개인정보 및 주요정보
암호화 관리 지침

제1장: 총칙

제1조: 목적

본 지침은 개인정보 및 주요정보의 보호를 위해 법적 요구사항을 반영하여 암호화 대상, 암호 강도, 암호 사용 정책 및 암호키 관리 절차를 수립하고, 이러한 정보를 저장·전송·전달할 때 암호화를 적용하는 것을 목적으로 한다. 이를 통해 정보 유출 및 위변조를 방지하고, 법적 준수사항을 이행하며, 기업 내에서 취급하는 모든 민감정보를 안전하게 보호한다.

제2조: 적용 범위

본 지침은 회사 내에서 취급하는 모든 개인정보 및 주요정보에 적용되며, 해당 정보의 수집, 처리, 저장, 전송, 공유, 삭제에 이르는 모든 단계에서 적용된다. 또한, 회사와 계약을 체결한 외부 협력업체도 이 지침을 준수해야 하며, 이를 위반할 경우 계약상 불이익을 받을 수 있다.

제3조: 정의

- **개인정보**: 개인을 식별할 수 있는 모든 정보로서 이름, 주소, 전화번호, 이메일, 주민등록번호 등이 포함된다.
- **주요정보**: 회사의 경영, 재무, 기술, 고객 정보 등 기업 경쟁력에 영향을 미칠 수 있는 모든 정보.
- **암호화**: 특정 알고리즘을 사용하여 데이터를 인가된 사용자만 읽을 수 있도록 변환하는 과정.
- **암호키**: 암호화 및 복호화에 사용되는 비밀 정보.
- **법적 요구사항**: 개인정보보호법, 정보통신망법, GDPR 등 국내외 법률 및 규정에서 요구하는 사항.

제2장: 암호화 정책

제4조: 암호화 대상

- 개인정보와 주요정보는 반드시 암호화하여 보호해야 하며, 이 대상에는 다음과 같은 데이터가 포함된다:
    - 직원 및 고객의 개인식별정보(이름, 주민등록번호, 주소, 전화번호 등)
    - 신용카드 정보, 은행계좌 번호 등 금융정보

    - 경영계획, 재무정보, 기술적 설계 및 제품 계획
    - 기타 법적 요구사항에 따라 보호가 필요한 정보
- 암호화 대상 데이터의 범위는 정기적으로 검토되어 변경 가능하며, 법적 기준에 맞춰 수정된다.

제5조: 암호화 강도

- **대칭키 암호화**: AES-256 이상의 강력한 암호화 알고리즘을 적용해야 하며, 모든 저장된 데이터는 이 방식으로 암호화된다.
- **비대칭키 암호화**: RSA 2048 비트 이상의 강도를 사용하여 민감한 정보 전송에 적용한다.
- **해시 알고리즘**: 민감 정보의 검증을 위해 SHA-256 이상의 해시 알고리즘을 사용하며, 특히 비밀번호 저장 시에는 '솔트(salt)' 기법을 포함한 해시를 적용하여 보안을 강화한다.
- 암호화 알고리즘 및 강도는 최신 보안 기술과 표준을 준수해야 하며, 법적 요건이 강화되면 해당 요구사항에 맞춰 강도를 주기적으로 검토 및 갱신한다.

제6조: 암호 사용 정책

- **암호 생성 기준**: 암호는 최소 12 자리 이상의 길이를 가져야 하며, 대문자, 소문자, 숫자, 특수문자를 반드시 포함해야 한다. 이는 비밀번호 예측 및 무차별 대입 공격을 방지하기 위한 강도 설정이다.
- **암호 사용 기한**: 암호는 최소 90 일마다 변경해야 하며, 동일한 암호를 재사용하는 것은 금지된다.
- **암호 보관 방법**: 암호는 절대 평문(plaintext)으로 저장되지 않으며, 안전한 암호화 방식을 사용하여 보호해야 한다. 암호 저장 시 해시 함수와 함께 '솔트(salt)'와 '페퍼(pepper)' 기술을 적용하여 보안을 강화한다.
- **암호 사용 시 보안**: 직원은 기업 내부 시스템에 접속하거나 데이터를 접근할 때 이중 인증(2FA)을 통해 신원을 추가로 확인해야 한다. 특히 민감 정보에 접근할 경우 OTP(One-Time Password) 또는 하드웨어 토큰을 사용할 것을 권장한다.

제7조: 암호 키 관리 정책

암호 키는 암호화된 데이터의 안전성을 보장하기 위한 중요한 요소이므로, 그 생성, 사용, 보관 및 폐기 절차는 철저하게 관리되어야 한다.

1항. 암호 키 생성 및 배포

- 암호 키는 암호화 전용 하드웨어 보안 모듈(HSM)에서 생성하여 안전성을 보장하며, 해당 키는 평문으로 유출되지 않도록 보호된 환경에서만 생성 및 사용되어야 한다.
- 암호 키 배포는 반드시 암호화된 통신 채널을 통해 이루어져야 하며, 외부 위협으로부터 보호하기 위해 비대칭키 암호화(RSA)를 사용하여 전송한다.

2항. 암호 키 보관

- 암호 키는 안전한 암호화 키 관리 시스템(KMS)에서 보관되며, 물리적 접근이 제한된 서버에서만 접근이 가능하다.
- 암호 키 보관 장소는 별도로 보호되며, 접근 권한은 최소화하여 엄격히 관리해야 한다. 무단 접근을 방지하기 위해 로그 기록을 유지하고 주기적인 모니터링을 실시한다.

