|  |
| --- |
| **[23년도 K카드사 개인정보 수탁사 점검 프로젝트]** |
| **법무법인 대한**  **수탁사 점검 결과보고서** |
| *Version 1.0* |

**2023. 12. 14**



**제·개정 이력**

| **버전** | **변경일** | **변경 사유** | **변경 내용** | **작성자** | **비고** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 2023-12-14 | 최초작성 | 수탁사 점검 보고서 서식 수립 | 정민식 |  |
| 1.1 | 2023-12-17 | 수정작성 | 진단 결과 수정 | 정민식 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **개요**
   1. **점검 목적**

K카드사의 개인정보처리 업무를 위탁 수행하는 수탁사의 개인정보 보호수준을 파악하여, K카드사 고객정보의 안전한 처리 여부를 확인하고, 식별한 미흡사항에 대해 수탁사 현황에 맞는 개선방안을 수립하여 수탁사의 정보보호수준 향상을 도모함에 목적이 있음

* 1. **수탁사 정보 및 처리업무**

| **No.** | **수탁사명** | **위탁업무 유형** | **위탁 업무** |
| --- | --- | --- | --- |
| 05 | 법무법인 대한 | PC기반 | 소송위임 사건처리  개인정보 유출관련 손해배상 청구 |

* 1. **점검 방식 및 일정**

| **점검 방식** | **점검 일시** | **수탁사 사업장 주소** |
| --- | --- | --- |
| 대면 점검 | 2023년 12월 5일  / 14:00 ~ 17:00 | 서울시 중구 퇴계로 100 스테이트타워 남산 8층 |

* 1. **담당자 정보**

| **ㅇㅇㅇ 계약 부서 / 담당자** | **수탁사 담당자 성명** | **수탁사 담당자 전화번호 / 이메일 주소** |
| --- | --- | --- |
| 변호사 |  | 02-316-xxxx |
|  |  |

* 1. **점검인력 정보**

| **소속** | **성명** | **직책** | **이메일 주소** |
| --- | --- | --- | --- |
| 컨설팅커벨 | 정민식 | 책임 컨설턴트 | wjdalstlr@gmail.com |
| 컨설팅커벨 | 이주형 | 선임 컨설턴트 | dlwngud@gmail.com |

| **수탁사**  **개인정보취급자 수** | **개인정보 처리 수량**  **(K카드사 개인정보 限)** | **정보보호 솔루션 및 보호조치** |
| --- | --- | --- |
| 3명 | 월 약 50건 | VDI, 안티바이러스(V3), DLP, VPN, 암호화 조치(AES-256), 보안USB, 파일삭제프로그램 |
| **자체 개인정보**  **처리시스템 운용 여부** | **개인정보 저장 유형** |
| O | 개인 PC, AWS클라우드 |
| **처리 개인정보 종류** | **파기확인서 제출** |
| 이름, 주민등록번호, 연락처, 주소 | O |

* 1. **수탁사 개요**



1. **점검 결과**
   1. **총평**

법무법인 대한은 PC기반 유형의 수탁사로서, 최초 69개 점검기준으로 점검을 수행하였으나, 수탁사 업무 현황에 따라 34개의 점검기준으로 추가적으로 클라우드 점검을 수행하였다.

법무법인대한은 내부관리계획 수립 및 패스워드 기준 수립에서 양호한 보안수준을 유지하고 있으나, 정보보안서약서를 정기적으로 재징구하지 않고, 위기대응 절차가 수립되어 있지 않음과 같은 미흡사항이 식별되어 정보보호서약서를 정기적으로 재징구하고, 위기대응 절차 수립 등의 개선방안을 수립하고 이행조치 계획을 수립함.

