재해·재난 대비 개인정보 및 정보처리시스템 위기대응 매뉴얼

2024. 3.

목포과학대학교

목 차

I 개 요

1. 관련

○ 개인정보보호법 제29조(안전조치 의무)

○ 개인정보보호법 시행령 제30조(개인정보의 안전성 확보조치)

○ 개인정보의 안전성 확보조치 고시 **제11조(재해·재난** 대비 안전조치)

○ 교육부 사이버 분야 위기대응 실무 매뉴얼

2. 추진 목적

○ 최근 지진, 화재 등 재해·재난 대응의 중요성이 높아짐에 따라 학내 개인정보 및 정보처리시스템 보호를 위한 위기대응 체계 수립하고 신속한 복구와 원활한 업무 처리의 재개를 위해 관련 절차 등의 대책 마련

3. 적용 범위

○ 본 매뉴얼에서 정의한 **재해·재난** 발생 시 목포과학대학교에서 운영하는 개인정보 및 정보처리시스템 운영 및 관리에 한하여 적용

○ 위기 상황 해제 시까지 개인정보 및 정보처리시스템의 운영에 필요한 모든 행동 요령을 포함

4. 용어 정의

○ **(개인정보)** 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보

가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 함

다. 가목 또는 나목을 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보

○ **(개인정보 처리)** 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위

○ **(정보시스템)** 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계

○ **(개인정보처리시스템)** 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템

○ **(고유식별정보)** 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호

○ **(민감정보) 사상·신념, 노동조합·정당의 가입·탈퇴,** 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보

○ **(재해·재난)** 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고

○ **(개인정보처리시스템 위기)** 개인정보처리시스템이 장애로 인해 가동이 전면 중단되거나 중단 가능한 시간을 초과하는 경우

○ **(백업)** 잘못되거나 부주의한 조작으로 인하여 데이터가 손실될 것에 대비하여 미리 남겨둔 복사본

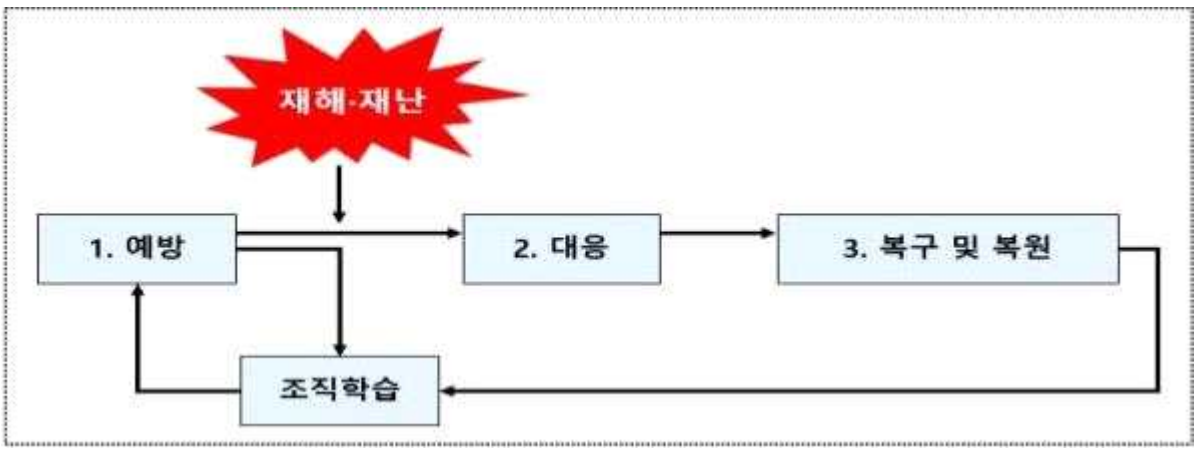
○ **(재해복구시스템)** 재해·재난 발생 시 데이터를 보존하고 자동 복구하는 장치

