개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
1	2017-09-13	2017-09-13	초도 제정
2	2023-12-01	2023-12-01	디오토 상호변경
3	2024-08-01	2024-08-01	넥스오토 상호변경
4	2024-08-01	2024-08-01	네트워크 절차 내용 추가

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

목 차

1. 개요

1.1 목적

본 지침서는 사내 네트워크 구성 및 외부 네트워크와 연결 시 요구되는 정보보호의 수준을 향상시킴으로써 안정적인 네트워크 인프라를 운영하는데 목적을 둔다.

1.2 적용범위

사내 네트워크 및 인터넷과 같은 외부와 연결되는 모든 네트워크를 그 적용범위로 하며, 그 시스템을 직접 관리, 운영하는 담당자들을 대상으로 한다.

1.3 용어 정의

1.3.1 인터넷 구간

인터넷 관련 서비스를 목적으로 불특정 다수의 접속을 허용한다.

1.3.2 DMZ 구간

① **서비스를 목적으로 하는 네트워크로 불특정 다수의 접속을 허용한다.**

② **외부의 불량 침입으로 인한 서비스의 장애를 최소화 하기 위하여 서버별 port단위로 접근통제를 하여야 하며 취약한 포트(FTP, Telnet 등)은 Source와 Destination 별 포트관리를 해야 한다.**

1.3.3 내부 네트워크 구간

① **외부로부터의 침입에 대비한 접근차단시스템이 운영되어야 한다.**

② **업무용 이외나 보안상 취약한 포트가 있을 경우 차단한다.**

③ **이외나 보안상 취약한 포트가 있을 경우 차단한다.**

④ **업무용 네트워크와 사무전화기 IP대역은 분리하여 사용한다.**

1.4 책임 및 권한

1.4.1 전사보안책임자

① **네트워크 시스템 전반에 대한 관리 책임을 가진다.**

② **네트워크 보안 관리가 수행되도록 감독할 책임을 가진다.**

③ **시스템 도입 및 철수에 대한 승인과 책임을 가진다.**

1.4.2 기술보안담당자

① **네트워크 장비의 보안취약점을 점검하여 네트워크 운영담당자에게 보안 개선을 지시한다.**

② **보안사고 발생 시 사고대응을 하며, 보안책임자에게 보고한다.**

1.4.3 네트워크 운영담당자

① **기술보안담당자와 겸임할 수 있다.**

② **네트워크 장비의 모니터링 성능관리, 장애, 변경관리를 수행한다.**

③ **신규 장비 도입 발생 시 장비검토, 설치계획을 수립한다.**

④ **취약점 발견 시 기술보안담당자 및 필요 시 보안책임자에게 보고 후 조치한다.**

⑤ **보안사고 발생 시 사고대응을 하며, 보안책임자 및 필요 시 대표이사에게 보고한다.**

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

2. 네트워크 시스템 운영

2.1 시스템 도입 및 설치

2.1.1 네트워크의 변경, 증설 등 환경의 변화에 따라 네트워크 시스템의 도입, 폐기 요구가 있는 지 모니터링 하여야 하며, 적절한 도입 시기를 파악해야 한다.

2.1.2 시스템 도입 시, 서류상의 비교검토를 하며, 필요 시 BMT(Bench Marking Test)를 통한 결과를 장비의 선정 기준으로 삼는다.

2.1.3 기존 네트워크 장비와의 연동을 위한 보안성 검토를 수행해야 한다.

2.1.4 네트워크 구성형태에 따른 위험을 사전 분석 및 평가해야 한다.

2.1.5 시스템은 물리적 보안이 되어 있는 통제구역에 설치되어야 한다. 단, 사용자 시스템과 직접 연결이 되는 네트워크 Switch, 무선AP 등은 그 특성에 따라 일반구역에 설치 가능하다.

2.1.6 설치 후 자산관리 목록을 갱신하며, 결과를 보안책임자에게 보고한다.

2.1.7 외부 네트워크와 내부 네트워크의 접점 구간에는 방화벽이나 IPS 등 접근차단시스템이 운영되어야 한다.

2.2 시스템 보안설정

2.2.1 장비의 관리자 선정, 기본ID 삭제, 기본 비밀번호 변경, 기술적 보안의 구성 점검 등을 하여야 한다.

2.2.2 네트워크 장비에 대한 접근권한은 주기적으로 점검하고, 변동 사항 발생 시 보안책임자에게 보고하여야 한다.

2.2.3 장비 접속은 콘솔을 통하는 것을 원칙으로 하고, 운영 및 모니터링을 위한 원격접속이 필요할 경우 운영자 단말기를 지정하여 운영한다.

2.2.4 네트워크 장비에 원격접속 시 세션타임아웃을 구성하여 접속하여야 한다.

