37조 제2항에 의하여 정보주체의 권리가 제한될 수 있고, 정정 및 삭제 요구의 경우 기타 법령에서 해당 개인정보가 수집 대상으로 명시되어 있는 경우 그 삭제를 요구할 수 없음을 명시하고 있다. 마지막으로 개인정보 처리에 대한 요구를 한 자가 본인이거나 정당한 대리인인지를 확인하는 별도 절차가 있는 것으로 판단된다.

추가적으로 도로교통혁신안전센터 내 '개인정보 파기 지침'을 제작하여, 개인정보의 파기 및 삭제 계획을 수립하고 실행 중에 있다. 기본적으로 개인정보가 보유기간 만료 등으로 더 이상 그 필요가 없게 된 경우, 정당한 사유가 없는 한 5일 이내 파기하는 것을 원칙으로 한다.

단 『공공기록물 관리에 관한 법률』등 다른 법령에서 보존해야 하는 경우에는 예외로 규정하고 있으며, 불필요하게 된 개인정보를 파기하지 않고 보존하는 경우에는 그

개인정보는 다른 개인정보와 분리하여 저장 . 관리하고 있다. 추가적으로 개인정보보호 분야별 책임관은 개인정보의 보유 기간 만료 등에 따른 구체적 파기 시점 . 방법 등을 반영한 개인정보 파기계획을 수립하고 시행하며, 파기 계획의 경우 개인정보 처리방침에 포함하여 시행 가능함을 규정하였다.

본 기관에서의 개인정보 관련 파일 파기 절차는 다음과 같다. 아래 [그림 3]의 공정을 진행한 뒤, 소속 및 산하기관의 개인정보 보호책임관은 개인정보 파일을 동록하거나 삭제할 때 행정안전부 개인정보 보호책임관에게 개인정보파일 파기결과를 보고해야함을 규정하고 있다.

[그림 3] 개인정보파일 파기 절차 흐름도

(출처: 도로교통혁신안전센터)

개인정보파일 파기 시에는 완전 파괴(소각 및 파쇄), 전용 소자장비 이용, 데이터 덮어쓰기 및 포맷 등의 방법을 사용하고 있다. 만일 개인정보의 전체가 아닌 일부만을 파기하고 위에서 언급된 방법으로의 삭제가 어려운 경우, 파일의 형태에 따라 아래와 같이 처리하고 있다. 파기 업무 내역 및 파기 요청은 각각 '개인정보파일 파기 관리대장'과 '개인정보파일 파기 요청서' 양식에 따라 관리되고 있다.

○ 전자적 파일 형태의 경우: 삭제 후 복구 및 재생되지 않도록 관리.감독

○ 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 해당 부분 마스킹, 천공 등으로 삭제

본 기관에서는 아래 3가지 목적을 위해 개인정보를 수집하고 있으며, 이용 목적이 변경되는 경우에는 개인정보보호법 제18조에 따라 별도의 동의를 받는 등 필요 조치를 이행하고 있다.

① 홈페이지 회원 가입 및 관리

② 운전면허시험 업무 처리

③ 개인정보파일의 등록 및 공개

도로교통혁신안전센터는 법령에 따른 개인정보 보유·이용기간 또는 정보주체로부터 개인정보를 수집 시에 동의 받은 개인정보 보유·이용기간 내에서 개인정보를 처리·보유하고 있으며, 각 파일에 대한 개인정보 항목 & 개인정보 처리 및 보유 기간은 다음과 같다.

번호	개인정보파일명	운영근거	보유기간
1	사용자 정보	도로교통법 제73조 제4항	3년
2	특별교통안전교육 관리	도로교통법 제73조	준영구
3	고령운전자 교통안전교육	도로교통법 제73조 제5항	준영구
4	SMS, E-mail 관리자료	도로교통법 시행령 제87조의3	30년
5	교통안전교육 접수 자료	도로교통법 시행령 제87조의3	준영구
6	국제운전면허발급 처리자 명부	도로교통법 시행령 제87조의3	10년
7	연습운전면허발급 처리자 명부	도로교통법 시행령 제87조의3	10년
8	운전면허 재발급 처리자 명부	도로교통법 시행령 제87조의3	10년
9	운전면허증 취득자 명부	도로교통법 시행령 제87조의3	10년
10	적성검사 안내통지 암호화 연계정보	도로교통법 제123조	10년
11	면허시험 응시내역	도로교통법 시행령 제87조의3	준영구
12	온라인 교통안전교육 회원정보	도로교통법 제73조, 제53조의3	2년
13	직원 인적사항	근로기준법 제41조	영구
14	교통빅데이터 통계정보	도로교통법 제123조	10년

[표 9] 개인정보파일별 처리 및 보유기간

(출처: 개인정보보호위원회, 개인정보 포털_개인정보처리방침)

번호	개인정보파일명	개인정보 항목(필수)
1	사용자 정보	이름, 생년월일, 휴대폰번호, 아이디, 비밀번호, IP주소, 상위기관명, 소속기관명
2	특별교통안전교육 관리	이름, 휴대전화번호, 주민등록번호, 운전면허번호
3	고령운전자 교통안전교육	이름, 생년월일, 주소, 휴대전화번호
4	SMS, E-mail 관리자료	이름, 휴대전화번호, 이메일, 주민등록번호
5	교통안전교육 접수 자료	이름, 주민등록번호
6	국제운전면허발급 처리자 명부	이름, 주소, 주민등록번호, 운전면허번호
7	연습운전면허발급 처리자 명부	이름, 주소, 주민등록번호, 연습면허번호
8	운전면허 재발급 처리자 명부	이름, 주소, 주민등록번호, 운전면허번호
9	운전면허증 취득자 명부	이름, 주소, 주민등록번호, 운전면허번호
10	면허시험 응시내역	이름, 주민등록번호, 장애조건
11	온라인 교통안전교육 회원정보	이름, 생년월일, 휴대전화번호, 아이디, 성별, 교육이수번호
12	직원 인적사항	이름, 주민등록번호, 주소, 휴대전화번호, 이메일, 임용일, 진급일, 현부서 이동일, 사진, 사번, 성별, 연령, 부서, 직종, 직급, 근무이력, 학력, 경력, 담당업무
13	교통빅데이터 통계정보	<필수항목 없음>

[표 10] 개인정보파일별 처리 및 보유기간

(출처: 도로교통혁신안전센터_개인정보관리방침)

2.1.4. 개인정보 영향평가 & 개인정보 보호수준 평가

본 센터는 운영하고 있는 개인정보 처리시스템이 정보주체의 개인정보파일에 미칠 영향에 대해 조사, 분석, 평가하기 위해 「개인정보 보호법」제33조에 따라 2023년도 개인정보 영향평가를 수행하였다. 이름, 생년월일, 집주소, 연락처, 주민등록번호, 운전면허번호를 포함한 '특별교통안전교육관리 고령운전자 교통안전교육' 개인정보파일이

그 대상이였으며, 2024년 현재 동종업계 내 개인정보 사고에 대한 개인정보 관리체계 변경이 이루어지면서 새로히 개인정보 영향평가를 진행할 계획이다.

본 센터에서는 정보주체의 개인정보를 안전하게 관리하기 위해 「개인정보보호법」 제11조의2에 따라 매년 개인정보보호위원회에서 실시하는 "개인정보 보호수준 평가"를 받고 있음이 확인되었다. 최근 2022, 2023년 각각에 대해 A등급을 획득하였으며, 2023년도 평가 이후 개인정보 처리절차가 일부 개선되었다.

2.1.5. 개인정보의 안전성 확보조치

본 센터는 「개인정보보호법」 제29조에 따라 안전성 확보에 필요한 기술적, 관리적, 물리적 조치를 수행하고 있으며, 그 목록은 다음과 같다.

