개인정보보호의 안전성 확보를 위한

내부관리 계획

2016. 03. 14.

강릉원주대학교 총무과

목 차

제 1장 추진배경

□ 목 적

개인정보보호 내부관리계획(이하 '내부관리계획'이라 한다)은 개인정보 보호법 제29조(안전조치의무)와 관련된 **내부관리계획의 수립 및 시행 의무**에 따라 제정하는 것으로 우리 대학교가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 않도록 함을 목적으로 한다.

□ 적용범위

내부관리계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보를 포함하여 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보 및 영상정보처리기기에 적용된다. 또한 개인정보를 취급하는 교직원외 외부 위탁업체에 대하여도 적용한다.

제2장 내부관리 계획의 수립 및 시행

□ 내부관리계획의 수립 및 승인

① 개인정보보호 담당자는 우리 학교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.

② 개인정보보호 담당자는 내부관리계획의 수립 시 개인정보 보호와 관련한 법령 및 관련 규정을 준수하여 수립하여야 한다.

③ 개인정보 보호책임자는 개인정보보호 담당자가 수립한 내부관리계획의 타당성을 검토하고 승인하여야 한다.

④ 개인정보보호 담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 12월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.

⑤ 개인정보보호 담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 2월 말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

□ 내부관리계획의 공표

① 개인정보 보호책임자는 제3조에 따라 내부관리계획을 승인하고, 매년 2월 말까지 당해 연도 내부관리계획을 공표 한다.

② 내부관리계획은 대학 교직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있을 때에는 이를 공지하여야 한다.

제3장 개인정보보호 조직 편제

□ 용어 정의

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “개인정보” 라 함은 생존하는 개인에 관한 정보로서 성명/주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 정보(해당 정보만으로 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있을 때에는 그 정보를 포함한다.)를 말한다.
2. “개인정보처리자” 라 함은 업무를 목적으로 개인정보파일을 운용하기 위하여 개인정보를 처리하는 기관으로서, “강릉원주대학교” 를 말한다.
3. “개인정보보호 책임자” 라 함은 우리 학교의 개인정보보호 업무 및 조직을 총괄하여 지휘·감독하는 자를 말한다.
4. “개인정보보호 관리자” 라 함은 개인정보보호 책임자의 개인정보 보호업무에 대해 위임을 받아 업무를 총괄하고 관리하는 자를 말한다.
5. “개인정보보호 분야별 관리자” 라 함은 개인정보 보호 관리자를 도와 우리 대학 각 부서의 개인정보 업무를 관리·감독하는 자를 말한다.
6. “개인정보보호 담당자” 라 함은 개인정보 보호책임자(관리자)를 보좌하여 개인정보보호업무에 대한 실무를 처리하는 자를 말한다.
7. “개인정보보호 시스템 책임자” 라 함은 개인정보보호를 위한 전산시스템 운영에 대한 업무조직을 총괄하여 지휘·감독하는 자를 말한다.
8. “개인정보보호 시스템 담당자” 는 개인정보보호 시스템 책임자를 보좌하여 개인 정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 관리하고 개인정보보호 업무를 추진하는 자를 말한다.
9. “개인정보보호 시스템 분야별 관리자” 는 해당부서에서 운영하는 홈페이지 및 서버의 개인정보보호를 위한 업무를 관리하는 자를 말한다.

10. “개인정보보호 분야별 시스템 담당자” 는 해당부서에서 운영하는 홈페이지 및 서버를 운영하는 자로 분야별 관리자를 보좌하여 실무를 담당하는 자를 말한다.
11. “개인정보취급자” 라 함은 우리 학교 내에서 정보주체의 개인정보를 수집, 보관, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
12. “개인정보처리시스템” 이라 함은 우리 학교 내에서 사용하는 데이터베이스, 서버를 포함한 개인정보를 처리하는 모든 시스템을 말한다.
13. “영상정보처리기기” 란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

