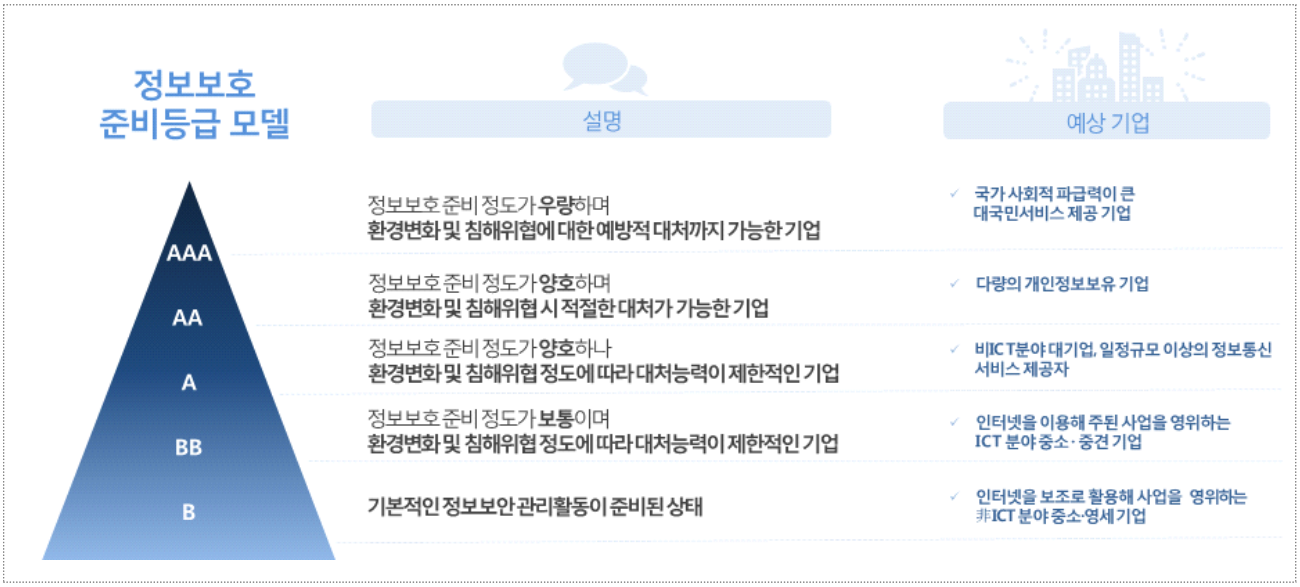
「정보보호 준비도 평가」 평가기준 및 방법

<2014.10.28>

□ 준비도 평가 등급 모델

o 정보보호 준비등급은 기업의 정보보호 인프라 확충 수준 및 정보보호 활동 수행 여부 등을 고려하여 5단계로 구분

<정보보호 준비도 평가 등급 모델>



□ 준비도 평가 프레임워크

o 필수항목(기반지표·활동지표)과 선택항목으로 구성하고 개인정보보호 및 산업 분야별 특성을 고려하여 확장할 수 있도록 설계

<정보보호 준비도 평가 프레임워크>

□ 평가지표 구분

o 필수항목(기반지표·활동지표)과 선택항목으로 구성하고 개인정보보호 및 산업 분야별 특성을 고려하여 확장할 수 있도록 설계

<정보보호 준비도 평가 지표 구분>

구분	설명	주요항목
기반지표 (필수)	정보보호 정책.경영.의사결정 구조(리더십)와 보안투자 및 인력.조직 등 필수적인 보안 인프라(자원관리)를 평가(7개)	정보보호 최고책임자의 자격 및 역할, 정보보호 의사결정 과정.구조, 정보보호 계획 수립.이행, 정보보호 예산 및 집행, 정보보호 인력.조직 보유 등
활동지표 (필수)	관리적.물리적.기술적 정보보호조치 현황 및 체계적인 보안활동 수행 여부를 평가(16개)	연간 임직원 정보보호 교육(횟수, 시간), 내.외부자 보안관리, 연간 취약점 점검 수준 및 횟수, 침해사고 대응체계(모의훈련 실시 등) 구축, 백업 및 복구체계 구축
선택지표	선택지표는 기업이 선택 할 수 있는 지표로서 금융, 교육, 의료 및 기타 산업별 요구사항에 대하여 확장가능하게 운영할 수 있도록 설계	개인정보보호 지표의 경우 「개인정보보호법」및「정보통신망법」에서 규정하는 개인정보보호 필수항목에 대한 준수 여부를 평가(7개)

□ 평가항목 및 기준

지표	구분	평가지표		점수
기반지표	1. 정보보호 리더십	1.1	정보보호 최고책임자(CISO) 지정	5
		1.2	정보보호 의사소통 및 정보제공	5
		1.3	정보보호 운영방침	4
	2. 정보보호 자원관리	2.1	정보보호 추진계획	4
		2.2	정보보호 인력 및 조직	4
		2.3	정보보호 예산 수립 및 집행	4
		2.4	정보보호 이행점검	4
활동지표	1 관리적 보호활동	1.1	정보보호 교육 수행	5
		1.2	자산관리	4
		1.3	인적보안	4
		1.4	외부자 보안	5
	2. 물리적 보호활동	2.1	정보통신시설의 환경 보안	4
		2.2	정보통신시설의 출입 관리	4
		2.3	사무실 보안	4
	3. 기술적 보호활동	3.1	취약점 점검	5
		3.2	정보보호 사고탐지 및 대응	5
		3.3	시스템 개발 보안	4
		3.4	네트워크 보안	4
		3.5	정보시스템 및 응용프로그램 인증	5
		3.6	자료유출 방지	4
		3.7	시스템 및 서비스 운영 보안	5
		3.8	백업 및 IT재해복구	4
		3.9	PC 및 모바일기기 보안	4