① 내부관리계획의 수립 및 시행

② 개인정보 취급 직원의 최소화 및 교육

③ 정기적인 자체 감사 실시

④ 개인정보의 암호화

⑤ 해킹 등에 대비한 기술적 대책

⑥ 개인정보에 대한 접근 제한

⑦ 접속기록의 보관 및 위변조 방지

⑧ 문서보안을 위한 잠금장치 사용

⑨ 비인가자에 대한 출입 통제

2.1.6. 개인정보 암호화 조치

본 센터에서는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통해 송신하거나, 보조저장매체 등을 통해 전달하는 경우 반드시 암호화하고 있으며, 비밀번호는 일방향 암호화(해쉬함수)를 통해 복호화되지 않도록 저장하고 있다. 암호화 절차는 다음과 같다.

① 내부관리계획의 수립 및 시행

② 개인정보 취급 직원의 최소화 및 교육

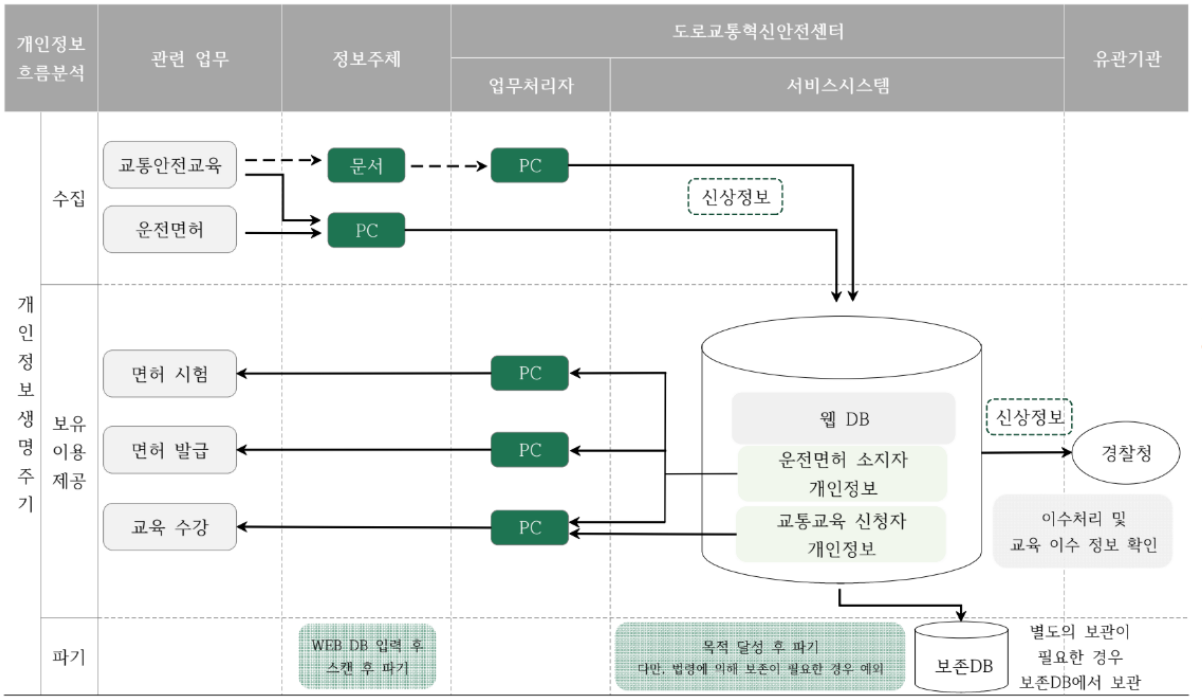
③ 정기적인 자체 감사 실시

④ 개인정보의 암호화

2.1.7. 개인정보 흐름

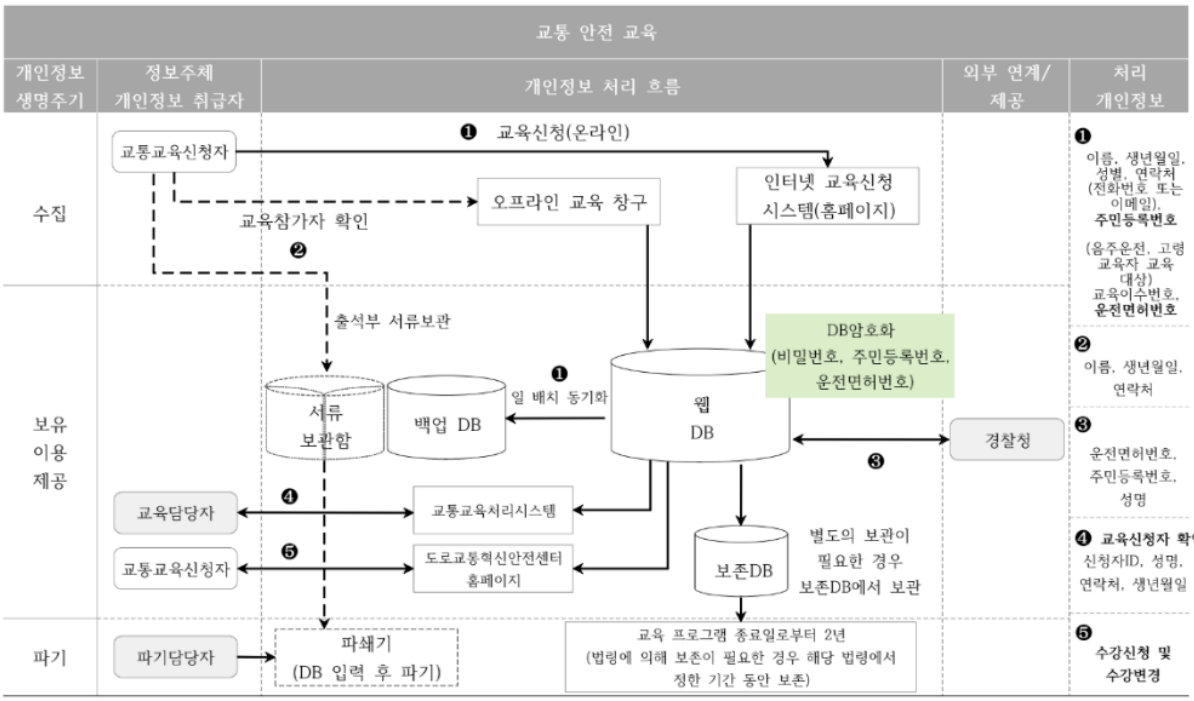
본 센터는 운전 면허 시험 및 발급 & 재발급 서비스와 교통 안전 교육 서비스를 포함한 전체 업무에 대해 각각의 개인정보 흐름을 다루고 있다. 운전면허 관련 업무에서 다루는 개인정보 주체는 약 3700만명이며, 교통교육 업무에서 활용되는 개인정보 주체는 약 1000만명으로 파악된다.

모든 서비스는 개인정보 생명주기에 따라 수집, 보유/이용/제공, 그리고 파기 과정을 거치며, 그 상세는 아래 3가지 도식과 같다.



