목 차

1. 개요

본 보안 가이드라인은 기업의 정보보호를 강화하기 위한 목적으로 작성되었다. ISO/IEC 27001:2022을 기반으로 하며, 27002의 통제조건을 포함하고 있다. 추가로, 클라우드 서비스 환경에서의 보안과 개인정보 보호를 위해 27017과 27018 표준을 통합하였다.

기업의 정보보호 조직 구성부터 자산 관리, 인적 및 물리적 보안, 통신 및 운영 관리에 이르기까지 다양한 보안 영역에 대한 지침을 제공한다. 클라우드 환경에서의 보안 특성을 고려하여, 클라우드 서비스 선택부터 보안 조치까지의 가이드를 포함하고 있다.

특히, 클라우드 마 이그레이션의 전 과정을 위한 단기, 중기, 장기 보안 전략을 포괄적으로 작성하여, 마이그레이션의 각 단계에서 보안 요구사항을 세밀하게 고려하도록 하였다.

또한, 잠재적 위험에 대응하고 시스템을 복구하기 위한 프로세스도 강조하였다. 이 가이드라인을 통해 기업 기업은 정보보호를 체계적으로 접근하고, 지속적인 보안 강화 활동을 추진할 수 있다.

2. 조직 보안

본 조직 보안 섹션은 유통기업의 정보보호 정책 수립을 위한 핵심 요소들에 중점을 둔다. 조직 내에서의 보안 역할과 책임에 대한 명확한 정의, 권한 관리를 통한 접근 제어, 공급망 내에서의 정보보호 전략, 보안 사건에 대한 체계적인 증거 관리, 클라우드 환경에 적합한 보안 지침, 법률 및 표준에 대한 컴플라이언스 확보, 그리고 보안 사고 대응 방안이 포함된다. 이를 통해 조직은 정보보호에 관한 정책을 체계적으로 구성하고 실행할 수 있는 기반을 마련할 수 있다.

A. 보안 역할과 책임

기업 하이브리드 클라우드를 도입함에 있어, 상품 및 물류 데이터의 흐름과 저장이 복잡해질 것이다. 따라서 ISO/IEC 27001 표준에 따라, 정보보호 관리 시스템(ISMS)의 구축과 운영에 대한 전반적인 기준을 제시하고자 한다. 경영진은 정보보호 정책을 수립하며, 이 정책은 내부 시스템과 클라우드 환경 간의 상호 작용, 그리고 위험 관리를 포함해야 한다(ISO/IEC 27001:5.2, A.6.1.1).

기업의 직원 및 파트너들은 정보보호 역할 및 책임을 명확히 해야 한다. 데이터 액세스 권한을 부여하고 관리하는 방법, 직원 훈련, 물리적 보안, 백업 절차 등의 보안 통제 방안을 포함하며, 이는 하이브리드 클라우드의 복잡한 환경에서의 데이터 보호를 위한 핵심 기준이 된다(ISO/IEC 27002: A.6.1.2, A.7.2.2, A.11.1.4, A.12.3.1).

기업이 다양한 클라우드 서비스 제공자와 협력할 때, 클라우드 환경에서의 정보보호 책임을 명확히 구분하며, 클라우드 서비스 제공자와 고객 간의 책임을 분리한다. 이 표준은 클라우드 서비스 고객이 클라우드 환경에서 데이터를 안전하게 처리하기 위해 고려해야 할 보안 측면에 대한 지침을 제공한다(ISO/IEC 27017: 5.1, 6.3.1, 9.5.1).

보안 역할과 책임 설정에 있어 클라우드 환경에서 개인식별정보(PII)를 처리할 때의 보호 조치를 고려해야 한다. 이는 데이터의 유출 방지, PII의 저장 및 전송에 대한 보안 조치, 그리고 클라우드 서비스 제공자의 고객에 대한 개인정보 접근 권한 관리 등을 포함한다(ISO/IEC 27018: A.6.2, A.8.2, A.9.2).

이에 따른 정책적 예시는 다음과 같다.

