정보보호관리규정 4-5-13

규정번호 4-5-13
제정일자 2018.8.27
최근개정 2024.5.3
개정차수 2차 개정
관리부서 정보관리팀

제1조(목적) 이 규정은 명지전문대학(이하 “대학”라 함) 의 자산에 대한 내·외부로부터의 훼손, 변조, 도난, 유출 등의 다양한 형태의 위협으로부터 효과적으로 보호하기 위한 정보보호 상위 규정과 구성원이 준수하여야 할 정보보호 규정을 정함을 목적으로 한다. 정보보호를 위한 최상위 규정으로서 대학이 적용받는 고등교육법, 개인정보보호법, 정보통신망법 등 정보보호와 관련된 법령 준수와 정보보호를 위한 정보보호 관리체계의 구축, 운영, 개선 업무를 위하여 필요한 사항을 규정하여 대학 구성원 및 외부 인력이 준수해야 할 정보보호 활동 범위와 기준을 제시하는데 목적이 있다.(개정 2024.5.3.)

제2조(적용범위) 이 규정은 대학 구성원 대상으로 적용되며, 계약관계에 의하여 대학의 자산에 접근하는 모든 제3자에게도 적용된다. 이 규정에서 사용되는 용어는 각 하위 정보보호지침에서 규정된 ‘용어의 정의’를 사용한다.(개정 2024.5.3.)

제3조(용어정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.(개정 2024.5.3.)

1. 시스템 관리자 : 정보시스템의 운영 및 관리를 담당하는 자
2. 정보보호 사고: 보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출·변조되어 업무수행에 지장을 초래하는 사고
3. 정보시스템 : 컴퓨터의 본체, 주변장치 및 단말장치, 통신장비 등의 전부 또는 일부로써 구성되는 하드웨어 및 소프트웨어 총칭
4. 제3자 : 방문객, 피교육자, 일용근로자와 같이 교직원이 아닌 외부인 또는 대학과 계약관계에 있는 타 회사(조직) 및 이에 속하는 직원
5. 보호구역 : 중요정보 및 중요시설에 대한 비인가자의 접근을 통제하기 위한 장소로서 제한구역, 통제구역을 지정
6. 제한구역 : 대학의 보호구역으로, 중요정보를 취급하는 장소로서 출입에 안내가 요구되는 보호구역
7. 통제구역 : 대학의 보호구역으로, 중요시설 설치·운영하는 장소로서 제한된 인원만 출입이 가능한 보호구역
8. 보안사고 : 대학의 자산이나 대학 업무에 손해를 줄 수 있거나 대학의 보안 절차를 위배하는 행동
9. 구성원 : 교수, (계약)직원, 조교, 학생, 용역업체 직원 및 시간제근로자 등 포함(신설 2024.5.3.)

제4조(책임사항) 대학의 정보보호에 대한 책임은 모든 구성원에게 있으며 이를 위하여 정보보호 관련 규정을 모든 구성원이 숙지하여 준수하여야 한다.(개정 2024.5.3.)

① 모든 구성원이 본 규정의 내용을 숙지하여 생활화하기 위해서 적절한 교육이 시행되어야 하며, 정보보호 담당부서는 이에 대한 책임이 있다.(개정 2024.5.3.)

② 법적, 규범적, 해당 감독기관(행정안전부, 교육부, 방송통신위원회 등)의 요구사항이 만족되어야 한다.

③ 정보보호 훈련은 모든 구성원에게 적용되어야 한다.(개정 2024.5.3.)

④ 정보보호에 대한 위반은 실제적이거나 의심스러운 경우 모두 정보보안담당관에게 보고되어야 하며, 정보보안담당관은 이를 면밀히 조사해야 한다.

⑤ 정보보안담당관은 규정의 유지관리 및 이행을 위한 충고 및 지침 제공의 직접적인 책임을 가진다.

⑥ 본 규정을 준수하여야 하는 책임은 모든 구성원에게 해당한다.(개정 2024.5.3.)

제5조(정보보호 정의) ① 정보의 생성, 저장, 처리, 송신, 수신시에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 비용대비 효과적으로 방지하여 정보에 대한 기밀성, 무결성, 가용성을 확보하는 것이다.

