





**제·개정 이력**

| **버전** | **변경일** | **변경 사유** | **변경 내용** | **작성자** | **비고** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 2023-12-25 | 최초작성 | 수탁사 종합결과보고서 서식 수립 | 정민식 |  |
|  |  |  |  |  |  |

**목차**

[**1. 점검 목적 1**](#_heading=h.gjdgxs)

[**2. 점검 근거 1**](#_heading=h.30j0zll)

[**3. 점검 항목 1**](#_heading=h.1fob9te)

[**4. 점검 진단 기준 9**](#_heading=h.3znysh7)

[**4.1. 진단 기준 9**](#_heading=h.2et92p0)

[**4.2. 보안준수율 산출식 9**](#_heading=h.tyjcwt)

[**4.3. 보안준수율 분류 기준 9**](#_heading=h.3dy6vkm)

[**5. 점검 대상 10**](#_heading=h.1t3h5sf)

[**6. 점검 업체 목록 10**](#_heading=h.4d34og8)

[**7. 총평 11**](#_heading=h.2s8eyo1)

[**8. 점검 결과 분석 12**](#_heading=h.17dp8vu)

[**9. 개선 방안 및 제언 14**](#_heading=h.26in1rg)

[**9.1. 주요 시사점 및 개선방향 14**](#_heading=h.wtmv5r4k58wx)

[**9.2. 개선과제 및 기대효과 15**](#_heading=h.6ati3ewqmf21)

**그림 목차**

[[표 1]](#_heading=h.35nkun2) [점검항목](#_heading=h.44sinio)2

[[표 2] 진단기준](#_heading=h.1ksv4uv) 9

[[표 3] 보안준수율 분류 기준](#_heading=h.44sinio) 9

[[표 4] 점검 제외 대상](#_heading=h.2jxsxqh) 10

[[표 5] 점검 업체 목록](#_heading=h.z337ya) 10

# **1. 점검 목적**

본 프로젝트는 K카드사의 업무를 수탁받아 수행하고 있는 18개의 수탁사에 대해 법에서 요구하는 사항의 준수 여부를 점검하여 XXX에 개인정보보호 수준을 평가하고 개선방안을 제시하는 것을 목표로 함

# **2. 점검 근거**

다음과 같은 법률 및 고시를 기반으로 이번 프로젝트의 점검을 수행하였음

* 개인정보보호 관련 회사 규정
* 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
* 신용정보보호법 제17조(처리의 위탁)
* K카드사 개인정보보호 규정 및 ‘개인정보 보안관리 약정서’(위수탁계약)

※ 단, 업무 위탁과 달리 제휴업무(제3자) 제공은 관리∙감독 대상 제외

# **3. 점검 항목**

* 수탁사 점검 항목은 수탁사가 준수하여야 하는 관리적, 기술적, 물리적으로 총 세 가지 영역으로 구성되어 있음
* 관리적 영역 30개, 기술적 영역 36개, 물리적 영역 3개, 녹취 영역 0개, 총 69개 항목으로 구성되어 있음
* 영역별 No는 관리적 영역인 경우 PM, 기술적 영역인 경우 PT, 물리적 영역인 경우 PP로 명시함
* 법률 근거가 명확하지 않은 경우 ‘권고’ 항목으로 분류하고, 법률 근거가 명확한 경우 ‘필수’ 항목으로 분류함

