▣위험 식별 및 대응 방안

주요리스크	대응방안
정보보안 인식 제고 기술의 발전에 따라 정보보안 공격이 다양해지고 있습니다. 이러한 보안 사고는 외부 해킹 뿐만 아니라 내부 임직원으로부터 시작 되는 경우도 많습니다. 시스템 보안과 더불어 임직원의 보안 인식 강화가 요구됩니다.	임직원을 대상으로 정기 정보보안 및 개인정보교육을 진행하고 있으며, PC 패스워드 정책, 부재 시 PC 잠금화면, 책상 위 중요 파일 유무 상태 등의 비정기 내부 보안 감사를 수행합니다. 또한, 개개인의 보안 분별력 제고 및 보안의식 향상을 위해 지속적인 보안 모의훈련을 진행하여 정보보안에 대한 인식을 높여가고 있습니다.
IT 재해복구 및 장애대응 천재 지변이나 인재 발생 시 중요 IT 인프라, 소프트웨어 시스템 등의 작업이 불가능합니다. 미리 자산 가치를 식별하고 재해복구 및 장애 대응서비스를 수립하는 등 비즈니스 연속성 계획 관리가 필요합니다.	비즈니스 연속성 계획(BCP, Business Continuity Planning)을 수립하여 IT 서비스를 중단 없이 수행할 수 있게 정책을 적용하고 있으며, IT센터에 문제가 생기더라도 서비스가 유지될 수 있게 소산지를 운영하여 백업 및 복구를 진행하고 있습니다. 더불어 계획한 복구시점 목표(RPO, Recovery Point Objective)와 복구시간 목표(RTO, Recovery Time Objective)를 맞추기 위해 재해복구 모의훈련을 매년 1회 수행하는 등 최대의 서비스 가용성을 유지하고자 노력하고 있습니다.