| 안산대학교 | 보안업무규정 | 규정번호 | 3-1-12 |
|---|---|---|---|
| | | 제정일자 | 2017.03.01. |
| | | 개정일자 | 2024.09.01. |
| | | 개정차수 | 3차 |
| | | 소관부서 | 행정지원처 |

## 제1장 총 칙

제1조(목적) 이 규정은 대통령령 제26140호 보안업무규정(이하“보안업무규정”이라 한다) 제39조 내지 제41조와 보안업무규정시행규칙 제67조, 교육부 보안업무규정시행세칙(이하 “보안업무규정시행세칙”이라 한다) 제2조에 따라 안산대학교(이하 “대학”라 한다)의 보안업무에 필요한 사항을 정함을 목적으로 한다.

제2조(적용범위) 이 규정은 대학의 행정부처와 각 학과, 부속기관, 부설기관 및 산하기관(이하 “당해 기관”이라 한다)에 적용한다.

제3조(보안관리자) ① 대학의 보안담당관은 행정지원처장으로 한다.

② 보안담당관의 효율적인 업무수행을 위하여 다음 각 호와 같이 분임보안담당자를 둔다.

1. 인원보안 분임 담당자 : 교원 및 조교는 교무인사팀장, 직원은 총무인사팀장
2. 문서보안 분임 담당자 : 총무인사팀장
3. 시설보안 분임 담당자 : 시설안전팀장
4. 정보보안 분임 담당자 : 전산정보팀장
5. 행정부처 및 각 학과의 보안 분임 담당자는 다음 각 목과 같다.
   가. 각 행정부처에서 지정한 1인
   나. 교수 연구실은 해당교원, 실험·실습실은 해당 학과장, 학과사무실은 학과조교
   다. 부속기관, 부설기관 및 산하기관(이하 “당해기관”이라 한다)은 당해기관 책임자

제4조(보안담당관의 임무) 보안담당관의 임무는 다음 각 호와 같다.

1. 자체 보안업무 수행에 필요한 계획조정 및 감독
2. 보안교육
3. 비밀소유현황조사
4. 규정 및 지침의 입안 서약의 집행
5. 정보보안과 관련된 업무 등
6. 보안진단 및 보안업무 심사분석에 관한 사항
7. 보안감사 및 보안점검
8. 분임보안담당자의 지휘 및 감독에 관한 사항
9. 기타 보안업무 전반에 관한 지도, 조정 및 감독에 관한 사항

## 제2장 보안심사위원회

제5조(보안심사위원회) ① 대학은 보안업무의 효율적인 운영과 업무계획의 수립 및 기타 보안에 관한 중요한 사항을 심의·결정하기 위하여 보안심사위원회(이하 “위원회”라 한다)를 둔다.

② 위원회는 다음 각 호의 사항을 심의·결정한다.

1. 이 규정의 개·폐에 관한 사항
2. 분야별 보안대책의 수립에 관한 사항
3. 신원특이자의 임용 등 인사관리 중 보안에 관한 사항

4. 보안사고, 보안위반자의 심사 및 처리에 관한 사항
5. 연간 보안업무에 대한 지침과 그 이행상태의 확인처리에 관한 사항
6. 기타 총장의 지시나 위원장(보안담당관)이 필요하다고 인정하는 사항

제6조(구성) 위원회의 구성은 다음 각 호와 같으며, 당연직으로 한다.

1. 위원장 : 행정지원처장
2. 부위원장 : 전산정보원장
3. 위　원 : 교무처장, 입학홍보협력처장, 학생성공처장, 산학협력처장, 전략기획처장
4. 간　사 : 해당업무 담당자
5. 서　기 : 간사 중 1인을 위원장이 정하는 자

제7조(회의) 위원회의 회의는 위원장이 필요하다고 인정할 때 또는 관련 부서장의 요구가 있을 때 소집한다. 다만, 위원회의 소집이 곤란하거나 긴급을 요하는 경우에는 서면결의로서 회의 소집에 갈음할 수 있다.

