자산관리지침

자산관리지침

문서번호: 가비아-GL-05

개정번호: VERSION 1.3

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 제16조 예외적용 책임자 변경 기존: 정보보호관리자, 개정: 정보보호최고책임자
Version 1.3	2019.02.26	안광해	제9조 (자산의 중요도 평가), 제13조 (기타 정보자산의 관리)관련 서식 결재라인 변경(정보보호관리자 삭제)
Version 1.3	2019.03.01	안광해	정보보호책임자 · 최고책임자 승인 정보보호위원회 의결 및 지침 시행

목 차

제1장 일반사항

제1조 (목적)

본 지침은 (주)가비아 (이하 "회사"라 함) 클라우드 서비스 공공 zone의 모든 정보시스템 및 설비를 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 규정함을 그 목적으로 한다.

제2조 (적용범위)

이 지침은 회사의 클라우드 서비스 정보통신설비 및 시설에 대하여 적용하며 신규 도입 또는 폐기되는 자산에 대해서 자산 분류와 관리를 위한 분류체계의 수립과 관련하여 지침의 정함에 따른다.

제3조 (용어정의)

1. 정보시스템: 사내·외 정보통신서비스를 제공하기 위한 서버, 네트워크 장비, 정보보호시스템과 운영·관리에 필요한 컴퓨터 장치 및 네트워크 장비 등을 의미한다.
2. 설비: 사내·외 정보통신서비스를 제공하기 위한 용도와 정보시스템의 가용성에 직·간접적으로 중대한 영향을 끼칠 수 있는 정보통신시설의 관리·운영의 용도로 설치된 부대시설 등의 정보통신설비를 의미한다.
3. 정보자산: 정보보안의 범위 및 적용 대상이 되는 정보시스템, 전산자료 및 이를 이용·관리·보호하는 물적 자산을 포함한다.
4. 자산 분류: 정보시스템에서 적절한 보호 통제가 취해질 수 있도록 자산을 체계적으로 구분하는 것을 의미한다.
5. 중요도: 정보자산의 기밀성, 무결성, 가용성을 의미한다.
6. 기밀성: 정보가 비 인가된 자에 의해 누설되거나 공개되지 않는 것을 의미한다.
   정보자산 또는 데이터가 전송, 백업, 보관 중에 허가 받지 않은 사람에게 노출되지 않아야 함을 의미한다.
7. 무결성: 정보나 정보시스템이 의도적 또는 비의도적으로 변조되지 않는 것을 의미한다.
   정보가 전송되고 저장되는 과정에서 완전성과 정확성을 유지하는 것을 의미한다
8. 가용성: 인가자에 의하여 정보나 정보시스템이 사용 가능하게 하는 것을 의미한다.

제4조 (책임사항)

1. 소유자

1.1 정보시스템 및 설비의 운영·관리의 책임을 갖는다.
1.2 신규 설비 및 시설의 경우 자산의 가치를 평가하고 "별지 1. 자산목록관리대장"에 업데이트해야 한다.

2. 정보보호책임자
2.1 정보시스템 및 설비에 대한 "별지 1. 자산목록관리대장"을 작성한다.
2.2 정보시스템 및 설비의 신규 등록, 폐기를 수행하고 정기적으로 자산실사를 통해 자산목록을 갱신한다.

3. 정보보호최고책임자
3.1 정보시스템 및 설비의 자산목록을 항상 최신으로 관리할 책임을 갖는다.
3.2 정보시스템 및 설비의 소유자(또는 소유부서), 관리자(책임자), 담당자를 적절히 지정한다.

4. 정보자산사용자
4.1 정보자산사용자는 정보보호책임자의 관리 하에 정보자산을 실질적으로 업무에 사용하는 자로서, 각 정보시스템 및 설비의 관리자와 담당자가 이에 속한다.
4.2 정보자산 사용 시 정보자산의 유출 및 파손 사고 등이 발생하였을 경우 이에 대한 최종 책임은 정보자산사용자가 진다.
4.3 정보자산사용자는 정보보호책임자의 허가 아래 정보자산을 사용해야 하고, 비인가 등 통제되지 아니한 정보자산을 포함하여 업무와 무관한 어떠한 정보자산에도 접근을 시도해서는 아니 된다

제2장 자산목록

제5조 (클라우드 서비스 시스템 구성도)

클라우드 서비스 시스템 구성도는 정보자산의 위치, 현황을 확인할 수 있도록 작성하며, 구성도 작성 시 다음의 사항을 포함하여 '정보통신망 구성도'에 작성한다.