Ⅱ 위기대응 절차

1. 절차 개요

○ 위기 발생 시 **예방, 대응, 복구 및 복원으로** 이루어지는 3가지 단계를 체계적으로 수행하여야 함

<재해·재난 대비 위기대응 절차도>



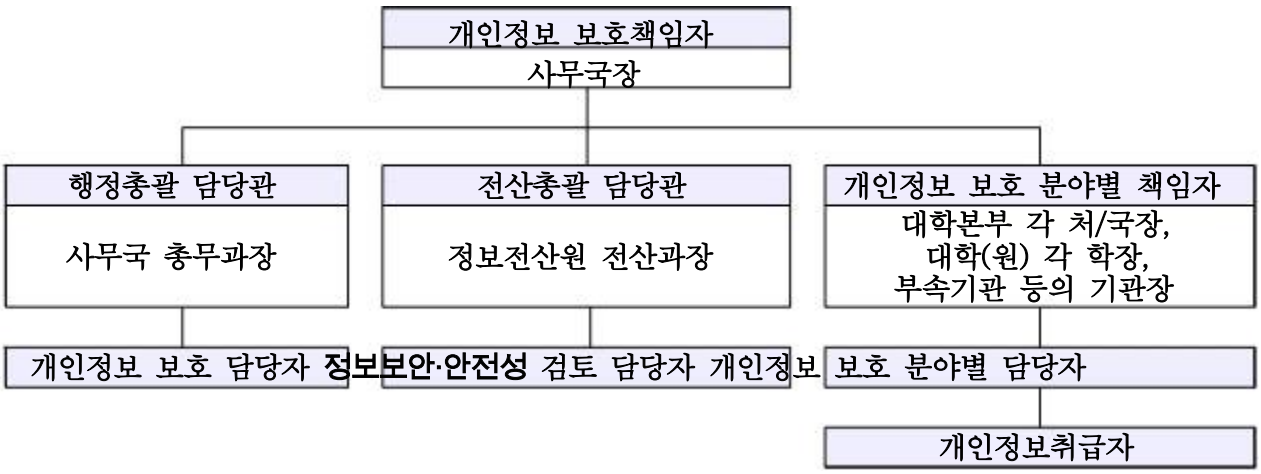
2. 단계별 정의 및 업무

예방	▶ **위기 상황이 발생 시 예상되는 문제들을 미리 보완하고 대비** · 위기대응 매뉴얼 관리 · 백업 등 정보시스템, 보안시스템, 정보통신 기반 관리 · 재해복구시스템 관리 등 · 개인정보처리시스템 등 정보시스템별 관리 계획 수립 · 정보처리시스템의 불필요한 정보 파기, 암호화 상시 점검 ▶ **주기적 점검을 통해 위기대응 준비** · 정보처리시스템, 백업시스템, 네트워크 장비 및 보안장비, 서버실 등 정기 점검 · 비상발전기, 무정전전원장치(UPS), 공조 시설 등 점검 · 비상시 인력 운영 및 수급 계획 점검
대응	▶ **재해 · 재난 위기대응 체계에 따라 대응 실시** · 화재진압, 직원 대피, 비상전력 공급, 침수 차단 등 신속한 초기대응 실시 등 · 초기비상대응 ⇨ 위기대응 조직 구성 ⇨ 피해분석 및 위기 상황 선포 ⇨ 등급별 위기 상황 대응 ▶ **위기대응 조직을 소집하고 위기 등급을 정의하여 위기 상황 선포** · 개인정보처리시스템 담당자는 피해 현황 및 복구 예상 시간을 파악하여 개인정보처리시스템 책임자 및 개인정보보호 책임자에게 즉시 보고 · 정보시스템 운영·관리 부서와 유기적 협조 ※ 비상연락체계를 가동하고 위기대응 조직의 역할에 따라 대응 실시
복구 및 복원	▶ **복구 목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시** · 업무 긴급성, 업무 영향도 등을 종합적으로 고려·판단하여 복구 우선순위가 높은 업무부터 단계적으로 복구 ▶ **복구 및 복원이 완료되면 위기 상황의 종료를 선언하고 위기대응 시 발견되는 문제점 위기대응 체계에 반영하여 개선** · 개인정보처리시스템 책임자는 위기 상황 종료 시 기관에 위기 종료 선언 ▶ **위기 상황으로 인한 대응 사례 전파 및 교육 실시**