제8조(위원장 및 직무대행) ① 위원장은 보안업무에 관한 책임자로서 위원회의 업무를 관장하고 회의를 소집하며 그 의장이 된다.

② 위원장이 유고시에는 부위원장 또는 위원장이 지정하는 위원이 그 직무를 대행한다.

제9조(의사정족수) ① 위원회의 의사는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

② 가부동수인 경우에는 부결된 것으로 본다.

③ 위원회의 결의사항은 총장의 재가로서 효력을 발생한다.

## 제3장 인원보안

제10조(신원조사) ① 신원조사는 인원보안 분임 담당자가 실시하여야 하며, 그 결과 회보사항을 신중히 고려하여 임용하여야 한다.

제11조(신원조사의 대상) 신원조사는 다음 각 호에 해당하는 사람 중 국가안전보장에 한정된 국가 기밀을 취급하는 직위에 임용될 예정인 사람으로 한다.

1. 교직원 임용예정자(다만, 비정규 직원의 경우 특별한 경우를 제외하고는 생략한다)
2. 비밀취급 인가 예정자
3. 장비 및 자재 등의 관리자나 기밀 보안상 필요하다고 인정하는 자
4. 기타 법령이 정하는 자

제12조(신원조사의 요청) 신원조사의 요청은 특별한 사유가 없는 한 인원보안 분임 담당자가 담당함을 원칙으로 한다.

제13조(교직원의 보안교육) 보안담당관은 교원, 조교 및 직원의 임용과 동시에 보안의 중요성에 대하여 충분한 교육을 실시하여야 한다.

## 제4장 문서보안

### 제1절 비밀의 취급

제14조(비밀의 취급) 비밀을 취급하는 자는 비밀의 안전관리를 위하여 본 규정이 정하는 바에 따른 보안조치를 취하여야 한다.

제15조(비밀취급의 인가) ① 비밀취급인가에 관한 모든 사항은 보안업무규정시행세칙에서 정한 바를 준용한다.

② 대학의 비밀취급인가에 관한 사무는 행정지원처에서 주관하고, 비밀취급인가권자는 총장이 하며, 비밀취급인가의 등급별 부여대상은 다음과 같다.

1. II급 비밀취급인가대상 : 총장, 보안담당관 및 총장이 필요하다고 인정하는 자

제16조(서약의 집행) 보안담당관은 비밀취급인가자의 발령 후 3일 이내에 비밀취급인 가자를 일정한 장소에 소집하여 [별지 제1호 서식]에 의한 서약을 집행하고 비밀취급업무에 필요한 기초교육을 실시한다.

제17조(비밀취급 인가해제) ① 비밀취급인가를 받은 자가 전보하거나 퇴직하였을 경우에는 당연 해제된 것으로 보며, 별도 서면 해제발령을 하지 않는다.

② 비밀취급인가가 해제된 자에 대하여는 비밀취급인가 대장에 해제사유 및 일시를 기록하고 주서로 삭제하여야 하며, 인사기록카드에도 해제사항을 기록하여야 한다.

## 제2절 비밀의 분류 및 재분류

제18조(비밀의 분류 및 재분류) 비밀의 분류 및 재분류는 보안업무규정, 보안업무규정 시행규칙 보안업무규정시행세칙 내용에서 정하는 바에 의한다.

## 제3절 비밀의 수발(접수·발송)

제19조(비밀의 수발) ① 비밀의 수발은 문서보안 분임 담당자를 경유하여 취급자의 직접 접촉에 의하여 수발함을 원칙으로 한다.

② 취급자의 직접 접촉이 불가능한 경우에는 보안업무시행규칙 [별지 제2호 서식]의 이중봉투로 된 등기우편으로 수발하여야 한다.

③ 타 기관으로부터 접수된 비밀은 즉시 보안담당관에게 인계하고 즉시 비밀관리기록부에 등재 하여야 한다.

제20조(비밀 수발담당자의 지정) 대학의 비밀문서 수발을 위하여 문서보안 분임 담당자가 수발을 담당하여야 한다.