데이터 권한 이동 및 임시 허용		
정책조항	세부이행항목	이행지침
데이터 이동 절차 (ISO 27001 - A.12.3, ISO 27002 - 13.2, ISO 27017 - 13.2)	데이터 이동 계획	CSP 의 Compute Engine 인스턴스나 Persistent Disks 에서 데이터를 이동하기 전에 어떤 데이터를 어디로, 언제, 어떻게 이동할지에 대한 계획을 세워야 한다.
	통제	Cloud IAM (Identity and Access Management)을 사용하여 이동할 데이터에 대한 접근 권한을 설정한다. 예를 들어, 특정 프로젝트의 개발자는 데이터 이동을 위해 임시로 compute.instanceViewer 또는 compute.diskViewer 역할을 부여받을 수 있다.
	이동 확인	데이터 이동이 완료된 후, Cloud Monitoring 과 Cloud Logging 을 사용하여 데이터 이동 로그를 확인하고, 원하는 대로 데이터가 이동되었는지 검증한다.

임시 권한 부여 절차 (ISO 27001 - A.9.2, ISO 27002 - 9.2.6, ISO 27017 - 9.1)	임시 권한 요청	요청자는 필요한 권한과 사용 기간, 권한이 필요한 이유를 문서화하여 보안 팀에 제출한다.
	승인 및 부여	보안 팀은 요청을 검토 후, Cloud IAM 에서 요청자에게 임시 권한을 부여한다.
	임시 권한 해제	부여된 권한의 사용 기간이 끝나면, 자동화 도구나 수동 절차를 통해 해당 권한을 해제한다.

교육 프로세스 (ISO 27002 - 7.2, ISO 27018 - 7.2)	
교육 주제	교육 개요
CSP 기본 교육	교육 대상: 모든 클라우드 사용자 내용: CSP 콘솔 사용법, 기본 서비스 소개, IAM 사용법, 기본적인 보안 원칙 등 자료: CSP 공식 문서, 동영상, 퀴즈
하이브리드 클라우드 보안 교육	교육 대상: 클라우드 관련 업무를 수행하는 팀 내용: 하이브리드 클라우드의 구조, 데이터 이동 시 주의점, CSP 에서의 보안 사례 및 활용 방법 등 자료: 사례 기반의 문서, 시뮬레이션, 팀별 워크샵
보안 인식 교육	교육 대상: 전 직원 내용: 최근의 보안 사건, CSP 환경에서의 주요 위협, 보안 인식 향상을 위한 실용적인 팁 등 자료: 보안 뉴스, 보안 사건 분석 리포트, 퀴즈 및 시뮬레이션 게임

B. 정보 관리

하이브리드 클라우드를 도입한 기업 유통 기업의 정보 관리는 복잡한 환경에서 중요한 정보를 안전하게 보호하고 관리하는 것이 중요하다. ISO/IEC 27002 기준에 따라 정보는 그 중요도와 민감도에 따라 명확하게 분류되어야 한다(ISO/IEC 27002: 5.12). 이 분류된 정보는 라벨링을 통해 분류 수준이 명확하게 표시되어야 한다(ISO/IEC 27002: 5.13). 특히 정보의 안전한 전송은 암호화와 같은 보안 기술을 활용하여 진행되어야 한다(ISO/IEC 27002: 5.14).

클라우드 환경, 특히 하이브리드 클라우드에서는 클라우드 서비스 제공자와의 계약에 정보 보호 요구사항이 포함되어야 한다(ISO/IEC 27002: 5.23, ISO/IEC 27017: 6.3.1). 데이터의 소유, 위치, 백업, 복구 및 삭제에 관한 명확한 절차와 책임이 정해져야 한다(ISO/IEC 27002: 5.23, ISO/IEC 27017: 6.3.2). 또한 사용자 인증 정보는 안전하게

보호되어야 한다(ISO/IEC 27002: 5.17). 지적 재산권과 관련된 정보도 적절한 보안 조치를 적용하여 관리되어야 한다(ISO/IEC 27002: 5.32).

