kt ds

협력사 보안점검

이행증적

|  |  |
| --- | --- |
| 협력사명 | OOOOO |
| 업무서비스명 | 케이뱅크 채널시스템 SPA전환 |
| 점검자 | 홍길동 |



# 개인정보관리책임자 지정

|  |  |
| --- | --- |
| **점검항목** | 개인정보관리책임자 지정 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 개인정보보호책임자의 지정 및 명시  - 개인정보보호책임자의 역할 및 책임 명시 - 개인정보보호책임자 임명 관련 자료(인사명령 등), 개인정보보호 조직도, 직무기술서 등 | |

# 정보보호서약서 징구

|  |  |
| --- | --- |
| **점검항목** | 정보보호서약서 징구 |
| **이행 증적** | |
| kbank투입시 진행했던 보안서약서(업체별 별도작성) | |
| **확인사항** | |
| - 정기적인 서약서 징구 여부 확인(연 1회 이상)  - 보안서약서의 안전한 보존 및 관리  - ktds 정보보호서약서 첨부(kt 정보보호서약서 X) | |

# 정보보호교육

|  |  |
| --- | --- |
| **점검항목** | 정보보호교육 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 정보보호 교육 계획서 작성 여부  - 연 1회 이상 교육 시행 및 교육 시 참석자 대장 작성 여부  - 개인정보취급자 중 교육 대상 누락인원 발생 및 추가 교육 이행 여부X)  - 개인정보보호교육계획서, 교육 확인서(참석자 목록), 교육결과 보고서 등 증적 첨부 | |

# 개인정보보호를 위한 자체 정기점검 시행

|  |  |
| --- | --- |
| **점검항목** | 개인정보보호를 위한 자체 정기점검 시행 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 정기적 자체점검활동 및 미조치사항에 대한 이행여부  - 내부점검 결과서, 보안점검 체크리스트 등 증적 첨부 | |

# 내부관리계획 수립 및 시행, 변경 관리

|  |  |
| --- | --- |
| **점검항목** | 내부관리계획 수립 및 시행, 변경 관리 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 내부관리계획이 최고경영층으로부터 내부 결재(승인) 여부  - 법적 요구사항을 반영 재〮개정 이력 관리 여부  - 모든 임직원 및 관련자에게 알릴 수 있도록 공지 또는 게시 여부  - 개인정보보호 내부관리계획서 또는 개인정보보호 정책/지침/절차서와 이의 전사 공지내역 등 | |

# 재위탁

|  |  |
| --- | --- |
| **점검항목** | 재위탁 |
| **이행 증적** | |
| 대상아님 | |
| **확인사항** | |
| - 재위탁이 필요한 경우의 절차와 보안요구사항 정의 여부  - 개인정보처리 업무 재위탁 시 위탁계약서 내 요구되는 사항 준수 여부  - ktds 개인정보처리 업무 재위탁 시 위탁계약서 | |

# 재위탁사의 보호조치

|  |  |
| --- | --- |
| **점검항목** | 재위탁사의 보호조치 |
| **이행 증적** | |
| 대상아님 | |
| **확인사항** | |
| - 재수탁자의 개인정보보호 점검활동에 대한 주기적인 확인  - 재수탁자에 대한 개인정보보호 교육 이행 확인  - 재수탁자에 대한 개인정보보호서약서 징구 확인 | |

# 협력사계정관리시스템 등록

|  |  |
| --- | --- |
| **점검항목** | 협력사계정관리시스템 등록 |
| **이행 증적** | |
| 텍스트, 스크린샷, 평행, 번호이(가) 표시된 사진  자동 생성된 설명 | |
| **확인사항** | |
| - 모든 협력사 직원에 대해 통합계정관리시스템(http://idms.kt.com)에 등록 여부  - 직무변경, 퇴사 등 협력사 직원의 계약 내용 및 정보 변경 시 현행화 여부 | |

# IP신청

|  |  |
| --- | --- |
| **점검항목** | IP신청 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 모든 협력사 직원에 대해 사내IP관리시스템(http://ktip.kt.com)에서 IP 발급 여부  - 1인 1IP 사용을 원칙으로하며 사내 기준의 IP 허용대역 사용 여부  - 계약 종료 시 IP 회수 여부 | |

# 업무 투입/종료 점검표 작성

|  |  |
| --- | --- |
| **점검항목** | 업무 투입/종료 점검표 작성 |
| **이행 증적** | |
| 투입시점의 점검표는 없음. 종료(철수) 시점의 점검표 | |
| **확인사항** | |
| - 업무 투입 및 종료 시 점검표 작성 여부 | |