1. 기밀성(Confidentiality): 자산이 적절한 수준의 비밀성을 유지하면서 공개되지 않으며 오직 인가된 사람만이 정보에 접근할 수 있다.
2. 무결성(Integrity): 자산의 고유 성질이 인가되지 않은 내부 또는 외부로부터 변경 또는 변조되지 않고 정확성과 완전성을 유지할 수 있다.
3. 가용성(Availability): 인가된 사용자가 자산을 이용하고자 할 때 해당 자산의 이용 가능한 정도를 나타내며 해당 정보와 관련한 자산에 접근할 수 있음을 보장하는 것이다.

② 대학은 정보를 보호하기 위하여 특정 규정, 지침, 절차, 조직 구조 및 소프트웨어 기능을 포함하는 적절한 범위의 통제를 수행한다.

③ 정보보호는 조직이 제공하고 있는 업무 등에 관련된 정보보호 관련 법적 요구사항을 반영하여 수립하여야 한다.

제6조(정보보호 목표) 정보보호의 목표는 대학 업무의 연속성을 보장하고, 정보보호 사고로 인한 시스템 및 자원의 피해를 최소화하는 것이다.

제7조(정보보호 범위) ① 정보보호는 대학을 대상으로 한다. 정보보호 대상이 되는 대학의 자산은 다음을 포함한다.(개정 2024.5.3.)

1. 정보자산
2. 문서자산
3. 소프트웨어 자산
4. 하드웨어 자산
5. 기타 자산

② 정보보호의 범위를 설명하기 위하여 다음과 같은 내용이 포함된 문서를 작성하여야 한다.

1. 주요 서비스 및 업무 현황
2. 서비스 제공과 관련된 조직
3. 정보보호 조직, 주요 설비 목록
4. 정보시스템 목록 및 네트워크 구성도
5. 문서 목록 (예: 규정, 지침, 매뉴얼 등)

제8조(정보보호 관리규정 및 지침) ① 정보보호 관리규정 및 지침의 운영 및 관리

1. 정보보안담당자는 규정 및 지침을 내부문서로 관리한다.
2. “정보보호 관리규정”은 대학의 업무와 관련된 모든 어플리케이션 서비스 및 운영에 적용한다.
3. 규정에 제시된 문서와 지침은 모두 작성하는 것을 원칙으로 한다.
4. 정보보호 관리규정 및 지침은 이행계획에 따라 이행결과를 정보보안담당관 또는 총장의 승인을 받아야 한다.(개정 2024.5.3.)
5. 정보보호 관리규정 및 지침 제/개정 시 관련문서는 최신본으로 게시판 또는 문서로 공표한다.(개정 2024.5.3.)
6. 정보보호 관리규정 및 지침은 관련법령 및 내부 규정과 연계성이 있는지 확인한다.
7. 정보보호 관리규정 및 지침 시행일은 정보보안담당관 또는 총장의 승인 시점일로부터 시작된다.(개정 2024.5.3.)
8. 정보보호 관리규정 및 지침의 적절성을 유지하기 위하여 정보보호 담당부서의 장은 최소 1년 주기로 검토하고 필요시 개정안을 마련하여 정보화추진위원회에서 검토하고 총장의 승인을 받는다.
9. 다음과 같은 상황이 발생한 경우를 포함하여 주기적으로 정보보호 관리규정 및 지침 문서의 타당성을 검토하여 반영한다.
    - 내부감사(점검 등) 수행 결과(개정 2024.5.3.)
    - 중대한 보안사고 발생
    - 개인정보 및 정보보호 관련 법령 제·개정
    - 새로운 위협 또는 취약점 발견
    - 정보보호 환경의 중대한 변화
    - 조직 업무 환경의 변화 (예: 신규 업무)
    - 정보시스템 환경의 중대한 변화 (예: 차세대 시스템 구축)
10. 정보보호 관리규정 및 지침은 제정, 개정, 배포, 폐기 등의 이력을 확인할 수 있어야 한다.

② 정보보호 관리규정 및 지침의 수립 절차

1. 대학업무의 위험성 평가 후 대학업무의 정보위협 영향에 따라 규정을 수립한다.
2. 사업목표와 환경에 대한 이해를 바탕으로 향후 사업 성공을 위해 시급히 정보보호가 요구되는 영역과 지속적으로 관리해 나가야 할 영역을 구분하여 정립한다.
3. 정보보호와 관련하여 현행 IT 아키텍처뿐만 아니라 향후의 IT 도입 방향 및 아키텍처를 고려한다. 이를 통해 정보보호 체계 설계 단계에서 장기적 관점을 견지하고, 향후 정보보호 요구에

부합하는 방향을 설정할 수 있도록 한다.

