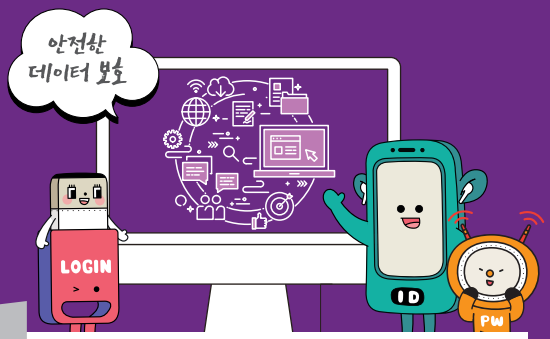
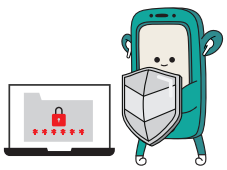
안전한 데이터 보호를 위한

NAS 보안수칙



01 암호화 사용

저장된 데이터를 디스크 및 파일 레벨에서 암호화하고, SSL/TLS 암호화를 통해 데이터 전송 중에도 보호합니다.

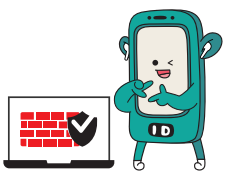


02 접근 제어와 권한 관리

사용자와 그룹별로 적절한 접근 권한을 설정하고, 최소한의 권한 원칙을 준수하여 데이터에 엄격한 접근을 제한합니다.

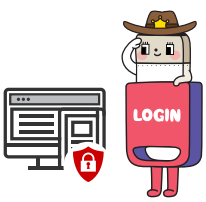
03 네트워크 보안

불필요한 서비스 포트 차단, 방화벽 설정 및 안전한 원격 액세스를 위해 VPN 사용 등으로 NAS 장비를 안전하게 보호합니다.



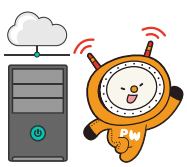
04 펌웨어 및 소프트웨어 업데이트

주기적인 펌웨어, 운영 체제, 소프트웨어 업데이트를 통해 최신 보안 패치를 유지하고 취약점을 예방합니다.



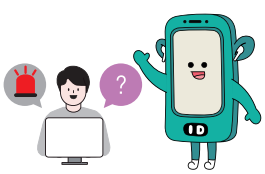
05 백업 및 복원 전략

주기적인 데이터 백업을 통해 데이터 손실을 방지하고, 복원 테스트를 수행하여 빠르게 데이터를 회복할 수 있는지 확인합니다.



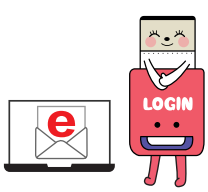
06 감사 로깅과 모니터링

모든 활동에 대한 감사 로그를 설정하고, 비정상적인 활동을 감지하기 위해 실시간 모니터링과 이벤트 알림을 활용합니다.



07 업데이트된 및 안전한 앱 사용

공식 패키지 센터에서 신뢰할 수 있는 앱을 다운로드하고, 주기적인 패치 및 보안 업데이트를 수행하여 보안 취약점에 대비합니다.



08 랜섬웨어 방지

데이터에 읽기 전용 권한을 할당하여 랜섬웨어로부터 데이터를 보호하고, 랜섬웨어 안티 솔루션을 활성화하여 악성코드를 차단하며, 사용자에게 랜섬웨어에 대한 주기적인 교육을 제공합니다.

과학기술정보통신부

KISA 한국인터넷진흥원