분류		항목코드	점검 항목	방법	조치 현황	판단기준
계정 관리	1	PC-01	패스워드의 주기적 변경	로컬 보안 정책 (secpol.msc) 계정 정책->암호 정책	최대 암호 사용 기간 "548일" 설정 최소 암호 사용 기간 "1일" 설정 최근 암호 기억 설정되어 있음	**양호** : 최대 암호 사용 기간이 "90일"이하로 설정되어 있는 경우 **취약** : 암호 사용 기간이 "제한 없음"이거나 "90일"을 초과하여 설정되어 있는 경우
	2	PC-02	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	로컬 보안 정책 (secpol.msc) 계정 정책->암호 정책	"최소 암호 길이 속성" 을 "9문자(이상)"으로 설정	**양호** : 복잡성을 만족하는 패스워드 정책이 설정되어 있는 경우 **취약** : 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우
	3	PC-15	복구 콘솔에서 자동 로그온을 금지하도록 설정	로컬 그룹 정책 편집기(gpedit.msc) 컴퓨터 구성->window 설정 ->보안설정->로컬정책->보안옵션 -> 복구 콘솔 자동 로그온 허용 "사용 안 함"으로 설정 ₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩setup₩recoveryconsole (securitylevel DWORD 값 0)	복구 콘솔 자동 로그온 허용 "사용 안 함"으로 설정	**양호** : 복구 콘솔 자동 로그온 허용이 "사용 안 함"으로 설정되어 있는 경우 **취약** : 복구 콘솔 자동 로그온 허용이 "사용"으로 설정되어 있는 경우
서비스 관리	4	PC-03	공유 폴더 제거	공유 폴더 (FSMGMT.MSC) 고급 공유 설정 regedit->₩HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters₩AutoShareServer (AutoShareServer DWORD 값 0), 없을시 키값 생성	공유 폴더 불필요 시 삭제 공유 폴더 필요 시 적절한 접근권한 부여 및 암호 설정 조치 후 AutoShareServer(또는, AutoShareWks)값 변경으로 자동 공유 방지	**양호** : 불필요한 공유 폴더가 존재하지 않거나 공유폴더에 접근권한 및 암호가 설정되어있는 경우 **취약** : 불필요한 공유 폴더가 존재하거나 접근권한 및 암호 설정 없이 공유폴더를 사용하는 경우
	5	PC-04	항목의 불필요한 서비스 제거	서비스 (services.msc)	아래 불필요한 서비스 모두 "사용 안함"으로 설정함 (Cryptographic Services, DHCP Client, Distributed Link Tracking Client, DNS Client, Human Interface Device Service, Print Spooler, Remote Registry)	**양호** : 일반적으로 불필요한 서비스(아래 목록 참조)가 중지되어 있는 경우 **취약** : 일반적으로 불필요한 서비스(아래 목록 참조)가 구동 중인 경우
	6	PC-05	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	로컬 그룹 정책 편집기(gpedit.msc) 관리 템플릿->windows messenger 사용안함으로 설정시 ₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Policies₩Microsoft₩Messenger₩Client (PreventRun DWORD 값 1)	"Windows Messenger를 실행하지 않음" 설정	**양호** : Windows Messenger가 실행 중지된 상태이거나 상용 메신저가 설치되지 않은 경우 **취약** : Windows Messenger가 실행 중이거나 상용 메신저가 설치되어 있는 경우
	7	PC-16	파일 시스템이 NTFS 포맷으로 설정	컴퓨터 관리(compmgmt.msc) 저장소->디스크 관리	모든 드라이브가 NTFS 파일 시스템을 사용하고 있음	**양호** : 모든 디스크 볼륨의 파일 시스템이 NTFS인 경우 **취약** : 모든 디스크 볼륨의 파일 시스템이 FAT32인 경우
	8	PC-17	대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티부팅이 가능하지 않도록 설정	시스템 속성(sysdm.cpl) 고급->시작 및 복구 시스템 구성(msconfig) 부팅	하나의 OS만 설치하여 운영되고 있음	**양호** : PC 내에 하나의 OS만 설치되어 있는 경우 **취약** : PC 내에 2개 이상의 OS가 설치되어 있는 경우
	9	PC-18	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정	**N/A**	2022년 6월 15일부로 Internet Explorer 지원 안함	**양호** : "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 설정이 "사용"으로 설정되어 있는 경우 **취약** : "브라우저를 닫을 때 임시 인터넷 파일 폴더 비우기" 설정이 "사용"으로 설정되어 있지 않은 경우
