

재해·재난 대비 개인정보처리시스템 위기대응 매뉴얼

I. 개요

1. 목적

- 최근 지진, 화재 등재해·재난 대응의 중요성이 높아짐에 따라 개인 정보처리 시스템 보호를 위한 위기대응 체계 수립
- 재해·재난 발생 시 개인정보처리시스템의 신속한 복구와 원활한 업무 처리의 재개를 위해 관련 절차 등의 대책 지원

2. 관련 법률

- 개인정보보호법 제29조, 시행령 제30조, 개인정보의 안전성 확보조치 고시 제12조

3. 적용범위

- 본 매뉴얼에서 정의한 재해·재난 발생 시 개인정보처리시스템의 위기대응에 한하여 적용
- 개인정보처리시스템 위기 상황 해제 시까지 개인정보처리시스템의 운영에 필요한 모든 행동 요령을 포함

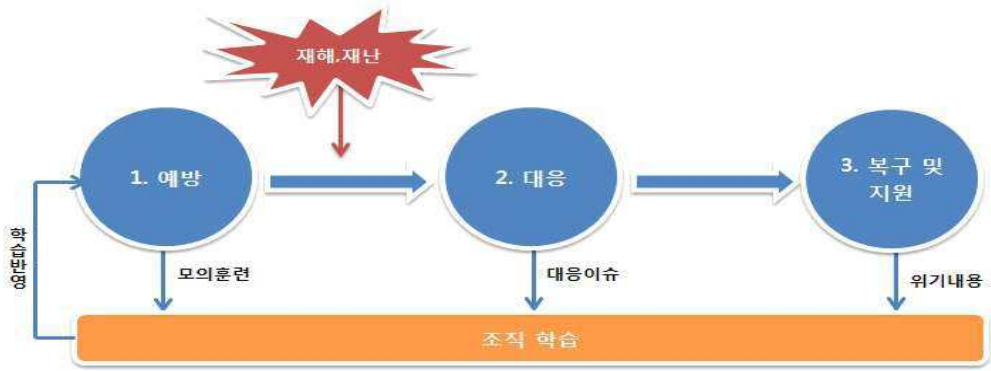
4. 용어 정의

- 재해·재난 : 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고
- 개인정보처리시스템 위기 : 개인정보처리시스템이 재해·재난으로 인한 장애로 인해 개인 정보가 유출, 손실, 훼손 되거나 서비스 제공이 중단 가능한 시간을 초과하는 경우
- 백업 : 잘못되거나 부주의한 조작으로 인하여 데이터가 손실될 것에 대비하여 미리 남겨 둔 복사 본
- 재해복구시스템 : 재해·재난 발생 시 데이터를 보존하고 자동 복구 하는 장치
- 재해복구시스템 복구 수준 : 본원 또는 IDC에서 기관을 위해 정의한 재해복구서비스의 복구 수준

II. 위기대응 절차

1. 절차 개요

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



2. 단계별 정의

가. 1단계 : 예방

- 개인정보처리시스템 책임자와 담당자는 위기상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비
 - 개인정보처리시스템 불필요한 개인정보의 파기, 암호화 상시 점검
 - 개인정보처리시스템 보안 조치 상시 점검
 - 개인정보 유·노출 방지를 위한 정기점검(월 1회 이상) 및 후속조치 이행 등
- 개인정보처리시스템 관리 기관(부서)의 위기대응 조직, 위기등급, 복구목표 등 위기대응 체계 검토
 - 재해·재난 발생 시 비상연락망 체계 구축 및 점검
 - 비상 시 인력운영 및 수급 계획 점검
 - 유지보수 및 위탁운영 업체 비상연락망 체계 구축 및 위기대응 능력 점검 등
- 개인정보처리시스템의 주기적 백업 및 위기대응 훈련 실시를 통해 위기대응 준비
 - 개인정보처리시스템 담당자는 정기적인 데이터 백업, 점검 등을 실시하여 ‘붙임2(백업 관리대장)’서식에 따라 관리
 - 재난·재해 발생에 대비한 데이터 복구, 장애 대응 등 모의훈련 실시 등