1. 작성대상
2. 작성자
3. 작성일자
4. Version 정보

정보통신망 구성도는 항상 최신의 정보를 참조할 수 있도록 업데이트한다. 정보보안책임자는 네트워크, 서버 등의 정보통신설비의 변동사항이 발생한 경우나 UPS, 백업시설 등의 정보통신시설의 변동사항이 발생한 경우 관련부서에 자료를 요청하여 '별지 2. 클라우드 정보통신망 구성도'를 업데이트 한다. 업데이트는 변동사항이 발생한 후 일주일 이내에 완료한다.

제6조 (자산목록관리)

1. 정보보호책임자는 자산을 식별하고 분류하여 자산 별 소유관계와 등급을 명확히 정의하고 '자산목록관리대장'에 작성하여 관리한다.
2. 회사 내 자산목록은 정보보호최고책임자가 관리의 책임을 가진다.
3. 정보보호책임자는 신규 등록된 자산에 대해 기밀성, 무결성, 가용성 측면에서 자산의 중요도 평가를 통해 적절한 보호 대책을 적용한다.
4. 자산 구분
   정보시스템 자산에는 그 자산 외부 또는 잘 보이는 곳에 식별표를 부착한다. 다만, 중요자산에 대해 외부에 알릴 위험이 있을 경우 그 표지를 생략할 수 있다.

제7조 (자산목록구분)

클라우드 서비스 정보자산에 대해 아래와 같이 구분한다. 정보자산의 종류는 아래 세부 내역에 정의된 항목 이외에도 자산의 효율적인 관리상 필요시 정보보호최고책임자의 승인을 받아 추가 항목을 정의할 수 있다.

구분		세부 내역
정보시스템 자산	서버	DNS, DB, 공개서버(Web, Mail), 파일서버, Billing서버, EDI서버, 관리용 서버, 응용서버, 로그서버, NC서버, 백업서버 등
	네트워크	라우터, 스위치, 교환장비, NAS, 망연동장비, 허브 등
	정보보호 시스템	침입차단시스템, 침입탐지(방지)시스템, 가상사설망장비(VPN), 출입통제시스템(지문인식), 보안관제시스템, 바이러스 월 등
	웹서비스	홈페이지
	PC	사내 업무용 PC, 업무용 노트북, 업무용 테블릿 PC
	가상자원	OS Image, 하이퍼바이저
설비자산	CCTV, 출입통제시스템, 소화기, UPS, 항온 항습기 등	
기타정보 자산	S/W, 스토리지, 전자문서, 인쇄물, 휴대용 저장매체, 개인정보 데이터 등	

제3장 자산분류 및 관리

제8조 (자산의 분류기준)

1. 정보자산의 분류기준
   1.1 각 정보자산은 사용자, 소유자, 담당자가 명확히 구분되어야 한다.
   1.2 정보자산의 적절한 보호를 위해 기밀성, 무결성, 가용성 측면의 등급이 정의되어야 한다.
   1.3 정보보호책임자는 연 1회 주기로 "별지 1. 자산목록관리대장"을 작성 및 갱신한다. 필요시 외부업체의 지원을 받을 수 있다.
   1.4 정보보호책임자는 정보자산이 추가, 변경, 폐기될 경우 정보자산 분류기준에 따라 정보자산을 분류한다.
   1.5 정보자산은 유형에 따라 분류하여 관리하며, 정보자산의 효율적인 관리상 필요 시 추가 항목을 정의할 수 있다.

2. 정보자산 목록구성
정보자산 목록은 정보자산명, 소유자, 관리자, 담당자, 기밀성, 무결성, 가용성, 보관위치, 보안등급 등의 항목으로 구성된다. 단, 자산의 속성을 고려하여 별도의 항목을 추가 혹은 삭제할 수 있다.

제9조 (자산의 중요도 평가)

자산의 분류기준은 정보통신설비의 기밀성, 무결성, 가용성 관점에서 중요도를 평가하여 분류한다. 자산의 가치는 기밀성, 무결성, 가용성 평가 중 가장 높은 값으로 정의하며, 중요도는 각각의 평가 값을 H=3, M=2, L=1로 계산하여 합산한 점수로 정의한다.
자산의 가치를 평가하는 기준은 다음과 같다.

