정보보안 · 관리규정

제정 : 2009.11.01
개정 : 2011.05.01
개정 : 2011.11.22
개정 : 2014.07.01
개정 : 2015.06.17
개정 : 2016.03.01
개정 : 2017.07.01
개정 : 2018.09.13
개정 : 2019.12.13
개정 : 2020.03.01
개정 : 2021.12.01
개정 : 2022.10.01
개정 : 2023.10.16

제1장 총 칙

제1조(목적) 이 규정은 대원대학교(이하 “본 대학교” 라 한다.)에서 보유한 정보자산이 내·외부의 사용자에 의해 불법 유출, 파괴, 변조, 오남용 되는 것으로부터 보호하기 위하여 유통되는 정보를 취급하거나 이용할 시 준수해야할 기본적인 사항과 불건전 정보의 기준을 정하고, 이를 체계적으로 관리함으로서 본 대학교의 정보자산을 안전하고 신뢰성 있게 운영하고자 하는데 있다. <개정 2011.11.22., 2020.03.01.>

제2조(적용 대상 및 범위) ① 적용 대상은 교내의 모든 기관으로 한다.
② 본 대학교의 정보자산 보호와 운영에 관하여 따로 규정되는 경우를 제외하고는 이 규정에 따른다. <개정 2020.03.01.>

제3조(용어의 정의) ① “정보시스템”이라 함은 업무용/연구용/개인용/공용의 용도로 이용하는 본 대학교의 모든 PC, 서버 등의 컴퓨터와 컴퓨터에 내장된 소프트웨어, 유/무선 전산망을 연결하는 네트웍장비, IP주소, 도메인주소, 메일주소등 유/무형의 정보시스템 전체를 말한다. <개정 2020.03.01., 2021.12.01.>
② “정보자산”이라 함은 본 대학교의 정보시스템에 내장되어 다운로드, 업로드, 조회, 인쇄를 할 수 있는 문자/부호/음성/영상 등의 전자적인 형태로 작성된 데이터와 백업된 데이터 그리고 각종 명부 등 문서화된 출력물을 말한다. <개정 2020.03.01.,

2021.12.01.>

③ “개인정보” 라 함은 개인에 관한 정보로서 정보에 포함되어 있는 성명, 주민등록번호, 사용자계정 등의 항목을 통하여 개인을 식별할 수 있는 정보를 말한다. <개정 2021.12.01.>

④ “시스템관리자” 라 함은 각 부서에 소속되어 시스템의 루트(root) 권한을 가지고 시스템을 운영/관리하는 자를 말한다. <개정 2021.12.01.>

⑤ “데이터베이스관리자” 라 함은 데이터베이스를 운영/관리하는 자를 말한다. <개정 2021. 12. 01.>

제2장 위원회

제4조(구성) ① 체계적/효율적인 보안정책 수립·심의 및 관리를 위하여 정보보안심사위원회(이하 “위원회” 라 한다)를 둔다. <개정 2021.12.01.>

② 위원장은 미래전략처장이 되며 위원은 전산운영위원회 위원으로 구성한다. <개정 2015.06.17., 2018.09.13., 2020.03.01., 2021.12.01., 2022.10.01., 2023.10.16.>

제5조(기능) ① 위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의·결정한다. <개정 2021.12.01.>

1. 정보보안정책 심의와 학내 정보보안의 총 관장
2. 정보보호정책 및 총괄 계획 심의
3. 정보보안사고 처리의 책임을 심의·의결 <개정 2021.12.01.>
4. 정보보안교육 및 정보보안 준수사항 감사
5. 기타 정보보안관련 제반업무의 총괄

제6조(정보보안팀의 구성과 역할) ① 위원회 산하에 정보보안팀을 구성하여 본 대학교에 관련된 정보보안 제반사항을 담당한다. <개정 2020.03.01.>

② 어떤 상황에서도 교육과 연구에 지장이 발생하지 않도록 정보시스템을 유지·관리한다. <개정 2021.12.01.>

③ 정보보안팀은 별도로 구성할 수 있다. 다만, 별도 구성을 하지 않으면 미디어팀에서 역할을 수행할 수 있다. <개정 2016.03.01., 2020.03.01., 2021.12.01., 2022.10.01., 2023.10.16.>

제3장 보 안

제7조(기본수칙) ① 정보시스템 사용자는 개인별 사용자계정 및 패스워드의 기밀을 유지

해야 하며, 본래의 발급 목적으로만 사용하여야 한다.
② 교직원 및 학생은 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다. <개정 2021.12.01.>
③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 하여서는 아니 된다.
④ 제7조제3항에 언급된 행위를 한 자가 발견된 경우에는 소속부서의 장 또는 정보보안팀에게 알려야 한다. <개정 2021.12.01.>
⑤ 정보자산과 연관된 저작권·특허권 및 소프트웨어 라이선스의 사용조건을 숙지하고 이를 준수하여야 한다. <개정 2021.12.01.>
⑥ 학내 전산망을 신설·변경 및 폐기하고자 하는 경우에는 본 대학교의 사전승인을 얻어야 한다. <개정 2020.03.01., 2021.12.01.>
⑦ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니한다.
⑧ 모든 정보자산은 보안등급에 따라 분류·관리한다. <개정 2021.12.01.>
⑨ 본 대학교는 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안정책 및 규정의 준수여부를 평가한다. 다만, 학내 모든 사용자는 이에 적극 협조하여야 한다. <개정 2020.03.01.>
⑩ 업무와 관련해 습득한 정보자산을 본 대학교의 허가 없이 외부에 누출해서는 아니 된다. <개정 2020.03.01.>
⑪ 정보보안 사고의 책임은 원칙적으로 사용자 본인에게 있다.
⑫ 각 행정부서는 개인정보보호 관련하여 법정대장을 비치하여 작성· 관리하여야 한다. <개정 2021.12.01.>
⑬ 신규임용되는 정보보호 인력에 대해서 보안서약서 작성 및 정보보호에 대한 교육이 진행되어야 한다. <신설 2011.05.01.> <개정 2021.12.01.>
⑭ 모든 정보자산 관련 장비들의 도입 시 기본설정 정보 및 비밀번호는 반드시 본 대학교에 맞게 변경하여야 한다. <신설 2011.05.01.> <개정 2020.03.01.>
⑮ 모든 전산장비에 대해서는 보안관리 책임자를 지정하여야 한다. 다만, 보안관리 책임자를 지정하지 않은 경우 미래전략처장을 정으로 미디어팀장을 부로 당연직으로 지정한다. <신설 2011.05.01.> <개정 2015.06.17., 2018.09.13., 2021.12.01., 2022.10.01., 2023.10.16.>

제8조(보안등급 기준) ① 보안등급의 분류기준은 다음의 각 호에 따라 정한다.
1. 정보의 중요도
2. 정보(시스템)의 절취 및 불법변경 시 손실 가치
3. 정보(시스템)의 파괴 시 복구비용
4. 정보의 사용권자

② 정보자산의 보안등급 및 사용자 인가는 전항의 기준에 따라 정보자산을 보유한 부서의 장이 별도로 정한다.