Ⅲ 위기대응 체계

1. 위기대응 조직의 구성

○ 조직 체계도



○ 업무분장 및 역할

구분	주요 역할
개인정보 보호책임자	· 위기대응 업무의 총괄 · 위기 선포 및 위기대응 조직 구성원에게 업무를 지시 · 위기대응 상황 종료 시 결과 공유 등
행정총괄 담당관 (총무과장)	· 위기 상황 발생 시 각 업무기능의 현황 파악 및 복구 총괄 · 책임자의 위기 선포에 따라 위기 상황 전파 · 평상시 개인정보 위기대응 절차 및 계획 검토
전산총괄 담당관 (전산과장)	· 정보보안 총괄 업무수행 · 평상시 정보보안 위기대응 절차 및 계획의 검토
개인정보 보호 분야별 책임자	· 책임자의 위기 선포에 따라 위기 상황 전파 · 개인정보보호 활동 지원
개인정보 보호 담당자	· 비상연락망 및 유관기관과의 연락망 가동·정보공유 · 개인정보처리시스템 상시·정기 점검 및 후속조치 실시 · 개인정보 위기대응 절차 및 계획 수립
정보보안·안전성 검토 담당자	· 개인정보처리시스템의 기술적 보안·복구 및 운용 담당 · 책임자 및 담당관 지시에 따라 필요한 활동 지원 · 정보보안 위기대응 절차 및 계획 수립
개인정보 보호 분야별 담당자	· 개인정보의 처리 기준 이행 · 개인정보보호 활동 참여
개인정보취급자	· 개인정보의 처리 기준 이행 · 개인정보보호 활동 참여

○ 개인정보처리시스템 담당자는 조직의 인력 변동 시 각각의 역할이 누락 없이 인수 · 인계되도록 해야 함

2. 위기 등급의 분류 및 대응

구분	판단기준	비고
관심 (Blue)	· 장애 발생 직후 S/W 및 H/W의 이중화 구성으로 중단 없이 서비스가 제공되는 경우 · 파일시스템이 이중화 구성되어 디스크 하나에 장애 발생 시 자동으로 대체 되는 경우 · 정전 등 발생 시 전원 이중화 구성으로 중단없이 서비스되는 경우 · 평상시 운영 절차에 의거 수행	징후 감시 활동
주의 (Yellow)	· 장애 발생 후 인지 / 접수 즉시 간단한 조치로 서비스 재개가 가능한 경우 · 네트워크 라인의 절단, 비적격 전류 인입으로 일시적인 서버 중지, WEB/WAS, DBMS 등 주요 프로세스 일시 장애 · 임의 백업 수행, DATA 복구 계획 재점검 · 비상연락망에 의해 연락 체계 수립	협조 체계 가동
경계 (Orange)	· 장애 발생 후 인지 / 접수 즉시 해당 필요 사항 조치 후 1시간 이내 서비스 재개가 가능한 경우 · 응용 S/W의 오류로 인해 서비스가 중지되어 해당 업무 개발자가 조치해야 할 경우 · 긴급 백업 수행, 대피 우선순위에 의거 장비 및 내역 확인 · 비상연락망 가동 및 장비 반출 계획 수립	대비 계획 점검
심각 (Red)	· 재해/재난 발생으로 서버 보관 장소에 직접적인 피해가 발생한 경우 · 교체에 많은 시간이 걸리는 H/W 부품 등의 파손이 대량 발생하여 2시간 이상 서비스가 불가능한 경우 · 대피 우선순위에 의거 장비 및 DATA 미디어 반출	즉각 대응 태세 돌입

3. 복구 목표의 설정

◯ 복구 목표의 정의

- 복구목표시간 (RTO : Recovery Time Objective)
  : 가동 중단 시스템을 복구하여 정상 조작 재개하는 데 걸리는 시간
  (예) 거의 즉시, 1시간 미만, 4시간 미만, 12시간 미만, 1~4일 등
- 복구목표시점 (ROP : Recovery Point Objective)
  : 가동 중단 전의 데이터를 보존해야 하는 특정 최소 시점
  (예) 데이터 손실 없음, 마지막 저장(매주, 매일) 등
- 복구우선순위 (RP)
  : 가동 중단 시스템의 복구 순서로 숫자가 낮을수록 우선 복구 대상

◯ 위기 등급별 복구목표시간(RTO)

구분	판단기준	비고
관심 (Blue)	1시간 미만	중단 없음
주의 (Yellow)	4시간 미만	일시 중단
경계 (Orange)	12시간 미만	1시간 이내 중단
심각 (Red)	1~2일	H/W 파손

