

# **재해 · 재난 대비 개인정보처리시스템 위기대응 매뉴얼**

2020. 06

[illegible]

# I. 개 요

## 1. 목적

- 갑작스런 재난 재해 또는 부정한 목적의 인위적인 위협로부터 개인정보 처리시스템을 보호하기 위하여 재난 재해 사항을 체계적으로 정립하고, 피해를 최소화할 수 있도록 한국환경정책·평가연구원(이하 연구원)이 효율적으로 대응하기 위한 대응절차와 조치사항을 규정

## 2. 관련 법규 등 규정

- 「개인정보보호법」 (제29조)
- 「개인정보보호법 시행령」 (제30조)
- 「개인정보의 안정성 확보조치 기준」 (제12조 1항)
- 「전산보안업무규칙」 (KEI)
- 「정보시스템 긴급 재난복구 계획(안)」 (KEI)
- 「개인정보 침해대응 절차서」 (KEI)
- 「개인정보 보호지침」 (KEI)

## 3. 적용범위

- 본 매뉴얼에서 정의한 재해·재난 발생 시 개인정보처리시스템의 운영 및 관리에 한하여 위기 상황 해제 시까지 개인정보처리시스템의 운영에 필요한 모든 행동요령을 포함

## 4. 용어 정의

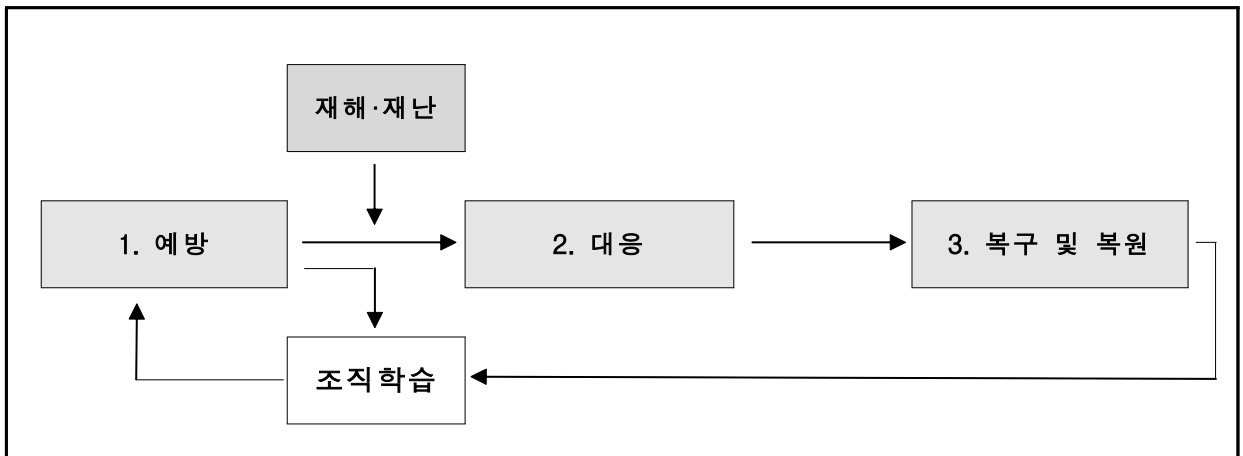
- 재해·재난 : 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고

- 개인정보처리시스템 위기 : 개인정보처리시스템이 장애로 인해 가동이 전면 중단되거나 중단 가능한 시간을 초과하는 경우
- 재해복구시스템 : 재해·재난 발생 시 데이터를 보존하고 자동 복구하는 장치
- 백업 : 잘못되거나 부주의한 조작으로 인하여 데이터가 손실될 것에 대비하여 미리 남겨둔 복사본

## II. 위기대응 절차

### 1. 절차 개요

#### ○ 개인정보처리시스템 위기대응 절차



### 2. 단계별 정의

#### ○ 1단계 : 예방

- 위기상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비
- 위기대응 조직, 위기등급, 복구목표 등 위기대응 체계 검토
- 주기적 백업 실시 및 위기대응 훈련 실시를 통해 위기대응 준비

#### ○ 2단계 : 대응

- 재해·재난으로 위기상황이 발생하여 위기대응 체계에 따라 대응 실시
- 위기대응 조직을 소집하고 위기등급을 정의하여 위기상황 선포
- 비상연락체계를 가동하고 위기대응 조직의 역할에 따라 대응 실시

#### ○ 3단계 : 복구 및 복원

- 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시

- 복구 및 복원이 완료되면 위기상황의 종료를 선언하고 위기대응 시 이슈사항을 위기대응 체계에 반영하여 개선
- 위기상황으로 인한 피해를 수습하고 위기내용 학습