* 1. **점검 결과**

점검 결과에 대한 판단 기준과 보안준수율에 대한 산정 기준은 아래와 같음

| **진단 기준** | **반영 값** | **설명** |
| --- | --- | --- |
| 양호 (Y) | 1 | · 개인정보보호 통제가 구현되어 실행되고 있는 상태 |
| 미흡 (P) | 0.5 | · 개인정보보호 통제가 일부만 적용되어 있는 상태 |
| 취약 (N) | 0 | · 개인정보보호 통제가 이루어지지 않는 상태 |
| 해당사항 없음 (N/A) | - | · 진단 항목에 해당사항 없음 |

|  |
| --- |

점검 결과 법무법인 대한은 보안준수율이 63.79%로 미흡수준이며, 32개의 양호(Y), 8개의 미흡(P), 17개의 취약(N)으로 식별되었습니다.

| **No.** | **영역** | **분류 기준** | **점검항목** | **진단 결과** |
| --- | --- | --- | --- | --- |
| 1 | **관리적 영역** | **개인정보보호 관리체계** | 개인정보보호를 위한 내부관리계획을 수립하고 있는가? | Y |
| 2 | **관리적 영역** | **개인정보보호 관리체계** | 내부관리계획서는 승인을 받아 공표하고 있는가? | Y |
| 3 | **관리적 영역** | **개인정보보호 관리체계** | 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? | Y |
| 4 | **관리적 영역** | **개인정보보호 관리체계** | 내부관리계획의 이행실태를 점검하고 있는가? | Y |
| 5 | **관리적 영역** | **개인정보보호 관리체계** | 개인정보 처리방침을 수립하여 정보주체가 확인할 수 있도록 공개하고 있는가? | Y |
| 6 | **관리적 영역** | **개인정보보호 관리체계** | 계정관리 절차를 수립하고 있는가? | Y |
| 7 | **관리적 영역** | **개인정보보호 관리체계** | 개인정보처리시스템의 패스워드 기준을 수립하고 있는가? | Y |
| 8 | **관리적 영역** | **개인정보보호 관리체계** | 중요정보에 대한 암호화 적용 기준을 수립하고 있는가? | Y |
| 9 | **관리적 영역** | **개인정보보호 관리체계** | 암호화 키는 적절한 절차에 따라 안전하게 관리되고 있는가?  [클라우드1]  Key Pair(PEM)를 통해 EC2 인스턴스에 접근하고 있는가?  [클라우드2]  Key Pair(PEM) File의 보관 위치가 쉽게 유추할 수 없는 공간에 보관되어 있는가? | P |
| 10 | **관리적 영역** | **개인정보보호 관리체계** | 보조저장매체에 대한 반출입 절차를 수립하고, 이에 따라 반출입이 이루어지고 있는가? | Y |
| 11 | **관리적 영역** | **개인정보보호 관리체계** | 보조저장매체를 허가없이 사용 할 수 없도록 통제 기준을 수립하고 있는가? | Y |
| 12 | **관리적 영역** | **개인정보보호 관리체계** | 무선통제 기준과 사용 승인절차를 수립하고 있는가? | N/A |
| 13 | **관리적 영역** | **개인정보보호 관리체계** | 개인정보 파기 절차 및 기준을 수립하고, 파기 후 이력 관리를 하고 있는가? | Y |
| 14 | **관리적 영역** | **개인정보보호 관리체계** | 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가?  [클라우드]  클라우드 리소스 백업 정책이 존재하는가? | N |
| 15 | **관리적 영역** | **개인정보보호 관리체계** | 개인정보보호 자체 점검을 정기적으로 시행하고 있는가? | Y |
| 16 | **관리적 영역** | **개인정보보호 관리체계** | 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? | N |
| 17 | **관리적 영역** | **정보보호 조직** | 개인정보보호책임자 및 담당자를 지정하고 있는가? | Y |
| 18 | **관리적 영역** | **정보보호 조직** | 개인정보보호 조직 및 인력의 역할과 책임이 정의되어 있는가? | Y |
| 19 | **관리적 영역** | **개인정보취급자 관리** | 개인정보취급자의 목록을 관리하고 있는가? | N |
| 20 | **관리적 영역** | **개인정보취급자 관리** | 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | P |
