,

|  |
| --- |
| **[23년도 K카드사 개인정보 수탁사 점검 프로젝트]** |
| **사업 수행계획서** |
| *Version 1.0* |

**2023. 12. 1**



**제·개정 이력**

| **버전** | **변경일** | **변경 사유** | **변경 내용** | **작성자** | **비고** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 2023-12-01 | 최초수립 | 수행계획서 서식 최초작성 | 이단비 |  |

**목차**

[**1.** **점검목적……………………………………………………………………………………………………………………………..**](about:blank) **3**

[**2.** **점검근거……………………………………………………………………………………………………………………………..**](about:blank) **3**

[**3.** **점검주기……………………………………………………………………………………………………………………………..**](about:blank) **3**

[**4.** **점검 수행인력………………………………………………………………………………………………………………………**](about:blank) **3**

[**5.** **점검기준……………………………………………………………………………………………………………………………..**](about:blank) **3**

[**6.** **점검항목……………………………………………………………………………………………………………………………..**](about:blank) **4**

[**7.** **점검대상……………………………………………………………………………………………………………………………..**](about:blank) **8**

[**8.** **점검방법……………………………………………………………………………………………………………………………..**](about:blank) **9**

[**9.** **프로젝트 수행 일정……………………………………………………………………………………………………………..**](about:blank) **10**

[**10.** **점검업체 목록…………………………………………………………………………………………………………………**](about:blank) **10**

* 1. **점검목적**
* K카드사의 개인정보 처리 업무를 수탁 받아 수행하고 있는 수탁사에 대해 법에서 요구하는 사항을 체계적∙효과적으로 관리∙감독하여 고객의 개인정보를 안전하게 보호하기 위함
  1. **점검근거**
* 개인정보보호 관련 법률 및 회사 규정에 근거하여 점검을 실시
  + 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
  + 신용정보⋅보호법 제17조(처리의 위탁)
  + 위·수탁사 개인정보보호 규정 및 ‘개인정보 보안관리 약정서’(위수탁계약)

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

* 1. **점검주기**
* 관련법률 등에 의거 점검주기는 연 1회를 기본 진행(수탁사에 조치 여부에 따라 회수 조정 가능)
  1. **점검 수행인력**

|  | **수행내용** | **수행일정** | **담당자** |
| --- | --- | --- | --- |
| 1조 | PM/ PL, 산출물 관리 | 2023-11-11 ~ 2023-12-28 | 김낙준 수석 컨설턴트 |
| 현장점검 1팀 수행원 | 2023-11-11 ~ 2023-12-28 | 정민식 책임 컨설턴트 |
| 현장점검 1팀 수행원 | 2023-11-11 ~ 2023-12-28 | 이주형 선임 컨설턴트 |
| 현장점검 1팀 수행원 | 2023-11-11 ~ 2023-12-28 | 이단비 책임 컨설턴트 |
| 현장점검 1팀 수행원 | 2023-11-11 ~ 2023-12-28 | 김서영 선임 컨설턴트 |
| 2조 | PL, 산출물 관리 | 2023-11-11 ~ 2023-12-28 | 양우성 수석 컨설턴트 |
| 현장점검 2팀 수행원 | 2023-11-11 ~ 2023-12-28 | 백지윤 책임 컨설턴트 |
| 현장점검 2팀 수행원 | 2023-11-11 ~ 2023-12-28 | 박정민 선임 컨설턴트 |
| 현장점검 2팀 수행원 | 2023-11-11 ~ 2023-12-28 | 이승준 책임 컨설턴트 |
| 현장점검 2팀 수행원 | 2023-11-11 ~ 2023-12-28 | 전지훈 선임 컨설턴트 |

* 1. **점검기준**
* 개인정보 관련 법률 및 고시와 가이드, 수탁자 계약 시 포함된 ‘개인정보 처리 위탁 보안관리 약정서’ 등의 내용을 포함하여 점검기준을 수립

| **구분** | **내용** |
| --- | --- |
| 관련 법률/고시 | * 신용정보보호법 및 신용정보업 감독규정 * 개인정보보호법 및 개인정보의 안전성 확보조치 기준(고시) |
| 관련 가이드 | * 개인정보 처리 위∙수탁 안내서(2020.12), 행정안전부 |
| 수탁자 기준 | * 개인정보보호 규정 (26조 업무위탁에 따른 개인정보의 처리 제한) * 개인정보 보안관리 약정서 (위·수탁계약) |