### III. 위기대응 체계

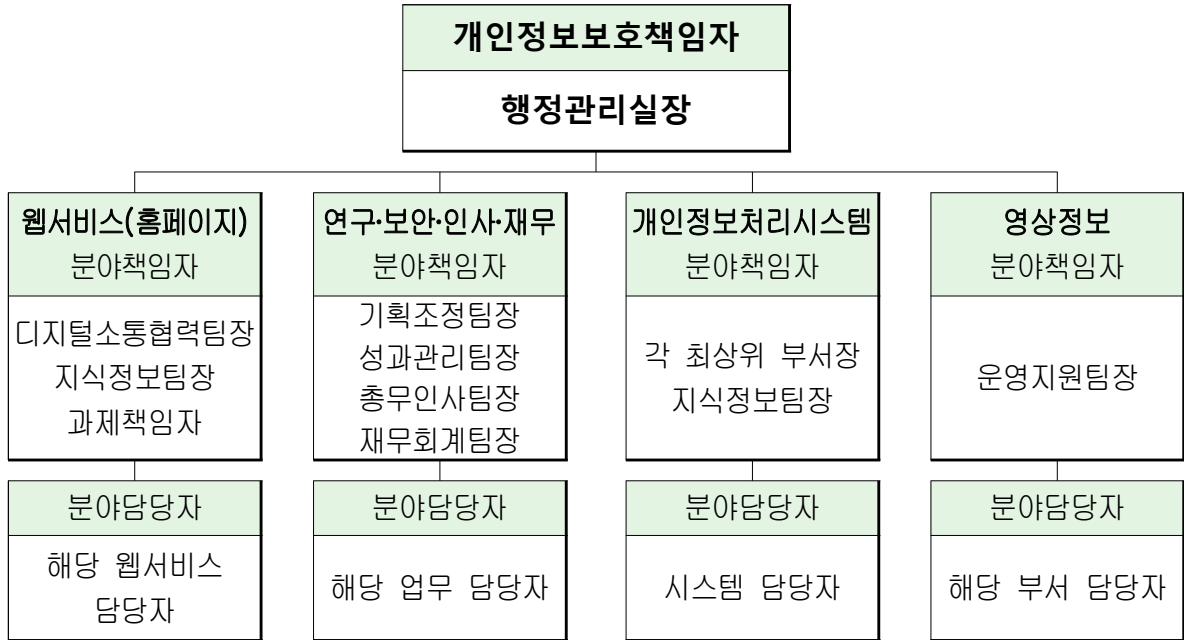
#### 1. 개인정보처리시스템 구성

##### ○ 홈페이지 및 원내 업무 시스템

번호	사이트명	URL	비고
1	KEI 대표홈페이지	www.kei.re.kr	
2	KEI 온라인 채용시스템	keirecruit.kei.re.kr:8091	
3	환경평가검토정보 (EIA)	eia.kei.re.kr	
4	국가기후변화적응센터	kaccc.kei.re.kr	
5	사이버환경정책교육원	cyberedu.kei.re.kr	
6	기후변화 리스크 평가지원 도구	cras.kei.re.kr	
7	KEI 외부전문가 풀	업무시스템	

## 2. 위기대응 조직의 구성

### ○ 개인정보보호업무 수행 체계도



### ○ 재난·재해 발생시 업무 담당자별 역할

구 분	역 할
개인정보처리시스템 책임자	<ul style="list-style-type: none"> <li>- 위기대응 업무의 총괄</li> <li>- 위기선포 및 위기대응 조직 구성원에게 업무를 지시</li> <li>- 위기대응 상황 종료 시 결과를 공유</li> </ul>
개인정보처리시스템 분야책임자	<ul style="list-style-type: none"> <li>- 위기상황 발생 시 각 업무기능의 복구 총괄</li> <li>- 책임자의 위기선포에 따라 위기상황 전파</li> <li>- 유관 기관과 연락망 가동 및 정보공유</li> <li>- 평상 시 위기대응 절차 및 계획의 검토</li> </ul>
개인정보보호 담당자	<ul style="list-style-type: none"> <li>- 위기 사항 보고 및 전파</li> <li>- 평상 시 위기대응 계획 수립 및 검토</li> </ul>
분야담당자	<ul style="list-style-type: none"> <li>- 개인정보처리시스템의 기술적 복구 및 운용 담당</li> <li>- 책임자 및 담당자 지시에 따라 필요한 활동 지원</li> </ul>