| 21 | **관리적 영역** | **개인정보취급자 관리** | 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? | Y |
| 22 | **관리적 영역** | **개인정보 재위탁** | 수탁자의 재위탁을 원칙적으로 금지하고 있으나 계약 이행을 위하여 불가피하게 재위탁을 하는 경우, 당사의 기준에 따라 재위탁하는가?  [녹취]  녹취 근거에 따라 수탁자가 개인정보 수집범위를 준수하고 있는가?  [녹취2]  수탁자의 재위탁을 원칙적으로 금지하고 있으나 계약 이행을 위하여 불가피하게 재위탁을 하는 경우, 당사의 기준에 따라 재위탁하는가? | N/A |
| 23 | **관리적 영역** | **개인정보 재위탁** | 재위탁이 다년간 계약된 경우 계약사항을 매년 검토하고 있는가? | N/A |
| 24 | **관리적 영역** | **개인정보 재위탁** | 재수탁자의 목적 달성 후 파기, 반납에 관한 사항 및 파기확인서에 대해 확인하고 있는가? | N/A |
| 25 | **관리적 영역** | **개인정보 재위탁** | 재수탁자 및 재수탁자의 임직원의 보안서약서를 제출하도록 관리하고 있는가? | N/A |
| 26 | **관리적 영역** | **개인정보 재위탁** | 재수탁자의 개인정보취급자 대상에 대해 관리·감독 하고 있는가? | N/A |
| 27 | **관리적 영역** | **개인정보 처리** | 개인정보는 위탁목적에 한하여 이용하고 있는가?  [녹취]  수탁자의 녹취 근거가 계약서 등에 존재하는가? | Y |
| 28 | **관리적 영역** | **개인정보 처리** | 수탁사가 자체적으로 고객정보 수집시 정보 수집과 관련하여 고객의 사전동의를 관계 법령에 따라 적절히 받고 있는가?  [녹취]  수탁자가 개인(신용)정보 녹취 시 고객의 사전동의를 관계법령에 따라 적절히 받고 있는가? | Y |
| 29 | **관리적 영역** | **개인정보 처리** | 수탁사가 타 수탁업체와 개인(신용)정보를 공유 하고 있는가?  [녹취]  수탁사가 타 수탁업체와 녹취 정보를 공유 하고 있는가? | Y |
| 30 | **관리적 영역** | **개인정보 처리** | 타 수탁업체와 정보 공유시, 정보 공유 근거가 계약서, 약정서 등에 존재하는가? | N/A |
| 31 | **기술적 영역** | **접근제어** | 사용자별 계정(1인1계정)을 부여하여 관리하고 있는가?  [클라우드1]  관리자 권한을 보유한 다수 계정이 존재하지 않고 불필요한 계정이 존재하지 않는가?  [클라우드2]  IAM 사용자 계정(1인1계정)을 부여하여 관리하고 있는가?  [클라우드3]  사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있는가?  [클라우드4]  IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재하지 않는가? | N |
| 32 | **기술적 영역** | **접근제어** | 관리자를 제외한 계정의 권한은 최소한으로 제한하여 부여하고 있는가?  [녹취 영역1]  수탁자의 녹취시스템 및 관련 백업 시스템 등에 대해 권한 없는 자가 내/외부에서 접근 불가능한가?  [녹취 영역2]  수탁사의 녹취시스템에 대해 사용자 계정 및 접근권한을 관리하고 있는가?  [클라우드 1]  Admin Console 계정을 서비스 용도로 사용하지 않는가?  [클라우드 2]  AWS Admin Console 계정에 Access Key가 존재하지 않고 IAM 사용자 계정에 대한 Access Key 사용 주기가 60일 이내인가?  [클라우드 3]  인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가?  [클라우드 4]  네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가?  [클라우드 5]  기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | N |
| 33 | **기술적 영역** | **접근제어** | 퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가? | P |
| 34 | **기술적 영역** | **접근제어** | 개인정보취급자의 권한변경 이력을 기록하고 있는가? | P |
