

주요정보통신기반시설 보안관리 세부지침

제1장 총 칙

제1조 (목적) 이 지침은 항공교통본부(이하 "교통본부"라 한다)와 그 소속기관이 보유한 정보통신기반시설의 보안에 필요한 사항을 정의하여 정보통신기반시설을 사이버 침해 위협으로부터 효과적으로 보호·운영 관리함을 목적으로 한다.

제2조 (적용범위) 이 지침은 교통본부와 그 소속기관에 대하여 적용한다.

제3조 (정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "정보보안" 또는 "정보보호"라 함은 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송·수신되는 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 「국가사이버안전관리규정」 제2조제3호의 사이버안전을 포함한다.
2. "정보시스템"이라 함은 「전자정부법」 제2조제13호에 따른 서버, 네트워크 장비, 보안장비, 데이터베이스, 응용프로그램 등 정보통신기반시설 운영을 위한 기기와 소프트웨어를 말한다.
3. "내부망"이라 함은 교통본부에서 운영하는 정보통신망 중에서 인터넷과 분리된 업무 전용(專用) 정보통신망을 말한다.
4. "인터넷망"이라 함은 교통본부에서 운영하는 정보통신망 중에서 소속 직원 등이 이용하는 인터넷과 연동된 정보통신망을 말한다.
5. "시스템관리자"란 「항공교통본부 주요정보통신기반시설 보호지침」 제5조의 기반시설 운영·유지관리 분야 정보보호책임자를 말한다.
6. "사용자"란 시스템관리자, 시스템운영자 등 정보시스템을 관리·운영하는 자를 말한다.
7. "휴대용 저장매체"라 함은 디스켓·CD·외장형 하드디스크·USB메모리 등 정보를 저장할 수 있는 것으로 PC·서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

제4조(기반시설 정보보안담당관) ① 정보통신기반시설의 보안관리 업무의 총괄 책임자는 「항공교통본부 정보보안업무지침」 제5조에 명시된 정보보안담당관으로 지정한다.

제5조(시스템관리자의 업무) ① 시스템관리자는 다음 각 호의 보안업무를 수행한다.

1. 정보시스템 보안 설정 및 관리 업무
2. 정보시스템 변경작업에 대한 적절성 검토
3. 정보시스템의 주기적인 보안점검
4. 침해사고 발생 시 시스템 분석 지원 업무
5. 재해발생 시 정보시스템 복구 업무
6. 정보자산 목록 갱신 및 중요도 평가
7. 정보자산 중요도, 보안등급 및 검토/분류, 보안 대책 수립

제2장 시설 보안

제6조(보호구역 시설) ① 정보통신기반시설이 존재하는 항공관제장비실 및 항공관제제어실은 「항공교통본부 보안업무규정」 제34조(보호구역)에 따라 통제구역으로 지정한다.

② 통제구역으로 설정된 곳에는 「국토교통부 보안업무규칙」 [별지 제8호 서식]에 따른 표지를 출입문 중앙부 또는 잘 보이는 곳에 부착하여야 한다. 단, 보안에 민감한 시설로 외부에 노출을 극히 제한하는 시설의 경우 정보보안담당관과 협의하여 생략할 수 있다.

③ 통제구역으로 지정된 시설은 다음 각 호의 보호설비를 구축, 운영하여야 한다.

1. 모든 출입문에 출입통제 장치 및 CCTV 설치
2. 휴대용 저장매체를 보관할 수 있는 용기 비치
3. 정전에 대비한 비상전원 공급 및 시스템의 안정적 중단 등 전력관리 대책
4. 비상조명 장치 등 비상탈출 대책
5. 화재 방지를 위한 탐지기, 경보기 및 소화설비

④ CCTV 운용 시 다음 각 호의 보호대책을 적용하여야 한다.