## 2. 위기등급의 분류

### ○ 위기등급

구 분	역 할
1등급	<ul style="list-style-type: none"> <li>- 개인정보처리시스템 장애시간이 지정시간 이상 지속되는 경우</li> <li>- 개인정보처리시스템 운용의 전면 중단</li> <li>- 데이터의 중대한 손상으로 복구 불가</li> <li>- 개인정보처리시스템 장비의 전원공급 단절</li> </ul>
2등급	<ul style="list-style-type: none"> <li>- 개인정보처리시스템 장애시간이 지정시간 이하로 지속되는 경우</li> <li>- 개인정보처리시스템 운용 시 일부 기능 작동 중단</li> <li>- 데이터의 일부 손상으로 복구 필요</li> <li>- 개인정보처리시스템 장비의 전원공급 이상</li> </ul>
3등급	<ul style="list-style-type: none"> <li>- 개인정보처리시스템 장애가 일시적으로 발생한 경우</li> <li>- 개인정보처리시스템의 운용이 일시적 작동 중단</li> <li>- 데이터의 경미한 손상이나 운영에 지장 없음</li> </ul>

## 3. 복구목표의 설정

### ○ 재해·재난 시 복구목표시간 및 시점 분류

위험요소	분 류	복구목표시간(RTO)	복구목표시점(RPO)	위기등급
재난 재해	화재/폭발	국지적 화재/피해	화재소화 매뉴얼 수행	2등급
		광범위 피해	시스템 재구성 및 백업복구 매뉴얼 수행	1등급
	홍수/누수	누수 소량 시	장애 복구 매뉴얼 수행	2등급
		서버실 침수	시스템 재구성 및 백업복구 매뉴얼 수행	1등급



	정 전	1시간 미만	장애 복구 매뉴얼 수행	2등급
		1시간 이상	서비스중지-시스템다운-절차서수행	1등급
	지진/파손	부분 파손	장애 복구 매뉴얼 수행	2등급
		전소 및 대형파손	시스템 재구성 및 백업복구 매뉴얼 수행	1등급

## 4. 복구 및 백업관리

### ○ 백업 및 복구 우선순위

- 개인정보처리시스템의 복구 순위는 [붙임1] 개인정보처리시스템 구성 현황의 중요도 등급을 따름

### ○ 한국환경정책·평가연구원의 업무연속성 목표시간은 다음과 같음

- 핵심업무는 데이터 유실이 없어야 하고, 24시간 이내에 복구 목표로 구축
- 주요업무는 데이터 유실이 없어야 하고, 7일 이내 복구 목표로 구축
- 일반업무는 백업 및 소산 데이터로 복구 목표시간 없이 서비스를 복구

### ○ 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

### ○ 복구목표시점(RPO : Recovery Point Objective)

- 업무를 계속적으로 수행하기 위해 손실된 데이터에 대한 유실 허용 시점

- 개인정보처리시스템의 책임자는 업무 영향도를 고려하여 담당 시스템의 복구목표 시점을 정의

## ○ 피해수준별 복구방법

피해수준	복구방법	복구 절차
데이터 손상	데이터복구	· 백업 데이터로부터 자료 복원
운영체제/프로그램 오류발생	어플리케이션 복구	· 백신프로그램을 이용, 악성코드 제거 · 공격에 의한 취약점 제거 · 어플리케이션 소스 및 DB 복원을 통한 수정·재설치 · 어플리케이션 복구 확인
운영체제 복구불가능	운영체제 재설치	· 운영체제 및 응용프로그램 재설치 · 백업 데이터로부터 자료 복원 · 운영체제 재설치 완료 후 정상상태 복귀 확인
하드웨어 손상	하드웨어 교체	· 동일 하드웨어로 교체

## ○ 백업관리

- 모든 서버 공통 주 1회 Full 백업 / 주 6회 증분백업 / 보관주기 6개월  
'붙임4(한국환경정책·평가연구원 정보시스템 긴급 재난복구 계획 참조)'

