|  |
| --- |
|  |
| **[23년도 k카드사 개인정보 수탁사 점검 프로젝트]** |
| **나우정보**  **수탁사 점검 결과보고서** |
| *Version 1.0* |

**2023. 12. 12**



**제·개정 이력**

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

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** |
| 01 | 나우정보 | 서버기반 | 앱안심인증  본인인증 중계 |

* 1. **점검 방식 및 일정**

|  |  |  |
| --- | --- | --- |
| **점검 방식** | **점검 일시** | **수탁사 사업장 주소** |
| 서면 점검 | 2020년 11월 27일  / 13:00 ~ 15:00 | 서울시 마포구 마포대로 |

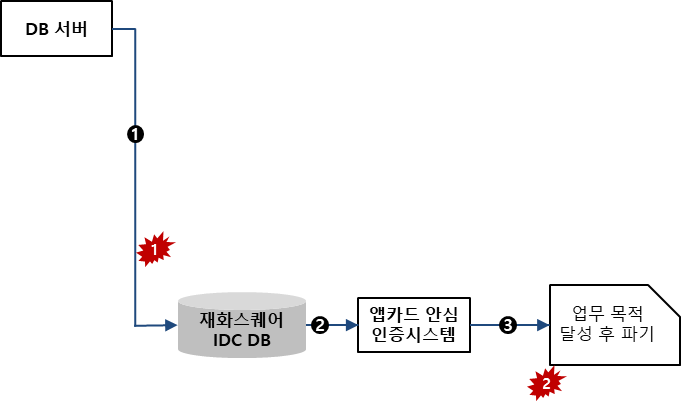
* 1. **담당자 정보**

|  |  |  |
| --- | --- | --- |
| **ㅇㅇㅇ 계약 부서 / 담당자** | **수탁사 담당자 성명** | **수탁사 담당자 전화번호 / 이메일 주소** |
| 마케팅기획파트 / 김국민 | 문용석 | 휴대폰-0000-0000 / sutak@sutaksa.com |
| 정길상 | 인터넷-0000-0000 / witak@witaksa.com |

* 1. **점검인력 정보**

|  |  |  |  |
| --- | --- | --- | --- |
| **소속** | **성명** | **직책** | **이메일 주소** |
| 컨설팅커벨 | 백지윤 | 책임 컨설턴트 | 이메일 주소 |
| 컨설팅커벨 | 박정민 | 선임 컨설턴트 | 이메일 주소 |

| **수탁사**  **개인정보취급자 수** | **개인정보 처리 수량**  **(ㅇㅇㅇ 개인정보 限)** | **정보보호 솔루션 및 보호조치** |
| --- | --- | --- |
| 2명 | 일 20,000건 | 내부관리계획최신화, 파기확인서 작성, 백업계획수립, 마스킹기준 수립, 업무권한최소 지정, 권한변경이력 3년이상 보관, 패스워드설정 의무화, 안티바이러스 소프트웨어 최신화, 워터마크 적용, |
| **자체 개인정보**  **처리시스템 운용 여부** | **개인정보 저장 유형** |
| 재화스퀘어 IDC내 DB서버 이용 | 재화스퀘어DB |
| **처리 개인정보 종류** | **파기확인서 제출** |
| 이름, 휴대폰번호, 생년월일 | 파기확인서 미작성 |

* 1. **수탁사 개요**
  2. **개인정보 처리현황**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **구분** | **개인정보 처리 흐름** | | | | **처리개인정보** |
| 수집 | 저장 | 이용 | 파기 |
| [정보주체]  고객/임직원 |  |  |  |  | 1. **개인정보제공**   : 이름, 휴대폰번호, 생년월일   1. **개인정보저장**   :이름, 휴대폰번호, 생년월일   1. **녹취정보**   **:**이름, 휴대폰번호, 생년월일 |
| [위탁사]  K카드 |  |  |  |  |
| [수탁사]  나우정보 |  |  |  |  |
| [재수탁자]  -해당없음- |  |  |  |  |
| 주요업무  흐름설명 | •K카드로 부터 DB서버로 전송 | •재화스퀘어 IDC 내 DB서버에 저장 |  | 자동 DB 프로세저 일 1회 구동으로 파기  보관 기간이 지난 개인정보에 대하여 매일 자동 삭제함 |
| Weak Point |  | * 패스워드 기준 미비 * 기본 및 사용자 공유폴더 사용이 제한됨 | * 개인정보의 출력에대한 규정 미비 * 개인정보처리시스템 접속 제한 설정 미비 * 개인정보처리시스템 접속기록 보관 미비 |  |  |

1. **점검 결과**
   1. **총평**

나우정보는 서버기반 유형의 수탁사로서, 최초 69개 점검기준으로 점검을 수행함.

