강릉원주대학교 전산망 운영지침 전부개정 전문

제정 2014.04.07.
개정 2018.07.06.
개정 2021.01.28.
개정 2023.02.21.

제1조(목적) ① 본 지침은 강릉원주대학교(이하 “대학”이라 한다) 정보통신망 (이하 “전산망”이라 한다)을 합리적이고 효과적으로 관리·운영하여 원활한 전산망 서비스를 제공하는 것을 목적으로 한다.

제2조(용어 정의) 본 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “전산망”이라 함은 복수의 컴퓨터와 단말장치를 통신회선망과 공통프로토콜에 의하여 상호 통신이 가능하게 하는 개념을 말한다.
2. “포트”라 함은 다른 장치에 접속되는 물리적 또는 논리적 위치를 말한다.
3. “랜(LAN)”이라 함은 통신장비 또는 컴퓨터 연결을 위해 사용되는 통신선을 말한다.
4. “통신장비”라 함은 전산망 구성을 위한 통신접속 장비를 말한다. 라우터, 스위치, 허브 등이 있다.
5. “전산망 장비실”이라 함은 건물 내 통신장비 및 분배 시설이 위치하는 공간을 말한다.
6. “무선중계기(AP)”라 함은 유선랜과 무선랜을 연결해주는 장치를 말한다.
7. “도메인(Domain)”이라 함은 인터넷상의 컴퓨터 주소를 알기 쉽게 영문으로 표현한 것을 말한다.

제3조(지원 범위) ① 전산망은 대학의 학칙에 명시된 교육조직, 행정조직, 부속시설, 산학협력단 및 학교기업 등으로서 강릉캠퍼스 및 원주캠퍼스에 위치하고, 정보화본부장이 승인한 경우에 한하여 지원한다. 다만, 학생생활관의 기숙시설은 제외한다.

② 제1항을 제외한 구역은 자체적으로 전산망을 구축하여 정보화본부장의 승인을 받아 본 지침을 준수하는 조건으로 대학 전산망에 연결할 수 있다.

제4조(신·증축 건물의 통신시설 및 장비) ① 건물의 신·증축으로 인해 전산망 관련 시설 및 장비의 이전 혹은 설치가 필요한 경우, 소요 경비는 해당 건물 신·증축 공사의 예산에 계상하는 것을 원칙으로 한다.

② 신·증축 건물의 시공 시에는 다음 각 호의 통신 시설이 포함되어야 하며, 건물 설계 시 담당기관(부서)은 LAN 시설에 대하여 반드시 정보화본부와 협의하여야 한다.

1. 광케이블은 Single-Mode(LC타입)로 8 Core 이상을 기본으로 설치하며, 상위 접속지점 등 제반 사항에 대하여 정보화본부와 사전 협의한다.
2. 건물 내의 모든 실에 UTP 케이블 2회선 이상(CAT.5E 이상, 2구 Outlet 포함)을 설치하며 그 길이는 75m를 초과할 수 없다.
3. UTP 케이블 길이가 75m를 초과하는 건물에는 광케이블을 포설한다.
4. 랙(Rack)은 FDF, Patch Panel, 장비 등을 수용할 수 있는 크기로 하며, 전원은 단독으로 설치하고 UPS 전원 활용을 권장한다.
5. 준공 시 케이블(광, UTP) 도면과 시험성적서, 선번장 등 서류(또는 파일형태)를 정보화본부에 제공

하고, Patch Panel, Outlet, 패치코드에 식별 라벨을 부착한다.

6. 전산망 장비실에는 통풍 및 환기시설을 설치한다.

7. 사무실 내 사용자케이블(Outlet↔PC) 및 스위칭 허브 장비는 사용자가 갖춘다.

8. 무선중계기(AP), POE 등 무선랜 장비 설치는 정보화본부에서 운영 중인 관리장비와의 연동가능 여부를 사전 검토하여야 한다.

9. 무선중계기 컨트롤러 설치가 필요한 경우는 AP 수량에 따라 정보화본부에서 지정하는 장비로 해당 기관에서 구매하여야 한다.