선택지표	개인정보보호	1	개인정보 최소수집	P
		2	개인정보 수집 고지 및 동의획득	P
		3	개인정보취급방침	P
		4	이용자 권리 보호	P
		5	개인정보의 관리적 보호조치	P
		6	개인정보의 기술적 보호조치	P
		7	개인정보 파기	P

※ 세부 기준은 [붙임] 정보보호 준비도 평가 항목 및 기준 참조

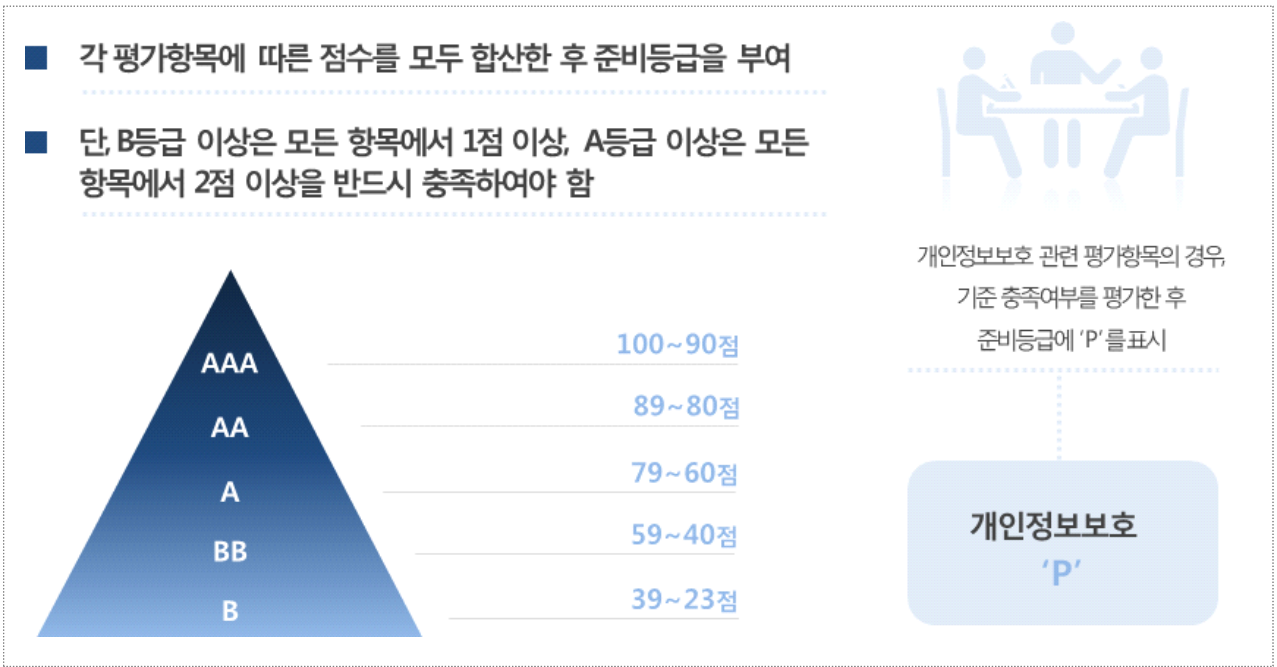
□ 정보보호 준비도 등급의 산정 방법

o 각 평가항목에 따른 점수를 모두 합산한 후 준비등급을 부여하되, **B등급 이상은 모든 항목에서 1점 이상, A등급 이상은 모든 항목에서 2점 이상**을 반드시 충족하여야 함