4. 정보보호지침 항목을 도출한다.
5. 대상이 되는 자산 및 업무 현황파악을 바탕으로 정보보호지침을 수립하고 그 결과를 반영한다.
6. 수립된 정보보호지침은 적용성 및 적정성 여부를 검토하여 수정한다.

제9조(정보보호 조직 운영) ① 정보보호 기반구조

1. 대학 내 정보보호 활동을 관리하기 위한 정보보호조직을 구성·운영하며, 각 구성원은 본인에게 부여된 정보보호 책임과 역할을 수행한다.
2. 총장은 정보보호에 대한 최종적인 책임이 있으며, 정보보호 관리규정을 최종 승인한다.
3. 정보화추진위원회는 전사적인 정보보호 활동에 대한 수용 및 지원, 중대 정보보호 사고에 대한 대책 협의를 수행한다.(개정 2024.5.3.)
4. 정보보안담당관은 교무위원급 또는 정보보호 담당부서의 장으로 지정하고, 정보보호 업무를 총괄한다.
5. 정보보안담당관은 대학 사업방향에 기초한 정보보호 계획을 수립하여 시행한다.
6. 정보보호 담당부서는 정보보호 실무를 수행하는 중심 조직으로써 개인정보보호 활동을 포함한 지속적인 정보보호 대책의 적용, 정보보호 취약성 점검을 통한 정보보호 사고 예방 및 대응 지원 업무를 수행한다.
7. 부서별 정보보안담당자는 정보보호에 대한 부서별 특정 역할 및 책임을 수용하며 정보보호 담당부서와 긴밀한 협조체제를 유지하여 부서 내 자산관리와 정보보호 활동 수행 및 홍보 업무를 주도한다.

[참조문서] 정보보호 조직운영지침

제10조(인적 보안) ① 정보보호에 대한 책임과 역할

1. 교직원

   모든 교직원은 채용 시 정보보호서약서를 제출하여야 하며, 업무상 취득한 대학 또는 제 3 자 소유의 정보를 대학의 사전승인 없이 누설해서는 아니 된다

   대학의 중요정보에 접근하는 개인정보취급자는 비밀유지서약서를 제출해야 한다.

2. 관련 부서

   교직원은 퇴직 시 비밀유지서약서를 작성하며, 내·외부 정보시스템에 접속을 제한(계정 삭제 등) 하여야 한다.(개정 2024.5.3.)

② 교직원에 대한 정보보호 교육

1. 정보보호 교육담당자는 교직원 및 외부자를 대상으로 정보보호 교육을 정기적 또는 비정기적으로 실시하여야 한다.
2. 정보보호 교육담당자는 정보보호 교육 연간 계획을 수립하고, 계획에 따라 연 1회 이상 정보보호 교육을 실시한다.
3. 정보보호 직무자는 기본 정보보호 교육 이외에 정보보호와 관련된 별도의 직무교육을 이수하

여야 한다.(개정 2024.5.3.)

③ 제3자 접근에 대한 보안

1. 제3자의 접근으로부터 대학의 정보시스템과 정보자산을 보호하기 위해서 다음과 같은 통제를 시행하여야 한다.

대학의 정보 또는 IT 시설에 대하여 제3자의 접근을 허용할 경우 정보보호 담당부서는 접근을 요청하는 부서에게 보안통제를 적용하게 한 후 제3자의 접근을 허용해야 한다.

제3자 접근을 승인할 시에는 접근을 요청하는 부서는 반드시 정보자산보호서약서를 징구하여야 하며, 제3자에게 대학의 보안요구 사항을 주지시킬 의무가 있다.

④ 외주용역

1. 외주용역 직원은 교직원과 동일한 수준의 정보보호 요구사항을 준수하여야 한다.
2. 제3자와의 계약 필요시 계약서에는 제3자가 준수하여야 할 대학 보안요구사항을 포함하여야 한다.
3. 대학의 정보시스템 및 네트워크의 일부 또는 전부를 외주업체와의 계약으로 제공받을 경우에도 외주업체의 계약서에 외주업체가 준수하여야 할 대학 보안 요구사항이 포함되어야 한다.
4. 표준개인정보처리위탁계약서 내에 보안관련 문구가 있어야 한다.(개정 2024.5.3.)
5. 정보자산에 대한 접근은 해당 부서의 담당자가 허용하는 것을 원칙으로 한다.
6. 외주용역 업무를 관장하는 해당 부서장은 용역 인력 및 용역 회사로부터 정보자산보호서약서를 반드시 받아 관리해야 한다.
7. 외주용역 업체 임직원에 대하여 규정, 지침, 절차의 준수 및 보안책임을 교육한다.

