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

**2023. 12. 13**



**제·개정 이력**

| **버전** | **변경일** | **변경 사유** | **변경 내용** | **작성자** | **비고** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 2023-12-13 | 최초작성 | 수탁사 점검 보고서 서식 수립 | 김서영 |  |

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** |
| 8 | 제니스시스템 | 문서 | 카드인편배송 |

* 1. **점검 방식 및 일정**

|  |  |  |
| --- | --- | --- |
| **점검 방식** | **점검 일시** | **수탁사 사업장 주소** |
| 서면 점검 | 2023년 12월 07일  / 09:00 ~ 16:00 | 경기도 성남시 중원구 둔촌대로 |

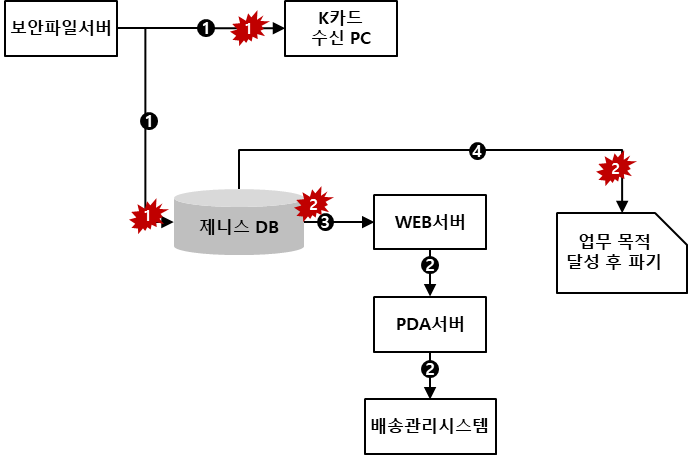
* 1. **담당자 정보**

|  |  |  |
| --- | --- | --- |
| **K카드사 계약 부서 / 담당자** | **수탁사 담당자 성명** | **수탁사 담당자 전화번호 / 이메일 주소** |
| 지원사업본부 / 카드사업본부 | 박춘홍 대표이사 | - |
| 배정호 팀장 | 031-777-xxxx |

* 1. **점검인력 정보**

|  |  |  |  |
| --- | --- | --- | --- |
| **소속** | **성명** | **직책** | **이메일 주소** |
| 컨설팅커벨 | 이단비 | 책임 컨설턴트 | dandan00boan@gmail.com |
| 컨설팅커벨 | 김서영 | 선임 컨설턴트 | s0yeonghh@gmail.com |
| 컨설팅커벨 | 이승준 | 책임 컨설턴트 | 이승준@gmail.com |

|  |  |  |
| --- | --- | --- |
| **수탁사**  **개인정보취급자 수** | **개인정보 처리 수량**  **(K카드사 개인정보 限)** | **정보보호 솔루션 및 보호조치** |
| 3명 | 200,000 건 | DRM솔루션, DB 데이터 암호화, V3 백신, 카스퍼스키 백신, 서버접근제어 솔루션(NAC), 보안USB, 포트락 |
| **자체 개인정보**  **처리시스템 운용 여부** | **개인정보 저장 유형** |
| 배송관리시스템, WEB서버, DB서버, PDA서버, K카드 수신PC | 자체DB, K카드수신전용PC |
| **처리 개인정보 종류** | **파기확인서 제출** |
| 이름, 연락처(가상번호), 주소, 생년월일, 성별 | 월 1회 |

* 1. **수탁사 개요**
  2. **개인정보 처리현황**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **구분** | **개인정보 처리 흐름** | | | | **처리개인정보** |
| 수집 | 저장 | 이용 | 파기 |
| [정보주체]  고객/임직원 |  |  |  |  |  |
| [위탁사]  K카드사 |  |  |  |  |
| [수탁사]  제니스  시스템 |  |  |  |  |
| 주요업무  흐름설명 | • K카드사 보안파일서버로부터 FTP 파일을 제공받음 | • 제니스시스템 DB, K카드수신전용PC에 개인정보 데이터 암호화 저장 | • ID/PW  (공통계정+개별계정)+보안코드를 통한 계정 로그인 후 접속  • WEB서버는 개인정보를 받아옴  • 카드인편배송 시 PDA서버를 통해 배송 정보 확인  • 배송관리  시스템에서 배송정보를 통해 배송 관리 | • 일배치를 통해 자동삭제  • 60일 보관 후 파기  • 월1회 파기확인서를 통해 결과 보고 |
| Weak Point |  | • 개인정보 분리보관이 해당 없는게 맞는지 확인 필요  • 개인정보가 5만명 이상인지 이하인지 파악 후 보관기간 확인 필요 |  | • 파기 기준, 절차 정의되어있지 않음 |  |

1. **점검 결과**
   1. **총평**

제니스시스템은 문서기반 유형의 수탁사로서, 최초 69개 점검기준으로 점검을 수행함.