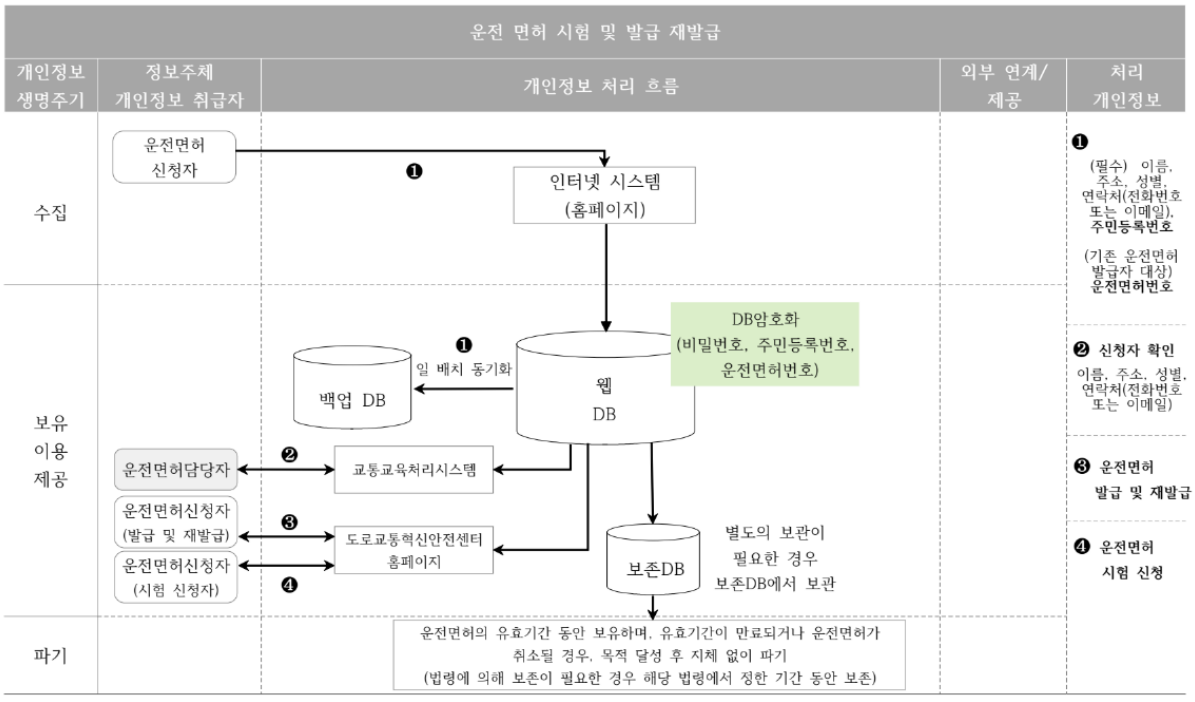
[그림 4] 전 서비스에 대한 개인정보흐름도

(출처: 도로교통혁신안전센터)



[그림 5] 교통 안전 교육 서비스에 대한 개인정보흐름도

(출처: 도로교통혁신안전센터)



[그림 6] 교통 안전 교육 서비스에 대한 개인정보흐름도

(출처: 도로교통혁신안전센터)

운전면허와 교통교육 관련 개인정보 흐름의 경우는 다음과 같다.

○ 수집

운전면허 발급 및 시험 신청자를 대상으로 이름, 주소, 성별, 연락처(전화번호 또는 이메일), 주민등록번호(기존 운전면허 발급자 대상), 운전면허번호 등을 온라인 홈페이지에서 수집한다. 수집 근거는 이용자 동의와 도로교통법 제87조의3에 존재한다.

○ 보유·이용

수집된 정보는 Web DB에 암호화된 형태로 보유되며, 주민등록번호, 운전면허번호, 비밀번호(일방향) 등이 포함된다. 이는 운전면허와 국제운전면허의 발급, 갱신 및 관리, 운전능력 평가(적성검사) 및 인증, 운전면허 취득에 관한 서비스 제공을 위해 이용된다.

○ 제공

현재 운전면허 관련 개인정보는 외부로 제공되지 않고 있는 상태로 파악된다.

○ 파기

개인정보들은 운전면허의 유효기간 동안 보관되며, 유효기간이 만료되거나 운전면허가 취소될 경우 목적 달성 후 지체 없이 파기된다. 법령에 의해 보존이 필요할 경우, 해당 법령에서 정한 기간 동안 보존하고, 파기는 일단위로 DB 관리자가 수행하는 체계이다.

교통교육 서비스의 경우, 아래와 같은 개인정보 흐름을 가진다.

○ 수집

교통교육 신청자 및 교육 참석자를 대상으로, 이름, 생년월일, 성별, 연락처(전화번호 또는 이메일), 주민등록번호(음주운전, 고령 교육자 대상), 교육이수번호, 운전면허번호 등을 온라인(홈페이지) 및 오프라인(교육 참석자 명단)에서 수집한다. 수집 근거는 이용자 동의와 도로교통법 제87조의3에 존재한다.

○ 보유·이용

수집된 정보는 Web DB에 암호화된 형태로 보유되며, 주민등록번호, 운전면허번호, 비밀번호(일방향) 등이 포함된다. 이를 교육 콘텐츠 제공 및 교육 신청 관리, 교육 이수 확인, 교육 관련 정보 제공, 교육 서비스 개선을 위한 통계 분석 및 설문 조사, 기타 교육 관련 행정업무 처리를 위해 이용하고 있다.

○ 제공

교통교육 이수처리 및 교육이수 정보 확인을 위해 도로교통혁신안전센터 교육운영처에서 경찰청으로 운전면허번호, 주민등록번호, 성명을 실시간 DB 연동 방식으로 제공하고 있다. 통신 구간은 암호화되며, 제공 근거는 개인정보 보호법 제17조 및 제18조에 존재한다.

○ 파기

관련 정보는 교육 프로그램 종료일로부터 2년 동안 보유하며, 이후에는 목적 달성 후 지체 없이 파기된다. 파기는 일단위로 DB 관리자에 의해 DB에서 이루어지며, 오프라인 자료는 주단위로 교육 담당자가 문서 절단 방식으로 파기하고 있다.

2.1.8. 개인정보시스템 위기대응 절차 및 백업 복구 계획

본 센터에서는 최근 지진, 화재 등 재해 . 재난 대응의 중요성이 높아짐에 따라 개인정보처리시스템 보호를 위한 위기대응 체계 수립하였고, 재해 . 재난 발생 시 개인정보처리시스템의 신속한 복구와 원활한 업무 관리의 재개를 위해 관련 절차 등의 대책을 지원하고 있다.

재해/재난 발생 시 개인정보처리시스템 위기대응 절차 및 백업/복구 계획 매뉴얼에서 정의한 재해·재난 발생 시, 개인정보처리시스템의 운영 및 관리에 한해서만 적용된다. 또 개인정보처리시스템 위기 상황 해제 시 까지 개인정보처리시스템의 운영에 필요한 모든 행동요령을 포함한 문서('재해/재난 발생 시 개인정보처리시스템 위기대응 절차 및 백업/복구 계획')를 생성하며 관리 중에 있다.

단, 재단 자체 운영 중인 개인정보처리시스템을 제외한 정부통합전산센터를 통해 개인정보처리시스템을 운영할 경우, 정부통합전산센터의 대응 절차 및 매뉴얼을 우선 적용하고 있다.

용어 정의 상세는 다음과 같다.

○ 재해·재난: 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고

○ 개인정보처리시스템 위기: 개인정보처리시스템이 장애로 인해 가동이 전면 중단되거나 중단 가능한 시간을 초과하는 경우

○ 재해복구시스템: 재해·재난 발생 시 데이터를 보존하고 자동 복구하는 장치

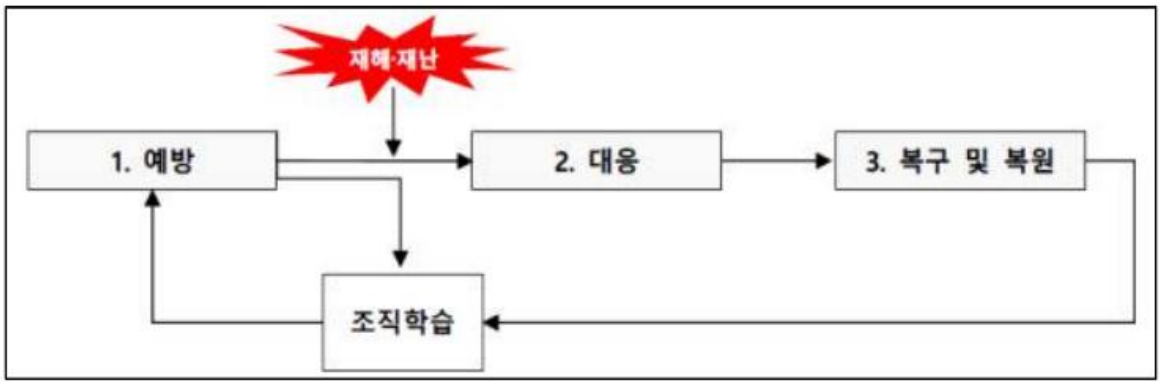
○ 백업: 잘못되거나 부주의한 조작으로 인하여 데이터가 손실될 것에 대비하여 미리 남겨둔 복사본

위기 대응 절차는 크게 예방, 대응, 복구 및 복원의 세 단계로 이루어진다.