10. 무선중계기(AP)는 정보화본부에서 지정하는 보안성이 검증된 장비로 설치한다.

11. 무선중계는(AP)는 벽 또는 천정에 매립하지 않고 밖으로 부착하여 설치한다.

③ 신·증축 건물에 신규 설치된 전산망 장비는 정보화본부장의 승인을 얻어 정보화본부로 관리 전환할 수 있으며, 관리 전환하려는 대상 장비의 물품명, 수량, 가격 및 무상하자보수 기간 등의 정보, 기술지원확약서를 정보화본부에 제공하여야 한다.

제5조(전산망 포트 관리) ① 건물 내 각 호실당 1개의 전산망 포트 연결을 지원하며, 각 호실에서 2대 이상의 단말기에서 네트워크를 접속하고자 할 경우 자체적으로 허브(스위치) 장비를 구매하여야 한다.

② 각 호실에서 10대 이상의 단말기 사용으로 추가 포트사용 및 설치가 필요할 경우에는 정보화본부와 협의하여야 한다.

③ LAN포트 파손 및 신설 시에는 해당 기관(부서)의 자체 예산으로 한다.

④ LAN 포트가 설치된 호실의 구조가 변경될 경우, 해당 호실에서 사용 가능한 포트는 기존과 동일하게 유지되어야 하며 포트 배치 비용은 해당 호실 구조 변경 예산에 계상한다.

제6조(무선랜 운영) ① 정보화본부에서 설치한 장비 외 무선랜 장비의 설치는 정보화본부와 사전협의가 필요하며, 해당 기관에서 장비 및 설치비용을 부담하고 기술지원 및 관리 운영은 정보화본부에서 지원한다. 시설 구축 및 운영은 제4조 제2항의 제7호~제11호에 따른다.

② 사용자가 임의로 무선중계기(AP)를 설치할 수 없으며, 임의로 설치된 무선중계기는 정보화본부의 철거 요청 시 즉시 철거하여야 한다.

③ 무선중계기(AP) 설치 시 주변의 무선중계기(AP) 간에 간섭현상이 일어나지 않게 최대한 채널을 조정하여 설치한다. (방송통신위원회 권고사항인 1,5,9,13 채널 중에서 사용한다.)

④ 대학 무선랜(GWNU_WLAN)은 통합계정(대학 포털사이트 로그인 계정)을 이용하여 인증 후 사용할 수 있으며, 공공무선랜(GWNU_FREE_WIFI)은 인증 절차 없이 사용할 수 있다.

⑤ 일반인을 대상으로 하는 대학 행사 시 임시 아이디를 정보화본부로부터 발급받아 무선랜을 사용할 수 있다.

⑥ 글로벌 무선랜 공동 활용 서비스 “eduroam”에 가입되어 있는 교육·연구 기관 소속 사용자는 별도의 허가 없이 소속기관에서 인증받고 eduroam 서비스를 이용할 수 있으며, 정보화본부에서는 필요에 따라 포트 및 대역폭을 제한할 수 있다.

제7조(IP주소 운영) ① IP주소 할당 대상자는 대학 구성원으로 하며, 대학 포털사이트에서 신청하여 정보화본부의 승인을 받아 사용하여야 한다.

② 할당된 IP주소에 대한 책임자 및 사용자, 단말기의 정보 변경에 따른 신규, (명의)변경, 반납, 갱신 등은 대학 포털사이트에서 신청한다.

③ 1개의 MAC주소(랜카드의 물리적주소) 당 1개의 IP주소를 할당하며, 사용자가 임의로 MAC주소를 변경할 경우 할당된 IP주소는 정보화본부에서 강제로 회수할 수 있다.

④ IP주소를 6개월 이상 미사용하면 IP주소 관리시스템에서 사용중지 되며, 사용중지 후 6개월이상 경과하면 정보화본부에서 강제로 회수할 수 있다.

제8조(도메인 운영) ① 도메인은 IP주소를 할당받은 사용자가 대학 포털사이트에서 신청하여 정보화본부의 승인을 받아야 사용할 수 있다.

