

| 1.1. 관리체계 기반 마련

항목	1.1.1 경영진의 참여
인증기준	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 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?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.1. 관리체계 기반 마련

항목	1.1.2 최고책임자의 지정
인증기준	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
주요 확인사항	<ul style="list-style-type: none">최고경영자는 정보보호 및 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가?정보보호 최고책임자 및 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 있으며 관련 법령에 따른 자격요건을 충족하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.1. 관리체계 기반 마련

항목	1.1.3 조직 구성
인증기준	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보보호 최고책임자 및 개인정보 보호책임자의 업무를 지원하고 조직의 정보보호 및 개인정보보호 활동을 체계적으로 이행하기 위해 전문성을 갖춘 실무조직을 구성하여 운영하고 있는가? • 조직 전반에 걸친 중요한 정보보호 및 개인정보보호 관련사항에 대하여 검토, 승인 및 의사결정을 할 수 있는 위원회를 구성하여 운영하고 있는가? • 전사적 정보보호 및 개인정보보호 활동을 위하여 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자로 구성된 실무 협의체를 구성하여 운영하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.1. 관리체계 기반 마련

항목	1.1.4 범위 설정
인증기준	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
주요 확인사항	<ul style="list-style-type: none">조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 관리체계 범위를 설정하고 있는가?정의된 범위 내에서 예외사항이 있을 경우 명확한 사유 및 관련자 협의·책임자 승인 등 관련 근거를 기록·관리하고 있는가?정보보호 및 개인정보보호 관리체계 범위를 명확히 확인할 수 있도록 관련된 내용(주요 서비스 및 업무 현황, 정보시스템 목록, 문서목록 등)이 포함된 문서를 작성하여 관리하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.1. 관리체계 기반 마련

항목	1.1.5 정책 수립
인증기준	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책을 수립하고 있는가? • 정보보호 및 개인정보보호 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 지침, 절차, 매뉴얼 등을 수립하고 있는가? • 정보보호 및 개인정보보호 정책·시행문서의 제·개정 시 최고경영자 또는 최고경영자로부터 권한을 위임받은 자의 승인을 받고 있는가? • 정보보호 및 개인정보보호 정책·시행문서의 최신본을 관련 임직원에게 접근하기 쉬운 형태로 제공하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.1. 관리체계 기반 마련

항목	1.1.6 자원 할당
인증기준	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보보호 및 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고 있는가? • 정보보호 및 개인정보보호 관리체계의 효과적 구현과 지속적 운영을 위해 필요한 자원을 평가하여 필요한 예산과 인력을 지원하고 있는가? • 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립·시행하고 그 추진결과에 대한 심사분석?평가를 실시하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 1.2. 위험 관리

항목	1.2.1 정보자산 식별
인증기준	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보자산의 분류기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하고 있는가?식별된 정보자산에 대해 법적 요구사항 및 업무에 미치는 영향 등을 고려하여 중요도를 결정하고 보안등급을 부여하고 있는가?정기적으로 정보자산 현황을 조사하여 정보자산목록을 최신으로 유지하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.2. 위험 관리

항목	1.2.2 현황 및 흐름분석
인증기준	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화하고 있는가?• 관리체계 범위 내 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여 개인정보흐름도 등으로 문서화하고 있는가?• 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 개인정보 흐름을 주기적으로 검토하여 흐름도 등 관련 문서의 최신성을 유지하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.2. 위험 관리

항목	1.2.3 위험 평가
인증기준	조직의 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 조직 또는 서비스의 특성에 따라 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하고 있는가? • 위험관리 방법 및 절차(수행인력, 기간, 대상, 방법, 예산 등)를 구체화한 위험관리계획을 매년 수립하고 있는가? • 위험관리계획에 따라 연 1회 이상 정기적으로 또는 필요한 시점에 위험평가를 수행하고 있는가? • 조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별하고 있는가? • 위험식별 및 평가 결과를 경영진에게 보고하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.2. 위험 관리

항목	1.2.4 보호대책 선정
인증기준	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
주요 확인사항	<ul style="list-style-type: none">식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 보호대책을 선정하고 있는가?보호대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호대책 이행계획을 수립하고 경영진에 보고하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.3. 관리체계 운영

항목	1.3.1 보호대책 구현
인증기준	선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 이행계획에 따라 보호대책을 효과적으로 구현하고 이행결과의 정확성 및 효과성 여부를 경영진이 확인할 수 있도록 보고하고 있는가?• 관리체계 인증기준 별로 보호대책 구현 및 운영 현황을 기록한 운영명세서를 구체적으로 작성하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.3. 관리체계 운영

항목	1.3.2 보호대책 공유
인증기준	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영 되도록 하여야 한다.
주요 확인사항	<ul style="list-style-type: none">구현된 보호대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하고 있는가?구현된 보호대책을 운영 또는 시행할 부서 및 담당자에게 관련 내용을 공유 또는 교육하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.3. 관리체계 운영

