1. 관리체계 수립 및 운영(16개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
1.1.	관리체계 기반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.	(관)2.1 경영진 참여	(관)1.2.1 경영진의 참여
		1.1.2	최고책임자의 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.	(보)2.1.1 정보보호 최고책임자 지정	(관)1.3.1 개인정보보호 책임자의 지정
		1.1.3	조직 구성	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.	(관)2.2 정보보호 조직구성 및 자원할당 (보)2.1.2 실무조직 구성 (보)2.1.3 정보보호 위원회	(관)1.3.2 조직의 구성
		1.1.4	범위 설정	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.	(관)1.2 범위설정	(관)1.1.3. 범위설정
		1.1.5	정책 수립	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.	(관)1.1 정보보호정책의 수립 (보)1.1.1 정책의 승인 (보)1.1.2 정책의 공표 (보)1.2.2 정책시행 문서수립 (보)10.1.1 접근통제 정책 수립 (보)11.1.1 운영절차 수립	(관)1.1.1 정책의 수립 (보)8.1.1 접근통제 정책 수립 (보)8.4.1 운영절차 수립
		1.1.6	자원 할당	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.	(관)2.2 정보보호 조직구성 및 자원할당	(관)1.3.2 조직의 구성
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.	(보)4.1.1 정보자산 식별	(관)2.1.1. 개인정보 식별
		1.2.2	현황 및 흐름분석	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	NEW	(관)2.1.2 개인정보 흐름파악
		1.2.3	위험 평가	조직의 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.	(관)3.1 위험관리 방법 및 계획 수립 (관)3.2 위험식별 및 평가	(관)2.2.1 위험관리 방법 및 계획 수립 (관)2.2.2 위험식별 및 평가
		1.2.4	보호대책 선정	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.	(관)3.3 정보보호대책 선정 및 이행계획 수립	(관)2.2.3 이행계획 수립 및 보호대책 구현
1.3.	관리체계 운영	1.3.1	보호대책 구현	선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.	(관)4.1 정보보호대책의 효과적 구현	(관)2.2.3 이행계획 수립 및 보호대책 구현
		1.3.2	보호대책 공유	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.	(관)4.2 내부 공유 및 교육	(관)4.2.1 내부 공유 및 교육
		1.3.3	운영현황 관리	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.	(관)5.2 정보보호 관리체계 운영현황 관리	(관)4.1.1 개인정보보호 개선 활동
1.4.	관리체계 점검 및 개선	1.4.1	법적 요구사항 준수 검토	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.	(관)5.1 법적 요구사항 준수검토	(관)3.1.1 법적 요구사항 준수검토

1. 관리체계 수립 및 운영(16개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
		1.4.2	관리체계 점검	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.	**(관)5.3 내부감사**	**(관)3.1.2 내부 감사**
		1.4.3	관리체계 개선	법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.	**(관)5.3 내부감사**	**(관)3.1.2 내부 감사**

2. 보호대책 요구사항(64개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.	(보)1.2.1 상위 정책과의 연계성 (보)1.3.1 정책의 검토 (보)1.3.2 정책문서 관리	(관)1.1.2 정책의 유지관리
		2.1.2	조직의 유지관리	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.	(보)2.2.1 역할 및 책임	(관)1.3.3. 역할 및 책임
		2.1.3	정보자산 관리	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.	(보)4.1.2 정보자산별 책임할당 (보)4.2.1 보안등급과 취급	(관)2.1.1. 개인정보 식별
2.2.	인적 보안	2.2.1	주요 직무자 지정 및 관리	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.	(보)6.1.1 주요 직무자 지정 및 감독	(보)7.2.1 개인정보 취급자 감독
		2.2.2	직무 분리	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.	(보)6.1.2 직무 분리	(보)8.4.2 직무분리
		2.2.3	보안 서약	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.	(보)6.1.3 비밀유지서약서	(보)7.2.2 보안서약서
		2.2.4	인식제고 및 교육훈련	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.	(보)5.1.1 교육계획 (보)5.1.2 교육대상 (보)5.1.3 교육내용 및 방법 (보)5.2.1 교육시행 및 평가	(보)7.1.1 교육 및 훈련 시행,평가
		2.2.5	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.	(보)6.2.1 퇴직 및 직무변경 관리	(보)7.2.3 퇴직 및 직무변경 관리
		2.2.6	보안 위반 시 조치	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.	(보)6.2.2 상벌규정	(보)7.2.1 개인정보 취급자 감독
2.3.	외부자 보안	2.3.1	외부자 현황 관리	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.	NEW	NEW
		2.3.2	외부자 계약 시 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.	(보)3.1.1 외부자 계약 시 보안요구사항 (보)8.3.1 외주개발 보안	(보)7.3.1 외부 위탁 계약 (보)8.6.5 외주개발 보안
		2.3.3	외부자 보안 이행 관리	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.	(보)3.2.1 외부자 보안 이행관리 (보)8.3.1 외주개발 보안	(보)7.3.3 위탁자 관리,감독
		2.3.4	외부자 계약 변경 및 만료 시 보안	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.	(보)3.2.2 외부자 계약 만료 시 보안	NEW
2.4.	물리 보안	2.4.1	보호구역 지정	물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.	(보)7.1.1 보호구역지정	(보)9.2.1 보호구역의 지정 및 관리

