암호 통제 관리지침

암호 통제 관리지침

문서번호: 가비아-GL-13

개정번호: VERSION 1.4

정보보호 책임자	정보보호 최고책임자

개정이력

개정 번호	개정일자	담당자	개정 내용
Version 1.0	2016.10.26	안광해	정보보호책임자 · 최고책임자 승인 정보보호위원회 의결 및 지침 시행
Version 1.1	2016.12.22	안광해	정보보호위원회 의결 및 개정 지침 시행
Version 1.2	2017.04.21	안광해	이행심사 조치 사항 부칙 제10조 예외적용 책임자 변경 기존: 정보보호책임자, 개정: 정보보호최고책임자
Version 1.3	2018.08.06	안광해	제 4조 암호 사용 문구 수정
Version 1.4	2019.02.26	안광해	제8조 (암호키 관리) 내용 수정 기존: 정보보호관리자, 개정: 정보보호책임자
Version 1.4	2019.03.01	안광해	정보보호책임자 · 최고책임자 승인 정보보호위원회 의결 및 지침 시행

목 차

제1장 암호통제

제1조 (목적)

본 지침은 (주)가비아(이하 "회사"라 함)의 클라우드 서비스 공공 zone 운영에 이용되는 개인정보의 암호화를 통해 데이터의 내/외부 유출 및 변조의 위험을 최소화시킴으로써 개인정보를 포함한 업무상 정보의 보안성을 확보하는 것을 그 목적으로 한다.

제2조 (적용범위)

이 지침은 회사의 개인정보 업무를 처리하는 부서 및 임직원을 그 적용 범위로 한다.

제3조 (책임사항)

① 정보보호최고책임자
암호화 관련업무에 대한 책임자를 지정하고 정기적으로 관리 상태를 확인한다.

② 정보보호책임자
암호화 관련 업무를 총괄관리하며, 암호화 점검사항을 보고 받고 검토한다.

제4조 (암호사용)

① 회사에서 업무상 개인정보를 인터넷을 통하여 외부로 송수신 할 경우 암호화(SSL)나 파일 패스워드 지정 등의 암호를 적용해야 한다.

② 개인정보를 다루는 개인정보취급자는 시스템 또는 정보통신망 접속에 사용되는 비밀번호를 일방향 암호화하여 저장한다.

③ 개인정보취급자는 개인정보를 개인용컴퓨터(PC)에 저장 할 때 암호화 한다.

④ 시스템 개발 시 개발담당자는 암호 및 인증시스템에 적용되는 키에 대하여 주입, 운용, 갱신, 폐기에 대한 절차 및 방법에 따라 안전하게 관리한다.

⑤ 운영 시스템의 암호 및 인증시스템에서 이용하고 있는 키와 테스트 시스템에서 테스트용으로 사용되고 있는 키는 동일한 키를 사용하지 않아야 한다.

⑥ 암호화된 알고리즘을 사용한다.

제5조 (암호선정)

① 회사에서 취급하는 모든 개인정보에 대하여 안전하게 보호하기 위한 암호 알고리즘을 선정해야 한다.

② 서비스 이용자 및 내부 임직원 비밀번호 저장 시 단방향(해쉬) 방식의 암호화

알고리즘을 이용하며 SHA-256 이상 암호화 알고리즘을 이용한다.

제6조 (암호화 범위)

① 회사가 보유하고 있는 고객의 고유식별정보(주민등록번호, 계좌번호, 신용카드 번호 등)는 AES-128 또는 SEED-128 이상 암호화 알고리즘을 이용한다.
② 회사의 개인정보 및 인증정보를 송수신 할 경우 보안서버 구축(SSL) 등의 조치를 통한 암호화 하여야 한다.

제7조 (암호화 키의 접근통제)

① 암호키에 대한 접근은 암호키를 생성한 소유자와 암호키 관리 책임이 부여된 정보보호최고책임자 및 정보보호 책임자에 한하여 접근할 수 있다.
② 암호키에 대한 접근 권한을 가진 사용자의 명단을 목록화하여 주기적으로 점검되어야 하며, 암호키 접근 권한은 최소한으로 부여되어야 한다.
③ 암호화키는 소스코드나 텍스트 파일 형태의 평문으로 저장되어서는 안된다.
④ 암호키의 변경 및 접근에 관한 정보들의 기록은 1년 동안 별도 로그 저장소에 보관되어야 한다.

제8조 (암호키 관리)

① 암호키는 생성 시 사용기간을 정하여 기간 만료 시 폐기 절차에 따라 폐기하고 재생성해야 한다.
② 생성된 암호키는 별도의 안전한 장소에 소산하여 보관해야 한다.
③ 사용기간이 만료되기 이전에 암호키 유출, 분실, 변경 등의 사유로 암호키를 폐기할 수 있다.
④ 사용기간 내 폐기된 암호키는 재생성 절차를 거쳐 신규 생성하고 정보보호책임자의 승인을 득한다.
⑤ 키를 변경해야 할 때와 어떻게 변경해야 하는지에 관한 키 변경 또는 갱신 절차를 수립하고 이행해야 한다. 단, 암호화된 키가 하나도 없으면 갱신 절차를 수립하지 않을 수 있다.
⑥ 손상된 키의 취급 절차를 수립하고 이행해야 한다.
⑦ 키 손상 시 시스템 또는 암호화 된 정보의 복구를 위해 시스템에 저장되어 있는 암호화키를 별도의 매체에 저장 후 안전한 장소에 보관하여야 한다.
⑧ 암호화키의 적정성을 주기적으로 검토하고 암호키 유출, 암호키에 접근 할 수 있는 담당자의 변경, 암호시스템 해킹이 의심되는 경우, 즉시 변경하여야 한다.

⑨ 단, 암호키 변경 시 비용과 회사의 정보자산 및 업무 중요도를 고려하여 자체적으로 정하여 적용하도록 한다.

부칙

제9조 (시행일)

본 지침은 정보보호위원회 의결 완료일부터 시행된다.

제10조 (예외적용)

다음 각 호에 해당하는 경우에는 본 지침에서 명시한 내용일지라도 정보보호 최고 책임자의 승인을 받아 예외 취급할 수 있다.

1. 기술환경의 변화로 적용이 불가능할 경우
2. 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우
3. 기타 재해 등 불가항력적인 상황일 경우

제11조 (경과조치)

특별한 사유에 의하여 본 지침에 정하는 요건을 충족하지 못한 경우에는 시행일로부터 3 개월이내에 개선방안을 강구하여야 한다.

제2장 관련서식

별지 1. 암호화 키의 접근통제

암호키접근 관리대장

점 검 자		확 인 자			정보보호책임자	정보보호최고책임자
점검 일자						
접 근 명						

암호키 접근권한 사용자 명단				
암호키 접근가능자 명단	NO	직책명	책임자명	서명
	1			
	2			
	3			

암호키 접근자 정보사항	
부 서 명	
성 명	
연 락 처	
접근일자	201 년 월 일

NO	접근일자	접근명	접근목적	비고
1				
2				
3				
4				
5				
6				
7				
8				