※ 개인정보보호 관련 평가항목의 경우, 기준 충족여부를 평가한 후 준비등급에 'P'를 표시

환산점수	100 ~ 90점	89 ~ 80점	79 ~ 60점	59 ~ 40점	39 ~ 23점	개인정보보호
준비등급	AAA	AA	A	BB	B	P

<준비도 평가 등급의 산정>



[붙임] 정보보호 준비도 평가기준

1) 기반지표

구분	평가지표			평가기준	배점
1. 정보보호 리더십	1.1	정보보호최고 책임자 (CISO) 지정	최고경영자는 정보보호 최고책임자를 지정하여 정보보호를 총괄하는 책임과 권한을 부여하는가?	조직의 정보보호를 총괄하는 정보보호최고책임자(CISO)를 공식적으로 지정하고 있으며 정보보호 관련 책임과 권한이 있다. (CISO 지정 : 0.5점, 상근임원급 지정 : 1점)	1
				정보보호최고책임자는 다음 사항을 명확히 인지하고 있으며 정보보호 관련 실질적인 업무를 수행하고 있다. - 정보보호최고책임자의 책임과 역할(0.25점) - 조직이 준수해야하는 관련 법령(0.25점) - 조직의 정보보호 목표 및 주요 보호대상(0.25점) - 정보보호 전년도 예산집행 내역 및 당해연도 예산내역(0.25점)	1
				정보보호 또는 정보기술 분야의 학력 또는 정보보호 전문자격을 갖추고 2년 이상 정보보호 분야 업무를 수행한 경력을 보유한 사람을 정보보호최고책임자로 지정하고 있다 - 자격 : CISSP, CISA, 정보보안기사, ISMS심사원, PIMS심사원, PIPL심사원 또는 이에 상응하는 자격 - 학력 : 정보보호 또는 정보기술 분야의 학사 이상 또는 이에 상응하는 경력 *※ 석사의 경우 1년, 박사의 경우 2년을 해당분야의 경력으로 인정함*	1
				정보보호최고책임자는 정보기술 관련조직과 독립적인 위치에서 정보보호 전담업무를 수행하고 있다.	1
				정보보호최고책임자는 전사 정보보호 전략수립, 정보보호 감사 등을 수행할 수 있는 권한이 있다.	1
	1.2	정보보호 의사소통 및 정보제공	정보보호에 관한 의사소통 및 정보제공이 이루어지는가?	정보보호조직(또는 담당자)은 임직원에게 주기적으로 정보보호 관련 정보를 제공(뉴스레터, 정보보안 실천퀴즈, 정보보안 실천가이드 등)하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1
				정보보호 기술, 관련 법률에 대한 외부 전문가 자문 또는 인증(준비도 평가 제외)을 연 1회 이상 수행하고 있다.	1
				정보보호 관련 담당자와 이해관련 부서의 실무자가 정보보호 관련 사항에 대해 주기적인 의사소통 활동을 수행하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1
				정보보호최고책임자와 경영진 또는 이해관련 부서 책임자가 참여하여 주요 정보보호 사안을 결정하는 자리를 정기적으로 마련하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1
				최고경영자(CEO)에게 정보보호활동 보고를 정기적으로 수행하는 등 최고경영자와 정보보호조직(또는 담당자)간의 주기적인 의사소통을 하고 있다. (반기1회 : 0.5점 분기1회 : 1점)	1

구분	평가지표			평가기준	배점
	1.3	정보보호 운영방침	국내외 관련규정을 검토하여 정보보호 운영방침(또는 정책, 지침 등)을 정하고 모든 구성원에게 공표하는가?	정보보호 운영방침을 문서화하고 있으며 다음의 사항을 포함하고 있다. - 경영진의 정보보호 운영방침 준수의지(0.25) - 정보보호 관련 법규에서 요구하는 정보보호 준수사항(0.25) - 관리적인 측면의 정보보호 준수사항(0.25) - 기술적인 측면의 정보보호 준수사항(0.25)	1
				정보보호 운영방침은 최고경영자 서명과 시행일을 명기하여 공표하고 모든 구성원이 쉽게 접할 수 있는 방식으로 공개하고 있다.	1
				정보보호최고책임자는 조직의 운영방침 적합여부 및 법령의 변화 등을 확인하여 연1회 이상 개정하고 있다.	1
				문서화된 인사규정 등에 정보보호운영방침 위반에 따른 상벌규정을 명시 및 시행하고 있다.	1
2. 정보보호 자원관리	2.1	정보보호 추진계획	정보보호최고책임자는 연간 정보보호 추진계획을 수립하고 이행여부를 정기적으로 점검하는가?	기업의 정보보호 현황을 분석하고 그 결과에 따른 주요 정보보호 대책을 수립하고 있다. *※ 기업의 정보보호 현황 분석은 정보보호 준비도 평가기준 등 정보보호 관련 기준 활용*	1
				수립된 정보보호 대책을 이행하기 위해 다음의 사항이 포함된 연간 정보보호 추진계획을 문서화하고 있다. - 목표 업무 별 대상범위 구체화(0.25) - 업무별 수행주체 지정(0.25) - 목표달성을 위한 방법(0.25) - 추진일정(0.25)	1
				연간 정보보호 활동에 대한 목표 및 세부적인 추진계획을 최고경영자가 승인하였다.	1
				정보보호최고책임자가 정기적으로 당해 연도의 정보보호 추진계획을 점검하고 미흡한 사유를 확인하여 원활한 추진이 이루어지도록 하고 있다. (반기1회 : 0.5점, 분기1회 : 1점)	1
	2.2	정보보호 인력 및 조직	정보보호 전담조직을 구성하거나 전담인력을 운영할 수 있도록 지원하는가?	정보보호 활동의 계획 수립 및 수행 등의 정보보호 업무를 수행하는 담당자를 지정하고 역할 및 책임을 문서화하고 있다. (겸임인력 : 0.5점, 전담인력 : 1점)	1
				정보보호 관련 경력 또는 자격 등의 전문성을 갖춘 인력을 정보보호 담당자로 보유하고 있다. (전문인력 구성 50% : 0.5점, 80% : 1점) - 경력 : 2년 이상의 정보보호 관련 경력 보유 - 자격 : CISSP, CISA, 정보보안기사, ISMS심사원, PIMS심사원, CPPG, 기타 이와 상응하는 자격	1
				정보보호 담당자는 전문성 강화를 위해 매년 일정시간 이상의 정보보호 전문교육 또는 세미나에 참여하고 있다. (12시간 이상 : 0.5점, 40시간 이상 : 1점)	1