항목	1.3.3 운영현황 관리
인증기준	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 관리체계 운영을 위해 주기적 또는 상시적으로 수행해야 하는 정보보호 및 개인정보보호 활동을 문서화하여 관리하고 있는가?• 경영진은 주기적으로 관리체계 운영활동의 효과성을 확인하고 이를 관리하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.4. 관리체계 점검 및 개선

항목	1.4.1 법적 요구사항 준수 검토
인증기준	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 조직이 준수하여야 하는 정보보호 및 개인정보보호 관련 법적 요구사항을 파악하여 최신성을 유지하고 있는가?• 법적 요구사항의 준수여부를 연 1회 이상 정기적으로 검토하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.4. 관리체계 점검 및 개선

항목	1.4.2 관리체계 점검
인증기준	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
주요 확인사항	<ul style="list-style-type: none">법적 요구사항 및 수립된 정책에 따라 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검 계획을 수립하고 있는가?관리체계 점검 계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 경영진에게 보고하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 1.4. 관리체계 점검 및 개선

항목	1.4.3 관리체계 개선
인증기준	법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계 상의 문제점에 대한 근본 원인을 분석하여 재발방지 및 개선 대책을 수립?이행하고 있는가?재발방지 및 개선 결과의 정확성 및 효과성 여부를 확인하기 위한 기준과 절차를 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.1. 정책, 조직, 자산 관리

항목	2.1.1 정책의 유지관리
인증기준	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보보호 및 개인정보보호 관련 정책 및 시행문서에 대한 정기적인 타당성 검토 절차를 수립·이행하고 있는가? • 조직의 대내외 환경에 중대한 변화 발생 시 정보보호 및 개인정보보호 관련 정책 및 시행문서에 미치는 영향을 검토하고 필요시 제·개정하고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 시 이해 관계자의 검토를 받고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 내역에 대하여 이력 관리를 하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.1. 정책, 조직, 자산 관리

항목	2.1.2 조직의 유지관리
인증기준	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보보호 및 개인정보보호 관련 책임자와 담당자의 역할 및 책임을 명확히 정의하고 있는가? • 정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하고 있는가? • 정보보호 및 개인정보보호 관련 조직 및 조직의 구성원간 상호 의사소통할 수 있는 체계 및 절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.1. 정책, 조직, 자산 관리

항목	2.1.3 정보자산 관리
인증기준	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 식별된 정보자산에 대하여 책임자 및 관리자를 지정하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.2. 인적 보안

항목	2.2.1 주요 직무자 지정 및 관리
인증기준	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하고 있는가?주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고 그 목록을 최신으로 관리하고 있는가?업무상 개인정보를 취급하는 자를 개인정보취급자로 지정하고 목록을 최신으로 관리하고 있는가?업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.2. 인적 보안

항목	2.2.2 직무 분리
인증기준	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하여 적용하고 있는가?• 직무분리가 어려운 경우 직무자간 상호 검토, 상위관리자 정기 모니터링 및 변경사항 승인, 책임추적성 확보 방안 등의 보완통제를 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.2. 인적 보안

항목	2.2.3 보안 서약
인증기준	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받고 있는가? • 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가? • 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가? • 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보관하고 필요시 쉽게 찾아볼 수 있도록 관리하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.2. 인적 보안

항목	2.2.4 인식제고 및 교육훈련
인증기준	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보보호 및 개인정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 교육 계획을 수립하고 경영진의 승인을 받고 있는가? • 관리체계 범위 내 모든 임직원과 외부자를 대상으로 연간 교육계획에 따라 연1회 이상 정기적으로 교육을 수행하고, 관련 법규 및 규정의 중대한 변경 시 이에 대한 추가교육을 수행하고 있는가? • 임직원 채용 및 외부자 신규 계약 시, 업무 시작 전에 정보보호 및 개인정보보호 교육을 시행하고 있는가? • IT 및 정보보호, 개인정보보호 조직 내 임직원은 정보보호 및 개인정보보호와 관련하여 직무별 전문성 제고를 위한 별도의 교육을 받고 있는가? • 교육시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.2. 인적 보안

항목	2.2.5 퇴직 및 직무변경 관리
인증기준	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 퇴직, 직무변경, 부서이동, 휴직 등으로 인한 인사변경 내용이 인사부서, 정보보호 및 개인정보보호 부서, 정보 시스템 및 개인정보처리시스템 운영부서 간에 공유되고 있는가? 조직 내 인력(임직원, 임시직원, 외주용역직원 등)의 퇴직 또는 직무변경 시 지체 없는 정보자산 반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.2. 인적 보안

항목	2.2.6 보안 위반 시 조치
인증기준	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">임직원 및 관련 외부자가 법령과 규제 및 내부정책에 따른 정보보호 및 개인정보보호 책임과 의무를 위반한 경우에 대한 처벌 규정을 수립하고 있는가?정보보호 및 개인정보 보호 위반 사항이 적발된 경우 내부 절차에 따른 조치를 수행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.3. 외부자 보안