제9조(보안점검) ① 정보보안팀은 교내 주요서버 및 각 연구실의 서버에 대해 년 1회 이상의 정기점검과 필요시 수시점검을 실시한다. 다만, 사이버보안 진단의 날 자체 점검 진행시 해당 점검 결과로 보안 점검을 대체할 수 있다. <개정 2014.07.01., 2021.12.01.>
② 보안점검 대상 및 분야를 해당 부서에 통보하고, 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비한다.
③ 보안점검을 실시한 후 그 결과를 총장에게 보고한 후 해당 부서에 통보한다.
④ 해당 부서에서는 지적사항을 즉각 시정하고 그 결과를 위원장에게 보고한다.
⑤ 정보보안팀은 필요시 각 부서의 보안점검 지적사항에 대한 시정 여부를 확인할 수 있다.

제9조의2(정보보호 수준진단) ① 정보보안팀은「교육부 정보보안기본지침」제73조에 따라 국가정보보안 정책 이행 여부를 확인하기 위해 매년 교육부장관이 정하는 정보보호 수준진단 대상 · 기준, 진단항목, 진단기간, 진단결과 제출방법에 따라 자체 정보보호 수준진단을 하여야 한다. <개정 2021.12.01.>
② 정보보안팀은 제1항에 따라 자체 진단한 결과의 객관성 확보를 위해 증빙자료를 확보하여야 한다. <개정 2021.12.01.>
③ 정보보안팀은 제1항에 의한 자체 진단결과를 종합 분석하여 향후 정보보호 수준 향상을 위해 활용할 수 있다. <개정 2021.12.01.>
[본조신설 2016.03.01.]

제10조(사고의 처리) 보안사고가 발생할 경우 정보보안팀은 다음 각 호의 단계에 따라 적절한 조치를 하여야 한다.
1. 침입자의 침입예방을 위하여 침입가능성이 있는 부분을 수시로 점검하여 불법침입자의 침입을 사전에 예방한다.
2. 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각 점검해야 한다.
3. 침입자가 현재 시스템에 침투해 해킹을 하고 있을 경우 필요한 조치를 즉각 취하고 보고하여야 한다. <개정 2021.12.01.>
4. 침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우, 즉시 보고하고, 보안진단 도구나 체크리스트를 이용하여 정보자료의 이상 유무를 점검하여야 한다. <개정 2021.12.01.>

제11조(보안 교육) ① 학내 의사결정자, 사용자 및 시스템 관리자를 대상으로 정보보안 교육을 실시한다. <개정 2021.12.01.>

② 보안에 대한 의식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 보안사고를 최소화한다.

③ 보안교육은 년 1회의 정기교육과 필요에 따라 수시교육을 실시하며, 정보보안 담당자는 교육부 정보보안기본지침을 따른다. <개정 2013.04.01., 2020.03.01., 2021.12.01.>

제4장 정보시스템 관리

제12조(사용자 정의) 정보시스템을 사용할 수 있는 자는 다음 각 호와 같다.

1. 본 대학교 교원·직원·재학생 및 졸업생 <개정 2020.03.01., 2021.12.01.>
2. 연구소 및 부속기관의 장이 사용을 인정한 자

제13조(적절성 확보) ① 학내 정보시스템 이용자는 정보시스템 사용에 있어 적절성을 유지하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재조치를 취할 수 있다.

1. 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우
2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반사용자가 'root' 패스워드 또는 타 사용자의 패스워드를 획득하고자 해킹하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
6. 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
7. 사용자 계정 및 패스워드를 상호 공유하는 행위
8. 시스템관리자가 특별한 사유 없이 'root' 패스워드를 일반사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위
10. 인터넷을 통해 자살 사이트나 음란 사이트 등 반사회적인 유해사이트에 접속·개설하는 경우 <개정 2021.12.01.>
11. 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우
12. 학교 이념과 규정에 어긋나는 내용을 전자게시판에 공지한 경우
13. 소유자의 허락 없이 통신내용을 감청하거나, 복사, 변조, 삭제한 경우
14. 원하지 않는 전자우편 발송 등으로 다른 사용자들에게 피해를 주는 경우
15. 소프트웨어 사용약관이나 저작권 보호관련 법을 위반하는 경우
16. 고의적으로 자원을 남용하는 경우
17. 데이터 보안을 무시하거나 보안취약점을 노출시킨 경우

18. 고의로 컴퓨터나 전산망을 손상시키거나 과도한 부하를 야기시키는 프로그램을 설치·수행하거나 다른 사용자에게 전달한 경우(단, 보안 또는 성능 시험을 위하여 본 대학교로부터 허가받은 활동일 경우는 예외로 한다.) <개정 2020.03.01., 2021.12.01.>

② 정보시스템별 사용자 접근 및 사용내역을 기록하여 보관하여야 한다. <신설 2011. 05.01.>

제14조(처벌) ① 제13조의 규정된 사항에 해당할 경우에는 사용자의 계정을 회수하여 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 처벌 사항은 위원회에서 심의·결정한다. <개정 2021.12.01.>

② 정보시스템의 불법사용으로 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. 「개인정보보호법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 법적 조치 <개정 2021.12.01.>
2. 학칙에 따른 징계 조치
3. 정보시스템의 손해발생에 대한 손해배상 청구

제5장 네트워크 관리

제15조(네트워크 관리) ① 네트워크관리는 일관성과 기밀성을 위해 통합관리를 원칙으로 한다.

② 운영부서의 관리자는 네트워크 신규설치 및 변경 시 정보보안팀에 변경정보를 통보해야 한다.

③ 네트워크 IP주소는 사용자가 임의로 변경할 수 없다.

④ 라우터 패스워드는 제19조에 규정된 계정관리에 따른다.

⑤ 외부접속자의 “root" 로그인은 허용하지 않는다.

⑥ 일정횟수 접속 실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.

⑦ 네트워크 IP주소 등록요구 시 관리자에게 사용목적 등을 기재하여 신청서를 제출하여야 한다.

