**① 기술보호 관리 규정 보유 및 실시 여부**

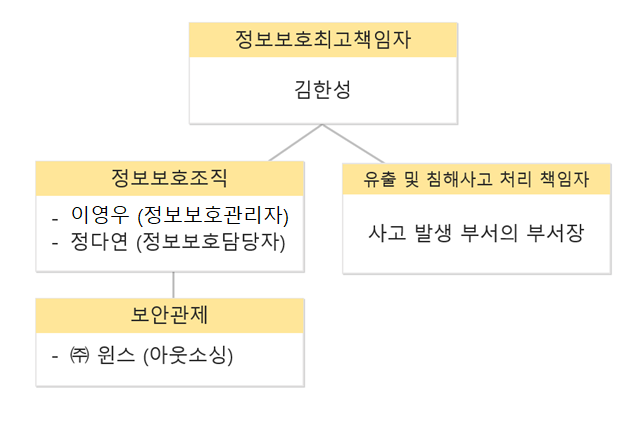
-정보보호 정책 공표 및 실무 지침 제정 (붙임2-1 ‘GME 보안지침 제정.zip’)

**② 보안관리 전담인력 지정 여부(담당자지정 및 보안감사 실시 등)**

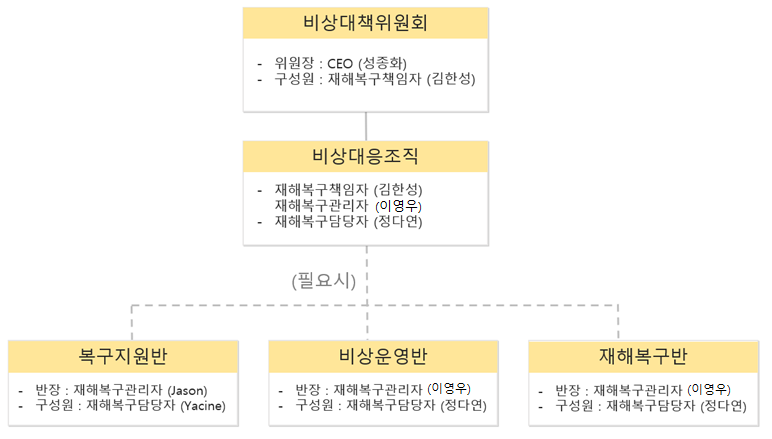
**1) 담당자 지정**

-정보보호조직 운영: 정보보호최고책임자, 정보보호관리자, 정보보호담당자

-침해사고 대응조직 운영



-재해복구조직 운영



**2) 보안감사 실시**

- 정보보호서비스전문기업을 통한 연 1회 전자금융기반시설 취약점 점검(모의해킹, 인프라, 관리체계진단) 실시

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

**③ 정기적인 기술보호 교육 실시 여부(전직원 대상)**

-미 실시

**④ 전 직원 비밀유지서약 및 핵심직원 전직금지서약 체결 여부**

-(붙임2-2) ‘비밀 유지 및 경업 금지 서약서.pdf’ 참고

-연 1회 서약 현황 점검

**⑤ 핵심기술 인력 퇴직 후 사후관리(영업비밀 인수인계, 준수의무 등)**

-미 실시

**⑥ 중요 기술 영업비밀 분류 및 관리 여부(자산 중 영업비밀 등급부여)**

**1) 고객 개인정보 관리**

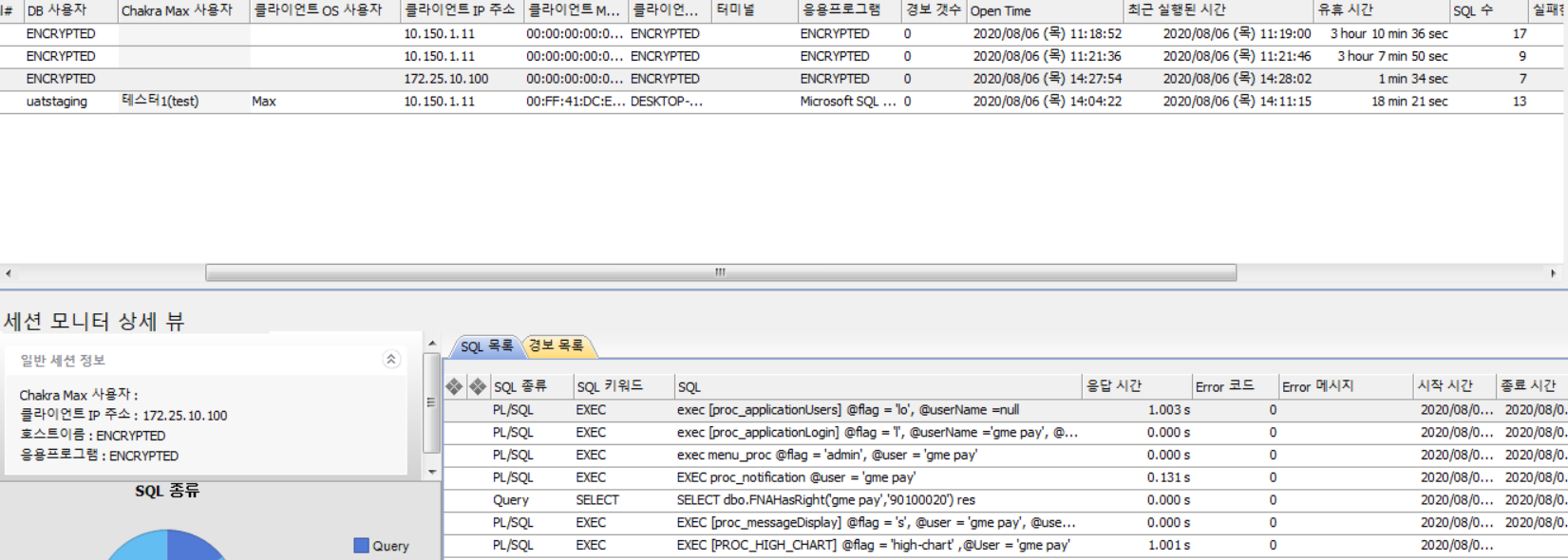
-고객 개인정보에 대한 접근은 내부망에서만 가능하도록 물리적으로 중요단말망을 분리

-중요 자료인 고객 개인정보는 개인정보처리시스템을 지정하여 별도로 관리(데이터베이스, 어드민 시스템)

-개인정보처리시스템의 계정은 신청을 통해 발급하며, 역할기반으로 권한을 제어