항목	2.3.1 외부자 현황 관리
인증기준	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의 이용 현황을 식별하고 있는가? • 업무 위탁 및 외부 시설·서비스의 이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호대책을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.3. 외부자 보안

항목	2.3.2 외부자 계약 시 보안
인증기준	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 중요정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁업체를 선정하는 경우 정보보호 및 개인정보 보호 역량을 고려하도록 절차를 마련하고 있는가? 외부 서비스 이용 및 업무 위탁에 따른 정보보호 및 개인정보보호 요구사항을 식별하고 이를 계약서 또는 협정서에 명시하고 있는가? 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수해야 할 정보보호 및 개인정보보호 요구사항을 계약서에 명시하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.3. 외부자 보안

항목	2.3.3 외부자 보안 이행 관리
인증기준	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 있는가? • 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선계획을 수립?이행하고 있는가? • 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 동의를 받도록 하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.3. 외부자 보안

항목	2.3.4 외부자 계약 변경 및 만료 시 보안
인증기준	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근제한 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 외부자 계약만료, 업무 종료, 담당자 변경시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근제한 삭제, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하고 있는가? 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할 수 있도록 절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.1 보호구역 지정
인증기준	물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">물리적, 환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역 지정기준을 마련하고 있는가?물리적 보호구역 지정기준에 따라 보호구역을 지정하고 구역별 보호대책을 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.2 출입통제
인증기준	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 보호구역은 출입절차에 따라 출입이 허가된 자만 출입하도록 통제하고 있는가?• 각 보호구역에 대한 내·외부자 출입기록을 일정기간 보존하고 출입기록 및 출입권한을 주기적으로 검토하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.3 정보시스템 보호
인증기준	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보시스템의 중요도, 용도, 특성 등을 고려하여 배치 장소를 분리하고 있는가?• 정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안을 마련하고 있는가?• 전력 및 통신케이블을 외부로부터의 물리적 손상 및 전기적 영향으로부터 안전하게 보호하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.4 보호설비 운영
인증기준	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온도·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립하여 운영하고 있는가? • 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.5 보호구역 내 작업
인증기준	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업신청 및 수행 절차를 수립·이행하고 있는가?보호구역내 작업이 통제 절차에 따라 적절히 수행되었는지 여부를 확인하기 위하여 작업 기록을 주기적으로 검토하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.6 반출입 기기 통제
인증기준	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템, 모바일기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하고 있는가?반출입 통제절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.4. 물리 보안

항목	2.4.7 업무환경 보안
인증기준	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호대책을 수립·이행하고 있는가? • 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유?노출을 방지하기 위한 보호대책을 수립·이행하고 있는가? • 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력?복사물을 안전하게 관리하기 위해 필요한 보호조치를 하고 있는가? • 개인 및 공용업무 환경에서의 정보보호 준수여부를 주기적으로 검토하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.5. 인증 및 권한관리

항목	2.5.1 사용자 계정 관리
인증기준	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	<ul style="list-style-type: none"> • 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?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.5. 인증 및 권한관리

항목	2.5.2 사용자 식별
인증기준	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가?불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 보완대책을 마련하여 책임자의 승인을 받고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.5. 인증 및 권한관리

항목	2.5.3 사용자 인증
인증기준	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하고 있는가?정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증 수단 또는 안전한 접속수단을 적용하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 2.5. 인증 및 권한관리

항목	2.5.4 비밀번호 관리
인증기준	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템에 대한 안전한 사용자비밀번호 관리절차 및 작성규칙을 수립·이행하고 있는가?정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성 규칙을 수립·dh 이행하고 있는가?개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.5. 인증 및 권한관리

항목	2.5.5 특수 계정 및 권한 관리
인증기준	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 관리자 권한 등 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하고 있는가? 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하는 등 통제절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.5. 인증 및 권한관리

항목	2.5.6 접근권한 검토
인증기준	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남기고 있는가? 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토주체, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하고 있는가? 접근권한 검토 결과 접근권한 과다 부여, 권한부여 절차 미준수, 권한 오남용 등 문제점이 발견된 경우 그에 따른 조치절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.1 네트워크 접근
인증기준	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가? • 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역간 접근통제를 적용하고 있는가? • 네트워크 대역별 IP주소 부여 기준을 마련하고 DB서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가? • 물리적으로 떨어진 IDC, 지사, 대리점 등과의 네트워크 연결 시 전송구간 보호대책을 마련하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.2 정보시스템 접근
인증기준	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 서버, 네트워크시스템, 보안시스템 등 정보시스템 별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가? • 정보시스템에 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가? • 정보시스템의 사용목적과 관계없는 서비스를 제거하고 있는가? • 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 2.6. 접근통제