[참조문서] 인적 보안지침

제11조(침해사고 대응) 대학의 업무 활동을 방해하는 침해사고가 발생했을 때 이에 대한 효율적인 처리 및 복구를 위한 대응체계를 갖추어 피해를 최소화하고, 업무수행 및 서비스 제공의 연속성을 확보하여야 한다.

① 침해사고 대응

1. 해킹 바이러스 등으로 인한 침해사고 발생에 대비하여 대학 전체에 걸쳐 침해사고 대응계획을 개발하고 유지하기 위한 관리 프로세스를 수립한다.
2. 침해사고 대응계획은 침해사고 정의 및 범위, 대응체계(보고 및 조치 체계), 대응방법 및 절차, 복구 방법 및 절차, 증거자료 수집 및 보관 등을 포함한다.
3. 침해사고 대응계획은 정기적으로 테스트되고 그 유효성을 검증한다.
4. 침해사고 대응계획의 변경 절차를 수립하고, 변경된 침해사고 대응계획을 관련 구성원에게 교육하고 공지한다.(개정 2024.5.3.)

[참조문서] 침해사고 대응지침

제12조(정보보호조치 점검)

① 대학의 정보보호 업무활동은 유관기관의 관계법령을 준수하고, 정보보안담당관은 유관기관의 관계 법령을 문서화하여 관리할 책임이 있다.(개정 2024.5.3.)

② 정보보안담당관은 유관기관의 관계 법령의 최신성을 유지·준수할 수 있도록 문서화하고 관리할 책임이 있다.

③ 정보보안담당관은 연간 정기 정보보호 감사(점검 등)계획을 수립하여 이행할 책임이 있고 그 계획을 총장에게 보고 후 내부감사(점검 등)를 수행한다.(개정 2024.5.3.)

④ 정보보호 담당부서는 정보보호 규정의 준수여부, 정기 정보보호 감사(점검 등) 및 필요시 비정기 감사를 수행한다. 그 결과는 정보보안담당관에게 보고해야 하며 차년도 정보보호 계획에 반영한다.(개정 2024.5.3.)

⑤ 정보보호 담당부서는 정보시스템에 대한 기술적 취약성 점검을 정기적으로 이행한다.

⑥ 정보보호 담당부서는 보안 침해사고에 대비하여 보고 및 대응절차를 문서화하고 보안 사고가 발생하거나 발생 가능성이 있을 경우 정보보안담당관의 지시 하에 피해를 최소화하기 위한 조치를 신속히 취하여야 한다.

⑦ 모든 구성원은 보안 사고와 보안 체계의 취약점을 발견하면 지체 없이 정보보호 담당부서와 소속 부서(장)에게 수립된 절차에 의거하여 보고한다.(개정 2024.5.3.)

[참조문서] 취약점 점검지침, 침해사고 대응지침

⑧ 정보보안담당관은 보고된 보안사고 관련 자료를 분석하여 재발 방지를 위한 노력을 하여야 하며, 보안사고 발생 시 사고가 내부자의 소행으로 판명될 경우 징계할 수 있다.(개정 2024.5.3.)

[참조문서] 인적 보안지침, 침해사고 대응지침

제13조(자산분류와 통제) ① 대학의 모든 중요 자산을 적절히 보호하기 위해 자산 목록을 작성하고, 각 자산에 대한 관리자를 명시한다.

② 부서별 정보보안담당자는 부서 내 정보시스템 자산을 별도의 목록으로 관리한다.

③ 정보시스템 자산은 정보, 하드웨어, 소프트웨어, 문서, 기타 자산으로 구분되며, 각 자산에 대한 보관장소, 소유자, 관리자 및 비밀성, 무결성, 가용성에 따른 등급을 자산목록에 명기한다.

④ 정보보호 담당부서는 대학 자산에 대한 위험분석을 주기적으로 실시하여, 보호대책을 마련한다.