구분	평가지표			평가기준	배점
				정보보호 활동의 계획 수립 및 수행 등의 정보보호 업무를 수행하는 전담조직을 구성하고 있으며 정보기술인력 대비 5% 이상, 최소 2명 이상으로 구성하고 있다. - 직제로 규정되지 않은 비공식 조직 : 0.5점 - 공식적인 직제로 규정된 전담조직 : 1점	1
	2.3	정보보호예산수립 및 집행	지속적인 정보보호 관리를 위하여 적절한 관리적, 기술적 정보보호 예산을 집행하는가?	관리적, 기술적 정보보호 활동 등을 포함한 정보보호 예산을 수립하여 문서화하고 최고경영자가 이를 승인하고 있다.	1
				정보기술(IT) 부문 예산 대비 일정부분 이상을 정보보호 활동을 위한 예산으로 할당하고 있다. (5%이상 : 0.3점, 7%이상 : 0.6점, 10%이상 : 1점)	1
				정보보호 예산의 집행실적을 주기적으로 검토하고 있다. (정보보호최고책임자 : 분기1회 이상, 최고경영자 : 반기 1회 이상)	1
				전년도 정보보호 활동 부문 투자가 정보기술(IT) 부문 투자 대비 일정부분 이상 이행되었다. (5%이상 : 0.3점, 7%이상 : 0.6점, 10%이상 : 1점)	1
	2.4	정보보호 이행점검	정보보호최고책임자는 정보보호 활동에 대한 정기적인 이행점검(또는 감사)을 수행하는가?	정보보호최고책임자 주관으로 조직의 정보보호 활동이 유지·관리되고 있는지 여부에 대하여 최소 연 1회 이상 이행점검을 수행하고 있다. (부분범위 : 0.5점, 전사범위 : 1점)	1
				정보보호 이행점검 계획은 다음의 사항을 포함하고 있다. - 정보보호 이행점검 구성원(0.25) - 이행점검 일정(0.25) - 이행점검 범위(조직·물리·시스템)(0.25) - 정보보호 운영방침, 관리적, 물리적, 기술적인 준수사항을 포함한 이행점검 항목(0.25)	1
				정보보호 이행점검 결과는 보고서로 작성하여 최고경영자에게 보고하였으며 이해관련 부서에 전달되어 시정조치가 요구사항대로 이행되고 있다.	1
				정보보호 이행점검은 전문성, 독립성을 갖춘 조직이 수행하고 있다. - 전문성(0.5) : 해당분야 관련 경력 또는 자격을 가진 자 - 독립성(0.5) : 점검대상 부서 또는 담당자와 관련이 없는 제3자	1

2) 활동지표

구분	평가지표			평가기준	배점
1 관리적 보호활동	1.1	정보보호 교육 수행	전체 임직원을 대상으로 정보보호 교육을 수행하는가?	교육대상, 교육시간, 교육방법, 교육내용, 불참자 관리방안 등을 포함한 연간 정보보호 교육계획을 수립하고 이에 따라 교육을 수행하고 있다. (계획대비 70%이상 : 0.5점, 90%이상 : 1점)	1
				전체 임직원 및 외부위탁사를 대상으로 정보보호 교육을 수행하고 있다. - 주요 업무수행자 대상 정보보호 교육수행(0.3점) - 전체 임직원 대상 정보보호 교육수행(0.6점), - 외부위탁사 포함 정보보호 교육수행(1점)	1
				정보보호 교육의 내용을 대상자의 직위 및 업무 특성에 따라 구분하여 수행하고 있다. - 일반직원 대상 정보보호 교육(0.25) - 임원 대상 정보보호 교육(0.25) - 정보기술부문 직원대상 정보보호 교육(0.25) - 외부 위탁사 대상 정보보호 교육(0.25)	1
				정보보호 교육 참여율, 만족도, 개선사항을 포함한 교육 결과보고서를 작성하여 정보보호 최고책임자에게 보고하고 있다. (단순보고 0.3점, 참여율 70%이상: 0.5점, 90%이상: 1점)	1
				전체 임직원의 교육 참여율을 높이기 위하여 인센티브 또는 제재 방안을 마련하여 시행하고 있다.	1
	1.2	자산관리	정보시스템 등의 전체 정보자산 목록 현황을 파악하고 각 정보자산의 보안등급을 식별하는가?	정보시스템 자산목록 및 구성현황을 문서 또는 시스템의 형태로 항상 최신의 내용으로 관리하고 있다. - 정보자산 목록 : 자산분류, 자산명, 용도, IP주소, 물리적 위치, 관리담당자를 반드시 포함 - 구성현황 : 네트워크 구성을 포함한 정보시스템 구성도	1
				서비스중요도 등에 따른 정보시스템의 보안등급 식별 기준을 수립하고 기준에 따른 등급을 부여하여 그 결과를 자산목록 등에 포함하여 관리하고 있다.	1
				정보시스템자산의 변경사항(패치, 장애처리, 보안점검이력, 용도변경 등)에 대한 기록을 유지관리하고 있다.	1
				정보시스템 목록의 내역(자산명, 용도, IP주소, 물리적 위치, 관리담당자)과 실제시스템이 일치하는지 여부를 현장점검을 통해 연1회 이상 확인하고 있다.	1
	1.3	인적보안	임직원의 입사, 퇴사, 주요업무 수행에 대한 정보보호서약 등의 인적보안 활동을 하는가?	영업비밀, 개인정보 등의 관련 법률 사항, 회사 정보보호 원칙 및 위반 시 징계 등의 내용을 포함하는 정보보호 서약서를 수립하여 입사 시 징구하고 있다.	1
				퇴사 시 정보보호 서약에 대한 내용을 환기시키거나 별도의 정보보호 서약서를 징구하고 있다. - 정보보호 서약 내용 환기: 0.5점 - 별도의 서약서 징구 : 1점	1
				퇴사, 휴직 또는 직무이동 시 사무실 출입 권한, 시스템 접근 권한 등을 확인하여 해당 권한을 지체 없이(최소 5일 이내) 회수하고 있다.	1

