|  |
| --- |
|  |
| **[23년도 K카드사 개인정보 수탁사 점검 프로젝트]** |
| **세종네트웍스**  **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 | 김낙준 |  |

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** |
| 07 | 세종 네트웍스 | 서버 기반 | 콜센터 운영 |

* 1. **점검 방식 및 일정**

|  |  |  |
| --- | --- | --- |
| **점검 방식** | **점검 일시** | **수탁사 사업장 주소** |
| 서면 점검 | 2023년 11월 28일  / 14:00 ~ 17:00 | 서울시 중구 중림동 |

* 1. **담당자 정보**

|  |  |  |
| --- | --- | --- |
| **K 카드사 계약 부서 / 담당자** | **수탁사 담당자 성명** | **수탁사 담당자 전화번호 / 이메일 주소** |
|  |  |  |
|  |  |

* 1. **점검인력 정보**

|  |  |  |  |
| --- | --- | --- | --- |
| **소속** | **성명** | **직책** | **이메일 주소** |
| 컨설팅커벨 | 김낙준 | 수석 컨설턴트 | 김낙준@gmail.com |
| 컨설팅커벨 | 김서영 | 선임 컨설턴트 | 김서영@gmail.com |

| **수탁사**  **개인정보취급자 수** | **개인정보 처리 수량**  **(K카드 개인정보 限)** | **정보보호 솔루션 및 보호조치** |
| --- | --- | --- |
| 3명 | 300,000 건 | 매체제어, 문서보안, 웹방화벽, 보안USB |
| **자체 개인정보**  **처리시스템 운용 여부** | **개인정보 저장 유형** |
| 자체구축 | 녹취서버 |
| **처리 개인정보 종류** | **파기확인서 제출** |
| ID/PW | 월 1회 |

* 1. **수탁사 개요**
  2. **개인정보 처리현황**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **구분** | **개인정보 처리 흐름** | | | | **처리개인정보** |
| 수집 | 저장 | 이용 | 파기 |
| [정보주체]  고객/임직원 |  |  |  |  |  |
| [위탁사]  ㅇㅇㅇ |  |  |  |  |
| [수탁사]  ㅁㅁㅁ |  |  |  |  |
| 주요업무  흐름설명 |  |  |  |  |
| Weak Point |  |  |  |  |  |

1. **점검 결과**
   1. **총평**

세종네트웍스는 서버 기반 유형의 수탁사로서, 최초 69개 점검기준으로 점검을 수행함.

세종네트웍스는 관리자를 제외한 계정의 권한은 최소한으로 제한하여 부여, 화면보호기 설정와 같은 양호한 보안수준을 유지하고 있으나, 1인 1계정을 부여하여 관리, 보조저장매체 사용 통제와 같은 미흡사항이 식별되어 녹취서버 유지보수를 위한 OS 접근 시 관리자 계정을 공용으로 사용하지 않도록 책임자의 선별을 통해 권한 최소화, 개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터 사용 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 동국ITX은 보안준수율이 62.5%로 미흡수준이며, 5개의 양호(Y), 2개의 미흡(P), 1개의 취약(N)으로 식별되었습니다.

| **No.** | **영역** | **분류 기준** | **점검항목** | **진단 결과** |
| --- | --- | --- | --- | --- |
| 1 | **관리적 영역** | **개인정보취급자 관리** | 개인정보취급자의 목록을 관리하고 있는가? | N |
| 2 | **관리적 영역** | **개인정보취급자 관리** | 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | N |
| 3 | **기술적 영역** | **개인정보취급자 관리** | 내부관리계획서는 정기적으로 적정성 여부를 검토하여 갱신하고 있는가? | N |
| 4 | **기술적 영역** | **접근제어** | 사용자별 계정(1인1계정)을 부여하여 관리하고 있는가? | N |
| 5 | **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?"  퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가?  일정시간 이상 업무처리를 하지 않는 경우, 화면보호기 설정이 적용되어 있는가?  개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터를 사용하는가?  안티바이러스 소프트웨어를 설치 및 운영하고 있는가?  보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? | Y |
| 6 | **기술적 영역** | **접근제어** | 퇴직 및 전배 시 부여 권한을 즉시 회수하고 있는가? | N/A |
| 7 | **기술적 영역** | **접근제어** | 일정시간 이상 업무처리를 하지 않는 경우, 화면보호기 설정이 적용되어 있는가? | Y |
| 8 | **기술적 영역** | **개발 및 테스트** | 개발 및 테스트 시 실데이터가 아닌 별도의 테스트 데이터를 사용하는가? | N/A |
| 9 | **기술적 영역** | **악성프로그램 관리** | 안티바이러스 소프트웨어를 설치 및 운영하고 있는가? | P |
| 10 | **기술적 영역** | **매체제어** | 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? | N |
| **보안준수율** | | | | **43.75%** |

* 1. **주요 미흡사항 및 보호대책 수립 현황**

| **점검 항목** | **개선방안** |
| --- | --- |
| 개인정보취급자의 목록을 관리하고 있는가? | 전산 유지보수 담당자의 취급자 리스트를 만들어 개인정보취급자의 목록화가 필요함. |
| 개인정보취급자를 대상으로 개인정보보호서약서를 징구하고 있는가? | 보호서약서를 확인할 수 있도록 작성 및 추합하여야함. |
| 개인정보보호교육을 정기적(연 1회 이상)으로 시행하고 관련 증적을 보관하고 있는가? | 교육 시행 증적을 만들어 개인정보보호보 교육이 이루어지고 있음을 증명할 수 있도록 하여야함. |
| 사용자별 계정(1인1계정)을 부여하여 관리하고 있는가? | 녹취서버 유지보수를 위한 OS 접근 시 관리자 계정을 공용으로 사용하지 않도록 책임자의 선별을 통해 권한 최소화가 필요함. |
| 안티바이러스 소프트웨어를 설치 및 운영하고 있는가? | 안티바이러스 프로그램의 업데이트를 1일1회 이상 설정해야 함. |
| 보조저장매체를 허가없이 사용 할 수 없도록 통제하고 있는가? | 보조저장매체의 반출입 및 사용 통제를 위한 매체제어 솔루션 보유사항, 물리적 보안 통제 현황 등이 포함된 내용이 내부관리계획서에 작성되어야함. |