2.2.5 설치 되는 장비의 시간을 동기화하여 무결성을 보장하여야 한다.

2.2.6 Data, Voice 장비는 장비 별로 기본 보안 설정을 정의하고, 적용하여야 한다.

2.3 시스템 운영

2.3.1 네트워크 장비 및 통신회선에 대해 최소 일 1회 이상 모니터링을 하여 장애에 대비하여야 한다.

2.3.2 ACL(Access Control List)을 이용한 접근통제를 할 때는 보안취약점 및 변경내역에 대한 검토를 한 후, 네트워크 운영담당자가 적용한다.

2.3.3 시스템 변경 발생 시 계획서 및 완료사항을 보안책임자에게 보고하여야 한다.

2.3.4 시스템 장애 시 신속한 업무 복구를 위해 구성정보를 6개월 마다 백업을 하여야 하며, 정보는 1년 동안 보관하여야 한다.

2.3.5 시스템 구성정보 변동사항 발생 시 백업을 하여야 하며, 정보는 1년 동안 보관하여야 한다.

2.3.6 장애 발생 시 신속한 대응을 하여야 하며, 보안책임자에게 보고하여야 한다.

2.3.7 네트워크 장비에 대한 장애 방지를 위하여 주기적으로 장비의 점검을 실시하고, 그 결과를 보안책임자에게 보고하고, 문제점은 조치를 취하여야 한다.

2.3.8 모니터링 도구를 이용하여 서비스중인 회선에 대한 트래픽 용량과 장비에 대하여 사용률을 모니터링하고, 매월 정기점검 보고서를 작성하여 전사보안담당자에게 제출한다.

2.4 **시스템 폐기**

시스템의 매각이나 폐기를 위하여 반출 전에 초기화 명령어나 버튼 등을 활용하여, 내부의 라우팅, 비밀번호 등의 설정정보를 초기화하여야 한다.

2.5 VPN 시스템 운영 절차

2.5.1 VPN 계정 발급 기준

① VPN 계정은 업무상 외부 접속이 불가피한 임직원에 한하여 발급한다.

② 계정 발급 시 소속 부서장의 승인과 정보보안그룹의 보안 점검을 거쳐야한다.

③ 계정은 개인 식별이 가능한 사용자 단위로만 발급하며 공용 계정은 금지한다.

④ 사용목적, 접속대상시스템, 사용기간등을 명확히 기록한다.

2.5.2 계정 및 권한 변경 절차

① 업무변경, 프로젝트 종료, 또는 장기 미사용 계정에 대해서는 권한을 재검토한다.

② 권한변경요청은 소속 부서장이 승인한 요청서를 제출해야 하며, 정보보안그룹은 타당성 검토 후 반영한다.

③ 변경 이력을 관리대장에 기록하여 최소 1년간 보관한다.

2.5.3 권한 회수 및 계정 삭제

① 퇴사자, 전환배치자, 불필요 접속자에 대해서는 즉시 VPN 계정을 회수한다.

② 회수는 정보보안그룹 및 보안담당자의 통보 즉시 처리하며, 처리 결과는 기록에 남긴다.

③ 정기적으로 VPN 계정 목록을 점검하여 유휴 계정을 폐기한다.

2.5.4 접속 기록관리 및 감사

① VPN 접속 이력은 최소 6개월간 보관하며, 분기 1회 이상 접속 내역을 감사한다.

② 접속 실패 다수 발생 비업무 시간 접속 등의 이상 징후는 정보보안그룹 확인 후 대응한다.

3. 네트워크 관리 통제

3.1 네트워크 연결, 설치, 변경에 따른 승인

3.1.1 네트워크 신규 접속, 변경, 해지 작업은 승인을 득한 후 진행되어야 한다.

3.1.2 사설/공인 IP의 관리는 네트워크 운영담당자가 관리하며, 승인을 득한 후 신규 부여 및 회수/변경 등의 업무를 진행한다. 필요에 따라 선 작업 후 보고 할 수 있다.

3.2 네트워크 구성 정보 관리

3.2.1 허가 없이 네트워크의 구성도, 주소, 구성환경, 관련 시스템 정보 등을 무단으로 유출하여서는 안 되고, 외부로 공개되는 자료는 민감한 내용(IP등)을 삭제한 후 공개한다.

3.2.2 네트워크 구성도, 현황 자료, 네트워크 주소할당자료 등 네트워크 관련 모든 자료는 인가된 자만이 접근 가능하도록 안전하게 보관한다.

3.3 네트워크 소프트웨어 보안관리

3.3.1 장비의 펌웨어, 운영체제의 각종 버그 또는 보안 홀을 예방하기 위하여 네트워크 장비의 보안관련 패치나 권고안이 발표되는 것을 지속적으로 모니터링하며 보안 패치 적용여부를 검토 후 적용한다.

