ISMS-P 준수

컴플라이언스 분석보고서

Teiren ISMS-P Compliance Analysis Report

| 1.1 관리체계 기반 마련

Teiren 1. 관리체계 수립 및 운영



|  |  |
| --- | --- |
| 항목 | * + 1. 경영진의 참여 |
| 인증 기준 | 최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다. |
| 주요 확인사항 | * 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가? * 경영진이 정보보호 및 개인정보보호 활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립/이행하고 있는가? |

| 증거 자료 예시

|  |
| --- |
| * 정보보호 및 개인정보보호 보고 체계(의사소통계획 등) * 정보보호 및 개인정보보호위원회 회의록 * 정보보호 및 개인정보보호 정책/지침 (경영진 승인내역 포함) * 정보보호계획 및 내부관리 계획 (경영진 승인내역 포함) * 정보보호 및 개인정보보호 조직도 |

| 증적 관리

|  |  |  |
| --- | --- | --- |
| Teiren 가이드 항목 | 증거 자료 | 운영 현황 |
| 1.1 조직도 | 조직도 / [Teiren][ISMS-P]1.1\_개인정보보호조직도.pdf | 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있음 |

Teiren ISMS-P 준수 컴플라이언스 분석보고서 01

| 1.1 관리체계 기반 마련

Teiren 1. 관리체계 수립 및 운영



|  |  |
| --- | --- |
| 항목 | * + 1. 최고책임자의 지정 |
| 인증 기준 | 최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산∙인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다. |
| 주요 확인사항 | * 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가? |
| * 정보보호 최고책임자 및 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 있으며 관련 법령에 따른 자격요건을 충족하고 있는가? |
| 관련 법규 | * 개인정보보호법 제29조(안전조치의무), 제 31조(개인정보 보호책임자의 지정) * 정보통신망법 제45조의 3(정보보호 최고책임자의 지정 등) * 개인정보의 안전성 확보조치기준 제4조(내부관리계획의 수립·시행) * 개인정보의 기술적·관리적 보호조치 기준 제3조(내부관리계획의 수립·시행) |

| 증거 자료 예시

|  |
| --- |
| * 정보보호 최고책임자 및 개인정보 보호책임자 임명관련 자료(인사명령, 인사카드 등) * 정보보호 및 개인정보보호 조직도 * 정보보호 및 개인정보보호 정책·지침 * 직무기술서(정보보호 최고책임자 및 개인정보 보호책임자의 역할 및 책임에 관한 사항) * 정보보호 최고책임자 지정 내역 * 내부관리계획(개인정보 보호책임자 지정에 관한 사항) |

| 증적 관리

|  |  |  |
| --- | --- | --- |
| Teiren 가이드 항목 | 증거 자료 | 운영 현황 |
| 1.1 사용자 계정 관리 | 냥 | 냥냐링냥냥 |

Teiren ISMS-P 준수 컴플라이언스 분석보고서 02

| 2.4 물리 보안

Teiren 2. 보호대책 요구사항



|  |  |
| --- | --- |
| 항목 | 2.5.1 사용자 계정 관리 |
| 인증 기준 | 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록∙해지 및 접근권한 부여∙변경∙말소 절차를 수립∙이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다. |
| 주요 확인사항 | * 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한의 등록∙변경∙삭제에 관한 공식적인 절차를 수립∙이행하고 있는가? |
| * 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성∙등록∙변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가? |
| * 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시키고 있는가? |
| 관련 법규 | * 개인정보 보호법 제29조(안전조치의무) * 개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리) * 개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제) |

| 증거 자료 예시

|  |
| --- |
| * 사용자 계정 및 권한 신청서 * 사용자 계정 및 권한 관리대장 또는 화면 * 정보시스템 및 개인정보처리시스템별 접근권한 분류표 * 정보시스템 및 개인정보처리시스템별 사용자, 관리자, 개인정보취급자 목록 |

| 증적 관리

Teiren ISMS-P 준수 컴플라이언스 분석보고서 03

|  |  |  |
| --- | --- | --- |
| ISMS-P 항목 | 증거 자료 | 준수 여부 |
| 2.5.1 사용자 계정 관리 |  | IAM 사용자의 MFA를 활성화해 접근권한 및 개인정보보호 관리가 이루어지고 있음 |
| 2.5.1 사용자 계정 관리 | 텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진  자동 생성된 설명 | IAM 사용자가 그룹에 사용자를 속하게 함으로써 최소한의 접근 권한만을 상속받아 사용함. |
| 2.5.1 사용자 계정 관리 |  | AWS Root 계정 자격증명의 액세스키를 활성화하지 않고 보호하고 있음. |
| 2.5.1 사용자 계정 관리 | 텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진  자동 생성된 설명 | AWS Organization 서비스에 AWS 계정에 대한 조직을 구성해 정보 시스템에 대한 접근 권한을 적절히 관리하고 있음 |

Teiren 2. 보호대책 요구사항



Teiren ISMS-P 준수 컴플라이언스 분석보고서 04