〔별표 7〕 인증평가 일부 생략의 범위(제11조 관련)

< 제11조제1항제1호에 따른 일부 생략 신청 시 생략의 범위 >

분야		항목
2. 인적보안	2.1. 내부인력 보안	2.1.1. 고용계약
		2.1.3. 직무 분리
		2.1.4. 비밀유지서약서
	2.2. 외부인력 보안	2.2.1. 외부인력 계약
		2.2.2. 외부인력 보안 이행 관리
		2.2.3. 계약 만료 시 보안
	2.3. 정보보호 교육	2.3.1. 교육 프로그램 수립
		2.3.2. 교육 시행
		2.3.3. 평가 및 개선
3. 자산관리	3.1. 자산 식별 및 분류	3.1.1. 자산 식별
		3.1.2. 자산별 책임할당
		3.1.3.보안등급 및 취급
5. 침해사고관리	5.1. 침해사고 대응 절차 및 체계	5.1.1. 침해사고 대응절차 수립
		5.1.2. 침해사고 대응체계 구축
	5.2. 침해사고 대응	5.2.1. 침해사고 보고
		5.2.2. 침해사고 처리 및 복구
	5.3. 사후관리	5.3.1. 침해사고 분석 및 공유
		5.3.2. 재발방지
6. 서비스연속성관리	6.1. 장애대응	6.1.1. 장애 대응절차 수립
		6.1.2. 장애 보고
		6.1.3. 장애 처리 및 복구
		6.1.4. 재발방지
	6.2. 서비스 가용성	6.2.1. 성능 및 용량 관리
8. 물리적 보안	8.1. 물리적 보호구역	8.1.1. 물리적 보호구역 지정
		8.1.2. 물리적 출입통제
		8.1.3. 물리적 보호구역 내 작업

		8.1.5. 공공장소 및 운송 · 하역구역 보호
		8.1.6. 모바일 기기 반출 · 입
	8.2. 정보처리 시설 및 장비보호	8.2.1. 정보처리시설의 배치
		8.2.2. 보호설비
		8.2.3. 케이블 보호
		8.2.4. 시설 및 장비 유지보수
		8.2.5. 장비 반출 · 입
		8.2.6. 장비 폐기 및 재사용
9. 가상화 보안	9.1. 가상화 인프라	9.1.5. 공개서버 보안
10. 접근통제	10.1. 접근통제 정책	10.1.1. 접근통제 정책 수립
10. 접근통제	10.2. 접근 권한 관리	10.2.2. 관리자 및 특수 권한관리
		10.2.3. 접근권한 검토
	10.3. 사용자 식별 및 인증	10.3.1. 사용자 식별
		10.3.2. 사용자 인증
		10.3.3. 강화된 인증 수단 제공
		10.3.4. 사용자 패스워드 관리
		10.3.5. 이용자 패스워드 관리
11. 네트워크 보안	11.1. 네트워크 보안	11.1.1. 네트워크 보안 정책 수립
		11.1.2. 네트워크 모니터링 및 통제
		11.1.3. 네트워크 정보보호시스템 운영
		11.1.5. 네트워크 분리
		11.1.6. 무선 접근통제
12. 데이터 보호 및 암호화	12.2. 매체 보안	12.2.1. 저장매체 관리
		12.2.2. 이동매체 관리
	12.3. 암호화	12.3.1. 암호 정책 수립
		12.3.2. 암호키 관리
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	13.1.1.보안요구사항정의
		13.1.2. 인증 및 암호화 기능
		13.1.3. 보안로그 기능
		13.1.4. 접근권한 기능

		13.1.5. 시각 동기화
	13.2. 구현 및 시험	13.2.1. 구현 및 시험
		13.2.3.시험 데이터 보안
		13.2.4.소스 프로그램 보안
	13.3. 외주 개발 보안	13.3.1. 외주 개발 보안
	13.4. 시스템 도입 보안	13.4.1.시스템 도입 계획
		13.4.2. 시스템 인수

< 제11조제1항제2호에 따른 일부 생략 신청 시 생략의 범위 >

분야		항목
1. 정보보호 정책 및 조직	**1.1.정보보호 정책**	**1.1.1. 정보보호 정책 수립**
		1.1.2. 정보보호 정책 검토 및 변경
		1.1.3. 정보보호 정책문서 관리
	1.2.정보보호 조직	**1.2.1. 조직 구성**
		1.2.2. 역할 및 책임 부여
2. 인적보안	2.1. 내부인력 보안	2.1.1. 고용계약
		2.1.3. 직무 분리
		2.1.4. 비밀유지서약서
	2.3. 정보보호 교육	2.3.2. 교육 시행
4서비스 공급망 관리	4.1. 공급망관리 정책	4.1.1. 공급망 관리 정책 수립
5. 침해사고관리	5.1. 침해사고 대응 절차 및 체계	5.1.1. 침해사고 대응절차 수립
	5.2. 침해사고 대응	5.2.1. 침해사고 보고
		5.2.2. 침해사고 처리 및 복구
	5.3. 사후관리	5.3.1. 침해사고 분석 및 공유
		5.3.2. 재발방지
6. 서비스연속성관리	6.1. 장애대응	6.1.1. 장애 대응절차 수립
		6.1.2. 장애 보고
		6.1.3. 장애 처리 및 복구
		6.1.4. 재발방지

7. 준거성	7.1. 법 및 정책 준수	7.1.1. 법적요구사항 준수
		7.2.1. 독립적 보안감사
9. 가상화 보안	9.1. 가상화 인프라	9.1.1.가상자원 관리
11. 네트워크 보안	11.1. 네트워크 보안	11.1.1. 네트워크 보안 정책 수립
12. 데이터 보호 및 암호화	12.1. 데이터 보호	12.1.1. 데이터 분류
		12.1.2. 데이터 소유권
		12.1.5. 데이터 추적성
		12.1.6. 데이터 폐기
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	13.1.1.보안요구사항정의
		13.1.2. 인증 및 암호화 기능
		13.1.4. 접근권한 기능
	13.2. 구현 및 시험	13.2.1. 구현 및 시험
		13.2.3.시험 데이터 보안
		13.2.4.소스 프로그램 보안
	13.3. 외주 개발 보안	13.3.1. 외주 개발 보안