# 개인정보취급자 권한 관리

|  |  |
| --- | --- |
| **점검항목** | 개인정보취급자 권한 관리 |
| **이행 증적** | |
| 권한 관리는 kbank 시스템으로 kbank담당자가 수행함  프로젝트 팀에서 확인불가 | |
| **확인사항** | |
| - 개인정보처리시스템의 접근 권한 관리 여부 및 직무변경/퇴직자 등 불필요한 권한 관리 여부  - 개인정보시스템의 개인정보취급자 목록, 사용자 계정 및 권한 관리대장 또는 화면 등 증적 첨부 | |

# 접근통제

|  |  |
| --- | --- |
| **점검항목** | 접근통제 |
| **이행 증적** | |
| DBSAFER와 쿼리원    업무망 네트워크 접근제어 | |
| **확인사항** | |
| - 운영서버는 운영용 접근제어시스템, 개발서버는 개발용 접근제어시스템 경유 여부  - 서버를 경유하거나 방화벽을 통해 직접 타 사버에 접속 금지  - 업무상 필요한 경우 CISO의 사전 승인 필요  - 개인정보처리시스템의 접근통제 설정화면 등 증적 첨부 | |

# 목적 외 이용 금지

|  |  |
| --- | --- |
| **점검항목** | 목적 외 이용 금지 |
| **이행 증적** | |
| kbank투입시 진행했던 보안서약서(업체별 별도작성)로 대체 | |
| **확인사항** | |
| - 개인정보를 처리하는 협력사가 계약된 업무 범위 이외의 목적으로 고객정보 이용 불가  - 동의 없이 제 3자에게 고객정보를 제공하지 않도록 관리 필요  - 위탁 계약서 사본, 개인정보보호서약서, 위탁업체 개인정보관리 실태 점검 보고서 등 증적 첨부 | |

# 개인정보 조회

|  |  |
| --- | --- |
| **점검항목** | 개인정보 조회 |
| **이행 증적** | |
| kbank투입시 진행했던 보안서약서(업체별 별도작성)로 대체 | |
| **확인사항** | |
| - 고객정보는 업무상 목적에 맞게 필요한 범위 내에서 최소수집, 최소조회를 원칙으로 목적 외 이용 금지  - 접속 및 접속 기록을 정기적으로 보관 및 점검 필요  - 업무상 필요한 최소 범위로 권한 부여하도록 관리  - 접속 및 조회 로그이력, 개인정보보호서약서 등 증적 첨부 | |

# 물리적 보호조치

|  |  |
| --- | --- |
| **점검항목** | 물리적 보호조치 |
| **이행 증적** | |
| (노트북 시건장치)  텍스트, 배터리, 전자제품, 케이블이(가) 표시된 사진  자동 생성된 설명  (일일보안점검) | |
| **확인사항** | |
| - 고객정보를 취급하는 서버/DB가 운영되는 공간에 대한 접근통제  - 고객정보 서류 등을 보관 장소에 잠금장치 설치  - 개인정보를 취급하는 장소의 물리적 보안 촬영, 출입대장관리 및 출입기록, 접근통제가 적용된 문서보관장소 사진 및 화면 등 증적 첨부 | |

# 자료보관 보호조치 - 파일

|  |  |
| --- | --- |
| **점검항목** | 자료보관 보호조치 - 파일 |
| **이행 증적** | |
| 문서보안 적용  텍스트, 스크린샷, 컴퓨터, 디스플레이이(가) 표시된 사진  자동 생성된 설명 | |
| **확인사항** | |
| - 개인정보취급자 단말기 내 개인정보 저장 시 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 암호화  - 불법적인 유/노출 및 접근 등으로부터 보호 - 단말기 내 개인정보파일 암호화 저장 화면(문서보안 프로그램 적용 화면) 등 증적 첨부 | |

# 자료보관 보호조치 – 서류

|  |  |
| --- | --- |
| **점검항목** | 자료보관 보호조치 – 서류 |
| **이행 증적** | |
| Kbank프로젝트룸에 프린트기 없음  문서 출력하지 않음 | |
| **확인사항** | |
| - 고객정보가 포함된 문서의 보관은 시건 장치가 적용된 안전한 장소에 보관  - 접근통제가 적용된 개인정보 문서보관장소 사진 또는 화면 등 증적 첨부 | |