-DB접근제어 솔루션인 ChakraMax를 이용하여 데이터베이스 클라이언트 또는 어드민 시스템을 이용해 고객 개인정보 데이터를 조회할 시 로그를 저장→누가, 언제, 어떤 개인정보를 조회하였는지 확인 가능

[ChakraMax 감사 화면]



테이블이(가) 표시된 사진

자동 생성된 설명

**2) 소스코드 관리**

-소스코드에 대한 접근은 내부망에서만 가능하도록 물리적으로 중요단말망을 분리

-소스코드의 형상은 SVN에서 관리하며, 업무관련자에게만 계정을 부여

-상용화된 운영 소스코드에 대한 읽기 및 쓰기 권한은 PM에게만 부여

테이블이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

**⑦ 중요 서류 별도 관리 여부(중요문서 관리번호 부여 등)**

중요 데이터를 백업하는 외장 HDD 매체에 대하여 관리대장을 작성

테이블이(가) 표시된 사진

자동 생성된 설명

**⑧ 중요 설비 및 장치에 대한 통제구역 설정 및 관리 여부**

-주요 전산시스템을 KT 목동IDC에 구축함으로써 CCTV, 출입통제를 통한 보안 안정성을 확보

텍스트, 스크린샷, 전자기기, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

-본사 내 전산실 입구에 ‘통제구역’ 팻말을 부착하고, CCTV, 서버실 도어락을 설치하여 보안 안정성을 확보

텍스트, 실내, 작업대, 테이블이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**⑨ 중요 기술 특허 및 임치 여부**

-특허 미 보유 / 임치하지 않음

**⑩ 정보시스템 보안 관리 여부(데이터 암호화, 허가 USB활용 등)**

-DB내 주요정보 암호화

-DB 접근제어

-비인가자의 네트워크 접근 차단

-물리적 망분리

-매체 제어

텍스트이(가) 표시된 사진

자동 생성된 설명