나우정보는 [보조저장매체에 대한 사용절차 정의], [외부망에서 개인정보처리시스템으로의 접근 차단]와 같은 양호한 보안수준을 유지하고 있으나, [개인정보보호교육 정기적 시행], [개인정보처리시스템 접속 제한 설정]와 같은 미흡사항이 식별되어 [교육을 연 1회 이상으로 정례화], [패스워드 입력 실패시의 설정기준 요구] 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 나우정보는 보안준수율이 75%로 보통수준이며, 31개의 양호(Y), 13개의 미흡(P), 8개의 취약(N)으로 식별되었습니다.

| **No.** | **영역** | **분류 기준** | **점검항목** | **진단 결과** |
| --- | --- | --- | --- | --- |
| 1 | **관리적 영역** | **내부관리계획 수립 및 관리** | 개인정보보호를 위한 내부관리계획을 수립하고 있는가? | P |
| 2 | **관리적 영역** | **내부관리계획 수립 및 관리** | 내부관리계획서는 승인을 받아 공표하고 있는가? | N |
| 3 | **관리적 영역** | **내부관리계획 검토** | 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? | P |
| 4 | **관리적 영역** | **내부관리계획 실태점검** | 내부관리계획의 이행실태를 점검하고 있는가? | P |
| 5 | **관리적 영역** | **개인정보 처리방침 수립** | 개인정보 처리방침을 수립하여 정보주체가 확인할 수 있도록 공개하고 있는가? | Y |
| 6 | **관리적 영역** | **계정관리 절차 수립** | 계정관리 절차를 수립하고 있는가? | Y |
| 7 | **관리적 영역** | **패스워드 생성 기준 수립** | 개인정보처리시스템의 패스워드 기준을 수립하고 있는가? | Y |
| 8 | **관리적 영역** | **암호화 정책 기준 수립** | 중요정보에 대한 암호화 적용 기준을 수립하고 있는가? | Y |
| 9 | **관리적 영역** | **암호화 키 관리절차 수립** | 암호화 키는 적절한 절차에 따라 안전하게 관리되고 있는가? | Y |
| 10 | **관리적 영역** | **보조저장매체 통제 절차 수립** | 보조저장매체에 대한 반출입 절차를 수립하고, 이에 따라 반출입이 이루어지고 있는가? | Y |
| 11 | **관리적 영역** | **보조저장매체 통제 절차 수립** | 보조저장매체를 허가없이 사용 할 수 없도록 통제 기준을 수립하고 있는가? | Y |
| 12 | **관리적 영역** | **무선네트워크 통제 절차 수립** | 무선통제 기준과 사용 승인절차를 수립하고 있는가? | N/A |
| 13 | **관리적 영역** | **개인정보 파기 기준 수립** | 개인정보 파기 절차 및 기준을 수립하고, 파기 후 이력 관리를 하고 있는가? | P |
| 14 | **관리적 영역** | **백업 및 복구관리** | 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가? | P |
| 15 | **관리적 영역** | **개인정보 점검 및 조치** | 개인정보보호 자체 점검을 정기적으로 시행하고 있는가? | P |
| 16 | **관리적 영역** | **개인정보 표시 및 출력 관리정책 수립** | 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? | N |
| 17 | **관리적 영역** | **개인정보 보호 책임자 지정 및 업무** | 개인정보보호책임자 및 담당자를 지정하고 있는가? | Y |
| 18 | **관리적 영역** | **개인정보 보호 책임자 지정 및 업무** | 개인정보보호 조직 및 인력의 역할과 책임이 정의되어 있는가? | P |
| 19 | **관리적 영역** | **개인정보취급자 목록 관리** | 개인정보취급자의 목록을 관리하고 있는가? | P |
| 20 | **관리적 영역** | **보안 서약** | 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | P |
| 21 | **관리적 영역** | **개인정보보호 교육** | 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? | N |
| 22 | **관리적 영역** | **개인정보 처리 재위탁 계약** | 수탁자의 재위탁을 원칙적으로 금지하고 있으나 계약 이행을 위하여 불가피하게 재위탁을 하는 경우, 당사의 기준에 따라 재위탁하는가? | N/A |
| 23 | **관리적 영역** | **개인정보 재위탁 보호조치** | 재위탁이 다년간 계약된 경우 계약사항을 매년 검토하고 있는가? | N/A |
| 24 | **관리적 영역** | **개인정보 재위탁 보호조치** | 재수탁자의 목적 달성 후 파기, 반납에 관한 사항 및 파기확인서에 대해 확인하고 있는가? | N/A |
| 25 | **관리적 영역** | **보안 서약** | 재수탁자 및 재수탁자의 임직원의 보안서약서를 제출하도록 관리하고 있는가? | N/A |
| 26 | **관리적 영역** | **재수탁자에 대한 관리감독** | 재수탁자의 개인정보취급자 대상에 대해 관리·감독 하고 있는가? | N/A |
| 27 | **관리적 영역** | **개인정보 목적 외 이용 및 제공** | 개인정보는 위탁목적에 한하여 이용하고 있는가? | 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? | 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? | N |
| 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? | P |
| 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? | 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) | 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? | N/A |
| 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/A |
| 56 | **기술적 영역** | **개인정보처리시스템** | 개인식별번호 및 신용카드번호 등의 중요정보를 출력(화면/인쇄)하는 경우 마스킹 처리하고 있는가? | Y |
| 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? | P |
| 59 | **기술적 영역** | **매체제어** | 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? | Y |
| 60 | **기술적 영역** | **매체제어** | 기본 및 사용자 공유폴더 사용을 제한하고 있는가? | N |
| 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? | Y |
| 68 | **물리적 영역** | **보호구역 관리** | 보호구역을 구분하고, 보호구역별 접근통제를 적용하고 있는가? | Y |
| 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** | | | | **75%** |