② 할당된 도메인에 대한 책임자, 사용자, 단말기 정보(메일서버, 네임서버 운영 등) 등 정보 변경 발생 시 대학 포털사이트에서 신청한다.

③ 대학 도메인은 대학에서 사용 중인 IP주소에 한하여 사용할 수 있다. 다만, 교외 기관, 클라우드 서비스 등에서 사용하는 외부 IP주소는 정보화본부장의 승인을 받아 사용할 수 있다.

④ 한 개의 IP주소에 대해 최대 4개까지의 도메인(호스트) 발급을 허용한다.

⑤ 반납된 IP주소와 연계된 도메인, 메일서버, 네임서버는 IP주소 반납처리 시 자동 반납된다.

⑥ 다음 각 호의 경우 해당 도메인 서비스를 즉시 중단할 수 있다.

1. 음란사이트 운영
2. 상업적 용도의 사이트 운영
3. 지식재산권 침해 및 개인정보보호 미이행
4. 기타 법률에 위반되거나 미풍양속을 저해하는 내용 게재

제9조(서비스 포트 운영) ① 교외에서 교내로의 주요 서비스포트 접근은 차단하며 교내에서 교외로의 모든 포트 접근은 허용한다. 다만, 취약한 서비스용, 일부 웜/바이러스 유포용, 데이터베이스(DB) 접속용 등의 서비스포트([별표1])는 정보화본부에서 별도로 관리하며 보안상 차단조치된다.

② 차단된 포트를 교육·연구·업무 목적 등으로 사용하고자 할 때에는 다음 각 호와 같이 신청하여야 한다.

1. 서비스포트 접근신청은 사용자가 대학 포털사이트에서 신청한다.
2. 발신지의 IP주소가 고정되지 않는 서비스포트 허용신청은 불허하며, 대학에서 제공하는 SSL VPN 서비스를 이용하여야 한다.
3. 보안이 취약한 서비스포트(Telnet, FTP 등)는 접근신청을 할 수 없으며, 안전한 원격용 서비스포트(SSH, SFTP 등)는 포트번호를 변경한 후 신청하여야 한다.

③ 사용자가 서비스 포트를 신청하면 정보화본부에서는 계정 비밀번호 안전도, 최신 보안업데이트 상태, 백신프로그램 설치 유무 및 업데이트 상태 등을 점검·확인 후 서비스 포트 사용을 허용여부를 결정한다.

④ 서비스 포트 허용 후 보안업데이트 미비, 백신 미설치 등 안전성이 미확보된 상태로 운영하는 것이 발견된 경우, 정보화본부에서 안전성 확보를 위한 긴급 보안 조치를 요청할 수 있으며, 조치가 완료될 때까지 해당 서비스 포트는 차단한다.

⑤ 서비스 포트 사용 신청자는 허가받은 서비스 포트를 주기적으로 점검하고 사용하지 않는 서비스 포트는 즉시 반납하여야 한다.

⑥ 방화벽에서 1년 이상 사용한 로그가 없거나 반납된 IP주소와 연계된 서비스 포트는 정보화본부에서 사전통지 없이 차단한다.

⑦ 사용자 단말기(PC 등)에서 대학 내 서비스용 프로그램을 직접 운영 중이거나 프로그램 개발·유지관리 등을 목적으로 대학 내 서버에 대한 포트 접근이 필요한 경우에는 제12조에 따른다.

⑧ 대학 전산망을 보호하기 위해 차단포트 목록은 조정될 수 있다.

제10조(SSL VPN 서비스 운영) ① 사용자는 대학에 재학·재직 중인 교내 구성원으로 제한하며, 서비스 이용은 대학 포털사이트에서 신청한다.

② 연구, 채용 등 특별한 목적으로 외부사용자의 VPN 서비스 이용이 필요할 경우 정보화본부와 사전협의하여야 한다.

③ VPN 서비스의 사용기간은 다음과 각 호와 같다.

1. 교육·연구용 사용기간은 신청일로부터 최대 12개월로 한다.
2.업무(원격근무)용 사용기간은 원격근무 기간으로 한다.
3.개발, 유지보수 작업용 사용기간은 작업에 필요한 최소한의 시간으로 한다.