특히, 개인식별정보는 ISO/IEC 27018의 가이드라인을 따라 특별한 보호 조치를 받아야 한다(ISO/IEC 27002: 5.34, ISO/IEC 27018: 6.1.1). 이러한 데이터의 수집, 저장, 처리, 전송 및 삭제 절차는 명확해야 한다. 정보 보안의 효과성을 보장하기 위해서는 독립적인 보안 검토가 정기적으로 수행되어야 한다(ISO/IEC 27002: 5.35). 모든 이해관계자가 정보 보안에 관한 정책, 규칙 및 표준을 이해하고 준수하도록 지속적인 교육이 필요하다(ISO/IEC 27002: 5.36).

이에 따른 정책적 예시는 다음과 같다.

정책조항	정책 소개	이행지침
정보 분류 및 라벨링 (ISO 27002 - 8.2)	모든 정보는 생성 시 공개/내부용/민감/기밀 중 하나로 분류해야 한다.	공개: 회사 브로셔, 홍보 자료. 내부용: 내부 연차 보고서, 기사 경로 정보. 민감: 수탁사 정보, 제품 정보, 현재 상태정보. 기밀: 내부 직원 정보, 사용자 정보, 계약서.
사용자 인증 정보 관리 (ISO 27002 - 9.2, ISO 27017 - 9.2)	사용자의 인증 정보는 정기적으로 변경되어야 하며, 복잡한 패턴을 준수해야 한다.	CSP 의 IAM 과 Cloud IAP 를 사용하여 사용자 접근 제어와 인증을 강화한다.
개인 정보 보호 (ISO 27018 - 5.1)	모든 개인 정보, 특히 기사 및 내부 직원의 정보는 ISO 27018 및 관련 규정을 준수하여 처리해야 한다.	고객, 수탁사, 기사 및 내부 직원의 정보에 대한 접근 권한을 제한한다. 데이터를 CSP 에 저장하기 전에 개인식별정보(PII)를 암호화하거나 익명화하여 보호한다.
상태정보 및 물류 데이터 관리 (ISO 27017 - 12.1)	상태정보 및 데이터는 적절한 보안 수준을 유지하여 처리해야 한다.	CSP 의 스토리지 및 네트워크 솔루션을 사용하여 데이터의 무결성과 가용성을 보장한다. 데이터의 변경, 이동, 삭제에 대한 로그를 지속적으로 모니터링하고 저장한다.

C. 공급망 관리

조직의 공급망 관리는 정보 보안에 있어 중요한 부분을 차지하며, 복잡한 정보 환경에서의 신뢰와 안정성을 확보하는 핵심적인 역할을 한다.

ISO/IEC 27002의 5.19 항목에 따라, 공급업체와의 관계에서 정보 보안을 관리하기 위해서는 초기 계약 체결 단계부터 서비스 제공이 종료될 때까지 모든 단계에서의 보안을 고려해야 한다. 공급업체와의 계약에는 정보 보안 요구사항이 포함되어야 하며, 특히 공급업체가 제공하는 ICT 서비스와 관련된 보안 위험을 고려하여 관리 계획을 세워야 한다(ISO/IEC 27002: 5.20, 5.21).

이와 더불어, 공급업체로부터 제공받는 서비스의 모니터링, 검토 및 변경 관리는 지속적으로 수행되어야 한다. 이는 서비스 수준 합의(SLA)의 일환으로 이루어질 수 있으며, 서비스 제공 중 발생하는 모든 보안 이슈에 대한 적시 대응과 해결을 위한 프로세스가 포함되어야 한다(ISO/IEC 27002: 5.22).

기업의 공급망에서 정보 보안은 핵심적이다. ISO/IEC 27002 기준에 따라, 공급업체와의 계약은 보안 요구사항을 명확히 명시해야 하며, ICT 공급망 내 데이터의 이동과 보관을 철저히 관리해야 한다. 계약상의 정보 보안 조치, 데이터 처리 방법, 종료 시의 데이터 반환 또는 파기 절차 등이 중요하며, 공급업체 서비스의 보안 상태는 지속적으로 모니터링되어야 한다. 특히, 클라우드 환경에서는 ISO/IEC 27017과 27018의 지침에 따라 데이터 위치, 책임 분배 및 개인식별정보의 보호가 강조되어야 한다. 기업은 이러한 세부 항목을 바탕으로 공급망의 정보 보안을 강화해야 한다. (ISO/IEC 27017: 6.4.1, ISO/IEC 27018: 6.2.1).