□ 강릉원주대학교 개인정보 관리 조직도

□ 역할별 업무

직책	담당자	수 행 업 무
개인정보 보호 책임자	사무국장	- 개인정보 보호 계획의 수립 및 시행 - 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 - 개인정보 처리와 관련한 불만의 처리 및 피해 구제 - 개인정보파일의 보호 및 관리·감독 - 개인정보보호 및 사용자에 대한 교육계획 수립 및 시행
개인정보보호 관리자/ 분야별관리자	- 총무과장(총괄) - 주요부서 과•실장 및 선임자	- 개인정보파일의 보호 및 관리·감독 - 개인정보취급자의 개인정보처리 이력 - 개인정보 처리와 관련된 불만 처리 - 부서 내 개인정보보호 업무 추진계획 수립 - 부서 내 개인정보보호 담당자와 취급자 지정 - 부서 내 개인정보보호 대책의 운영 관리 책임 - 부서 내 개인정보처리시스템 접근 권한 관리 - 개인정보보호 서약서 징구 - 부서 내 개인정보보호 관련 보안관리 활동 - 부서 내 개인정보 관리 현황 정기 점검 - 부서 내 개인정보취급자 명단 관리 - 부서 내 개인정보 침해사고 및 관리현황 보고 - 기타 개인 정보 보호 관리자가 요구하는 사항 처리
부서별 개인정보 보호 담당자	개인정보보호 관리자 (책임자)가 지정하는 자	- 개인정보보호 관리자(책임자)를 보좌하여 개인정보 보호업무에 대한 실무
부서별 개인정보 취급자	개인정보보호 관리자 (책임자)가 지정하는 자	- 부서별 개인정보 처리 관련 업무 수행 - 개인정보보호 규정 준수 및 처리활동 수행 - 정보주체의 의견 수렴 및 불만사항 접수
개인정보보호 시스템 책임자	정보전산원장	- 대학 내 운영되는 전산시스템의 정보보호 및 개인정보보호 계획의 수립 및 시행 - 대학 내의 모든 전산시스템의 보호·및 관리감독 - 개인정보보호를 위한 시스템 도입 계획수립 및 시행
개인정보보호 시스템 담당자	정보전산원 주무 또는 선임자	- 개인정보보호시스템 책임자를 보좌하여 전산시스템의 정보보호와 개인정보보호의 업무를 수행 - 시스템운영과 관련된 자체계획의 수립 및 감독 - 대학 내 시스템으로 운영되는 홈페이지, 서버 등의 정보보호와 개인정보보호 업무의 지휘·감독 - 개인정보보호와 관련된 정책의 수립 및 집행
개인정보보호 시스템 분야별 관리자	운영부서장 또는 과·실장	- 부서에서 운영 중인 홈페이지 및 전산시스템의 정보보호와 개인정보보호를 위한 기본계획 수립 및 운영 - 소속부서 사용자 컴퓨터 개인정보보호에 관한 업무 - 소속부서 개인정보보호에 관련된 제반 업무
개인정보보호 시스템별 담당자	운영부서 선임자	- 개인정보보호 시스템 분야별 관리자를 보좌하여 개인정보보호 및 정보보호에 관련된 업무 추진 - 운영 중인 홈페이지 및 전산시스템의 정보보호 및 개인정보보호와 관련된 업무의 수행

□ 개인정보 보호책임자 및 전산시스템 책임자의 지정

① 우리 대학은 “개인정보 보호법 시행령 제32조 제2항의 사항” 에 의하여 행정사무를 총괄하는 **사무국장을 “개인정보 보호책임자”** 로 하고, 개인정보 보호책임자의 업무를 위임받아 진행하는 자를 **“개인정보보호 관리자”** 로 하며, 개인정보를 처리하는 부서의 담당자를 “개인정보 분야별 관리자, 또는 취급자” 로 한다.

② 대학 내에서 운영 중인 전산시스템의 개인정보보호를 위하여 **정보전산원장을 “개인정보보호 시스템 책임자”** 로 하고, 시스템보호를 위한 처리업무를 담당하는 자를 “개인정보보호 시스템 담당자” 로 하며, 각 부서에서 운영하는 홈페이지 및 전산시스템의 보호를 위하여 부서의 장 또는 과·실장을 “개인정보보호 시스템 분야별 관리자”, 실제 운영자를 “분야별 시스템 담당자” 로 한다.

□ 개인정보보호 책임자의 의무와 책임

① 개인정보 보호책임자는 정보주체의 개인정보를 보호하고 개인정보와 관련한 정보주체의 불만을 처리하기 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보보호 교육 계획의 수립 및 시행
5. 개인정보파일의 보호 및 관리·감독
6. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

② 개인정보 보호책임자는 제1항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리현황, 처리체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보보호 책임자는 개인정보 보호와 관련하여 이 지침 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 총장에게 개선조치를 보고하여야 한다.

□ 개인정보 취급자의 범위 및 의무와 책임

① 개인정보취급자의 범위는 우리 학교 내에서 정보주체들의 개인정보 수집, 보관, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.