④ VPN 계정은 사용자의 사번(학번)으로 생성하고, 초기패스워드는 정보화본부에서 임의로 설정하여 제공한다.

⑤ 원격서비스(SSH, 원격데스크톱 등) 사용은 지양하고, 실험·연구용으로 부득이하게 사용이 필요할 경우 정보화본부 보안담당자의 검토를 거쳐 2차 인증 적용 후 사용한다.

⑥ 제⑤항의 경우 정보보안을 위해 VPN서비스 목적지에서 대학 주요 정보시스템으로의 접근을 차단할 수 있다.

⑦ 사용자의 VPN 서비스 이용 시 개인정보유출 방지 등 보안 강화를 위하여 해당 단말기의 외부 인터넷 접속을 차단할 수 있다.

⑧ VPN 사용기간이 만료되었음에도 연장 신청하지 않으면 사용자 정보를 삭제한다.

⑨ VPN 서비스 사용자는 다음 각 호의 사항을 준수하여야 한다.

1. 부여받은 사용자 계정정보를 타인에게 대여하거나 공유는 불허한다.
2. 외부인에게 사용자 계정정보가 유출되지 않도록 유의하고, 유출이 의심되면 즉시 정보화본부로 사용자 정보 변경을 요청하여야 한다.
3. 신청한 사용 목적 외 다른 목적으로 VPN 서비스 사용을 금지한다.
4. 원격서비스 이용 시 해당 시스템을 통하여 다른 교내 단말기로의 접속을 금지한다.
5. 사용목적 종료, 사용기간 초과 및 계약종료 등의 이유로 해당 서비스 이용이 불필요할 경우 즉시 정보화본부에 통보하여야 한다.

제11조(네트워크 관리 및 정보보안) ① 대학 전산망은 학칙에서 정하는 교육·연구·학술 활동에 우선 이용될 수 있도록 정보화본부에서 지원한다.

② 정보화본부는 효율적이고 안정적인 네트워크 운용을 위해 다음 각 호의 사항을 수행한다.

1. 무단 IP주소 사용자 및 영리 목적 사용자는 네트워크 접근을 차단한다.
2. 트래픽 관리, 이상유·무 진단, 장애 예방 및 감지를 위해 네트워크 모니터링을 실시한다.
3. 과다한 트래픽 유발로 회선 이용을 점유하거나 장애 트래픽, 보안사고 관련 트래픽 등으로 예상되는 경우 특정 그룹 및 이용자에 대해 개별 모니터링 할 수 있으며, 다수의 이용에 피해를 줄 수 있다고 판단되면 네트워크 사용을 조절할 수 있다.
4. 게임 및 증권사이트 등 학술·연구에 부적합한 사이트는 공지 후 사용을 차단 또는 조정할 수 있다.
5. 전산망의 원활한 운영을 위하여 긴급히 조치가 필요하거나 보안사고가 접수되면 해당 장비를 사전 통보 없이 네트워크로부터 차단할 수 있다.
6. 제5호의 경우 해당 사고 해결 및 관련 추가 문제가 존재하지 않는 경우에만 네트워크 재접속을 허용한다.

② 정보화본부는 전산망 정보보안을 위해 다음 각 호의 사항을 수행한다.

1. 전산망 접속 단말기의 보안취약점 및 법 위반사항이 발견되면 기관 및 사용자에게 해당문제의 개선조치를 요청한다.
2. 제1호의 개선조치를 미이행할 경우 네트워크에 접속을 차단할 수 있으며, 해당 문제가 개선된 경우에만 네트워크 재접속을 허용한다.
3. 동일 IP주소에서 지속적인 보안사고가 발생할 때에는 해당 기관을 대상으로 정보보안 감사 및 교육을 실시할 수 있다.
4. 학내 정보보안 및 불법 소프트웨어 근절 등을 위해 정보화본부에서는 학내 정보시스템의 정보를 수집할 수 있다.
5. 전산망에 연결되는 단말기는 정보보호를 위하여 정보화본부에서 배포하는 보안프로그램을 반드시 설치하여야 한다.
6. 기관 또는 사용자가 백신소프트웨어를 별도로 구매하여 사용하고자 할 경우, ‘백신소프트웨어 설치제외 신청서’ [별지 제1호 서식]를 정보화본부로 제출하여 신청한다. 다만, 구매한 백신소프트웨어의 라이센스 기간 만료 시 신청내용은 무효화 된다.