## 5. 위기대응훈련

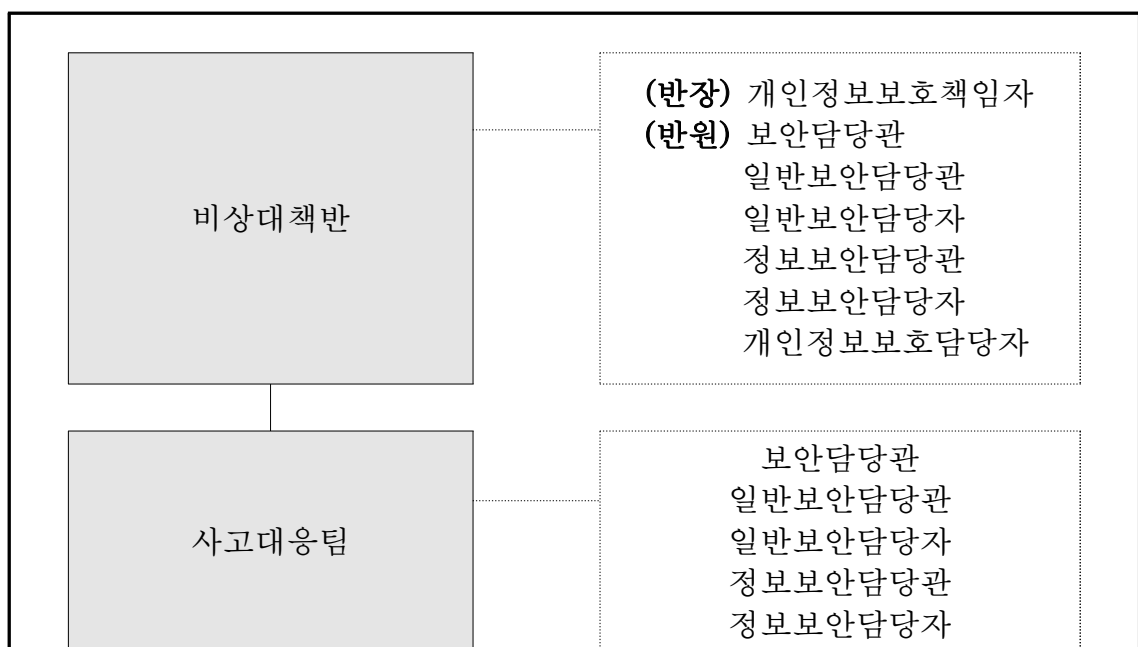
- 개인정보처리시스템의 위기가 발생하는 경우 피해를 최소화 하고 신속한 복구를 위해 주기적으로(연 1회 이상) 정전대비· 장애발생 등 위기대응 훈련을 실시해야 함
- 위기대응 훈련 시에는 평시 서비스 운영 중에 재해·재난 복구

시스템이 정상 작동되는지 확인해야 하며 위기상황 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
  - 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 반영하여 개선해야 함

## 6. 비상대응 인적 조직

- 재해·재난 위기 발생 시 신속히 복구조직을 구성 및 운영
- 비상연락망을 통해 재난·재해 발생 시 유기적으로 협조하여 신속히 복구를 할 수 있도록 해야 함 ‘붙임3(비상연락망 참조)’



	<p>개인정보보호담당자 정보시스템 관리자 운영지원팀 유지보수 업체</p>
--	--

○ 재해·재난 복구 업무

- 개인정보시스템 운영 인력 소집
- H/W 기능상태 파악/피해 정보 수집
- 복구 소요시간 예측 및 보고

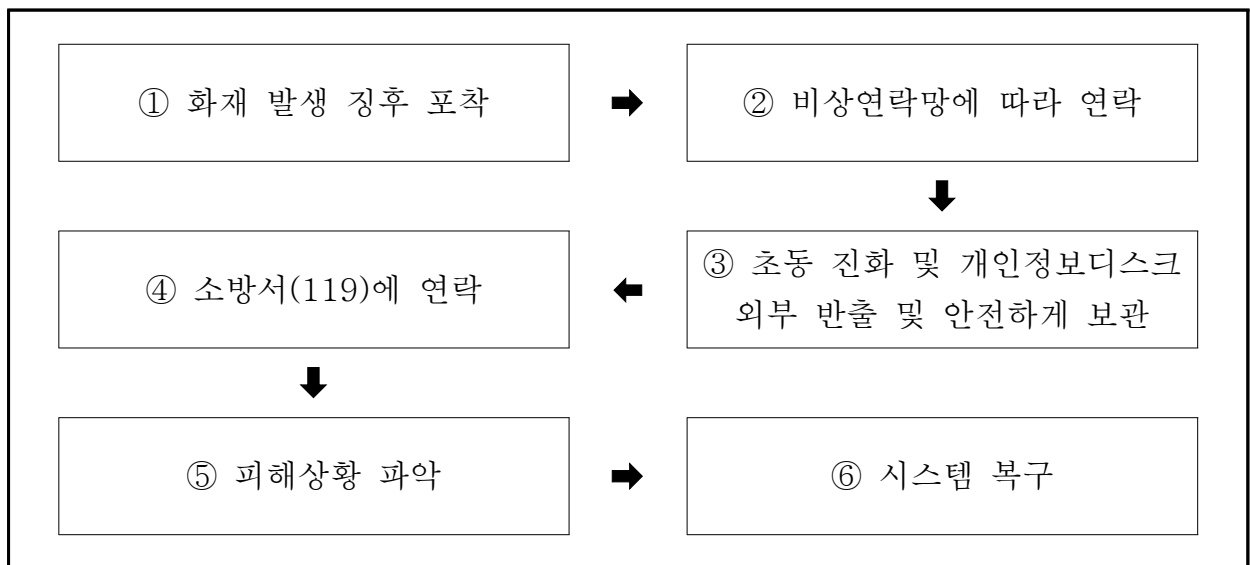
○ 개인정보시스템 복구 및 재배치 업무

- 장비, 유실 소스 데이터 관련 초기 피해 상황 관리
- DB 및 File의 상태 분석 및 데이터의 분석
- 개인정보 관련 전산장비 가동 불가능 시 데이터 백업 복구 실시
- 상실된 개인정보 데이터를 조사하고 운용 가능 시스템으로 재배치