② 개인정보취급자는 정보주체의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보보호 활동 참여
2. 개인정보보호 내부관리계획의 준수 및 이행
3. 개인정보의 기술적·관리적 보호조치 기준 이행
4. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검
5. 기타 정보주체의 개인정보보호를 위해 필요한 사항의 이행

제4장 개인정보의 수집 · 이용

□ 개인정보의 수집 및 수집 제한

① 정보주체로부터 개인정보를 수집하는 경우에는 정보주체의 동의를 얻어야 하며, 그 수집 목적의 범위에서 이용할 수 있다. 정보주체의 개인정보를 수집하는 경우는 다음과 같다.

1. 온라인 홈페이지의 회원양식을 통한 정보 수집
2. 개인정보 수집·활용 동의서(서면) 또는 홈페이지를 통한 정보 수집
3. 교육 또는 회의 참석자에 대한 방명록을 통한 정보 수집

② 제1항의 규정에 따른 동의는 “서면” 또는 “홈페이지 동의” 란에 대한 표시 등의 방법에 따른다.

③ 제1항의 규정에도 불구하고 다음에 해당하면 개인정보를 수집할 수 있다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
3. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
4. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 매우 급한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
5. 개인정보처리자의 정당한 이익을 달성하는 데 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니할 때에 한한다.

④ 기본적인 인권에 관한 민감한 개인정보(민감 정보) 및 고유 식별번호에 대한 수집은 금지한다. 다만, 정보주체의 자발적·명시적 동의 또는 수집 대상 개인정보가 명시된 법률에 근거한 경우에는 수집을 허용한다.

⑤ 정보주체의 개인정보를 수집하는 경우, 적법하고 공정한 수단에 의하여 서비스 제공 및 업무처리에 직접 관련되어 필요한 최소한의 정보를 수집하여야 한다.

□ 개인정보의 수집에 대한 고지

① 정보주체로부터 개인정보보호법 제16조 2항 규정에 따른 동의를 받고자 하는 경우 또는 개인정보를 제3자로부터 받는 경우에는 미리 다음 각 호의 사항을 서면 또는 인터넷 홈페이지 등을 통하여 내용을 쉽게 확인할 수 있도록 정보주체에 알리거나 개인정보처리방침에 명시하여야 한다.

1. 개인정보 보호책임자의 성명, 소속, 전화번호
2. 개인정보의 구체적인 수집목적 및 이용목적
3. 동의 거부 및 철회, 열람 또는 정정 요구 등 정보주체 및 법정대리인의 권리와 그 행사방법
4. 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용
5. 정보주체로부터 수집하고자 하는 개인정보 항목
6. 수집하는 개인정보의 보유·이용기간 및 법적 근거 등 보유 근거
7. 기타 개인정보에 대한 처리 또는 관리 방식

□ 개인정보의 이용 및 제공의 제한

① 개인정보를 개인정보보호법 제18조에 따른 고지의 범위 또는 개인정보처리방침에 명시한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니 된다. 다만, 정보주체의 별도 동의가 있거나 다음 각 호의 1에 해당하는 경우에는 예외로 한다.

1. 다른 법률에 특별한 규정이 있는 경우
2. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소 불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 긴급히 필요하다고 인정되는 경우
3. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
4. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서, 국가 개인정보보호위원회의 심의·의결을 거친 경우
5. 조약, 그 밖의 국제협정 이행을 위하여 외국정부 또는 국제기구에 제공하는데 필요한 경우

6. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
7. 법원의 재판업무 수행을 위하여 필요한 경우
8. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

② 다른 개인정보처리자로부터 정보주체의 개인정보를 받은 자는 정보주체의 별도 동의가 있거나 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 받은 목적 외의 용도로 이용하거나 제3자에게 제공하여서는 아니 된다.

③ 제1항 및 제2항의 규정에 따른 정보주체의 동의를 얻고자 하는 때에는 미리 정보주체에 개별적으로 서면, 전자우편, 전화 등의 방법으로 알려야 한다.

□ 개인정보취급자의 제한

① 개인정보 분야별 관리자는 개인정보를 취급할 수 있는 자를 다음 각 호의 1에 해당하는 자로 정하여 최소한으로 제한하여야 한다.
1. 개인정보주체를 직접 상대로 하여 업무를 수행하는 자
2. 개인정보관리 업무를 수행하는 자
3. 데이터베이스를 포함한 전산 관련 업무를 수행하는 자
4. 기타 업무상 개인정보의 취급이 불가피한 자

□ 개인정보처리의 위탁

① 업무상 타인에게 개인정보의 수집・취급・관리 등을 위탁하는 경우에는 서면, 전자우편, 전화 또는 홈페이지를 통하여 미리 그 사실을 정보주체에 고지 또는 공개하여야 한다.