제12조(정보시스템 원격접근) ① 유지보수, 개발 등의 목적으로 대학 외부에서 원격접근이 필요할 경우 ‘원격서비스 허용요청서’ [별지 제2호 서식]를 작성하여 해당 정보시스템 운영담당자에게 요청하고, 운영담당자는 대학 포털사이트에서 정보화본부로 방화벽 차단정책 변경을 신청한다.

② 원격접근 신청 시 ‘사용기간’ 은 사용이 필요한 최소한의 시간으로 신청하여야 하며, 업무시간 외(18시 이후, 주말, 공휴일 등) 원격접근은 지양한다.

③ 원격지 개발 등 장기간 원격접근이 필요할 경우 정보화본부와 협의하여 정보보안 사항을 점검 후 진행한다.

④ 정보화본부에서 관리하는 주요 정보시스템의 접근을 위한 접근제어시스템 계정 발급요청은 ‘접근제어시스템 계정 사용 신청서’ [별지 제4호 서식]를 작성하여 정보화본부로 신청한다.

⑤ 프로그램 개발·유지 관리 등을 위해 교내단말기(PC, 서버 등)에서 정보화본부 서버의 특정 포트에 연결이 필요한 경우 ‘시스템 접근요청서’ [별지 제3호 서식]를 작성하여 정보화본부로 신청한다.

⑥ 정보화본부의 시스템을 보호하기 위해 사용자의 시스템접근은 사전 공지 없이 차단·조정할 수 있다.

제13조(외부기관 및 업체의 전산망 사용 제한) ① 외부기관 및 업체는 최대 4개의 IP주소까지 신청할 수 있으며, 그 이상 IP주소가 필요할 경우 정보화본부와 협의하여야 한다.

② 상업적인 용도(DNS 서버, 호스팅 서비스 등)로 서버 운영 및 전산망 사용을 원칙적으로 불허하며, 상업적인 이용이 발견되면 IP주소 회수 등 전산망 사용을 금지한다.

③ 과도한 트래픽 사용, 보안사고 등으로 대학 교육·행정업무의 원활한 운영을 저해할 경우 대역폭 제한, 포트차단 등 전산망 사용을 제제할 수 있다.

제14조(사용료 과금) ① 정보화본부는 다음 각 호에 해당하는 대학 전산망 자원을 사용하는 기관 또는 개인에게 자원 운용에 소요되는 비용의 전액 또는 일부를 징수할 수 있다.

1. IP 주소
2. Domain
3. 광케이블 및 LAN Port
4. 정보화본부장이 정한 기타 네트워크 자원

제15조(사용자 의무 및 벌칙) ① 전산망 사용자는 '강릉원주대학교 정보보안 기본지침' 등 전산망 이용을 위한 각종 제 규정을 반드시 준수하여야 한다.

② 정보화본부는 다음 각 호의 어느 하나에 해당하는 전산망 사용자에 대해 지도 또는 경고한다.

1. 전산망 제공 목적 이외의 용도로 사용하거나 자신의 사용 권한을 무단으로 타인에게 양도한 경우
2. 해킹, 스푸핑, 스니핑 등 악의적인 의도로 전산망을 사용한 경우
3. 허가받지 않은 시스템의 전산망 연결이나 허가받지 않은 IP주소의 사용한 경우
4. 변조된 IP 및 MAC 주소를 사용하여 전산망에 연결하는 경우
5. 고의로 컴퓨터 및 보조 장치, 전산망의 정상적인 운용을 방해한 경우
6. 고의로 컴퓨터나 전산망을 손상하거나 과도한 부하를 발생시키는 프로그램을 설치, 수행하거나 다른 사용자에게 전달한 경우
7. 데이터 보안을 무시하거나 보안취약점을 노출한 경우
8. 고의로 전산망 자원을 남용하는 경우
9. 소유자의 허락 없이 통신 내용을 감청하거나, 복사, 변조, 삭제한 경우
10. 허가받지 않은 서브넷을 구성한 경우
11. 불법 소프트웨어를 사용한 경우
12. 승인되지 않은 인터넷 전화기를 사용한 경우
13. 기타 전산망 운영에 불편을 초래하는 경우