## IV. 재난·재해 위기 대응 상황별 매뉴얼

### 1. 화재 발생시 대응 매뉴얼

#### ○ 화재 사고 대응 흐름도



#### ○ 부분적 화재시

- 작은 화재시 실내 비치된 소화기를 이용하여 조기 진압한다.
- 초기 진화가 어려울 경우 비상연락망에 의거 연락한다.

① 소화를 붙이 난 곳으로 옮깁니다.	② 손잡이 부분의 안전핀을 뽑습니다.
	

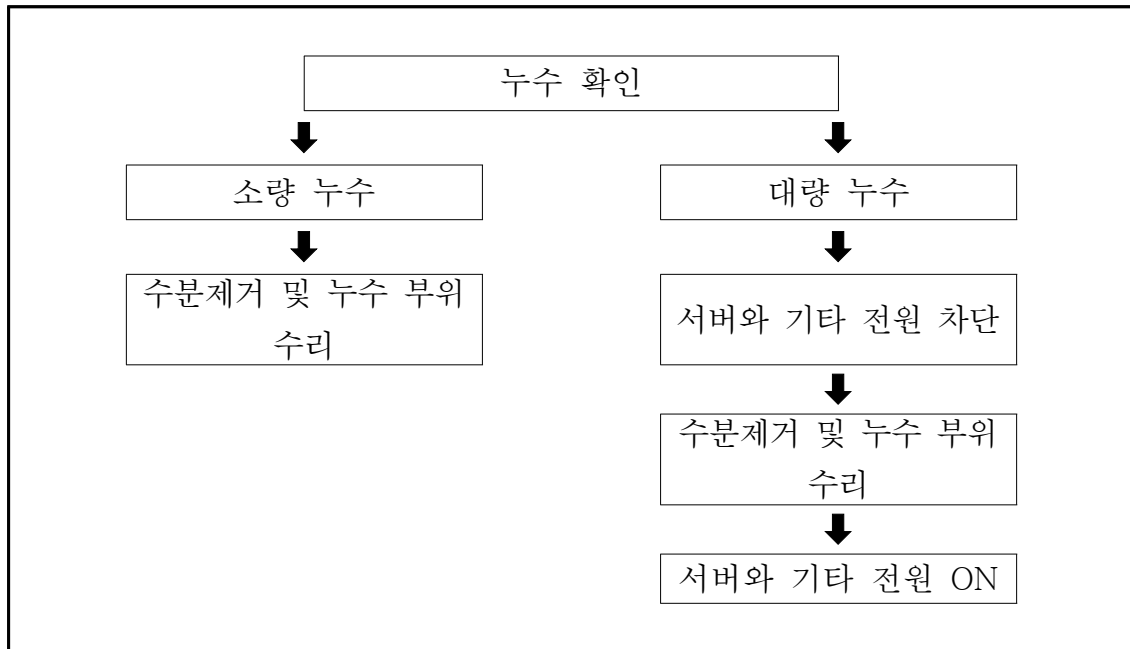
<p>③ 바람을 등지고 몸에서 멀리 팔을 최대한으로 뻗어 호스를 불쪽으로 향합니다.</p>	<p>④ 손잡이를 힘껏 움켜쥐고 비로 쓸어내듯 뿔어 냅니다.</p>
	

## ○ 대형 화재시

- 소방서(119)로 신고한다.
- 화재가 번져 전기시설물 및 2차적인 문제가 야기 될 수 있는 곳은 전원 OFF 한다.
- 반출 우선순위에 의거 개인정보처리시스템 및 개인정보가 담긴 Media 등을 반출한다.