⑧ 전산망은 가능한 개방적으로 운영하되, 악의적 목적으로 사용되는 일부 통신에 대해서는 제재를 가할 수 있으며, 입시기간 및 기타 학내 중요행사시 불필요한 서비스는 일정 기간동안 차단 할 수 있다. <개정 2021. 12. 01.>

제16조(네트워크 보호) ① 네트워크의 안전한 운영을 위해 방화벽 등의 보안 시스템을 운영하여야 한다.

② 서비스를 위해 개방된 포터 이외의 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 금지하며 부득이 하게 접근을 할 때는 방화벽 개방 요청서나 이에 준하는 요

청서 제출 후 보안 시스템을 통해서만 접근이 가능하다.
③ 본 대학교에 유해하거나 불필요하다고 판단되는 웹사이트 및 원격 사용자의 공중망 네트워크를 통한 접속을 인증시스템 또는 방화벽에 의해 통제 할 수 있다. <개정 2020.03.01.>
④ 신뢰할 수 없는 정보시스템 및 서버로의 접속을 보호하기 위해 네트워크 정책을 설정하여 통제 할 수 있다
⑤ 외부에서 내부로의 모든 접속시도는 LOG 관리되어야 하며, 지정횟수 이상의 패스워드 입력오류 시에는 해당 사용자로부터의 접속 시도를 차단할 수 있다. <개정 2013.04.01., 2020.03.01.>
⑥ 네트워크에 비정상적인 트래픽 발생 시 문제가 해결될 때까지 해당 컴퓨터나 단위 전산망을 캠퍼스망으로부터 단절시킬 수 있다.
⑦ 무선네트워크의 사용은 기본적으로 접속프로그램을 통한 아이디·패스워드 인증을 통해 인증된 사용자만 사용이 가능하며 아이디·패스워드 인증을 받지 못하는 장비에 한해서 Mac Address 인증 신청서를 제출하면 등록 후 Mac Address 인증을 통한 무선네트워크 사용이 가능하다. <개정 2021.12.01.>
⑧ 무선네트워크를 사용할 때 사용자인증을 받지 않고 사용하기 위해서는 반드시 WPA2 등 무선네트워크 암호화 설정 후 암호화를 통해서만 사용한다. <개정 2013.04.01., 2020.03.01.>

제6장 서버 관리

제17조(운영 및 관리) ① 서버등록 시 관리자에게 신청서를 제출하여야 한다.
② 시스템 관리자는 최소 월 단위로 패스워드를 변경해야 한다.
③ 시스템 개발 및 운영부서의 장은 응용프로그램 개발계획 단계에서 보안정책에 근거한 응용프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.
④ 슈퍼유저의 권한은 정보보안업무 담당자·시스템 관리자로 제한한다. <개정 2021.12.01.>
⑤ 장애복구나 점검을 위해 루트 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시하고, 작업종료 후 루트계정과 패스워드를 변경한다.
⑥ 장애복구나 점검을 위해 서버에 접속이 필요할 때는 관리자가 지정한 PC에서만 작업을 하여야 하고 부득이하게 노트북 등 특정 단말기를 사용하여야 할 때는 시스템 관리자 입회하에 작업을 하여야 한다. <신설 2011.05.01.>
⑦ 백업지침은 별도로 정하며, 반드시 지침에 따라 주기적인 백업을 실시한다.
⑧ 각 부서는 백업 미디어별로 적절한 사용연수를 정하여 노후된 백업미디어에 대해서는 사용하지 아니한다. <개정 2021.12.01.>
⑨ 정보시스템 관리를 위해 시스템별 개별 관리대장 〔별지서식 21호〕를 작성하여 주기

적인 보안패치를 하고, 시스템의 기본 상태에 대한 점검 및 미사용 포트점검을 [별지서식 22호]에 따라 매일 실시하여야 한다. <신설 2017.07.01.> <개정 2021.12.01.>

제18조(보안관리) ① 전체 시스템에 대한 보안관리와 전반적인 방향설정 및 주기적인 보안점검은 정보보안팀에서 실시한다.

② 개별 서버에 대한 보안관리는 각 서버의 관리자가 담당한다.

제19조(계정관리) ① 사용자 계정분류는 그 사용목적에 따라 분류하고, 그 기준은 따로 정한다.

② 사용자별 또는 그룹별로 접근권한을 부여한다.

③ 실습용 ID는 해당학기 종료 후 말소한다.

④ 특별한 사유 없이 1학기 이상 사용하지 않는 계정은 학기 시작 일주일 이내에 말소한다. <개정 2021.12.01.>

⑤ 비밀번호가 없는 계정은 사용을 금지한다. <개정 2011.05.01.>

⑥ 모든 비밀번호는 숫자 문자의 조합으로 패스워드 안전성검사 프로그램을 통해 검증결과가 '상' 이상으로 나와야 하며 비밀번호 관리대장은 별도로 암호화하여 보관한다. <신설 2011.05.01.> <개정 2021.12.01.>

⑦ 일정횟수 접속 실패 시 사용을 금지한다.

⑧ 슈퍼유저는 Console 및 특정 단말에서만 접속을 허용한다.

⑨ 사용자 계정(메일 포함)의 등록·변경 및 폐기 절차는 다음 각 호에 따른다. <개정 2021.12.01.>

1. 사용자 계정 : 사용자 등록이나 변경 또는 폐기 신청서를 작성한 후에 시스템 관리자에게 통보하되, 외부사용자는 반드시 사용기간 및 목적 등의 사유를 명확히 해야 한다. <개정 2021.12.01.>

2. 시스템관리자 : 내용을 검토한 후에 사용자 계정을 등록이나 변경 또는 폐기하고, 사용자에게 그 사실을 통보한다. <개정 2021.12.01.>

3. 사용자 계정을 등록하거나 변경 또는 폐기할 경우 : 일반적인 사항은 월 단위로 부서장에게 사후 보고한다. 다만, 특별한 상황이 발생할 경우에 한하여 부서장의 허가를 받은 후에 작업을 실시한다. <개정 2021.12.01.>

4. 휴직자의 계정 : 휴직기간동안 잠정 폐쇄를 원칙으로 한다. <개정 2021.12.01.>

5. 퇴직자 : 사직원 제출 시(졸업생은 졸업 시) 별도의 사유가 없는 한 사용자 계정을 반납 하도록 한다. <개정 2021.12.01.>

제7장 전산자료 및 데이터베이스 관리

제20조(자료의 관리) ① 데이터베이스 로그인 계정 관리기준은 DBMS 관리자(DBA)·응용

프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다. <개정 2021.12.01.>

② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업하여 분리보관 하여야 한다.

③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한해야 한다.

④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.

