디지털복합기 도입·운용가이드 : 보안기능 점

*** 본 보안기능 점검 사항에서 디지털복합기는 다음 조건을 모두 만족하는 디지털 사무용 기기를 의미한다.**
- 인쇄(프린트), 복사, 스캔, 팩스 기능 중 2가지 이상의 기능을 제공
- 전자문서 저장용 비휘발성 저장매체(HDD, SSD 등)를 내장하고 있거나 별도 구매를 통해 장착할 수 있는 기기. 단, 비휘발성 저장매체는 디지
자문서가 유지되는 모든 저장매체를 의미
*** 단일 기능만을 제공하더라도 인쇄물을 전자 문서화하거나 그 반대의 기능을 제공하는 모든 디지털 사무용 기기는 본 가이드를 활용하여 점검하**
한 CC인증 여부는 향후 점진적으로 적용할 예정임

□ 사용자 데이터 보호

소항목	번호	점검 사항	확인 사항
잔여 정보 보호	R01	o 디지털복합기는 비휘발성 저장매체에 저장되는 전자문서에 대한 완전삭제 또는 데이터 암호화 기능을 제공해야 한다.	o 완전삭제 기능 지원 확인(*예시: 지원 ○, 미지원 ×*) - 하드디스크(HDD)의 경우, 완전포맷 1회 수행(저장매체를 '난수'로 중복 저장하는 방식(덮어쓰기하는 방식)으로 삭제하는 방법)(*예시: 지원 ○, 미지원 ×*) 또는 완전포맷 1회 수행보다 완전삭제 강도가 높은 방법( ) - 하드디스크(HDD)를 제외한 기타 비휘발성 저장매체의 경우 CC 인증에서 인증한 완전삭제 기능 o 데이터 암호화 기능 지원 확인(*예시: 지원 ○, 미지원 ×*)

□ 업데이트 및 백업

소항목	번호	점검 사항	확인 사항
펌웨어 업데이트	R02	o 디지털복합기는 펌웨어 업데이트 기능을 제공해야 한다.	o 디지털복합기의 펌웨어 업데이트 기능 지원 확인(*예시: 지원 ○, 미지원 ×*)

□ 감사기록

소항목	번호	점검 사항	확인 사항
감사기록 생성 기능	R03	o 디지털복합기는 주요 감사사건에 대해 감사기록을 생성하는 기능을 제공해야 한다. 주요 감사사건은 도입기관의 보안정책을 따른다.	o 생성되는 감사기록의 종류 확인(*예시: 관리자 로그인, 작업(출력, 복사, 스캔, 팩스 등)의 형태와 일시 등*)
감사기록 내 포함 정보	R04	o 디지털복합기의 각 감사기록에는 최소한 다음의 정보가 포함되어야 한다. - 사건 발생 일시 - 사건 유형 - 사건을 발생시킨 주체의 신원(가능한 경우) - 작업 내역 및 결과(성공/실패) - 기타 추가적인 정보	o 각 감사기록이 포함하는 정보 확인 - 사건 발생 일시(*예시: 지원 ○, 미지원 ×*) - 사건 유형( ) - 사건을 발생시킨 주체의 신원(가능한 경우)( ) - 작업 내역 및 결과(성공/실패)( ) - 기타 추가적인 정보(*예시: 작업의 형태, 관리자 또는 사용자의 식별 정보 등*) o 다음 감사기록은 명시한 정보가 감사기록에 추가로 포함되는지 확인 - 작업(출력, 복사, 스캔 등)의 시작 또는 완료 : 작업의 형태(*예시: 지원 ○, 미지원 ×*) - 관리자 또는 사용자에 대한 식별 및 인증 성공/실패 : 관리자 또는 사용자의 식별정보(가능한 경우)( )
감사기록 조회 기능	R05	o 디지털복합기는 제품 구성요소로부터 생성된 모든 감사기록을 인가된 관리자가 해석할 수 있는 방법으로 조회할 수 있는 기능을 제공해야 한다.	o 인가된 관리자의 감사기록 조회 기능 존재 여부 확인(*예시: 지원 ○, 미지원 ×*) o 감사기록의 해석 가능 여부 확인(*예시: 지원 ○, 미지원 ×*)
감사기록 조회 제한	R06	o 디지털복합기는 명시적으로 사용자에게 감사기록을 조회할 수 있는 권한이 주어지는 경우를 제외하고는 사용자가 감사기록을 조회하는 것을 금지하는 기능을 제공해야 한다.	o 사용자의 감사기록 접근 제한 여부 확인(*예시: 제한 ○, 미제한 ×*)