## 2. 누수시 대응 매뉴얼

### ○ 누수시 대응 흐름도



### ○ 소량 누수 시

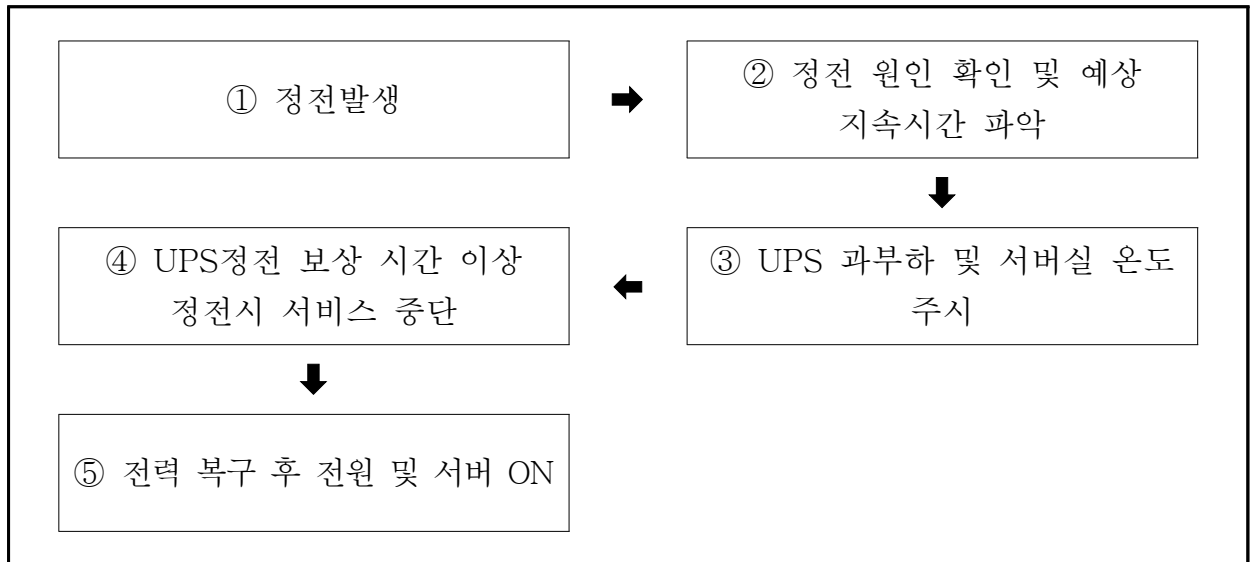
- 소량 누수 시 수분을 제거하고, 가습기나 기타 부품의 누수여부를 확인하여 유지보수업체에 교체할 것을 요구
- 서버실 바닥 침수 여부를 확인하여 침수가 확인된다면 누수로 인해 전기시설물 및 2차적인 문제가 야기될 수 있는 곳은 전원을 OFF
- 신속히 수분을 제거한 후 전원 ON

### ○ 시스템실 전체 침수 시

- 시스템중지 및 전원차단, 백업복구수행

### 3. 정전시 대응 매뉴얼

#### ○ 정전시 대응 흐름도



#### ○ 정전유형별 대처요령

- UPS정전 보상 시간 미만 정전 예상
  - 1) 자동으로 UPS 충전지 배터리로 전원 출력이 전환된다.
  - 2) 한국전력으로 연락하여 예상정전지속 시간을 확인한다.
  - 3) 한국전력 문제가 아니라면 관리사무소로 문의하여 정전지속시간을 확인한다.
  - 4) 서버랙과 UPS를 주시하여 과부하가 걸리는지 주의한다.
  - 5) 항온항습기가 UPS와 연결이 되어있지 않은 관계로 서버실 온 습도를 항시 예의 주시한다.
- PS정전 보상 시간 이상 지속될 것으로 예상될 경우 : 서비스 중지
- UPS 고장
  - 1) 자동으로 바이패스로 절체되어 부하에 공급
  - 2) 신속히 유지보수업체에 연락하여 수리
  - 3) 고장해소 시 다시 자동 또는 수동으로 ON되고 부하를 균등하게 재분배하여 운전
- BYPASS : 신속히 유지보수업체와 연락하여 BYPASS원인을 파악 및 수리



# 붙임 1

## 개인정보처리시스템 구성 현황

우선 순위	시스템 명	개인정보 보유량	중요도	민감·고유식별 정보 포함 여부	주된 시스템 연계 장비·설비 등
1	온라인채용 입사지원서	1,425	가	없음	web, was, DB서버
2	KEI 외부 전문가 풀	1,861	가	없음	web, was, DB서버
3	사이버환경정책 교육원 홈페이지 회원관리	17,480	나	없음	web, was, DB서버
4	대표 홈페이지 뉴스레터 회원관리	15,923	나	없음	web, was, DB서버
5	환경평가검토 정보	1,799	다	없음	web, was, DB서버
6	국가기후변화 적응센터	6,210	다	없음	web, was, DB서버
7	기후변화 리스크 평가지원 도구	191	다	없음	web, was, DB서버

## 백업 관리 대장

[illegible]