3항. 암호 키 폐기

- 더 이상 사용하지 않는 암호 키는 안전하게 폐기해야 하며, 폐기 절차는 디지털 및 물리적 복구가 불가능하도록 안전하게 이루어져야 한다.
- 폐기된 암호 키는 별도로 기록하여, 사고 발생 시 감사할 수 있도록 문서화한다.

4항. 암호 키 주기적 교체

- 민감 정보 보호 강화를 위해 암호 키는 주기적으로 변경해야 하며, 교체 주기는 최소 1 년을 초과하지 않아야 한다. 법적 요구사항에 따라 더 자주 교체할 수 있다.
- 암호 키 교체 시점마다 키 재사용이 되지 않도록 주의하며, 교체 절차는 내부 보안팀의 승인을 받아 진행해야 한다.

제8조: 데이터 저장 시 암호화

- 개인정보 및 주요정보는 물리적, 논리적 위치에 관계없이 반드시 암호화된 상태로 저장되어야 하며, 이때 AES-256 이상의 대칭키 암호화를 사용해야 한다.
- 데이터베이스에 저장되는 정보는 필드 수준에서 암호화가 적용되며, 특히 중요한 필드(예: 주민등록번호, 신용카드 번호 등)는 반드시 암호화한다.

- 파일 시스템에 저장되는 모든 민감 정보는 파일 단위로 암호화해야 하며, 암호화된 파일은 접근 제어 정책에 의해 관리된다.

제9조: 데이터 전송 시 암호화

- 회사 내외부 네트워크를 통한 데이터 전송 시 SSL/TLS 와 같은 강력한 암호화 프로토콜을 사용해야 하며, 민감 정보를 전송할 때는 반드시 암호화된 통신 채널을 사용해야 한다.
- 외부로 민감 정보가 전송될 때는 PGP, S/MIME 와 같은 이메일 암호화 기술을 사용해야 하며, 비인가된 사용자가 이메일을 열람할 수 없도록 조치한다.
- 네트워크 전송 과정에서 데이터 패킷이 가로채지거나 변조되지 않도록 실시간 모니터링 및 로그 기록을 유지해야 한다.

제10조: 데이터 전달 시 암호화

- 개인정보 및 주요정보가 물리적 매체(예: USB, 외장하드)를 통해 전달될 때는 반드시 매체에 암호화가 적용되어야 하며, 외부로 전달되는 매체는 암호화된 채널에서만 사용된다.
- 매체를 통한 데이터 전달 시에는 BitLocker 또는 유사한 드라이브 암호화 솔루션을 사용해야 하며, 암호는 별도 안전한 방법으로 전송해야 한다.
- 민감 정보가 포함된 문서 또는 파일을 공유할 때는 ZIP 암호화, PDF 암호화 등 별도의 파일 암호화를 적용하며, 암호는 외부 전송 경로를 통해 전달하지 않도록 한다.

제3장: 법적 요구사항 준수 및 내부 절차

제11조: 법적 요구사항 준수

- 기업은 개인정보보호법, 정보통신망법, GDPR 등의 국내외 법적 요구사항을 준수해야 하며, 암호화 대상, 암호 강도, 암호 키 관리 등의 절차는 이러한 법적 기준에 부합해야 한다.
- 법적 요구사항은 정기적으로 검토하여 최신 법률 변경 사항이 반영되도록 하고, 해당 요구사항을 반영한 암호화 정책을 수립 및 유지해야 한다.
- 법적 요구사항 위반 시 기업에 대한 제재나 벌금이 부과될 수 있으므로 모든 부서는 해당 기준을 철저히 준수해야 한다.

제12조: 내부 감사 및 모니터링

- 정보보안 부서는 정기적인 감사를 통해 암호화 정책 준수 여부를 점검해야 하며, 암호화 과정에서 발생할 수 있는 보안 취약점을 사전에 파악하여 대응한다.
- 암호화된 데이터에 대한 접근 로그는 주기적으로 검토하여 비정상적인 접근이 있는 경우 즉시 대응할 수 있도록 한다.
- 기업 내 암호화 관련 사고 발생 시 사고 대응 절차에 따라 빠르게 복구 및 대응해야 하며, 사고 분석 결과를 바탕으로 추가적인 보안 개선이 이루어져야 한다.

제4장: 교육 및 인식 제고

제13조: 직원 교육

- 모든 임직원은 개인정보 및 주요정보 보호와 관련된 법적 요구사항 및 암호화 지침에 대해 정기적인 교육을 받아야 한다.
- 암호화 기술, 보안 위험 요소, 데이터 보호 절차에 대해 충분한 인식을 가질 수 있도록 체계적인 교육 프로그램을 마련하며, 이 과정에서 암호화 관련 최신 기술 동향을 전달한다.
- 보안 사고 시 직원의 즉각적인 대응을 위한 교육도 포함되며, 실제 시나리오 기반의 모의 훈련을 통해 인지도를 높인다.

제14조: 인식 제고 캠페인

- 정기적으로 내부 보안 캠페인을 실시하여 모든 직원이 암호화 및 개인정보 보호의 중요성을 인식할 수 있도록 한다.
- 내부 인트라넷, 뉴스레터, 포스터 등을 활용하여 법적 요구사항 및 암호화 절차를 지속적으로 상기시키고, 암호화 사용의 중요성을 알린다.

제5장: 기타

제15조: 지침 유지 및 개선

- 본 지침은 주기적으로 검토되어 최신 법적 요구사항과 보안 기술을 반영한 상태로 유지되며, 수정 사항이 있을 경우 즉시 모든 임직원에게 공지한다.

- 지침 수정이 필요할 경우 보안 담당 부서에서 내부 결재 절차를 거쳐 승인을 받아 적용한다.

제16조: 시행일

본 지침은 20XX 년 X 월 X 일부터 시행한다.