항목	2.6.3 응용프로그램 접근
인증기준	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 차등 부여하고 있는가?• 일정 시간동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가?• 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하고 있는가?• 개인정보 및 중요정보의 표시제한 보호조치의 일관성을 확보할 수 있도록 관련 기준을 수립하여 적용하고 있는가?• 개인정보 및 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하여 운영하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.4 데이터베이스 접근
인증기준	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 있는가?데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.5 무선 네트워크 접근
인증기준	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위해 인증, 송수신 데이터 암호화 등 보호대책을 수립·이행하고 있는가?인가된 임직원만이 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립·이행하고 있는가?AD Hoc 접속 및 조직내 허가 받지 않은 무선 AP 탐지·차단 등 비인가된 무선네트워크에 대한 보호대책을 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.6 원격접근 통제
인증기준	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격 협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 장애대응 등 부득이하게 허용하는 경우 보완대책을 마련하고 있는가? • 내부 네트워크를 통해서 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가? • 재택근무, 원격협업, 스마트워크 등과 같은 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호대책을 수립?이행하고 있는가? • 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리시스템에 접속하는 단말기는 관리용 단말기로 지정하고 임의조작 및 목적 외 사용 금지 등 안전조치를 적용하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.7 인터넷 접속 통제
인증기준	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P4P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">관련 법령에 따라 인터넷망 차단 의무가 부과된 경우 대상자를 식별하여 안전한 방식으로 인터넷망 차단 조치를 적용하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.7 인터넷 접속 통제
인증기준	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제정책을 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.6. 접근통제

항목	2.6.7 인터넷 접속 통제
인증기준	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P3P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">주요 정보시스템(DB서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.7. 암호화 적용

항목	2.7.1 암호정책 적용
인증기준	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는가?암호정책에 따라 개인정보 및 주요정보의 저장, 전송, 전달 시 암호화를 수행하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.7. 암호화 적용

항목	2.7.2 암호키 관리
인증기준	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.
주요 확인사항	<ul style="list-style-type: none">암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가?암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.8. 정보시스템 도입 및 개발 보안

항목	2.8.1 보안 요구사항 정의
인증기준	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보시스템을 신규로 도입·개발 또는 변경하는 경우 정보보호 및 개인정보보호 측면의 타당성 검토 및 인수 절차를 수립·이행하고 있는가?• 정보시스템을 신규로 도입·개발 또는 변경하는 경우 법적 요구사항, 최신 취약점 등을 포함한 보안 요구사항을 명확히 정의하고 설계 단계에서부터 반영하고 있는가?• 정보시스템의 안전한 구현을 위한 코딩 표준을 수립하여 적용하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 2.8. 정보시스템 도입 및 개발 보안

항목	2.8.2 보안 요구사항 검토 및 시험
인증기준	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템의 도입, 개발, 변경 시 분석 및 설계 단계에서 정의한 보안 요구사항이 효과적으로 적용되었는지를 확인하기 위한 시험을 수행하고 있는가?정보시스템이 안전한 코딩 기준 등에 따라 안전하게 개발되었는지를 확인하기 위한 취약점 점검이 수행되고 있는가?시험 및 취약점 점검 과정에서 발견된 문제점이 신속하게 개선될 수 있도록 개선계획 수립, 이행점검 등의 절차를 이행하고 있는가?공공기관은 관련 법령에 따라 개인정보처리시스템 신규 개발 및 변경 시 분석·설계 단계에서 영향평가기관을 통해 영향평가를 수행하고 그 결과를 개발 및 변경 시 반영하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 2.8. 정보시스템 도입 및 개발 보안

항목	2.8.3 시험과 운영 환경 분리
인증기준	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가?• 불가피한 사유로 개발과 운영환경의 분리가 어려운 경우 상호검토, 상급자 모니터링, 변경 승인, 책임추적성 확보 등의 보안대책을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.8. 정보시스템 도입 및 개발 보안

항목	2.8.4 시험 데이터 보안
인증기준	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가?• 불가피하게 운영데이터를 시험 환경에서 사용할 경우 책임자 승인, 접근 및 유출 모니터링, 시험 후 데이터 삭제 등의 통제 절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.8. 정보시스템 도입 및 개발 보안

항목	2.8.5 소스 프로그램 관리
인증기준	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.
주요 확인사항	<ul style="list-style-type: none">비인가된 자에 의한 소스 프로그램 접근을 통제하기 위한 절차를 수립·이행하고 있는가?소스 프로그램은 장애 등 비상시를 대비하여 운영환경이 아닌 곳에 안전하게 보관하고 있는가?소스 프로그램에 대한 변경이력을 관리하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.8. 정보시스템 도입 및 개발 보안