| **영역** | **영역별 No** | **통제사항** |
| --- | --- | --- |
| **관리적**  **영역** | PM-001 | 개인정보보호를 위한 내부관리계획을 수립하고 있는가? |
| PM-002 | 내부관리계획서는 승인을 받아 공표하고 있는가? |
| PM-003 | 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? |
| PM-004 | 내부관리계획의 이행실태를 점검하고 있는가? |
| PM-005 | 개인정보 처리방침을 수립하여 정보주체가 확인할 수 있도록 공개하고 있는가? |
| PM-006 | 계정관리 절차를 수립하고 있는가? |
| PM-007 | 개인정보처리시스템의 패스워드 기준을 수립하고 있는가? |
| PM-008 | 중요정보에 대한 암호화 적용 기준을 수립하고 있는가? |
| PM-009 | 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? |
| PM-010 | 보조저장매체에 대한 반출입 절차를 수립하고, 이에 따라 반출입이 이루어지고 있는가? |
| PM-011 | 보조저장매체를 허가없이 사용 할 수 없도록 통제 기준을 수립하고 있는가? |
| PM-012 | 무선통제 기준과 사용 승인절차를 수립하고 있는가? |
| PM-013 | 개인정보 파기 절차 및 기준을 수립하고, 파기 후 이력 관리를 하고 있는가? |
| PM-014 | 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가?  [클라우드]  클라우드 리소스 백업 정책이 존재하는가? |
| PM-015 | 개인정보보호 자체 점검을 정기적으로 시행하고 있는가? |
| PM-016 | 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? |
| PM-017 | 개인정보보호책임자 및 담당자를 지정하고 있는가? |
| **기술적**  **영역** | PM-018 | 개인정보보호 조직 및 인력의 역할과 책임이 정의되어 있는가? |
| PM-019 | 개인정보취급자의 목록을 관리하고 있는가? |
| PM-020 | 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? |
| PM-021 | 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? |
| PM-022 | 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? |
| PM-023 | 재위탁이 다년간 계약된 경우 계약사항을 매년 검토하고 있는가? |
| PM-024 | 재수탁자의 목적 달성 후 파기, 반납에 관한 사항 및 파기확인서에 대해 확인하고 있는가? |
| PM-025 | 재수탁자 및 재수탁자의 임직원의 보안서약서를 제출하도록 관리하고 있는가? |
| PM-026 | 재수탁자의 개인정보취급자 대상에 대해 관리·감독 하고 있는가? |
| PM-027 | 개인정보는 위탁목적에 한하여 이용하고 있는가? |
| PM-028 | 수탁사가 자체적으로 고객정보 수집시 정보 수집과 관련하여 고객의 사전동의를 관계 법령에 따라 적절히 받고 있는가? |
| PM-029 | 수탁사가 타 수탁업체와 개인(신용)정보를 공유 하고 있는가?  [녹취]  수탁사가 타 수탁업체와 녹취 정보를 공유 하고 있는가? |
| PM-030 | 타 수탁업체와 정보 공유시, 정보 공유 근거가 계약서, 약정서 등에 존재하는가? |
| PT-031 | 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? |
| PT-032 | 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? |
| PT-033 | 퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가? |
| PT-034 | 개인정보취급자의 권한변경 이력을 기록하고 있는가? |
| PT-035 | 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? |
| PT-036 | 개인정보처리시스템으로 일정시간 이상 업무처리를 하지 않는 경우, 시스템 접속을 자동 차단하고 있는가? |
| PT-037 | 일정시간 이상 업무처리를 하지 않는 경우, 화면보호기 설정이 적용되어 있는가? |
| PT-038 | 개인정보처리시스템 접속 제한 설정이 적용되어 있는가? |
| PT-039 | 모바일 기기를 통해 개인정보를 처리하는 경우, 안전한 보안 조치를 적용하고 있는가? |
| PT-040 | 외부망에서 개인정보처리시스템으로의 접근을 차단하고 있는가? |
| PT-041 | 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? |
| PT-042 | 고객관리시스템 접근에 대한 사후 감사를 수행하고 있는가? |
| PT-043 | 내부에서 개인정보처리시스템 접근 시 접근통제를 적용하는가? |
| PT-044 | 보안장비를 우회한 인터넷 접속을 방지하기 위하여 무선랜을 통제하고 있는가? |
| PT-045 | 개인정보처리시스템 접속이력에 관한 정보를 기록하고 있는가? |
| PT-046 | 개인정보처리시스템의 접속기록을 일정기간 이상 보관하고 있는가? |
| PT-047 | 개인정보처리시스템의 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? |
| **물리적**  **영역** | PT-048 | 수탁사 내부에서 개인정보 송·수신 시 암호화를 적용하고 있는가? |
| PT-049 | 당사와 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? |
| PT-050 | 수탁사 내 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가?  [클라우드]  클라우드 리소스 통신 구간 내 암호화 설정이 되어 있는가? |
|  | PT-051 | 중요정보 및 인증정보 저장 시 암호화하여 저장하고 있는가? |
| PT-052 | 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? |
| PT-053 | 개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터를 사용하는가? |
| PT-054 | 업무목적이 달성된 개인정보를 즉시 파기하고 있는가?  [녹취]  보존 기한이 만료된 녹취 파일을 파기하고 있는가? |
| PT-055 | 다른 법령에 의거, 개인정보를 보관하여야 할 경우 물리적/논리적으로 분리하여 저장하고 있는가? |
| PT-056 | 개인식별번호 및 신용카드번호 등의 중요정보를 출력(화면/인쇄)하는 경우 마스킹 처리하고 있는가? |
| PT-057 | 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? |
| PT-058 | 안티바이러스 소프트웨어를 설치 및 운영하고 있는가? |
| PT-059 | 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? |
|  | PT-060 | 기본 및 사용자 공유폴더 사용을 제한하고 있는가?  [클라우드]  RDS 서브넷 그룹 내 불필요한 가용영역이 존재하지 않는가? |
|  | PT-061 | 개인정보취급자 PC에 유해소프트웨어를 설치하지 않도록 통제하고 있는가? |
|  | PT-062 | 출력 시 워터마크를 적용하고 있는가? |
|  | PT-063 | 개인정보를 처리하는 중요단말기의 인터넷 사용을 제한하고 있는가? |
|  | PT-064 | 클라우드컴퓨팅서비스를 통하여 개인정보를 처리하는 단말기의 인터넷 사용을 차단하고 있는가? |
|  | PT-065 | 개인정보취급자 PC는 최신 패치를 적용하고 있는가? |
|  | PT-066 | 개인(신용)정보가 포함된 종이인쇄물 출력시 프린터 기기 자체에 저장된 파일을 관리하고 있는가? |
|  | PP-067 | 보호구역 지정 기준 및 각 보호구역 별 보호대책을 수립하고 있는가? |
|  | PP-068 | 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? |
|  | PP-069 | 개인정보가 포함된 문서 출력 시 안전조치를 취한 후 안전한 장소에 보관하며, 중요정보를 이동하는 경우 기밀성 및 무결성을 보장하도록 통제하고 있는가? |

