# 모두스쿨 시스템 보안 기술 표준 안내서

## 2026 기술 사양서 및 가이드라인

GUIDANCE FOCUS

**2026년 모두스쿨 시스템의 보안기술 적용 및 개인정보보호를 위한 보안 기술 안내**

| 인프라 | 사고율 | 정부 권고 | AI 보호 |
|---|---|---|---|
| AWS Cloud | 0.00% (ZERO) | KISA / MSIT | ACTIVE |

본 기술 안내서는 **과학기술정보통신부(MSIT)** 및 **한국인터넷진흥원(KISA)**의 기술 권고를 바탕으로 합니다. 모두스쿨은 졸업사진 작업시 개인정보유출 및 정보보호 및 디지털 위협으로부터 보호하기 위해 아래와 같은 핵심 보안 표준을 상시 운영하고 있습니다.

### 비즈니스 신뢰도 비교 분석표

| 보안 핵심 평가 지표 | 모두스쿨 시스템 | 일반 NAS/스토리지 |
|---|---|---|
| 계정 및 인증 보안 (MFA 적용) | **100% 준수** | 35% (취약) |
| 네트워크 경로 및 포트 관리 | **100% 준수** | 20% (위험) |
| 능동형 침입탐지 및 IP 차단 | **상시 가동** | 15% (노출) |
| 데이터 무결성 및 시점 복구(Snapshot) | **완벽 대응** | 40% (불안) |

** KISA 'NAS 보안 가이드라인' 및 AI 보안 기술 권고안 실측 기준 (2026)*

## 핵심 보안 기술 사양 상세 리스트

### 1 계정 체계 표준화 과기정통부·KISA 준수

**기본 관리자 계정 폐쇄**
'admin' 기본 계정 비활성화 및 전용 보안 계정 대체 완료.

**2단계 인증(MFA) 도입**
OTP 기반 '이중 보안 시스템 등록'으로 비인가 접근 차단.

### 2 네트워크 포트 관리 과기정통부·KISA 준수

**표준 서비스 포트 폐쇄**
기본 포트(5000, 5001) 상시 폐쇄 및 임의의 '전용 보안 포트 전환'.

**UPnP 및 서비스 최소화**
자동 포트 개방 해제 및 '불필요 서비스 통로 전면 차단'.

## 3 능동형 침입 탐지 과기정통부·KISA 준수

**국가별 IP 필터링**
국외발 접속 상시 봉쇄.

**실시간 자동 차단**
반복 로그인 실패 IP 추방.

**펌웨어 통합 관리**
최신 보안 패치 상시 적용.

## 4 데이터 무결성 보장 랜섬웨어 대응 표준

- '독립 디렉토리 격리': 업무 데이터와 핵심 시스템 영역 물리적 분리 적용.
- '시점 복구 시스템(Snapshot)': 공격 발생 전 상태로 즉각적인 원복 시스템 구축.

## 5 AI 및 딥페이크 대응 업계 수호 솔루션

**동적 메타데이터 워터마킹**
사진업로드시 사이트 정보를 메타데이터에 삽입하여 사진의 정당성을 증명합니다.
(개발완료)

**자동 워터마크 설정 기능**
무단 유출된 파일 경로를 추적하고 캡쳐를 방어하여 원본 가치를 지킵니다.
(개발완료)

**AI 변조 방지 노이즈 (Adversarial Noise)**
'지능형 워터마크 실시간 결합'으로 무단 유출 추적성 확보 및 캡처 원천 방어. (현재 개발중)

---

## CEO MANIFESTO

***"졸업앨범의 가치는 지키고, 디지털의 위험은 버리겠습니다."***

최근의 딥페이크 위협은 졸업앨범이라는 소중한 기록 문화를 위협하고 있습니다. 모두스쿨의 보안 표준은 단순히 사진을 보호하는 것을 넘어, 사진관의 비즈니스를 보호하고 학생들의 추억을 지키는 최후의 보루가 될 것입니다.

전통이 끊기지 않도록, 모두스쿨이 업계 최고의 방패가 되어 사장님들의 영업 현장을 끝까지 지켜내겠습니다.

ISSUED BY
**PARANSOFT**

REPRESENTATIVE
**정 왕 재**

© 2026 PARANSOFT. ALL RIGHTS RESERVED. CONFORMS TO MSIT/KISA SECURITY STANDARDS.