[참조문서] 자산 관리지침

제14조(의사소통 및 운영 관리) ① 운영 절차 및 책임

1. 정보보안담당자는 정보시스템 및 보안 시스템에 대한 운영 절차를 문서화하여 관리한다.
2. 정보시스템 기기, 응용 소프트웨어, 운영 프로그램의 변경 통제에 대한 절차를 정하고 수행한다.
3. 정보시스템의 오류, 서비스의 중단, 서비스 거부, 비밀성 침해 등이 발생할 경우 사고 처리를 위한 절차를 정하여 수행한다.

② 직무 분리

1. 정보자산과 서비스에 대한 비인가된 변조 또는 남용의 발생 가능성을 줄이기 위하여 시스템

운영과 정보보호 활동 직무는 직무분리 또는 보완통제 방안을 마련한다.

2. 시스템에 대한 사용자의 접근권한은 정기적 또는 비정기적으로 검토되어야 한다.(개정 2024.5.3.)

[참조문서] 인적 보안지침

③ 개발과 운영 환경의 분리

1. 개발 또는 운영 환경에 있어 개발 및 운영 시설은 분리되어야 한다.
2. 프로그램 개발 및 테스트 행위는 운용시스템과 분리되어 이루어져야 하며, 운용시스템 이관 전 충분한 테스트 및 관리자의 승인을 득하여 적용하여야 한다.

[참조문서] 서버 보안지침, 시스템개발 보안지침, 정보보호시스템 보안지침

④ 시스템 계획

1. 정보보호 담당부서는 시스템의 저장능력, 처리 속도 및 사용 용량에 대해 주기적으로 모니터링을 실시하고 필요 용량 계획을 수립할 수 있도록 관리한다.

⑤ 네트워크 모니터링

1. 정보보호 담당부서는 네트워크 트래픽을 모니터링하고, 이상 징후 발견 시 신속하게 대응하여야 한다.

⑥ 시스템 유지관리

1. 정보에 대한 백업

   시스템 관리자 및 백업 담당자는 중요한 정보와 소프트웨어에 대한 백업 계획을 수립하여 백업 및 복구테스트를 주기적으로 수행한다.

[참조문서] 서버 보안지침, 정보시스템 재해복구지침

2. 운영 로그

   시스템 관리자 및 정보보호 담당부서는 시스템 운영로그를 보관·관리하며 이를 주기적으로 분석한다.

3. 오류에 대한 로깅

   시스템 관리자 및 정보보호 담당부서는 시스템의 오류에 대한 로깅을 실시하고, 관리하며 이를 주기적으로 분석한다.

[참조문서] 서버 보안지침, 네트워크 보안지침, 정보보호시스템 보안지침

⑦ 네트워크 관리

1. 네트워크상의 정보와 기반 구조를 보호하기 위하여 컴퓨터 네트워크 접근은 통제되어야 하며, 내·외부 네트워크는 보안시스템으로 분리한다.
2. 또한 데이터베이스 서버와 웹 서버는 보안시스템으로 분리한다.

[참조문서] 서버 보안지침, 네트워크 보안지침, 정보보호시스템 보안지침

⑧ 저장 매체 폐기

1. 저장 매체를 폐기할 경우 저장내용을 식별할 수 없도록 소각, 완전파쇄 등의 방법을 사용하여 폐기한다.

2. 컴퓨터 시스템을 폐기할 때는 그 시스템의 기억 장치 내의 모든 자료를 삭제하고, 하드디스크는 파괴하거나 포맷한다. 또한 민감하거나 중요한 정보가 있는 보고서의 폐기는 반드시 파쇄기를 이용해 파쇄되어야 한다.

[참조문서] 물리적 보안지침, 서버 보안지침, 정보보호시스템 보안지침

⑨ 정보 취급 및 보안

1. 정보자산에 대한 비 인가된 접근, 폭로 및 오용을 방지하기 위해 정보자산 등급별 처리 지침을 수립하여 준수한다.

[참조문서] 인적 보안지침, 물리적 보안지침

⑩ 시스템 관련 문서의 보안

1. 시스템 담당자는 시스템 운영 문서를 비 인가된 접근으로부터 보호하기 위하여 물리적으로 안전한 장소에 보관하여야 하며, 전자적 형태의 파일의 경우 접근통제를 실시하여 인가된 사람만이 접근할 수 있도록 조치하여야 한다.