구분	평가지표			평가기준	배점
				개인정보취급자, 중요정보 및 시스템 접근자 등의 주요직무자 지정기준을 수립하여 주요직무자에게 업무특수성에 따른 정보보호 준수사항을 상기 시킬 수 있는 활동을 연1회 이상 수행하고 있다.	1
	1.4	외부자 보안	IT업무를 위탁하거나 정보자산에 접근을 허용한 외부자에 대하여 계약시 보안요구사항을 명시하고 보안관리감독이 이루어지는가?	정보기술 관련 업무 또는 개인정보 관련 업무를 위탁하거나 정보시스템, 보호구역 등에 접근을 허용한 외부자에 대하여 정보보호서약서를 징구하는 등 외부자 보안을 위한 활동을 수행하고 있다.	1
				IT업무 또는 정보자산에 접근하는 업무를 외부자에 위탁 시 계약서 또는 협약서 상에 다음과 같은 보안 준수사항을 반영하고 있다. - 위탁업무 목적과 범위 - 재위탁 금지 - 기술적인 보호조치 의무 - 주기적인 관리감독 권한 - 손해배상 - 관련 법률 요구사항 - 기타 필요하다고 판단되는 보안준수사항	1
				위탁업무를 수행하는 외부자가 계약만료 또는 업무 종료 시 제공받은 정보자산의 반납, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 등을 이행하는지 점검하고 있다.	1
				개인정보보호 등의 관련 법률 요구사항을 고려하여 업무위탁 규모, 중요도 등에 따른 관리주체, 관리방법 등을 포함하는 외부자 보안관리 정책을 수립, 시행하고 있다.	1
				위탁업무를 수행하는 외부자가 준수해야 하는 보안사항을 정의하여 월별 보안사항 점검을 수행하고 있다.	1
2. 물리적 보호활동	2.1	정보통신시설의 환경 보안	정보시스템이 운영되는 장소를 보호구역으로 지정하는가?	정보시스템이 운영되는 장소를 보호구역으로 지정하고 있다.	1
				정보시스템이 운영되는 장소의 시스템 및 인력을 화재로부터 보호하기 위해 필요한 설비를 갖추고 관리하고 있다. - 화재 감지 센서 설치(0.3) - 가스 소화장비 설치(0.3) - 분기별 소방전문가 점검(0.4)	1
				정보시스템에 안정적인 전력 공급을 위한 시설(무정전전원장치, 비상발전기 등)을 설치하고 관리하고 있다. (반기 1회 점검 : 0.5점, 분기 1회 점검 : 1점)	1
				정보시스템이 안정적인 환경에서 동작할 수 있도록 적절한 온도와 습도를 유지시키는 항온항습기 또는 에어컨을 설치하여 운영관리하고 있다. (반기 1회 점검 : 0.5점, 분기 1회 점검 : 1점)	1

구분	평가지표			평가기준	배점
	2.2	정보통신시설의 출입관리	정보시스템이 운영되는 장소를 보호구역으로 지정하고 해당 구역의 출입통제 설비를 갖추는가?	정보시스템이 운영되는 장소는 권한이 있는 자만 출입할 수 있도록 출입통제가 이루어지고 있으며 출입내역을 기록하고 있다.	1
				정보통신시설이 운영되는 장소의 방문자 관리를 수행하고 있다. - 방문자 출입 시 사전 등록 관리 : 0.3점 - 담당직원 상시 동행 : 0.3점 - 외부 접견구역 별도 마련 : 0.4점	1
				정보통신시설이 운영되는 장소의 출입 및 활동은 영상정보처리기기를 통해 기록 및 모니터링 되고 있다.	1
				정보통신시설이 운영되는 장소에서 노트북, 서버, 저장매체, 스마트기기 등의 반출입 관리절차를 마련하고 내역을 관리하고 있다. - 서버 등의 자산 반출입 통제(0.3) - 노트북, HDD, 이동식 저장매체 반출입 통제(0.4) - 스마트기기 반입통제(0.3)	1
	2.3	사무실 보안	사무실의 물리적인 환경 보안을 위하여 비인가자 출입통제, 중요 문서 보관, 사무실 보안점검 등의 보호 조치가 이루어지는가?	사무실 내에 문서파기를 위한 파쇄기, 중요 문서보관을 위한 시건장치가 있는 캐비넷 등이 구비되어 있다.	1
				출입통제, 문서관리 등 사무실 보안규정을 수립하고 준수여부를 확인하기 위하여 정기적인 사무실 보안점검을 수행하고 있다. (반기 1회: 0.3점, 분기 1회: 0.6점, 월1회: 1점)	1
				중요 문서를 대량으로 보관하는 문서고 및 보안 필요성이 높은 중요 사무실은 출입이 허용된 인원만 출입할 수 있도록 통제하고 있다.	1
				복사, 출력, 팩스, 스캔, 파일공유 등을 위한 공용 사무기기는 비인가자가 접근할 수 없도록 통제하고 있다.	1
3. 기술적 보호활동	3.1	취약점 점검	정기적인 기술적취약점 점검을 수행하고 발견된 취약점의 개선조치를 수행하는가?	취약점 점검 주기, 점검대상, 수행주체, 점검항목, 수행방법 등을 포함한 취약점 점검계획을 수립하고 있다. - 점검대상 : 서비스와 관련된 네트워크, 서버, 데이터베이스 등의 정보시스템과 웹서버, WAS, 웹사이트 등의 응용프로그램을 모두 포함	1
				조직이 관리하고 있는 전체 정보시스템 및 서비스에 대한 연간 정보보호 취약점 점검을 수행하고 그 결과를 정보보호최고책임자에게 보고하고 있다. (주요자산 및 법적 요구관리가 필요한 시스템 : 0.5점, 전체시스템 : 1점)	1
				정보보호 취약점 점검은 전문성을 갖춘 인력이 수행하고 있다. (내부인력을 활용한 취약점 점검 : 0.5점 외부 전문가를 활용한 취약점 점검 : 1점)	1
				공개 웹서버 및 개인정보처리시스템 등의 주요 자산에 대해서는 연2회 이상 취약점 점검을 수행하고 있다.	1