| 35 | **기술적 영역** | **접근제어** | 정기적으로 패스워드를 변경하고 관리하고 있는가?  [클라우드1]  AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 활성화 되어 있는가?  [클라우드2]  Admin Console 및 IAM 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을  설정하고 있는가? | Y |
| 36 | **기술적 영역** | **접근제어** | 개인정보처리시스템으로 일정시간 이상 업무처리를 하지 않는 경우, 시스템 접속을 자동 차단하고 있는가? | Y |
| 37 | **기술적 영역** | **접근제어** | 일정시간 이상 업무처리를 하지 않는 경우, 화면보호기 설정이 적용되어 있는가? | Y |
| 38 | **기술적 영역** | **접근제어** | 개인정보처리시스템 접속 제한 설정이 적용되어 있는가? | P |
| 39 | **기술적 영역** | **접근통제** | 모바일 기기를 통해 개인정보를 처리하는 경우, 안전한 보안 조치를 적용하고 있는가? | N/A |
| 40 | **기술적 영역** | **접근통제** | 외부망에서 개인정보처리시스템으로의 접근을 차단하고 있는가? | Y |
| 41 | **기술적 영역** | **접근통제** | 인터넷망(사외)에서 고객정보 관리시스템에 접속을 차단하고 있는가?(모바일접속,앱 포함)  [클라우드1]  보안 그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있지 않는가?  [클라우드2]  보안 그룹 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하지 않는가?  [클라우드3]  네트워크 ACL 내 인/아웃바운드에 대한 모든 트래픽이 허용되어 있지 않는가?  [클라우드4]  라우팅 테이블 내 ANY 정책이 설정되어 있지 않고 서비스 타깃 별로 설정되어 있는가?  [클라우드5]  인터넷 게이트웨이에 불필요하게 연결된 NAT 게이트웨이가 존재하지 않는가?  [클라우드6]  외부 통신이 필요한 리소스가 NAT 게이트웨이가 연결되어 있는가?  [클라우드7]  퍼블릭 액세스 차단이 설정되어 있거나, 퍼블릭 액세스를 허용할 경우 ACL을 버킷 소유자에게만 설정하고 있는가? | Y |
| 42 | **기술적 영역** | **접근통제** | 고객관리시스템 접근에 대한 사후 감사를 수행하고 있는가? | P |
| 43 | **기술적 영역** | **접근통제** | 내부에서 개인정보처리시스템 접근 시 접근통제를 적용하는가? | N |
| 44 | **기술적 영역** | **접근통제** | 보안장비를 우회한 인터넷 접속을 방지하기 위하여 무선랜을 통제하고 있는가? | N/A |
| 45 | **기술적 영역** | **접속기록** | 개인정보처리시스템 접속이력에 관한 정보를 기록하고 있는가?  [녹취]  녹취시스템의 접속기록을 일정기간 이상 보관하고 있는가? | N |
| 46 | **기술적 영역** | **접속기록** | 개인정보처리시스템의 접속기록을 일정기간 이상 보관하고 있는가?  [녹취]  녹취시스템의 접속기록을 일정기간 이상 보관하고 있는가? | Y |
| 47 | **기술적 영역** | **접속기록** | 개인정보처리시스템의 접속기록에 대해 적정성 여부를 점검하고 있는가?  [녹취]  녹취시스템의 접속기록에 대해 적정성 여부를 점검하고 있는가?  [클라우드1]  CloudTrail 관련 로그 파일에 SSE-KMS 암호화 설정이 되어있는가?  [클라우드2]  로그 그룹 생성 시 "KMS key ARN" 을 설정하여 사용하고 있는가?  [클라우드3]  AWS 사용자 계정(Console, IAM)의 로깅이 설정되어 있는가?  [클라우드4]  CloudWatch 로그 스트림으로 보관하고 있는가?  [클라우드5]  CloudWatch 로그 스트림으로 보관하고 있는가?  [클라우드6]  로그를 보관하고 있는 버킷의 "서버 액세스 로깅"이 설정되어 있는가?  [클라우드7]  VPC 플로우 로그 설정이 존재하는 경우  [클라우드8]  AWS 서비스 로그를 기준(최소 1년 이상)에 맞게 보관하고 있는가? | N |
| 48 | **기술적 영역** | **안전한 송∙수신** | 수탁사 내부에서 개인정보 송·수신 시 암호화를 적용하고 있는가? | N/A |
| 49 | **기술적 영역** | **안전한 송∙수신** | 당사와 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? | N |