감사기록 검색 기능	R07	o 디지털복합기는 AND, OR 등 논리적 관계 기준에 따른 선택적인 검토가 가능한 감사기록 검색 기능을 제공해야 한다.	o 사용자가 감사기록을 검색하거나 분류된 항목에서 선택적으로 조회가 가능한지 확인(*예시: 지원 ○, 미지원 ×*)
저장 감사기록의 설정 용량 초과 시 대응 기능	R08	o 디지털복합기는 감사기록 저장 용량 포화 시 적절한 방법(예 : 오래된 감사 레코드 덮어쓰기 등)으로 저장 실패에 대응하는 기능을 제공해야 한다.	o 감사기록 저장 용량 포화 시 대응 기능 지원 확인(*예시: 지원 ○, 미지원 ×*) o 포화 시 대응방법 서술(*예시 : 오래된 감사 레코드 덮어쓰기 등*)
감사기록 보호 기능	R09	o 디지털복합기는 저장된 감사기록 내 일부 내용에 대해 비인가된 삭제 및 변경이 발생하지 않도록 보호하는 기능을 제공해야 한다.	o 감사기록의 비인가된 삭제 및 변경 방지 기능 지원 확인 - 인가된 관리자에게만 감사기록 삭제 및 변경 기능 제공 여부(*예시: 지원 ○, 미지원 ×*)
감사기록 생성 시 신뢰할 수 있는 시간 참조 기능	R10	o 디지털복합기는 주요 사건에 대한 정확한 시간 정보 생성을 위해 신뢰된 OS 등을 이용하여 시간 정보를 생성하는 기능을 제공해야 한다. (예시) - 디지털복합기 자체의 시간 정보 - NTP 서버의 시간 정보	o 시간정보 생성 출처 확인(해당 항목에만 결과 표시) - 디지털복합기 자체의 시간 정보(*예시: 지원 ○, 미지원 ×*) - NTP 서버의 시간 정보( ) - 기타( )
잠재적인 보안위반 탐지 시 대응 행동	R11	o 디지털복합기는 보안 위반을 탐지한 경우, 인가된 관리자가 설정한 대응행동(예 : 알람, 관리자 웹페이지 메시지 등)을 수행하는 기능을 제공해야 한다.	o 지원하는 대응방법 및 기준 확인(해당 항목에만 결과 표시) - 보안위반 기준(*예시: 무결성 검사 결과 실패 발생 시*) - 대응 방법(*예시: 알람, 관리자 웹페이지 메시지 등*)