② 제1항의 규정에 따른 위탁계약을 체결하는 때에는 수탁자와 다음 각 호의 사항을 합의하여 서면 또는 전자적 기록으로 보존하여야 한다.
1. 기술적・관리적 보호 의무
2. 개인정보에 관한 비밀 유지 의무
3. 위탁업무 수행목적 외 개인정보의 처리 금지
4. 처리하는 개인정보의 제3자 제공 금지
5. 내부 규정에 따른 손해배상 책임
6. 기타 개인정보를 안전하게 처리하는 데 필요한 사항

③ 위탁 처리되는 개인정보가 안전하게 관리될 수 있도록 수탁자가 제2항 각 호의 내용을 성실하게 이행하는지에 대하여 위탁한 업무의 범위 내에서 적절한 감독을 하여야 한다.

④ 제1항의 규정에 따라 개인정보의 수집을 위탁받은 자가 개인정보를 수집하는 때에는 미리 위탁받은 사실을 정보주체에 알려야 한다.

⑤ 제1항의 규정에 따라 개인정보 수집·취급·관리 등을 위탁 받은 자는 개인정보를 위탁받은 목적 외의 용도로 이를 이용하거나 제3자에게 제공하여서는 아니 된다.

제5장 개인정보의 기술적·관리적 보호조치

□ 물리적 접근제한

① 개인정보 분야별 관리자(시스템 관리자 포함)는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.

② 개인정보 분야별 관리자(시스템 관리자 포함)는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람내용에 관한 관리대장을 작성하도록 하여야 한다.

③ 개인정보 보호책임자(시스템관리자 포함)는 물리적 접근제한 관리대장의 출입과 열람내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람할 수가 있는지를 점검하여 확인하여야 한다.

□ 출력 복사 시 보호조치

① 개인정보 분야별 관리자(시스템 관리자 포함)는 개인정보가 포함된 정보를 출력하거나 복사할 때 개인정보 유출 사고를 방지하는 보호조치를 취하여야 한다.

② 개인정보 분야별 관리자(시스템 관리자 포함)는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사할 때 출력·복사자의 성명, 일시 등을 기재하여 개인정보 유출 등에 관한 책임 소재를 확인할 수 있는 강화된 보호조치를 추가로 적용할 수 있다.

③ 개인정보취급자(시스템 관리자 포함)는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

□ 개인정보취급자 접근권한 관리 및 인증

① 개인정보 분야별 관리자와 시스템 관리자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.

② 개인정보 분야별 관리자와 시스템관리자는 개인정보취급 업무를 담당하는 직원의 담당업무에 따라 개인정보 취급권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정 및 삭제 권한)을 차등 부여한다.

③ 개인정보 분야별 관리자와 시스템관리자는 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 때 바로 개인정보처리시스템의 접근권한을 변경 또는 삭제한다.

④ 개인정보 분야별 관리자와 시스템관리자는 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증수단을 적용하여야 한다.

⑤ 개인정보 분야별 관리자와 시스템관리자는 제1항 내지 제4항에 의한 권한 부여, 변경 또는 말소에 대한 내용을 기록하고, 그 기록을 최소 3년간 보관한다.

□ 개인정보의 암호화

① 개인정보 분야별 관리자와 시스템관리자는 주민등록번호 등 개인정보보호법에서 규정한 고유 식별번호 및 민감 정보에 대해서는 암호화하여 저장하여야 한다.

② 개인정보취급자와 시스템관리자는 비밀번호를 사용하는 경우 최소 분기별 1회 이상 정기적으로 변경하여야 한다.

③ 개인정보 분야별 관리자와 시스템관리자는 정보통신망을 통해 정보주체의 개인정보 및 인증정보를 송수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다.

④ 개인정보취급자는 정보주체의 개인정보를 개인용 컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

□ 접근통제

① 개인정보 보호시스템 책임자는 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 다음 각 호의 기능을 포함한 시스템을 설치 및 운영한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보 보호 시스템 책임자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인 관련 정보를 비밀번호로 이용하지 않도록 비밀번호 작성가이드를 수립하고, 이를 적용 및 운용하여야 한다. 개인정보취급자는 개인정보 보호책임자가 수립한 비밀번호 작성가이드를 참고하여야 한다.