⑤ DBMS는 시스템과는 별도의 사용자 인증기능을 수행해야 한다.

⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.

⑦ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제20조의2(자료의 암호화) ① 개인정보처리시스템에 있는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. <개정 2020.03.01.>

② 개인정보처리시스템에 있는 고유식별정보, 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다. <개정 2021.12.01.>

[본조신설 2017.07.01.]

제20조의3(자료의 암호 키 관리) 암호키는 암호화된 데이터를 복호화할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 중요하며, 다음 각 호와 같이 라이프 사이클 단계별 암호 키 관리 절차를 갖는다. <개정 2021.12.01.>

1. 암호 키 생성 : 기밀 데이터를 암호화할 경우 정보보안담당관의 승인을 받아 생성한다.

2. 암호 키 이용 : 접근이 인가되지 않은 사용자는 암호화 키를 사용할 수 없도록 접근 통제하여야하며, 접근이 인가된 사용자 외에 암호화 키가 노출되지 않도록 관리하여야한다.

3. 암호 키 보관 : 키 자료의 보관은 무결성과 접근통제가 가능해야하며, 보관된 정보는 수정이 불가한 상태이어야 한다. 보관된 정보는 운영 데이터와 분리되어 보관되어야하며 키는 백업하여 잠금장치가 있는 곳에 물리적으로 보관할 수 있다. <개정 2021.12.01.>

4. 암호 키 배포 : 접근이 인가된 사용자 외에 암호 키가 노출되지 않도록 철저하게 관리해야 한다.

5. 암호 키 폐기 : 암호 키는 사용용도가 종료된 경우 정보보안담당관 승인 후 폐기한다.

〔본조신설 2017.07.01.〕

제21조(자료의 보관) ① 별도지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비해 소산계획을 수립하여 운영한다.

② 별도지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회하에 이용 및 변경할 수 있다.

제22조(자료의 파기) ① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리대장의 파기 확인란에 입회자는 파기 확인을 한다.

② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료 접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.

③ 소규모의 전산파지는 분쇄기를 이용하고, 대규모의 파지는 소각장에서 소각시키거나 그에 준하게 처리한다.

④ 정보시스템의 폐기 또는 교체 등으로 인해 자료의 완전 삭제가 필요할 때는 〔첨부1〕의 방법으로 삭제를 하여야 하고 〔별지 서식 20 호〕에 의거 대장관리를 한다. <신설 2014.07.01.> <개정 2020.03.01., 2021.12.01.>

제8장 응용프로그램 관리

제23조(응용프로그램 개발) ① 모든 응용프로그램은 접근하는 데이터의 정보등급에 따라 해당 응용프로그램의 보안등급을 설정한다.

② 응용프로그램의 계획서 및 설계서는 보안관리규정에 근거하여 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.

③ 별도지침에 의해 중요자료로 분류된 응용프로그램은 정보보안을 위해 사용자계정 및 패스워드를 설정해야 한다.

④ 응용프로그램에서 사용하는 사용자계정/패스워드 및 기타 전산망접근과 관계된 중요정보는 소스코드로부터 분리하여 1차 인식이 불가한 암호화된 형태로 존재해야 한다.

⑤ 별도지침에 의해 중요자료로 분류된 응용프로그램은 개발 시 시스템 사용에 대한 로그 정보를 관리함을 원칙으로 한다.

제24조(응용프로그램 운영) ① 응용프로그램 운영자는 응용프로그램 사용자 계정에 대한 패스워드 변경을 최소 6개월에 1회 이상 실시해야 한다.

② 응용프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석하여 자료의 불법접근 및 변조에 대한 위험성을 사전에 방지해야 한다.

③ 응용프로그램의 버전관리는 소스프로그램과 실행프로그램의 버전이 일관성을 유지하도록 한다.

④ 개발된 응용프로그램의 복제는 시스템관리자의 사전양해와 입회하에 실시해야 한다.

⑤ 응용프로그램의 추가 · 삭제 또는 변경은 부서장의 허가를 받은 후에 시스템 관리자의 의해 실시되어야 한다. <개정 2021.12.01.>

⑥ 응용프로그램(업무용 프로그램)의 사용은 해당 업무 담당자별로 자기 업무에 대해서만 업무용 프로그램을 사용할 수 있으며, 해당 업무에 대한 사용권한 요청은 권한요청서로 신청을 하고 사용 승인을 받아야 한다. <개정 2021.12.01.>

⑦ 운영 중인 시스템에는 응용프로그램의 소스프로그램을 설치하지 않는 것을 원칙으로 한다.

⑧ 별도지침에 의해 중요자료로 분류된 응용프로그램은 가동 전 위원회의 보안검증을 받아야 한다.

제9장 PC 관리

제25조(PC 관리) ① PC 기동 시 CMOS에서 제공하는 패스워드를 설정한다.

② 화면 보호기를 작동시켜야 하며 패스워드를 설정한다.

③ 장시간 자리를 비울 때는 전원을 끈다.

④ 자신의 업무에 사용하는 응용프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 안된다.

⑤ 이동식 저장장치를 사용할 때 또는 데이터를 전송할 때에는 바이러스 검사를 한다. <개정 2013.04.01., 2020.03.01.>

⑥ 중요한 정보는 PC내에 보관하지 아니하며, 별도의 이동식 저장장치에 담아 물리적인 보안이 철저한 위치에 보관한다. <개정 2013.04.01., 2020.03.01.>

⑦ 업무용 연구용 실습용 소프트웨어에 대해서 매 학기마다 소프트웨어 사용신청을 하여서 배정된 라이선스에 한해서 사용하여야 하며 배정받지 않거나 라이선스가 없는 소프트웨어에 대해서는 삭제하여야 한다.

⑧ 교내 PC사용자는 본 대학교에서 사용하는 보안정책을 따라야 하며, PC의 보안강화를 위해 교내에서 사용 배포하는 각종 에이전트(PMS, 개인정보 암호화 등)를 설치 운영하여야 한다. <신설 2020.03.01.>

제25조의2(노트북 및 휴대용 단말기 관리) ① CMOS, 로그온, 화면보호기에 비밀번호 설

정이 되어야 한다. <신설 2017. 07. 01.>

② 문서자료 보호를 위해 문서에 대해 암호화 또는 비밀번호 설정을 하여야 한다. <신설 2017. 07. 01.> <개정 2021. 12. 01.>

③ 업무자료의 보호를 위해 사용한 업무자료에 대해서 완전히 삭제를 하여야 한다. <신설 2017. 07. 01.> <개정 2021. 12. 01.>

제26조(바이러스 예방 및 조치) ① 정보보안팀은 컴퓨터 바이러스 발생이 우려되는 날짜에는 미리 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.

