정보보호실행계획서

정보보호실행계획서(2020)

문서번호: 가비아_GL_01

개정번호: VERSION 1.0

정보보호 책임자	정보보호 최고책임자

개정이력

개정 번호	개정일자	담당자	개정 내용
Version 1.0	2020.02.21	정명도	신규작성

목 차

1. 정보보호 실행계획서

1.1 목적

본 정보보호실행계획은 ㈜가비아 (이하 "회사"라 함)의 클라우드 서비스 공공 ZONE 정보보호방침을 기본으로 연간 정보보호에 대한 실행계획을 수립하여 정보보호의 체계적인 실행을 그 목적으로 한다.

1.2 적용범위

본 정보보호실행계획은 회사의 모든 임직원, 클라우드 서비스 관련 정보통신설비 및 시설에 대하여 적용된다.

1.3 용어정의

정보보호: 정보의 기밀성, 무결성, 가용성을 보장하기 위한 관리적, 기술적, 물리적 수단 또는 그러한 수단으로 이루어지는 행위를 의미한다.

2. 연간실행계획 목표 및 전략

2.1 목표

연간 정보보호계획에 대한 상세 일정, 예산 및 인력 배정을 통하여 체계적이고 효율적인 운영에 그 목적으로 한다.

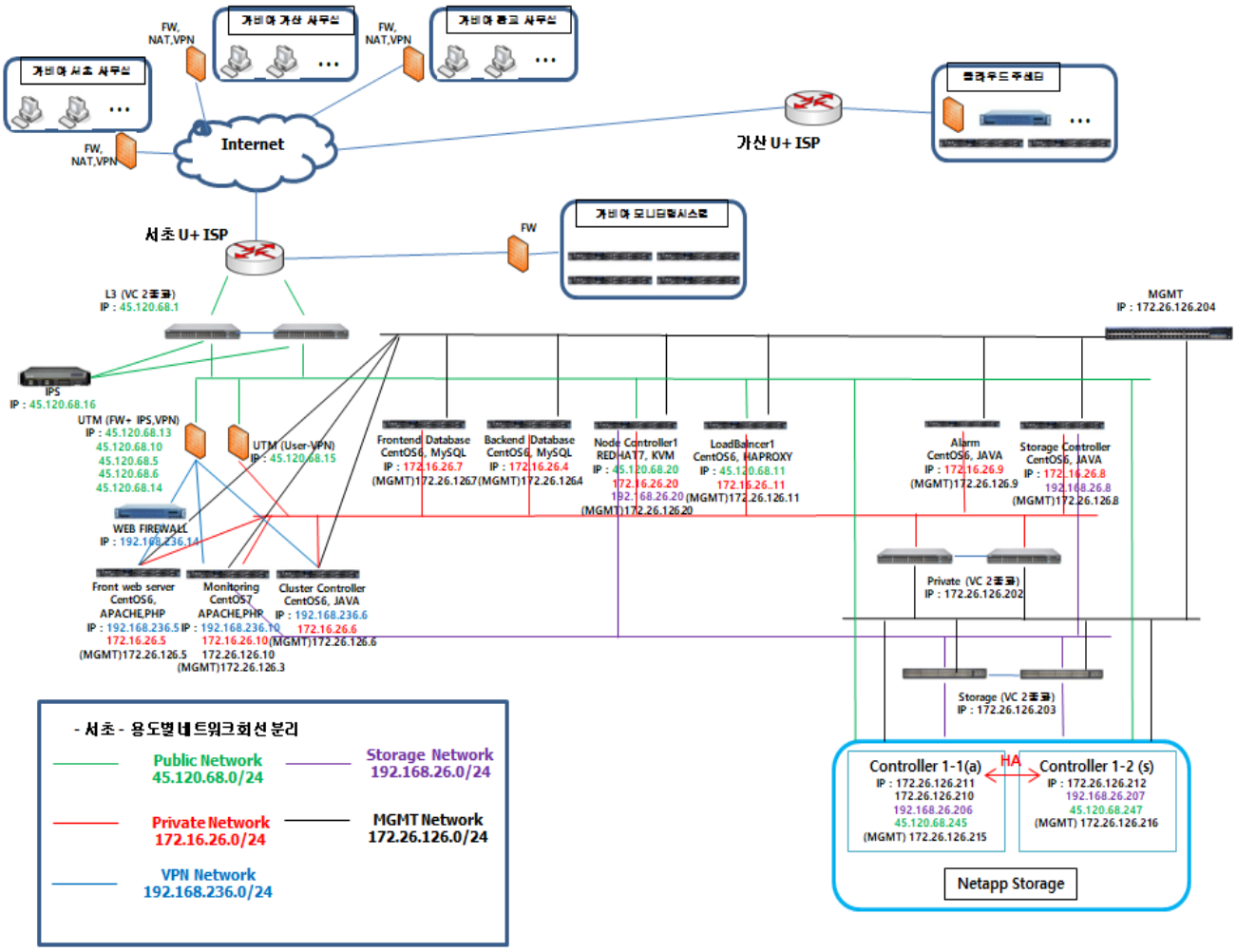
2.2 전략

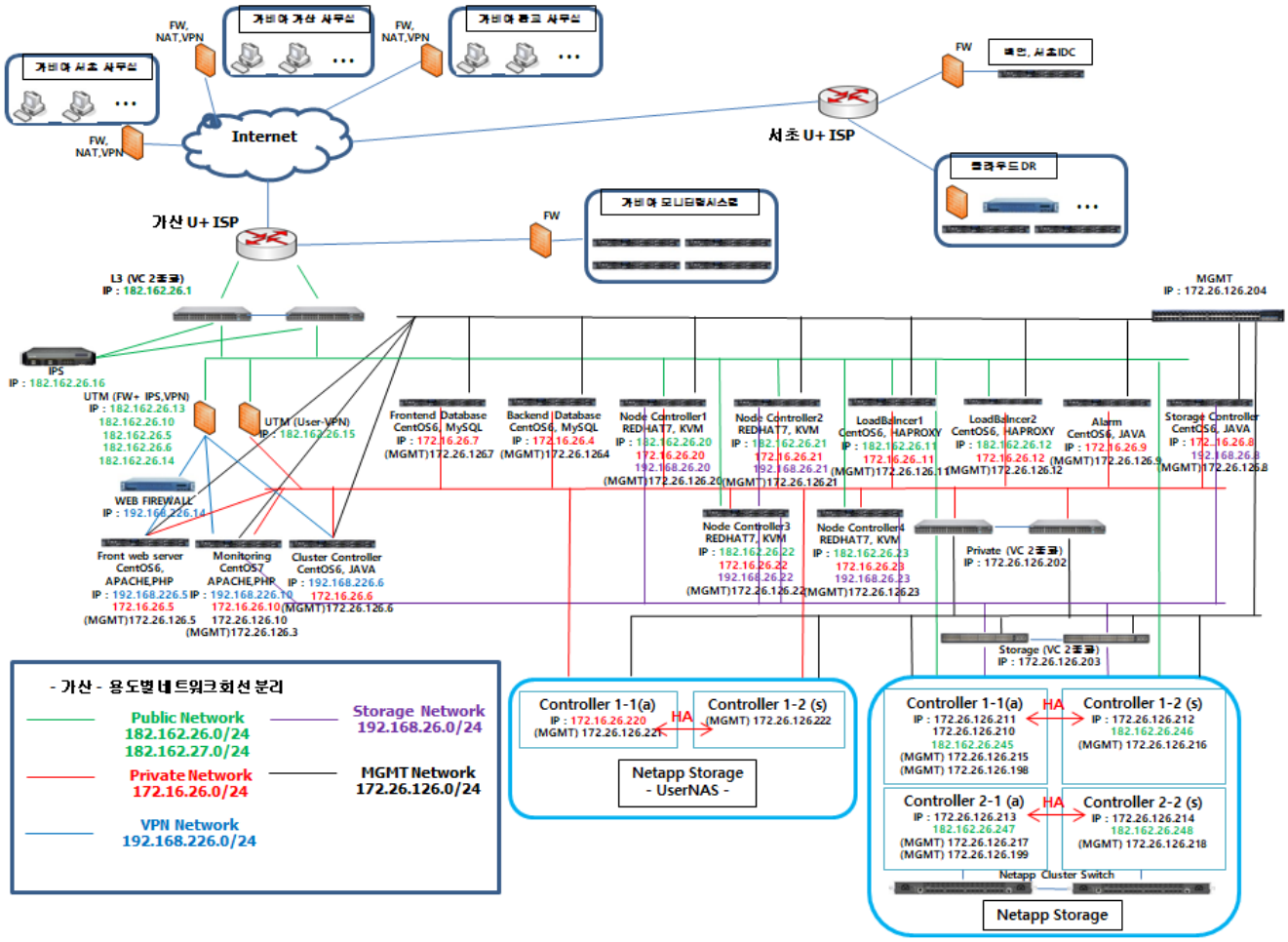
기년도 정보보호실행계획에 대한 이행 사항 및 새로운 보안 패러다임을 참조하여 조직의 상황에 맞추어 새로운 정보보호실행 계획을 수립한다.