먼저 1단계인 예방 단계에서는 위기상황이 발생하기 전에 예상되는 문제들을 미리 보완하고 대비한다. 이를 위해 위기대응 조직, 위기등급, 복구목표 등 위기대응 체계를 검토하고, 주기적으로 백업을 실시하며 위기대응 훈련을 통해 준비 상태를 유지하고 있다.

다음으로, 2단계인 대응 단계에서는 재해나 재난으로 위기상황이 발생하면, 위기대응 체계에 따라 즉시 대응이 이루어진다. 이때, 위기대응 조직을 소집하고 위기등급을 정의하여 위기상황을 선포하고, 비상연락체계를 가동하며 각 조직의 역할에 따라 대응한다. 초기 대응 단계에서는 위기징후를 자체적으로 인지하거나 직원, 관련업체, 유관기관 등으로부터 통보를 받아 파악하며, 기업지원팀이 위기상황을 접수하고 사고발생지역, 발생기간, 발생원인, 피해상황 등을 확인한다. 이후 접수된 관련 동향을 종합적으로 분석하여 피해 규모를 확인하고 재단 차원의 대응방안을 강구한다. 위기경보가 발령되면, 각 부서와 유관기관에 이를 전파하고, 피해상황별 초기 대응활동을 전개하며 개인정보 유출, 손실, 훼손 등의 파급효과를 고려하여 대응하는 절차를 거친다.

마지막으로, 3단계인 복구 및 복원 단계에서는 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원을 실시한다. 복구 및 복원이 완료되면 위기상황 종료를 선언하고, 대응 과정에서 발생한 이슈를 위기대응 체계에 반영하여 개선한다. 또한, 위기상황으로 인한 피해를 수습하고 발생한 위기내용을 학습하여 향후 대응에 반영하고 있다.



[그림 7] 위기 대응 단계 순서도

(출처: 도로교통혁신안전센터)

시스템 백업의 경우, 개인정보처리시스템 담당자는 신속한 업무 복구를 위해 백업대상을 선정하고 필요한 내용을 주기적으로 백업하고 있다. 백업 대상은 DB, 개발소스 및 메일 데이터, 로그, 서버OS 등 중요도가 높다고 판단되는 데이터이다. 개인정보처리시스템 담당자는 안전한 백업매체를 선정하고 백업의 주기 및 소산 유무를 결정해야 하고, 백업매체는 비인가자가 접근할 수 없는 격리 된 곳에 보관하여 비인가자에 의한 백업정보 유출이 일어나지 않도록 하고 있다.

이 외에도 위기 발생 시 피해 최소화 및 신속한 복구를 위해 연 1회 이상 위기대응 훈련을 실히하고 있으며, 비상연락망을 구성하고 있다.

2.1.9. 기타 사항

본 센터는 '개인정보 자동 수집장치의 설치·운영 및 거부에 관해 쿠키를 사용하고 있지 않은 것으로 기재되어 있다. 본 문서에서의 '쿠키'란 이용자에게 개별적인 맞춤서비스를 제공하기 위해 이용정보를 저장하고, 수시로 불러오는 데이터 파일을 의미한다.

또 '가명정보 처리'의 경우 처리 목적 및 항목을 포함, 모든 사항에 대해 해당되지 않는 상태로 기재되어 있다. '개인정보시스템 보안 지침'에서 개인정보 가명처리 기준에 대해 목적을 포함 다수의 조를 기재하고 있지만, 본 기관에서는 해당사항이 없어 적용되지 않고 있는 상태이다.

개인정보보호 책임자의 경우 정보주체의 민원처리 및 피해 시 구제를 위해 정보보호처 2인을 담당자로 규정하고 있다. 개인정보 열람 청구 접수 및 처리 업무의 경우 '고객지원부서'에서 담당하고 있으며, 열람청구 부서 이외에 [개인정보 포털]을 통해서도 청구를 진행할 수 있는 체계이다.

또 '개인정보관리방침' 문서에 권익 침해 구제에 대해 문의할 수 있는 기관 정보를 기재해놓았으며, 영상정보처리기기의 설치 및 운영에 대해서는 [영상정보처리기기 설치·운영 현황]에 상세 기술된 상태이다. 이에 대해 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록·관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구 삭제를 진행하고 있다. 영상 정보의 경우 영상정보 관리책임자 또는 관리담당자에게 미리 연락하고, 담당 부서를 방문하여 확인이 가능하다.

확인 요청 시 일전에 언급된 정보주체의 영상정보 열람 등 요구에 대한 조치에 따라 개인영상정보 열람·존재확인 청구서로 신청하여야 하며, 정보주체 자신이 촬영된 경우 또는 명백히 정보주체의 생명·신체·재산 이익을 위해 필요한 경우에 한해 열람을 허용하고 있다.

그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항법령, 정책 또는 보안기술의 변경이 발생했을 경우, 지체없이 도로교통혁신안전센터 홈페이지에 변경사항을 고지하는 시스템으로 파악되었다.

2.2. 관리보안 체계 및 규정 분석

2.2.1. 관리적 보안 체계

본 센터는 자체 시스템 보안 지침을 통해 접근권한 관리를 비롯한 다수 지침을 수행 중에 있다. 먼저 접근 권한 관리지침의 경우 사용자(직원) 아이디(이하 "사용자 ID" 라 한다) 및 권한 관리에 대한 준수사항을 규정하여, 개인정보 등 중요자료 취급에 대한 안전성 확보를 목적으로 하고 있다.

사용자 ID의 경우 임의 양도, 대여, 위탁이 불가하도록 규정하고 있으며, 등록되어있는 사용자 ID의 사용여부를 주기적으로 확인하고 있다. 또 불필요한 ID의 경우 사용을 즉각 중지하도록 조치하고 있으며, ID 변경 및 삭제는 불가한 체계이다. ID는 크게 개인과 특수목적용 ID로 나뉘어져 있으며, 등록 절차는 다음과 같다.

순서	개인 ID	특수목적용 ID
1	인사 등록	특수목적용 인증서 발급
2	개인용 인증서 발급	사용자 ID 등록
3	사용자 ID 등록	

[표 11] ID 분류별 등록 순서

(출처: 도로교통혁신안전센터_개인정보시스템 보안 지침)

또 접근 통제적 측면에서 고유식별정보를 처리하는 인터넷 홈페이지를 연 1회 이상 점검하여, 취약점이 존재하는지 여부를 검사하고 있다. 만일 개인정보취급자가 일정 시간 이상 업무를 처리하지 않는 경우, 자동으로 시스템 접속을 차단시켜 불법적 접근을 방지하고 있다. 개인정보취급자에 대한 접근통제 교육 또한 진행되고 있는 것으로 확인되었다.