## 비 상 연 락 망

작성일 : 2020. 06

### 1. 비상대책반 연락망

구 분	부 서 명	담 당 자	연 락 처
개인정보보호책임자	행정관리실	김 용 구	044-415-7500
보안담당관	행정관리실	김 용 구	044-415-7500
일반보안담당관	총무인사팀	이 영 순	044-415-7510
일반보안담당자	총무인사팀	김 정 두	044-415-7846
정보보안담당관	지식정보팀	천 재 홍	044-415-7604
정보보안담당자	지식정보팀	양 준 모	044-415-7466
개인정보보호담당자	지식정보팀	김 영 인	044-415-7602

### 2. 관련 부서 연락망

구 분	부 서 명	담 당 자	연 락 처
시설·운영담당관	운영지원팀	염 기 웅	044-415-7727
시설·운영담당자	운영지원팀	최 정 욱	044-415-7808

### 3. 유지보수 업체 연락망

업체명	담당자	연락처
(주)아이티트렌드	윤 봉 기	02-2638-5006
(주)아이티트렌드	장 도 원	02-2638-5030

### 4. 유관 공공기관 연락망

기관명	담당자	연락처
국무조정실	강 철	044-200-2792
경제인문·사회연구회	이 수 한	044-211-1330

# 정보시스템 긴급 재난복구 계획(안)

2017. 12.



한국환경정책·평가연구원  
Korea Environment Institute

[illegible]

# 정보시스템 긴급 재난복구 계획(안)

## 제1장 총칙

제1조 (목적) 이 지침은 KEI 정보시스템 긴급재난복구에 관한 절차를 정함을 목적으로 한다.

제2조 (적용범위) 적용범위는 다음 각 호와 같다.

1. 서버시스템의 재난복구
2. 네트워크 시스템의 재난복구
3. 데이터, 어플리케이션 등 정보서비스 재난복구

## 제2장 서버시스템의 재난복구

제3조 (시스템SW백업) ①시스템SW 장애를 대비하기 위해 시스템SW 백업을 실시하여 물리적 접근통제와 화재 등의 위험 요소로부터 보호되는 장소에 보관한다.

②시스템SW백업은 다음 각 호에 따라 실시한다.

1. 백업대상 : 정보서비스를 제공하는 서버로 전자결재시스템, 행정정보시스템, DBMS 시스템, e-mail 시스템 등 주요 정보시스템의 시스템 파티션을 파일단위로 전체 백업한다.
2. 백업주기 : 매주 1회 전체 백업 및 매일 증분 백업을 실시한다.
3. 백업방법 : 백업시스템(VTL기반 - VERITAS NETBACKUP)을 이용하여 1차 백업 후 Tape 드라이브를 이용하여 2차 백업을 실시한다.

제4조(하드웨어 백업) 유지보수 계약을 통해 장애발생 가능성이 있는 파트에 대한 예비 부품을 확보한다.

제5조(시스템SW복구) ①전산서버실과 독립된 별도의 통제된 안전한 공간에 보관된 백업 데이터를 사용하여 복구한다.

②시스템SW 복구는 다음 각 호의 순으로 실시한다.

1. 시스템SW 장애가 발생한 서버의 시스템SW를 재설치 한다.
2. VTL 백업시스템에 백업된 데이터를 이용하여 시스템SW 파일을 재설치한 서버에 복구(recovery)한다.
3. 복구가 완료되면 시스템의 이상 유무를 확인한 후 서비스를 구동한다.

제6조(하드웨어 복구) 서버 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약업체는 대체 하드웨어를 조달하여 신속히 교체 복구한다.

## 제3장 네트워크 시스템의 재난복구

제7조(소프트웨어 백업) ①백업 대상은 인터넷 라우터, 백본 스위치, 방화벽, 웹방화벽 IPS, UTM, DDoS시스템 및 네트워크를 위한 L2 ~ L4 스위치의 설정파일로 한다.

- ①정보시스템 유지보수 시 정기백업(월/분기), 설정 변경 시 (수시백업) 실시한다.
- ②tftp를 통한 백업 또는 자체파일 내려받기를 이용하여 백업한다.
- ③전산서버실에 위치한 별도의 파일서버에 보관한다.

제8조(하드웨어 백업) 유지보수 계약을 통해 장애발생 가능성이 있는 파트에 대한 예비 부품을 확보한다.

제9조(소프트웨어 복구) 서버실 파일서버에 백업된 파일을 사용하여 복구하며, 복구절차는 다음 각 호와 같다.

1. 펌웨어 장애 발생 시스템을 대체 장비로 교체한다.  
(설정 또는 정책파일만 장애시 생략한다.)
2. 백업 받아 두었던 설정파일을 준비한다.
2. 시스템에 적용하고 재부팅 한다.
3. 부팅 후 백업된 설정파일을 적용하여 시스템의 설정을 복구한다.
4. 복구가 완료되면 시스템의 이상 유무를 확인 및 통신상태를 점검한다.
5. 펌웨어 장애 발생 시스템의 펌웨어 작업은 각 유지보수 업체에서 별도로 실시한다.
6. 펌웨어 작업이 완료된 시스템에 설정파일을 적용한다.
7. 설정파일이 적용된 시스템을 테스트한다.
8. 테스트가 완료된 시스템을 대체장비와 서로 교체한다.
9. 장비 장애시점 전과 후를 비교하며, 정상 유무를 판단한다.

