과학기술정보통신부 Ministry of Science and ICT

KISA

기업 및 기관 관리 담당자 편

디지털 영상저장·전송 장치 운영을 위한 보안수칙

관련 법령 준수 및 안내판 설치 등	IP카메라의 설치·운영 장소에 따라 관련 법령에서 정한 규정을 준수해야 함 ※ 어린이집(영유아보육법), 수술실(의료법), 동물보호시설(동물보호법) 등은 개별 법령을 우선 적용하며 그 외 개별 법령에서 정하지 아니한 사항은 개인정보보호법이 적용됨 필수 촬영 목적, 관리책임자 연락처 등이 기재된 안내판을 부착 금지 녹음 기능의 사용, 사생활 침해 우려 장소(화장실, 탈의실 등) 설치는 금지 ※ 사업장내 근로상황 모니터링 목적의 IP카메라 설치는 사전 동의 또는 노사협의 필요
안전한 관리자 계정 설정	관리 계정에 강력한 조합(예: 8자리 이상, 특수문자 필수 포함 등) 비밀번호를 사용하고 6개월 이내에 주기적으로 변경하여 무단 접근을 방지해야 함
이중 인증 기능 설정	이중 인증을 지원하는 제품이라면 관리자 계정에 이중 인증을 활성화해 사용해야 함
업데이트 버전 확인	주기적으로 제조사의 홈페이지나, 사용 중인 앱/소프트웨어를 확인하여 펌웨어/소프트웨어 업데이트가 있으면 즉시 업데이트해야 함
포트 포워딩 (외부 접속) 확인	필요시에만 포트 포워딩(외부 접속)을 사용하며, 주기적으로 포트 설정을 점검하여 불필요한 포트는 비활성화해야 함
공유기 보안 상태 확인	설치 시 해당 네트워크의 공유기/스위치에 대한 보안 설정을 점검, 비밀번호를 강력하게 설정(예: 8자리 이상, 특수문자 필수 포함 등)하도록 안내 및 설정하고, 무선네트워크 사용 시 WPA3 등 최신 보안 프로토콜을 사용하는지 확인해야 함
접근 제한 정책 확인	관리 서버 및 시스템에 접근 가능한 IP를 제한하여, 무작위 접근을 차단해야 함
정기적인 로그 모니터링	접속 로그 점검을 매월 정기적으로 수행해야 함
비정상 접근 알림 설정	비정상 접근 시도에 대한 알림 기능이 있는 경우 이를 설정하고, 불필요한 알림과 섞이지 않도록 관리해야 함
관리자 계정 관리	관리자 계정은 최소한의 권한만 설정하고, 주기적인 관리자 계정 현황 점검을 통해 전출·퇴직자 계정은 미사용 시 계정 비활성화 또는 삭제해야 함
사내 보안 정책 관리	기업의 전체 네트워크 보안·관리 정책 대상 장비에 DVR/NVR 등 영상 장비를 필수로 포함시켜야 함
정기적인 네트워크 점검	영상 장비와 연결된 네트워크에 대한 보안 점검을 정기적으로 수행해야 함
백업 및 복구계획 수립	영상정보 같은 중요한 데이터는 정기적으로 백업(별도의 장치 등) 하고, 신속한 복구가 가능하도록 절차 수립 및 주기적인 복구 훈련을 해야 함
보안인증 안내	[KC 인증] 전파법 규정에 따라 품질·내구성 보증, 해킹에 의한 보안 등을 인증받은 제품 [TTA 인증] 공공기관 사용을 위해 받아야 하는 IP카메라 보안인증 확인 (공공기관용IP카메라/무선영상전송장비) (TTA 인증 현황: https://cs.tta.or.kr/tta/notification/ttaCertProductListR.do) [KISA IoT 보안인증] 한국인터넷진흥원(KISA)이 운영하는 IoT 보안인증 (정보통신망연결기기등 정보보호인증)을 획득한 제품은 보안 기능이 강화된 제품이니 구매 시 참고하세요. (KISA 인증 현황 : https://www.ksecurity.or.kr/user/extra/kisis/310/iot/iotList/jsp/LayOutPage.do)