제니스시스템은 중요정보에 대한 암호화 적용 기준 수립, 개인정보처리시스템의 패스워드 기준 수립와 같은 양호한 보안수준을 유지하고 있으나, 개인정보처리시스템 접속 제한 설정, 모바일 기기를 통한 개인정보 처리하는 경우, 안전한 보안 조치 적용와 같은 미흡사항이 식별되어 접속 제한 설정 적용, 모바일 기기 접근 통제, 분실/도난을 대비한 비밀번호 설정 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 제니스시스템은 보안준수율이 72.64%로 보통수준이며, 32개의 양호(Y), 13개의 미흡(P), 8개의 취약(N)으로 식별되었습니다.

| **No.** | **영역** | **분류 기준** | **점검항목** | **진단 결과** |
| --- | --- | --- | --- | --- |
| 1 | **관리적 영역** | **개인정보보호 관리체계** | 개인정보보호를 위한 내부관리계획을 수립하고 있는가? | P |
| 2 | **관리적 영역** | **개인정보보호 관리체계** | 내부관리계획서는 승인을 받아 공표하고 있는가? | Y |
| 3 | **관리적 영역** | **개인정보보호 관리체계** | 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? | P |
| 4 | **관리적 영역** | **개인정보보호 관리체계** | 내부관리계획의 이행실태를 점검하고 있는가? | P |
| 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? | Y |
| 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? | N |
| 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? | N |
| 14 | **관리적 영역** | **개인정보보호 관리체계** | 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가? | P |
| 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? | P |
| 19 | **관리적 영역** | **개인정보취급자 관리** | 개인정보취급자의 목록을 관리하고 있는가? | P |
| 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? | P |
| 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? | N/A |
| 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? | N/A |
| 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? | Y |
| 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? | Y |
| 33 | **기술적 영역** | **접근제어** | 퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가? | Y |
| 34 | **기술적 영역** | **접근제어** | 개인정보취급자의 권한변경 이력을 기록하고 있는가? | P |
| 35 | **기술적 영역** | **접근제어** | 정기적으로 패스워드를 변경하고 관리하고 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? | N |
| 39 | **기술적 영역** | **접근통제** | 모바일 기기를 통해 개인정보를 처리하는 경우, 안전한 보안 조치를 적용하고 있는가? | P |
| 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) | N/A |
| 42 | **기술적 영역** | **접근통제** | 고객관리시스템 접근에 대한 사후 감사를 수행하고 있는가? | Y |
| 43 | **기술적 영역** | **접근통제** | 내부에서 개인정보처리시스템 접근 시 접근통제를 적용하는가? | Y |
| 44 | **기술적 영역** | **접근통제** | 보안장비를 우회한 인터넷 접속을 방지하기 위하여 무선랜을 통제하고 있는가? | Y |
| 45 | **기술적 영역** | **접속기록** | 개인정보처리시스템 접속이력에 관한 정보를 기록하고 있는가?  [녹취]  녹취시스템 접속이력에 관한 정보를 기록하고 있는가? | Y |
| 46 | **기술적 영역** | **접속기록** | 개인정보처리시스템의 접속기록을 일정기간 이상 보관하고 있는가?  [녹취]  녹취시스템의 접속기록을 일정기간 이상 보관하고 있는가? | N |
| 47 | **기술적 영역** | **접속기록** | 개인정보처리시스템의 접속기록에 대해 적정성 여부를 점검하고 있는가?  [녹취]  녹취시스템의 접속기록에 대해 적정성 여부를 점검하고 있는가? | Y |
| 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? | Y |
| 50 | **기술적 영역** | **안전한 송∙수신** | 수탁사 내 네트워크 연결 시 안전한 방법을 사용하여 연결하고 있는가? | Y |
| 51 | **기술적 영역** | **데이터 암호화** | 중요정보 및 인증정보 저장 시 암호화하여 저장하고 있는가? | N/A |
| 52 | **기술적 영역** | **데이터 암호화** | 개인정보를 PC에 저장하는 경우 암호화하여 저장하고 있는가?  [녹취]  녹취 파일을 저장하는 경우 암호화하여 저장하고 있는가? | Y |
| 53 | **기술적 영역** | **개발 및 테스트** | 개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터를 사용하는가? | Y |
| 54 | **기술적 영역** | **개인정보 관리 및 파기** | 업무목적이 달성된 개인정보를 즉시 파기하고 있는가?  [녹취]  보존 기한이 만료된 녹취 파일을 파기하고 있는가? | P |
| 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/A |
| 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? | N |
| 60 | **기술적 영역** | **매체제어** | 기본 및 사용자 공유폴더 사용을 제한하고 있는가? | Y |
| 61 | **기술적 영역** | **매체제어** | 개인정보취급자 PC에 유해소프트웨어를 설치하지 않도록 통제하고 있는가? | Y |
| 62 | **기술적 영역** | **매체제어** | 출력 시 워터마크를 적용하고 있는가? | N |
| 63 | **기술적 영역** | **단말기관리** | 개인정보를 처리하는 중요단말기의 인터넷 사용을 제한하고 있는가? | Y |
| 64 | **기술적 영역** | **단말기 관리** | 클라우드컴퓨팅서비스를 통하여 개인정보를 처리하는 단말기의 인터넷 사용을 차단하고 있는가? | N/A |
| 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/A |
| 67 | **물리적 영역** | **보호구역 관리** | 보호구역 지정 기준 및 각 보호구역 별 보호대책을 수립하고 있는가? | P |
| 68 | **물리적 영역** | **보호구역 관리** | 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? | P |
| 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/A |
| **보안준수율** | | | | **72.64%** |