접속 프로그램 보관 및 점검과 관련된 주기의 경우, 본 센터는 5만명 이상의 정보주체에 대한 개인정보를 처리하는 기관이니 개인정보처리시스템 접속기록을 최소 2년 이상 보관 및 관리하고 있다. 접속 기록은 월 1회 이상 정기적으로 점검하고 있으며,

필요한 경우 추가적인 조치를 취한다고 기재되어있다. 하지만 어느 경우가 추가 조치가 필요한 경우인지, 또 정확히 어떤 조치를 행하는지는 기재되어있지 않다. 마찬가지로 개인정보 다운로드 행위 발견 시 사유를 판단하고 추가 조치를 취한다고 기재되어있지만, 정확히 어느 조치를 취하는지, 어느 경우가 조치가 필요한 경우인지는 기재되어있지 않다. 접속기록을 생성할 때는 타임스탬프를 포함해서 기록의 정확성을 보장하고 있으며, 변경 이력을 별도 관리 중에 있다.

위험도 분석의 경우 아래 절차를 통해 시행되며, 분석 기준은 다음과 같다.

[그림 8] 위험도 분석 기준 구성

(출처: 도로교통혁신안전센터)

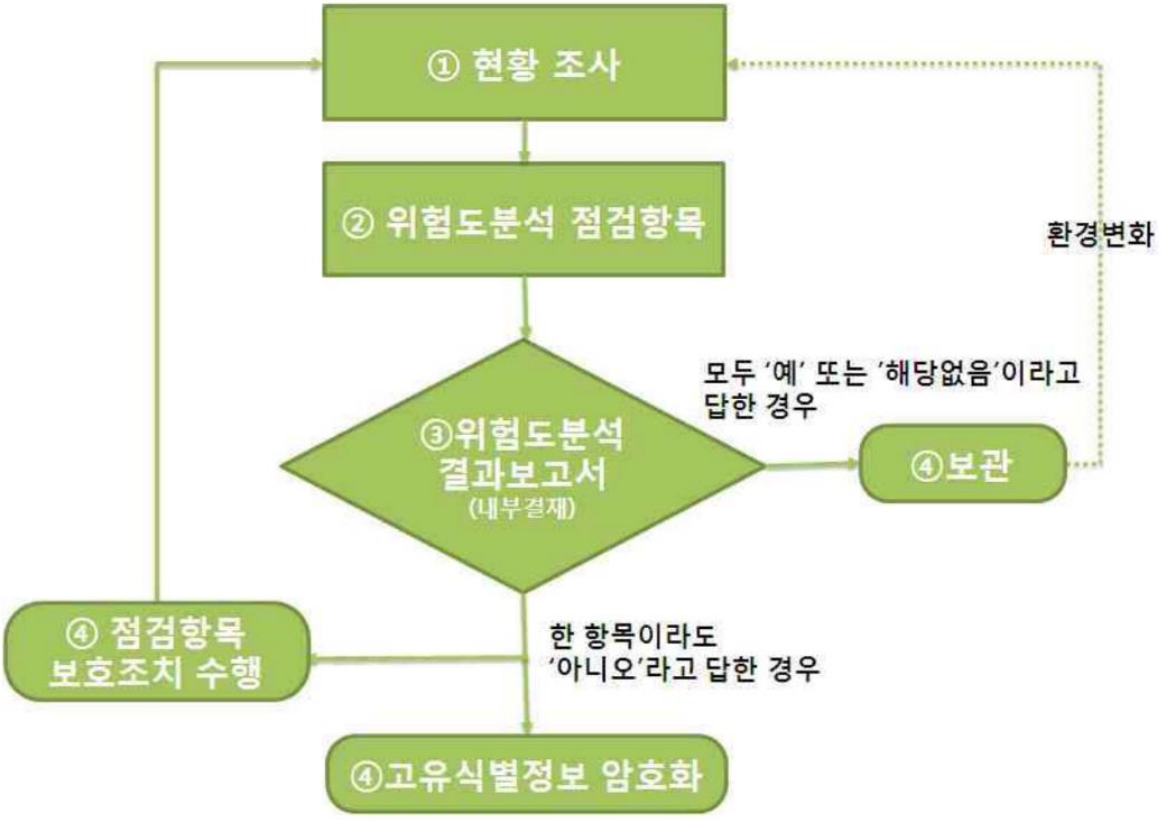
① 위험도 분석을 위해 개인정보파일 및 고유식별정보 보유 여부 등 현황조사

② 개인정보파일 단위로 위험도 분석 점검 항목별 점검을 수행

③ '위험도 분석 결과보고서'를 작성하여 내부결재 후 보관

④ 점검 결과에 따라 고유식별정보 암호화 등을 수행

시행 주기의 경우 공식 문서에 언급된 바가 없었으나, 대면 문의를 통해 연 1회 이상 진행하고 있음을 답변받을 수 있었다.



[그림 9] 위험도 분석 절차

(출처: 도로교통혁신안전센터)

별도로 정보통신시스템 백업 방침을 수립하여 백업 관리 대장과 함께 운용 중에 있다. 공용 계정 사용 금지 및 불필요 계정 삭제 등 실제 수행되는 보호 방침도 있었으나, '정해진 관리자만 시스템에 접속할 수 있도록 접근 통제 실시' 와 인터넷 분리 환경 구축 등 실제 네트워크 상과 상이하게 운용되는 부분 또한 존재하였다.

2.2.2. 서약서 및 공고 내용

본 센터에서는 내부자산 보호를 위해 외부 용역용, 입사자용, 퇴사자용, 재직자용 비밀유지 서약서 및 보안서약서를 구비하여 운용하고 있다. 또 외부 용역 채용 철차에 사용되는 응시원서에 응시자의 개인정보를 수집하고 있다.

2.3. 내부 물리보안 체계 및 규정 분석

2.3.1. 내부 기록물 & 기기 보안 체계

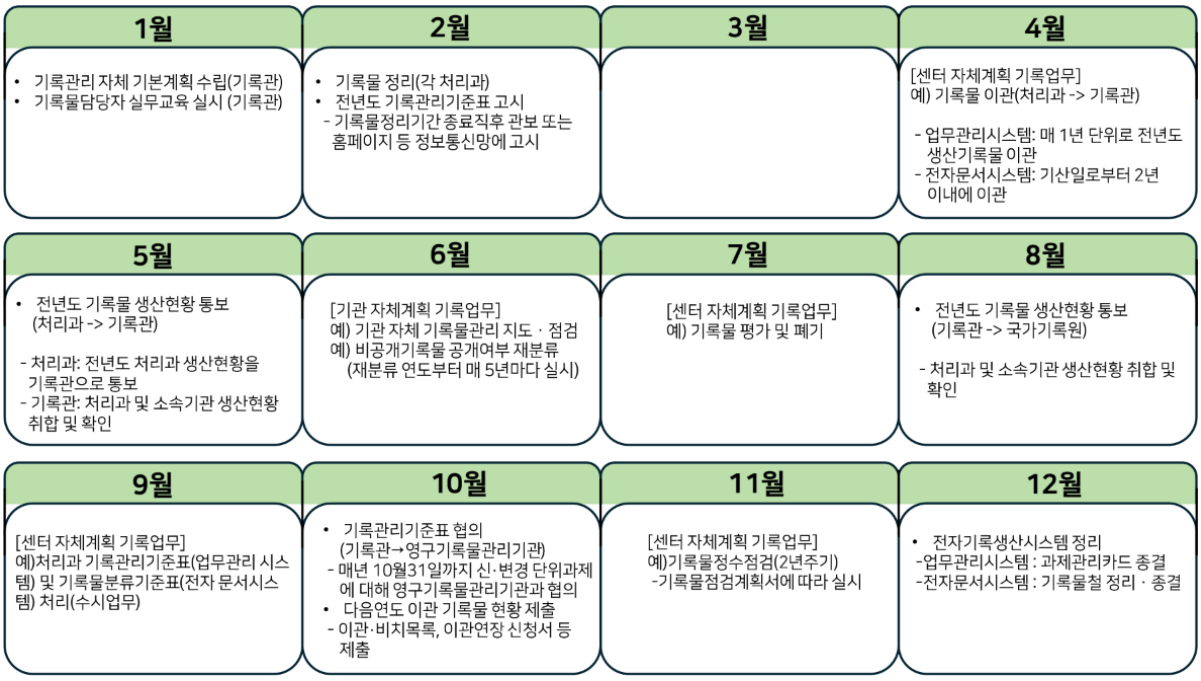
본 센터에서는 문서생명주기를 설정하여 생산부터 평가/폐기까지의 과정에서 각 문서를 관리하고 있다. 각 과정에 대한 기록물 관리 체계 상세는 다음과 같다.