② 윈도우 부팅시 바이러스 체크기능을 설정하여 부팅시 바이러스를 진단할 수 있도록 한다.

③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.

④ 알려진 바이러스의 경우에는 해당 바이러스를 치료할 수 있는 진단 프로그램을 구비한다.

제10장 시스템실 운영 · 관리

제27조(시스템실 시설기준) ① 출입구에 입실자를 식별 및 로깅 가능한 출입보안장치(CCTV, 이중잠금장치)를 설치하거나 출입 시 담당자와 대동하여야 한다. <개정 2017. 07. 01.>

② 자동화재경보 설비를 설치하고, 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 소화설비를 설치한다.

③ 정전에 대비하여 별도의 전원공급 시설을 둔다.

④ 온도와 습도를 적절히 유지할 수 있는 항온항습시설을 설치한다.

제28조(시스템실 운영 및 관리) ① 시스템실의 운영을 담당하고 있는 부서장은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.

② 시스템실의 운영자는 운영일지 및 장애일지를 작성해야 한다.

③ 시스템 운영자는 주기적으로 로그화일을 분석해야 하며, 시스템에 이상이 발견되었을 경우에는 보안사고 처리지침에 따라 즉시 조치를 취하고 이를 정보보안팀 및 부서장에게 보고해야 한다.

④ 시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.

⑤ 시스템실 자료보관실 및 통신실은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

⑥ 시스템실 내에서는 카메라 소지 및 촬영을 제한할 수 있다. <신설 2017. 07. 01.>

제11장 USB메모리 등 보조기억매체 관리

제29조(보조기억매체사용) ① 업무상의 비밀자료 및 중요자료가 보관되어 있는 보조기억매체는 사용 시 보조기억매체 관리대장에 등록 후 사용하여야 한다.

② 보조기억매체의 사용은 해당업무의 팀장 책임하에 관리 사용하는 것을 원칙으로 하며 그 팀장이 관리책임자가 된다.

③ 보조기억매체의 관리번호는 팀·과명, 사용용도, 연번으로 한다.(예:디지원-인증서-01)

제30조(보조기억매체 불용처리 및 재사용) ① 업무상 목적으로 사용한 보조기억매체는 불용처리 시 물리적 파기를 원칙으로 하며 그 사실을 보조기억매체 관리대장에 기록하여야 한다.

② 보조기억매체의 재사용을 위해서는 반드시 수록된 자료를 완전히 삭제·포맷 후 재사용하여야 하며 그 사실을 보조기억매체 관리대장에 기록하여야 한다.

제31조(보조기억매체 분실 시 대처방안) 보조기억매체의 분실 시 즉시 관리책임자에게 보고하여야 하며, 공인 인증서용은 즉각 등록을 해지하고 보조기억매체 취급자에게 사용상의 주의를 환기시켜야 한다.

제12장 기 타

제32조(보유기간) 보안규정을 위해 사용되는 각종 양식 자료는 제출받은 후 유효 효력이 끝나는 시점에 파기하여야 한다.

제33조(시행세칙) 이 규정의 운용에 필요한 세부사항은 시행세칙으로 따로 정할 수 있다.

제34조(준용) 이 규정에 명시되지 않은 사항은 관계 법령(전기통신법, 전기통신사업법, 통신비밀보호법, 개인정보보호법)과 본 대학교의 제반규정에 따른다. <개정 2012. 01. 30.>

제35조(원격근무 보안관리) ① 재택 · 파견 · 이동근무 등 원격근무를 지원하기 위한 정보시스템을 도입 · 운영할 경우 기술적 · 관리적 · 물리적 보안 대책을 수립할 수 있다. <신설 2017. 07. 01.>

② 원격근무 가능 업무 및 공개 · 비공개 업무 선정기준을 수립하되 대외비 이상 비밀자료를 취급하는 업무는 원격근무 대상에서 원칙적으로 제외하되 반드시 수행해야 하는 경우 보안대책 강구 후 수행 여부를 결정한다. <신설 2017. 07. 01.>

③ 모든 원격근무자에게 별지서식 23호 서식의 보안서약서를 징구할 수 있다. <신설 2017. 07. 01.>

④ 원격근무자는 원격근무시 해킹에 의한 업무자료 유출을 방지하기 위하여 작업 수행 전 백신으로 원격근무용 PC점검 · 원본자료 저장금지 등 보안조치를 수행하여야 한다. <신설 2017. 07. 01.>

부 칙

이 규정은 2009년 11월 일부터 시행한다.

부 칙

이 규정은 2011년 5월 1일부터 시행한다.

부 칙

이 규정은 2013년 4월 1일부터 시행한다.

부 칙

이 규정은 2014년 7월 1일부터 시행한다.

부 칙

이 규정은 2020년 3월 1일부터 시행한다.

부 칙

이 규정은 2021년 12월 1일부터 시행한다.

부 칙

이 규정은 2022년 10월 1일부터 시행한다.

부 칙

이 규정은 2023년 10월 16일부터 시행한다.

[별지 서식 1호]

개인정보화 파일대장

보유목적			
보유근거			
수집방법		대상범위	
대상인원수		보유기간	
열람예정일		사용부서	
열람청구부서 및 주소			
열람제한항목		열람제한사유	
제공기관			
제공근거			
제공항목			
기록항목			

[별지 서식 2호]

개인정보 침해신고 처리대장

접수내용		신고개요	처리결과	결재		비고
접수일시	신고자 인적사항			담당자	부서장	

[별지 서식 3호]

처리정보 제공대장

① 화 일 명			
② 피제공기관			
③ 제공일자		④ 제공주기	
⑤ 제공형태		⑥ 이용기간	
⑦ 이용목적			
⑧ 제공근거			
⑨ 제공항목			
⑩ 비고			

[별지 서식 4호]

개인정보열람(정정)청구 처리대장

일자	청구인 인적사항		정보주체인 적사항	열람(정정) 내용	처리결과	결재		비고
	성명	연락처				담당자	부서장	

[별지 서식 5호]

IP 신청서

IP 신청서	결재	담당		팀장	원장

학과/부서명		사용자	
E-mail			
사 용 호 실			
Lan Card 종류			
어댑터주소 (Mac Address)	- - - - -		
IP 신청 개수	( ) 개		
사 용 용 도			

년 월 일

소 속: 신청자명 : (인)

대원대학교 미래전략처장 귀하

[별지 서식 6호]