4. 백업 관리

◯ 정보처리시스템 담당자는 신속한 업무 복구를 위해 백업 대상(개인정보 및 정보시스템)을 선정하고 필요한 내용을 주기적으로 백업해야 함

◯ 백업 대상은 DB, 개발 소스 및 데이터, 로그, 서버 OS 그리고 기타 중요도가 높다고 판단되는 데이터를 대상(개인정보 포함)으로 함

◯ 정보처리시스템 담당자는 안전한 백업 매체를 선정하고 백업의 주기 및 소산 유무를 결정해야 함

◯ 백업 매체는 비인가자가 접근할 수 없는 격리된 곳에 보관하여 비인가자에 의한 백업 정보 유출이 일어나지 않도록 해야 함

◯ 백업 매체의 물리적인 접근통제 및 백업 일자 목록은‘붙임3(백업 관리대장)’에 기록하여 유지·관리해야 함

5. 위기대응 훈련

◯ 개인정보처리시스템 등 정보시스템의 위기가 발생하는 경우 피해를 최소화하고 신속한 복구를 위해 연 1회 이상 위기대응 훈련을 실시

◯ 위기대응 훈련은 평시 서비스 운영 중에 **재해·재난** 복구시스템이 정상 작동 되는지 확인해야 하며 위기 상황 발생 시와 동일하게 위기대응 조직의 역할을 수행해야 함

◯ 위기대응 훈련 시에는 다음의 사항을 유의하여 실시해야 함

- **재난·재해** 복구시스템의 정상 작동
- 위기대응 조직 구성원별 역할 숙지
- 복구 목표의 달성
- 실데이터의 안정성 보존
- 비상 연락망 정상 가동 상황
- 위기대응 체계 운용 시 이슈 사항

◯ 개인정보처리시스템 관리부서는 위기대응 훈련 종료 후 훈련 시 도출된 미흡한 사항 및 이슈 사항을 위기대응 체계에 반영하여 개선해야 함

6. 비상연락망 구성

◯ 위기대응 조직원, 관련 업체 등으로 이뤄진 비상연락망을‘붙임2(비상연락망)’에 기록관리 해야 함

◯ 비상연락망은 별도 수립하여 위기대응팀간 공유(연 1회 이상)

◯ 비상연락망을 주기적(연 1회 이상)으로 검토하고 평상시에도 연락 체계를 활용하여 정보를 공유해야 함

◯ 위기 상황 발생 시 위기 상황 종료 시까지 비상연락망을 가동하여 신속한 대응을 지원해야 함

붙임 1 개인정보처리시스템 구성 현황

우선 순위	시스템명	담당 부서	민감·고유 식별 정보 포함 여부
1	통합정보시스템	정보관리소	주민등록번호 포함
2	입학관리시스템	입학홍보처	주민등록번호 포함
3	도서관리시스템	도서관	해당 없음

※ DB서버, Web서버, 어플리케이션 서버, 보안장비 등 개인정보처리시스템에 미치는 영향을 고려하여 중요한 연계 장비· 설비 위주로 작성

※ 우선순위는 시스템별 개인정보 보유량, 민감정보 고유식별정보 보유 여부 등을 종합적으로 고려·검토하여 결정

붙임 2 비상연락망

비상연락망

작성일자 : 2024년 23

1. 비상대책반 연락망

담당업무	담당자	연락처
개인정보보호책임자(CPO)	정보관리소소장	061-270-2550
개인정보보호 분야별 책임자 (개인정보처리시스템 운영 부서)	교무혁신처장	061-270-2550
	입학처장	061-270-6542
	산학협력처장	061-270-2737
	도서관장	061-270-2562
행정총괄 담당관	행정지원처 과장	061-270-2807
전산총괄 담당관	전산팀장	061-270-2504
개인정보보호 담당자	전산팀장	061-270-2504
정보보안 담당자	전산팀장	061-270-2504

2. 관련부서 연락망

부서명	담당업무	연락처
정보관리소	통합정보시스템 관리	061-270-2504
입학처	입학관리시스템 관리	061-270-2542
도서관	도서관리시스템 관리	061-270-2562

3. 관련업체 연락망

업체명	담당업무	연락처
㈜진학어플라이	입학관리시스템 유지보수	1544-7715

붙임 3 백업 관리대장 (양식)

백업 관리대장

No	백업 시행일	백업 시행자	반출여부			라벨	내역	반출일	반출자	반출 확인	회수일	회수자	회수 확인
			반출 안함	내부 소산	외부 소산								