1. 업무망, 인터넷망, 기반시설망과 물리적으로 네트워크를 분리·운영
2. CCTV의 관리자 페이지 접속시 비밀번호를 사용하도록 설정
3. CCTV 관리서버는 비인가자의 접근이 불가하도록 물리적인 보호조치

제7조(출입관리) ① 정보통신기반시설 설치·운영 장소는 출입통제시스템을 설치하고 인가된 사용자만 출입이 가능하도록 통제하여야 한다.

② 통제구역의 출입이 빈번한 출입자는 상시출입자로 지정하여 [별지 제1호

서식] ‘상시출입자 명부’를 작성·관리하고 주기적으로 상시출입자의 적정성을 검토하여야 한다.

③ 상시출입자 외의 일시적으로 출입하는 자는 [별지 제2호 서식] ‘통제구역 출입자 명부’에 따라 출입내역을 기록하고 그 내용을 3개월 이상 보관하여야 한다.

④ 외부인의 통제구역 출입 시 입회자의 안내를 받아야 하며 퇴실 시까지 상시 동행하여야 한다.

제8조 (휴대용 기기 반출·입) ① 외부 휴대용 기기의 반입은 원천 금지하고 불가피하게 반입·사용하는 경우 다음 각 호의 보호대책을 적용하여야 한다.

1. [별지 제3호 서식] ‘휴대용 기기 반출·입 대장’을 작성
2. 악성코드 감염여부 및 무결성 검사

제3장 정보통신기반시설 도입

제9조(정보통신기반시설 도입시 고려사항) ① 제어시스템을 도입·운용하고자 할 경우 사업 계획 단계(사업 공고 전)에서 국가정보원장이 배포한 「국가·공공기관 제어시스템 보안가이드라인」을 준수하여야 한다.

② 국가안보상 중요한 정보통신기반시설을 운용할 경우 인터넷 및 일반사무용 내부망과 분리·구축하여야 한다.

③ 제2항에도 불구하고 정보통신기반시설을 인터넷망과 연동할 필요가 있을 경우 연동 구간에 일방향 전송장비 설치 등 안전한 망 연동 수단을 설치·운용하여야 한다.

④ 정보보호시스템은 국내용 CC인증을 받았거나 보안적합성 검증을 받은 제품을 도입하여야 한다.

제10조 (보안성 검토) ① 정보통신기반시설의 도입, 변경으로 정보시스템 구성 환경에 중대한 변화가 있는 경우 시스템관리자는 정보보안담당관에게 보안성 검토를 의뢰하여야 한다.

② 보안성 검토에 관련한 세부사항은 「항공교통본부 정보보안업무지침」 제2장 정보화사업 보안 제2절(보안성 검토)을 준용한다.

제11조 (정보시스템 설치시 보안설정) ① 정보통신기반시설은 물리적 보안이 구성되어 있는 보호구역에 설치한다.

② 운영체제 및 장비의 최초 설정된 계정 및 비밀번호의 초기값을 변경하여야 하며, 시스템의 설치 목적에 따른 기능을 제외한 모든 기능을 해제(불필요한 서비스 및 포트 제거)하여야 한다.

③ 정보시스템 최초 설치 시(운영체제 재설치 포함) [별지 제4호 서식] ‘보안

요구사항’을 참고하여 ‘주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드’에 따라 보안설정을 적용하여야 한다. 시스템관리자는 [별지 제5호 서식] ‘보안 요구사항 검수항목’에 따라 보안 요구사항 반영여부를 점검하고 그 결과를 정보보안담당관에게 보고하여야 한다.

④ 시스템의 소프트웨어는 안정성이 입증된 가장 안전한 버전을 사용하여야 하며, 최신 보안 업데이트를 적용하여야 한다.

제12조(정보시스템 자산관리) ① 시스템관리자는 PC·서버, 네트워크 장비 등 정보통신기반시설 관련 자산을 [부록 2] 「정보자산관리지침」에 따라 정보자산의 식별, 분류, 중요도 평가 및 보안등급 분류 후 [부록 2] 「정보자산관리지침」 [별지 제1호 서식] ‘자산관리대장’에 기록하여야 한다.