| 50 | **기술적 영역** | **안전한 송∙수신** | 수탁사 내 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가?  [클라우드]  클라우드 리소스 통신 구간 내 암호화 설정이 되어 있는가? | N |
| 51 | **기술적 영역** | **데이터 암호화** | 중요정보 및 인증정보 저장 시 암호화하여 저장하고 있는가? | Y |
| 52 | **기술적 영역** | **데이터 암호화** | 개인정보를 PC에 저장하는 경우 암호화하여 저장하고 있는가?  [녹취]  녹취 파일을 저장하는 경우 암호화하여 저장하고 있는가?  [클라우드1]  EBS 및 볼륨 리소스에 암호화가 활성화되어 있는가?  [클라우드2]  RDS 데이터베이스 암호화가 활성화되어 있는가?  [클라우드3]  Amazon S3 키(SSE-S3)로 서버 측 암호화 사용 또는 SSE-KMS로 서버 측 암호화가  설정되어 있는가? | Y |
| 53 | **기술적 영역** | **개발 및 테스트** | 개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터를 사용하는가? | N/A |
| 54 | **기술적 영역** | **개인정보 관리 및 파기** | 업무목적이 달성된 개인정보를 즉시 파기하고 있는가?  [녹취]  보존 기한이 만료된 녹취 파일을 파기하고 있는가? | Y |
| 55 | **기술적 영역** | **개인정보 관리 및 파기** | 다른 법령에 의거, 개인정보를 보관하여야 할 경우 물리적/논리적으로 분리하여 저장하고 있는가? | N |
| 56 | **기술적 영역** | **개인정보처리시스템** | 개인식별번호 및 신용카드번호 등의 중요정보를 출력(화면/인쇄)하는 경우 마스킹 처리하고 있는가? | N |
| 57 | **기술적 영역** | **개인정보처리시스템** | 개인정보처리시스템을 대상으로 정기적인 취약점 진단을 시행하고 있는가?  [녹취 영역1]  녹취시스템 관리현황을 정기적으로 점검하고 있는가?  [녹취 영역2]  수탁사의 녹취시스템에 대해 수탁사 또는 위탁사가 모의해킹 테스트 등 보안 취약점 점검을 수행하고 있는가? | Y |
| 58 | **기술적 영역** | **악성프로그램 관리** | 안티바이러스 소프트웨어를 설치 및 운영하고 있는가? | Y |
| 59 | **기술적 영역** | **매체제어** | 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? | Y |
| 60 | **기술적 영역** | **매체제어** | 기본 및 사용자 공유폴더 사용을 제한하고 있는가?  [클라우드]  RDS 서브넷 그룹 내 불필요한 가용영역이 존재하지 않는가? | P |
| 61 | **기술적 영역** | **매체제어** | 개인정보취급자 PC에 유해소프트웨어를 설치하지 않도록 통제하고 있는가? | N |
| 62 | **기술적 영역** | **매체제어** | 출력 시 워터마크를 적용하고 있는가? | Y |
| 63 | **기술적 영역** | **단말기관리** | 개인정보를 처리하는 중요단말기의 인터넷 사용을 제한하고 있는가? | P |
| 64 | **기술적 영역** | **접속통제** | 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성ㆍ운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하고 있는가? | Y |
| 65 | **기술적 영역** | **단말기관리** | 개인정보취급자 PC는 최신 패치를 적용하고 있는가? | Y |
| 66 | **기술적 영역** | **단말기관리** | 개인(신용)정보가 포함된 종이인쇄물 출력시 프린터 기기 자체에 저장된 파일을 관리하고 있는가? | N |
| 67 | **물리적 영역** | **보호구역 관리** | 보호구역 지정 기준 및 각 보호구역 별 보호대책을 수립하고 있는가? | N |
| 68 | **물리적 영역** | **보호구역 관리** | 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? | N |
| 69 | **물리적 영역** | **출력물 관리** | 개인정보가 포함된 문서 출력 시 안전조치를 취한 후 안전한 장소에 보관하며, 중요정보를 이동하는 경우 기밀성 및 무결성을 보장하도록 통제하고 있는가? | N |
| **보안준수율** | | | | **63.79%** |

