NEXAUSTO	넥스오토 서버접근통제운영지침	문서번호 : NEX-BO-T-07
개정일 : 2025-02		개정차수: 1

개정이력

차수	재(개)정 일자	시행일자	주요 개정 내용
1	2025-02-01	2025-02-01	초도 제정
2			
3			

목 차

1. 개요

1.1 목적

서버 및 데이터베이스(DB)에 대한 접근을 통제하여 정보 유출, 무단 변경 및 삭제를 방지하고, 안전한 시스템 운영을 보장한다.

2. 적용 범위

본 절차서는 넥스오토가 운영하는 모든 물리적·가상 서버 및 데이터베이스(DB)에 적용된다.

3. 통제 대상

3.1 인적 대상

3.1.1 내부 인력

1) 개발팀, 보안관련부서 등 시스템 접근이 요구되는 부서의 정규직 및 계약직 인원

2) 직무상 서버 또는 DB에 접근 권한이 필요한 부서 소속 관리자

3.1.2 외부 인력

1) 위탁 운영을 수행하는 외주 인력

2) 프로젝트 단위로 일시적 접근이 필요한 협력업체 개발자 및 관리자

3.2 시스템 대상

3.2.1 서버 자산

1) 웹서버, 애플리케이션 서버, 파일서버 등 내부 서비스 제공 서버

2) 클라우드 기반 가상 인스턴스 포함

3.2.2 데이터베이스 자산

1) 관계형 데이터베이스 (Oracle, MSSQL, MariaDB 등)

2) 비관계형 데이터베이스 (MongoDB, Redis 등)

4. 접근 신청 및 승인 절차

4.1 접근 신청

4.1.1 신청 대상

1) 신규 업무 수행으로 접근 권한이 필요한 인력

2) 기존 인력 중 권한 확대 또는 시스템 추가 접근이 필요한 자

4.1.2 신청 방식

1) '서버 및 DB 접근 신청서'를 작성하여 시스템명, 목적, 필요 기간, 요청 권한 수준 등을 명확히 기재해야 한다

2) 신청서는 해당 부서장의 검토 및 서명을 받은 후, 정보보안팀에 전자결재 또는 이메일로 제출해야 한다

3) 긴급 접근의 경우 사후 승인을 포함한 별도 절차에 따라 예외 적용 가능하다.

4.2 승인 및 검토

4.2.1 승인 주체

1) 해당 부서장

2) 정보보안 담당자
3) 정보보안 책임자

4.2.2 승인 기준

1) 업무상 필요성 및 요청 범위의 적정성 여부 검토
2) 최소 권한 부여 원칙에 따른 제한적 권한 부여 여부 확인
3) 외부 인력의 경우 보안서약서 체결

4.3 권한 부여

4.3.1 부여 절차

1) 관리자 권한은 정보보안 그룹의 협의를 거쳐 정보보안 책임자의 최종승인을 받고 부여한다.
2) 사용자 권한은 역할 기반 최소 권한만 부여한다.

4.3.2 이력관리

1) 권한 부여 및 변경 내역은 이력대장에 기록하여 관리한다.

4.4 사용자 통보

4.4.1 통보 내용

1) 계정 생성 여부, 접근 방법, 유효 기간, 보안 수칙 등 관련 사항은 신청자에게 안내한다.
2) 사용자 계정은 반드시 개인 식별 가능하게 생성되어야 하며, 타인과 공유를 금지한다.

5. 접근 관리 및 회수

5.1 접근 로그 수집 및 점검

5.1.1 로그 수집 항목

1) 사용자 ID, 접근 일시, IP 등 정보를 수집한다.
2) 로그는 최소 6개월 이상 보관을 원칙으로 한다.

5.1.2 로그 점검

1) 인가된 권한 외 이상 행위 여부를 주기적으로 점검한다.
2) 로그점검은 최소 월 1회 이상 검토한다.

5.2 권한 회수 절차

5.2.1 회수 조건

1) 퇴사, 부서 이동, 업무 변경 등 사유 발생 시
2) 프로젝트 종료 또는 권한 유효 기간 만료 시
3) 30일 이상 미사용 계정

5.2.2 회수 방식

1) 시스템 관리자는 즉시 권한 회수를 시행하고, 결과를 기록한다.
2) 회수 대상자 및 소속 부서에 회수 결과를 통보한다.

6. 예외 및 긴급 접근

6.1 접근 처리

6.1.1 사전 승인

1) 정기 점검, 야간/휴일 작업 등은 사전 접근 요청서를 통해 승인을 받아야 한다.
2) 승인 시 접근 대상 시스템, 작업 목적 및 시간, 요청자 신원을 명시해야 한다.

6.1.2. 사후 승인

1) 긴급 장애 조치 등 불가피한 사전 미승인 접근 시, 해당 보안담당자에게 구두 승인을 받고 진행 후, 24시간 이내 사후 승인을 요청하고 결과 보고서를 제출해야 한다.

7. 정기 점검 및 문서화

7.1 권한 정기 점검

7.1.1 점검 주기

1) 분기 1회 이상 권한 사용 현황을 점검하여 불필요 권한을 식별하고 회수 조치한다.
2) 불필요 권한 식별 후 즉시 회수 진행한다.

7.1.2 점검 보고

1) 점검 결과는 기록으로 보관하며, 정보보안책임자에게 보고한다.
2) 관련 기록은 최소 1년간 보관한다.