② ‘자산관리대장’은 항상 최신의 현황이 반영되어야 하며 연 1회 이상 정보시스템 변동 여부를 확인하여야 한다.

③ 정보통신기반시설 정보자산 관리에 관련된 구체적인 사항은 [부록 2] 「정보자산관리지침」을 따른다.

제13조 (정보통신기반시설 변경) ① 정보통신기반시설의 폐기 또는 용도변경 등의 사유로 정보시스템을 반출하는 경우 반출 전에 정보시스템의 저장장치를 데이터 복구가 불가능하도록 완전삭제 또는 물리적으로 파쇄 하여야 한다.

② 변경된 정보시스템 현황은 ‘자산관리대장’에 즉시 반영하여 갱신하며 정보보안담당관에게 보고한다.

③ 전자정보 저장매체의 불용처리에 관련된 구체적인 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용처리지침」을 따른다.

제4장 계정 관리

제14조 (사용자 관리) ① 사용자 계정의 생성은 [별지 제6호 서식] ‘접근권한 신청서’를 작성하여 시스템관리자의 승인을 받아 생성한다.

② 시스템관리자는 정보통신기반시설에 대한 접근권한 및 시스템 사용상의 권한 설정 시 다음 각 호를 준수해야 한다.

1. 정보시스템의 운영 중인 계정 외의 모든 불필요한 계정을 삭제한다.
2. 계정 부여 시 신청자의 업무에 따라 필요한 최소한의 권한으로 차등 부여한다.
3. 관리자 계정의 비밀번호는 정보시스템 운영 관련자 외에 누구에게도 공유 또는 유출해서는 안 된다.
4. 정보시스템 접속 시 ID/PW, 접속경로, 인증서 등이 하드코딩 되지 않도록 설정한다.
5. 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임

이 사용자 본인에게 있음을 명확히 인식시켜야 한다.

③ 관리자 권한을 가진 계정은 시스템관리자의 승인 하에 최소한의 인원에게 부여하여야 하며, 관리자 계정 현황은 별도로 [별지 제7호 서식] ‘관리자 계정 관리대장’에 기록하고 관리하여야 한다.

④ 시스템관리자 변경 시에는 모든 장비의 비밀번호를 변경하고, 퇴직 시에는 사용자 계정과 비밀번호를 삭제한다.

⑤ 시스템관리자는 정보시스템 계정 및 접근권한 부여 현황을 [별지 제8호 서식] ‘접근권한 점검결과’를 활용하여 분기 1회 이상 점검하고 해당 결과를 정보보안담당관에게 보고하여야 하며 접근권한 점검 시 권한의 과다 부여, 오남용 등 문제점이 발견된 경우 원인 분석 후 즉시 보완하여야 한다.

⑥ 사용자 계정은 1인 1계정을 사용하고 공용계정 및 추측 가능한 식별자는 사용하지 않는 것을 원칙으로 한다. 단, 불가피하게 공용계정의 사용이 필요한 경우 정보보안담당관의 승인을 득하여야 한다.

⑦ 시스템관리자는 사용자 계정 삭제 시 다음 각 호를 준수한다.

1. 계정을 삭제해야 하는 사유가 발생 시에는 즉시 삭제한다.

2. 퇴직, 휴직, 인사이동, 계약해지 등에 따른 업무 변동 시 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공용계정 변경 등 기반시설에 대한 접근을 통제한다. 단, 삭제할 수 없는 계정의 경우 비밀번호를 변경한다.

제15조 (비밀번호 생성 및 관리) ① 초기, 임시 비밀번호는 로그인 시 지체 없이 변경하며 모든 사용자 계정은 비밀번호가 부여되도록 하고 비밀번호는 최소한 3개월마다 변경한다.