제21조(오착비밀의 반송절차) ① 다른 기관으로부터 접수한 비밀은 그 발행기관의 승인 없이는 이를 다른 기관으로 발송할 수 없다.

② 잘못 전달된 비밀(오착비밀)은 문서보안 분임 담당자를 통하여 발행기관에 반송하여야 하며 스스로 발행(타)기관에 발송하여서는 안 된다.

제22조(비밀접수증) ① 모든 비밀을 접수하거나 발송할 때에는 그 사실을 확인하기 위하여 비밀 접수증을 사용하며, 보안업무 시행규칙에 따라 작성하고 보안담당관이 보관·관리하여야 한다.

② 비밀접수증 관리방법은 다음 각 호와 같다.

1. 비밀접수증 철과 비밀문서 수발대장은 일반문서 대장과 구분하여 5년간 보관하여야 하며 비밀을 등기우편으로 발송할 때의 등기우편물 영수증에 대해서도 같다.
2. 비밀접수증은 직접 접촉에 의하여 교부되는 때를 제외하고는 발송비밀의 내부봉투와 외부 봉투 사이에 삽입하여 접수증만을 절취하여 즉시 발송기관에 발송하여야 한다.

## 제4절 비밀의 보관 및 관리

제23조(비밀보관) ① 대학의 비밀문서의 보관은 보안담당관이 관리함을 원칙으로 한다.

② 비밀보관용기는 철제 2중 캐비닛을 원칙으로 하며, 반드시 2중 시건 장치를 하여야 한다.

③ 비밀의 보관은 외부에 알리거나 나타내는 어떠한 표시도 하여서는 아니 되며, 다음과 같이 보관책임자 표시를 하여야 한다.

| | 보관책임자 |
|---|---|
| 정 | |
| 부 | |

제24조(비밀보관 책임자) ① 보안담당관은 비밀의 보관단위 부서 또는 보관단위 사무실 별로 정 · 부 2명의 보관책임자를 두어야 하며, 정 보관책임자는 보안담당관, 부 보관책임자는 총장이 지정한 비밀취급인가자로 한다.

② 정 보관책임자는 부 보관책임자를 지휘 · 감독하며 다음 각 호의 임무를 수행한다.

1. 비밀의 도난, 누설, 분산 및 기타 손괴 등의 방지를 하여야 하며 비밀의 최선 관리에 노력하여야 한다.
2. 비밀관리 기록부, 비밀열람 기록부, 대출부, 영수증철 등의 기록 유지와 확인을 하여야 한다.

③ 부 보관책임자는 정 보관책임자의 지휘를 받아 비밀의 선량한 관리에 노력하여야 하며 정 보관책임자 부재시 그 직무를 대행한다.

제25조(비밀의 인계인수) 비밀의 인계인수는 비밀관리기록부의 최종기입란 밑에 적색 2개의 주선으로 마감하고 다음과 같이 인계인수 내용을 기재한다.

비밀인계인수

(  )급 비밀 (  ) 건

(  )급 비밀 (  ) 건

계 (  ) 건

위와 같이 정히 인계·인수함

년 월 일

인계자 직 성명 (인)

인수자 직 성명 (인)

확인자 보안담당관 성명 (인)

제26조(비밀관리 기록부) 보안담당관은 비밀의 전반적인 관리사항을 기록하기 위하여 비밀관리 기록부를 작성, 비치하여 5년간 보존하여야 한다.

제27조(비밀 관리번호 부여방법) ① 비밀 관리번호는 일련번호를 부여한다.

② 비밀관리번호는 동일문서 또는 책자라 하더라도 반드시 별개의 관리번호를 부여하여야 한다. 다만, 자체에서 작성한 비밀은 원본과 보관용에만 번호를 부여하고 배부처로 발송되는

비밀은 번호를 부여하지 않는다.

③ 자체 내에서 작성한 비밀은 최고 결재권자(총장)가 결재하여 그 내용이 확정된 후에 관리번호를 부여한다.

④ 관리번호의 표시는 보안업무시행규칙 제40조제3항에 의한 규격으로 표시하여야 한다.