* 1. **점검항목**
* 수탁사 점검항목은 수탁사가 준수하여야 하는 관리적/기술적/물리적영역으로 구성되어 있음

| **NO** | **항목**  **CODE** | **유형** | **영역** | **점검항목** |
| --- | --- | --- | --- | --- |
| 1 | PM-001 | **기본** | **관리적** | 개인정보보호를 위한 내부관리계획을 수립하고 있는가? |
| 2 | PM-002 | **기본** | **관리적** | 내부관리계획서는 승인을 받아 공표하고 있는가? |
| 3 | PM-003 | **기본** | **관리적** | 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? |
| 4 | PM-004 | **기본** | **관리적** | 내부관리계획의 이행실태를 점검하고 있는가? |
| 5 | PM-005 | **기본** | **관리적** | 개인정보 처리방침을 수립하여 정보주체가 확인할 수 있도록 공개하고 있는가? |
| 6 | PM-006 | **기본** | **관리적** | 계정관리 절차를 수립하고 있는가? |
| 7 | PM-007 | **기본** | **관리적** | 개인정보처리시스템의 패스워드 기준을 수립하고 있는가? |
| 8 | PM-008 | **기본** | **관리적** | 중요정보에 대한 암호화 적용 기준을 수립하고 있는가? |
| 9 | PM-009 | **기본** | **관리적** | 암호화 키는 적절한 절차에 따라 안전하게 관리되고 있는가? |
| 10 | PM-010 | **기본** | **관리적** | 보조저장매체에 대한 반출입 절차를 수립하고, 이에 따라 반출입이 이루어지고 있는가? |
| 11 | PM-011 | **기본** | **관리적** | 보조저장매체를 허가없이 사용 할 수 없도록 통제 기준을 수립하고 있는가? |
| 12 | PM-012 | **기본** | **관리적** | 무선통제 기준과 사용 승인절차를 수립하고 있는가? |
| 13 | PM-013 | **기본** | **관리적** | 개인정보 파기 절차 및 기준을 수립하고, 파기 후 이력 관리를 하고 있는가? |
| 14 | PM-014 | **기본** | **관리적** | 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가? |
| 15 | PM-015 | **기본** | **관리적** | 개인정보보호 자체 점검을 정기적으로 시행하고 있는가? |
| 16 | PM-016 | **기본** | **관리적** | 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? |
| 17 | PM-017 | **기본** | **관리적** | 개인정보보호책임자 및 담당자를 지정하고 있는가? |
| 18 | PM-018 | **기본** | **관리적** | 개인정보보호 조직 및 인력의 역할과 책임이 정의되어 있는가? |
| 19 | PM-019 | **기본** | **관리적** | 개인정보취급자의 목록을 관리하고 있는가? |
| 20 | PM-020 | **기본** | **관리적** | 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? |
| 21 | PM-021 | **기본** | **관리적** | 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? |
| 22 | PM-022 | **기본** | **관리적** | 수탁자의 재위탁을 원칙적으로 금지하고 있으나 계약 이행을 위하여 불가피하게 재위탁을 하는 경우, 당사의 기준에 따라 재위탁하는가? |
| 23 | PM-023 | **확장** | **관리적** | 재위탁이 다년간 계약된 경우 계약사항을 매년 검토하고 있는가? |
| 24 | PM-024 | **확장** | **관리적** | 재수탁자의 목적 달성 후 파기, 반납에 관한 사항 및 파기확인서에 대해 확인하고 있는가? |
| 25 | PM-025 | **확장** | **관리적** | 재수탁자 및 재수탁자의 임직원의 보안서약서를 제출하도록 관리하고 있는가? |
| 26 | PM-026 | **확장** | **관리적** | 재수탁자의 개인정보취급자 대상에 대해 관리·감독 하고 있는가? |
| 27 | PM-027 | **기본** | **관리적** | 개인정보는 위탁목적에 한하여 이용하고 있는가?  (녹1: 수탁자의 녹취 근거가 계약서 등에 존재하는가?  녹2: 녹취 근거에 따라 수탁자가 개인정보 수집범위를 준수하고 있는가?) |
| 28 | PM-028 | **기본** | **관리적** | 수탁사가 자체적으로 고객정보 수집시 정보 수집과 관련하여 고객의 사전동의를 관계 법령에 따라 적절히 받고 있는가? |
| 29 | PM-029 | **기본** | **관리적** | 수탁사가 타 수탁업체와 개인(신용)정보를 공유 하고 있는가? |
| 30 | PM-030 | **기본** | **관리적** | 타 수탁업체와 정보 공유시, 정보 공유 근거가 계약서, 약정서 등에 존재하는가? |
| 31 | PT-031 | **기본** | **기술적** | 사용자별 계정(1인1계정)을 부여하여 관리하고 있는가? |
| 32 | PT-032 | **기본** | **기술적** | 관리자를 제외한 계정의 권한은 최소한으로 제한하여 부여하고 있는가? |
| 33 | PT-033 | **기본** | **기술적** | 퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가? |
| 34 | PT-034 | **기본** | **기술적** | 개인정보취급자의 권한변경 이력을 기록하고 있는가? |