항목	2.8.6 운영환경 이관
인증기준	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.
주요 확인사항	<ul style="list-style-type: none">신규 도입·개발 및 변경된 시스템을 운영환경으로 안전하게 이관하기 위한 통제 절차를 수립·이행하고 있는가?운영환경으로의 이관 시 발생할 수 있는 문제에 대한 대응 방안을 마련하고 있는가?운영환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.1 변경관리
인증기준	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립·이행하고 있는가?정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.2 성능 및 장애관리
인증기준	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보시스템의 가용성 보장을 위하여 성능 및 용량을 지속적으로 모니터링 할 수 있는 절차를 수립·이행하고 있는가?• 정보시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우에 대한 대응절차를 수립·이하고 있는가?• 정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립·이행하고 있는가?• 장애 발생 시 절차에 따라 조치하고 장애조치보고서 등을 통해 장애조치내역을 기록하여 관리하고 있는가?• 심각도가 높은 장애의 경우 원인분석을 통한 재발방지 대책을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.3 백업 및 복구관리
인증기준	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하고 있는가? • 백업된 정보의 완전성과 정확성, 복구절차의 적절성을 확인하기 위하여 정기적으로 복구 테스트를 실시하고 있는가? • 중요정보가 저장된 백업매체의 경우 재해?재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.4 로그 및 접속기록 관리
인증기준	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그관리 절차를 수립하고 이에 따라 필요한 로그를 생성하여 보관하고 있는가? 정보시스템의 로그기록은 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 로그기록에 대한 접근권한은 최소화하여 부여하고 있는가? 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 필요한 항목을 모두 포함하여 일정 기간 안전하게 보관하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.5 로그 및 접속기록 점검
인증기준	정보시스템의 정상적인 사용을 보장하고 사용자 오·남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템 관련 오류, 오·남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차를 수립·이행하고 있는가?로그 검토 및 모니터링 결과를 책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하고 있는가?개인정보처리시스템의 접속기록은 관련 법령에서 정한 주기에 따라 정기적으로 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.6 시간 동기화
인증기준	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보시스템의 시간을 표준시간으로 동기화하고 있는가?시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.9. 시스템 및 서비스 운영관리

항목	2.9.7 정보자산의 재사용 및 폐기
인증기준	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구?재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보자산의 안전한 재사용 및 폐기에 대한 절차를 수립·이행하고 있는가? • 정보자산 및 저장매체를 재사용 및 폐기하는 경우 개인정보 및 중요정보를 복구되지 않는 방법으로 처리하고 있는가? • 자체적으로 정보자산 및 저장매체를 폐기할 경우 관리대장을 통해 폐기이력을 남기고 폐기확인 증적을 함께 보관하고 있는가? • 외부업체를 통해 정보자산 및 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전히 폐기했는지 여부를 확인하고 있는가? • 정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장매체 내 정보를 보호하기 위한 대책을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.1 보안시스템 운영
인증기준	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 조직에서 운영하고 있는 보안시스템에 대한 운영절차를 수립·이행하고 있는가? • 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? • 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가? • 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가? • 보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가? • 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 관련 법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.2 클라우드 보안
인증기준	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서 (SLA 등)에 반영하고 있는가? • 클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하고 있는가? • 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가된 접근, 권한 오남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호대책을 적용하고 있는가? • 클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.3 공개서버 보안
인증기준	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 공개서버를 운영하는 경우 이에 대한 보호대책을 수립·이행하고 있는가? • 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가? • 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시절차를 수립·이행하고 있는가? • 조직의 중요정보가 웹사이트 및 웹서버를 통해 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.4 전자거래 및 핀테크 보안
인증기준	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위해 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
주요 확인사항	<ul style="list-style-type: none">전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호대책을 수립·이행하고 있는가?전자거래 및 핀테크 서비스 제공을 위하여 결제시스템 등 외부 시스템과 연계하는 경우 송·수신되는 관련 정보의 보호를 위한 대책을 수립·이행하고 안전성을 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.5 정보전송 보안
인증기준	타 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통해 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 있는가?• 업무상 조직 간에 개인정보 및 중요정보를 상호교환하는 경우 안전한 전송을 위한 협약체결 등 보호대책을 수립·이행하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.6 업무용 단말기기 보안
인증기준	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안 설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안 설정 등의 보안 통제 정책을 수립·이행하고 있는가? • 업무용 단말기를 통해 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료공유프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하고 있는가? • 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 보안대책을 적용하고 있는가? • 업무용 단말기기에 대한 접근통제 대책의 적절성에 대해 주기적으로 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.7 보조저장매체 관리
인증기준	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 외장하드, USB메모리, CD 등 보조저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하고 있는가? • 보조저장매체 보유현황, 사용 및 관리실태를 주기적으로 점검하고 있는가? • 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용을 제한하고 있는가? • 보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가? • 개인정보 또는 중요정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.8 패치관리
인증기준	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치 관리 정책 및 절차를 수립·이행하고 있는가? • 주요 서버, 네트워크시스템, 보안시스템 등의 경우 설치된 OS, 소프트웨어 패치적용 현황을 주기적으로 관리하고 있는가? • 서비스 영향도 등에 따라 취약점을 조치하기 위한 최신의 패치 적용이 어려운 경우 보완대책을 마련하고 있는가? • 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가? • 패치관리시스템을 활용하는 경우 접근통제 등 충분한 보호대책을 마련하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.10. 시스템 및 서비스 보안관리