제28조(비밀관리 기록부 갱신방법) ① 비밀관리기록부의 갱신은 보안담당관의 사전승인을 얻어야 하며, 갱신내용을 기재한 후 보안담당관의 검열을 받아야 한다.

② 구대장의 이기 방법은 다음과 같다.

신대장으로 이기하였음.

급비밀 건

급비밀 건

계 건

년 월 일

이기자 직 성명 (인)

확인자 담 당 자 성명 (인)

검열자 담 당 관 성명 (인)

③ 신대장의 이기 방법은 다음과 같다.

구대장에서 이기하였음.

급비밀 건

급비밀 건

계 건

년 월 일

이기자 직 성명 (인)

확인자 담 당 자 성명 (인)

검열자 담 당 관 성명 (인)

제29조(비밀의 복제, 복사 및 발간 통제) ① 비밀을 발간 또는 복제, 복사하고자 할 때에는 반

드시 보안담당관의 사전 통제를 받아야 한다.

② 비밀을 외부업체에 의뢰하여 발간하고자 할 때에는 보안담당관의 승인을 받아야 한다.

③ 제 2항의 승인은 [별지 제3호 서식]에 의한 “비밀(대외비)문서발간승인신청서”에 의한다.

④ 제 2항의 규정에 의한 승인을 받지 않은 비밀은 복제, 복사 또는 발간할 수 없다.

⑤ 비밀을 발간 또는 복제, 복사하여 관계기관에 배부하고자 할 때에는 사본번호를 포함한 배부처를 작성비밀원본(기안문)에 첨부하여 결재를 받아 시행하여야 한다.

⑥ 비밀을 생산할 때에는 반드시 비밀취급 인가자가 작성하여야 한다.

⑦ 비밀 발간에 있어서 보관용 비밀은 3부를 초과할 수 없다.

제30조(비밀 발간의 보안조치) ① 비밀의 발간은 자체시설을 이용함을 원칙으로 한다.

② 비밀문서의 발간 또는 복제, 복사하는 자는 보안담당관의 입회하에 하여야 한다.

제31조(비밀의 열람 및 결재) ① 개개의 비밀에는 그 비밀문건 말미에 비밀열람기록전을 반드시 첨부하여야 한다.

② 비밀열람기록전은 비밀을 파기할 때 그 비밀과 분리하여 별도로 5년간 보관하여야 한다.

③ 업무상 비밀을 열람할 때에는 열람에 앞서 비밀열람기록전에 관계사항을 기재하고 날인한 후 열람하여야 하며, 결재할 때에도 또한 같다.

제32조(비밀의 지출) ① 비밀의 지출을 원할 때에는 보안담당관의 승인을 얻어 문서보안 분임담당자의 입회하에 비밀을 지출하여야 한다.

② 비밀 지출자는 지출 후의 보안대책 및 사후 회수 등에 관하여 특별한 보안조치를 취하여야 한다.

③ 비밀을 지출 휴대하고 다닐 때에는 반드시 포장하거나 밀봉한 봉투에 의하여야 한다.

제33조(비밀의 파기) ① 비밀의 파기는 소각, 용해 또는 기타방법으로 원형을 완전히 소멸시켜야 한다.

② 비밀의 파기는 보안담당관 또는 보안담당관이 지정한 입회자의 참여 아래 처리담당자가 파기 하여야 한다.

③ 파기가 끝나면 즉시 비밀관리기록부의 파기란에 일시를 기입한 후 날인하고, 파기 확인란에는입회자의 확인을 받아야 한다.

제34조(안전지출 파기계획) ① 보안업무규정 제28조 및 보안업무시행규칙 제49조에 따라 비상시 비밀보안을 철저히 유지 관리하기 위한 비밀 및 중요문서 안전지출 및 파기계획을 수립하여야 한다.

② 전항의 계획은 평상시 보다 공휴일 또는 일과후 등 평상시의 지휘계통이 없을 때 발생될 비상사태에 대비하기 위한 계획이어야 하며, 실천 가능성 여부를 검토하여 작성하여야 한다.