② 비밀번호는 2종류(영문 대문자 및 소문자, 숫자, 특수문자) 이상의 문자를 조합하여 최소 10자리 이상 또는 3종류 이상의 문자를 조합하여 최소 9자리 이상의 길이로 구성한다.

③ 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력 오류가 연속하여 발생한 경우 즉시 해당 사용자 계정의 접속을 차단하도록 한다.

④ 기타 비밀번호 생성 및 관리와 관련된 구체적인 사항은 「항공교통본부 정보보안업무지침」 제73조(비밀번호 관리)를 따른다.

제5장 접근통제

제16조 (접근통제) ① 정보통신기반시설에 대한 접근가능 사용자 및 사용자 그룹, 접속 대상 시스템 및 응용프로그램, 접속 목적 등을 식별하여 정의하고 정의된 사용자 이외에는 접근을 허용하지 않는다.

② 정보통신기반시설의 네트워크는 사설 IP를 이용하여 구축하며 개발, 운영, 테스트, 교육 등 기능별 네트워크 대역을 분리하고 서로간의 접근이 불가하도록 접근통제 정책을 적용하여야 한다.

1. 네트워크 대역 분리(망간 혼용 금지)
2. 분리된 네트워크 대역 간의 원격 접속 금지
3. 불필요한 접근 정책 설정 금지

③ 교통본부 기관 외부에 위치한 정보시스템과 연계되어 작업이 수행되어야 하는 경우 해당 네트워크 구간은 정보보호시스템을 이용하여 논리적인 망분리 및 접근통제를 적용하여야 한다.

제17조(원격 유지보수) ① 인터넷 등 외부 네트워크를 통한 원격 유지보수는 원칙적으로 금지한다.

② 서버·보안장비·네트워크 장비 등의 관리자 페이지 접속을 위한 관리 전용 PC를 지정·운영하여야 한다.

③ 제2항의 관리 전용 PC만 접근이 가능하도록 서버, 네트워크 장비, 보안장비 정책에 설정하여 운영한다.

④ 유지보수, 장애처리 등의 필요성에 의하여 제3자에게 접근권한을 부여해야 할 경우, 시스템관리자의 승인 하에 임시적으로 권한을 부여하고 관련 업무 종료 시 권한을 회수한다.

제18조(비인가 시스템 접근통제) ① PC·서버, 네트워크 장비의 USB·LAN 포트 등 입출력장치 단자는 잠금장치 또는 보안스티커 등을 사용하여 물리적으로 봉인하여야 하며, 해당 봉인장치는 [별지 제12호 서식] ‘봉인장치 관리대장’을 활용하여 사용내역을 기록하여야 한다.

② 비인가 무선AP 사용 점검을 반기 1회 이상 실시하고 점검결과를 정보보안담당관에게 보고하여야 한다.

③ 해당 정보시스템이 제공하는 서비스 포트 이외의 불필요한 포트는 차단되어야 하며, 시스템에 설치된 서비스를 조사하여 불필요한 서비스는 제거한다.

④ 공유 폴더의 필요성을 검토하여 불필요한 공유 기능을 제거한다.(기본공유 제거)

⑤ 정보시스템에 접속한 후 사용자나 다른 시스템으로부터 일정시간(10분 이상) 동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시키는 설정을 적용한다. 단, 개발 업무 및 모니터링 등 정보통신기반시설 운영상 예외 필요시 시스템관리자 승인 하에 제외할 수 있다.

제6장 운영관리

제19조 (운영 및 성능관리) ① 시스템관리자는 기반시설에 대한 구동, 조작 방법, 명령어 사용법, 운용 순서, 장애 조치 및 비상연락망 등 정보통신기반시설 운영매뉴얼을 작성한다.

② 시스템관리자는 정보시스템의 정상 작동 여부 확인 및 시스템 자원 상태 감시가 가능한 모니터링 환경을 구축한다.