⑪ 인터넷 보안

1. 전자거래시스템 등과 같이 인터넷 기반의 서비스를 이용할 경우 정보의 변조, 공개, 계약부인과 같은 위협으로부터 보호 받을 수 있는 통제대책을 적용하여야 한다.

⑫ 전자 우편 보안

1. 이용자는 민감하거나 중요도가 높은 정보는 인터넷을 통한 전자우편의 형태로 전달 시 보안대책(파일 암호화 등)을 강구해야 한다. 파일을 첨부하거나 첨부된 파일을 받기 전에 항상 바이러스 감염 여부를 검사해야 한다.(개정 2024.5.3.)

[참조문서] 접근 통제지침, 서버 보안지침

⑬ 일반에게 공개된 시스템

1. 일반인에게 공개되는 전자적인 정보에 대한 무결성 확보 방안이 적용되어야 한다.
2. 일반인에게 공개되는 전자적 형태의 정보(대학 홈페이지 등에 수록된 정보)는 관련 법규에 준하여 보호하여야 한다.
3. 대학 홈페이지 등 공개서버에 중요정보를 게시하는 경우 해당 부서장의 승인을 득한 후 공개하여야 한다.(개정 2024.5.3.)
4. 민감한 정보의 경우 정보 수집 시 또는 저장 시에도 보호되어야 한다.

[참조문서] 서버 보안지침

제15조(접근통제) ① 접근통제 지침

1. 대학 정보자산의 비인가적인 침해를 방지하기 위하여 정보자산 등급에 따른 접근통제 지침이 수립되어 시행되어야 한다.
2. 모든 정보시스템은 반드시 사용자 인증과정을 거쳐야 접근이 가능하도록 하여야 한다.

② 네트워크 분리

1. 업무특성 또는 보안요구 사항에 따라 필요한 경우 네트워크는 분리되어 운영되어야 한다. 웹 서버와 데이터베이스 서버는 분리되어야 한다.

③ 운영체제 접근 제어

1. 정보보호 측면에서 필요할 경우 자동 단말기 식별기능(IP Address에 의한 통제 등)을 적용하여 특정 위치에서의 연결만을 허용하며, 원격 접속 시, 루트 권한으로 접근할 수 없다. 단 암호화 통신을 통한 루트권한의 접근은 허용한다.
2. 관리자 계정의 패스워드는 숫자와 문자, 특수문자 등을 혼합하여 9자리 이상으로 작성한다.(개정 2019.02.25.)

④ 이동 컴퓨팅(Mobile Computing)

1. 노트북 PC 등과 같은 휴대용 컴퓨터의 원외 사용시 사용자는 절도와 같은 물리적 위협 및 비인가된 논리적 접근으로부터 기기를 보호할 수 있도록 조치를 취하여야 한다.

[참조문서] 암호 통제지침, 접근 통제지침, 서버 보안지침

제16조(물리적 보안) ① 통제구역

1. 중요 정보가 보관되거나 처리되는 지역은 사전에 통제구역으로 설정되어야 하며, 관리책임자를 정하여 이를 관리하여야 한다.
2. 통제구역은 비인가된 접근이나 손상을 방지하기 위하여 별도의 출입통제 장치 및 감시시설 고정형 영상정보처리기기(CCTV) 등을 갖추어야 한다.(개정 2024.5.3.)

② 보호구역의 출입통제 관리

1. 보호구역은 출입자격자와 비자격자를 구분하여 보호구역별 출입자격자 명단을 관리하여야 한다.
2. 보호구역을 관리하는 책임자는 보호구역 출입자격자 명단에 대한 적합성 여부를 주기적으로 점검하여야 한다.
3. 보호구역 내에서 일하거나 보호구역에 접근하는 대학 구성원은 항상 그 구역 내에서 요구되는 절차에 따라야 한다.(개정 2024.5.3.)
4. 권한없는 자의 보호구역 출입이 필요할 경우 출입은 반드시 담당자와 동행하여 권한없는 자의 작업을 종료 시까지 관리감독하며, 장비가 반·출입될 경우 '보호구역 장비 반·출입 신청서'에 반·출입물품을 명시하여야 한다.(개정 2024.5.3.)