가치	기밀성	무결성	가용성
H	해당 정보통신설비가 보유하고 있는 정보의 유출 시 사업, 업무운영, 이미지 등에 치명적 영향을 미침	해당 정보통신설비가 보유하고 있는 정보의 변조 시 사업, 업무운영, 이미지 등에 치명적 영향을 미침	해당 정보통신설비 또는 정보통신설비가 보유하고 있는 정보의 파괴 또는 정지 시 사업, 업무운영, 이미지 등에 치명적 영향을 미침

M	해당 정보통신설비가 보유하고 있는 정보의 유출 시 사업, 업무운영, 이미지 등에 다소 중요한 영향을 미침	해당 정보통신설비가 보유하고 있는 정보의 변조 시 사업, 업무운영, 이미지 등에 다소 중요한 영향을 미침	해당 정보통신설비 또는 정보통신설비가 보유하고 있는 정보의 파괴 또는 정지 시 사업, 업무운영, 이미지 등에 다소 중요한 영향을 미침
L	해당 정보통신설비가 보유하고 있는 정보의 유출 시 사업, 업무운영, 이미지 등에 약간의 영향을 미침	해당 정보통신설비가 보유하고 있는 정보의 변조 시 사업, 업무운영, 이미지 등에 약간의 영향을 미침	해당 정보통신설비 또는 정보통신설비가 보유하고 있는 정보의 파괴 또는 정지 시 사업, 업무운영, 이미지 등에 약간의 영향을 미침

자산의 평가 기준에 따라 정보통신설비에 대해 평가를 수행하고 그 결과에 따라 자산을 분류하며, 이는 정보보호담당자가 별지 5. 자산 중요도 평가표를 통해 진행하고 반기별로 정보보호책임자의 결재를 득해야 한다.

중요도	평가결과
H	자산의 중요도가 8 이상인 경우
M	자산의 중요도가 5 이상이거나 7 이하인 경우
L	자산의 중요도가 4 이하인 경우

제10조 (자산의 분류)

1. 자산의 평가는 자산의 소유자가 수행한다.
2. 정보보호책임자는 자산 소유자의 평가 결과를 검토하고 그 결과를 토대로 자산을 분류한다.
3. 정보통신서비스를 제공하기 위해 사용되는 정보통신설비 중에 중요도 평가 결과가 M이상(중요도 5 이상)인 자산을 구분한다.

제11조 (자산의 접근권한)

1. 전 임직원과 협력업체는 자산에 대한 접근을 알 필요 원칙과 최소 권한 부여의 원칙에 따라 결정한다.
2. 또한 접근권한이 없는 자산이나 업무와 무관한 자산에 접근을 시도해서는 안 된다.

3. 정보통신설비 및 시설의 접근권한 부여는 각 설비 및 시설의 관리책임자에게 권한이 있으며, 정보보호최고책임자는 이를 주기적으로 점검해야 한다.

제12조 (자산의 관리)

1. 자산의 등록 및 갱신
   1.1 신규 자산의 등록은 부서 담당자가 신규자산목록을 작성하여 정보보호책임자에게 등록한다.
   1.2 정보보호책임자는 자산목록 및 자산의 평가결과를 토대로 '별지 1. 자산목록관리대장'을 업데이트 한다.
   1.3 정보보호책임자는 년 1회 자산목록관리대장을 토대로 자산현황을 점검하고, 누락된 사항이 있을 경우 변경사항을 업데이트 한다. 자산실사 결과 및 변경사항에 대해서는 정보보호최고책임자에게 보고한다.
   1.4 자산의 소유자는 년 1회 자산의 가치를 재검토한다.

2. 정보자산 변경관리
   2.1 운영체제 업그레이드, 상용 소프트웨어 설치, 운영 중인 응용프로그램 기능 개선, 네트워크 구성 변경, CPU/메모리/저장장치 증설 등 정보시스템 관련 자산 변경, 신규 설비의 도입, 기존 장비의 변경 및 폐기가 필요한 경우 작업계획서를 통해 변동 사항을 명시하고 책임자 검토·승인을 이행하여야 한다. 또한 이용자에게 작업 영향이 있을 경우 이 사실을 이용자에게 최소 작업 시행 3일 전에 통지해야 한다.
   2.2 변경 작업 이후에는 변경된 자산과 기존 시스템간의 호환성, 정상 작동 여부, 정책 설정 내역 등을 테스트하여 작업 결과 보고서를 작성해야 한다. 작성된 작업 결과 보고서는 작업 대상 장비의 소유자, 정보보호책임자에게 보고되어야 하며, 작업 결과 보고서에는 자세한 호환성 검증 내역을 별도 문서로 첨부해야 한다.