3. 정보보호 시설 및 설비 현황

3.1 시스템 구성도

상세한 시스템 구성도는 아래 '가비아_클라우드서비스_시스템구성도'를 참조한다. (2020년도 구성도 필요)





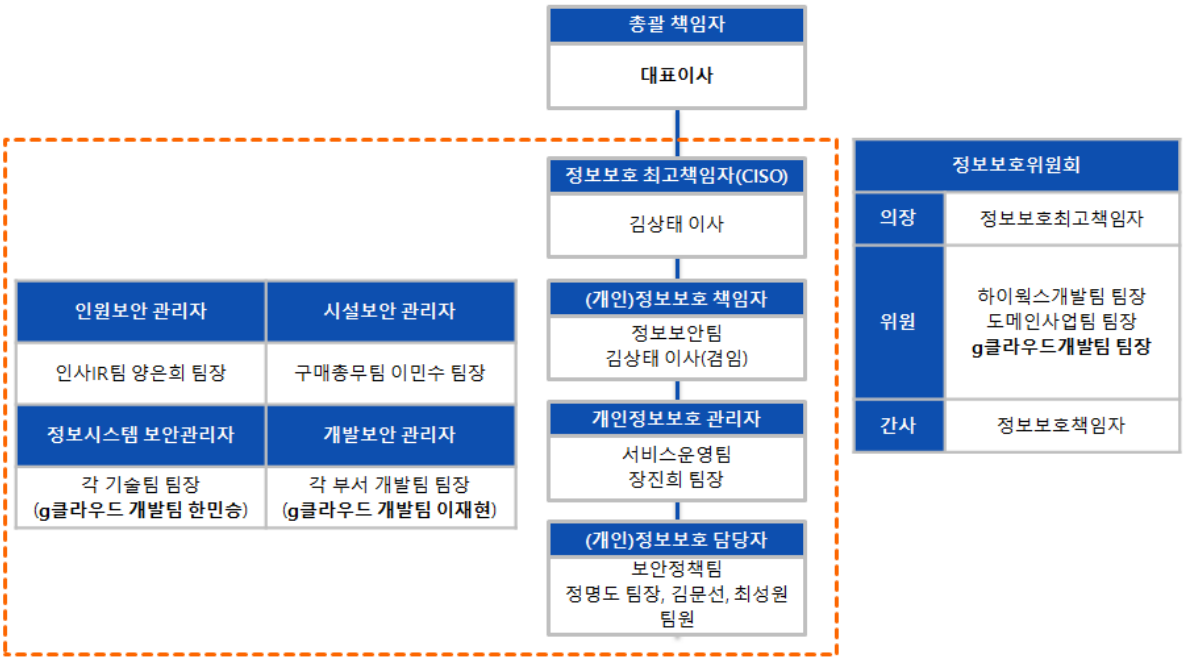
3.2 정보통신 자산현황

상세한 정보통신 자산현황은 '자산목록대장'을 참조한다.

3.3 정보보호조직

3.3.1 정보보호 조직도

㈜가비아 정보보호조직도



3.3.2 조직 정의 및 역할

정보 통신 서비스를 안전하게 제공하고 정보보호 활동을 체계적으로 이행하기 위해 조직 특성에 적합한 정보보호 조직을 구성한다.

- 정보보호최고책임자: 정보보호조직을 구성 운영하면서 정보보호 활동에 대한 계획, 집행, 통제 등 총괄을 담당한다. 개인정보보호 책임자를 겸임한다
- 정보보호책임자: 회사의 정보보호 방침, 지침, 계획, 절차 등의 검토 승인과 침해 사고 등 비상 상황 시 수행 실무를 총괄한다. 2020년은 정보보호최고책임자가 정보보호책임자도 겸임한다
- 정보보호담당자: 정보보호책임자의 지시 하에 연간 정보보호 활동 및 감사 계획을 수립하고 정보보호 책임자의 승인을 득한다.
- 인원/시설/정보시스템/개발 보안관리자
  -인원/시설 보안 관리자는 임직원의 채용 및 퇴사 시 보안 서약 등을 집행하고 정보보호 교육계획 수립 및 결과를 보고한다. 또한 회사의 보호 구역에 대한 출입통제 관리 및 공용 사무 기기 등에 대한 자산을 관리한다.