이에 따른 정책적 예시는 다음과 같다.

공급망 정보 보안		
고려 항목	세부 항목	이행지침
계약 체결 (ISO27002 6.2.1, ISO27001 A.15.1.1)	보안 요구사항 포함	모든 공급업체와의 계약서에는 정보 보안 요구사항이 포함되어야 한다. 이는 데이터 처리, 보관, 이동, 접근 권한 관리 및 기타 보안 관련 항목을 포함한다.
	ICT 서비스의 보안 리스크 평가	공급업체가 제공하는 ICT 서비스에 대한 보안 위험을 평가하고, 필요한 경우 추가적인 보안 요구사항을 계약에 포함시켜야 한다.
		CSP IaaS 를 사용하여 데이터를 이동 및 보관할

데이터 관리 (ISO27002 8.2.3, ISO27002 8.3.2)	데이터 이동 및 보관	때, 암호화, IAM 정책, VPC 피어링 등 CSP 의 보안 기능을 적극 활용하며, 보안 규정에 따라 관리해야 한다.
	데이터 종료 시 절차	계약 종료 시 공급업체로부터 반환받아야 하는 데이터와 파기해야 하는 데이터에 대한 정책 및 절차를 마련하고 이행해야 한다.
서비스 모니터링 및 변경 관리 (ISO27002 12.4.1, ISO27002 6.1.3)	SLA 관리	서비스 수준 합의에 따라 공급업체 서비스의 성능 및 보안 상태를 지속적으로 모니터링해야 한다. SLA 위반 시 책임 및 대응 조치에 대해 명시해야 한다.
	보안 이슈 대응	CSP IaaS 환경에서 발생하는 보안 이슈에 대한 대응 프로세스를 마련하고, 공급업체와 협력하여 적시에 해결하는 방안을 강구해야 한다.
하이브리드 클라우드 환경에서의 보안 강화 (ISO/IEC 27017 6.3.1, ISO/IEC 27018 5.5.1, ISO/IEC 27018 5.3.1)	데이터 위치 및 책임 분배	ISO/IEC 27017 및 27018 에 따라 클라우드 환경에서의 데이터 위치와 책임 분배를 명확히 해야 한다.
	개인 식별 정보 보호	ISO/IEC 27018 에 따라 클라우드 환경에서 처리되는 개인식별정보의 보호를 강화해야 한다.
지속적 교육 및 인증 (ISO27002 7.2.2, ISO27001 A.18.1.3)	보안 교육	공급업체 및 내부 직원 대상으로 CSP IaaS 와 하이브리드 클라우드의 보안 교육을 지속적으로 실시해야 한다.
	보안 인증	공급업체 및 기업 의 서비스가 ISO/IEC 27K 시리즈와 같은 국제 표준에 부합하는지 지속적으로 검증하고 인증을 갱신해야 한다.

SLA 세부 내용		
고려 항목	세부 항목	세부 내용
서비스 가용성 및 성능 (ISO27002 12.1.3)	가용성	CSP IaaS 서비스는 99.9%의 연간 가용성을 목표로 한다. 예를 들면, 한 달 동안 서비스는 최대 43 분 동안 중단될 수 있다.
	응답 시간	웹페이지나 애플리케이션 로딩은 3 초 이내로, 실제 기업 의 테스트 환경에서는 평균 1.5 초 내외로 응답하는 것을 확인하였다.
보안 및 개인정보		CSP IaaS 에서 처리하는 모든 데이터는 전송 및