3. 자산의 폐기
   3.1 자산의 폐기는 폐기사유 발생시점에 자산의 소유자가 부서장의 승인을 받아 정보보호책임자에게 통보한다.
   3.2 정보보호책임자는 해당 자산을 '자산목록관리대장'에서 삭제하고, 정보보호 최고책임자에게 변동사항에 대해 보고한다.
   3.3 자산의 폐기는 국내에서 진행한다.

4. 정보자산 보호등급별 정보자산관리담당자의 역할
   4.1 'H'급 정보자산: 회사 내·외부에 부당하게 노출되거나 반출될 경우, 회사의 업무

활동에 중대한 영향을 미칠 가능성이 있는 정보자산으로서 '업무상 접근 권한을 가진 한정된 직원'에게만 접근되도록 관리하여야 하고 해당 자산의 이동, 폐기 등 처리시 정보보호최고책임자의 승인 하에 처리

4.2 'M'급 정보자산: 업무상 회사 내부에서 취급되어야 하고 외부 반출 시 상당한 문제를 야기하거나 손실을 가져오는 정보자산으로서 '업무상 접근 권한을 가진 한정된 직원'에게만 접근되도록 관리되어야 하고 해당 자산의 이동, 폐기 등 처리시 정보보호책임자의 승인 하에 처리

4.3 'L'급 정보자산: 상기 'H'급, 'M'급 정보자산 이외의 정보자산으로 회사 외부에 반출되어도 회사의 업무 활동에 끼치는 영향이 미미한 정보자산으로서 해당 자산의 이동, 폐기 등 처리시 정보자산관리담당자의 책임 하에 처리

5. 정보자산 목록의 유지관리

5.1 정보자산관리담당자는 관리목록 상의 정보자산에 대한 중요도를 재평가하기 위해 정기적으로 실사를 수행할 수 있으며, 자산목록의 유지·관리 활동을 수행한다.

5.2 정보자산을 도입하거나 새로운 정보자산이 생성될 때에는 다음 각 호의 절차에 따라 정보자산 목록을 작성하여야 한다.

가. 정보자산관리담당자는 정보자산을 도입하거나 새로운 자산이 생성될 때 정보자산 목록 작성

나. 해당 정보자산관리담당자는 본 지침에서 제시한 정보자산 목록 작성방법에 따라 '별지 1. 자산목록 관리대장'의 양식에 정보자산 목록 작성.

5.3 정보자산이 추가, 변경, 폐기될 경우 정보자산 분류기준에 따라 정보자산을 분류하고 목록을 작성하여야 하며, 변경이력을 관리하여야 한다.

제13조 (기타 정보자산의 관리)

1. 기타 정보자산 관리대상

출력 화면, 휴대용 저장매체(테이프, CD/DVD, USB 메모리, 이동식 하드디스크 등),각종 데이터, 전자 문서 등(이하 '기타 정보자산'이라 한다)의 유·무형 정보자산을 대상으로 한다.

2. 기타 정보자산의 보호등급 분류

기타 정보자산의 보호등급은 다음 각 호와 같다.

1) 'H'급 정보: 회사 내·외부에 부당하게 공개되거나 누설될 경우, 회사의 조직 활동에 중대한 영향을 미칠 가능성이 있는 정보로서 '업무상 접근 권한을 가진 한정된 직원'에게만 제공되도록 관리되어야 하는 다음 각 목의 정보

가) 핵심정보: 업무상 중요하게 취급되는 정보
나) 개인정보: 개인을 식별할 수 있는 정보

2) 'M'급 정보: 업무상 회사 내부에서 취급되어야 하는 정보로서, 외부 유출 시 상당한 문제를 야기하거나 손실을 가져와 취급 및 배포를 통제해야 하는 다음 각 목의 정보