-정보시스템 보안 관리자는 각 정보시스템 도입 시 보안성 검토, 중요 시스템에 대한 백업 계획 수립 및 백업 등을 수행한다. 또한 정보시스템 취약점에 대한 진단 및 조치를 행한다
-개발보안 관리자는 응용프로그램 개발 시 보안성 검토, 개발 및 테스트 소스 관리, 응용프로그램 취약점 진단 및 조치를 행한다

- 개인정보보호 관리자: 회사의 모든 서비스 고객의 개인정보를 관리한다
- 정보보호위원회: 정보보호업무 수행을 위한 정책 및 규정을 개발, 검토하고 보안 이슈 발생 시 대책 논의 및 처리를 수행한다. 또한 기타 정보보호 정책, 지침, 절차의 수행을 위해 협의한다.

3.3.3 담당자 및 연락처

역 할	담 당 자	연 락 처
총괄 책임자	대표이사	-
정보보호최고책임자((개인)정보보호책임자 겸임)	김상태 이사	010-5671-5081
정보보호담당자	정명도 팀장	010-4402-8862
	김문선 팀원	010-2077-2657
	최성원 팀원	010-2711-0434
개인정보 관리자	장진희 팀장	010-5497-8835
인원보안 관리자	양은희 팀장	010-5379-0825
시설보안 관리자	이민수 팀장	010-9111-4210
정보시스템보안 관리자	마성준 팀장	010-8834-0067
	김동우 팀장	010-9074-9393
	한민승 팀장	010-3132-4351
	김도형 팀장	010-7677-1397
	장인환 팀장	010-9094-5437
	장기훈 팀장	010-6345-5137
	김영규 팀장	010-3745-9684
	전득상 팀장	010-8867-3767
	윤종민 팀장	010-3099-4566
	정광진 팀장	010-7314-3854
개발보안 관리자	이태석 팀장	010-6336-5971
	이민관 팀장	010-5349-0669
	김덕연 팀장	010-5157-2482
	정현철 팀장	010-9048-6577
	김정현 팀장	010-5772-0879
	송태형 팀장	010-3347-1510

	이재현 팀장	010-3426-6804
	도병권 팀장	
	백승대 팀장	010-4983-1808
	김동주 팀장	010-8923-0329

3.4 정보보호 문서현황

구분	문 서 명	문서내용 및 목적
정책서	정보보호방침	최고경영자의 정보보호 방침 및 기본정보보호 방향을 설정하기 위하여 규정된 문서
지침서	정보보호조직운영지침	정보보호 활동을 위한 기반조직의 구성과 운영에 대한 사항을 규정함으로써 회사의 정보보호 관리를 지속적으로 이루게 하기 위한 지침서
	인적관리지침	내부임직원 및 제3자에 대한 준수사항 설명 및 보안교육에 대한 규정을 기술한 지침서
	침해사고대응지침	발생하는 침해사고에 신속하게 대응하기 위한 준비와 대응절차를 기술하여 침해사고로부터의 피해를 최소화하고 후속 보안 대책을 세울 수 있도록 하기 위한 지침서
	자산관리지침	모든 정보통신설비 및 시설을 대상으로 하고 있으며, 주요 자산의 식별 및 분류, 분류 자산의 지속적 관리, 자산의 훼손, 변조, 도난 유출 등의 다양한 형태의 침해 위협으로부터 주요 자산을 비용대비 효과적으로 보호하기 위하여 자산 분류 지침을 정하기 위함임
	네트워크보안관리지침	네트워크에서 준수해야 할 내용을 규정하여 네트워크를 보다 안전하게 관리, 운영하도록 하기 위함임
	서버보안관리지침	대내외 서버상에 보관 또는 처리되는 정보의 기밀성, 무결성, 가용성을 유지하기 위해 지켜야 할 준수사항의 규정함을 목적으로 함
	정보보호시스템 보안관리지침	침입차단시스템, 바이러스월 등의 정보보호시스템의 운영 및 관리를 위한 보안 요구사항을 정의함으로써, 효과적인 정보보호시스템 운영을 통해 실수나 고의로 외부 네트워크로부터 내부 시스템 및 데이터 등의 자원에 접근하여 정보의 누출, 손상, 파괴 등 일련의 불법적 행위를 방어하고 탐지하기 위함임
	취약점점검지침	정보통신설비에 대한 주기적인 보안 점검을 수행함으로써 주요 자산의 위협에 대한 노출을 최소화하기 위함임
	물리적보안지침	정보통신설비 및 시설 등을 포함한 조직의 정보자산에 대한 안전한 유지와 보호를 위하여 정보통신시설에 대한 출입통제, 백업을 위한 설비 및 시설의 설치·운영 등에 대한 물리적 보안에 대해 규정함을 목적으로 함