보호 (ISO27002 10.1.1, ISO27017 9.5.1, ISO27018 9.4, ISO27002 9.1.2, ISO27017 9.1.3, ISO27018 9.2)	데이터 보호	저장 시 암호화된다. 예로, 기업 회사 데이터는 AES-256 암호화 알고리즘을 사용하여 보호된다.
	접근 제어	기업 의 개발팀은 read-only 권한만 부여받아, 실제로 데이터 변경이나 삭제는 할 수 없다.
	개인정보 보호	CSP IaaS 에서 처리하는 고객의 주소나 전화번호와 같은 개인 정보는 별도의 보안 레이어로 보호된다.
보안 인사이던트 및 대응 (ISO27002 16.1.2, ISO27002 16.1.6)	인사이던트 알림	보안 사건 발생 시, 기업 의 보안 담당자에게 2 시간 이내로 알려야 한다. 예를 들어, 데이터 유출 사건이 발생하면, 이를 2 시간 내에 이메일과 전화로 통보받는다.
	인사이던트 대응 및 복구	사건 발생 후 4 시간 이내에 대응 조치를 시작하며, 예를 들면, 데이터 유출을 차단하고, 유출된 데이터의 범위를 조사한다.
서비스 검토 및 개선 (ISO27002 12.7, ISO27002 12.1.2)	성능 및 보안 검토	매 분기별로 CSP IaaS 성능과 보안 상태를 검토한다. 이 검토에서는 지난 3 개월 동안의 서비스 다운타임, 응답 시간, 보안 사건 등이 포함된다.
	서비스 업데이트 및 변경 관리	기업 에게는 서비스 변경이 예정된 경우 최소 1 주일 전에 알림이 갑니다. 이를 통해 기업 은 준비를 하거나 필요한 조치를 취할 수 있다.
보상 및 패널티 (ISO27002 18.1.3)		만약 SLA 항목을 지키지 못할 경우, 서비스 비용의 10%를 다음 달 청구서에서 할인해준다. 예를 들어, 가용성이 한 달 동안 99%로 떨어진 경우, 기업 은 다음 달 청구서에서 10%의 할인을 받게 된다.

D. 사고 관리

기업이 정보 보안 사건에 효과적으로 대응하기 위해서는 먼저 사건 발생 가능성을 고려한 다양한 시나리오를 준비하고 이를 꾸준히 업데이트하는 것이 중요하다. 또한, 사건 대응을 위한 전용 팀을 구성하고 이 팀이 사용할 도구와 자원, 그리고 정확한 대응 절차를 미리 계획해야 한다(ISO/IEC 27002: 5.24). 그리고, 모든 이벤트가 사건은 아니므로, 보안 이벤트 발생 시 중요도, 영향 범위 등을 신속하게 평가하여 그 심각성을 파악하고, 이를 바탕으로 대응 조치를 결정하는 것이 필요하다(ISO/IEC 27002: 5.25).

사건이 확인되면 즉각적인 대응은 매우 중요하다. 사건의 확산을 방지하고 원인을 찾아 수정 조치를 취하는 것이 필요하며, 필요한 경우, 외부 전문가나 기관과 협력하여 대응할 수도 있다(ISO/IEC 27002: 5.26). 사건 발생 후에는 깊은 분석을 통해 재발을 방지하는 전략을 마련해야 한다. 이 과정에서 사건 발생의 근본 원인뿐만 아니라 대응 과정에서의 문제점도 함께 분석하는 것이 중요하다(ISO/IEC 27002: 5.27). 또한, 법적인 문제나 보안 사건의 근본 원인을 파악하기 위해 관련된 모든 정보와 데이터를 체계적으로 수집하고 보관해야 한다. 데이터의 무결성을 보장하기 위한 특별한 절차나 도구를 사용할 수도 있다(ISO/IEC 27002: 5.28).

클라우드 환경에 대한 추가적인 보안 조치는 ISO/IEC 27017과 ISO/IEC 27018의 권고사항을 참조하면 된다. 클라우드에서의 데이터 보호, 사건 대응 및 개인식별정보와 관련된 사건 처리에 대한 세부적인 지침이 포함되어 있어, 클라우드 환경에서의 보안 조치를 더욱 효과적으로 수행할 수 있다.