* 1. **주요 미흡사항 및 보호대책 수립 현황**

| **점검 항목** | **개선방안** |
| --- | --- |
| 암호화 키는 적절한 절차에 따라 안전하게 관리되고 있는가? | 암호화키 관리 절차, 기준 수립 필요. |
| 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가? | 백업 및 복구 계획 등을 포함한 위기대응  절차를 수립하여야 함. |
| 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? | 저장된 개인정보는 사용중을 제외하고는 마스킹 처리 필요. |
| 개인정보취급자의 목록을 관리하고 있는가? | 개인정보취급자에 대한 목록을 관리 필요. |
| 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | 개인정보보호 서약서를 정기적으로 재징구하여야 함. |
| 퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가? | 불필요한 계정 여부 확인 및 현행화 필요. |
| 개인정보취급자의 권한변경 이력을 기록하고 있는가? | 계정권한 관리 필요. |
| 개인정보처리시스템 접속 제한 설정이 적용되어 있는가? | 불법 로그인 시도 시 경고 필요. |
| 고객관리시스템 접근에 대한 사후 감사를 수행하고 있는가? | 월 1회 사후감사 실시 필요. |
| 내부에서 개인정보처리시스템 접근 시 접근통제를 적용하는가? | 내부 개인정보처리시스템 접근 통제 필요 |
| 개인정보처리시스템 접속이력에 관한 정보를 기록하고 있는가? | 처리한 정보주체 정보, 수행업무 등 접속기록의 상세내용 저장 필요 |
| 개인정보처리시스템의 접속기록에 대해 적정성 여부를 점검하고 있는가? | 개인정보처리시스템의 접속기록 및  개인정보 다운로드 사유에 대해 적정성  여부를 점검 필요. |
| 당사와 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? | 안전한 전송 수단(VPN, 전용선 등) 적용 필요. |
| 수탁사 내 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? | 안전한 전송 수단(VPN, 전용선 등) 적용 필요. |
| 다른 법령에 의거, 개인정보를 보관하여야 할 경우 물리적/논리적으로 분리하여 저장하고 있는가? | 개인정보를 별도의 물리적/논리적 DB에 분리 필요. |
| 개인정보 표시제한 및 이용 시 보호조치 | 중요 정보에 대해 마스킹을 하여야 함. |
| 기본 및 사용자 공유폴더 사용을 제한하고 있는가? | 공유폴더 속 데이터 삭제 조치 필요. |
| 개인정보취급자 PC에 유해소프트웨어를 설치하지 않도록 통제하고 있는가? | 유해소프트웨어 설치 제한 필요. |
| 개인정보를 처리하는 중요단말기의 인터넷 사용을 제한하고 있는가? | 변호사PC(로컬)에 대한 인터넷 사용 차단 필요. |
| 개인(신용)정보가 포함된 종이인쇄물 출력시 프린터 기기 자체에 저장된 파일을 관리하고 있는가? | 프린터 기기에 저장된 메모리 또는 스풀 주기적 삭제 필요. |
| 보호구역 지정 기준 및 각 보호구역 별 보호대책을 수립하고 있는가? | 보호구역 지정 기준 수립 및 보호구역 별 보호대책 명시 필요 |
| 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? | 보호구역 중요도별로 구분 및 보호구역 별 보호대책 필요 |
| 개인정보가 포함된 문서 출력 시 안전조치를 취한 후 안전한 장소에 보관하며, 중요정보를 이동하는 경우 기밀성 및 무결성을 보장하도록 통제하고 있는가? | 캐비넷에 대한 별도의 잠금장치 시건 필요. |