구분	평가지표			평가기준	배점
				정보보호 취약점 점검 결과에 대한 개선조치를 수행하고 그 결과를 정보보호최고책임자에게 보고하고 있다. (80%이상: 0.5점, 90%이상: 0.7점, 98%이상: 1점) *※ 취약점 개선조치 내용의 적정성은 전문가 증명필요*	1
	3.2	정보보호 사고탐지 및 대응	해킹 또는 중요 정보 유출 등의 침해사고 발생 시 신속하게 탐지하고 대응할 수 있는 체계를 유지하는가?	침해사고를 탐지할 수 있는 정보보호 시스템을 운영하고 이벤트 기록을 유지하고 있다. - 침입차단시스템 도입(0.5점) - 그 외 침해사고 탐지를 위한 정보보호시스템 도입(0.5점)	1
				침해사고 대응을 위한 조직, 역할, 대응절차, 비상연락체계 등을 문서화하고 최신으로 유지하고 있다.	1
				해킹 또는 중요 정보 유출 등의 침해사고 발생을 대비하여 지속적인 정보시스템 모니터링을 수행하고 있다. (주간관제 : 0.5점, 24시간/365일 관제 : 1점)	1
				정보보호 사고유형에 따른 적합한 대응방안을 마련하고 있다. - 지능형 지속공격(APT 공격) - DDoS대응체계(DDoS대피소 이용 등) - 개인정보유출 - 그 외 신규공격 기법	1
				매년 침해사고 대응 체계를 점검할 수 있도록 모의훈련을 실시하고 훈련결과와 문제점에 대한 개선방안 및 조치결과를 정보보호최고책임자에게 보고하고 있다. (내부인력으로 자체 모의훈련 수행 : 0.5점, 외부 전문가를 활용한 모의훈련 수행 : 1점)	1
	3.3	시스템 개발 보안	시스템 개발 시 개발환경 보안 및 안전한 코딩 규칙 적용 등의 개발 보안 조치가 이루어지는가?	시스템 개발 시 최소한의 법적요구사항(암호화등)을 포함하여 보안요구사항을 정의하고 개발 시에 반영하고 있다.	1
				개발자는 안전한 코딩규칙을 적용할 수 있는 전문교육을 이수하였거나 안전한 코딩 규칙 적용 여부를 검사할 수 있는 점검도구를 사용하고 있다. - 안전한 코딩 교육이수(0.5점) - 코딩 규칙 점검도구 이용(0.5점)	1
				개발이 완료된 프로그램을 실 운영환경으로 이관하기 전 취약점 점검 및 조치를 수행하고 있다.	1
				개발서버(또는PC)와 운영서버를 분리구성하고 개발서버에는 개인정보등의 실제 운영하는 데이터가 아닌 시험 데이터를 이용하고 있다.	1

구분	평가지표			평가기준	배점
	3.4	네트워크 보안	네트워크 보안을 강화하기 위하여 침입차단, 네트워크분리, 인터넷차단 등의 대책을 강구하는가?	네트워크에 대한 비인가 접근을 통제하기 위해 유선네트워크 및 허용된 무선AP에 접속할 수 있는 PC, 노트북 등의 기기를 지정하여 운영하고 있다. 또한, 무선AP 사용 시 SSID, 안전한 암호화 전송(WPK2 이상) 등의 보안설정을 적용하여 운영하고 있다.	1
				개인정보 등 중요 정보를 대량으로 취급하는 서버와 해당 서버에 접근하는 단말PC 등에 대하여는 인터넷 차단 등의 조치를 수행하고 있다.	1
				침입차단시스템을 통해 내부망과 외부망을 분리하고 웹서버 등의 공개 서버에 대하여는 내부망과 분리된 DMZ를 구성하여 운영하고 있다.	1
				무선침입차단시스템 등을 통해 인가되지 않은 무선 AP사용을 탐지 및 차단하는 등의 조치를 수행하고 있다.	1
	3.5	정보시스템 및 응용프로그램 인증	정보시스템 및 어플리케이션에 대한 접근통제를 강화하기 위하여 접속단말 지정, 원격접근 통제, 사용자인증 강화 등의 대책을 적용하는가?	정보시스템 및 어플리케이션에 대한 관리자 및 사용자 접근시 복잡도, 길이 등을 고려한 안전한 비밀번호를 사용하며 주기적으로 비밀번호를 변경하고 있다. (반기 1회 : 0.5점, 분기 1회 : 1점) *※ 안전한 비밀번호 : 영문대문자, 영문소문자, 숫자, 특수문자 중 3종류 문자 조합 시 8자리 이상 , 2종류 조합 시 10자리 이상의 길이로 구성*	1
				정보시스템/어플리케이션의 식별 및 인증, 원격접근 등에 대한 보안정책 또는 지침이 수립되어 있다.	1
				정보시스템/어플리케이션 보안정책 또는 지침에 따른 준수사항(접근권한, 장기간미사용, 퇴직/휴직/직무변경 등 포함)을 정기적으로 점검하고 있다. (반기 1회 점검 0.5점, 분기 1회 점검 : 1점)	1
				개인정보 등 중요정보를 대량으로 취급하는 정보시스템/어플리케이션에 대한 접근 가능 권한은 관련법률 준수사항을 고려하여 별도의 인가절차를 거친 관리자에게만 부여하고 있다. (접속단말을 위한 PC를 지정, 1인 1계정 사용)	1
				정보시스템 및 어플리케이션에 관리자 등의 권한을 가진 계정으로 접속하는 경우 ID/ PW 이외에 일회용 패스워드, 인증서 등과 같은 강화된 사용자 인증 방법을 적용하고 있다. (인터넷 등 외부접속시만 적용: 0.5점, 모든 관리자 계정 접속시 적용: 1점)	1