패치 관리	10	PC-06	HOT FIX 등 최신 보안패치 적용	업데이트 확인->업데이트 기록 보기	Windows Update 사이트에 접속하여 최신 패치 존재 여부 확인 및 패치 적용	**양호** : HOT FIX 설치 및 자동 업데이트 설정이 되어 있고 내부적으로 관리절차를 수립하여 이행하고 있는 경우 **취약** : HOT FIX가 설치되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
	11	PC-07	최신 서비스팩 적용	winver	Windows Update 사이트에 접속하여 최신 서비스팩 여부 확인 및 적용	**양호** : 최신 서비스팩이 적용 되어 있고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우 **취약** : 최신 서비스팩이 적용 되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
	12	PC-08	MS-Office, 한글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용	프로그램 및 기능(Appwiz.cpl)	설치된 응용 프로그램의 최신 보안 패치 적용	**양호** : 설치된 응용 프로그램의 최신 패치가 적용되어 있고 내부적으로 관리절차를 수립하여 이행하고 있는 경우 **취약** : 설치된 응용 프로그램의 최신 패치가 적용되어 있지 않거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
보안 관리	13	PC-09	바이러스 백신 프로그램 설치 및 주기적 업데이트	Virus Chaser 확인	백신 설치 완료 (Virus Chaser) 및 최신 업데이트 완료	**양호** : 백신이 설치되어 있고, 최신 업데이트가 적용 되어 있는 경우 취약 : 백신이 설치되어 있지 않거나, 최신 업데이트가 적용 되어 있지 않은 경우
	14	PC-10	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	Virus Chaser 확인	백신 설치 완료 (Virus Chaser) 및 최신 업데이트 완료	**양호** : 설치된 백신의 실시간 감시 기능이 활성화 되어 있는 경우 취약 : 백신이 설치되어 있지 않거나, 실시간 감시 기능이 비활성화 되어 있는 경우
	15	PC-11	OS에서 제공하는 침입차단 기능 활성화	방화벽(Firewall.cpl) ₩HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile (EnableFirewall DWORD 값 1)	Windows 방화벽 "사용"으로 설정	**양호** : Windows 방화벽 "사용"으로 설정되어 있는 경우 또는 유무료 기타 방화벽을 사용하고 있는 경우 **취약** : Windows 방화벽 "사용 안 함"으로 설정되어 있는 경우 또는 유무료 기타 방화벽을 사용하고 있지 않는 경우
	16	PC-12	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	화면 보호기 변경	화면 보호기를 설정 후 대기 시간을 10분으로 설정함 화면 보호기를 설정 후 "다시 시작할 때 암호로 보호(P)" 체크	**양호** : 화면보호기 설정(대기시간 10분 이하) 및 암호로 보호가 설정되어 있는 경우 **취약** : 화면보호기 설정(대기시간 10분 초과) 및 암호로 보호가 설정되어 있지 않은 경우
	17	PC-13	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	control->자동 실행 로컬 그룹 정책 편집기(gpedit.msc) 컴퓨터 구성->관리 템플릿 ->windows 구성 요소->자동 실행 정책->자동 실행 끄기 ₩HKEY_CURRENT_USER₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer (없으면 Explorer 키 생성 후 ff값입력)	미디어 자동실행 방지 설정	**양호** : 미디어 사용 시 자동 실행되지 않고 내부적으로 관리 절차를 수립하여 이행하고 있는 경우 **취약** : 미디어 사용 시 자동 실행되거나 내부적으로 관리 절차가 수립되어 있지 않은 경우
	18	PC-14	PC 내부의 미사용(3개월) ActiveX 제거	**N/A**	2022년 6월 15일부로 Internet Explorer 지원 안함	**양호** : 설치된 ActiveX를 주기적(매달 1번 권고)으로 점검하고 불필요한 ActiveX를 삭제하는 경우 **취약** : 설치된 ActiveX에 대한 주기적인 점검 및 삭제가 이루어지지 않는 경우
	19	PC-19	원격 지원을 금지하도록 정책이 설정	로컬 그룹 정책 편집기(gpedit.msc) 컴퓨터 구성->관리 템플릿->시스템->원격 지원->원격 지원 제공 구성	원격 지원 서비스 비활성화	**양호** : 원격 지원이 "사용 안 함"으로 설정 되어 있는 경우 **취약** : 원격 지원이 "사용"으로 설정 되어 있는 경우