제35조(비밀소유현황 조사보고) 보안담당관은 매년 6월말과 12월말을 기준하여 조사한 비밀소유 현황과 비밀취급인가자 현황을 익월 10일까지 교육부장관에게 보고하여야 한다.

## 제5장 시설보안

제36조(시설보안의 담당) 시설보안에 관한 일체의 사무는 행정지원처에서 담당한다. 다만, 부설 및 부속기관은 해당 기관장이 담당한다.

제37조(보호구역의 지정) 대학의 보호구역은 제한지역, 제한구역 및 통제구역으로 하며, [별지 제4호 서식]에 의한 “보호구역 대장”을 비치하여 기록 유지하고, 보호구역 추가지정 또는 해제시에도 보호구역 대장에 기록 유지한다.

1. 제한지역 : 교내 전 구역
2. 제한구역 : 이사장실, 총장실, MDF실, 기계실(본관·진리관·예지관), 전기실(진리관, 성실

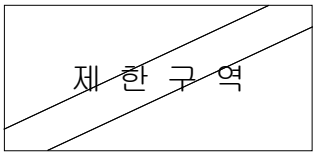
관, 도서관, 채플관, 창업지원단, 기숙사)

3. 통제구역 : 전산정보팀 장비실

제38조(보호구역의 관리) ① 제한구역 및 통제구역에는 관계직원 및 출입이 인가된 자 외에는 출입을 통제하여야 하며, [별지 제5호 서식]에 의한 “출입통제 대장”을 비치하여 기록 유지하여야 한다.

② 제한구역 또는 통제구역에는 그 출입문 중앙부 또는 잘 보이는 곳에 주서로 다음 예시와 같이 표시하여야 한다. 다만, 이사장실 및 총장실은 표시하지 아니할 수 있다.

(예시)




(15Cm ╳ 30Cm)


(15Cm ╳ 30Cm)

③ 제한구역 및 통제구역의 출입문에는 제2항의 표시 외에도 다음 예시의 표시를 할 수 있다.

(예시)

[제한구역]

| 관계직원외 출입을 금함 |
|---|

(10Cm ╳ 30Cm)

[통제구역]

| 비인가자는 출입을 금함 |
|---|

(10Cm ╳ 30Cm)

④ 보호구역에는 적당한 곳에 다음의 예시와 같은 관리책임자의 표지를 부착하여야 한다.

| 구 분 | ○○구역 관리책임자 |
|---|---|
| 정 | |
| 부 | |

(3Cm ╳ 9Cm)

제39조(보호구역의 관리책임) ① 이 규정 제37조에 의한 보호구역의 관리책임자를 다음 각 호와 같이 지정한다.

1. 제한지역 : 보안담당관
2. 제한구역
   가. 이사장실 및 총장실 : 동 시설의 관리를 담당하는 행정사무 담당자
   나. MDF실, 기계실(본관·진리관·예지관), 전기실(진리관, 성실관, 도서관, 채플관, 창업지원단, 기숙사) : 동 시설의 관리를 담당하는 1인
3. 통제구역 : 전산장비실은 동 시설의 관리를 담당하는 1인

② 보호구역의 관리책임자는 매월 1회이상 자체점검을 실시하여 관리상의 문제점 및 취약요소를 파악하고, 이상 발견시 이에 대한 대책을 수립하여 보호구역의 관리에 만전을 기하여야

한다.

제40조(시설방호) ① 대학 시설방호책임자는 총장이 되고 시설에 대한 제반관리는 행정지원처장이 책임을 지고 자체시설의 안전한 관리에 노력하여야 한다.

② 총장은 제1항의 규정에 의하여 자체시설방호에 대한 기본계획을 수립하여야 한다.

③ 시설방호계획에는 외래인 출입통제방안(주간 및 야간, 공휴일)과 당직근무제도(주야 경계 및 순찰 등) 등을 포함하여야 한다.

④ 공휴일 또는 일과후 등에 발생되는 비상사태에 대비하기 위한 비상연락망을 부서별 또는 지역별로 작성하여 당직실에 비치하며, 비상조치반으로서 각 건물에 배치된 방호원을 활용한다.

