R&D전문플랫폼 적용 보안 정책 및 기술

보안관리

○ 자체 보안업무 규정을 준수하고 개인정보보호법에 대한 대응을 지원하기 위해 자체 보안 감시 체계를 수행하고 자체보안 관리 및 통제를 상시화하여 보안위험을 사전예방

○ 정기적 보안점검 활동을 통하여 최적의 보안업무 수행

○ 운영되고 있는 보안 장비와 정보에 대하여 주기적인 안전 점검을 실시하여 보안시스템의 효율적 관리 및 고품질의 보안서비스 제공

침입차단 시스템 정책 점검	보안장비 상태 확인	로그 정보 분석
* 미사용 정책, 취약한 서비스 포트 정책 점검(원격, 공유폴더 등) * Source 및 Service Any 정책 점검 * 원격 접속에 대한 정책 점검	* CPU, Memory, Session 정보 확인 * 비인가자의 접근 정보 확인 * 장비의 보안취약점에 대한 패치 유/무 확인 * 특정 IP에 대한 과도한 접속 유무 파악	* 수집된 이벤트 로그 이상 유무 확인 * 탐지된 Signature에 대한 오탐 내역 분석 * 지정된 장소에 일별 로그 백업 유무 확인 * 로그 데이터 Size 점검 (비정상적으로 클 경우 확인)

물리적 보안

○ 클라우드 센터 출입을 관리하며 출입통제 관리감독 체계 유지

생체인식 출입통제장치, 접근 권한 차등부여, 실시간 보안 이상 징후 모니터링

○ 주요 설비에 대한 비인가자의 접근을 엄격히 제한

○ 내부망에 접근이 가능한 사무실 등은 출입 통제 장치와 CCTV 등 감시 시스템을 설치하여 관리하고 운영

○ 장비 및 데이터 저장 장치에 대한 물리적 접근이 가능한 전산실, 통신장비실, 관제실 등은 출입 통제 장치와 감시 시스템을 포함하여 24시간 관제 인원 상주 및 추가적인 출입 관리를 수행하여 엄격하게 접근을 통제

기술적 보안

서버접근 통제

- 안전한 시스템 운영을 위한 접근 권한 및 계정관리 체계 확보를 통해 보안성 강화와 작업 로깅 및 추적 감사를 통한 즉각적인 대응 체계 구축
- 시스템 사용자는 다음과 같이 구분되며 접근 권한에 차등을 부여함
  * 사용자(임직원)/관리자(시스템관리자)
  * 정보자산 유출방지를 위한 문서·파일 직원 별 조회/수정권한 제공
- 내·외부 사용자에 의한 불법적 자원 접근 및 파괴를 사전에 예방
- 시스템 접근에 대한 감시 및 식별, 접근 요구의 정당성에 대한 확인·승인·기록
  * 접속 경로를 일원화하고 사용자별로 접근 권한을 통제
  * 허용한 권한에 한해 명령어를 통제 설정, 명령어에 대한 감사정책 관리
  * 작업 상세 Audit 정보를 로깅
- 업무 담당자 및 관리자의 사용 로그를 모두 저장하며 수정 불가

- 그 외 계정과 비밀번호에 관한 내용은 정보보안 기본지침 및 상위 규정과 지침 이행
- 365일 24시간 중앙관제 모니터링을 통한 실시간 보안 관제 제공
- 모바일 백신 S/W 및 안티 키로깅 S/W 등 보안솔루션 탑재

DB 접근제어

- 데이터베이스 접근을 제어함으로써 개인정보 DB에 대한 접근 및 권한을 제어하고 SQL 감사 및 로깅 등을 통해 개인정보 유출을 사전에 차단하고 발생 위험을 최소화
- DB에 접근 권한을 가진 사용자가 권한을 남용하여 정보를 유출하거나 변조하는 위협으로부터 보호
- 특정 클라이언트 IP주소 또는 MAC주소, DB 사용자, 애플리케이션, 스케줄에 의한 액세스 권한을 제어
- 인증된 사용자에 대한 접근 허용 및 차단을 제어
- 클라이언트 IP 또는 사용자의 권한으로 차단(DML, DCL, DDL)
- 문자열 매칭 및 정규식 패턴 입력이 가능해야 하며 설정된 패턴 이외의 접근은 허용/차단이 되도록 컨트롤
- 애플리케이션에 관계없이 민감한 개인정보에 대해 Data Masking 처리
- 모든 접속경로에 대해 사용자별 접근통제 및 이력을 관리

DB 암호화

- 내·외부자에 의해 다양한 경로로 유출될 수 있는 개인정보 또는 민감한 정보에 대해 DB 암호화를 수행하여 DB 자체를 보호
- 정보통신망 이용 촉진 및 정보보호 등에 관한 법률의 암호화 대상 준수 철저

  * 비밀번호, 바이오정보, 주민등록번호 및 계좌정보 등의 금융정보 등을 암호화

- 개인정보보호법상의 암호화 대상 준수 철저

  * 주민등록번호, 운전면허번호, 여권번호, 외국인 등록번호 등을 암호화
  * 주요 정보 컬럼을 암호화
  * 암호화 컬럼을 Access한 모든 SQL의 Full Text를 로깅, 암호화 컬럼에 대한 접근대상 및 시간에 대하여 로깅
  * SQL Parsing 정보를 저장하여 추출 정보 로깅
  * 인가된 사용자도 DB에 접속하여 주요 정보에 대한 데이터 검색 시 지정된 건수만 복호화 조회 가능하도록 설정 (복호화 건수 제한, 대량의 데이터 유출 방지)

기타 보안

○ 한국인터넷진흥원(KISA)클라우드 컴퓨팅 서비스 보안요건을 만족

  * 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률-제23조제2항 정보보호에 관한 기준 및 클라우드컴퓨팅서비스 정보보호에 관한 기준

○ 보안 관련 법규를 준수하고 대외 보안 유지에 적극 협조

  * '국가정보보안기본지침','정보보호지침' 등 정보보호 관련 법규 및 행정규칙 준수

○ 보안취약점 진단을 실시하며 진단은 소프트웨어 보안 약점 진단원 수준 이상의 인력이 수행

○ 기술적 보안 취약점 제거 결과는 대외비 관리

○ 개인정보의 처리는 최신의 개인정보보호법을 철저히 준수하며 개인정보 처리업무 위탁에 따라 수탁자, 수집·이용목적, 개인정보 항목, 보유 및 이용기간, 동의 거부할 권리가 있다는 사실 및 거부에 따른 불이익을 필수로 안내 및 수집된 모든 개인정보는 보유기간 경과 시 즉시 파기 처리