기업은 이러한 가이드라인을 따라 사건 관리 전략을 발전시켜, 정보 자산을 효과적으로 보호하고, 사건에 빠르게 대응하는 체계를 구축해야 한다.

사고 관리 프로세스	
정책 항목	이행 지침
사건 대응 시나리오 준비 (ISO27002 16.1.5)	기업 은 정보 보안 사건, 데이터 유출, 물리적인 보안 사건(예: 냉장고 도난) 등 다양한 시나리오를 준비하고 검토한다. 이를 통해 정기적으로 직원 교육과 모의 훈련을 실시한다.
사건 대응 전용 팀 구성 (ISO27002 6.1.3)	기업 의 '보안 대응 전담팀'은 IT 보안 전문가, 물리적 보안 전문가, 그리고 유통 경영 전문가로 구성된다. 이 팀은 정보 보안과 물리적 보안의 최신 동향 및 대응 방안에 대한 연속적인 교육을 받는다.
사건 평가 및 심각성 파악	실시간 모니터링 시스템을 통해 네트워크 침입, 데이터 유출, 물리적 보안 위반 등의 사건을 감지하고 평가한다. 이 시스템은 위협의 종류와

(ISO27001 A.12.4, ISO27002 13.1.2)	수준을 바탕으로 사건의 심각성을 자동으로 파악한다.
즉각적인 대응 및 협력 (ISO27001 A.16.1, ISO27002 16.1.1)	보안 사건 발생 시, 기업 은 내부 대응팀과 함께 외부 보안 전문가나 정보 보안 관련 기관과의 협력을 통해 신속하게 대응한다. 또한, 기업 과 협력 업체 간의 보안 정보 공유 및 협력 프로토콜을 구축하여 보다 효과적인 대응이 가능하도록 한다.
사건 후 분석 및 재발 방지 전략 (ISO27002 16.1.7, ISO27017 11.2)	보안 전담팀은 사건 발생 후 원인 분석과 함께 대응 과정에서의 문제점을 상세히 분석한다. 이를 바탕으로 기술적, 인적, 제도적 측면에서의 재발 방지 전략을 수립하고 이를 실행한다.
기업 과 협력 업체 간의 보안 정보 공유 및 협력 프로토콜 구축: 추가 고려사항	
고려 항목	항목 설명
데이터 분류 및 접근 권한 (ISO27001 A.8.2, ISO27002 8.2.2, ISO27017 9.5, ISO27018 9.4)	보안 정보를 공유할 때, 해당 정보의 민감도 및 중요도를 분류하고, 접근 권한을 적절히 설정해야 한다. 모든 정보가 모든 협력 업체와 공유될 필요는 없으므로, 업체별로 어떤 정보에 접근할 수 있는지를 미리 정의해야 한다.
암호화 및 안전한 전송 (ISO27001 A.10.1, ISO27002 10.1.1, ISO27017 10.1, ISO27018 10.1)	중요한 보안 정보를 전송할 때는 데이터를 암호화하고 안전한 채널을 통해 전송해야 한다. 이로 인해 데이터가 중간에 노출되거나 탈취당하는 위험을 최소화할 수 있다.
응답 시간 및 대응 방안 동기화 (ISO27001 A.16.1, ISO27002 16.1.4, ISO27017 11.3)	보안 사건 발생 시 빠른 대응이 중요하므로, 기업 과 협력 업체 사이의 응답 시간을 명확히 하고, 대응 방안을 동기화하는 것이 필요하다.
계약 및 법률적 측면 검토 (ISO27001 A.18.1, ISO27002 18.1.3, ISO27017 15.1, ISO27018 14.2)	보안 정보 공유 및 협력 프로토콜은 법률적인 측면도 고려해야 한다. 정보 보호 및 개인정보 처리 관련 법률, 규정을 준수하면서 프로토콜을 구축하는 것이 중요하다.
프로토콜 검토 및 업데이트 (ISO27001 A.16.1, ISO27002 16.1.6)	보안 환경은 지속적으로 변화하므로, 구축된 프로토콜도 정기적으로 검토하고 필요한 경우 업데이트 해야 한다. 이를 위해 기업 과 협력 업체는 연간 또는 반기별로 보안 회의를 개최하여 현재의 프로토콜 상태와 개선 사항을 논의해야 한다.