③ 시스템관리자는 주요 정보시스템 성능관리(CPU, 저장장치, 메모리 등)를 통해 축적된 가용성 정보를 모니터링하고, 신규 시스템 도입 또는 업그레이드 등의 필요 여부를 검토 한다.

제20조 (취약점 점검) ① 정보보안담당관은 정보통신기반시설에 대해 연 1회 이상 취약점 분석·평가를 수행하여 결과에 따라 이행계획을 수립·시행하여야 한다. 정보보안담당관은 취약점 분석·평가 이력을 관리하며, 이전 취약점이 재발생하는 등의 문제점에 대한 보호대책을 강구한다.

② 정보보안담당관은 최신 보안취약점 발생 여부를 지속적으로 파악하고 정보통신기반시설에 미치는 영향을 분석하며, 시스템관리자는 해당 보안취약점을 조치하여야 한다.

제21조 (보안패치 관리) ① 시스템관리자는 정보통신기반시설의 소프트웨어 버전 정보, 패치일 등을 확인할 수 있도록 관리하고 최신 보안패치 여부를 주기적으로 확인하여야 한다.

② 시스템관리자는 정보통신기반시설의 운영체제, 시스템 유틸리티 등의 긴급하고 중요한 보정사항에 대하여는 즉각적인 패치 또는 패치 일정을 수립하여 진행하여야 한다.

③ 소프트웨어의 임의적 변경은 기능상의 오류를 발생시킬 위험이 있으므로 테스트 서버 등에 사전 적용하여 영향도 분석 후 변경하여야 한다.

④ 공개 인터넷 접속을 통한 패치적용은 원칙적으로 금지한다.

⑤ 서비스 영향도 등에 따라 최신의 패치 적용이 어려운 경우 시스템관리자는 해당 정보시스템에 대한 모니터링 강화 등 보완대책을 강구한다.

제22조 (로그관리) ① 시스템관리자는 감사 및 정보보호 사고 발생 시에 추적성을 확보하기 위하여 적절한 로그의 수준을 정의하며, 다음과 같은 사항을 고려한다.

1. 접속자, 정보시스템·응용프로그램 등 접속대상
2. 로그인·오프, 자료의 열람·출력 등 작업 종류 및 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

② 시스템관리자는 로그에 대해 아래와 같은 기준으로 관리한다.

1. 정보통신기반시설 접속내역을 기록한 로그에 대해서 문서화된 공식적인 요청이나 법률에 의한 협조 요청에 의하지 않고는 타인에게 공개할 수 없다.
2. 이벤트가 기록되어 있는 정보통신기반시설 로그는 최소 1년 이상 보관되도록 한다.
3. 정보시스템의 시간은 표준시로 동기화 한다.

③ 시스템관리자는 정해진 기준에 따라 로그가 생성되도록 시스템을 설정하

고, 로그기록에 대한 접근권한은 관리자 계정으로 제한한다.

④ 로그 데이터는 별도의 시스템 또는 저장장치를 통해 백업하고, 백업된 로그기록에 대한 접근권한은 최소화하여 부여한다.

⑤ 시스템관리자는 [별지 제9호 서식] ‘로그 점검결과’를 활용하여 월 1회 이상 사용자의 접속기록에 대한 로그분석을 수행하고, 점검 결과 이상유무 및 특이사항을 관리하며 침해사고 징후가 발견된 경우 「사이버안전 위기대응 실무매뉴얼」에서 정하는 절차에 따른다.

제23조 (바이러스 백신 설치 및 운영) ① 시스템관리자는 서버 및 PC에 바이러스를 진단·치료할 수 있는 백신 프로그램을 설치하고 다음 각 호의 기능을 사용하여야 한다. 단, 서버에 적합한 백신 프로그램이 없는 경우 운영체제 자체 방화벽을 사용하거나 생략 할 수 있다.