* 1. **클라우드 점검 결과**

클라우드 점검 결과에 대한 판단 기준과 보안준수율에 대한 산정 기준은 아래와 같음

| **진단 기준** | **반영 값** | **설명** |
| --- | --- | --- |
| 양호 (Y) | 1 | · 클라우드 운영 관리가 적절히 되고 있는 상태 |
| 미흡 (P) | 0.5 | · 클라우드 운영 관리가 일부만 적용되어 있는 상태 |
| 취약 (N) | 0 | · 클라우드 운영 관리가 이루어지지 않는 상태 |
| 해당사항 없음 (N/A) | - | · 진단 항목에 해당사항 없음 |

|  |
| --- |

클라우드 점검 결과 법무법인 대한은 보안준수율이 66%로 미흡수준이며, 16개의 양호(Y), 1개의 미흡(P), 8개의 취약(N)으로 식별되었습니다.

| **No.** | **영역** | **분류 기준** | **점검항목** | **진단 결과** |
| --- | --- | --- | --- | --- |
| 1 | **관리적 영역** | **계정 관리** | 관리자 권한을 보유한 다수 계정이 존재하지 않고 불필요한 계정이 존재하지 않는가? | Y |
| 2 | **관리적 영역** | **계정 관리** | IAM 사용자 계정(1인1계정)을 부여하여 관리하고 있는가? | N |
| 3 | **관리적 영역** | **계정 관리** | 사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있는가? | N |
| 4 | **관리적 영역** | **계정 관리** | IAM 그룹에 포함된 사용자 계정 중 불필요한 계정이 존재하지 않는가? | Y |
| 5 | **관리적 영역** | **계정 관리** | Key Pair(PEM)를 통해 EC2 인스턴스에 접근하고 있는가? | Y |
| 6 | **관리적 영역** | **계정 관리** | Key Pair(PEM) File의 보관 위치가 쉽게 유추할 수 없는 공간에 보관되어 있는가? | Y |
| 7 | **관리적 영역** | **계정 관리** | Admin Console 계정을 서비스 용도로 사용하지 않는가? | Y |
| 8 | **관리적 영역** | **계정 관리** | AWS Admin Console 계정에 Access Key가 존재하지 않고 IAM 사용자 계정에 대한 Access Key 사용 주기가 60일 이내인가? | N/A |
| 9 | **관리적 영역** | **계정 관리** | AWS 계정 및 IAM 사용자 계정 로그인 시 MFA가 활성화 되어 있는가? | Y |
| 10 | **관리적 영역** | **계정 관리** | Admin Console 및 IAM 계정의 패스워드 복잡성 기준 준수 및 암호 만료/재사용 제한을  설정하고 있는가? | Y |
| 11 | **관리적 영역** | **권한 관리** | 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | N |
| 12 | **관리적 영역** | **권한 관리** | 네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | N |
| 13 | **관리적 영역** | **권한 관리** | 기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | N |
| 14 | **관리적 영역** | **가상 리소스 관리** | 보안 그룹 내 인/아웃바운드의 포트가 Any로 허용되어 있지 않는가? | Y |
| 15 | **관리적 영역** | **가상 리소스 관리** | 보안 그룹 인/아웃바운드 규칙 내 불필요한 정책(Source, Destination)이 존재하지 않는가? | Y |
| 16 | **관리적 영역** | **가상 리소스 관리** | 네트워크 ACL 내 인/아웃바운드에 대한 모든 트래픽이 허용되어 있지 않는가? | N/A |
| 17 | **관리적 영역** | **가상 리소스 관리** | 라우팅 테이블 내 ANY 정책이 설정되어 있지 않고 서비스 타깃 별로 설정되어 있는가? | Y |
| 18 | **관리적 영역** | **가상 리소스 관리** | 인터넷 게이트웨이에 불필요하게 연결된 NAT 게이트웨이가 존재하지 않는가? | N/A |
| 19 | **관리적 영역** | **가상 리소스 관리** | 외부 통신이 필요한 리소스가 NAT 게이트웨이가 연결되어 있는가? | N/A |
| 20 | **관리적 영역** | **가상 리소스 관리** | 퍼블릭 액세스 차단이 설정되어 있거나, 퍼블릭 액세스를 허용할 경우 ACL을 버킷 소유자에게만 설정하고 있는가? | N/A |
| 21 | **관리적 영역** | **가상 리소스 관리** | RDS 서브넷 그룹 내 불필요한 가용영역이 존재하지 않는가? | Y |
| 22 | **관리적 영역** | **운영 관리** | EBS 및 볼륨 리소스에 암호화가 활성화되어 있는가? | N/A |
| 23 | **관리적 영역** | **운영 관리** | RDS 데이터베이스 암호화가 활성화되어 있는가? | N/A |
| 24 | **관리적 영역** | **운영 관리** | Amazon S3 키(SSE-S3)로 서버 측 암호화 사용 또는 SSE-KMS로 서버 측 암호화가  설정되어 있는가? | Y |
| 25 | **관리적 영역** | **운영 관리** | 클라우드 리소스 통신 구간 내 암호화 설정이 되어 있는가? | Y |
| 26 | **관리적 영역** | **운영 관리** | CloudTrail 관련 로그 파일에 SSE-KMS 암호화 설정이 되어있는가? | P |
| 27 | **관리적 영역** | **운영 관리** | 로그 그룹 생성 시 "KMS key ARN" 을 설정하여 사용하고 있는가? | Y |
| 28 | **관리적 영역** | **운영 관리** | AWS 사용자 계정(Console, IAM)의 로깅이 설정되어 있는가? | Y |
| 29 | **관리적 영역** | **운영 관리** | CloudWatch 로그 스트림으로 보관하고 있는가? | N/A |
| 30 | **관리적 영역** | **운영 관리** | CloudWatch 로그 스트림으로 보관하고 있는가? | N/A |
| 31 | **관리적 영역** | **운영 관리** | 로그를 보관하고 있는 버킷의 "서버 액세스 로깅"이 설정되어 있는가? | N |
| 32 | **관리적 영역** | **운영 관리** | VPC 플로우 로그 설정이 존재하는 경우 | N |
| 33 | **관리적 영역** | **운영 관리** | AWS 서비스 로그를 기준(최소 1년 이상)에 맞게 보관하고 있는가? | Y |
| 34 | **관리적 영역** | **운영 관리** | 클라우드 리소스 백업 정책이 존재하는가? | N |
| **보안준수율** | | | | **66%** |

