디지털복합기 운용 점검사항 V2.0

*** 기관 담당자가 직접 작성하시기 바랍니다.**
*** 다음 조건을 만족하는 디지털 사무용 기기가 운용 점검사항 대상임.**
- 전자문서 저장용 비휘발성 저장매체(HDD, SSD 등)를 내장하고 있거나 별도 구매를 통해 장착할 수 있는 기기.
*** 위의 조건을 만족하지 못하는 기기(예: 소형 프린터)는 대상이 아니므로 자유롭게 도입 가능(운용 점검사항 적용과 도입 확인서 제출 불필요)**

기관명	
제품명	
작성자	

도입 시 점검 사항

□ 형상 관리

소항목	점검사항	확인사항	확인
CC 인증 제품 확인	o 국내 CC 인증 제품은 인증서 또는 IT보안인증사무국 홈페이지 (https://itscc.kr) 인증제품 목록을 통해 제품의 인증 현황을 확인해야 한다. o 국제 CC 인증 제품은 CC 인증서 또는 국제 CC 홈페이지 (https://www.commoncriteriaportal.org) 인증제품 목록을 통해 제품의 인증 현황을 확인해야 한다.	o CC 인증서 확인 - 제품명 - 인증일 / 만료일 - 보증등급 - 인증번호 o 인증제품 형상 확인 - 인증제품명 - 구성요소 식별 및 세부버전	

□ 보안기능

소항목	점검사항	확인사항	확인

보안기능 확인	o 관리자는 도입한 디지털 복합기가 전자문서 완전삭제 또는 암호화 저장 기능이 있는지 확인해야 한다.	디지털 복합기 CC인증보고서에서 완전삭제(Image Overwrite) 또는 데이터 암호화(HDD Encryption) 기능 보유여부를 확인한다.	

운용 시 점검 사항

□ 저장 및 전송데이터 보호

소항목	점검사항	확인사항	확인
잔여 정보 보호	o 디지털복합기 비휘발성 저장매체에 전자문서를 저장하는 기능을 사용한다면, 관리자는 다음 중 한가지 이상의 방법으로 사용하도록 설정해야한다. - 각 작업 간에 비휘발성 저장매체에 저장된 전자문서 완전삭제 - 비휘발성 저장매체에 전자문서 암호화 저장	완전삭제(Image Overwrite) 또는 데이터 암호화(HDD Encryption) 기능 활성화여부 확인	
공유 저장소 사용 제한 및 접근제어	o 관리자는 디지털복합기의 공유 저장소에 스캔된 전자문서 등이 저장되지 않도록 설정해야 한다. 특히, 임의의 파일을 업로드 또는 다운로드할 수 있는 공유 저장소를 사용하지 않아야 한다. o 안전한 접근제어 기능(비밀번호, PIN 등)을 제공하는 경우 스캔된 전자문서를 PC에 직접 전송하거나(공유폴더는 사용 금지) 파일서버로 전송하여 관리할 수 있다. - 전송시마다 비밀번호 혹은 PIN 등의 인증 기능 제공 필요 - 단, 이 경우 내부망에서만 연결하여 사용하여야 하며 외부망에서는 사용할 수 없다. o 디지털복합기에 외부의 공유저장소로 전자문서를 전송시 사용하는 사용자 인증 정보가 저장되어 있는 경우 외부의 공유저장소로의 전자문서 전송 기능을 사용하기 전 사용자 인증을 수행하여 전송하도록 설정 운용하여야 한다.	o 안전한 접근제어 기능(비밀번호, PIN 등)을 제공하는 경우 전송시마다 비밀번호 혹은 PIN 등의 인증 설정여부 확인 o 디지털복합기에 외부의 공유저장소로 전자문서를 전송시 사용하는 사용자 인증 정보가 저장되어 있는 경우 외부의 공유저장소로의 전자문서 전송 기능을 사용하기 전 사용자 인증을 수행하여 전송하도록 운용	

전송데이터 암호화	o 관리자 및 사용자는 인쇄 또는 스캔한 전자문서의 전송 등 디지털복합기와 디지털복합기 외부의 타 IT개체(사용자 PC, 파일서버 등) 간에 중요 문서를 송수신하는 경우 전자문서를 암호화 또는 IPsec 등의 암호화 채널을 이용하여 전송할 것을 권고한다.	o 스캔된 전자문서 등을 별도의 공유 저장소로 전송하는 경우는 전자문서를 암호화하거나 IPsec 등의 암호화 채널을 이용하여 전송여부 확인	