	사용자보안지침	PC관리자와 최종사용자의 효율적이고 안전한 PC 보안관리 절차 통하여 사용자 보안에 대한 책임과 권한 및 통제지침들을 규정하고 기술적인 관리방법을 정함으로써 회사의 사업 연속성을 보장하고 사업손실을 최소화 하기 위함임
	개인정보관리지침	회사의 보안규정 및 정보보안 표준에 따른 요구사항과 관련하여 고객의 개인정보를 체계적으로 관리 및 보호하기 위함
	암호통제관리지침	암호정책, 암호 사용, 키 관리 방안에 대한 지침
	응용프로그램보안지침	응용프로그램의 개발, 유지보수 및 운영에 있어서 필요한 보안 관련 활동을 정의하여 사용자 정보의 손실, 변조, 오용을 예방하며 정보의 기밀성, 무결성, 가용성을 확보
	서비스연속성관리지침	정보시스템을 관리하고 운영하는 데 있어 정보시스템 장애, 재해 등의 비상사태 발생 시 신속한 대응을 통해 피해를 최소화하고 빠른 시간 내에 정상 업무를 재개하기 위함
	데이터베이스 운영관리지침	데이터베이스 보안관리의 기준을 제시하여 내·외부의 불법적인 위협으로부터 데이터베이스의 기밀성, 무결성 및 가용성을 확보하기 위한 지침서.
	정보보호감사지침	정보보호 정책 및 지침에서 정의하고 있는 제반 정보보호 활동 이행여부를 점검하고, 이를 개선하기 위한 보안감사 기준과 절차 규정을 목적으로 하는 지침.
	가상자원관리지침	하이퍼바이저, Host server 등 클라우드 시스템을 구성하기 위해 필수적인 가상화 관련 자원들의 관리 기준을 제시하여 각종 보안위협으로부터 안전한 가상화 시스템을 구축/운영하기 위한 지침서
계획서	정보보호실행계획서	정보보호 방침을 기본으로 분기별 정보보호에 대한 실행계획을 수립하여 정보보호의 체계적인 실행을 그 목적으로 함
	클라우드시스템백업계획서	클라우드 시스템의 로그, config, 소스 등에 대한 안전한 관리를 위해 백업 방식, 주기, 계획 등을 사전에 정의하는 것을 그 목적으로 함

4. 2020년 추진계획 및 예산(안)

4.1 추진계획

추진 사업명	주요 내용	대상	횟수
서비스 취약점 점검	주요 서비스 취약점 진단	서버, 네트워크, 정보보호시스템, DB, PC, 웹서비스	반기 1회
위험평가	위험 수준 측정	내부 자산 및 공통관리 위험 분석	년 1회
내부감사	클라우드 서비스 정보보호 관리체계운영실태 점검을 통한 정보보안 수준 향상 목적	정보보호관리체계 통제항목	년 1회
침해사고 및 재해 대응 모의훈련	가비아 내부 시스템 침해 시도 대응 훈련 침해사고 훈련은 공공 인증 업체와 KISA 공공 진행 예정	서버, 네트워크	년 1회
클라우드 서비스 공공 Zone 보안 인증	사후 평가/갱신심사	g클라우드 서비스 공공 Zone 정보시스템 전체	년 1회
교육	정보보호 일반 교육	전사	년 1회
	클라우드 정보보호 교육	클라우드 시스템 주요 접근 직무자	년 1회
	개인정보보호 교육	전사	년 1회

※ 기타로 보안 상품 추가가 있을 수 있음.