# 계정관리

|  |  |
| --- | --- |
| **점검항목** | 계정관리 |
| **이행 증적** | |
| 개별 계정으로 vdi에 접속  시스템접근시 개인 핸드폰의 kbank otp로 인증후 접속가능  계정관리 대장은 협력사에서 볼 수 없음 | |
| **확인사항** | |
| - 1인 1계정 사용 원칙이며, 타인과 계정 공유 금지  - 계정/암호를 공유하지 않도록 개별 ID 발급 및 관리 절차 준수  - 개인별 계정 발급 현황, 로그인 이력 등 증적 첨부 | |

# 비밀번호 관리

|  |  |
| --- | --- |
| **점검항목** | 비밀번호 관리 |
| **이행 증적** | |
| 텍스트, 스크린샷, 번호이(가) 표시된 사진  자동 생성된 설명 | |
| **확인사항** | |
| - 시스템 및 PC 계정에 대한 비밀번호 작성 규칙 수립 및 적용 여부  - 비밀번호 설정 화면, 비밀번호 강제적용 화면 등 증적 첨부 | |

# CMOS 비밀번호 관리

|  |  |
| --- | --- |
| **점검항목** | CMOS 비밀번호 관리 |
| **이행 증적** | |
| Kbank는 vdi사용  개발자 로컬pc에 CMOS 비밀번호 적용하지 않음 | |
| **확인사항** | |
| - PC 부팅 시 CMOS 패스워드 설정  - HDD Lock 설정  - 2가지 설정 필수 | |

# 보안SW설치 및 최신 업데이트 적용

|  |  |
| --- | --- |
| **점검항목** | 보안SW설치 및 최신 업데이트 적용 |
| **이행 증적** | |
| |  |  | | --- | --- | | dbsafer | Secuve AuthClient | |  |  | | Document Security | AhnLab Safe Transaction | |  |  | | 출력물보안 | PC Filter | |  |  | | 안랜 시큐러티 에이전트 |  | |  |  | | |
| **확인사항** | |
| - 바이러스 백신프로그램(V3, EPP), DRM, DLP, Privacy-I, NAC 설치 및 최신 업데이트 여부 | |

# 백도어 및 불법프로그램 사용 금지

|  |  |
| --- | --- |
| **점검항목** | 백도어 및 불법프로그램 사용 금지 |
| **이행 증적** | |
| 비인가프로그램 차단 | |
| **확인사항** | |
| - 개인정보취급자의 단말기에서 P2P, 토렌트, 메신저 프로그램 등 비인가프로그램, 공유 설정 등에 대한 통제  - 불법 인증 소프트웨어(crack, keygen, backdoor 등) 설치 및 사용하지 않도록 관리  - 단말기 내 설치프로그램 목록 화면, 비인가 프로그램 차단 시스템 화면 등 증적 첨부 | |

# PC 내 불필요한 개인정보 보유

|  |  |
| --- | --- |
| **점검항목** | PC 내 불필요한 개인정보 보유 |
| **이행 증적** | |
| 텍스트, 스크린샷, 컴퓨터, 멀티미디어이(가) 표시된 사진  자동 생성된 설명 | |
| **확인사항** | |
| - 업무용 PC 내 불필요한 개인정보를 보유하지 않아야함  - 필요 시 목적에 맞게 사용 후 즉시 파기  - Privacy-i에서 검출 내역 확인 | |

# 공유폴더 관리

|  |  |
| --- | --- |
| **점검항목** | 공유폴더 관리 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 업무PC 공유폴더 사용 금지  - 업무상 필요에 의해 공유폴더를 사용하는 경우 영문(대/소문자 혼합), 숫자, 특수문자 등을 혼용하여 최소 8자리 이상의 조합 비밀번호를 사용하고 사용 종료 즉시 공유 폴더 해제 | |

# 화면보호기 암호 설정 여부 확인

|  |  |
| --- | --- |
| **점검항목** | 화면보호기 암호 설정 여부 확인 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 화면보호기 동작시간이 10분 이내로 설정  - 재사용 방지를 위한 암호설정 부분 확인(암호는 주기적으로 변경) | |

# 휴대용 저장매체 사용 통제

|  |  |
| --- | --- |
| **점검항목** | 휴대용 저장매체 사용 통제 |
| **이행 증적** | |
|  | |
| **확인사항** | |
| - 매체제어솔루션, 포트 락커 또는 기타 방법으로 비인가 보조저장매체 사용 통제  - 승인 받은 저장매체만 사용 | |