| 35 | PT-035 | **기본** | **기술적** | 정기적으로 패스워드를 변경하고 관리하고 있는가? |
| 36 | PT-036 | **기본** | **기술적** | 개인정보처리시스템으로 일정시간 이상 업무처리를 하지 않는 경우, 시스템 접속을 자동 차단하고 있는가? |
| 37 | PT-037 | **기본** | **기술적** | 일정시간 이상 업무처리를 하지 않는 경우, 화면보호기 설정이 적용되어 있는가? |
| 38 | PT-038 | **기본** | **기술적** | 개인정보처리시스템 접속 제한 설정이 적용되어 있는가? |
| 39 | PT-039 | **기본** | **기술적** | 모바일 기기를 통해 개인정보를 처리하는 경우, 안전한 보안 조치를 적용하고 있는가? |
| 40 | PT-040 | **기본** | **기술적** | 외부망에서 개인정보처리시스템으로의 접근을 차단하고 있는가? |
| 41 | PT-041 | **기본** | **기술적** | 인터넷망(사외)에서 고객정보 관리시스템에 접속을 차단하고 있는가?(모바일접속,앱 포함) |
| 42 | PT-042 | **기본** | **기술적** | 고객관리시스템 접근에 대한 사후 감사를 수행하고 있는가? |
| 43 | PT-043 | **기본** | **기술적** | 내부에서 개인정보처리시스템 접근 시 접근통제를 적용하는가? |
| 44 | PT-044 | **기본** | **기술적** | 보안장비를 우회한 인터넷 접속을 방지하기 위하여 무선랜을 통제하고 있는가? |
| 45 | PT-045 | **기본** | **기술적** | 개인정보처리시스템 접속이력에 관한 정보를 기록하고 있는가? |
| 46 | PT-046 | **기본** | **기술적** | 개인정보처리시스템의 접속기록을 일정기간 이상 보관하고 있는가? |
| 47 | PT-047 | **기본** | **기술적** | 개인정보처리시스템의 접속기록에 대해 적정성 여부를 점검하고 있는가? |
| 48 | PT-048 | **기본** | **기술적** | 수탁사 내부에서 개인정보 송·수신 시 암호화를 적용하고 있는가? |
| 49 | PT-049 | **기본** | **기술적** | 당사와 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? |
| 50 | PT-050 | **기본** | **기술적** | 수탁사 내 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? |
| 51 | PT-051 | **기본** | **기술적** | 중요정보 및 인증정보 저장 시 암호화하여 저장하고 있는가? |
| 52 | PT-052 | **기본** | **기술적** | 개인정보를 PC에 저장하는 경우 암호화하여 저장하고 있는가? |
| 53 | PT-053 | **기본** | **기술적** | 개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터를 사용하는가? |
| 54 | PT-054 | **기본** | **기술적** | 업무목적이 달성된 개인정보를 즉시 파기하고 있는가? |
| 55 | PT-055 | **기본** | **기술적** | 다른 법령에 의거, 개인정보를 보관하여야 할 경우 물리적/논리적으로 분리하여 저장하고 있는가? |
| 56 | PT-056 | **기본** | **기술적** | 개인식별번호 및 신용카드번호 등의 중요정보를 출력(화면/인쇄)하는 경우 마스킹 처리하고 있는가? |
| 57 | PT-057 | **기본** | **기술적** | 개인정보처리시스템을 대상으로 정기적인 취약점 진단을 시행하고 있는가? |
| 58 | PT-058 | **기본** | **기술적** | 안티바이러스 소프트웨어를 설치 및 운영하고 있는가? |
| 59 | PT-059 | **기본** | **기술적** | 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? |
| 60 | PT-060 | **기본** | **기술적** | 기본 및 사용자 공유폴더 사용을 제한하고 있는가? |
| 61 | PT-061 | **기본** | **기술적** | 개인정보취급자 PC에 유해소프트웨어를 설치하지 않도록 통제하고 있는가? |
| 62 | PT-062 | **기본** | **기술적** | 출력 시 워터마크를 적용하고 있는가? |
| 63 | PT-063 | **기본** | **기술적** | 개인정보를 처리하는 중요단말기의 인터넷 사용을 제한하고 있는가? |
| 64 | PT-064 | **기본** | **기술적** | 클라우드컴퓨팅서비스를 통하여 개인정보를 처리하는 단말기의 인터넷 사용을 차단하고 있는가? |
| 65 | PT-065 | **기본** | **기술적** | 개인정보취급자 PC는 최신 패치를 적용하고 있는가? |
| 66 | PT-066 | **기본** | **기술적** | 개인(신용)정보가 포함된 종이인쇄물 출력시 프린터 기기 자체에 저장된 파일을 관리하고 있는가? |
| 67 | PP-067 | **기본** | **물리적** | 보호구역 지정 기준 및 각 보호구역 별 보호대책을 수립하고 있는가? |
| 68 | PP-068 | **기본** | **물리적** | 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? |
| 69 | PP-069 | **기본** | **물리적** | 개인정보가 포함된 문서 출력 시 안전조치를 취한 후 안전한 장소에 보관하며, 중요정보를 이동하는 경우 기밀성 및 무결성을 보장하도록 통제하고 있는가? |