E. 클라우드 지침

클라우드 환경에서 정보 보안을 유지하기 위해 기업은 몇 가지 핵심 지침을 고려해야 한다. ISO/IEC 27002는 정보 보안의 일반적인 기준을 제공한다. 클라우드 서비스를 선택하고 구성할 때, 정보 보안 관리를 위한 프레임워크를 확립하는 것이 중요하다. 이를 위해서는 정보 분류, 접근 제어, 암호화, 물리적 및 환경 보안, 그리고 교육 및 인식 프로그램과 같은 다양한 통제 방안들을 포함해야 한다.

클라우드 서비스는 추가로 특별한 고려사항을 필요로 한다. ISO/IEC 27017은 클라우드 환경에서의 정보 보안 통제에 관한 추가 지침을 제공한다. 특히 클라우드 서비스 공급자와의 관계에서 중요한 부분은 서비스 수준 계약(SLA)이다. SLA는 데이터 위치, 백업 및 복구, 서비스 가용성 및 데이터 무결성에 관한 세부사항을 포함해야 한다. 또한, 클라우드의 다중 계층 구조를 고려하여, 각 계층에서의 보안 책임 분배를 명확하게 하는 것이 중요하다.

클라우드 환경에 대한 추가 보안 조치	
추가 보안 항목	항목 설명
데이터 암호화 (ISO/IEC 27017 12.1.1)	기업은 과정에서 수집되는 민감한 정보(온도 데이터, 운송 경로, 고객 주문 정보 등)를 안전하게 보관하기 위해 클라우드에 저장될 때 end-to-end 암호화를 실시한다. 이를 위해 CSP 의 KMS 서비스를 활용하며, 외부와의 데이터 교류 시 HTTPS 를 기반으로 한 암호화 전송을 지향한다.
다중인증 (ISO/IEC 27017 9.2.3)	기업 직원 및 협력 업체는 물류 관리 시스템에 접근할 때 일반적인 로그인 정보 외에도 휴대전화 문자 메시지를 통한 OTP 를 입력하여야 한다. 이를 통해 무단 접근을 효과적으로 방지한다.
접근 제한 (ISO/IEC 27017 9.1.2)	기업 의 물류 및 주문 관리 팀만이 고객 주문 데이터와 관련된 클라우드 자원에 접근 권한을 가진다. 반면, 품질 관리 팀은 관련 데이터에만 접근할 수 있도록 설정되어 있다. CSP 의 IAM 기능을 활용해 이러한 권한 설정을 세분화하고 관리한다.
로그 및 감사 (ISO/IEC 27017 12.4.3)	모든 과정에서의 데이터 변경, 업데이트, 조회 로그는 CSP 의 로그 관리 시스템을 통해 저장된다. 이 로그는 품질 보증 및 재발 방지를 위한 내부 감사 시에 활용된다.
개인식별정보 보호 (ISO/IEC 27018 9.2.3)	기업 은 고객의 주문 및 배송 주소와 같은 개인정보를 별도의 보안 클라우드 스토리지에 저장한다. 해당 정보는 오직 주문 처리 및 배송 목적으로만 활용되며, 개인정보 접근 권한은 엄격하게 제한된다. 이 방식은

	ISO/IEC 27018 의 권고사항에 따라 관리된다.

3. 인적 보안

본 인적 보안 섹션은 기업 내 직원 및 관련 이해당사자들의 정보 보안 의무와 책임을 중심으로 설계되었다. 기업의 직원 및 관련자들은 정보 보안에 대한 책임감을 가져야 하며, 그러한 책임감은 고용 전부터 시작되어 고용 후까지 지속된다. 이 가이드라인은 각 고용 단계별로 필요한 보안 고려사항 및 요구사항을 제시한다.