가) 업무정보: 전자결재관련정보, 부서별 업무정보 등 업무상 중요하게 취급되어야 하는 정보로서 별도 관리책임자 혹은 업무담당자만이 취급 가능한 정보
나) 회사 내 공개정보: 회사 내 직원이 사용 가능한 게시판, 공용문서 등을 포함하며 회사 외 유출을 억제하여야 하는 정보

3) 'L'급 정보: 상기 'H'급, 'M'급 정보 이외의 정보로 회사 외부에 공표되거나 공개할 수 있는 홈페이지 정보, 공개 정보 등

4) 가비아 공공 zone 클라우드 정보시스템과 밀접히 연관된 데이터의 경우 '별지 5. 클라우드 시스템 데이터 평가표' 내용을 기반으로 클라우드 시스템 흐름에 기반한 특수한 평가 기준, 사전에 식별 가능한 데이터 유형, 유형별 보안등급 등의 상세 내용을 미리 정의하고, 이를 데이터 중요도 등급에 우선하여 준용한다.(단, 해당 문서에 없는 클라우드 관련 업무 데이터의 중요도 평가는 상기 1호~3호의 내용을 기반으로 평가해야 한다.) 또한 정보보호담당자는 연 1회로 해당 문서를 검토하여 문제가 없는지 확인하고 업데이트할 의무가 있으며, 정보보호책임자는 연 1회 해당 문서를 승인/관리할 책임을 가진다.

3. 기타 정보자산의 관리

1) 기타 정보자산의 효율적인 관리를 위하여 각 자산관리 바코드를 부착하여 관리한다. 단, 물리적 실체가 없는 정보자산(데이터) 등의 경우 예외로 한다.
2) 보안관련 사건의 기록은 기타 정보자산에 준하여 관리하며 "침해사고대응지침"에 따른다.

4. 기타 정보자산의 처리 절차

1) 기타 정보자산의 보호등급별 사용, 저장, 전송, 삭제 등(이하 '처리'라 한다)은 아래의

절차에 따른다.

가) 'H'급 정보의 처리는 정보보호최고책임자의 승인 하에 처리함을 원칙으로 한다.

나) 'M'급 정보의 처리는 정보보호책임자의 승인 하에 처리함을 원칙으로 한다.

다) 'L'급 정보의 처리는 정보자산관리담당자에게 보고 후 처리함을 원칙으로 한다.

2) 기타 정보자산의 불용처리

가) 기타 정보자산을 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 정보자산책임자의 승인 하에 수록된 자료가 유출되지 않도록 보안 조치하여야 한다.

나) 인쇄물, 출력화면을 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 해당 정보를 알아볼 수 없도록 분쇄기를 사용하거나 소각 처리하여야 한다.

다) 정보시스템 저장매체 및 자료를 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 '별지 3. 정보시스템 저장매체·자료별 폐기 절차'에 따르며, 이는 구매총무팀에서 작성 후 품의를 진행한다.

라) 서비스 운영 시 취득한 개인정보의 불용처리(교체·반납·양여·폐기 등)는 국내에서만 처리하며 국외 이전을 하지 않는다.

마) 서비스 운영 시 취득한 데이터는 서비스가 해지되면 반환하지 않고 바로 폐기한다.

부칙

제14조 (시행일)

본 지침은 정보보호위원회 의결 완료일부터 시행된다.

제15조 (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

제16조 (경과조치)

특별한 사유에 의하여 본 지침에 정하는 요건을 충족하지 못한 경우에는 발생일로부터 3 개월 이내에 개선방안을 강구하여야 한다.

제4장 관련서식

별지 1. 자산목록관리대장

별지 2. 클라우드 서비스 정보통신망 구성도

별지 3. 정보시스템 저장매체•자료별 폐기 절차

별지 4. 자산 중요도 평가표

별지 5. 클라우드 시스템 데이터 평가표

별지 1. 자산목록관리대장(샘플)

	구분	자산명	설명	대수	위치	소유자	관리자	담당자	관리부서	업체정보	C	I	A	등급
1														
2														
3														
4														

- 세부 내역 '자산목록대장' 참조

- 해당 자산의 유형, 가치, 소유자, 관리자, 사용자 등이 명시된 자산목록 필요

별지 2. 클라우드 시스템 구성도

- 세부 내역 '시스템 구성도' 참조

별지 3. 정보시스템 저장매체·자료별 폐기 절차

정보시스템 저장매체・자료별 폐기 절차

	구매총무팀		정보보호담당자	정보보호책임자
협조		승인		

수행 담당자			
부 서 명		직 급	
자 산 명			
성 명			(인 또는 서명)