* 1. **점검대상**
* 당사 수탁자 중 개인정보를 취급하는 수탁자에 대해 점검을 실시함
  + 개인정보를 취급하지 않은 수탁자는 점검대상에서 제외함
  + 재수탁자의 경우 수탁자와 계약 시 규정한 사항에 따라 수탁자가 점검하도록 규정되어 있으므로, 점검 대상에서 제외함

| **구분** | **설명** | **비고** |
| --- | --- | --- |
| 개인정보  미취급 | * 개인정보를 취급하지 않는 수탁자는 점검대상에서 제외 | * 회계법인 등 개인정보를 이용하지 않는 경우 |
| 재수탁자 | * 수탁자와 계약 시 ‘수탁자가 재 수탁자를 관리∙감독하도록 명시되어 있는 경우   - 별도의 계약 시 명시되어 있지 않은 경우 직접 점검을 실시함 | * 재수탁자 |

* 1. **점검방법**
* 당사 수탁자의 특성을 고려하여 점검방법을 구분함
  + 당사 수탁자의 점검은 현장점검을 기본적으로 함
  + 현장점검을 대체할 수 있는 충분한 사유가 있는 경우이거나, 현실적으로 현장점검이 어려운 경우 협의에 따라 서면점검으로 대체함

| **점검방법** | **상세설명** | **비고** |
| --- | --- | --- |
| 현장점검 | * 수탁사를 방문하여 점검항목을 기준으로 현장점검 실시 | * 체크리스트, 실사 |
| 서면점검 | * 수탁사의 상급기관에게 ‘개인정보 실태점검’등을 받는 경우   - CD/VAN 대상 금융보안원 합동점검 등  - 통신사 대상 방송통신위원회 실태점검 등  - 공공기관 대상 개인정보 실태점검 등  - 금융감독원 등 정부기관 점검 등 | * 점검결과보고서 대체 |
| * 주기적인 점검이 수행되는 정부부처, 공공기관 혹은 상급기관이거나, ISMS-P 인증을 유지, 국가 주요정보통신기반시설 등으로 지정되어 방문이 불가능한 경우 | * 수탁사 내부점검 결과보고서 |
| * 계약 체결 시 구체적으로 협의된 경우 | * 수탁사 내부점검 결과보고서 |