□ 시스템 구성

소항목	점검사항	확인사항	확인
내부망과 인터넷망 분리	o 관리자는 디지털복합기가 내부망와 인터넷망을 유무선 구분 없이 혼용하여 사용하지 않도록 구성해야 한다. - 디지털복합기의 2개 이상의 유무선 네트워크 인터페이스(유선 LAN, Wi-Fi AP를 이용한 중계 연결, Wi-Fi 직접 연결 등)를 활용하여 내부 네트워크와 외부 네트워크를 동시에 연결하지 않도록 한다. - 1대의 스위치에 내부 네트워크와 외부 네트워크를 연결한 후 해당 스위치를 디지털복합기에 연결하지 않도록 한다.(디지털복합기 외부에서 내부 네트워크와 외부 네트워크가 혼용된 경우로서 원칙적으로 불허함) - 기타 내부 네트워크와 외부 네트워크를 혼용하여 사용하지 않도록 한다.	o 내부망와 인터넷망을 분리하여 디지털복합기 설치 확인 o 디지털복합기의 불필요한 네트워크 인터페이스(Bluetooth, Wi-Fi 등)는 봉인 또는 분리하거나 사용하지 않도록 설정 확인	
디지털복합기의 위치	o 관리자는 디지털복합기를 라우터, 스위치, 또는 방화벽 뒤에 위치시키고, 임의적 접근통제 정책(Discretionary Access Control)을 적용해야 한다.	o 라우터, 스위치 또는 방화벽으로 **디지털 복합기** 통신을 통제 가능한 위치에 설치	
고정 IP 사용	o 관리자는 디지털복합기에 고정 IP 주소만을 할당해야 한다.	o 디지털복합기에 고정 IP 주소를 할당한다.	
출력 포트	o 관리자는 디지털복합기의 출력 서비스가 9100번 포트 또는 LPD(515번 포트) 또는 IPP(631번 포트)를 통해서만 이루지도록 설정해야 한다.	o 디지털복합기의 출력 서비스가 9100번 포트 또는 LPD(515번 포트) 또는 IPP(631번 포트) 이외의 포트에서는 불가능하도록 설정한다.	

□ 시스템 운용

소항목	점검사항	확인사항	확인
불필요 네트워크 서비스 제거	o 관리자는 디지털복합기에 불필요한 서비스가 사용되지 않도록 설정해야 한다. 이를 위해 관리자는 다음 2가지 내/외부 점검 결과를 비교하여 불필요한 서비스를 제거해야 한다. - (내부) 디지털복합기의 관리 페이지 또는 관리자 메뉴에서 허용한 네트워크 서비스를 확인한다. - (외부) nmap 등 포트 스캐닝 도구를 이용하여 디지털복합기 외부에서 오픈된 네트워크 서비스를 확인한다.	o 불필요한 서비스가 존재하는 경우 비활성화하도록 설정한다. o 디지털복합기 (외부)에서 점검한 결과, (내부)에서 허용한 네트워크 서비스가 아닌 네트워크 서비스가 열려있는 경우 백도어일 수 있으므로 즉시 확인 후 조치를 취한다.	
통신 프로토콜	o TCP/IP 이외의 프로토콜은 사용하지 않아야 한다.	o TCP/IP 이외의 프로토콜이 활성화되어 있는지 확인한다.	
SNMP 운용	o 관리자는 SNMP V1, V2에 대해 읽기 권한만 허용하도록 설정해야한다.	o 디지털복합기 상태 등 정보를 확인하기 위한 용도로 사용할 경우 SNMP V1, V2의 읽기 권한만 허용하도록 사용해야 한다.	
	o SNMP를 지원하는 경우 V3 이상을 사용해야 한다.	o SNMP V3 사용 확인	
	o SNMP 비밀번호는 안전한 비밀번호 기준에 맞게 관리자가 지정하여 운용해야 한다.	o 안전한 SNMP 비밀번호 지정 확인	
제품 업데이트	o 관리자는 디지털복합기를 취약점이 없는 버전의 펌웨어로 업데이트하여 운용할 것을 권고한다.	o 디지털복합기의 펌웨어 버전을 확인하고, 취약점이 존재하는 펌웨어의 경우 취약점이 없는 버전의 펌웨어로 업데이트한다.	
	o 디지털복합기 업데이트 시 디지털복합기 개발업체로부터 안전한 방식(오프라인 등)으로 업데이트 데이터를 제공받아야 한다.	o 신원이 확인된 설치기사가 직접 방문 등 신뢰된 채널을 통해서 제공받아 안전한 방식으로 업데이트해야 한다.	
이동식 저장매체 사용 제한	o USB, Flash 드라이브 등의 이동식 저장 매체는 디지털복합기에 연결하여 사용하지 않고, 디지털복합기의 사용하지 않는 USB 포트는 봉인한다. 특히, 인터넷에서 사용하는 이동식 저장 매체를 내부 업무망에 연결된 디지털복합기에 연결하지 않도록 하여야한다.	o 부득이하게 이동식 저장매체를 디지털복합기에 연결하여 사용하기 위해서는 이동식 저장매체에 대한 악성코드 감염여부 확인, 전자문서의 암호화 저장 등 별도의 보안조치를 취한 후 사용하여야 한다. o 이동식 저장매체를 사용한 경우 사용 내역을 남기고, USB 포트를 다시 봉인해야 한다.	
인터넷망에서의 작업 제한	o 인터넷망에서 저장 또는 송신이 허용되지 않은 문서는 인터넷에 연결된 디지털복합기에서 복사, 스캔을 수행하지 않도록 해야 한다.	o 인터넷망에서 저장 또는 송신이 허용되지 않은 문서(즉, 내부에서만 사용 가능한 문서)는 내부망에 연결된 디지털복합기에서만 복사, 스캔을 수행해야 한다.	
외부 네트워크에서의 데이터 전송 제한	o 외부 네트워크에 연결된 디지털복합기에서 스캔한 전자문서를 이메일로 전송하는 기능(Scan to SMTP) 또는 외부로부터 수신한 전자문서를 별도의 처리 없이 외부로 재전송하는 기능을 사용하지 않아야 한다.	o 외부 네트워크에 연결된 디지털복합기의 이메일 전송 기능(SMTP) 비활성화 확인	