나. 2단계 : 대응

- 재해·재난으로 위기상황이 발생하여 위기대응 체계에 따라 대응 실시
 - 재해·재난 발생 시 화재진압, 직원대피, 비상전력 공급, 침수차단 등 신속한 초기대응 실시 등
- 위기대응 조직을 소집하고 위기등급을 정의하여 위기상황 선포
 - 개인정보처리시스템 담당자는 피해현황 및 복구 예상시간을 파악하여 개인정보처리시스템 책임자 및 개인정보보호 책임자에게 즉시 보고
 - 개인정보처리시스템 책임자는 피해정도를 판단하여 위기등급을 선포하고

위기등급별 대응 계획에 따라 대응 실시

- 비상연락체계를 가동하고 위기발생·대응 조직의 역할에 따라 대응 실시
 - 개인정보처리시스템 책임자 및 담당자는 재해·재난 발생으로 개인정보 침해 발생 시 관련 법령에 따라 개인정보주체에게 유출을 통지하고 관련기관에 개인정보 유출 사실 신고

다. 3단계 : 복구 및 복원

- 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시
 - 개인정보처리시스템 내 업무 긴급성, 업무 영향도 등을 종합적으로 고려·판단하여 복구 우선순위가 높은 업무부터 단계적으로 복구하고, 정기적으로 백업된 데이터를 이용하여 복원 실시
- 복구 및 복원이 완료되면 위기상황의 종료를 선언하고 위기대응 시 이슈사항을 위기대응 체계에 반영하여 개선
 - 개인정보처리시스템 책임자는 위기상황 종료 시 기관에 위기종료 선언
 - 개인정보처리시스템 담당자는 위기상황 종료 시 대응 및 조치결과를 개인정보처리시스템 책임자에게 보고하고, 개인정보처리시스템 책임자는 이를 향후 위기대응 체계에 반영 검토
- 위기상황으로 인한 피해를 수습하고 위기내용 조직학습 실시
 - 개인정보처리시스템 책임자는 재해·재난으로 인한 개인정보처리시스템의 개인정보 침해 발생에 대한 피해 수습
 - 위기내용 재발 방지 및 피해 최소화를 위한 기관 교육 실시

III. 위기대응 체계

1. 개인정보처리시스템 구성

- 홈페이지 및 시스템
- 전산망 : 인터넷망 및 내부 업무 전산망

개인정보처리시스템	URL
학사.행정 포털 시스템	https://ktis.kookje.ac.kr

- 개인정보처리시스템의 변경 사항은 ‘붙임1(개인정보처리시스템 현황)’에 기록하여 유지·관리해야 함.

2. 위기대응 조직 구성 및 역할

구분	역 할
개인정보처리시스템 책임자	<ul style="list-style-type: none"> • 소관 개인정보처리시스템 위기대응 업무의 총괄 • 위기선포 및 위기대응 조직 구성원에게 업무를 지시 • 위기대응 상황 종료 시 결과를 공유 • 위기 발생 시 사고 처리 및 예방에 대한 총괄책임
개인정보처리시스템 담당자	<ul style="list-style-type: none"> • 위기상황 발생 시 각 업무기능의 복구 총괄 • 책임자의 위기선포에 따라 위기상황 전파 • 유관 기관과 연락망 가동 및 정보공유 • 평상 시 위기대응 절차 및 계획의 검토 • 위기 발생 시 사고 분석, 대응, 복구 등의 처리와 재발방지에 대한 책임
기술담당자	<ul style="list-style-type: none"> • 개인정보처리시스템의 백업, 기술적 복구 및 운용 담당 • 책임자 및 담당자의 지시에 따라 필요한 활동 지원