항목	2.10.9 악성코드 통제
인증기준	바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용단말기 등을 보호하기 위하여 보호대책을 수립·이행하고 있는가? • 백신 소프트웨어 등 보안프로그램을 통하여 최신 악성코드 예방/탐지 활동을 지속적으로 수행하고 있는가? • 백신 소프트웨어 등 보안프로그램은 최신의 상태로 유지하고 필요시 긴급 보안업데이트를 수행하고 있는가? • 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.11. 사고 예방 및 대응

항목	2.11.1 사고 예방 및 대응체계 구축
인증기준	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가? • 보안관제서비스 등 외부 기관을 통해 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응절차의 세부사항을 계약서에 반영하고 있는가? • 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.11. 사고 예방 및 대응

항목	2.11.2 취약점 점검 및 조치
인증기준	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보시스템 취약점 점검 절차를 수립하고 정기적으로 점검을 수행하고 있는가? • 발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가? • 최신 보안취약점 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하고 있는가? • 취약점 점검 이력을 기록관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대해 보호대책을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.11. 사고 예방 및 대응

항목	2.11.3 이상행위 분석 및 모니터링
인증기준	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.
주요 확인사항	<ul style="list-style-type: none"> 내·외부에 의한 침해시도, 개인정보 유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가? 침해시도, 개인정보유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상 행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.11. 사고 예방 및 대응

항목	2.11.4 사고 대응 훈련 및 개선
인증기준	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.
주요 확인사항	<ul style="list-style-type: none">침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련계획을 수립하고 이에 따라 연1회 이상 주기적으로 훈련을 실시하고 있는가?침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.11. 사고 예방 및 대응

항목	2.11.5 사고 대응 및 복구
인증기준	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가? • 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체(이용자) 통지 및 관계기관 신고 절차를 이행하고 있는가? • 침해사고가 종결된 후 사고의 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하고 있는가? • 침해사고 분석을 통해 얻어진 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.12. 재해복구

항목	2.12.1 재해·재난 대비 안전조치
인증기준	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별하고 있는가? 핵심 IT 서비스 및 시스템의 중요도 및 특성에 따른 복구 목표시간, 복구 목표시점을 정의하고 있는가? 재해 및 재난 발생 시에도 핵심 서비스 및 시스템의 연속성을 보장할 수 있도록 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구 계획을 수립·이행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 2.12. 재해복구

항목	2.12.2 재해 복구 시험 및 개선
인증기준	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.
주요 확인사항	<ul style="list-style-type: none">수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험계획을 수립·이행하고 있는가?시험결과, 정보시스템 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토?보완하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 15세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보주체에게 개인정보 수집 동의를 받는 경우 동의방법 및 시점은 적절하게 되어 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 20세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 정보주체 및 법정대리인에게 동의를 받은 기록을 보관하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 14세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보를 수집하는 경우 정보주체 동의, 법령상 의무준수, 계약 체결·이행 등 적법 요건에 따라 수집하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 18세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">법정대리인의 동의를 받기 위하여 필요한 최소한의 개인정보만을 수집하고 있으며, 법정대리인이 자격 요건을 갖추고 있는지 확인하는 절차와 방법을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 16세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체에게 개인정보 수집 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 명확히 표시하여 알아보기 쉽게 표시하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 19세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">만 14세 미만의 아동에게 개인정보 처리와 관련한 사항 등의 고지 시 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 표현하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 21세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하거나 정보주체에게 알리고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 17세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">만 14세 미만 아동의 개인정보에 대해 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.1 개인정보 수집·이용
인증기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 22세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체의 동의 없이 개인정보의 추가적인 이용 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 이용이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보 처리방침에 공개하고 이를 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.2 개인정보 수집 제한
인증기준	개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을 수집하여야 하며, 정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 않아야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보를 수집하는 경우 그 목적에 필요한 범위에서 최소한의 정보만을 수집하고 있는가?정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 있는가?정보주체가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 3.1. 개인정보 수집 시 보호조치