제10조(하드웨어 복구) 네트워크 시스템의 하드웨어 장애가 발생했을 경우 유지보수

계약에 의거 계약업체의 대체 하드웨어를 조달하여 신속히 교체 복구한다.

제11조(복구 우선순위) 재난에 의거 다수 지역에서 장애가 동시 발생했을 경우는 다음 각 호의 순에 의거 복구를 시행한다.

1. 인터넷 관문
2. 백본 L2스위치
3. 네트워크 연결을 위한 L2/L3/L4 스위치

## 제4장 데이터, 어플리케이션 등 정보서비스 재난 복구

제12조(백업시스템을 이용한 백업) ①각 주요서버에 대해서 일별 Online 백업, 월별 소산백업을 진행한다.

②중요데이터, 어플리케이션 등 정보서비스는 백업시스템을 이용하여 다음 각 호와 같이 일별 Online 백업을 실시한다.

1. 백업대상은 정보서비스를 제공하는 서버로 별표1과 같으며, 대상은 변경될 수 있다.
2. 백업방법은 백업시스템의 운영환경 및 백업 대상장치 및 백업용량에 따라 설정된 백업 정책에 의해 일별 증분백업 및 주별 일괄백업을 수행한다.
3. 백업주기는 별표1과 같다.

③월1회 주기로 백업시스템을 이용하여 백업된 데이터들에 대해서 다음 각 호와 같이 소산 백업을 실시한다.

1. 백업 대상 데이터는 백업시스템에 보관중인 모든 백업데이터로 한다.
2. 소산 백업방법은 백업시스템의 백업 데이터복사기능을 이용하여 소산용 Tape 드라이브의 미디어에 백업데이터 복사한다.
3. 백업 데이터를 재 백업(이중 백업)한 Tape 드라이브의 미디어는 독립된 별도의 통제된 안전한 공간에 보관한다.

④소산 백업한 백업데이터 복사본은 전산서버실과 백업서버실에 격월로 보관하며 다음 각 호와 같이 처리한다.

- 1.보관방법은 전산서버실과 백업서버실에 이중 보관한다.
- 2.보관주기는 1개월로 한다.

제13조 (재난·재해 시 백업시스템을 이용한 복구)

①백업시스템(VERITAS NETBACKUP) 솔루션은 데이터 복사가 가능한 솔루션으로



데이터를 독립된 별도의 통제된 안전한 공간에 독립된 Tape 드라이브에 이중 복사하여 보관한다.

②백업대상서버는 전자결재시스템, 행정정보시스템, DBMS 시스템, e-mail 시스템, KETI 대표 홈페이지 등 KETI에서 운영하고 있는 정보시스템 서버들이다.

③백업대상파일은 별표1과 같다.

④백업방법은 전산서버실과 백업서버실 스케줄에 의한 데이터를 복사 및 보관한다.

제14조(사용자실수에 의한 데이터 손실복구) 백업시스템에 의해 백업된 데이터를 사용하여 다음 각 호와 같이 복구를 실시한다.

1. 주기적인 백업을 수행한 백업 데이터를 이용하여 데이터 복구를 수행한다.
2. 데이터가 소실된 대상 서버에서 백업시스템 복구명령 또는 GUI 매니저를 이용하여 손실된 데이터(파일 또는 파일 시스템)를 복구한다.
3. 복구된 데이터에 대한 정합성 및 활용성 테스트를 진행한다.

제15조(재난에 의한 데이터 손실 복구) ①백업시스템과 Tape 드라이브에 저장된 백업데이터를 사용하여 복구한다.

②시스템 하드웨어와 데이터의 완전 파손 시 백업시스템에 백업된 데이터를 사용하여 다음의 순서로 복구를 진행한다.

1. 유지보수 계약업체를 통해 파손된 하드웨어의 대체 하드웨어를 신속하게 준비한다.
2. 시스템 OS 복구는 서버 시스템의 재난복구계획을 참조한다.
3. 데이터, 어플리케이션의 복구는 준비된 시스템에 백업시스템을 사용하여 백업데이터를 순서에 따라 복구한다.
4. 데이터 복구 완료 시 해당 시스템에 대한 어플리케이션 서비스를 재개한다.

## 부 칙

①(시행일) 이 지침은 2014년 4월 18일부터 시행한다.

## 부 칙

①(시행일) 이 지침은 2017년 12월부터 시행한다.