3. 재난.재해에 따른 파급효과 및 초기대응

가. 위기의 정의

- 재해·재난으로 인한 개인정보처리시스템 위기는 아래와 같이 손실, 유출 및 훼손, 중단으로 구분됨

영역	위기	재해.재난 발생 시 파급효과	초기대응 방안
개인정보	유출	재해·재난으로 인해 개인정보가 유출된 경우	<ul style="list-style-type: none"> • 개인정보 침해사고 대응절차의 [붙임 4] 긴급대응 조치 방법의 개인정보 유출에 따라 대응
	손실 및 훼손	재해·재난으로 인해 개인정보가 유출되지는 않았으나 전부 또는 일부가 사용할 수 없게 된 경우	<ul style="list-style-type: none"> • 손실범위 확인 (25%/50%/75%) • 긴급복구 진행 확인
서비스	중단	재해·재난으로 인해 개인정보 자체는 안전하게 보관되고 있지만 서버 또는 네트워크의 장애 등으로 인해 서비스가 제공되지 못하는 경우	<ul style="list-style-type: none"> • 장애 위치 확인 • 긴급 절차로 서비스 제공 • 장애 복구 진행

나. 위기 등급 분류

심각도	시스템 중요도	심각도 상태
심각도1	1등급	<ul style="list-style-type: none"> • 시스템 전체 혹은 일부의 사용불가
	1등급	<ul style="list-style-type: none"> • 75% 이상의 사용자의 어플리케이션 접속 불가능 • 75% 이상의 개인정보 손실 및 훼손
심각도2	1등급	<ul style="list-style-type: none"> • 즉각적이지는 않지만 중요한 시스템의 핵심부분이 기능적으로 정확히 동작하지 않으며, 그로 인하여 일부 업무에 영향을

		끼치는 상태
	2등급	<ul style="list-style-type: none"> 시스템 혹은 일부의 사용 불가
	2등급	<ul style="list-style-type: none"> 50%이상의 사용자의 어플리케이션 접속 불가능 75%이상의 개인정보 손실 및 훼손
심각도3	2등급	<ul style="list-style-type: none"> 즉각적이지는 않지만 중요한 시스템의 핵심부분이 기능적으로 정확히 동작하지 않으며, 그로 인하여 일부 업무에 영향을 끼치는 상태
	3등급	<ul style="list-style-type: none"> 시스템 전체 혹은 일부의 사용 불가
	3등급	<ul style="list-style-type: none"> 25%이상의 사용자의 어플리케이션 접속 불가능 25%이상의 개인정보 손실 및 훼손

다. 위기 등급에 따른 대응

- 개인정보처리시스템 담당자는 위기 상황에 대한 등급에 따라 대응계획을 수립해야 함

심각도	대응 수준
심각도1	<ul style="list-style-type: none"> 발생 즉시 CPO에게 보고 CPO가 공식적인 위기 상황 선포 및 대응 총괄 필요시 외부 전문가 포함 위기대응팀 구성 위기 종료 후 사후 조치 계획 수립 및 이행
심각도2	<ul style="list-style-type: none"> 정보화관리부 수준에서 대응, 필요한 경우 CPO에게 보고 위기대응팀 구성 위기 종료 후 CPO에게 공식 보고
심각도3	<ul style="list-style-type: none"> 개인정보보호 담당자 수준에서 대응 해당 개인정보처리시스템 담당자로 위기대응팀 구성 위기 종료 후 학술정보센터 부장에게 보고

4. 복구목표의 설정

가. 백업 및 복구 우선순위

- 개인정보처리시스템 책임자는 개인정보처리시스템의 위기 상황 발생 시 신속한 대응 및 복구를 위해 복구목표시간(RTO) 및 복구목표시점(RPO)을 정하고 복구 방안을 마련하여야 함
- 복구목표는 개인정보처리시스템별 긴급성, 업무 영향도를 고려하여 우선순위를 정해야 하며 위기선포 시부터 적용함

나. 복구목표시간 (RTO : Recovery Time Objective)

- 업무 중단 시점부터 업무를 복구하기 위한 목표 시간
- 개인정보처리시스템의 책임자는 업무 영향도를 고려하여 담당 시스템의 복구목표 시간을 조정
- 개인정보보호담당자는 업무 영향도를 고려하여 기관 전산 장비의 복구목표시간을 조정