제41조(소방관리) 소방안전관리자는 방화 또는 소방작업의 신속하고도 효과적인 실시를 위하여 기준에 의한 소화시설을 완비하고 수시 점검을 실시하고, 연 2회 소방작동기능점검 및 소방시설 종합정밀점검을 실시함은 물론 연 1회 소방관서와 합동으로 소방훈련을 실시하여야 한다.

## 제6장 전산보안

제42조(준용규정) 이 규정에서 정하는 전산보안에 관한 세부사항은 전산보안기본지침에 따른다.

제43조(사이버보안진단의 날 실시) ① 보안담당관은 '사이버·보안 진단의 날'을 실시하여 자체 점검을 통한 보안진단을 실시하여야 한다.

② 사이버보안진단의 날은 매월 세 번째 수요일에 실시하여야 하며(다만, 진단의 날이 공휴일인경우나 불가능할 때에는 익일에 실시한다.)그 내용을 기록·유지하여야 한다.

제44조(전산보안기본지침) ① 보안담당관은 보안 업무수행을 위하여 이 규정 및 상위 규정에 반하지아니하는 범위내에서 자체적으로 전산보안기본지침(이하 "기본지침"이라 한다.)을 정할 수 있다.

② 보안담당관은 대학의 정보통신서비스의 안정성과 정보의 신뢰성을 확보하는데 필요한 정보보호조치를 내용으로 하는 기본지침을 수립 시행하여야 한다.

③ 보안담당관은 제2항의 기본지침을 최신의 내용으로 유지하여야 한다.

제45조(침해사고 대응관리) ① 보안담당관은 긴급한 침해사고가 발생하였을 때에는 모든 이용자에게 대응책을 신속하게 알릴 수 있는 체계를 마련하여야 한다.

② 보안담당관은 불법행위나 이상 징후가 탐지되었을 때에는 수립된 대응·복구계획에 따라 즉각적인대응조치를 취하고, 침해사고와 관련한 접속기록 등 적절한 증거자료를 수집·보관하여야 한다.

제46조(학사정보자료의 안정적 보관) ① 학사정보 등 주요 전산정보자료를 백업 후 내화금고 등에보관하여야 하며 별도의 물리적 공간에 자료를 관리하여야 한다.

제47조(전산실 운영관리) 보안담당관은 다음 각 호와 같이 전산실을 운영·관리하여야 한다.

1. 전산실에 위치한 장비에 대한 도난, 파손, 변경, 불법적인 사용 등의 방지 대책수립
2. 정전 등으로 인해 중요 데이터의 손상 및 손실을 방지하기 위하여 데이터 백업 등 필요한 대책수립
3. 전산실의 출입 통제장치 설치를 통한 출입자의 통제

제48조(정보보호시스템 등의 운영관리) 보안담당관은 다음 각 호와 같이 정보통신 서비스의 안정성과 정보의 신뢰성 확보를 위한 관리적·기술적·물리적 수단을 갖추고 이를 운영, 관리하여야 한다.

1. 침입차단시스템 등의 정보보호시스템을 설치하여 운영하거나 이에 상응하는 정보보호조치수립

2. 프로그램의 보안취약점을 발견한 때에는 필요한 대책을 수립

3. 주요 정보시스템 및 서비스와 같은 정보자산에 대한 백업 및 복구 절차를 수립

제49조(이용자 제한조치 및 고지) ① 보안담당관은 다음 각 호에 해당하는 행위를 한 이용자에 대하여 계정정지, 접속제한 등 정보통신서비스를 제한할 수 있다.