③ 정보화본부는 다음 각 호의 어느 하나에 해당하는 사용자의 전산망 사용을 1주일 금지한다.

1. 임의로 서브넷(공유기, 무단 AP 등 사용)을 구성하여 사용 중인 경우
2. 지도 및 경고를 3회 이상 받은 경우
3. 제①항에 3개 이상 해당하는 경우

④ 다음 각 호의 어느 하나에 해당하는 사용자는 "보안심사위원회"를 열어 보안위규자 심사 및 처리한다.

1. 거듭된 지도 및 경고에도 지속해서 동일한 문제를 발생시키는 경우
2. 대학 전산망 일부 또는 전체를 마비시켜 심각한 피해가 발생한 경우

⑤ 전산망 서비스 사용 중 발생하는 보안사고 및 법적 분쟁은 사용자에게 그 책임이 있다.

부칙<2014.07.04.>

이 지침은 공포한 날부터 시행한다.

부칙<2018.07.06.>

이 지침은 공포한 날부터 시행한다.

부칙<2021.01.28.>

이 지침은 공포한 날부터 시행한다.

부칙<2023.02.21.>

이 지침은 공포한 날부터 시행한다.

[별표1]

차단 서비스포트 목록

서비스 포트	서비스명	차단 방향
TCP 21	FTP(파일전송)	학외→학내
TCP 22	SSH(보안 원격접속)	
TCP 23	Telnet(원격접속)	
TCP 25	SMTP(보내는 메일)	학 외 ↔ 학 내 (양방향 차단)
UDP 53	DNS(도메인 서비스)	학외→학내
TCP 80	HTTP(웹서비스)	학외→학내
TCP 443	HTTPS(웹서비스)	
TCP 8080	HTTP(웹서비스)	
TCP 110	POP3(받는 메일)	
TCP 143	IMAP(받는 메일)	
TCP 1433	MS_SQL(DB접속)	학 외 ↔ 학 내 (양방향 차단)
TCP 1434	MS_SQL(DB접속)	
TCP 1521	Oracle(DB접속)	
TCP 3050	FireBird(DB접속)	
TCP 3306	MySQL(DB접속)	
TCP 3389	MSTSC(윈도우 원격접속)	학외→학내
TCP 5432	PostgreSQL(DB접속)	학 외 ↔ 학 내 (양방향 차단)
TCP 5800	VNC(윈도우 원격접속)	학외→학내
TCP 5900		
기타	웜.바이러스 유포 의심 서비스 포트	학 외 ↔ 학 내 (양방향 차단)

[별지 제1호 서식]

백신소프트웨어 설치 제외 요청서

결 재 [정보화본부]		
담 당	팀 장	정보보안담당관

신청인	소 속		신청인구분
	성 명		교수 ( ) 직원 ( ) 조교 ( ) 기타(계약직등) ( )
	연 락 처		
사용기종		□ P C □ Server □ 기타	
사용 IP 주소			
단말기 MAC 주소			
설치 제외 사유			

단말기 관리미흡 등으로 인하여 교내외의 전산망에 피해를 주거나 보안상 문제가 생길 경우 신청인에게 전적인 책임이 있으며, 이러한 문제를 방지하기 위한 최대한의 사전조치를 취하겠습니다. 따라서 위와 같이 백신소프트웨어 설치 제외를 요청 드립니다.

※ IP 및 MAC 주소 확인 방법 : 시작 ▶ 실행 ▶ cmd ▶ c:₩>ipconfig -all 에서 Physical Address 를 반드시 알려주시기 바랍니다.