구분	평가지표			평가기준	배점
	3.6	자료유출 방지	개인정보 등의 중요 정보 유출을 대비한 전송 및 저장 시 암호화, 정보유출 탐지 등의 대책을 적용하는가?	개인정보보호법 등 법률을 고려한 중요 정보의 전송 및 저장 시 암호화를 하고 있다.	1
				정보시스템 저장매체 및 휴대용 저장매체를 통한 중요정보 유출을 방지하기 위한 대책을 마련하고 있다. - 정보시스템 또는 이동형 저장매체의 폐기 또는 재사용시 저장매체에 기록된 중요정보는 복구 불가능하도록 완전삭제 수행(0.5) - 정보시스템 또는 이동형 저장매체의 분실시 자료유출 통제 방안 마련(0.5)	1
				내부자에 의한 중요정보의 정보유출을 차단, 탐지할 수 있는 보안시스템을 운영하고 있다. - 온라인 유출통제(0.2) : 네트워크DLP 등 - 오프라인 유출통제(0.2) : USB 매체통제, 엔드포인트 DLP 등 - 출력물 유출통제(0.2) : 출력물 보안(워터마킹) 등 - 기타 보안시스템(0.4) : DRM, VDI, 통합모니터링 등	1
				정보유출을 차단, 탐지할 수 있도록 보안시스템서버, 데이터베이스 등의 로그를 분석하여 오용, 남용 등으로부터 적극적인 대응을 하고 있다. (월1회 로그 점검 : 0.5점, 일일 또는 상시점검 : 1점)	1
	3.7	시스템 및 서비스 운영 보안	시스템 및 서비스 운영보안을 강화하기 위하여 정보시스템 보안패치, 서버 백신 설치, 운영로그의 기록 및 보관 등의 대책을 적용하는가?	서버 등의 시스템에 백신 설치, 패치, 인터넷 차단 등 악성코드에 대한 대책을 적용하고 있다.	1
				정보보호 시스템 유형별로 관리자 지정, 최신정책 업데이트, 룰셋변경, 이벤트 모니터링의 절차를 수립하여 현황을 관리하고 있다. - 정보보호 시스템의 룰셋 변경시 사전에 보안성을 검토하고 승인하는 절차를 수립하여 적용 - 최신 패턴 또는 SW 업데이트 현황을 파악하여 최신성을 유지 - 이벤트 모니터링 절차 수립	1
				정보시스템, 보안시스템 등 기록해야 할 로그의 유형을 정의하여 일정기간(최소 6개월 이상) 보존하고 있다.	1
				시스템 및 서비스의 운영(변경, 인수, 성능, 장애해결 등)의 절차를 명시적으로 수립하여 이행하고 있다.	1
				원격작업에 대한 대책을 마련하고 통제를 수행하고 있다.	1
	3.8	백업 및 IT 재해복구	IT재해재난 시 적시에 복구할 수 있도록 백업 소산 및 복구 절차가 있는가?	데이터 무결성 및 정보시스템 가용성 유지를 위한 백업 및 복구 절차를 수립하고 있으며 백업 대상 시스템과 백업대상 데이터를 정하여 정기적인 백업을 수행하고 있다.	1
				중요 백업 데이터를 비인가자의 접근으로부터 차단하고 외부 환경적인 위험으로부터 보호하기 위하여 내화금고 등에 안전하게 보관하고 있다.	1
				백업시스템을 이용한 실시간 백업 체계를 갖추고 중요 백업본은 일정거리 이상에 소산 백업을 실시하고 있다.	1

구분	평가지표			평가기준	배점
				백업 데이터를 활용하여 연 1회 이상의 재해 복구 훈련을 수행하고 있다. (연 1회 : 0.5점, 반기 1회 : 1점)	1
	3.9	PC 및 모바일 기기 보안	업무용 PC에 악성코드 감염을 차단하기 위한 보안대책이 적용되어 있는가?	자체점검을 수행할 수 있도록 PC관리 점검 사항을 정리하여 배포하고 있다.	1
				업무용 PC에 백신 설치 및 업데이트 설정, 로그인 패스워드, 운영체제 보안패치, 공유폴더 제거 등의 PC보안 조치 사항을 주기적으로 점검하고 있다. (분기별 1회 : 0.5점, 월별 1회 : 1점)	1
				PC보안조치 사항을 중앙에서 관리 및 적용할 수 있는 시스템을 구축하여 운영하고 있다. - 패스워드(0.25) - 공유폴더관리(0.25) - 백신 설치 및 자동 업데이트(0.25) - 패치관리(0.25)	1
				업무목적으로 사용하는 모바일 기기(노트북, 스마트폰, 스마트패드 등)에 대한 보안지침을 마련하고 이행하고 있다. - 기기에 대한 보안설정(비밀번호, 루팅금지 등) - 악성코드 방지 정책(백신설치 등) - 분실 및 도난 대응(분실시 데이터 삭제 등)	1

