

	넥스오토	문서번호 : NEX-BO-T-03
개정일 : 2024-08-01	정보유출통제지침	개정차수: 3

개정이력

차수	재(개)정 일자	시행일자	주요 개정 내용
1	2024-08-01	2024-08-01	초도 제정
2	2024-09-03	2024-09-03	지침 구성 변경에 따른 개정
3	2025-02-25	2025-02-25	대용량파일 송수신 통제, 저장매체 폐기절차 수정

목 차

1. 개요

- 1.1 목적
- 1.2 적용범위
- 1.3 책임 및 권한

2. 네트워크 통제

- 2.1 인터넷 통제
- 2.2 대용량 파일 송수신 통제
- 2.3 기타

3. PC 통제

- 3.1 중요문서 관리
- 3.2 악성코드 차단
- 3.3 이동식 저장매체 통제
- 3.4 저장매체 폐기

4. 서버시스템 통제

1. 개요

1.1 목적

본 지침서는 사내의 중요정보에 대한 IT적인 통제지침을 제시함으로써 정보자산의 보안성과 안정성을 유지하는데 필요한 사항을 제공하는데 목적을 둔다.

1.2 적용범위

사내 정보자산과 이를 취급하는 정보자산소유자를 대상으로 한다.

1.3 책임 및 권한

1.3.1 모든 임직원

- 1) 회사에 근무하는 모든 인력은 허가된 범위 내에서 정보자산을 이용할 수 있는 권한이 있으며, 불법사용에 의한 보안사고의 최종 책임은 해당 인력에게 있다.

2. 네트워크 통제

2.1 인터넷 통제

2.1.1 인터넷을 통한 모든 정보의 송수신은 회사의 보안시스템을 통해야한다.

2.1.2 회사 내부에 승인되지 않는 별도의 인터넷 회선은 차단되어야 한다.

2.2 대용량 파일 송수신 통제

2.2.1 통제 기준

- 1) 대용량 파일 송수신은 정보유출, 악성코드 유입 등의 보안위험이 존재하므로, 보안정책에 따라 통제한다.
- 2) 외부와의 파일 송수신은 승인된 보안 채널(예: 사내 파일전송시스템, 암호화된 전송 경로)을 통해서만 가능하다.
- 3) 승인되지 않은 경로(FTP, 텔넷, 메신저, 외부 클라우드 등)를 통한 송수신은 금지한다.

2.2.2 대용량 파일 기준

- 1) 파일 크기가 100MB 이상인 경우를 대용량 파일로 정의한다.
(※ 파일 성격에 따라 부서별 세부 기준을 정할 수 있으며, 보안관리자의 승인을 받아야 함)

2.2.3 송수신 승인 절차

- 1) 외부로의 대용량 파일 전송 시, 반드시 부서장 및 정보보안담당자의 사전 승인을 받아야 한다.
- 2) 수신 시에는 출처 확인 및 악성코드 검사를 반드시 거쳐야 하며, 필요 시 격리 시스템을 통해 확인한다.
- 3) 승인 요청 시 다음 항목을 포함해야 한다:
 - ㉠ 파일명 및 크기
 - ㉡ 전송 목적
 - ㉢ 수/발신자 정보
 - ㉣ 사용 채널
 - ㉤ 보관 기간 및 위치

2.2.4 로그 기록 및 보관

- 1) 모든 대용량 파일 송수신 내역은 자동으로 기록되어야 하며, 최소 6개월 이상 보관해야 한다.
- 2) 정보보안팀은 정기적으로 송수신 이력을 검토하여 이상 행위를 탐지한다.

2.2.5 위반 시 조치

- 1) 위반자는 정보보안 위반행위로 간주하며, 사내 보안 정책에 따라 징계 또는 접근 권한 제한

등의 조치가 이루어진다.

2.3 기타 네트워크 통제는 네트워크보안지침을 따른다.

3. PC 통제

3.1 중요문서 관리

3.1.1 PC내 대외비 이상 중요한문서는 암호화를 하여 유출 위험을 최소화한다.

3.1.2 PC내 비밀등급 이상의 문서는 저장시에 정보보안그룹의 허가를 받고 저장하여야하고
문서 파일의 삭제 및 이동시 정보보안그룹의 동의하에 진행하여야한다.

3.2 악성코드 차단

3.2.1 정기적인 패치 운영관리가 이뤄져야 보안패치의 설치현황이 관리되어야 한다.

3.2.2 PC내 방화벽 또는 백신의 유효성 및 업데이트를 주기적으로 확인하여야한다.

3.3 이동식 저장매체 통제

3.3.1 이동식 저장매체를 통제하기 위한 솔루션이 적용되어 있거나 그에 상응하는 운영관리를
하여야 하며, 승인된 사용자만 이동식 저장매체를 사용할 수 있어야 한다.

3.3.2 이동식 저장매체 솔루션이 적용되어 있는 경우 권한신청/삭제/계정관리는 기술보안담당자가
수시로 점검하여 정보보안그룹과 공유한다.

3.3.3 회사에서 인가 되지 않은 비보안 USB 같은 이동식 매체는 반입을 할 수 없으며 회사에서
제공하는 보안USB만 사용할 수 있다.

3.3.4 이동식 저장 매체 관리대장을 작성하여 사용자, 지급현황, 회수 및 등록 현황 등을 수시로
관리해야하며 예외자 목록도 별도로 관리해야 한다.

3.3.5 이동식 저장매체를 통해 민감하고 중요한 정보 저장시 암호화 하거나 접근제어를 통해
유출위험을 최소화 한다.

3.4 저장매체 폐기

3.4.1 회사에서 사용되는 데이터가 기록될 수 있는 모든 매체를 대상으로 한다.

3.4.2 폐기 프로세스는 다음과 같다.

- PC, 서버, 기타 장치의 변경 및 처분으로 인한 저장매체의 변경사항 발생시 재사용 및 불용
여부를 정보보안그룹에서 결정하여 CSO에 보고후 승인을 진행한다.
- 재사용 승인시 : 데이터 완전삭제 프로그램을 이용하여 삭제후 재사용 진행한다.
- 불용으로 폐기 승인시 : 완전파괴(소각, 파쇄), 전용 소자장비(디가우저)를 이용하여 삭제

3.4.3 저장매체를 폐기할 경우 폐기 일자, 폐기 담당자, 폐기 사유, 폐기 방법, 폐기 사진 등을
명시한 저장매체 폐기관리대장을 기록 보관한다.

3.4.4 외부업체를 통하여 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고, 해당 절차에
따라 완전히 폐기되었는지 확인하고 CSO에 최종적으로 폐기 확인을 보고한다.

4. 서버시스템 통제

4.1 서버시스템 정보유출통제는 시스템보안지침을 따른다.