

ISO/IEC 27002:2022 개정판

전문가와 자세히 알아보기

ISO/IEC 27002 개요

1. ISO/IEC 27002의 정의

ISO/IEC 27002:2022 정보보안, 사이버보안 및 개인정보보호 - 정보보안통제는 조직의 정보 보안 표준에 대한 지침을 제공하고 정보 보안 관리를 위한 모범 사례를 제공합니다. 본 지침은 조직의 보안 통제 선택, 구현, 관리에 집중하며 비즈니스 고유의 정보 보안 위험 환경을 고려합니다.

2. ISO/IEC 27002가 전체 개정판인가요?

예, ISO/IEC 27002:2022는 표준의 전체 개정판이며, 2013년 버전을 업데이트합니다. ISO/IEC 27002:2022 발행 이후에는 2013년 버전은 철회됩니다.

3. ISO/IEC 27002:2022 개정판에서 변경된 내용은 무엇인가요?

개정된 ISO/IEC 27002:2022는 기존 통제를 재구성하여 보안 통제 수가 114개에서 93개로 감소했습니다. 또한 더 이상 모범 사례를 반영하지 않는 일부 통제를 제거하였습니다. ISO/IEC 27002 표준의 최신판에는 11개의 새로운 통제가 도입되었습니다. 새로운 통제는 위협 인텔리전스, 클라우드 서비스 사용을 위한 정보 보안, 데이터 유출 방지와 같은 측면을 포함합니다. 이를 통해 사이버 공격의 특성이 변화해도 기업은 정보 보안을 지속적으로 제어할 수 있습니다.

4. ISO/IEC 27002의 새로운 내용은 무엇인가요?

ISO/IEC 27002는 기업이 쉽게 채택할 수 있도록 검토하여 필요한 통제를 간과하지 않게 하는 것이 목표입니다. 본 표준은 기술, 조직, 인력, 물리적 통제의 4가지 영역을 사용합니다. 본 표준은 NIST 사이버보안 프레임워크(식별, 보호, 탐지, 대응, 복구 및 통상 기밀성/무결성/가용성) 등 보조 장치뿐 아니라, 탐지, 예방, 수정으로 이름 붙인 통제 유형을 사용합니다. 또한, 속성을 사용해 서로 다른 대상을 위해 다양한 관점에서 통제를 필터링, 정렬, 표시할 수 있습니다.

5. ISO/IEC 27002는 부속 지침서입니다. 우리 조직에서 취할 행동은 무엇인가요?

위험 평가와 필요한 통제를 검토하여 정보 보안, 클라우드 보안, 데이터 보안에 대한 모범 사례를 유지하고 새로운 지침과 일치하는지 확인할 것을 권장합니다. 그러면 미래의 위험을 극복하는 것이 좀 더 용이해집니다. 또한, 이 변경에 따라 ISO 27001에 대한 업데이트가 필요하므로 조직의 인증서 업그레이드를 준비하시기 바랍니다.

Inspiring trust for a more resilient world.

ISO/IEC 27002:2022가 조직에게 주는 이점

6. ISO/IEC 27002:2022가 내 조직에게 어떤 도움을 주나요?

- 정보보호시스템(ISMS)을 설정하는 과정에서 적절하고 알맞은 보안 통제를 식별할 수 있습니다
- ISMS의 모범 사례를 만들 수 있습니다
- 정보 보안과 관련된 법적 허용 및 규제, 규율, 계약적 요구 사항을 충족합니다
- 위험 관리를 강화하고 정보 보안 침해 가능성을 감소시킵니다
- 조직의 ISMS에 대한 신뢰를 높입니다
- ISMS을 전반적으로 견고하게 만들고 회복력을 높이며 위험 관리를 강화합니다
- 산업, 혁신, 기반 시설에 관한 유엔 지속가능발전목표 9에 기여합니다

ISO/IEC 27001:2013의 영향

7. ISO/IEC 27002 개정으로 ISO/IEC27001도 2022년에 변경되나요?

개정된 ISO/IEC 27002:2022에 대한 부록 A 통제 부분을 업데이트하고, 2014년과 2015년에 발표된 2개의 미미한 정정사항을 포함하기 위해 ISO/IEC 27001이 부분적으로 수정될 예정입니다. ISO/IEC 27001: 2022년은 2022년 2분기에 발표될 것으로 예상됩니다. 적절한 시기에 관련 절차를 안내해 드리겠습니다.

8. ISO/IEC 27001이 개정되면 어떤 영향이 있나요?

전환 평가가 필요하며, 고객의 범위, 사이트 수, 시스템, 각 조직의 복잡성에 따라 고객별 계획을 정의하여 통제 및 ISMS가 업데이트된 표준을 충족하는지 확인해야 합니다.

9. ISMS를 구현하고 있거나 ISO/IEC 27001 인증을 취득하려는 조직에 ISO/IEC 27002 개정이 의미하는 바는 무엇인가요?

조직이 ISO 27001을 구현하고 있거나 인증을 받을 준비가 되었는지와 관계없이 새 버전에서 제공하는 지침을 활용하여 조직이 가진 ISMS의 이점을 극대화하는 것이 중요합니다. ISO 27002:2022는 조직에 적합한 통제를 식별하고 구현하기 위한 참조 역할을 하게 될 것입니다.

Inspiring trust for a more resilient world.