생산	공단에서 수행하는 모든 업무의 과정과 결과가 기록물로 생산 및 등록되며, 비전자기록물은 전자화 방안에 따라 전자화된 상태로 관리
등록	모든 기록물은 센터의 전자기록생산시스템으로 생산 또는 접수등록번호가 부여되어 등록
분류	처리 완결된 기록물철은 기록관리기준표에 따라 처리과별과 단위과제별로 분류해 기록물등록대장에 등록
정리	기록관장은 생산 완결된 기록물에 대해 정리를 위해 매년 2월말까지 공개여부 접근권한 재분류, 분류·편철·확정 등을 진행
이관	기록관은 생산 완결된 기록물을 보존기간 기산일로부터 2년의 범위 이내에 이관받아야 함
보존	기록관에서 인수한 기록물은 기록물 형태, 처리과 등을 구분해 서고에 배치해야 함
평가 및 폐기	기록물평가심의회를 구성, 운영해 평가 및 폐기 심의

[표 12] 문서 생명주기별 관리방안

(출처: 도로교통혁신안전센터_문서생명주기)

또 본 센터에서는 월 단위로 연간 기록업무를 관리하고 있으며, 월별 상세 업무 수행 내역은 다음과 같다. 기관 자체계획 기록 체계를 생성하여 진행하고 있으며, 기록물 정리의 경우 각 처리과가 담당한다. 단 4월 기록물 이관 업무에서부터는 담당 단위가 처리과에서 기록관으로 변경되며, 8월에 다시 국가기록원으로 변경되는 체계이다. 10월에는 기록관이 영구기록물관리기관과 단위 과제 등 기록관리기준표에 대한 협의를 진행한다. 이후 12월에 전자기록생산 시스템을 정리하고, 각 관리 시스템 자료들을 종결하는 구조이다.



[그림 10] 연간 기록관리업무

(출처: 도로교통혁신안전센터_문서생명주기)

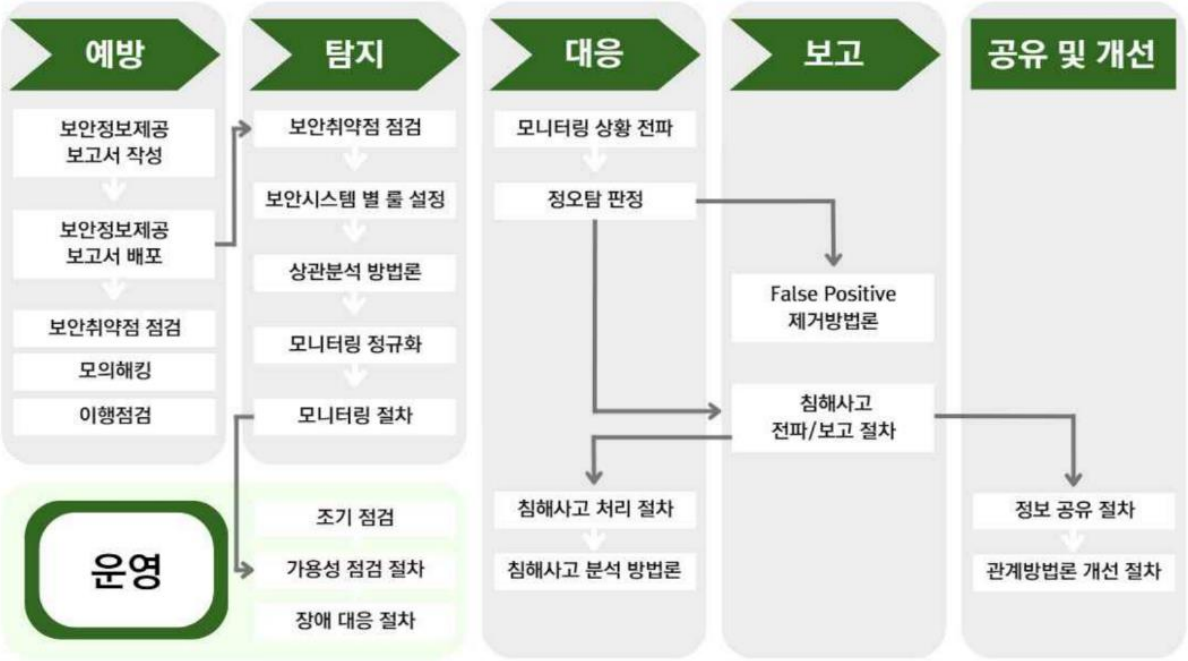
이 밖에도 교통신호제어기 이력카드, CCTV 영상정보 관리대장, 영상물요청서 등을 통해 정보자산의 흐름을 관리하는 체계가 있는 것으로 파악되었다.

2.3.2. 모니터링 및 내부감사 체계

본 센터에서는 자체 실시간 보안 모니터링 프로세스를 정립하여 운용 중에 있다. 프로세스는 예방, 탐지, 대응, 보고, 공유 및 개선 단계로 이루어져 있으며, 각 프로세스에 대한 분석 상세는 다음과 같다.

먼저 예방 절차의 경우 잠재적인 보안 위협 방지를 위한 과정으로, 보안정보제공 보고서 작성을 포함한 5가지 보안 업무가 수행된다. 이어 탐지 절차의 경우 실시간으로 보안 위협을 탐지하여 신속 대응을 진행하는 과정으로, 보안취약점 점검부터 모니터링 정규화 작업이 수행된다. 이어 대응 절차의 경우 이전 과정에서 탐지된 위협에 대해 상황 전파, 정상 여부 판정 등의 대응활동이 수행된다. 이전 과정들에서 산출된 결과를 토대로 보고하고, 이후 해당 경험을 공유하여 개선 방안을 수립하는 과정까지 진행되는

구조이다. 모니터링 프로세스에 대한 Overview는 다음과 같다.



[그림 11] 보안 모니터링 절차

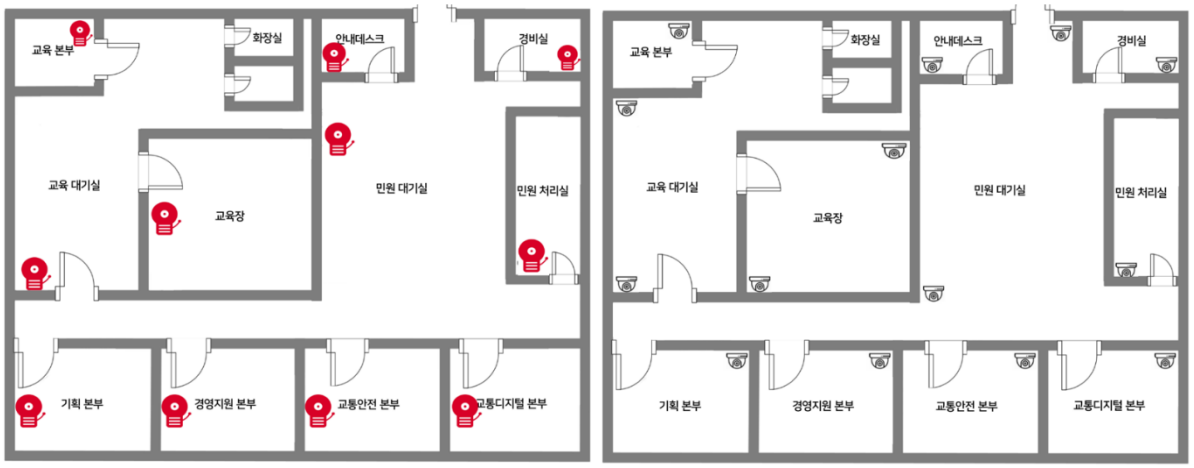
(출처: 도로교통혁신안전센터)

본 센터에서는 운전면허, 교육, 경영지원, 교통디지털, 기획본부에 대해 정보보안 감사를 수행 중에 있다. 정보보안 감사의경우 감사 위원회에서 진행하며, 연 1회 실시되고 있는 상태이다. 정보보안 감사는 '위험 분석' 시스템과 동일한 체계로, 정보보안 관리 규정/정보보안 관리체계 내부감사 매뉴얼/침해사고 대응 매뉴얼/정보자산 및 위험관리 매뉴얼/외주 보안관리 매뉴얼 외 10개의 체크리스트를 기반으로 수행되는 구조이다.