* 1. **주요 미흡사항 및 보호대책 수립 현황**

| **점검 항목** | **개선방안** |
| --- | --- |
| 개인정보보호를 위한 내부관리계획을 수립하고 있는가? | 내부관리계획 개정 (16가지 필수 사항 모두 포함) |
| 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? | 개인정보보호법이 2023. 9. 15 개정됨에 따라 내부관리계획 개정 |
| 내부관리계획의 이행실태를 점검하고 있는가? | 개인정보보호법이 2023. 9. 15 개정됨에 따라 내부관리계획 개정 |
| 보조저장매체를 허가없이 사용 할 수 없도록 통제 기준을 수립하고 있는가? | 통제 기준 수립, 사용 이력 관리 필요 |
| 개인정보 파기 절차 및 기준을 수립하고, 파기 후 이력 관리를 하고 있는가? | 파기 기준, 절차 정의 해야함 |
| 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가? | 백업 및 복구 계획 수립 |
| 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? | 내부 정책을 통한 마스킹 기준 수립 필요 |
| 개인정보보호 조직 및 인력의 역할과 책임이 정의되어 있는가? | 실제 역할 별 업무수행 이루어지는지 확인 |
| 개인정보취급자의 목록을 관리하고 있는가? | 개인정보취급자 최소한으로 지정 및 목록의 최신성 유지 |
| 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | 누락 인원 여부 확인 |
| 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? | 교육 미이수자에 대한 관리감독 수행 |
| 개인정보취급자의 권한변경 이력을 기록하고 있는가? | 회수 이력 관리 |
| 개인정보처리시스템 접속 제한 설정이 적용되어 있는가? | 접속 제한 설정 적용해야함 |
| 모바일 기기를 통해 개인정보를 처리하는 경우, 안전한 보안 조치를 적용하고 있는가? | -모바일 기기 접근 통제  -모바일 기기 분실/도난 등을 대비한 비밀번호 설정, 자동 잠금 설정  -책임자의 승인 득하여야함 |
| 개인정보처리시스템의 접속기록을 일정기간 이상 보관하고 있는가?  --------------------------------  [녹취]  녹취시스템의 접속기록을 일정기간 이상 보관하고 있는가? | 개인정보가 5만명 이상인지 이하인지 파악후 보관기간 확인 필요 |
| 업무목적이 달성된 개인정보를 즉시 파기하고 있는가?  --------------------------------  [녹취]  보존 기한이 만료된 녹취 파일을 파기하고 있는가? | 파기관리대장 작성 |
| 다른 법령에 의거, 개인정보를 보관하여야 할 경우 물리적/논리적으로 분리하여 저장하고 있는가? | 해당없음이 맞는지 확인 필요 |
| 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? | 보조저장매체 사용통제 필요 |
| 출력 시 워터마크를 적용하고 있는가? | 워터마크 적용 필요 |
| 보호구역 지정 기준 및 각 보호구역 별 보호대책을 수립하고 있는가? | 보호구역 지정 기준 명시 필요  보호구역별 보호대책 수립 필요 |
| 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? | 접근 이력 점검 필요 |