항목	3.1.3 주민등록번호 처리 제한
인증기준	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
주요 확인사항	<ul style="list-style-type: none">주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가?주민등록번호의 수집 근거가 되는 법조항을 구체적으로 식별하고 있는가?법적 근거에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.4 민감정보 및 고유식별정보의 처리 제한
인증기준	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도 동의를 받아야 한다.
주요 확인사항	<ul style="list-style-type: none">민감정보는 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가?고유식별정보(주민등록번호 제외)는 정보주체로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하고 있는가?재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알리고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.5 개인정보 간접수집
인증기준	정보주체 이외로부터 개인정보를 수집하거나 제3자로부터 제공받는 경우에는 업무에 필요한 최소한의 개인정보를 수집하거나 제공받아야 하며, 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보주체 이외의 제3자로부터 개인정보를 제공받는 경우 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통해 명시하고 있는가? • 공개된 매체 및 장소에서 개인정보를 수집하는 경우 정보주체의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하고 있는가? • 서비스 계약 이행을 위해 필요한 경우로서, 서비스 제공 과정에서 자동수집장치 등에 의해 수집·생성하는 개인정보의 경우에도 최소수집 원칙을 적용하고 있는가? • 정보주체 이외로부터 수집하는 개인정보에 대해 정보주체의 요구가 있는 경우 즉시 필요한 사항을 정보주체에게 알리고 있는가? • 정보주체 이외로부터 수집한 개인정보를 처리하는 경우 개인정보의 종류·규모 등이 법적 요건에 해당하는 경우 필요한 사항을 정보주체에게 알리고 있는가? • 정보주체에게 수집 출처에 대해 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.1. 개인정보 수집 시 보호조치

항목	3.1.6 영상정보처리기기 설치·운영
인증기준	고정형 영상정보처리기기를 공개된 장소에 설치·운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 경우 법적 허용 요건에 해당하는지를 검토하고 있는가? • 공공기관 등이 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하고 있는가? • 고정형 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가? • 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기를 운영하는 경우 법적 허용 요건에 해당하는지를 검토하고 있는가? • 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우 불빛, 소리, 안내판 등의 방법으로 촬영 사실을 표시하고 알리고 있는가? • 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는가? • 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 파기하고 있는가? • 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 계약서에 반영하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 3.1. 개인정보 수집 시 보호조치

항목	3.1.7 마케팅 목적의 개인정보 수집?이용
인증기준	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보 처리에 대한 동의를 받는 경우 정보주체가 이를 명확하게 인지할 수 있도록 알리고 별도 동의를 받고 있는가? • 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 경우 수신자의 명시적인 사전 동의를 받고 있으며, 2년마다 정기적으로 수신자의 수신동의 여부를 확인하고 있는가? • 전자적 전송매체를 이용한 영리목적의 광고성 정보 전송에 대해 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우 영리목적의 광고성 정보 전송을 중단하도록 하고 있는가? • 영리목적의 광고성 정보를 전송하는 경우 전송자의 명칭, 수신거부 방법 등을 구체적으로 밝히고 있으며, 야간 시간에는 전송하지 않도록 하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 3.2. 개인정보 보유 및 이용 시 보호조치

항목	3.2.1 개인정보 현황관리
인증기준	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하고 있는가?• 공공기관이 개인정보파일을 운용하거나 변경하는 경우 관련된 사항을 법률에서 정한 관계기관의 장에게 등록하고 있는가?• 공공기관은 개인정보파일의 보유 현황을 개인정보 처리방침에 공개하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.2. 개인정보 보유 및 이용 시 보호조치

항목	3.2.2 개인정보 품질보장
인증기준	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체에게 관리절차를 제공하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보를 최신의 상태로 정확하게 유지하기 위한 절차 및 방안을 수립·이행하고 있는가?정보주체가 본인의 개인정보에 대하여 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.2. 개인정보 보유 및 이용 시 보호조치

항목	3.2.3 이용자 단말기 접근 보호
인증기준	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받고 있는가?이동통신단말장치 내에서 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우, 정보주체(이용자)가 동의하지 않아도 서비스 제공을 거부하지 않도록 하고 있는가?이동통신단말장치 내에서 해당 접근권한에 대한 정보주체(이용자)의 동의 및 철회방법을 마련하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 3.2. 개인정보 보유 및 이용 시 보호조치

항목	3.2.4 개인정보 목적 외 이용 및 제공
인증기준	개인정보는 수집 시의 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 개인정보는 최초 수집 시 정보주체로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가?• 개인정보처리자로부터 개인정보를 제공받은 경우 제공받은 목적의 범위 내에서만 이용·제공하고 있는가?• 개인정보를 수집 목적 또는 개인정보처리자로부터 제공받은 목적의 범위를 초과하여 이용하거나 제공하는 경우 정보주체에게 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는가?• 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우 제공받는 자에게 이용목적?방법 등을 제한하거나 안전성 확보를 위해 필요한 조치를 마련하도록 요청하고 있는가?• 공공기관이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하고 있는가?• 공공기관 등이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하는 등 절차를 마련하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.2. 개인정보 보유 및 이용 시 보호조치