*** 비밀번호 작성가이드 별첨 참고**

③ 개인정보 보호시스템 책임자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템과 개인정보취급자의 컴퓨터에 보안 프로그램 설치 등의 조처를 취할 수 있다.

④ 개인 정보 보호 관리자는 매월 셋째 주 수요일을 사이버보안 진단의 날로 지정하여 부서별 정기점검을 시행하도록 한다.

□ 접속 기록의 위변조 방지

① 개인정보 분야별 관리자는 접속 기록의 위변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입/출력, 수정 등 DB 접근)하는 경우에는 처리일시, 처리내용 등 접속기록을 저장한다.

② 개인정보 보호책임자는 제1항의 접속기록에 대해 년 2회 이상 정기적으로 확인·감독한다.

③ 개인정보 시스템 관리자는 제1항의 접속기록에 대해 위·변조 방지를 위해 백업 보관하며, 보관기간은 최소 6개월 이상으로 한다.

□ 보안프로그램의 설치 및 운영

① 개인정보보호 시스템 책임자는 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프로그램 등의 보안 프로그램을 설치·운영하여야 한다.

② 보안 프로그램은 항상 최신의 버전으로 업데이트 하여야 한다.

③ 보안 프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시간 감시 기능을 적용하여야 한다.

□ 개인용컴퓨터 개인정보보호 프로그램 설치 및 운영

① 교직원(이하 교내에서 근무하는 모든 ‘교원’ 및 ‘직원‘ 을 통칭한다.)의 경우 교내에서 컴퓨터를 사용함에서 ‘개인정보보호법 제21조’에 따라 불필요한 개인정보는 재생 및 이용되지 않게 파기하여야 하며, ‘개인정보보호법 제24조’에 의거 고유 식별 정

보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 암호화하여 안전성 확보를 위한 PC 개인정보보호 프로그램을 설치·운영하여야 한다.

② PC 개인정보보호 프로그램은 항상 최신의 버전으로 업데이트 하여야 한다.

③ 컴퓨터사용 교직원들은 PC 개인정보보호 프로그램의 실시간 감시기능을 항시 적용하고 최소 월 2회 이상 사용 중인 컴퓨터 내의 개인정보보호대상 파일 검사를 이행하여야 한다.

④ 제3항의 검사에서 검출된 개인정보보호대상 파일은 암호화하여 분리 보관하여야 하며, 불필요하거나 보관이 필요치 않으면 경우 반드시 폐기하여야 한다.

⑤ 개인정보보호대상 파일의 종류는 다음과 같이 명시한다.

1. 개인 신상 식별정보(이하 주민 번호, 외국인 번호, 여권 번호, 운전면허, 건강보험 번호 해당)
2. 금융정보(이하 계좌번호, 카드 번호 해당)
3. 일반개인정보(이하 E-MAIL 주소, 유무선 전화번호, 사업자/법인번호, 주소 해당)

⑥ 개인정보보호 시스템 관리자는 PC 개인정보보호 프로그램을 이용하여 최소 월 1회 이상 교내 컴퓨터를 대상으로 개인정보보호대상 파일 검사를 이행하고 암호화 또는 삭제 조치하지 않은 개인정보보호대상 파일 검출 시 해당 컴퓨터의 사용자에게 검출된 개인정보보호대상 파일의 리스트를 첨부하여 서면 통보하고 개인정보보호 분야별 관리자와 부서장에게 보고한다.

⑦ 제6항의 대상 컴퓨터 사용자는 1주일 이내에 개인정보보호 시스템 관리자가 첨부한 개인정보보호대상 파일에 대한 조치를 완료 후 개인정보보호 분야별 관리자에게 보고하여야 하고, 개인정보보호 분야별 관리자는 이를 개인정보 보호책임자에게 서면통보하여야 한다. 이를 이행하지 않거나 추후 점검에서 2차 검출 시 추가적인 제재 조치를 취할 수 있다.

□ 영상정보처리기기의 설치와 운영관리

① 영상정보처리기기 운영·관리부서인 총무과장(이하 개인 영상정보 보호책임자)은 영상정보처리기기 설치 시 “개인정보보호법 제23조”에 따라 전문가와 이해관계인의 의견수렴 절차를 거쳐야 한다.

② 제1항에 따라 영상정보처리기기를 설치·운영하려는 경우 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다.

③ 제1항에 따라 영상정보처리기기를 설치·운영하려는 경우 녹음기능을 사용하여서는 아니 되며, 기기의 임의조작하거나 다른 곳을 비춰서는 아니 된다.