2. 보호대책 요구사항(64개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
		2.4.2	출입통제	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.	(보)7.1.4 출입통제	(보)9.2.2 출입통제 및 사무실 보안
		2.4.3	정보시스템 보호	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.	(보)7.2.2 시스템 배치 및 관리 (보)7.2.1 케이블 보안	NEW
		2.4.4	보호설비 운영	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온도·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다.	(보)7.1.2 보호설비	(보)9.2.1 보호구역의 지정 및 관리
		2.4.5	보호구역 내 작업	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.	(보)7.1.3 보호구역 내 작업	(보)9.2.1 보호구역의 지정 및 관리
		2.4.6	반출입 기기 통제	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.	(보)7.1.5 모바일 기기 반출입	(보)9.3.3 이동컴퓨팅 관리
		2.4.7	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.	(보)7.3.1 개인업무 환경 보안 (보)7.3.2 공용업무 환경 보안	(보)9.2.3 개인업무 환경 보안 (보)9.2.2 출입통제 및 사무실 보안
2.5.	인증 및 권한관리	2.5.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.	(보)10.2.1 사용자 등록 및 권한부여	(보)8.1.2 개인정보취급자 등록 (보)8.1.3 개인정보취급자 권한관리
		2.5.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.	(보)10.3.2 사용자 식별	(보)8.1.6 개인정보취급자 인증 및 식별
		2.5.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.	(보)10.3.1 사용자 인증	(보)8.1.6 개인정보취급자 인증 및 식별
		2.5.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.	(보)10.3.3 사용자 패스워드 관리 (보)10.3.4 이용자 패스워드 관리	(보)8.1.7 비밀번호 관리
		2.5.5	특수 계정 및 권한 관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.	(보)10.2.2 관리자 및 특수권한 관리	(보)8.1.4. 특수권한 관리
		2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.	(보)10.2.3 접근권한 검토	(보)8.1.5 개인정보취급자 접근 권한 검토 (보)8.1.3 개인정보취급자 권한관리
2.6.	접근통제	2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.	(보)10.4.1 네트워크 접근	(보)8.3.1 네트워크 접근
		2.6.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.	(보)10.4.2 서버 접근	(보)8.3.2 서버접근

2. 보호대책 요구사항(64개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
		2.6.3	응용프로그램 접근	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.	(보)10.4.3 응용프로그램 접근	(보)8.3.3 응용프로그램 접근
		2.6.4	데이터베이스 접근	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.	(보)10.4.4 데이터베이스 접근	(보)8.3.4 데이터베이스 접근
		2.6.5	무선 네트워크 접근	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.	(보)11.2.7 무선네트워크 보안	NEW
		2.6.6	원격접근 통제	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.	(보)11.2.5 원격운영 관리 (보)11.2.6 스마트워크 보안	(보)8.3.5 원격운영 접근
		2.6.7	인터넷 접속 통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.	(보)10.4.6 인터넷 접속	(보)8.3.6 인터넷 접속 통제
2.7.	암호화 적용	2.7.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.	(보)9.1.1 암호 정책 수립	(보)8.5.1 암호화 정책 수립 (보)8.5.2 암호화 적용
		2.7.2	암호키 관리	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.	(보)9.2.1 암호키 생성 및 이용	(보)8.5.2 암호화 적용
2.8.	정보시스템 도입 및 개발 보안	2.8.1	보안 요구사항 정의	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.	(보)8.1.1 보안 요구사항 정의 (보)11.2.1 정보시스템 인수	(보)8.6.2 개발 시 보안조치
		2.8.2	보안 요구사항 검토 및 시험	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.	(보)8.2.1 구현 및 시험 (보)11.2.1 정보시스템 인수 (보)8.1.2 인증 및 암호화 기능 (보)8.1.3 보안로그 기능 (보)8.1.4 접근권한 기능	(보)8.6.1 개인정보 영향평가 (보)8.6.2 개발 시 보안조치
		2.8.3	시험과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.	(보)8.2.2 개발과 운영 환경 분리	(보)8.6.3 개발과 운영환경 분리
		2.8.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.	(보)8.2.4 시험 데이터 보안	(보)8.6.4 시험 데이터 및 소스프로그램 보안
		2.8.5	소스 프로그램 관리	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.	(보)8.2.5 소스 프로그램 보안	(보)8.6.4 시험 데이터 및 소스프로그램 보안
		2.8.6	운영환경 이관	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.	(보)8.2.3 운영환경 이관	(보)8.6.3 개발과 운영환경 분리
2.9.	시스템 및 서비스 운영관리	2.9.1	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.	(보)11.1.2 변경관리	NEW