4. 네트워크시스템 접근 통제

4.1 물리적 접근 통제

통신망 및 네트워크 장비는 물리적으로 출입이 통제되는 시설이 갖추어진 곳에 설치되어야 한다.

4.2 통신망 접근 통제

4.2.1 네트워크 운영담당자를 제외한 인원의 통신망의 접근은 통제되어야 한다.

4.2.2 유지보수업체에 의한 유지보수 작업 시 중요정보가 노출되지 않도록 보안조치를 취하여야 한다.

1) 네트워크 운영 담당자 감독
2) 출입 대장 기록 및 작업 일지 작성
3) 신원보증 및 허가된 특정 인원만으로 출입통제
4) 별도의 계정 부여 및 접근권한에 대한 통제

4.3 외부에서 사내네트워크 연결 통제

4.3.1 내부 네트워크는 외부로부터의 접속을 차단함을 원칙으로 한다.

① 내부와 외부네트워크의 접점구간에는 방화벽, IPS 등의 침입차단시스템이 적용되어야 한다.

② 내부 네트워크는 NAT(Network Address Translation)을 적용하여 사설IP를 사용함으로써 외부에서의 무단침입을 차단하여야 한다.

③ 외부에서 접속하여야 하는 홈페이지 또는 web 업무 시스템은 DMZ를 구성하여 서비스를 하여야 하며 WAS 및 DB서버는 내부 서버 팜에 두어야 한다.

4.3.2 외부에서 내부로의 접속이 필요한 경우는 다음의 내용을 준수하여 오픈 한다.

① 시스템 간 접속이 필요한 경우는 NAT(Network Address Translation)을 적용, 공인IP 생성 및 필요한 포트 오픈 후 보안책임자에게 보고하여야 한다.

② 사용자의 접속이 필요한 경우는 VPN(Virtual Private Network)을 사용하여야 하며, 승인 시 보안책임자에게 보고하여야 한다. VPN 계정은 기간을 명시하여 권한을 부여하되, 정기적으로 사용 실태를 점검하여 미사용 계정은 권한회수 등 조치를 취해야 한다.

4.3.3 ACL(Access List)는 주기적으로 검토하여야 한다.

4.4 중요 네트워크의 분리

4.4.1 정보자산의 중요도 및 위험도가 높은 자산에 대해서는 별도의 보안시스템 구축 또는 네트워크 분리를 하여야 한다.

4.4.2 주기적인 취약점 점검을 하며, 문제 사항이 있을 경우 대응책을 수립한다.

4.5 무선 통신 수단 접근통제

4.5.1 인가되지 않은 무선 통신수단(Access Point, WI-FI, 블루투스, WIBRO, 테더링, NFC 등)은 사용을 금지한다.

4.5.2 비인가 무선 통신수단에 대한 차단 정책이 수립되어야 하며, 필요 시 비인가 무선 통신수단을 차단하는 솔루션을 적용해야 한다.

4.5.3 무선랜 장비 설치 시 기본적인 보안설정을 정의한 후 적용하여야 하며, Default ID는 별도의 ID로 변경하여 사용하여야 한다.

4.5.4 무선LAN(랜) 사용자에 대한 보안 및 데이터의 안전한 전송을 위하여 사용자 인

증, 데이터 암호화, 권한제어가 가능한 WPA2 기법을 적용하여야 한다. 단, 단말지원이 불가능할 경우에만 128bit 이상의 WEP(Wired Equivalent Privacy) 암호화 키를 사용한다.

4.6 로그관리

4.6.1 보안사고 또는 업무상 문제 발생 시 증거확보, 원인파악을 위하여 다음과 같은 내용이 로그에 포함되어야 한다.

① 사내망 및 네트워크 시스템에 대한 사용자의 접근 내역

② 네트워크 시스템에 대한 오류 및 문제 로그

4.6.2 모든 로그는 비 인가자가 접근불가해야 하고, 3년 이상 보관한다.

5. 중요 네트워크 관리

5.1 중요 네트워크 정의

5.1.1 재품생산에 영향을 실시간으로 영향을 미치는 개발정보, 서열정보 등을 다루는 네트워크 업무망을 의미한다.

5.1.2 양산, 신차, AS 도면 및 부품정보를 다루는 연구소 망과 실시간으로 서열 정보를 생산현장에 배포하여 생산 및 실적 취합을 하는 FA망이 이에 해당된다.

5.2 운영 기준

5.2.1 연구소와 FA망의 관리는 팀보안 담당자가 실시간 장애 여부를 확인한다.

5.2.2 장애 발생 시 비상사태에 준하는 대응으로 신속 정확하게 복구를 실시한다.

5.2.3 매일 팀 보안 담당자는 중요 네트워크 망의 회선 점검을 실시하고 장애 발생 시 즉시 기술보안담당자에게 보고하고 조치를 받도록 한다.