* 1. **클라우드 주요 미흡사항 및 보호대책 수립 현황**

| **점검 항목** | **개선방안** |
| --- | --- |
| IAM 사용자 계정(1인1계정)을 부여하여 관리하고 있는가? | 1인 1계정을 부여하여 운영 하여야 함. |
| 사용자 정보(이름, 이메일, 부서 등)가 IAM 사용자 태그에 설정되어 있는가? | IAM 사용자 태그 설정이 필요함. |
| 인스턴스 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | IAM 사용권한이 각각 서비스 역할에 맞게 설정 하여야 함. |
| 네트워크 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | - IAM 사용 권한에 대해 각각 서비스 역할에  맞게 설정하여 운영하여야 함. |
| 기타 서비스 IAM 사용 권한이 각각 서비스 역할에 맞게 설정되어 있는가? | 역할에 맞게 지정하여 사용 권한을 설정하여야 함. |
| CloudTrail 관련 로그 파일에 SSE-KMS 암호화 설정이 되어있는가? | 암호화 설정유무 확인 필요함. |
| 로그를 보관하고 있는 버킷의 "서버 액세스 로깅"이 설정되어 있는가? | 서버 액세스 로깅을 설정하여야 함. |
| VPC 플로우 로그 설정이 존재하는 경우 | VPC 플로우 로그 설정하여 운영하여야 함. |
| 클라우드 리소스 백업 정책이 존재하는가? | 리소스 백업 정책을 수행하여 운영하여야 함. |