4.2 예산(안)

2020 년 정보보호관리체계 운영 소요 예산(안)					
구분	항목		예산 내역	비용(원)	비고
클라우드 서비스 공공 Zone 보안인증 사후 평가	o 정보통신설비 부문	문서 관리	인증 수수료	무료	-
		운영 관리			
	o 정보통신시설 부문	문서 관리			
		운영 관리			
	o 기타 부문	-	-	-	-
보안 상품 추가	추가할 보안 상품 규정하지 않음..	-	제휴 상품 내부 인력 개발 예정 예산 X	판매 시 수익 Share	-
정보보호 교육	o 클라우드 특화 교육	-	교육비	10,800,000 원	단가(60 만원) X 인원(18 명)
총 사업비				10,800,000 원	

※ 정보보호 교육비는 변동될 수 있음.

4.3 세부사항

4.3.1 서비스 취약점 점검

4.3.1.1 목적

현재 운영되고 있는 정보시스템에 대하여 취약점을 발견하고 그에 대한 대응책을 수립하는데 그 목적이 있다.

4.3.1.2 세부일정

■ 2020년 3월/9월 (상황에 따라 변동될 수 있음)

4.3.1.3 수행범위 및 방법

■ 수행범위: 자산목록대장 참조

■ 방 법: 자동 툴 점검 및 수동 점검

4.3.2 위험평가

4.3.2.1 목적

회사의 자산을 식별하여 각 자산 별로 중요도를 평가하고, 해당 위협과 취약성을 평가하여 위험을 산출하고, 각 위험에 대해 비용대비 효과적인 대응책을 수립하여 자산들의 위험 수준을 감소시키는데 그 목적이 있다..

4.3.2.2 세부일정

■ 2020년 9월 예정 (상황에 따라 변동될 수 있음)

4.3.2.3 수행범위

■ 수행범위: 취약점 점검으로 취약점이 발견된 자산

4.3.3 내부감사

4.3.3.1 목적

각종 위협요인으로 인해 발생하는 재난 또는 위기로 사업 운영상 문제 발생에 대비하여 효율적인 예방 / 대응 / 복구를 위하여 재해복구 훈련을 수행한다.

4.3.3.2 개요

■ 기간: 2020년 12월 예정 (상황에 따라 변동될 수 있음)
■ 대상: (주)가비아
■ g클라우드 개발팀 정대원 팀장
■ 정보보안팀 김상태 팀장, 정명도 팀장
■ 관리적 보안감사자 1명
■ 기술적 보안감사자 1명

4.3.3.3 감사내용

■ 클라우드 서비스 정보보호관리체계 관리과정 요구사항 점검
■ 클라우드 서비스 정보보호관리체계 정보보호대책 요구사항 점검
■ (주)가비아 정보보호 관련내규 준수여부

..

4.3.4 침해사고 및 재해 대응 모의훈련

4.3.4.1 목적

㈜가비아 내부 시스템의 침해 시도 시 구축된 절차에 따른 대응 훈련을 함으로써 실제 이슈 발생시 빠르고 정확한 대응을 익히는데 목적이 있다.

4.3.4.2 세부일정

2020년 10월 예정 (재해 대응 모의 훈련 일정임. 내부 사정에 따라 변동될 수 있음)
※ 침해사고 훈련은 공공 클라우드 인증 업체와 KISA의 공동 진행으로 이뤄지므로 타 업체나 KISA에 의해 일정 변동이 있을 수 있음.

4.3.4.3 수행범위 및 방법
■ 수행범위: (주)가비아 클라우드 공공 zone 내부정보보호시스템

4.3.5 클라우드 서비스 공공 Zone 보안인증제 인증 사후 평가
4.3.5.1 목적
클라우드 서비스 보안 인증에 대한 사후 평가

4.3.5.2 세부일정
보안인증제 인증획득: 2017년 5월
보안인증제 사후 평가 신청서 제출: 2020년 3월 13일 예정
보안인증제 사후 평가 심사: 2020년 3월말 예정

4.3.5.3 수행범위 및 방법
■ 수행범위: (주)가비아 클라우드 서비스 공공 Zone 정보 시스템
■ 방법: 내부 시스템에 대한 관리체계 수립 및 적용.

4.3.6 교육
4.3.6.1 목적
정보보호구성원과 전 임직원의 정보보호 관련 인식 제고 및 전문 지식 습득

4.3.6.2 세부일정
개인정보처리 위탁계약 교육: 2020년 12월 예정
정보보안 교육: 2020년 12월 예정

4.3.6.3 교육 내용 및 대상
■ 교육 내용: 기본 교육 + 개인정보보호교육+ 클라우드 특화 교육(해당자에 한함)
■ 교육 대상: 전 임직원