1. 부당한 방법으로 정보통신망에 의하여 처리·보관·전송되는 타인의 정보를 훼손하거나타인의 비밀을 침해·도용 또는 누설하는 행위

2. 트로이목마, 컴퓨터바이러스 등 악성 프로그램의 유포행위

3. 음란·폭력물 등의 불건전한 자료의 게재·유포행위

4. 정보시스템에 장애를 유발시킬 목적으로 다량의 데이터 또는 트래픽을 유발·전송하는 행위

5. 수신자의 명시적인 수신거부 의사에 반하는 광고성 전자우편·SMS를 전송하는 행위

6. 기타 정보보호에 해가 되는 행위

② 보안담당관은 제1항에 의한 제한을 하고자 하는 경우에는 사전에 이를 이용자에게 고지하거나학내 정보망에 게시할 수 있다.

③ 보안담당관은 제1항에 해당하는 행위가 발생하였을 때에는 그 사실을 이용자에게 고지하여야 한다. 다만, 이용자에게 경미한 영향을 미치거나, 신속히 처리해야 하는 등의 긴급한 상황일 경우에는 고지하지 아니할 수 있다.

제50조(이용자 제재) ① 사용자의 계정을 정지·삭제 하여 정보시스템 및 네트워크 사용을 제한 또는 금지하며, 그에 따른 구체적 제재사항은 위원회에서 심의·의결한다.

② 정보시스템의 불법사용으로 대학에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호와 같이 제재 조치를 취할 수 있다.

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법 등 관련 법령에 의한법적 조치

2. 정보시스템의 손해발생에 대한 손해배상 청구

③ 정보보안 점검활동 및 보안조치 불이행시 당해기관 또는 구성원에 대해 다음과 같이 재제조치를 취할 수 있으며, 완료될 때 까지 유지 할 수 있다.

1. 1차 : 서면통보

2. 2차 : 네트워크 사용량 제한

3. 3차 : 네트워크 사용 통제

제51조(계정관리) ① 보안담당관은 이용자의 중요정보 및 패스워드 누출 방지를 위한 보호조치를하여야 한다.

② 이용자는 자신의 계정 및 패스워드가 외부로 노출되지 않도록 유의하고 패스워드는 주기적으로 변경하여야 하며, 안전한 패스워드를 사용하여야 한다.

③ 주요 정보시스템 및 서비스 대상의 사용자 계정 정보를 관리, 발급, 변경, 삭제 등을 하기위한 처리절차를 수립하여야 한다.

④ 퇴직으로 신분변동 시 사용자의 모든 정보시스템 접근을 즉시 차단한다. 다만, 퇴직교직원의메일은 3개월까지 사용할 수 있으며 총장의 승인을 득한 경우 1개월의 추가 사용이 가능하다.

⑤ 업무담당자의 긴급한 신변상의 문제발생 시 새 업무담당자의 정보시스템에 대한 접근을 허용할 수 있다. 다만, 부서장의 요청과 총장의 승인을 득한 경우에 한하여 접근을 허용 할 수 있다.

⑥ 삭제 <2024.09.01.>

제52조(정보시스템 기본보안 사항) ① 이용자는 발송자를 확인할 수 없는 전자우편 또는 제공자가분실한 컴퓨터프로그램 등에 대해 안정성여부를 확인하고 실행하여야 한다.

② 이용자는 자신의 컴퓨터에 최신의 컴퓨터바이러스 방지프로그램을 설치하여 침투여부를 수시로 점검하고, 침투한 경우에는 이를 제거·복구하여야 한다.

③ 이용자는 자신의 컴퓨터의 운영체계와 응용프로그램에 대해 주기적인 업데이트를 실행하며필요한 보안조치를 반드시 적용하여야 한다.

④ 교내에 개인 또는 사설 등의 비인가 된 정보서비스, 네트워크 구성, 인터넷 서비스 등을 금지한다. 단 보안담당관의 승인 또는 연구목적의 구성은 가능하다.

제53조(정보화기기의 활용 및 폐기) ① 정보화기기라 함은 대학 내에서 사용되는 저장하드 및 메모리등 기타 정보가 저장되는 모든 매체를 통칭 한다.

② 정보화기기를 활용한 담당업무의 연속적 수행이 필요한 경우, 기존 담당자는 업무수행 자료를백업받고 업무수행 외적인 자료는 완전 포맷한 후 다음 담당자에게 인수인계 하여야 한다.