※ 개인용 백신소프트웨어 구입을 이유로 설치 제외를 요청하는 사용자는 백신 구입증빙서를 첨부하여 제출하시기 바랍니다.

2 0 년 월 일

신 청 자 : (인/서명)

부서(학과)장 : (인/서명)

강릉원주대학교 정보화본부장 귀하

[별지 제2호 서식]

원격서비스 허용 요청서

결 재 [정보화본부]		
담 당	팀 장	정보보안담당관

신청자	소 속		직급		성명	
	연락처					
사 용 기 간 (구체적인 작업시간 입력)		20 . . . : ~ 20 . . . :				
사 유		자세히 기재 부탁드립니다				
접속자 정보	IP					
	서비스	(예) ssh, sftp, 원격테스트톱, 오라클				
	보안점검	❑ 최신백신설치 ❑ 비밀번호(화면보호기 포함) 설정 ❑ 비인가 저장매체 접속차단 ❑ 산출물 저장 금지				
접근 대상	연번	IP	port 번호	사용기간		
	1	(예) 202.30.48.256	(예) 7777, 11521	사용기간이 상이할시 입력		
	2					
	3					
	4					
	5					

교내외 전산망에 **피해를 주거나 보안상 문제가 생길 경우 신청인에게 전적인 책임**이 있으며, 이러한 문제를 방지하기 위하여 **최대한의 사전조치**를 취하겠습니다. 따라서 위와 같이 원격서비스 허용을 요청드립니다.

신청일자 : 20 . . . 신청자 : (서명)

부서명: 담당자 : (서명)

강릉원주대학교 정보화본부장 귀하

[별지 제3호 서식]

시스템 접근 요청서

결 재 [정보화본부]		
담 당	팀 장	정보보안담당관

신청인	소 속		신청인구분
	성 명		교수 ( ) 직원 ( ) 학생 ( ) 외부자 ( )
	연 락 처	☎	

접속자				시스템 IP address	접속 PORT	사용기간	사용용도
IP address	소속	이름	ID				
. . .				. . .		/ ~ /	
. . .				. . .		/ ~ /	
. . .				. . .		/ ~ /	
. . .				. . .		/ ~ /	

[ID] 는 접근통제시스템사용(콘솔접속)이 필요할 때만 기입합니다.

위와 같이 시스템 접근을 요청합니다.

2 0 년 월 일

신 청 자 : (인/서명)

부서(학과)장 : (인/서명)

강릉원주대학교 정보화본부장 귀하

※ 굵은 테두리 안의 내용은 모두 기입하시기 바랍니다.

[별지 제4호 서식]

접근제어시스템 계정 사용 신청서

승 인		
담 당	팀 장	정보보안 담당관

신청자	소 속		성명		
	연락처		E-mail		
사 유		자세히 기재 부탁드립니다			
접속자 정보	접근자 IP		접근제어 ID		
	대상서버	예)웹서버	사용포트	예)ssh, RDP, http, telnet	
				예)ssh, RDP, http, telnet	
				예)ssh, RDP, http, telnet	
				예)ssh, RDP, http, telnet	
				예)ssh, RDP, http, telnet	
	보안점검	❑ 최신백신설치 ❑ 비밀번호(화면보호기 포함) 설정 ❑ 비인가 저장매체 접속차단 ❑ 산출물 저장 금지			
신청계정	ID	(예) ngsid	패스워드	영문,숫자,특수문자 포함 9자리 이상	
WinNGS 클라이언트 프로그램 설치 여부 확인 ☐ 설치 ☐ 미설치 *. 미설치시 설치프로그램은 메일로 전달합니다.					

교내외 전산망에 **피해를 주거나 보안상 문제가 생길 경우 신청인에게 전적인 책임**이 있으며, 이러한 문제를 방지하기 위하여 **최대한의 사전조치**를 취하겠습니다. 따라서 위와 같이 접근제어 계정을 신청합니다.

신청일자 : 20 . . . 신청자 : (서명)

부서명: 담당자 : (서명)

강릉원주대학교 정보화본부장 귀하