저장자료 / 저장매체	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
광디스크 (CD・DVD 등)	㉮	㉮	㉮
자기 테이프	㉮・㉯중 택일	㉮・㉯중 택일	㉮
반도체메모리 (EEPROM, USB 등)	㉮・㉰중 택일	㉮・㉰중 택일	㉮・㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮・㉯・㉰중 택일	㉮・㉯중 택일

㉮: 완전파괴(소각・파쇄・용해), ㉯: 전용 소자장비 이용 저장자료 삭제

㉰: 완전포맷 3회 수행 ㉱: 완전포맷 1회 수행

별지 4. 자산 중요도 평가표

자산 중요도 평가표

승인	정보보호담당자	정보보호책임자

*** 평가 수행일:**

수행 담당자			
부 서 명		직 급	
성 명	(인 또는 서명)		

*** 중요도 평가 자산 목록**

평가범위		물리 자산 + 가상 자원(OS Image, 하이퍼바이저)					
구분	자산명	항목별 점수(1~3)			총점	평가 등급	평가자 총평(서술형)
		기밀성	무결성	가용성			

별지 5. 클라우드 시스템 데이터 평가표 (샘플)

클라우드 시스템 데이터 평가표

	정보보호담당자	정보보호책임자
승인		

1. 문서 목표

클라우드 시스템 운영상 정형화된 데이터 유형을 식별하여, 해당되는 데이터들에 대해서는 클라우드 시스템 흐름의 특수성을 고려한 2. 평가 기준을 적용하고 이를 준용하여 보다 세밀한 클라우드 시스템 데이터 중요도 평가가 이루어질 수 있도록 한다.

2. 평가 기준

(1) 1차 기준

데이터 관리에 대한 법적 요구	해당 데이터 유형에 대한 법적 요구사항이 없는가? (Y/N)
외부 공개 가능 여부	외부 공개가 가능한 데이터 유형인가? (Y/N)
데이터 소유권 여부	해당 데이터는 당사 소유의 데이터인가? (Y/N)

* 위 세가지 문항에서 모두 Y인 데이터는 2차 기준을 적용하지 아니하고 'L 등급'의 중요도를 부여한다.

* 위 세가지 문항에서 한 개라도 N인 데이터는 2차 기준을 적용하여 데이터 중요도를 평가한다.

(2) 2차 기준(데이터 사고 영향)

가) 관리적 가용성에 대한 영향도	1~5점으로 번호 부여(높은 숫자일수록 영향도 高)
나) 시스템 가용성에 대한 영향도	1~5점으로 번호 부여(높은 숫자일수록 영향도 高)
다) 서비스 브랜드에 대한 영향도	1~5점으로 번호 부여(높은 숫자일수록 영향도 高)
라) 사고 발생 시 시스템 영향 범위	VM 단위: 1점 / NC 단위: 2점 / CC 및 SC단위: 4점 / Network 단위: 5점 / Storage 단위: 5점

* 총점이 10점 이상이면 중요도를 'H 등급'으로 부여한다.

* 총점이 10점 미만이면 중요도를 'M 등급'으로 부여한다.

3. 평가 결과표

*** 평가일:** 년 월 일 **/ 평가자:**

데이터 유형	데이터 발생 자산	경로 정보	보안등급

4. 보안등급별 접근/열람 권한자 기준

H 등급	1. 정보보호담당자 이상의 주요 정보보호직무자만 접근/관리 가능 2. 정보시스템 주요 접근 직무자에 한정하여 열람 가능
M 등급	1. 정보시스템 주요 접근 직무자에 한정하여 시스템적 접근/관리 가능 2. 가비아 클라우드사업부/정보보안실 전체 인원 열람 가능
L 등급	1. 정보시스템 주요 접근 직무자에 한정하여 시스템적 접근/관리 가능 2. 가비아 클라우드사업부/정보보안실/인프라운영실 전체 인원 열람 가능

첨부: 데이터 유형별 상세 평가 점수

데이터 유형	데이터 발생 자산	1 차 평가 (N 개수)	2 차 평가 항목별 점수				2 차 평가 총점	최종 보안 등급
			가)	나)	다)	라)		