1. 바이러스 백신은 항상 최신 버전의 엔진으로 유지
2. 실시간 감시 기능 및 정밀 검사 예약기능의 활성화(최소 월 1회 이상 정밀 검사를 수행) 단, 시스템의 부하를 고려하여 서비스에 지장을 초래할 경우 사용하지 않을 수 있다.

3. 검역소 및 시스템 로그 보관 기간은 1년 이상 설정

② 바이러스 발견 시 즉각 정보보안담당관에게 통보하고 해당 서버를 네트워크에서 분리해 추가적인 정밀 검사를 수행한다.

③ 저장매체의 악성코드 감염여부를 확인하기 위한 전용PC(클린PC)를 설치하고 휴대용 저장매체를 이용한 자료전송 시 악성코드 감염여부 및 무결성 검사를 수행한다. 단, 클린PC는 백신을 제외한 어떠한 S/W도 설치되지 않아야 한다.

제24조 (휴대용 저장매체 보안) ① 시스템관리자는 정보통신기반시설 운영 및 관리를 위해 사용되는 휴대용 저장매체를 지정하고 [별지 제10호 서식] ‘휴대용 저장매체 관리대장’을 작성·관리하여야 한다. 단, 휴대용 저장매체 관리시스템을 운용하는 경우 해당 관리시스템에 등록하여 관리할 수 있다.

② 정보통신기반시설 유지보수를 위한 USB 사용은 금지하고 자료전송 시 광디스크(CD/DVD 읽기전용)를 사용하여야 한다.

③ 외부에서 휴대용 저장매체를 반입·사용하는 경우 제8조제1항에 따른 보호대책을 시행하여야 한다.

④ 시스템관리자는 개별사용자의 휴대용 저장매체 무단 반출 및 미(未)등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 정기적으로 월 1회 이상 점검하고 [별지 제11호 서식] ‘휴대용 저장매체 점검대장’을 작성·관리하여야 한다.

⑤ 그 밖의 휴대용 저장매체 보안과 관련한 사항은 국가정보원장이 배포한 「USB메모리 등 휴대용 저장매체 보안관리지침」을 준수하여야 한다.

제25조(정보시스템 현황자료 관리) ① 다음 각 호의 정보통신기반시설 현황 자

료는 대외비로 등록하여 관리하여야 한다.

1. 기반시설 세부 구성현황(IP 세부 할당정보 포함)

2. ID/비밀번호 현황

3. 기반시설 설계도면

4. 그 밖의 보호할 필요가 있는 기반시설 관련 중요 자료

② 대외비 또는 비밀로 생산한 경우 다음의 보안대책에 따라 관리하여야 한다.

1. 비밀, 대외비 저장매체 별도 지정·보관 및 등급 간 혼용 보관 금지

2. 타 전산망과 분리된 PC 내 독립 폴더를 지정하고 암호화

3. 종이문서로 출력한 경우 금고 또는 이중철제캐비닛 등 잠금장치가 있는 안전한 용기에 보관

부 칙

제1조(시행일) 이 지침은 발령한 날부터 시행한다.

상시출입자 명부

(2020년 10월 기준)

[illegible]

통제구역출입자 명부

[illegible]

보안 요구사항

시스템명	주요 내용
문서화	○ 구성변경에 따른 운영매뉴얼 현행화 ○ 시스템 구성도, 정보자산관리대장, 변경이력관리 등 문서 현행화
계정 관리	○ 계정(ID·비밀번호)를 안전하게 관리하여 악의적인 공격자가 계정 정보를 획득·유추할 수 없게 함
서비스 관리	○ 서비스 목록 관리 및 불필요한 모든 서비스 제거
서비스 실행권한 관리	○ 제어 명령, 운영체제(O/S) 명령, 중요파일의 실행·열람 권한은 제어시스템 운영에 필요한 사용자에게 한해 최소화 부여 관리
운영환경 설정 관리	○ 기본(default) 비밀번호 변경, 시험용 계정 제거 등 제어시스템 운영 환경을 안전하게 설정
네트워크 관리	○ 제어망 구성, 접근통제 및 통신보호 등의 보안대책 적용
DB·웹 관리	○ 암호화, 인증, 서비스 취약점 분석 등 DB·웹 보안대책 적용
제어기기	○ 제어기기 인증, 암호화, 접근통제, 모니터링 등의 보안대책 적용
물리적 보안	○ 제어시스템 설치·운영 공간에 대한 물리적 접근통제 및 보호대책 적용
감사	○ 장애 및 사고분석, 재발 방지대책 수립을 위한 감사정책 수립 및 시행
안전한 S/W 개발	○ S/W 개발 프로세스에서 보안을 고려한 개발, 안전하지 않은 것으로 알려진 프로그래밍 사용 제한 등 S/W 취약점 최소화