**[표 1] 점검 항목**

# **4. 점검 진단 기준**

## **4.1. 진단 기준**

진단 결과는 다음과 같이 네 가지의 수준으로 분류하여 평가함

| **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 |

**[표 2] 진단 기준**

## **4.2. 보안준수율 산출식**

다음과 같은 산출식을 이용하여 보안준수율을 계산함

## **4.3. 보안준수율 분류 기준**

보안준수율은 다음과 같이 다섯 가지의 수준으로 분류하여 평가함

| **수준** | **준수율(%)** | **설명** |
| --- | --- | --- |
| 우수 | 90~100 | · 지속적인 측정과 관리를 통하여 새로운 위협도 대응할 수 있는 단계로서 매우 양호한 수준 · 개인정보보호 통제가 구현되어 실행되고 있으며 매우 양호 |
| 양호 | 80~89 | · 보안위협을 측정하고 관리하며 보안대책의 계획 및 이행을 지속화 할 수 있으며, 부분적인 개선이 필요한 수준 |
| 보통 | 70~79 | · 기본적인 기준을 가지고 핵심 보안위협에 대응하고 있으며, 다양한 개선이 필요한 수준 |
| 미흡 | 50~69 | · 보안위협에 일부 대응하나 명확한 기준 없이 임의 대응하고 있어 전체적인 개선이 필요한 수준 |
| 취약 | 0~49 | · 개인정보보호 통제가 거의 이루어지지 않아 전혀 보안위협에 대응하지 않는 수준 |

**[표 3] 보안준수율 분류 기준**

# **5. 점검 대상**

* K카드사 수탁사에 대해 점검을 실시함
* 재수탁자의 경우 수탁자와 계약 시 규정한 사항에 따라 점검 여부를 결정함

| **구분** | **설명** | **비고** |
| --- | --- | --- |
| 재수탁자 | - 수탁자와 계약 시 수탁자가 재수탁자를 관리∙감독하도록 명시되어 있는 경우  - 별도의 계약 시 명시되어 있지 않은 경우 직접 점검을 실시함 | 재수탁자 |