[참조문서] 물리적 보안지침

제17조(환경적 보안) ① 정보시스템 기기 보안 관리

1. 정보시스템 기기들은 적절히 보호된 상태로 설치되어야 하고, 비인가된 접근과 환경적 위해요소로부터 보호될 수 있는 곳에 위치하여야 한다.

② 장비의 처분과 재사용 과정에서의 보안

1. 장비를 폐기하거나 재사용하려 할 때는 모든 정보를 정보시스템으로부터 적절한 방법으로 삭제해야 한다. 특히 민감한 정보를 담고 있는 저장 매체를 폐기 또는 재사용 시 수록된 정보를 삭제 또는 덮어쓰기 등의 방법을 사용하여 정보 유출을 예방하여야 한다.

[참조문서] 물리적 보안지침, 서버 보안지침

③ 책상 정리 및 화면 보호 지침

1. 퇴근 시나 장기 출타 시 민감한 즉 대학의 대외비나 기밀 사항을 담고 있는 문서는 책상 위 등에 방치되어서는 안 되며, 시건장치가 부착된 문서 보관함에 보관되어야 한다.
2. 퇴근 시나 장기 출타 시 문서가 책상 위에 남겨져 있어서는 안 된다.
3. 패스워드가 설정된 화면보호기를 사용하여 10분 이상 시스템을 사용하지 않는 경우 자동으로 화면이 잠기도록 하여야 한다. 시스템 사용을 재개할 때는 다시 패스워드를 입력하고 사용하도록 해야 한다.

제18조(개인정보보호) 대학의 개인정보보호 업무는「개인정보보호법 및 동법 시행령」,「개인정보 안전성확보조치 기준」등에서 규정하는 준수사항, 정보주체의 권익보장 및 개인정보의 안전한 처리를 위한 규정을 수립하고 이행하여야 한다.

① 개인정보처리방침 수립 및 공개

1. 개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개), 같은 법 시행령 제31조(개인정보 처리방침의 내용 및 공개방법 등)를 준수한다.
2. 개인정보보호 법·령 및 기준의 준수를 위해 우리대학은 “개인정보처리방침”을 수립하고 시행한다.
3. “개인정보처리방침”은 개인정보보호 관령 법·령의 준수 및 정보주체의 권익을 보장하고 안전한 개인정보처리를 위한 규정을 정의하고 공개한다.

[참조문서] 개인정보처리방침

② 개인정보 내부관리계획 수립 및 시행

1. 개인정보보호법 제29조(안전조치 의무), 같은 법 시행령 제30조(개인정보의 안전성 확보조치)를 준수한다.
2. 개인정보보호 법·령 및 기준의 준수를 위해 우리대학은 “개인정보 내부관리계획”을 수립하고 시행한다.
3. “개인정보 내부관리계획”은 대학이 정보주체의 권익을 보장하고, 안전한 개인정보처리를 위한 관리적·기술적·물리적 개인정보보호 활동을 정의하고 시행한다.
4. “개인정보 내부관리계획”은 개인정보보호 관련 법·령 및 환경의 변화에 따라 주기적 검토 및 승인되어야 한다.

[참조문서] 개인정보 내부관리계획

제19조(예외적용) 다음 각 호에 해당하는 경우에는 본 규정에서 명시한 내용일지라도 정보보안 담당관의 승인을 받아 예외 취급한다.

① 기술환경의 변화로 적용이 불가능할 경우

② 관리적, 기술적인 이유로 지침의 적용을 보류할 긴급한 사유가 있을 경우

③ 기타 재해 등 불가항력적인 상황일 경우

부 칙

① (시행일) 이 규정은 2018년 8월 27일부터 시행한다.

② (다른 규정의 폐지) 이 규정의 시행과 동시에 정보보안규정, 정보보호규정, 개인정보보호규정은 폐지한다.

부 칙

이 규정은 2019년 2월 25일부터 시행한다.

부 칙

이 규정은 2024년 5월 3일부터 시행한다.(제1조, 제2조, 제3조제9호, 제4조, 제4조제1항·제3항·제6항, 제7조제1항, 제8조제1항제4호·제5호·제7호·제9호, 제9조제1항제3호, 제10조제1항제2호, 제10조제2항제3호·제4호, 제11조제1항제4호, 제12조제1항·제3항·제4항·제7항·제8항, 제14조제2항제2호, 제14조제12항제1호, 제14조제13항제3호, 제16조제1항제2호, 제16조제2항제3호·제4호)