2.3.3. 센터 내 물리적 설계 상세

본 센터는 보호구역과 일반구역으로 나누어지며, 보호구역은 제한구역과 통제구역으로 구성된다. 각 구역별로 출입 통제 시스템과 함께 '출입 관리 대장'을 활용하여 물리적 보안지침을 따르고 있다. 세부적으로는 전산시스템실의 업무 구역을 사무실과 주전산실로 나누어 출입을 통제하고 있다. 또 통제구역 내에서는 자산 보호를 위해 흡연, 음주, 취식을 금지하고 있으며, 각 구역별 상이한 보안관리 지침을 적용하고 있다.

구역별 CCTV와 화재경보기 설치 현황은 다음과 같으며, 화장실을 제외한 모든 구역에 설치되어있음을 확인하였다. 또 CCTV 설치 및 운영을 알리기 위해 CCTV안내문을 CCTV가 녹화 중인 모든 장소에 대해 부착하고 있음을 확인하였다.



[그림 12] CCTV(우) 및 화재경보기(좌) 설치 현황

(출처: 도로교통혁신안전센터)

2.4. 기술보안 체계 및 규정 분석

2.4.1. 데이터베이스 규정

본 센터에서는 도로종류, 시간대, 요일별로 교통사고 데이터를 파일화하여 관리 중에 있으며, 아래의 [그림 13]과 같이 관계형 데이터베이스를 사용하여 각 데이터를 구조화하였다.

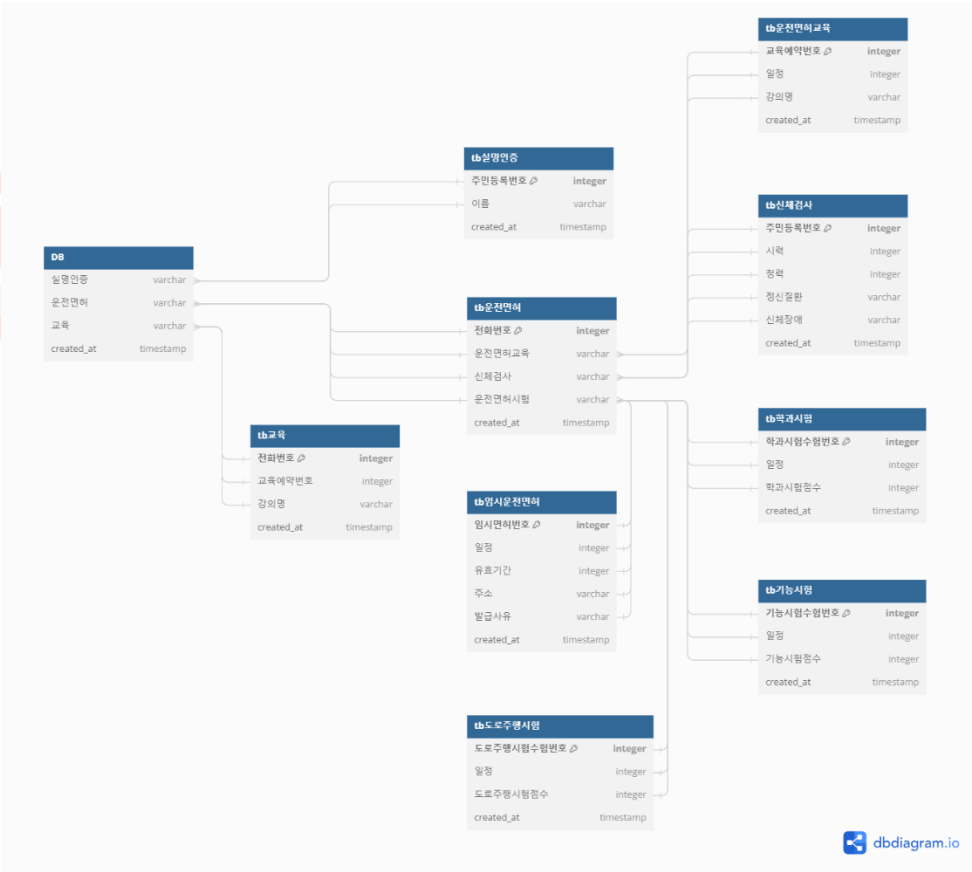
또 자체 데이터베이스 보안 관리지침을 수립하여 운용 중에 있으며, 암호화 및 복구/접근 통제에 대한 사항이 규정하고 있다. 데이터 암호화 측면의 경우 해독 불가능 상태로 처리하는 것에 중점을 두어, 저장 장소와 무관하게 대칭키 암호 알고리즘 및 일방향 해시(One-way Hash)를 사용하고 있는 상황이다. 기본적으로 성능 저하를 최소화하기 위해 컬럼 단위의 암호화를 적용하고 있으나, 불가피한 상황에 대해서만 파일 단위 암호화를 진행하고 있는 것으로 확인되었다. 사용 중인 암호 알고리즘에 대한 내용은 다음 [표 13]과 같다. 관련 암호화 기술 및 프로그램의 경우 3개월 주기로 정보보안담당관에 의해 감사가 수행되고 있으며, 적용 현황과 신뢰 수준 등을 평가받고 있다.

구분	공공기관
대칭키 암호 알고리즘	SEED, LEA, HIGHT, ARIA
공개키 암호 알고리즘	RSAES-OAEP
일방향 암호 알고리즘	SHA-224/256/384/512

[표 13] 암호화 키 및 패스워드 선택 기준

(출처: 개인정보보호위원회_개인정보 암호화 조치 안내서)

암호 키의 경우 암호화 키와 패스워드의 선택, 관리, 복구 항목으로 분류하여 규정하고 있으며, 위와 마찬가지로 정보보안담당관에 의해 3개월 주기로 보안 감사가 수행되고 있는 실정이다. 데이터 암호화 시에는 담당자의 승인을 받는 절차가 별도로 존재하며, 이어 암호화 키 관리대장에 등록되는 절차까지 진행되는 것으로 확인되었다. 암호화 키는 1년 단위로 변경되며, 마찬가지로 '암호화 키 관리 대장'에 폐기/생성/사용 등 모든 내역이 기록된다.



[그림 13] DB 운전 및 교육 구조도

(출처: 도로교통혁신안전센터)

암호화 키 및 패스워드는 아래 기준을 준수하여 선택되며, 그 상세는 다음 표와 같다.