④ 개인 영상정보 보호책임자와 개인정보보호 분야별 관리자는 다음 각 호의 항이 포함된 안내판을 설치하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 성명 및 연락처

⑤ 개인정보 보호책임자는 영상정보처리기기 운영·관리 방침을 수립하여 홈페이지 등에 공개하여야 한다.

⑥ 개인정보 분야별 관리자는 개인 영상정보기기의 운영을 위하여 기술적·관리적 보호조치를 준수하여야 한다.

□ 기술적 보호조치

① 우리 학교에서 보유하고 있는 개인정보관리의 안전성 확보를 위해 필요한 기술적 조치를 아래와 같이 계획하여 수행한다.

구분	보호조치	추진일정	시행부서
PC 개인정보 보호 강화	PC 개인정보 파일 분기별 검색	분기별	총무과
	개인정보보호 교육	년 2회	총무과
웹사이트 보안 강화	개인정보 노출 방지 취약점 점검	학기별 1회	전산원

② 개인정보의 안전한 관리를 위해 항목별 현황파악과 저장 시 필요한 법적 기준을 적용한다.

암호화 대상항목	DB명	개인정보처리시스템	처리부서	비고
주민등록번호	학사DB/행정DB	학사행정시스템	교육지원과/ 정보전산원/ 장학팀	
비밀번호	학사DB/행정DB	학사행정시스템		
카드번호	학사DB/행정DB	학사행정시스템		
통장번호	학사DB/행정DB	학사행정시스템		

□ 기술적·관리적 보호조치 수행계획

구분	항목	2016년	
		추진 월	내용
개인정보 관리체계 기반수립	개인정보보호 내부지침 및 가이드 개정	3월	개인정보지침 개정/제작
	개인정보취급자 인식제고	6월/10월	개인정보취급자 교육
개인정보 기술적 보호조치 방안	교내 컴퓨터 개인정보보호 대상 파일 관리 점검	분기별	교내 컴퓨터 점검
	백신 및 자동 패치 프로그램 점검	학기별	전체 웹사이트 점검
	서버 시스템 취약점 점검	학기별	전체시스템 취약점 파악
개인정보 관리적 보호조치 방안	웹사이트 개인정보 노출방지 점검	분기별	관련 법률과 개정사항 비교
	개인정보 파기 정책 및 절차 검토	6월~12월	관련법 반영하여 정책 개선

제6장 정기적인 자체점검 실시

□ 자체점검 주기 및 절차

① 개인정보보호 책임자는 개인정보보호를 위한 내부관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 점검하여야 한다.

② 개인정보보호 책임자는 개인정보 자체점검을 위한 대상, 절차 및 방법 등 점검의 시행에 관하여 필요한 별도의 계획을 수립할 수 있다.

③ 개인정보보호 자체점검은 매월 셋째 주 수요일 사이버보안 진단의 날에 관리자가 PC개인정보보호 프로그램을 사용하여 교내 모든 컴퓨터의 개인정보보호대상 파일의 유무 및 관리 사항을 점검한다. 사이버보안 진단의 날 외에 수시로 점검할 수 있다.

④ '사이버보안 진단의 날'을 지정하여 개인정보취급자(전교직원)의 컴퓨터 안전성 정기점검, 비밀현황 확인 등 자체보안점검을 시행한다.

1. 시행시기 : 매월 셋째 주 수요일
2. 주관부서 : 정보전산원

⑤ 개인정보보호 분야별 관리자는 본 계획의 준수 여부에 대한 자체점검을 시행하여 매년 3월 말까지 그 결과를 개인정보 보호책임자에게 통보한다.

□ 자체점검 결과 반영

① 개인정보보호 관리자는 자체점검 시행 결과 현황을 취합 정리하여 개인정보보호책임자에게 보고하여야 하며, 관련 자료는 문서로 만들어 보관한다.

② 개인정보보호책임자는 개인정보 보호를 위한 자체점검 시행 결과, 개인정보의 관리 운영상의 문제점을 발견하거나 관련 교직원이 본 계획의 내용을 위반할 때에는 총장에게 보고 후 시정·개선 또는 필요한 조치를 하여야 한다.

③ 개인정보보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 총장에게 보고 후 개인정보취급자 등에 대한 필요한 추가 조치를 요청할 수 있다.