**[표 4] 점검 제외 대상**

# **6. 점검 업체 목록**

* 점검을 실시하는 18개의 수탁사는 다음과 같으며, 각 업체의 점검일정과 점검방법을 표로 기술함
* 18개의 수탁사의 점검방법은 서면 점검을 기본으로 함
* 메가넷, 법무법인 대한, MS신용정보, 대일 전산에 대해서는 추가적으로 현장 점검을 실시함

| **번호** | **업체명** | **점검일정** | **점검방법** |
| --- | --- | --- | --- |
| 1 | **메가넷** | **2023.11.27** | **현장 점검** |
| 2 | **MS신용정보** | **2023.12.8** | **현장 점검** |
| 3 | **대일전산** | **2023.11.30** | **현장 점검** |
| 4 | **법무법인대한** | **2023.12.5** | **현장 점검** |
| 5 | **C데이타 시스템** | **2023.11.29** | **서면 점검** |
| 6 | **나우정보** | **2023.11.27** | **서면 점검** |
| 7 | **뉴테크커뮤니케이션** | **2023.12.4** | **서면 점검** |
| 8 | **동국ITX** | **2023.11.28** | **서면 점검** |
| 9 | **세종네트웍스** | **2023.11.28** | **서면 점검** |
| 10 | **제니스시스템** | **2023.12.7** | **서면 점검** |
| 11 | **향촌실업** | **2023.12.8** | **서면 점검** |
| 12 | **뉴베이스** | **2023.11.29** | **서면 점검** |
| 13 | **대한고용정보** | **2023.12.6** | **서면 점검** |
| 14 | **발보아물류** | **2023.11.30** | **서면 점검** |
| 15 | **세일즈마켓** | **2023.12.1** | **서면 점검** |
| 16 | **울트라서비스** | **2023.12.5** | **서면 점검** |
| 17 | **쿠폰마케팅** | **2023.12.1** | **서면 점검** |
| 18 | **티엠하우스** | **2023.11.30** | **서면 점검** |

**[표 5] 점검 업체 목록**

# **7. 총평**

* 본 보고서는 [수탁사 점검]에 대한 [점검결과 통계 분석] 결과를 종합하였습니다.

영역, 기반, 업무유형, 재위탁, 취급자 수, 클라우드로 기준을 잡고 [3.점검항목]에

기반하여 해당 항목의 양호, 미흡, 취약 여부를 판단 후 취약점과 보안준수율을

도출하였습니다. 18개의 수탁사 점검 결과 보안준수율 평균 68.2%로 측정되었습니다.

이에 따른 개선 방안 및 제언을 작성하여 향후 수탁사별 취약사항들에 대해 조치를

취할 수 있도록 하여 보안준수율을 향상시킬 수 있도록 하였습니다.

# **8. 점검 결과 분석**

* 수탁사의 영역별(관리, 기술, 물리) 보안준수율

관리 : 191개의 Y(양호), 125개의 P(미흡), 54개의 N(취약)으로 68.5%

기술 : 252개의 Y(양호), 58개의 P(미흡), 78개의 N(취약)으로 72.4%

물리 : 18개의 Y(양호), 10개의 P(미흡), 7개의 N(취약)으로 65.7%

* 수탁사의 기반별(서버, 문서, 단말, PC)) 보안준수율

서버 : 306개의 Y(양호), 126개의 P(미흡), 75개의 N(취약)으로 72.8%

문서 : 61개의 Y(양호), 33개의 P(미흡), 14개의 N(취약)으로 71.8%

단말 : 3개의 Y(양호), 6개의 P(미흡), 0개의 N(취약)으로 66.7%

PC : 91개의 Y(양호), 28개의 P(미흡), 50개의 N(취약)으로 62.1%

* 수탁사의 업무유형별 (콜센터, 문서, 상품판매, 유지보수, 본인인증중계, 배송) 보안준수율

콜센터 서비스 : 90개의 Y(양호), 47개의 P(미흡), 19개의 N(취약)으로 72.8%

전산시스템 운영 : 11개의 Y(양호), 9개의 P(미흡), 6개의 N(취약)으로 59.6%

채권관리 및 추심업무 : 45개의 Y(양호), 11개의 P(미흡), 5개의 N(취약)으로 82.8%

상품판매 : 77개의 Y(양호), 25개의 P(미흡), 13개의 N(취약)으로 77.8%

배송 : 68개의 Y(양호), 40개의 P(미흡), 26개의 N(취약)으로 65.7%

문서/비품 배송 및 보관 : 32개의 Y(양호), 13개의 P(미흡), 8개의 N(취약)으로 72.6%

사음품/모바일쿠폰 발송 : 59개의 Y(양호), 19개의 P(미흡), 33개의 N(취약)으로 61.7%

문서 폐기 업무 : 15개의 Y(양호), 8개의 P(미흡), 4개의 N(취약)으로 70.4%

본인인증 업무 : 31개의 Y(양호), 13개의 P(미흡), 8개의 N(취약)으로 72.1%

자문업무 : 33개의 Y(양호), 8개의 P(미흡), 17개의 N(취약)으로 63.8%

* 재위탁 有 수탁사별 분석(재위탁 관련 점검기준 항목)