키 비트 수	대칭키 암호 알고리즘	128bit 이상
	비대칭키 암호 알고리즘	2048bit 이상
패스워드 길이	최소 8자리	
패스워드 구성	대문자, 소문자, 숫자, 특수문자 혼용 필수	
패스워드 변경 주기	3개월	
패스워드 보호 체계	연속 5회 이상 로그인 실패 시 60분간 접속 차단	
금지 사항	- 사전적 단어 - 널리 알려진 단어 - 사용자 ID와 연관된 단어 - 개인정보 관련 내용 - 새로운 문자 구성/체계 - 동일 문자 반복 - 키보드 상의 나란한 문자열 - 일련번호 - 가족 이름, 생일, 전화번호	

[표 14] 암호화 키 및 패스워드 선택 기준 및 기타 정보

(출처: 도로교통혁신안전센터_DB보안관리지침)

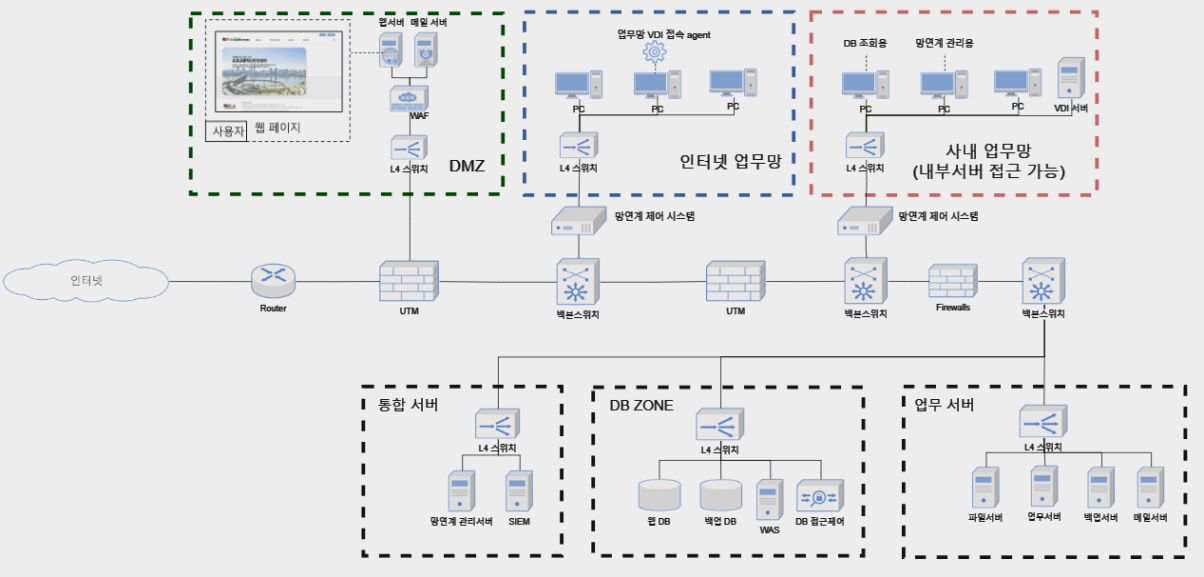
부가적으로 암호화 키 복구가 이루어질 경우 모든 과정을 '암호화 키 복구 대장'에 기록하고 있으며, 이는 정보보안담당자에 의해 관리되는 체계이다. 데이터 자체의 백업 및 복구에 대해서는 OS 및 시스템 SW, 전 데이터베이스, 전산 응용 프로그램 및 소스/특정 서버에 대해 이루어지고 있으며, 정기 백업 주기 및 보관 기간은 다음과 같다.

자료 백업 주기		자료 보관 기간
기간 단위	일일	2주
	주간	4주
	월간	4개월

[표 15] 백업 주기 및 자료보관 기간

(출처: 도로교통혁신안전센터_DB보안관리지침)

2.4.2. 네트워크 관리 체계



[그림 14] 정보시스템 컨설팅 후의 네트워크 구조도

(출처: 한라KPC)

본 펌(한라 KPC)에서 착수했던 교통망 클라우드 도입 및 네트워크 컨설팅(이하 '컨설팅 요청사항 1번')의 결과로서 제안되어, 도로교통혁신안전센터에서 운용 중이던 네트워크 구성도는 위와 같다.

DMZ 구역과 인터넷/사내 업무망을 분리함으로써 네트워크 세그멘테이션을 구현하였으며, 각 망 접속 시 '망연계 제어 시스템'을 거치도록 설정하여 접근 전 추가 인증 절차를 도입한 상태이다. 또 서버팜에 진입하기 전 백본스위치를 거치도록 구현하여, 추가 트래픽 관리 기제를 수립하였다. 개인정보 데이터가 저장되는 주요 서버의 경우, 접근까지 2개의 UTM을 포함한 다수의 보안장비를 거치도록 구현하여 보안성을 높였으며, 네트워크 상에서 통신되는 모든 데이터는 암호화된 채로 송/수신된다.

2.5. 기타 외부 보안자료 및 규정 분석

본 기관의 증적과 관련하여, 참고 및 분석된 외부 자료는 다음과 같다.

관련 법규	주요 내용
개인정보보호법	개인정보 처리 과정상의 정보주체와 개인정보처리자의 권리·의무 등 규정※ 공공·민간 구분 없이 모든 개인정보처리자에게 적용함
표준 개인정보 보호지침	개인정보취급자 및 처리자가 준수하여야 하는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부사항 규정
개인정보의 안전성 확보조치 기준	개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조· 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 최소한의 기준 규정
개인정보 영향평가에 관한 고시	영향평가 수행을 위한 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준 규정
개인정보 처리 방법에 관한 고시	공공기관의 개인정보 목적 외 이용 등에 따른 공고의 절차 및 방법, 개인정보 보호업무 관련 장부 및 문서 서식, 서면 동의 시 표시 방법에 관한 세부 사항 규정
개인정보 위험도 분석 기준	개인정보 처리시스템의 보호수준을 진단하여 암호화에 상응하는 조치필요 여부를 판단할 수 있는 기준을 규정
가명정보의 결합 및 반출 등에 관한 고시	결합전문기관 지정 및 가명정보의 결합・반출에 관한 기준・절차 등을 규정
개인정보 암호화 조치 안내서	개인정보처리자 및 정보통신 서비스 제공자들이 개인정보를 안전하게 저장 및 전송하는데 사용되는 기술인 암호화에 대한 안내를 제공

홈페이지 개인정보 노출방지 안내서	인터넷에 노출된 개인정보의 오남용을 예방하고, 개인정보처리자, 이용자를 대상으로 개인정보 노출 원인 및 조치 방법에 대한 안내를 제공
패스워드 선택 및 이용 안내서	안전한 패스워드의 생성부터 폐기까지 관리 전반에 대한 보안적 내용을 아내
암호 키 관리 안내서	NIST SP 800-57(암호 키 관리)에 필요한 기능을 기반으로 하여 안전한 키 관리에 필요한 기능 및 고려사항을 소개
개인정보 처리 위수탁 안내서	개인정보 처리를 위/수탁 시 위탁자와 수탁자가 인지하고 조치해야 하는 사항을 안내
암호 알고리즘 및 키 길이 이용 안내서	SEED, ARIA 등의 국산 암호 알고리즘을 포함, 보안 강도에 따라 선택 가능한 암호 알고리즘의 종류 및 키 길이, 유효기간을 소개
SW 개발 보안 가이드	소프트웨어 개발 생명 주기에 고려되어야 하는 보안 위협 최소화를 위해 각 단계별로 수행해야 하는 보안 활동들을 정의
온라인 개인정보 처리 가이드라인	온라인 상의 개인정보 처리에 있어 정보통신서비스 제공자/관리자가 숙지 및 이행해야 할 요소들을 안내
개인정보 유출 등 사고대응 메뉴얼	개인정보처리자 등이 처리하고 있는 개인정보에 대해 개인정보 유출 등 사고와 관련하여 신속한 대응과 그 피해를 최소화하기 위한 최소한의 사항 안내
개인정보처리방침 작성 가이드라인	개인정보보호법과 같은 법적 사항에 근거하여, 개인정보처리자의 개인정보 처리 기준 및 보호조치 등을 담은 개인정보 처리방침 작성에 대해 준수 및 필수 포함 사항을 안내

[표 16] 백업 주기 및 자료보관 기간

(출처: 한라 KPC & 개인정보보호위원회 & KISA)