개정이력

차수	재(개)정 일자	시행일자	주요 개정 내용
1	2024-08-03	2024-08-03	초도 제정

목 차

1. 개요

1.1 목적

본 지침서는 정보시스템의 서비스의 연속성을 보장하고, 재해복구에 대한 신속한 대응절차 및 재발방지를 통하여 정보시스템의 보안성과 안정성을 유지하는데 목적을 둔다.

1.2 적용범위

사내 모든 IT자산과 이를 관리하는 운영 담당자 및 정보보안 유관 부서들을 대상으로 한다.

1.3 책임 및 권한

1.3.1 CSO

1) 재해에 대비하여 평상시에는 모의 훈련을 총괄하고, 재해 복구 계획수립 및 대응을 총괄한다.

2) 재해발생시 재해복구대응 조직을 소집하고 대응 및 복구를 지휘한다.

1.3.2 정보보안그룹

1) 재해발생 모의 훈련을 주관하고, 각 정보시스템의 신속한 재해 대응 및 복구를 실시한다.

2) 필요시 대외 복구 전문기관의 도움을 받는다.

1.3.3 모든 임직원

1) 복구 대응 조직이 신속하고 정확한 복구가 이루어 질수 있도록 적극적으로 협력한다.

2) 복구가 완료되기 전까지 해당 시스템에 접근 및 제어를 금하도록 한다.

1.4 재해복구 대응 조직 구성

1.4.1 재해복구 대응조직은 CSO, 정보보안그룹(기술보안담당자, 관리보안담당자, 물리보안담당자), 각 부서 정보보안담당자로 구성한다.

1.4.2 CSO는 재해 선포, 정책 판단, 조직 총괄을 담당한다.

1.4.3 정보보안그룹은 해당 영역의 원인 분석, 복구 및 예방조치를 수행한다.

1.4.4 각 부서 정보보안담당자는 소속 부서의 초동대응을 수행한다.

1.5 조직별 역할 정의

1.5.1 CSO: 재해복구 총괄, 정책 판단, 재해 선포 및 종료

1.5.2 정보보안그룹 : 비상 체제 전환, 훈련 기획 및 실행

1) 기술보안담당자 : 장애 분석, 복구 실행, 자원 동원

2) 관리보안담당자 : 정책 보완, 문서화, 재발방지

3) 물리보안담당자 : 물리적 접근 통제, 구역 모니터링

1.5.3. 각 부서 정보보안담당자 : 소속 부서의 이상 징후 조기 탐지, 최초 상황 전파 및 대응 협조

2. 재해복구 대응 조직 운영

2.1 재해복구의 기준

2.1.1 재해 대응 및 업무 활동의 중단 최소화

2.1.2 대외비 이상의 중요 정보자산 및 업무 프로세스 보호

2.1.3 사내 업무와 연관된 모든 IT자산의 손상이나 파괴로부터 보호

2.2 비상대책 수립 및 운영

2.2.1 인위적 또는 자연적인 원인으로 인한 시스템 장애 발생에 대비하여 시스템 이원화, 백업관리, 복구 등 종합적인 재해방지 대책을 수립·시행하여야 한다.

2.2.2 장애, 재해, 파업, 테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 예방하고,

중단되는 경우 신속하게 복구할 수 있도록 비상대책에 반영해야한다.

1) 비상대응 조직이 구성 및 운용
2) 유관기관 및 관련업체 비상 연락망 구축
3) 재해복구계획(백업 활용)
4) 상황별 대응절차
5) 모의훈련의 실시
6) 보고 및 대외통보의 범위 및 절차

2.2.3 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비 장치를 확보하여야 한다.

2.2.4 비상사태에 대비하여 비상지원 인력확보를 포함한 안전대책을 반영해야한다.

1) 파업시, 핵심 전산 업무 종사자의 근무지 이탈에 따른 시스템 마비를 방지하기 위하여 핵심 전산 업무에 대한 비상지원 인력을 확보하여 운영해야한다.
2) 비상사태 발생시, 핵심 업무 시스템 마비 방지 및 신속한 원상복구 등을 위하여 시스템 운영에 대한 비상지원인력 또는 외부 전문 업체 활용 등 다각적인 방안 운영
3) 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 시스템 운영지침, 사용자 매뉴얼 등을 쉽고 자세하게 작성하고 최신 상태로 유지
4) 비상지원 인력에 대하여 전산 핵심업무 담당자 부재 시 동 업무 수행이 가능할 수 있는 수준으로 교육·훈련을 강화

2.2.5 비상대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신 정보로 유지하고 관리해야한다.

2.3 시스템 장애 대응 절차

2.3.1 대응 조직 및 역할

1) CSO
   ⓐ 장애 상황 전반을 총괄하고, 정책적 판단 및 외부 자원 연계를 지시한다.
2) 정보보안그룹
   ⓐ 장애 원인을 분석하고, 복구 작업을 주도한다.
   ⓑ 필요한 경우 외부 전문기관과의 연계를 추진한다.
3) 각 부서 정보보안담당자
   ⓐ 내 장애 발생 시 즉각 상황을 보고하고 초기 대응에 협조한다.