메가넷 : 1개의 Y(양호), 2개의 P(미흡), 1개의 N(취약)으로 50.0%

MS신용정보 : 5개의 Y(양호), 0개의 P(미흡), 0개의 N(취약)으로 100%

뉴테크커뮤니케이션 : 3개의 Y(양호), 2개의 P(미흡), 0개의 N(취약)으로 80%

뉴베이스 : 2개의 Y(양호), 4개의 P(미흡), 0개의 N(취약)으로 66.7%

대일전산 : 1개의 Y(양호), 0개의 P(미흡), 4개의 N(취약)으로 20%

대한고용정보 : 2개의 Y(양호), 4개의 P(미흡), 0개의 N(취약)으로 66.7%

쿠폰마케팅 : 1개의 Y(양호), 0개의 P(미흡), 5개의 N(취약)으로 16.7%

티엠하우스 : 1개의 Y(양호), 0개의 P(미흡), 5개의 N(취약)으로 16.7%

* 개인정보 취급자 수별 분석

대 : 220개의 Y(양호), 87개의 P(미흡), 80개의 N(취약)으로 68.1%

중 : 151개의 Y(양호), 59개의 P(미흡), 40개의 N(취약)으로 72.2%

소 : 90개의 Y(양호), 47개의 P(미흡), 19개의 N(취약)으로 72.8%

* 클라우드 사용 수탁사 분석

메가넷 : 13개의 Y(양호), 13개의 P(미흡), 3개의 N(취약)으로 67.2%

법무법인 대한 : 22개의 Y(양호), 8개의 P(미흡), 0개의 N(취약)으로 83.9%

# **9. 개선 방안 및 제언**

## **9.1. 주요 시사점 및 개선방향**

수탁사 점검 결과 분석을 통해 각 수탁사별 주요 취약점을 도출하고 이를 개선하기 위해 시사점으로

선정 후 이에 따른 개선 방향을 제시하였습니다.

1. 사용자별 접근 권한 설정을 통한 보안 강화와 보조저장매체를 통한 유출 방지 및 통제, 이에 따른 개인정보 보호를 위한 철저한 암호화 기술 확보가 필요하며 개인정보 출력 시 유출 방지를 위한 정책이 필요합니다.

[개선방향]

개인정보보호법 개정에 따른 전반적인 내부관리계획의 현행화가 필요합니다.

1. 개인정보 처리(제3자 포함) 후 파기 절차와 이력관리가 필요하며 이후 재난 등의 피해를 대비하고 복구 절차를 수립하여 계획해두어야 합니다.

[개선방향]

개인정보 라이프 사이클을 준수하여 개인정보 처리 절차를 마련하여야 합니다.

1. 재수탁을 이용하는 수탁사의 경우 위탁사에게 계약 내용을 포함한 개인정보 처리 이력의 정기적인 보고 체계가 수립되어 있어야 하며, 주기적인 관리·감독이 필요합니다.

[개선방향]

재수탁사에 대해 위탁사 수준의 관리·감독이 필요합니다.

1. 개인정보처리시스템에 대한 보안솔루션 도입과 암호화를 통한 접근 권한 설정 등 관리 개선이 필요합니다

[개선방향]

개인정보처리시스템의 관리 체계를 보완하여 적용해야합니다.

1. 클라우드 시스템 사용 시 IAM 권한 및 태그 설정을 통한 관리가 필요하며 클라우드 리소스 로그 및 백업 정책을 설정하여 관리할 필요가 있습니다.

[개선방향]

클라우드 사용 확대에 대비하여 클라우드 시스템 이용 시 관리 절차를 수립하여 적용시킬 수 있도록 해야합니다.

## 

## **9.2. 개선과제 및 기대효과**

## 개선방향을 통해 도출한 개선과제들을 조치 기간에 따라 3개월 이내 수행 가능할 시 단기, 6개월 이내 중기, 1년 이상의 경우 장기로 분류하였습니다.

## 단기 과제 개선 시 개선 전보다 약 7.76% 의 보안 준수율의 개선이 예상되며,

## 중,장기 과제까지 개선을 이행하면 개선 전보다 약 12.58% 의 보안 준수율 개선이 예상됩니다.