다. 복구목표시점 (RPO : Recovery Point Objective)

- 업무를 계속적으로 수행하기 위해 손실된 데이터에 대한 유실 허용시점
- 개인정보처리시스템의 책임자는 업무 영향도를 고려하여 담당 시스템의 복구목표 시점을 정의

5. 백업 및 복구방안

가. 개인정보 및 전산실 장비 백업 방안

- 소관분야 업무시스템담당자는 개인정보처리시스템 및 모든 전산 장비에 대해 복구목표 시점을 주기적으로 Backup 수행
- 백업은 전산실 및 IDC의 백업서버 및 별도 저장장치에 보관
- '서식2(백업 관리대장)'의 관리대장을 전산실 및 IDC에 비치하여 백업 후 기록 · 전산실 및 IDC 운영자는 백업을 수행하고 백업 대장을 관리하고 월단위로 시스템 담당자에게 보고

나. 개인정보 복구 방안

- 개별 개인정보처리시스템 담당자는 담당 개인정보처리시스템 내 개인정보의
- 손실 범위를 확인하고 개인정보보호 담당자에게 복구를 요청
- 개별 개인정보처리시스템 담당자는 개인정보처리시스템 내 개인정보의 복구를 확인하고 결과를 보고 개별 개인정보처리시스템 담당자는 개인정보보호 담당자와 협업하여 전체 복구 완료를 확인하고 결과를 CPO에게 보고

다. 서비스 복구 방안

- 개별 개인정보처리시스템 담당자는 담당 개인정보서비스가 중단된 경우 개인정보보호 담당자에게 보고
- 개인정보보호 담당자는 전산실 및 IDC 담당자와 협업하여 장애 위치를 확인 (필요 시 협의 하여 비상가동 및 장애 복구)

6. 위기대응 훈련

가. 위기대응 훈련 원칙

- 개인정보처리시스템의 위기가 발생하는 경우 피해를 최소화하고 신속하게 복구하기 위해 주기적으로 위기대응 훈련을 실시해야 함
- 평시 서비스 운영 중에 재해·재난 복구시스템이 정상 작동되는지 확인해야하며 위기상황 발생 시와 동일하게 위기대응 조직의 역할을 수행해야 함
- 위기대응 훈련 시에는 다음의 사항을 유의하여 실시해야 함
 - ✓ 실제 발생 가능한 사고에 대한 위기 시나리오를 통한 정기적 점검

- ✓ 재난·재해 복구시스템의 정상 작동
- ✓ 위기대응 조직 구성원별 역할 숙지
- ✓ 복구목표의 달성
- ✓ 실 데이터의 안정성 보존
- ✓ 비상 연락망 정상 가동상황
- ✓ 위기대응 체계 운용 시 이슈사항
- ✓ 위기대응 훈련 종료 후 훈련 시 도출된 미흡사항 및 이슈사항을 위기대응 체계에 반영 하여 개선함으로써 사후처리 및 지속관리에 활용

나. 위기대응 훈련

- 내부전산실의 재해복구를 위한 모의훈련을 수행함
- 재해복구 모의훈련은 년 1회 실시함
- 모의훈련은 4가지 유형 중에서 매년 연 초에 계획을 수립하여 수행함
 - ✓ 체크리스트(Checklist) 훈련: 재해복구를 위한 계획서를 검토하는 것으로 시스템 구성 변경 발생시, 다른 부서와의 기능적 공유 확인 등의 사유에 따른 확인 및 자체적인 평가를 위 해 수행함
 - ✓ 역할수행(Role Play) 훈련: 재해 상황별 시나리오에 의해 관련 담당자들의 역할과 행동절 차를 수행하는 훈련으로 시스템 환경, 인력운영 등의 이유로 모의전환 또는 실전환 훈련 을 실시하기 어려운 경우에 수행함
 - ✓ 모의전환 훈련: 모의전환 훈련은 전산실의 장비가 파손되어 교체한다는 시나리오를 기 반 으로 기존의 서비스를 유지하면서 별도의 네트워크를 구축하여 기존의 환경을 이관함. 실제 단계별로 전환 수행이 적절히 이루어지는지, 두 네트워크간 환경파일의 정합성이 보장 되는지 등의 절차와 기능을 검토함