2. 보호대책 요구사항(64개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
		2.9.2	성능 및 장애관리	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.	(보)11.2.3 성능 및 용량관리 (보)11.2.4 장애관리	NEW
		2.9.3	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.	(보)11.2.9 백업관리	(보)8.4.9 백업관리
		2.9.4	로그 및 접속기록 관리	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.	(보)11.6.2 로그기록 및 보존	(보)8.2.1 개인정보처리시스템 접속 기록 관리 (보)8.2.2 접속기록 모니터링
		2.9.5	로그 및 접속기록 점검	정보시스템의 정상적인 사용을 보장하고 사용자 오·남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.	(보)11.6.3 접근 및 사용 모니터링	(보)8.2.2 접속기록 모니터링
		2.9.6	시간 동기화	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.	(보)11.6.1 시각동기화	(보)8.2.1 개인정보처리시스템 접속 기록 관리
		2.9.7	정보자산의 재사용 및 폐기	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구·재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.	(보)11.4.1 정보시스템 저장매체 관리	(보)9.3.1 개인정보시스템 저장매체 관리
2.10.	시스템 및 서비스 보안관리	2.10.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.	(보)11.2.2 보안시스템 운영	(보)8.4.6 보안시스템 설치, 운용
		2.10.2	클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.	NEW	NEW
		2.10.3	공개서버 보안	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.	(보)11.2.8 공개서버 보안	(보)8.4.7 공개 서버 보안
		2.10.4	전자거래 및 핀테크 보안	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위해 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.	(보)11.3.1 전자거래 보안	NEW
		2.10.5	정보전송 보안	타 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통해 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.	(보)11.3.2 정보전송 정책 수립 및 협약체결	NEW
		2.10.6	업무용 단말기기 보안	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.	(보)10.4.5 모바일 기기 접근	(보)8.4.8 모바일 기기 관리
		2.10.7	보조저장매체 관리	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.	(보)11.4.2 휴대용 저장매체 관리	(보)9.3.2 휴대용 저장매체 관리
		2.10.8	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.	(보)11.5.2 패치관리	(보)8.4.10 패치 관리

2. 보호대책 요구사항(64개)

분야		항목		상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
		2.10.9	악성코드 통제	바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.	**(보)11.5.1 악성코드 통제**	**(보)8.4.3 악성코드 통제**
2.11.	사고 예방 및 대응	2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.	**(보)12.1.1 침해사고 대응절차 수립** **(보)12.1.2 침해사고 대응체계 구축**	**(보)7.4.1 침해사고 대응절차 및 체계구축**
		2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.	**(보)11.2.10 취약점 점검**	**(보)8.4.4 취약점 점검**
		2.11.3	이상행위 분석 및 모니터링	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.	**(보)11.6.4 침해시도 모니터링**	**NEW**
		2.11.4	사고 대응 훈련 및 개선	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.	**(보)12.2.1 침해사고 훈련**	**(보)7.4.2 침해사고 훈련 및 개선**
		2.11.5	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.	**(보)12.2.2 침해사고 보고** **(보)12.2.3 침해사고 처리 및 복구** **(보)12.3.1 침해사고 분석 및 공유** **(보)12.3.2 재발방지**	**(보)7.4.3 침해사고 대응**
2.12.	재해복구	2.12.1	재해, 재난 대비 안전조치	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.	**(보)13.1.1 IT재해복구 체계 구축** **(보)13.2.1 영향분석에 따른 복구대책 수립**	**NEW**
		2.12.2	재해 복구 시험 및 개선	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.	**(보)13.2.2 시험 및 유지관리**	**NEW**

3. 개인정보 처리단계별 요구사항(22개)