③ 보조기억매체 관리대장을 작성하여 관리하여야 하며 서식은 전산보안기본지침의 양식에 따른다.

④ 정보화기기의 폐기 시 부서장의 서명날인과 정보화기기에 본인의 서명 날인한 자료를 탈거하여 보안담당관에게 제출하여야 한다.

⑤ 보안담당관이 폐기승인한 정보화기기는 일정 공간 보관 후 물리적인 파기를 하여야 한다.

제54조(보안점검) 보안담당관은 정보보호를 위해 필요시 전산자원을 사용하는 정보시스템에 대하여보안점검을 수시로 실시 할 수 있다.

제55조(전산보안 실무담당자) ① 보안담당관은 대학의 정보보호를 효과적으로 운영하기 위하여 당해기관에 전산보안실무담당자(이하 “실무담당자”라 한다) 1인을 둔다.

② 실무담당자는 조교, 직원이어야 한다.

③ 실무담당자는 정보보안업무 관련 시행 사항에 대해 당해기관 구성원에게 업무내용을 전파하여야 한다.

④ 실무담당자는 사이버보안 진단의 날 시행 시 소속한 당해기관이 적극적으로 참여할 수 있도록협조 및 시행 결과를 보안담당관에게 보고하여야 한다.

⑤ 정보보안관련 특이사항 발생 즉시 보안담당관에게 보고하여야 한다.

## 제7장 보안조사 및 교육

제56조(보안사고) ① 보안사고의 범위는 비밀의 누설, 분실 및 비밀보관함의 파기와 보호구역 내 불법침입자에 의한 시설파기를 말한다.

② 보안사고가 발생하였을 때는 사고를 범하였거나 이를 인지한 자는 지체없이 자체 보고절차를 거쳐 보안심사위원회에 보고하여야 하며, 보안사고가 종결될 때까지 공개하여서는 안된다.

제57조(보안업무의 지도감독) ① 보안담당관은 교내 각 기관에 대하여 연 1회이상 지도 감사를 실시하여야 한다.

② 감사는 정기와 수시로 나누어 실시하되 정기지도감사는 연 1회, 수시지도감사는 보안담당관이 필요하다고 인정할 때 실시한다.

제58조(정기보안진단 실시) ① 행정부처 및 각 학과의 보안 분임 담당자는 매월 1회이상 자체 점검을 통한 보안진단을 실시하여야 한다.

② 정기보안진단은 매월 셋째주 수요일에 실시한다.

③ 진단결과 발견된 문제점에 대하여는 위원회에 부의하여 대책을 수립·이행할 수 있다.

제59조(보안교육) ① 보안담당관은 전 교직원에게 보안관리와 보안업무의 향상을 위하여 교육을실시하여야 한다.

② 보안 담당자는 매년 15시간 이상의 전문교육 이수를 통한 전문성 강화를 위해 노력하여야 한다.

③ 대학의 보안교육 강화를 위해 용역업체에 대해 연 1회이상 교육을 실시하여야 한다.

제60조(비밀관리부철의 보존) 다음 각 호의 자료는 비밀의 보호기간이 만료된 후 5년간 보존하여야 하며, 그 이전에 폐기하고자 할 때에는 총장의 승인을 받아야 한다.

1. 서약서철
2. 비밀접수증철
3. 비밀관리기록부
4. 비밀접수 및 발송대장
5. 비밀열람기록전(철)
6. 비밀대출부
7. 배부처(철)

## 제8장 보 칙

제61조(기타) 이 규정에 명시되지 않은 사항은 관련법령을 준용한다.

부 칙

① (시행일) 이 규정은 2017 년 3 월 1 일부터 시행한다.

② (경과조치) 이 규정 시행당시 종전의 정보보안에 대해서는 종전의 정보보안업무규정에 의하여 처리된 것으로 본다.

부 칙

이 규정은 2020 년 6 월 1 일부터 시행한다.

부 칙

이 규정은 2023 년 5 월 8 일부터 시행한다.

부 칙

이 규정은 2024 년 9 월 1 일부터 시행한다.