○ 모의훈련 절차

순서	훈련방법	수행내용	주관자
1	사전준비	<ul style="list-style-type: none"> • 업무 영향도 파악 • 일정 및 방법 협의 • 관련 상세 작업계획 작성 및 승인 	개인정보보호 담당자
2	재해선언	<ul style="list-style-type: none"> • 재해선포 및 통보 	개인정보보호 책임자
3	재해복구 가동	<ul style="list-style-type: none"> • 재해복구 가동작업 실시함 	학술정보원
4	업무테스트	<ul style="list-style-type: none"> • 자체테스트 실시, 정상유무 판단 	학술정보원
5	정상여부	<ul style="list-style-type: none"> • 재해복구 업무 수행여부 모니터링 	학술정보원

	모니터링		
6	재해복구 중단	<ul style="list-style-type: none"> 재해복구 가동 중지 	학술정보원
7	업무 복귀	<ul style="list-style-type: none"> 복기 작업 실시 	전체
8	결과정리	<ul style="list-style-type: none"> 일정, 절차 훈련결과 정리 미진사항 확인 및 조치 	개인정보보호 담당자

7. 비상연락망 구성

- 개인정보처리시스템 담당자는 위기대응 조직원, 유관 기관, 관련 업체 등으로 이뤄진 ‘붙임3(비상연락망)’ 에 기록관리 해야 함
- 개인정보처리시스템 담당자는 비상연락망을 주기적으로 검토하고 평상시에도 연락체계를 활용하여 정보를 공유해야 함
- 위기상황 발생 시 위기상황 종료 시까지 비상연락망을 가동하여 신속한 대응을 지원해야 함

[붙임 1] 개인정보처리시스템 구성 현황

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

우선 순서	시스템명	개인정보 보유량	민감·고유식별 정보 포함 여부	주된 시스템 연계장비·설비 등
1	학사·행정포털 시스템	186,344	포함	WEB, WAS, DB서버

[붙임 3] 비상연락망

○ 개인정보처리시스템 관리 기관(부서) 비상대책반 연락망

구분	직위	성명	전화번호	휴대폰
개인정보보호 책임자	사무처장	한봉희	031-6108-104	
정보보안 책임자	학술정보원장	김성철	031-6108-086	
개인정보보호 담당자	사무팀장	김태형	031-6108-736	
정보보안 담당자	전산정보팀장	정정환	031-6129-434	
개인정보보호 분야별 책임자	기획처장	장미혜	031-6108-107	
	교학처장	황호성	031-6108-111	
	입시홍보처장	김연수	031-6108-110	
	산학취업처장	이종대	031-6108-109	
	평생교육원장	오경숙	031-6108-105	
	각 학과장	각 학과	과사무실	
개인정보보호 분야별 취급자	기획과장	안병준	031-6108-096	
	시설관리팀장	이영학	031-6108-119	
	교학1팀장	황해룡	031-6108-710	
	교학2팀장	김택영	031-6108-721	
	입시홍보팀장	노정우	031-6108-701	
	산학취업과장	강병호	031-6129-352	
	현장실습팀장	임영웅	031-6129-460	
	취업팀장	신동철	031-6129-272	
	평생교육원부장	안명준	031-6129-249	
	평생교육원팀장	이준우	031-6108-726	
	학술정보원팀장	한경택	031-6108-727	
	국제교류센터팀장	김경민	031-6129-440	
	학생생활관팀장	고영우	031-6129-426	
	각 학과	조교	과사무실	

○ 협력업체

구분	업체명	담당자	연락처
서버	고우넷	신○왕	010-6309-****
네트워크	엑스퍼넷	허○영	010-7221-****
학사.행정 시스템	아이디노	최○달	070-7834-****
정보보안	아이티베이	강○구	010-6325-****
	아이앤테크	최○혁	010-5326-****
	포시스	박○태	010-9282-****