* 1. **주요 미흡사항 및 보호대책 수립 현황**

| **점검 항목** | **개선방안** |
| --- | --- |
| 001. 개인정보보호를 위한 내부관리계획을 수립하고 있는가? | 내부관리계획내 최신화 사항 반영 |
| 002. 내부관리계획서는 승인을 받아 공표하고 있는가? | 제정된 내부계획세에 대하여 승인 작업 실시 |
| 003. 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? | 23년9월 개인정보보호법 개정안 내용 내부관리계획에 포함 필요 |
| 004.  내부관리계획의 이행실태를 점검하고 있는가? | 9월 개정이후 필수 점검 항목중 취신화 필요 |
| 013. 개인정보 파기 절차 및 기준을 수립하고, 파기 후 이력 관리를 하고 있는가? | 파기 후 파기관리대장을 기록하고 파기확인서를 작성한다.  개인정보 파기 확인서를 제출한다. |
| 014. 재해 및 재난 발생 시 백업 및 복구 계획 등이 포함 된 위기대응 매뉴얼을 수립하고 있는가? | 위기대응 절차는 수립되어 있으나 백업 및 복구계획을 작성해야함  백업 및 복구대상, 주기, 방법 및 절차 등을 포함한다. |
| 015. 개인정보보호 자체 점검을 정기적으로 시행하고 있는가? | 점검을 진행한 결과보고서 증 점검이력을 기록한다. |
| 016. 개인(신용)정보의 출력(인쇄, 화면표시, 파일생성)에 대한 정책 및 규정이 수립되어 있는가? | 마스킹 기준을 수립해야됨 |
| 018. 개인정보보호 조직 및 인력의 역할과 책임이 정의되어 있는가? | 개인정보보호담당자 역할과 업무수행에대하여 명시해야함 |
| 019. 개인정보취급자의 목록을 관리하고 있는가? | 각 개인정보 취급자의 업무 범위 내에서만 취급하도록 조치(최소지정필요) |
| 020. 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | 누락인원에 대한 정보 추가 |
| 021. 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? | 개인정보보호 교육을 연 1회 이상으로 정례화시킴 |
| 034. 개인정보취급자의 권한변경 이력을 기록하고 있는가? | 권한변경 이력을 3년이상 안전하게 보관요구 |
| 035. 정기적으로 패스워드를 변경하고 관리하고 있는가? | 개인정보 취급자 PC에 패스워드 설정 의무화 |
| 036. 일정시간 이상 업무처리를 하지 않는 경우, 화면보호기 설정이 적용되어 있는가? | 다시시작하는경우 pc 화면보호기가 실행되도록 설정 |
| 038. 개인정보처리시스템 접속 제한 설정이 적용되어 있는가? | 패스워드설정 기준만 성립되어있음  패스워드 입력 실패시의 설정 기준이 요구됨 |
| 046. 개인정보처리시스템의 접속기록을 일정기간 이상 보관하고 있는가?  [녹취]  녹취시스템의 접속기록을 일정기간 이상 보관하고 있는가? | 개인정보처리시스템의 접속기록을 최소 1년이상 보관해야함 |
| 054. 업무목적이 달성된 개인정보를 즉시 파기하고 있는가?  [녹취]  보존 기한이 만료된 녹취 파일을 파기하고 있는가? | 파기이력에 대해서 기록함 |
| 058. 안티바이러스 소프트웨어를 설치 및 운영하고 있는가? | 자동 업데이트 필요 |
| 060. 기본 및 사용자 공유폴더 사용을 제한하고 있는가? | 공유폴더에 제거를 목표로하나, 불가피할경우 권한관리 필요 |
| 062. 출력 시 워터마크를 적용하고 있는가? | 출력시 워터마크를 적용하고, 출력 로그 기록해야함 |