□ 식별 및 인증

소항목	번호	점검 사항	확인 사항
식별 및 인증 기능	R12	o 디지털복합기는 관리자 또는 사용자의 신원을 검증하기 위해 식별 및 인증 기능을 제공해야 하며, 관리자 또는 사용자가 해당 식별 및 인증을 성공적으로 통과해야만 디지털복합기의 기능을 사용할 수 있도록 제한하는 기능을 제공해야 한다. - 단, 관리자 또는 사용자가 식별 및 인증을 성공적으로 완료하기 전에 팩스의 수신, 기기 정보, 작업의 진행 현황 확인 등 보안과 관련이 없는 메뉴의 사용(전자문서의 배출은 보안과 관련된 행동임) 등은 허용할 수 있다.	o (기기자체 또는 원격에서) 관리자 또는 사용자 식별 및 인증 기능 지원 방법 확인(해당 항목에만 결과 표시) - 패널(디지털복합기의 터치패드 또는 버튼 등)(*예시: 지원 ○, 미지원 ×*) - 스마트카드( ) - 생체인식( ) - HTTPS( ) - SNMP( ) - 기타( )
인증 실패 대응 기능	R13	o 디지털복합기는 관리자 또는 사용자 인증 실패가 기본값 또는 설정된 횟수(기본값 5회 이하)에 도달하면, 기본값 또는 설정된 시간(기본값 5분 이상) 동안 식별 및 인증 기능이 비활성화되는 기능을 제공해야 한다.	o 관리자 또는 사용자 인증 실패 시 대응 기능 확인 - 인증 실패 허용 횟수(5회 이하)(*예시: 지원 ○, 미지원 ×*) - 인증 실패 시 식별 및 인증 기능 비활성화 시간(5분 이상)( )

비밀번호 변경 및 안전한 설정 기능	R14	o 디지털복합기는 기존 모든 비밀번호(뿐만 아니라, PIN 등 기존 모든 인증 정보 중 비밀값에 해당하는 정보)에 대한 변경 기능을 제공해야 하며, 비밀번호 신규 등록 및 기존 비밀번호 변경 시 영문 알파벳 대문자/영문 알파벳 소문자/숫자/특수문자 중 3가지 이상의 규칙 조합이 가능하고 9자리 이상으로 구성할 수 있는 기능을 제공해야 한다. 또한, 디지털복합기는 미래의 비밀번호 안전성을 위해 15자리 이상의 비밀번호 구성을 지원하는 기능을 제공할 것을 권고한다.	o 제품이 지원하는 대상 별 기능 지원 확인(해당 항목에만 결과 표시) - 관리자 비밀번호(*예시: 지원 ○, 미지원 x*) - 일반 사용자 비밀번호( ) - 인증서버, 파일서버 등 연동 지원시 사전공유키( ) - SNMP v3 지원시 SNMP 인증(authentication) 비밀번호( ) - SNMP v3 지원시 SNMP 암호화(privacy) 비밀번호( ) - 기타( )
인증 피드백 보호 기능	R15	o 디지털복합기는 인증이 진행되는 동안 인증정보가 노출되지 않도록 관리자 또는 사용자에게 비밀번호를 보여주지 않거나 다른 형태의 문자 또는 도형으로 변형하여 보여주는 기능을 제공해야 한다. (예시) -"••••••••", "*********" 등	o 비밀번호 등의 인증정보를 입력하는 경우 입력한 비밀번호가 보이지 않거나 "••••••••", "*********" 등으로 변환되어 보이는지 확인(*예시: 보이지 않거나 변환되어 보이는 경우 ○, 비밀번호가 그대로 보이거나 비밀번호를 유추할 수 있는 경우 x*)
	R16	o 디지털복합기는 식별 및 인증 실패 시, 실패 이유(예 : ID 오류, 비밀번호 오류 등)를 식별 및 인증 정보를 입력한 관리자 또는 사용자에게 제공하지 않아야 한다.	o 식별 및 인증 실패 시 실패 이유를 알려주는지 확인(*예시: 식별 및 인증 실패 이외의 어떠한 실패 이유도 알려주지 않는 경우 ○, "해당 ID 없음", "비밀번호 불일치" 등의 이유를 알려주는 경우 X*)
인증데이터 보호 기능	R17	o 디지털복합기의 관리자 및 사용자 비밀번호가 제품에 하드코딩 되거나 평문(단순 인코딩 포함)으로 저장되지 않아야 한다.	o 제품이 지원하는 대상 별 기능 지원 확인(해당 항목에만 결과 표시) - 관리자 비밀번호(*예시: 지원 ○, 미지원 x*) - 일반 사용자 비밀번호( )