2.3.2 장애 발생 시 대응 흐름

1) 장애를 최초 인지한 담당자는 정보보안그룹에게 즉시 보고한다.
2) 정보보안그룹은 상황을 파악 후 CSO에게 장애 사실 및 예상 영향 범위를 보고한다.
3) 필요 시 CSO는 비상대응을 지시하고, 복구 작업 착수를 승인한다.

2.3.3 보고, 승인, 복구 및 기록

1) 복구 진행 중 주요 결정 사항은 CSO의 사전 승인을 받는다.
2) 장애 조치가 완료되면 정보보안그룹은 조치 결과 및 피해 내역을 문서화한다.
3) 기록된 장애내역은 추후 재발 방지 분석 및 훈련 자료로 활용한다.

2.3.4 사후 분석 및 재발 방지

1) 장애 처리 후, 정보보안그룹은 장애 원인 및 대응 과정에 대한 분석 회의를 주관한다.
2) 분석 결과는 관련 지침 또는 프로세스 개선에 반영하며, 필요 시 구성원 교육을 실시한다.

3. 재해복구 대응 절차

3.1 재해발생 보고 및 재해선포

3.1.1 각 시스템 업무당담자는 재해 발생시 정보보안그룹에 통보하고 정보보안그룹은 CSO에게 보고한다.

3.1.2 복구 진행시 예상 복구시간이 허용 가능한 범위를 초과하여 정상적인 업무 수행에 지장을 초래하면 정보보안그룹은 보안협의체를 소집하고 CSO는 재해를 선포한다.

3.2 재해대응조직 운영 및 복구

3.2.1 재해가 선포가 되면 재해 대응조직을 가동하역 각 부문 별로 신속한 대응을 진행한다.

3.2.2 CSO는 전체 복구 상황을 총괄하고 최종 정책적인 판단을 한다.

3.2.3 정보보안그룹은 비상체제로 전환하고 각자 맡은 비상조직 임무에 신속히 투입된다.

3.2.4 최초 상황이 발견되었을 때 발견자는 일시, 장소, 사고 내용 등을 비상대응조직에 최대한 자세하고 신속하게 통보한다.

3.2.5 비상조직은 비상연락망 및 비상근무체계를 가동하고, 상황을 신속하게 처리하도록 한다.

3.2.5 상황처리 및 정상적인 업무 연속성을 유지하기 위하여 복구 계획을 세우고 집행한다.

3.2.6 복구중 외부 전문기관의 도움이 필요할 때는 신속하게 CSO에게 보고 및 승인 후 진행하도록 한다.

3.2.7 기술보안 담당자는 장애 및 재해 내역의 기술적 검토와 해결안을 마련하고, 주기적으로 상황을 확인하며, 가용한 인적·물적자원을 동원하여 시스템을 복구한다.

3.3 재해종료 선언 및 사후조치

3.3.1 재해로 인한 수습이 최종 마무리되면 문서화하여 추후 재발을 방지하기 위해 다음과 같이 대응한다.

1) CSO는 재해상황 종료를 선언한다.

2) CSO는 재해 상황이 종료되면 비상대응 조직의 해산을 결정하고 사후 조치한다.

3) 정보보안그룹은 피해상황 정리와 재해발생 조치 보고서를 작성하고, 사후 모니터링을 실시하여 재발 방지에 노력한다.

3.4 업무 영향 평가

3.4.1 재해방지 대책을 정기적으로 시험 및 검토하며, 정보시스템 비상대책에 대한 영향평가를 실시하여야 한다.

3.4.2 재해 또는 장애 발생시, 업무의 영향 정도를 파악하여 우선순위를 기준으로 복구한다.

3.4.3 정보시스템의 복구 절차는 해당 시스템의 운영 지침을 참고하고, 각 시스템의 업무담당자들은 지속적인 교육을 통해 내용을 숙지한다.

4. 모의훈련 및 예방

4.1 모의훈련

4.1.1 정보보안그룹은 재해복구를 위해 연간 모의 훈련 계획을 수립 및 운용한다.

4.1.2 정보시스템 비상대책에 따라 연 1회 해킹, 서비스거부 공격 등 전사적 침해사고에 대비한 비상대응 및 복구 훈련을 실시한다.

4.1.3 모의 훈련 종료 후, 정보보안 그룹은 훈련 결과를 분석하고 도출된 문제점 및 개선방안을 시스템 재해복구계획에 반영하고, 필요에따라 구성원들에게 교육을 실시한다.

4.1.4 정보보안그룹은 업무 내용의 변화를 재해복구계획에 반영하기 위하여 정기적 검토 및 갱신을 실시한다.

4.2 예방

4.2.1 재해 발생 시에도 신속하게 정상 업무가 가능하도록 주요 시스템의 주기적인 점검과 백업을 실시한다.