항목	3.2.5 가명정보 처리
인증기준	가명정보를 처리하는 경우 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 가명정보를 처리하는 경우 목적 제한, 가명처리 방법 및 기준, 적정성 검토, 재식별 금지 및 재식별 발생 시 조치사항 등 가명정보를 적정하게 처리하기 위한 절차를 수립하고 있는가? • 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이는 개인을 알아볼 수 없도록 적정한 수준으로 가명처리를 수행하고 있는가? • 다른 개인정보처리자와 가명정보를 결합하는 경우 결합전문기관 또는 데이터전문기관을 통해 결합하고 있는가? • 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리, 관련 기록의 작성·보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하고 있는가? • 가명정보 처리목적 등을 고려하여 가명정보의 처리 기간을 적정한 기간으로 정하고 있으며, 해당 기간이 경과한 경우 자체 없이 파기하고 있는가? • 개인정보를 익명처리하는 경우 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 특정 개인을 알아볼 수 없도록 적정한 수준으로 익명처리하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제4자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 사항을 명확하게 고지하고 다른 동의사항과 구분하여 적법하게 동의를 받고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제7자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보를 제3자에게 제공하는 경우 안전한 절차와 방법을 통해 제공하고 제공 내역을 기록하여 보관하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제6자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제9자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체의 동의 없이 개인정보의 추가적인 제공 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 제공이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보 처리방침에 공개하고 이를 점검하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보를 제3자에게 제공하는 경우 정보주체 동의, 법령상 의무준수 등 적법 요건을 명확히 식별하고 이를 준수하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제8자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.1 개인정보 제3자 제공
인증기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제5자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 명확히 표시하여 알아보기 쉽게 하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.2 개인정보 처리 업무 위탁
인증기준	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 공개하여야 한다. 또한 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는가?재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.3 영업의 양도 등에 따른 개인정보 이전
인증기준	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none"> • 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 필요한 사항을 사전에 정보주체에게 알리고 있는가? • 개인정보를 이전받는 자는 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실 등 필요한 사항을 정보주체에게 자체 없이 알리고 있는가? • 개인정보를 이전받는 자는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공하고 있는가?

| 증거 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.3. 개인정보 제공 시 보호조치

항목	3.3.4 개인정보 국외이전
인증기준	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보를 국외로 이전하는 경우 정보주체에게 국외 이전에 관한 고지 사항을 모두 알리고 별도 동의를 받거나, 인증 또는 인정 등 적법 요건을 준수하고 있는가?정보주체와의 계약의 체결 및 이행을 위한 개인정보의 국외 처리위탁·보관에 대해 정보주체에게 알리는 경우 필요한 사항을 모두 포함하여 적절한 방법으로 알리고 있는가?개인정보 보호 관련 법령 준수 및 개인정보 보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 있는가?개인정보를 국외로 이전하는 경우 개인정보 보호를 위해 필요한 조치를 취하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.4. 개인정보 파기 시 보호조치

항목	3.4.1 개인정보 파기
인증기준	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 개인정보의 보유기간 및 파기와 관련된 내부 정책을 수립하고 있는가?• 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하고 있는가?• 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하고 있는가?• 개인정보 파기에 대한 기록을 남기고 관리하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.4. 개인정보 파기 시 보호조치

항목	3.4.2 처리목적 달성 후 보유 시 조치
인증기준	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.
주요 확인사항	<ul style="list-style-type: none">개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우, 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하도록 관리하고 있는가?개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하고 있는가?분리 보관하고 있는 개인정보에 대하여 법령에서 정한 목적 범위 내에서만 처리 가능하도록 관리하고 있는가?분리 보관하고 있는 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.5. 정보주체 권리보호

항목	3.5.1 개인정보 처리방침 공개
인증기준	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 정보주체가 알기 쉽도록 개인정보 처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
주요 확인사항	<ul style="list-style-type: none">• 개인정보 처리방침에는 법령에서 요구하는 내용을 모두 포함하여 알기 쉬운 용어로 구체적이고 명확하게 작성하였는가?• 개인정보 처리방침을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하고 있는가?• 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 자체 없이 공지하고 정보주체가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1



| 3.5. 정보주체 권리보호

항목	3.5.2 정보주체 권리보장
인증기준	<p>정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 등 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 요구를 받은 경우 자체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.</p>
주요 확인사항	<ul style="list-style-type: none"> • 정보주체 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지 및 동의 철회 등(이하 '열람등요구'라 함)을 개인정보 수집방법·절차보다 어렵지 아니하도록 권리 행사 방법 및 절차를 마련하여 공개하고 있는가? • 정보주체 또는 그 대리인이 열람등요구를 하는 경우 규정된 기간 내에 열람등요구에 따른 필요한 조치를 하고 있는가? • 정보주체 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 자체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하고 있는가? • 정보주체의 열람등요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는가? • 정보통신망에서 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한 경우 침해를 받은 자가 정보통신서비스 제공자에게 정보의 삭제 요청 등을 할 수 있는 절차를 마련하여 시행하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1

| 3.5. 정보주체 권리보호

항목	3.5.3 정보주체에 대한 통지
인증기준	개인정보의 이용·제공 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.
주요 확인사항	<ul style="list-style-type: none">법적 의무 대상자에 해당하는 경우 개인정보 이용·제공 내역 또는 그 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 정보주체에게 주기적으로 통지하고 있는가?개인정보 이용·제공 내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?

| 증적 관리

Teiren 가이드 항목	증거 자료	운영 현황
1.1.1 Article	자료1	운영현황1