제7장 개인정보보호 교육

□ 개인정보보호 교육 계획의 수립

① 개인정보보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립·시행한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

② 수립한 개인정보보호 교육 계획을 시행한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

□ 개인정보보호 교육의 시행

① 개인정보보호책임자는 정보주체정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 정기적으로 년 2 회 이상의 개인정보보호 교육을 시행한다.

② 년 2회의 정기 교육은 상반기에 1회, 하반기에 1회 실시하는 것을 원칙으로 하며, 최소 년 2회를 실시하는 것으로 한다.

③ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 상급기관, 외부 전문기관이나 전문가에 위탁하여 교육을 시행할 수 있다.

④ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호 책임자는 부서 회의 등을 통해 수시 교육을 시행할 수 있다.

제8장 개인 침해대응 및 피해 구제

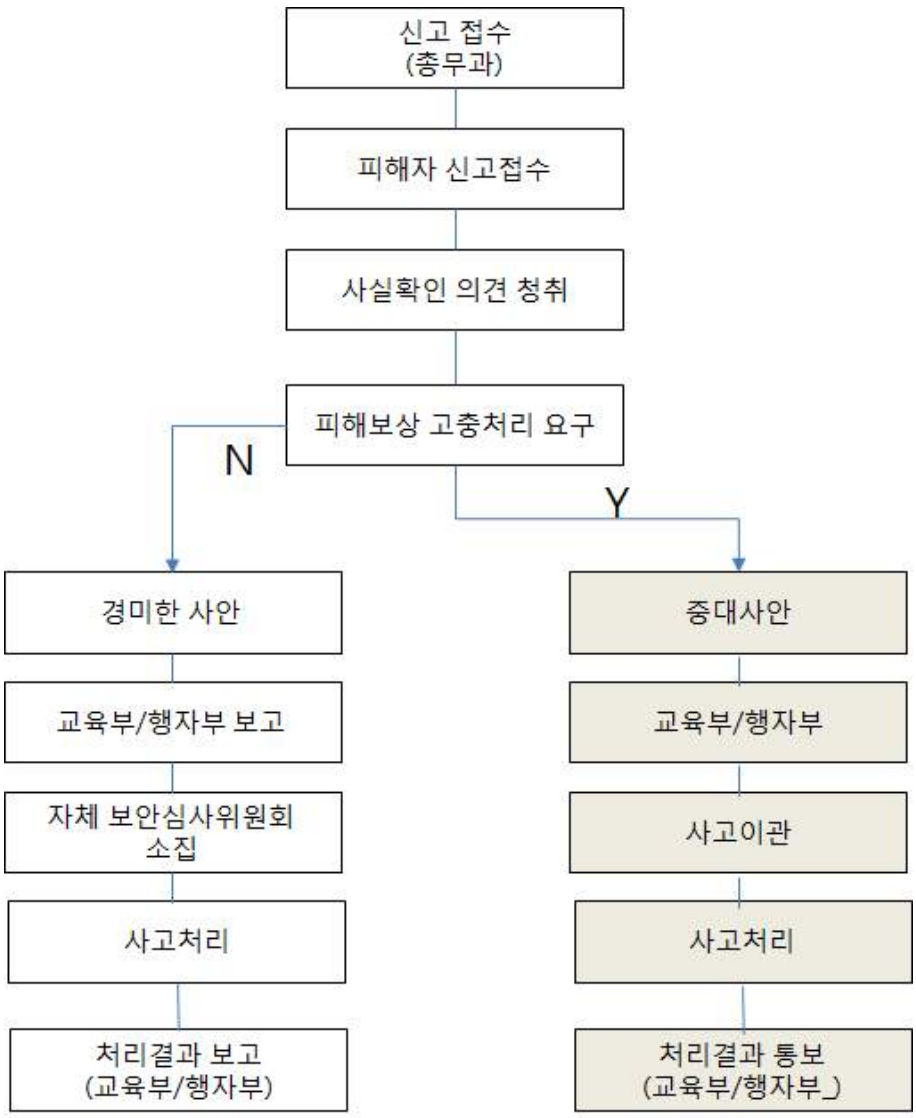
□ 침해대응 대책

① 개인정보보호시스템 책임자는 다음 사항에 의거 침해사고에 대한 처리 계획을 수립하고 시행한다

② 사고사실 고지

1. 침해사고 발생 시 정당한 사유가 없는 한 5일 이내에 해당 정보주체에 다음의 절차에 의하여 고지한다.
   - 유출된 개인정보의 항목
   - 유출된 시점과 그 경위
   - 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
   - 개인정보처리자의 대응조치 및 피해 구제절차
   - 정보주체에 피해가 발생하였을 때 신고 등을 접수할 수 있는 담당 부서와 연락처
2. 사고의 확산 및 추가 유출 방지를 위한 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급조치는 우선 조치한 후 정보주체에 고지

<처리절차도>



□ 피해구제 대책

① 피해예방 : 사전에 정보주체에 피해가 발생하지 않도록 개인정보보호 처리자는 개인정보보호법을 준수하고(본 내부관리 계획의 제1장~제6장에 대한 내용을 숙지하고 조치) 주의와 감독에 만전을 기하여야 함.