	R18	o 디지털복합기는 관리자 및 사용자의 인증정보가 재사용되는 것을 방지(예 : 타임스탬프 사용 등)하는 기능을 제공해야 한다.	o 관리자 및 사용자의 인증정보가 재사용되는 것을 방지하는 기능 지원 확인(*예시: 지원 ○, 미지원 x*)

□ 보안관리

소항목	번호	점검 사항	확인 사항
보안관리 기능	R19	o 디지털복합기는 인가된 관리자만 보안기능, 보안정책 및 중요 데이터 등을 설정 및 관리할 수 있는 보안관리 기능을 제공해야 한다.	o 장비가 지원하는 보안관리 기능 확인(*예시: 네트워크 서비스 설정, 비밀번호 변경 등*)
접속가능 IP 제한 기능	R20	o 디지털복합기는 사전 등록된 IP주소의 관리 콘솔만 관리 서버에 접속할 수 있도록 제한하는 기능을 제공해야 한다.	o 기능 지원 확인(해당 항목에만 결과 표시) - HTTPS( )(*예시: 지원 ○, 미지원 x*) - SNMP( ) - 기타( )

□ 전송데이터 보호

소항목	번호	점검 사항	확인 사항
전송 데이터 안전성 보장 기능	R21	o 디지털복합기는 관리자의 웹브라우저를 이용한 접속 등 디지털복합기와 연결된 모든 통신 수단에 대해 안전한 암호통신 프로토콜 제공해야 한다.	o 기능 지원 확인(해당 항목에만 결과표시) - HTTPS(*예시: 지원 ○, 미지원 x*) - IPsec( ) - 기타(*TLS V1.2 등*)

□ 자체시험

소항목	번호	점검 사항	확인 사항
자체시험 기능	R22	o 디지털복합기는 제품의 정확한 운용을 보장하기 위해 시동 시 또는 정규 운용 동안 주기적으로 또는 인가된 관리자가 요구 시 자체시험 기능을 제공해야 한다.	o 대상별 자체시험 기능 지원 확인(*예시: 지원 ○, 미지원 x*)

무결성 검사 기능	R23	o 디지털복합기는 인가된 관리자가 실행 가능한 코드의 무결성을 검증할 수 있는 기능을 제공해야 한다. (예시) - 펌웨어 등	o 사용 암호 알고리즘(*예시: SHA-256*) o 대상별 기능 지원 확인(해당 항목에만 결과 표시) - 펌웨어(*예시: 지원 ○, 미지원 x*) - 기타( )
	R24	o 디지털복합기는 장비가 수행한 무결성 검사 내용 및 결과를 관리자가 확인할 수 있는 기능을 제공해야 한다. (예시) - 패널 출력 - 감사데이터 생성 등	o 대상별 기능 지원 확인(해당 항목에만 결과 표시) - 패널 출력(*예시: 지원 ○, 미지원 x*) - 감사데이터 생성( ) - 기타( )
	R25	o 디지털복합기는 관리자가 R23)의 무결성 검사를 직접 실행하는 기능을 제공해야 한다.	o 기능 지원 확인(*예시: 지원 ○, 미지원 x*)

□ 안전한 세션관리

소항목	번호	점검 사항	확인 사항
세션 잠금/종료 기능	R26	o 디지털복합기는 관리자가 일정 시간(기본값 10분 이하) 동안 동작이 없을 경우, 세션을 잠거나 종료하는 기능을 제공해야 한다.	o 서비스 별 기능 지원 확인(해당 항목에만 결과 표시) - 패널(*예시: 지원 ○, 미지원 x*) - HTTPS( ) - SNMP( ) - 기타( ) o 기본값 혹은 설정값(*예시: 기본값 10분*)