분야			항목	상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
3.1.	개인정보 수집 시 보호조치	3.1.1	개인정보 수집 제한	개인정보는 서비스 제공을 위하여 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.	NEW	(생)5.1.1 개인정보 수집 제한
		3.1.2	개인정보의 수집 동의	개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.	NEW	(생)5.1.2 정보주체의 동의 (생)5.1.3 법정대리인 동의 및 고지
		3.1.3	주민등록번호 처리 제한	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.	NEW	(생)5.1.5 주민등록번호 수집이용제한 (생)5.1.6 주민등록번호 대체수단
		3.1.4	민감정보 및 고유식별정보의 처리 제한	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체(이용자)의 별도 동의를 받아야 한다.	NEW	(생)5.1.4 민감정보 및 고유식별정보의 수집 제한
		3.1.5	간접수집 보호조치	정보주체(이용자) 이외로부터 개인정보를 수집하거나 제공받는 경우에는 업무에 필요한 최소한의 개인정보만 수집·이용하여야 하고 법령에 근거하거나 정보주체(이용자)의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.	NEW	(생)5.1.7 간접수집 보호조치 (생)5.2.2 제공받은 개인정보의 관리
		3.1.6	영상정보처리기기 설치·운영	영상정보처리기기를 공개된 장소에 설치·운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.	NEW	(보)9.1.1 영상정보처리기기의 설치, 운영 제한 (보)9.1.2 영상정보처리기기의 설치,운영 사무의 위탁 관리
		3.1.7	홍보 및 마케팅 목적 활용 시 조치	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우에는 그 목적을 정보주체(이용자)가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.	NEW	NEW
3.2.	개인정보 보유 및 이용 시 보호조치	3.2.1	개인정보 현황관리	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.	NEW	(생)5.3.2 개인정보 파일관리
		3.2.2	개인정보 품질보장	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체(이용자)에게 관리절차를 제공하여야 한다.	NEW	(생)5.3.1 개인정보 품질 보장
		3.2.3	개인정보 표시제한 및 이용 시 보호조치	개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무상 반드시 필요하지 않은 개인정보는 삭제하거나 또는 식별할 수 없도록 조치하여야 한다.	NEW	(보)8.4.5 개인정보 표시제한 NEW 출력 복사시 보호조치 NEW 개인정보 비식별화
		3.2.4	이용자 단말기 접근 보호	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.	NEW	NEW
		3.2.5	개인정보 목적 외 이용 및 제공	개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.	NEW	(생)5.2.3 개인정보 목적 외 이용 및 제공
3.3.	개인정보 제공 시 보호조치	3.3.1	개인정보 제3자 제공	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.	NEW	(생)5.2.1 개인정보 제3자 제공
		3.3.2	업무 위탁에 따른 정보주체 고지	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 정보주체(이용자)에게 알려야 하며, 필요한 경우 동의를 받아야 한다.	NEW	(보)7.3.2 정보주체 고지

3. 개인정보 처리단계별 요구사항(22개)

분야			항목	상세내용	(개정 전)ISMS 인증기준	(개정 전)PIMS 인증기준
		3.3.3	영업의 양수 등에 따른 개인정보의 이전	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체(이용자) 통지 등 적절한 보호조치를 수립·이행하여야 한다.	NEW	(생)5.2.4 개인정보의 이전
		3.3.4	개인정보의 국외이전	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.	NEW	(생)5.2.4 개인정보의 이전
3.4.	개인정보 파기 시 보호조치	3.4.1	개인정보의 파기	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.	NEW	(생)5.4.1 개인정보 파기 규정 및 절차 (생)5.4.2 개인정보의 파기
		3.4.2	처리목적 달성 후 보유 시 조치	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.	NEW	NEW
		3.4.3	휴면 이용자 관리	서비스를 일정기간 동안 이용하지 않는 휴면 이용자의 개인정보를 보호하기 위하여 관련 사항의 통지, 개인정보의 파기 또는 분리보관 등 적절한 보호조치를 이행하여야 한다.	NEW	NEW
3.5.	정보주체 권리보호	3.5.1	개인정보처리방침 공개	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보처리방침을 수립하고, 이를 정보주체(이용자)가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.	NEW	(생)5.18 개인정보처리(취급)방침
		3.5.2	정보주체 권리보장	정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.	NEW	(생)6.1.4 권리행사의 방법 및 절차 (생)6.1.1 개인정보 열람 (생)6.1.2 개인정보 정정, 삭제 (생)6.1.3 개인정보 처리 정지 NEW 정보유통 보호대책 NEW 개인정보 동의 철회
		3.5.3	이용내역 통지	개인정보의 이용내역 등 정보주체(이용자)에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.	NEW	(생)6.1.2 개인정보 정정, 삭제