방화벽 개방 신청서

방화벽 개방 신청서	결재	담당		팀장	원장

학과/소속명		담당자명	
전화번호		핸드폰번호	
E-mail			
사용호실			
출발지 IP Address (외 부 서 버)			
목적지 IP Address (교 내 서 버)			
개방포트번호 (서 비 스 명)			
개방기간			
개방신청 사유			

년 월 일

소 속: 신청자명 : (인)

대원대학교 미래전략처장 귀하

(미디어팀 기록사항)

※ 처리 결과

1. 처리 일자 : 년 월 일
2. 처 리 자 :
3. 비 고 :

[별지 서식 7호]

서버등록 신청서

서버등록 신청서	결재	담당		팀장	원장

주 관 부 서	학과/부서명	
	관리책임자	직위 : 성명 : E-mail :
서버 시스템	서버관리자	소속 : 성명 : E-mail : 연락처 :
	설치장소	
	서 버 명	
	서버 IP Address	. . .
	서버용도	
	서버기종	
	사용 OS	
D N S	Domain Name	1)_____ 2)_____ 3)_____
외부사용자 접속 허용 서비스		Telnet ( ), WWW ( ), FTP ( ), Mail ( ) SSH ( ), 기타서비스 ( )

년 월 일

관리책임자 소속 : 책임자명 : (인)

시스템 관리(보안, 해킹)에 주의하며, 보안문제 발생 시 책임질 것을 서약하며

위와 같이 서버를 등록하고자 등록서를 제출합니다.

대원대학교 미래전략처장 귀하

(미디어팀 기록사항)

※ 처리 결과

1. 등록 일자 : 년 월 일
2. 등록자 :
3. 비 고 :

[별지 서식 8호]

홈페이지 개설 등록 신청서

홈페이지 개설 등록 신청서	결재	담 당		팀 장	원 장

신 청 자		계 정	
학과/부서명		개설자 ID	
관리자 성명		사용자 암호	
연 락 처			
사용기간			
사용용도			

계정에 대한 용량은 기본 100M로 제한 합니다.

[개인정보 수집 동의]

1. 수집·이용목적 : 홈페이지 개설을 위한 아이디 발급
2. 수집하는 개인정보 항목 : 학과/부서명, 아이디, 성명, 암호, 연락처
3. 개인정보의 보유 및 이용 기간 : 준영구(업무자의 업무 내역 로그 관리)
4. 동의를 거부 할 수 있으며, 거부 시 홈페이지 개설을 할 수 없습니다.

위와 같이 홈페이지를 개설하고자 신청서를 제출하며 개인정보의 수집·이용에 동의합니다.

년 월 일

신 청 자 : (인)

책 임 자 : (인)

대원대학교 미래전략처장 귀하

(미디어팀 기록사항)

※ 처리 결과

1. 등록 일자 : 년 월 일
2. 등록 ID :
3. 처리자 :
4. 비 고 :

[별지 서식 9호]

정품소프트웨어 사용 서약서 및 정보시스템 계정신청서

정품소프트웨어 사용 서약서 및 정보시스템 계정신청서	결재	계 장	계 장	팀 장	처 장
				전결	

정품소프트웨어 사용 서약서

본인은 대원대학교 및 대원대학교산학협력단에 근무하는 교·직원으로서 대원대학교내에서는 제공받은 컴퓨터만을 사용할 것이며 제공받은 컴퓨터에는 업무상 필요한 정품 소프트웨어와 정품 폰트 프로그램만을 사용할 것입니다. 또한 위 사항을 위반하여 발생되는 모든 문제에 대하여 민·형사상의 책임을 질 것을 서약합니다.

년 월 일

서약자 : (인)

정보시스템 계정 신청서

이 름		부 서		생년월일	
id(1)		id(2)		비밀번호(9자리)	
핸드폰		전 화		E-mail	
사용기간(목적)					

※ 정보시스템 계정 신청서 작성 시 유의사항 ※

1. 이름, 부서, 생년월일을 빠짐없이 기록한다.
2. ID(2)는 ID(1)을 이미 누군가가 사용하고 있을 경우 사용하고자 하는 ID를 기록한다.
   → 본 대학교 재학생시절 사용하던 ID 사용불가
   → ID의 첫째자리는 필히 영문자로 하며 영문과 숫자를 조합하여 6~9자리로 한다.
3. 비밀번호를 기록한다.
   → 비밀번호는 ID와 상이하고, **영문과 숫자 혼합하여 9~13자 이상으로 한다.**

[개인정보 수집 동의]

1. 수집·이용목적 : 학사행정 업무를 위한 각종 업무용 프로그램 아이디 발급
2. 수집하는 개인정보 항목 : 아이디, 부서명, 생년월일, 비밀번호, 핸드폰, 전화, 이메일
3. 개인정보의 보유 및 이용 기간 : 준영구(업무자의 업무 내역 로그 관리)
4. 동의를 거부 할 수 있으며, 거부 시 업무용 아이디 발급이 되지 않습니다.

위와 같이 계정을 등록하고자 신청서를 제출하며 개인정보 수집안내의 내용을 숙지하고 개인정보 수집 및 이용에 동의합니다.

년 월 일

서약자 : (인)

대원대학교 미래전략처장 귀하

이하 하단은 미디어팀 기재사항임(신청자는 기재하지 말 것)

전임자	이름		ID	
	※ 업무프로그램 사용정지 1. 그룹웨어조직도□ 2. Cool-Messanger□ 3. 학사□ 4. 기자재□ 5. 생활관□ 6. 홈페이지민원게시판□ 7. SMS권한□ 메일 그룹핑 삭제 : (1)교수모두□ (2)조교모두□ (3)직원모두□ (4)팀장□ (5)학과장□ (6) 산단□			
신청자	※ 업무프로그램 사용등록 1. 홈페이지□ 2. 그룹웨어조직도□ 3. Cool-Messanger□ 4. 학사□ 5. 기자재□ 6.생활관□ 7. 홈페이지민원게시판□ 8. SMS권한□ 메일 그룹핑 추가 : (1)교수모두□ (2)조교모두□ (3)직원모두□ (4)팀장□ (5)학과장□ (6) 산단□			
처리일자 : 년 월 일 / 처리자 : (인)				

[별지 서식 10호]

무선 랜 Mac Address 인증 신청서<삭제:2020.03.01.>

[별지 서식 11호]

소프트웨어 사용 신청서

순번	소프트웨어		수량	교과목	교수	위치		비고
	이름	버전				건물	호실	
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

[별지 서식 12호]

정보통신실 출입 대장

순번	내	용		
1	출입일자	20 년 월 일	출입자(외부인)	(인)
			입회자(디지원)	(인)
	출입장소			
	출입목적			
2	출입일자	20 년 월 일	출입자(외부인)	(인)
			입회자(디지원)	(인)
	출입장소			
	출입목적			

[별지 서식 13호]

보안준수 서약서(외부인용)

본인은 대원대학교 미디어팀의 보안통제구역(인터넷을 통한 장비 접속 포함)에 출입하는 바, 다음사항을 준수할 것을 서약합니다.