보안 요구사항 검사항목

보안 요구사항		검수
항목	세부 항목	
ID/비밀번호 관리	필수 계정 이외의 계정 삭제	
	Default 계정 및 비밀번호 변경	
	기관 비밀번호(패스워드) 정책 반영	
접근 관리	로그인 실패횟수 제한 (잠금 기간 설정)	
	원격 관리 접근 통제 (관리자 IP 등록)	
	Session timeout 설정	
	로그온 시 경고 메시지 설정	
서비스 관리	불필요한 서비스와 프로그램 제거	
	안전한 통신 서비스 제공 (암호화 전송 통신, ex. ssh, sftp, https 등)	
감사	감사 로그를 남기도록 설정 (로그인, 경고메시지, 정책변경 로그)	
	원격 로그 서버 사용	
	NTP 서버 연동	

관리자계정 관리대장

[illegible]

접근권한 점검결과

확인자
/

점검자	성명		부서	
-----	----	--	----	--

점검대상	시스템명	
	관리책임자	

구분	점검항목	이상유무 (O,X)	결과 상세
1	공식적인 절차에 따른 접근권한 부여 여부		
2	접근권한 분류체계의 업무목적(직무) 및 보안정책 부합 여부		
3	접근권한 부여 승인자에 대한 적절성		
4	직무변경 시 기존 권한 회수 후 신규업무에 적합한 권한부여 여부		
5	업무목적 이외의 과도한 접근권한 부여 여부		
6	사용하지 않은 유휴계정 존재 여부		
7	특권자 계정 사용의 적절성 여부		

로그 점검결과

확인자
/

점검일				점검자	
대상 시스템명					
점검 로그 기간					
점 검 결 과					
구분	점검항목		이상유무 (O,X)	결과 상세	
1	로그인 실패				
2	시스템 파일에 대한 접근 실패				
3	의심스러운 사용자 명령의 발생				
4	접속이 필요 없는 시스템에서의 로그인				
5	비인가된 새로운 ID의 생성				
6	비인가된 새로운 서비스 생성				
7	기타 비정상 시스템 이벤트				

휴대용 저장매체 관리대장(000용)

< 관리자 : 김유0 >

연번	관리번호 (시리얼번호)	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고 (사유)
1	00-일반-01 (E-D900-04-3705B)	USB	19.11.11	항행전자부 과장 김OO	20.11.10	자성소거 후 재사용 (00-일반-03)	고장
2	00-일반-02 (NP00T512787J)	CD	19.07.19	항행전자부 홍OO	20.07.18	물리적 파기	용도 전환 (재사용)

* 일반용/비밀용/제어시스템용으로 구분하여 작성

[별지 제11호 서식]

휴대용 저장매체 점검대장

< 관리자 : >

[illegible]

봉인장치 관리대장

순번	장비명	봉인장치 식별부호	봉인/개봉, 일자	사용자	사용목적	관리자 확인
1	시험평가1	XX-XX-XX	개봉, 2020.06.01	항행전자부 과장 김OO	파일 전송	
2	교육훈련2	XX-XX-XX	개봉, 2020.12.12	항행전자부 홍OO	파일 전송	
3						
4						
5						