

<별표7> 망분리 대체 정보보호통제 <개정 2020. 11. 6., 2022. 12. 29., 2025. 2. 5.>

구분	통제 사항		
공통	○ 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료 ○ 지능형 해킹(APT)차단 대책 수립·적용 ○ 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링		
메일 시스템	○ 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용 ○ 메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용		
업무용 단말기	○ 사용자의 관리자 권한 제거 ○ 승인된 프로그램만 설치·실행토록 대책 수립·적용 ○ 전산자료 저장 시 암호화		
연구·개발	○ 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립·적용 ○ 연구·개발망과 내부망간 독립적인* 네트워크 구성 * 다만, 연구개발망과 규정 제15조제1항제3호의 내부 업무용시스템간 연결에 한하여 논리적 방식으로 분리 가능 ○ 연구·개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보(고유 식별정보, 개인신용정보 등) 처리여부 모니터링 ○ 연구·개발망의 침해사고 예방 및 사고대응 대책 수립·적용 ○ 중요 소스코드 등에 대한 외부 반출방지 및 망간 전송* 허용 등에 따른 보안관리 대책 수립·적용 * 다만, 연구개발망과 규정 제15조제1항제5호의 전산실간 전송시 개발산출물 등 필수적인 경우에 한함		
원격 접속	외부 단말기	공통	○ 백신 프로그램 설치, 실시간 업데이트 및 검사 수행 ○ 안전한 운영체제 사용 및 최신 보안패치 적용 ○ 로그인 비밀번호 및 화면 보호기 설정 ○ 화면 및 출력물 등으로 인한 정보유출 방지대책 적용
		업무용 단말기를 경유하여 내부망에 접속하는 경우 (간접접속)	○ 외부 단말기와 업무용 단말기의 파일 송·수신 차단
		외부 단말기에서 내부망에 직접 접속하는 경우 (직접접속)	○ 인가되지 않은 S/W 설치 차단 ○ 보안 설정 임의 변경 차단 ○ USB 등 외부 저장장치 읽기/쓰기 차단 ○ 전산자료 (파일, 문서) 암호화 저장 ○ 단말기 분실 시 정보 유출 방지 대책적용 (하드디스크 암호화, CMOS비밀번호 적용 등)
	내부망 접근통제	○ 업무상 필수적인 IP, Port에 한하여 연결 허용 ○ 원격접속 기록 및 저장(예: 접속자 ID, 접속일자, 접속 시스템 등)	
	인증	○ 이중 인증 적용(예: ID/PW + OTP) ○ 일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단	
	통신 회선	○ 안전한 알고리즘으로 네트워크 구간 암호화 ○ 내부망 접속시 인터넷 연결 차단 (단, 직접 내부망으로 접속하는 외부 단말기는 인터넷 연결 상시 차단) ○ 원격 접속 후 일정 유희시간 경과 시 네트워크 연결 차단	
	기타	○ 원격접속자에 대한 보안서약서 징구 ○ 공공장소에서 원격 접속 금지	