1. 본 대학교의 **업무와 관련한 기밀, 학생·교직원등 관련자의 개인정보** 또는 시설 등에 관하여 **업무상 인지한 보안사항**을 출입기간 중은 물론 그 이후에라도 일절 타에 누설하지 아니하겠음.
2. 본인은 물론 당사 직원이 보안사항을 외부에 누설시켜 사소한 문제라도 야기시켰을 경우에는 누설자가 **민·형사상 및 보안상의 책임과 관련법령에 의한 조치**에 따를 것을 서약하고, 본인(당사)에 대한 **계약업무의 등록취소, 부적당업자로 입찰참가자격 제한** 등 어떠한 제재조치를 취하여도 이의를 제기하지 않을 것임
3. 본 대학교 관계자의 허가(동의)없이 본 대학교의 시설 및 **물품을 파손하거나 외부로 유출**하지 아니하겠음.

Ⅰ. 보안통제구역

미디어팀(기계실) · 본관 장비실 및 각 건물 네트워크 장비실, 기타 관계자의 제한요청장소

Ⅱ. 관련근거

1. 개인정보보호법 - 제70조(벌칙), 제71조(벌칙), 제72조(벌칙)
   1) 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.
   2) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
      5. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
      6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자
   3) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
      3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자
2. 정보통신망이용촉진등에 관한 법률 - 제71조(벌칙), 제72조 (벌칙)
   1) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
      제48조제2항을 위반하여 악성프로그램을 전달 또는 유포한 자, 제48조제3항을 위반하여 정보통신망에 장애가 발생하게 한 자, 제49조를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자
   2) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
      제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자

20 년 월 일

소속/회사명 :
직 위 :
연 락 처 :
성 명 : **(인)**

[별지 서식 14호]

보조기억매체 관리대장

[관리책임자 :]

연번	관리번호	매체 형태	등록 일자	취급자	용도	불용처 리일자	불용처리방법 (재사용·용도)	비고
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

[별지 서식 15호]

업무용 프로그램 사용권한 요청서

업무용 프로그램 사용권한 요청서	결 재	담 당		팀 장	원 장

대상 업무 프로그램	(예 : 학사, 기자재, 입시 등)		
신청자 학과/부서명			
신 청 자			
권한요청 업무 상세메뉴 위치		권한요청버튼명	
		권한요청버튼명	
		권한요청버튼명	
		권한요청버튼명	
		권한요청버튼명	
		권한요청버튼명	
요 청 일 자			
권한요청이유			
업무담당자 확인	담당자 성명 : (인)		

본인의 업무가 아닌 업무에 대한 권한 요청 시 해당 업무 담당자의 확인을 반드시 받고 신청하시기 바랍니다.

위와 같이 해당업무의 원활한 처리를 위해서 사용권한을 신청합니다.

년 월 일

신 청 자 : (인)

대원대학교 미래전략처장 귀하

(미디어팀 기록사항)

※ 처리 결과

1. 접 수 자 :
2. 접수일자 : 년 월 일
3. 처 리 자 :
4. 처리일자 : 년 월 일

[별지 서식 16호]

업무용 프로그램 사용자 ID 등록 요청서

업무용 프로그램 사용자 ID 등록 요청서	결재	담 당		팀 장	원 장

대상 업무 프로그램	(예 : 학사, 기자재, 입시 등)
신청자 학과/부서명	
신 청 자	
신청자 PC IP 주소	IP Address :
	IP주소 확인 방법 : 컴퓨터의 시작 -> 실행 -> 'cmd' 입력후 엔터 -> 도스창 열림, 도스창에서 ipconfig 입력후 엔터 -> IP Address확인
신청자 사용 ID	ID :
	가능하면 웹 메일 ID와 동일하게 신청
사용 할 비밀번호	
요 청 일 자	
요 청 사 유	

[개인정보 수집 동의]

1. 수집·이용목적 : 학사행정 업무 프로그램 사용을 위한 아이디 발급
2. 수집하는 개인정보 항목 : 학과/부서명, 성명, 아이디, 비밀번호
3. 개인정보의 보유 및 이용 기간 : 준영구(업무자의 업무 내역 로그 관리)
4. 동의를 거부 할 수 있으며, 거부 시 업무용 프로그램 사용이 불가능합니다.

위와 같이 해당업무의 원활한 처리를 위해서 사용자 ID를 신청하며 개인정보의 수집·이용에 동의 합니다.

년 월 일

신 청 자 : (인)

대원대학교 미래전략처장 귀하

(미디어팀 기록사항)

※ 처리 결과

1. 접 수 자 :
2. 접수일자 : 년 월 일

- ID 등록을 위한 담당자 확인 방법 : 담당자명 : 확인방법 : (메일, 유선통화, 구두)

3. 처 리 자 :
4. 처리일자 : 년 월 일

[별지 서식 17호]

보 안 서 약 서(정보보호업무자용)

본 서약서는 본 대학교 재직기간뿐만 아니라 퇴사 이후에도 일정기간 적용될 수 있음을 인식하고 숙지하신 후 동의여부를 확인하여 주시기 바랍니다.

1. 본인은 정보보안업무 수행 중 직•간접적으로 취득한 보안정보, 개인정보 및 기타 이에 준하는 정보와 이를 생산, 보관, 유통, 폐기하는 과정에서 사용되는 모든 물리적 매체 및 산출자료(예:전산장비, 정보저장 및 전송장비, 보고서 등 서류, 사진, 전자파일, 기타 매체와 자료 등)가 본 대학교 소유의 정보자산(이하 "정보자산")임을 확인합니다.

2. 본인은 본 대학교 근무 중 알게 된 정보자산이 분실, 훼손, 침해되지 아니하도록 안전하게 사용•관리하고 보안관련 사고가 발생되지 않도록 하겠습니다. 그리고 동 정보자산을 지정된 업무에 사용할 목적을 제외하고는 무단 반출하거나, 개인적 용도나 제3자를 위한 정보로 이용하지 않겠으며, 제3자에게 누설, 공개, 변조, 복사, 촬영 및 기타 방법에 의한 복제 등의 행위를 일체 하지 않겠으며 본 대학교 보안계획을 성실히 따르겠습니다.