□ 관리자 운용

소항목	점검사항	확인사항	확인
전송 데이터 보호	o 디지털복합기에 관리자로 접근 가능한 모든 인터페이스를 확인하고 반드시 필요한 인터페이스만 사용해야 한다.	o 원격에서 접근가능한 인터페이스(무선은 사용 금지) 외부 접근 가능여부 확인 o 기기 자체(로컬)에서 접근가능한 인터페이스(키패드, 터치스크린 등)는 접근 비밀번호 설정 등 확인	
	o 암호 통신에 사용되는 암호알고리즘의 보안강도는 112비트 이상을 만족해야 한다.	o 암호 통신에 사용되는 암호 알고리즘 확인 - 해시 : SHA-224 이상 - 대칭키 암호 : 키 길이 128bit 이상 - 공개키 암호 : RSA 2048 이상, DSA(2048, 224) 이상 - 전자서명 : RSA-PSS 2048 이상, KCDSA (2048, 224) 이상 ECDSA/EC-KCDSA (B-233, B-283, K-223, K-283, P-224, P-256)	
비밀번호 관리	o 관리자는 디지털복합기에 존재하는 모든 계정에 기본적으로 설정된 비밀번호를 변경하거나 사용하지 않도록 설정하여 운용해야 한다. - 개발업체에서 명시적으로 공개하지 않은 별도의 계정(계정명/비밀번호 등)이 존재하는 경우 취약점이 있을 수 있으므로 개발업체에 기본 계정 정보를 요청한다. - 개발업체에서 제공하지 않은 계정이 발견된 경우 악의적인 백도어로 볼 수 있다. o 이 때, 관리자 비밀번호는 안전하게 설정해야 한다. 숫자키패드만 존재하여 비밀번호를 설정할 수 없는 경우 PIN을 사용할 수 있다.	o 기본 계정(제조사 유지보수 계정 및 외부 연동계정 포함) 삭제 o 계정명도 변경이 가능한 경우 계정명도 함께 변경할 것을 권고한다. o 안전한 비밀번호 사용	
	o 주기적(분기별 등)으로 비밀번호를 변경하여 사용해야 한다.	o 주기적 비밀번호 변경	