3) 선택지표(개인정보보호)

평가지표			평가기준	배점
1	개인정보 최소수집	개인정보 수집 목적에 따른 최소한의 개인정보를 수집하고 있는가?	개인정보의 수집목적에 따른 최소한의 개인정보를 수집하고 있으며 법령에서 허용하는 경우를 제외하고 주민등록번호를 수집·이용하지 않는다.	P
2	개인정보 수집 고지 및 동의획득	관련 법률에 따라 고지해야 할 사항을 명시적으로 알리고 동의를 받고 있는가?	개인정보 수집, 제3자 제공 및 위탁, 민감정보 수집, 고유식별정보 수집 등 법률에 따른 동의 및 별도 동의가 필요한 모든 사항에 대해 명시적으로 알리고 동의를 받고 있다.	P
		이용자의 동의 기록은 이용자가 탈퇴하여 관련 기록을 파기·폐기 전까지 안전하게 보관하고 있는가?	이용자의 동의 기록은 이용자가 탈퇴하여 관련 기록을 파기·폐기 전까지 안전하게 보관하고 있다.	P
3	개인정보 취급방침	수집 또는 관리하고 있는 개인정보 현황을 파악하여 개인정보취급(또는 처리)방침을 마련하고 게시하고 있는가?	법령에서 정하는 내용을 포함한 개인정보취급방침을 마련하고 이용자가 쉽게 확인할 수 있도록 고지하고 있다. 내용이 개정된 경우 개정 전 내용을 함께 확인할 수 있도록 한다.	P
4	이용자 권리 보호	이용자의 권리를 보호하기 위한 절차가 적용되어 있는가?	개인정보의 열람, 정정·삭제, 처리정지, 동의철회 요구를 받았을 때 지체 없이 필요한 조치를 취하고 있다.	P
5	개인정보의 관리적 보호조치	개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위한 관리적 보호조치를 적용하고 있는가?	개인정보관리/보호책임자(CPO)를 상근임원급 또는 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장으로 지정하고 있다.	P
			개인정보보호 관련 법령 및 고시에서 규정하는 사항을 포함한 개인정보 내부관리계획을 수립하여 시행하고 있다.	P
			개인정보취급자를 대상으로 법률에 따른 개인정보보호교육을 수행하고 있다. (정보통신망법: 연2회, 개인정보보호법: 연1회)	P
			개인정보 수탁사의 현황을 관리하고 있으며 계약서 상에 개인정보보호 관련 요건을 명시적으로 포함하고 있다.	P
			개인정보 수탁사에 대한 관리감독을 주기적으로 수행하고 있다. - 수탁사 개인정보취급자 목록 관리 - 수탁사 개인정보취급자에 대한 개인정보보호 서약서 징구 - 분기 1회 이상 점검 수행(교육수행 여부, 불필요한 개인정보 파기 여부 등) - 수탁사와의 계약 만료시 장비 반납, 계정 및 권한 말소, 개인정보 삭제 등의 보안조치	P
6	개인정보의 기술적 보호조치	개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위한 기술적 보호조치를 적용하고 있는가?	고유식별정보, 비밀번호 등은 법적 요구사항에 따라 안전한 알고리즘으로 암호화하고 있다.	P
			개인정보취급자의 접근권한은 업무수행에 필요한 최소한의 범위로 차등부여하고 권한 부여, 변경, 말소의 내역을 기록하여 법률에 따라 기록 보관을 하고 있다. (정보통신망법: 5년, 개인정보보호법: 3년)	P

평가지표			평가기준	배점
			개인정보처리시스템 접속 권한을 IP 주소 등으로 제한하고 있으며 외부에서 접속 시 공인인증서 등 안전한 인증수단을 적용하고 VPN, 전용선 등 안전한 접속수단을 사용하여 접근하고 있다.	P
			개인정보처리시스템의 접속기록은 6개월 이상 위·변조, 도난, 분실되지 않도록 안전하게 보관하고 있으며 법률에 따른 주기적인 점검을 하고 있다. (정보통신망법: 매월, 개인정보보호법: 반기 1회)	P
			개인정보처리자는 신종·변종을 포함한 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어를 설치하고 있으며 자동업데이트 기능 사용 또는 일1회 이상 업데이트를 실시하여 최신의 상태로 유지하고 있다.	P
			업무목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보를 마스킹하여 표시제한 조치를 취하고 있다.	P
			개인정보처리시스템에서 개인정보 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하여야 하며 출력항목을 최소화 하고 있다.	P
7	개인정보 파기	수집 목적이 달성된 개인정보는 지체 없이 파기하는가?	개인정보는 수집 목적이 달성 또는 종료되는 시점에 지체없이 파기한다. 단, 관련 법령 및 사전에 동의 받은 기간 동안은 보관할 수 있다.	P