5.2.4 기술보안담당자는 평상시 중요 네트워크 단선 여부 및 PING 테스트 등의 회선 점검을 실시하며, 네트워크에 연결된 PC 및 서버등을 모니터링 한다.

5.3 OA망 네트워크 관리

5.3.1 허용기준

① 모든 유선 네트워크는 외부사용자는 허용하지 않는 것을 기본 원칙으로 한다.

② 네트워크 장비 유지보스 등은 유선망의 외부 업체 점검이 필요할 경우는 예외로 한다.

5.3.2 허용절차

① 모든 유선 네트워크 연결 권한은 기술보안담당자가 통제하도록 한다.

② 네트워크 신규추가 및 유지보스 등 외부인의 작업이 필요한 경우 외부인에게 보안서약서를 징구하고 작업에 임하도록 한다.

③ 신규 장비가 추가되어 네트워크 등록이 필요한 경우, 기술보안담당자는 IP자원, 트래픽 규모, 보안성 문제들을 종합 검토하여 정보보안그룹의 협의를 거쳐 네트워크를 할당한다.

④ 외부인 보안서약서 작성 시 프로젝트명, 작업목적, 작업기간 등 정보를 같이 첨부하여 기술보안담당자의 승인을 받고 작업을 진행해야한다.

5.3.3 통제방법

① 네트워크 시스템의 최고관리자 권한은 기술보안담당자만이 제어할 수 있고, 최소한의 과리 계정만 생성하도록 한다.

② 작업이 허용된 PC등은 당사의 DRM프로그램을 설치해야 작업을 할 수 있으며, 기술보안담당자는 프로젝트기간에 수시로 로그를 확인하도록 한다.

③ 외부인이 유선 네트워크에 접속하여 작업 시 시작부터 끝까지 기술보안담당자

와 동석하여 작업한다.

5.4 무선네트워크 관리

5.4.1 허용기준

① 모든 무선 네트워크는 암호를 걸어 관리한다.
② OA망과 GUEST망은 별도 분리하여 관리한다.
③ OA망은 업무와 관련된 무선장비만 허용하며, GUEST망은 외부손님 및 휴대기기 WIFI사용 용도에 한하여 허용한다.

5.4.2 허용절차

① 모든 무선 네트워크 연결 권한은 기술보안담당자가 통제하도록 한다.
② OA망에 접속 시에는 장비명, 사용목적, 사용기간 등을 기재하여 기술보안담당자에게 신청한다.
③ 기술보안담당자는 신청한 장비의 신뢰도, 사용목적의 적절성, 허용 치 이상의 트래픽 증가 및 최신보안 패치 확인 등의 보안성 검토를 거쳐 허용한다.
④ 접속장비의 기간이 1주일 이상 장비 접속이 필요한 경우, 정보보안그룹의 협의를 거쳐 주변 네트워크의 영향을 검토하여 정규장비로 등록하고 관리한다.
⑤ GUSET망에 접속 시 해당 업무 팀보안 담당자가 통제한다.

5.4.3 통제방법

① 인가되지 않는 AP(Access Point)의 사용은 금한다.
② 네트워크 시스템의 최고관리자 권한은 기술보안담당자만이 제어할 수 있고, 최소한의 관리자 계정만 생성하도록 한다.
③ 모든 무선 AP 접속 암호는 WPA2-AES 인증 인상으로 설정한다.
④ 무선 AP는 기술보안담당자가 주 1회 이상 접속하여 비인가 장비 접속확인 및 설정값, 백업, 최신 펌웨어 업데이트 등을 시행한다.

5.5 중요네트워크 이중화 관리

5.5.1 이중화 대상 정의

① 이중화는 네트워크 장비의 이중화를 통하여 중요한 업무 네트워크의 안정성을 보장한다.
② 실시간 서열과 생산실적을 담당하는 FA망과 설계 및 도면취급을 담당하는 기술연구소 망이 이중화 대상이다.

5.5.2 이중화 기준

① 기존 네트워크 구성의 동일한 구성 및 사양으로 이중화를 진행한다.
② 장애발생 및 복구 시에도 중단이 없도록 네트워크 구성을 한다.
③ 이중화 장비 모두 활성화 시켜 동작하는 구성을 기본으로 하며, 장애가 발생해도 1대가 모든 트래픽을 처리할 수 있는 사양의 장비로 구성한다.

5.5.3 이중화 점검

① 월 1회 이중화된 네트워크 장비의 시험 테스트를 진행한다.
② 분기별로 로그를 수집하여 트래픽이 큰 폭으로 꾸준히 증가할 경우 충분한 성능을 갖춘 장비로 교체하여 최상의 상태를 유지해야한다.

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.