[참고] 개인정보보호법 제39조에 따라 정보주체는 개인정보처리자가 법을 위반한 행위로 손해를 입으면 손해를 배상할 수 있다. 이 경우 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다. 또한, 개인정보처리자가 이 법을 준수하고 상당한 주의와 감독을 게을리하지 아니하였을 때 개인정보의 분실도난유출 변조 또는 훼손으로 인한 손해배상 책임을 감경 받을 수 있다.

② 분쟁조정위원회 조정신청 : 정보주체가 피해 구제를 위하여 분쟁조정위원회로 분쟁조정을 신청할 때 조정위원회의 권고를 참고하여 원만한 해결을 위한 합의를 마련해야 함. (우리대학교는 보안심사위원회 회의안건 부의)

[참고] 개인정보보호법 제43조에 따라 정보주체는 비용, 절차 등의 사유로 소송을 통한 피해 구제가 어려울 경우 분쟁조정위원회로 분쟁조정을 신청할 수 있다.
이 분쟁조정위원회의 조정은 법원의 판결에 의하지 않고 조정위원회의 권고에 의하여 양당사자가 서로 양보하여 합의로서 해결하는 절차로 당사자가 수락하여 조정이 성립되면 법원의 확정판결과 동일한 효력이 발생하게 된다.

【별첨 1】 비밀번호 작성가이드

- 숫자, 문자, 특수 문자 등을 혼합하여 최소 8자리 이상의 길이로 구성하여야 한다.
- 사용자 계정(ID)과 동일하지 않은 것으로 사용하여야 한다. (abcd/abcd, admin/admin)
- 동일 단어 또는 숫자를 반복하여 사용하지 말아야 한다. (111111, aaabbbccc, 1234567 등)
- 사용된 비밀 번호는 재사용하지 말아야 한다.
- 동일 비밀 번호를 여러 사람이 공유하여 사용하지 말아야 한다.
- 동일 아이디와 비밀 번호를 여러 사이트에 사용하지 말아야 한다.
- 비밀 번호에 유효 기간을 설정하고 적어도 분기마다 1회 이상 정기적으로 변경하여야 한다.
- 2~3개의 비밀 번호를 교대로 사용하지 말아야 한다.

【별첨 2】

개인정보보호 담당자별 업무 구분내역

수행업무	사무국장	총무과 담당자	정보전산원장	정
• 개인정보보호 계획 및 내부계획의 수립 및 운영	○	○		
• 개인정보보호를 위한 운영에 관한 사항(교육 및 운영계획 등)	○	○		
• 개인정보보호를 위한 전산시스템 계획의 수립			○	
• 개인정보보호 Filtering 시스템 운영 및 유지보수		○	○	
• 대학 내 홈페이지 및 전산시스템의 점검 및 보호계획 수립 및 관리			○	
• 개인용 컴퓨터 개인정보보호 관리 업무	○	○		
• 개인정보보호시스템의 운영 및 등록정보관리			○	
• 개인정보처리실태와 관행의 정기조사 및 개선	○	○	○	
• 개인정보처리 불만의 처리 및 피해구제	○	○	○	
• 개인정보파일의 보호 및 관리 감독	○	○		
• 개인정보취급자의 정보처리 이력의 보관 및 관리			○	
• 부서 내 개인정보보호 업무 추진계획 수립			○	
• 개인정보보호 담당자 및 취급자의 지정	○	○		
• 부서 내 담당자 및 취급자 지정			○	
• 개인정보보호 대책의 운영 관리	○	○		
• 개인정보보호 관리자, 취급자 서약서 징구	○	○		
• 개인정보파일 사용자 분기별 정기점검계획수립 및 점검	○	○		
• 부서 내 개인정보처리시스템 접근 권한 관리				
• 부서 내 개인정보보호 서약서 징구				
• 부서 내 개인정보보호 월별 정기점검				
• 부서 내 정기적인 개인정보보호 점검 및 사이버진단실시				