* 1. **프로젝트 수행 일정**

| **번호** | **설명** | **내용** | **일시** |
| --- | --- | --- | --- |
| 1 | 환경 및 현황분석 | - 사업구조 분석. 개인정보 수탁사 현황 및 수탁사 점검 요구사항 파악 | * 2023-11-13 |
| 2 | 수행계획서 수립 | - 전체일정 수립. 전체 진단/평가/대책 구현 및 이행 일정 | * 2023-11-14 |
| 3 | 점검항목 현행화 및 Cloud 시스템 점검항목 도출 | - 자사 점검 체크리스트 기준으로 최신 법률 및 타사 Best Practice Case 반영 후 고객사 전달  - 기존 관리/기술/물리/녹취 영역 병합 검토  - 수탁사 개인정보처리시스템에 Cloud 이동 및 개인정보처리에 따른 점검방안 도출 | * 2023-11-16 |
| 4 | 사전 환경질의서 작성 | - 수탁사 별 사전 환경질의서 작성으로 현황 파악 | * 2023-11-22 |
| 5 | 수탁사 개인정보 처리 흐름도 수립 | - 수탁사 별 개인정보 처리 흐름도 상세 작성 후 점검 포인트 도출 | * 2023-11-24 |
| 6 | 체크리스트 배포 | - 점검 일정 및 체크리스트를 개인정보 수탁사에 배포 | * 2023-11-29 |
| 7 | 서면 점검 | - 점검 체크리스트 기반 서면 점검 수행 | * 2023-12-04 |
| 8 | 현장 점검 | - 개인정보처리방침 등 내규 점검  - 담당자 인터뷰  - 증적 확인 | * 2023-12-09 |
| 9 | 서면 및 현장 점검 결과 보고서 | - 서면 및 현장 점검 결과 보고서를 토대로 위탁사/수탁사 결과 확인 | * 2023-12-16 |
| 10 | 수탁사 점검에 따른 보안 수준 향상방안 도출 | - 위·수탁사 관리·감독 개선보고서를 통해 점검에 따른 보안수준 향상을 위한 개선조치 방안 도출 | * 2023-12-21 |
| 11 | 수탁사 교육 진행 | - 도출된 개선방안으로 수탁사 교육 진행 | * 2023-12-23 |
| 12 | 현업담당자 공유 | - 점검 최종 결과 및 개선사항 공유 | * 2023-12-28 |

* 1. **점검업체 목록**

| **번호** | **업체명** | **일정** | **점검방법** | **비고** |
| --- | --- | --- | --- | --- |
| 1 | 메가넷 | 2023-11-27 (월) | **현장점검** |  |
| 2 | 대일전산 | 2023-11-30 (목) | **현장점검** |  |
| 3 | 법무법인 대한 | 2023-12-05 (화) | **현장점검** |  |
| 4 | MS 신용정보 | 2023-12-08 (금) | **현장점검** |  |
| 5 | 나우정보 | 2023-11-27 (월) | 서면점검 |  |
| 6 | 동국 ITX | 2023-11-28 (화) | 서면점검 |  |
| 7 | 세종네트웍스 | 2023-11-28 (화) | 서면점검 |  |
| 8 | 뉴베이스 | 2023-11-29 (수) | 서면점검 |  |
| 9 | C 데이터시스템 | 2023-11-29 (수) | 서면점검 |  |
| 10 | 발모아 | 2023-11-30 (목) | 서면점검 |  |
| 11 | 티엠하우스 | 2023-11-30 (목) | 서면점검 |  |
| 12 | 쿠폰마케팅 | 2023-12-01 (금) | 서면점검 |  |
| 13 | 세일즈 마켓 | 2023-12-01 (금) | 서면점검 |  |
| 14 | 뉴테크커뮤니케이션 | 2023-12-04 (월) | 서면점검 |  |
| 15 | 울트라서비스 | 2023-12-05 (화) | 서면점검 |  |
| 16 | 대한고용정보 | 2023-12-06 (수) | 서면점검 |  |
| 17 | 제니스시스템 | 2023-12-07 (목) | 서면점검 |  |
| 18 | 향촌실업 | 2023-12-08 (금) | 서면점검 |  |