설정 변경 제한	o 관리자 이외에는 시스템의 관리와 관련된 설정을 변경할 수 없도록 해야 한다. 시스템의 관리의 예는 다음과 같다. - 사용자 계정의 생성 및 삭제 - 네트워크 설정의 변경(각 관리 프로토콜의 허용/비허용 설정, 전자문서의 송수신 포트 및 프로토콜 허용/비허용 등) - 관리자 설정의 변경(비밀번호 변경, 관리자 IP 변경 등) - 디지털복합기의 시간 설정(디지털복합기 자체의 시간 설정 또는 NTP 서버 설정 등) - 유/무선 인터페이스(Wi-Fi, Bluetooth, USB, LAN 등)의 허용과 비허용 - 디지털복합기 기능(출력, 복사, 스캔, 팩스 등)의 허용/비허용 - 디지털복합기 완전삭제 또는 전자문서 암호화 기능의 사용/중단 - 감사기록의 생성, 저장, 관리 - 기타 관리자만이 수행해야 하는 시스템 관리 설정 등	o 계정(사용자 또는 관리자) 생성, 변경 시 해당 계정에 필요한 권한만 할당하도록 한다. o 관리자에 한하여 시스템 설정을 변경할 수 있도록 조치하였는지 확인	

□ 사용자 인증

소항목	점검사항	확인사항	확인
사용자 인증 후 작업	o 인쇄 요청한 전자문서를 디지털복합기에서 사용자 인증(비밀번호, PIN, 지문인식, 스마트카드 인증 등) 후 인쇄물로 배출하는 기능(보안인쇄)이 있다면 해당 기능을 사용할 것을 적극 권장한다.	o 인쇄 요청한 전자문서를 디지털복합기에서 사용자 인증(비밀번호, PIN, 지문인식, 스마트카드 인증 등) 후 인쇄물로 배출하는 기능이 없을 경우 출력(배출)된 문서에 대하여 실제 출력을 수행한 사용자가 해당 문서를 취득할 수 있도록 철저히 관리 o 사용자 인증후 인쇄물로 배출하는 기능이 있을 경우 활성화여부 확인	

□ 감사

소항목	점검사항	확인사항	확인
감사기록 검토	o 관리자는 디지털복합기의 웹 관리페이지 또는 기기 자체에서 감사기록을 주기적으로 검토하여 적절한 조치를 취해야 하며, 디지털복합기로부터 주요 감사 사건을 개별적으로 수신한 경우 즉시 대응해야 한다. o 디지털복합기의 알림 기능(관리자 웹페이지의 메시지 등)이 존재하는 경우, 해당 기능을 활성화하여 사용해야 한다. o 디지털복합기의 알림 기능이 존재하지 않는 경우, 주기적으로 디지털복합기의 상태를 점검해야 한다. o 정확한 감사기록의 생성과 검토를 위해 디지털복합기의 감사 관련 보안기능을 올바르게 설정하여 운용한다.	o 디지털복합기의 웹 관리페이지 또는 기기 자체에서 감사기록 주기적으로 검토 등 보안절차 준수여부 확인	
팩스 사용 및 감사기록 생성	o 디지털복합기의 팩스 기능을 사용하는 경우, 다음 사항을 확인한다. - 팩스 송수신 이력이 감사기록으로 생성 및 저장되도록 설정되어야 한다. - 감사기록이 정확하게 생성 및 저장되는지 확인한다. - 특히, 외부 팩스 기능을 사용하는 경우 디지털복합기를 내부 네트워크에는 연결할 수 없으나 PSTN Fax Network Separation 기능에 대해 CC인증을 받은 제품의 경우에는 보안대책에 따라 운용할 수 있다. o 디지털복합기의 팩스 기능을 사용하지 않는 경우, 다음 사항을 확인한다. - 디지털복합기의 팩스 기능을 사용할 수 없도록 설정해야 한다. - 디지털복합기를 전화선에 연결하지 않아야 한다.	o 디지털복합기의 팩스 송수신 내용에 관한 감사기록은 다음 내용을 포함하여 생성 및 저장되는지 설정여부 확인 - 팩스 송수신자의 신원(전화번호 등) - 팩스 송수신 일시 등	

	o 관리자는 주기적으로 감사기록을 백업해야 한다.	o 디지털복합기와 물리적으로 분리된 지정된 저장소에 백업 등 보안절차 준수여부 확인	

□ 시스템 유지보수 및 백업

소항목	점검사항	확인사항	확인
유지보수	o 유지보수 작업은 원칙적으로 원격 작업은 금지하나, 부득이한 경우 반드시 정보보안담당관의 승인 후 수행해야 한다. - 단, 내부 네트워크에 연결된 디지털복합기는 원격으로 유지보수할 수 없다.	o 디지털 복합기 유지보수 작업에 대해 정보보안담당관의 승인 등 보안절차 준수여부 확인	