3. 본인은 본인에게 부여된 사용자 ID, 비밀번호 및 관리자용 ID, 비밀번호를 타인과 공동사용 또는 누설치 않겠습니다.

상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며, 본 서약서의 준수사항을 위반한 경우에는 "정보통신망이용촉진 및 정보보호 등에 관한 법률", “개인정보보호법” 등 관련 법령에 의한 일체의 민•형사상 책임을 감수할 것을 서약합니다.

년 월 일

소 속 :
직 책 :
생 년 월 일 :
서 약 자 : (날인 또는 서명)

대원대학교 미래전략처장 귀하

[별지 서식 18호]

용역업체 보안관리 점검 사항

대원대학교

순번	항 목	이행여부
1	용역업체 전산장비는 보안담당관 인가 후 반입 · 반출 * 반출시 보안담당관 통제 하에 저장자료 완전 삭제	
2	전산장비 반입 시마다 악성코드 감염여부 점검	
3	용역업체 노트북PC, 휴대형 저장매체 정기 보안점검	
4	용역업체에 제공된 자료가 있나?(자료 제공 시 보안조치 실시)	
5	외부사이트 접속 노트북PC에서 업무자료 저장 금지	
6	최신 백신 프로그램 설치	
7	비밀번호(9자리 이상) · 화면보호기 설정 및 분기 1회 변경	
8	비인가 저장매체 · 통신기기 접속통제	
9	업체 사용 전산망은 침입차단시스템 등을 활용하여 업무망과 분리하고 필요한 서버에만 제한적 접근 허용	
10	용역업체 직원의 계정은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여하되 기관 내부문서 접근 금지	
11	용역업체 직원의 'root' 계정 등 시스템에 중대한 영향을 끼칠 수 있는 계정에 대한 단독적인 접근을 불허	
12	용역업체 계정 생성 및 권한 부여 여부	
13	참여인원에게 패스워드 부여 여부	
14	시스템 설치, 운영체제 중요설정 변경 등이 필요한 경우 본 대학교 미디어티 직원의 통제 하에 작업	

대원대학교 시스템 보안을 위해 용역업체 작업자로서 위와 같이 조치하였음을 확인하며 위 사항으로 문제 발생 시 책임을 감수 하겠습니다.

년 월 일

회 사 명 :
직 위 :
연 락 처 :
성 명 : **(서명)**

대원대학교 확인자 소속 : **성명 :** **(서명)**

[별지 서식 19호]

기계실 출입 인가자 관리대장(보안장치 출입)

- 미디어팀 기계실의 전자 출입 인가자의 등록 및 삭제 관리 대장
- 개인정보 수집 및 이용 목적 : 보안장치를 통한 기계실 출입자 등록을 위함
- 수집하는 개인정보 항목 : 지문, 주민등록번호
- 개인정보의 보유 및 이용기간 : 사용자가 기계실 출입이 허용되는 시기까지
- 개인정보 수집 및 이용 동의를 거부할 수 있으나 거부 시 직접 기계실 출입을 할 수 없음

[관리책임자 : 미래전략처장]

연번	소속	이름	등록일자	개인정보 수집 이용 동의(싸인)	등록자	이용자 삭제일자	삭제자	비고
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

[별지 서식 20 호]

정보시스템 저장매체 · 자료별 삭제 이력 관리 대장

연번	저장자료	저장매체	매체갯수	삭제방법	삭제일자	작업자	보안담당관 확인	비고
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

- 저장자료 : 공개자료, 민감자료(개인정보 등), 비밀자료(대외비 포함)
- 저장매체 : 플로피디스크, 광디스크, 자기테이프, SSD, USB, 하드디스크
- 삭제방법 : 완전파괴, 전용소자, 완전포멧(3회), 완전포멧(1회)

[별지 서식 21호]

작성일	년 월 일	개별서버관리대장	결재	담당		팀장	원장
작성자							

자산번호		서버모델	
서버이름		IP Address	
서버역할		서버 OS	
도입일자		서비스/포트	
HW사양			

일 자	시스템 보안패치 이력

[별지 서식 22호]

작성일	년 월 일	기계실 장비 점검 일지 (서버, 네트워크)	결재	담당		팀장	원장
작성자							

	서버명	사용율(Cpu, Memory, Disk) 및 점검(서비스, Event Log) 현황						
		CPU	Memory	Disk 사용율(%)	서비스 정상 여부	Event Log 특이사항	불필요한포트제거 유무	LED
서버관리								

										SPAM MAIL
멀웨어 & mail	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □
	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	스팸 □
파일 위/변조	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	정상 □	
	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	이상 □	

네트워크 기타	장 애 내 역	조 치 내 역

Patch / Update	

[별지 서식 23호]

보안 서약서

본인은 _____년 __월 __일부로 원격근무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 부여받은 인증관련 정보 및 매체를 타인에게 유출하지 아니한다.

2. 나는 원격근무 중 작성, 저장, 열람, 출력한 문서는 업무 목적에만 활용하고 타인에게 유출하지 아니한다.

3. 나는 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스 백신 프로그램 및 기타 보안 프로그램을 설치하여 최신 상태로 유지한다.

4. 나는 기타 보안사항들을 성실히 준수하며 위반 시 관련 규정에 따라 어떠한 처벌도 감수한다.

년 월 일

서약자 소 속:
직급(직위) :
성 명 : 서명(인)

서약집행자 소 속:
직급(직위) :
성 명 : 서명(인)

[첨 부 1]

정보시스템 저장매체 · 자료별 삭제방법

저장 자료 / 저장 매체	공개자료	민감 자료 (개인정보 등)	비밀 자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크(CD · DVD등)	㉮	㉮	㉮
자기테이프	㉮ · ㉯중 택일	㉮ · ㉯중 택일	㉮
SSD · USB 등 반도체메모리 (EEPROM 등)	㉮	㉮	㉮
하드디스크	㉰	㉮ · ㉯ · ㉰중 택일	㉮ · ㉯중 택일

㉮ : 완전파괴(소각 · 파쇄 · 용해)

- 중요 내용이 저장된 플로피디스켓 · 광디스크 등의 파쇄시에는 파쇄조각의 크기가 가급적 0.8mm 이하가 되도록 조치

㉯ : 전용 소자장비 이용 저장자료 삭제

- 소자장비는 반드시 저장매체의 자기력보다 큰 자기력 보유

㉰ : 완전포멧 3회 수행

- 저장매체 전체를 ‘난수’ · ‘0’ · ‘1’ 로 각각 중복 저장하는 방식으로 삭제

㉱ : 완전포멧 1회 수행

- 저장매체 전체를 ‘난수’로 중복 저장하는 방식으로 삭제