직원 및 관계자 고용 전, 후보자의 적합성을 평가하는 초기 단계에서, 그들의 전력과 신뢰도를 검증하는 것이 중요하다. 이 검증은 후보자의 과거 경력, 교육 및 기타 관련 배경 정보를 통해 이루어지며, 관련 법률과 규정, 그리고 조직의 윤리 기준을 고려해야 한다. 특히 접근될 정보의 민감도와 잠재적 위험성에 따라 검증의 깊이와 범위를 조절해야 한다. 클라우드 기반의 환경에서 작업하는 기업의 경우, ISO 27017 및 ISO 27018 표준에 따라 후보자의 클라우드 서비스 경험 및 교육을 검토하는 것도 필요하게 된다.

직원이 조직에 합류한 후에도 정보 보안은 중요한 이슈이다. 계약서에는 직원의 정보 보안에 대한 책임이 명확히 명시되어야 하며, 이를 위반할 경우 취할 조치도 정의되어야 한다. 또한 모든 직원은 조직의 정보 보안 정책과 절차, 그리고 실제 보안 위반 사례에 대한 교육을 받아야 한다. 보안 위반 시 취할 조치에 대한 징계 절차는 투명하게 공개되어야 하며, 모든 직원에게 알려져 있어야 한다. 기밀 정보 보호를 위해, 직원들은 정보 보안에 대한 기밀성 협약서에 서명해야 한다. 또한, 직원들이 원격으로 작업하는 경우 특별한 보안 지침이 제공되어야 한다. 모든 직원들은 보안 사건이 발생했을 때 신속히 보고하는 절차와 이를 위한 채널에 대해 알고 있어야 한다.

직원의 퇴직, 관계자와의 계약 종료 후에도 그들에 대한 정보 보안 책임은 계속된다. 퇴직 시에는 보안 관련 절차와 직원의 계속되는 책임에 대해 명확하게 전달해야 한다.

인력 고용 시 고려사항		
고용 단계	고려사항	세부 이행 사항
고용 전 (ISO/IEC 27002: 7.2.2, ISO/IEC 27002: 7.1.1, ISO/IEC 27017: 6.3.1)	스크리닝	후보자의 배경을 철저하게 검증한다. 특히, 이전 직장에서의 관리나 관련 경험 및 이력을 확인한다.
	고용조건	직원의 정보 보안 책임을 계약에 명시한다. 예를 들어, IaaS 클라우드 환경에서의 데이터 보안을 강조해야 한다.
고용 중 (ISO/IEC 27002: 7.2.2, ISO/IEC	정보 보안 교육	데이터의 중요성, 클라우드 환경에서의 보안 프로토콜 등에 대한 교육을 주기적으로 진행한다.
	징계 절차	데이터 누출이나 보안 위반 시 징계 절차를 명시하며, 특히

27002: 7.3.1, ISO/IEC 27002: 13.2.4, ISO/IEC 27002: 6.2.2, ISO/IEC 27002: 16.1.1, ISO/IEC 27002: 16.1.2, ISO/IEC 27017: 11.1.4)		클라우드 환경에서의 위반에 대한 세부 절차를 강화한다.
	기밀성 협약	직원들과 기밀성 협약을 체결하며, 협약 내용에는 클라우드 환경의 데이터 보안에 대한 내용을 포함해야 한다.
	원격 근무	클라우드 접속 시 VPN 사용하며, 멀티 팩터 인증 활성화 등의 보안 절차를 도입한다.
	보안 사건 보고	클라우드 데이터 무단 접근이 감지된 경우 직원들은 1 시간 이내에 보안팀에게 신속하게 보고해야하며, 세부 보안 사건 발생 시마다의 보고 메커니즘 도입한다. 클라우드 환경에서의 사건에 대한 별도의 보고 채널 구축하는 것을 권고한다
고용 후 (ISO/IEC 27002: 9.2.3, ISO/IEC 27017: 9.2.3)	책임	퇴직한 직원의 클라우드 접근 권한을 즉시 해제한다. 이전 직원의 정보 보안 책임은 퇴직 후에도 계속됨을 알린다.

4. 물리 보안

회사는 정보와 자산을 보호하는 것이 매우 중요하다. 이 보호는 단순히 디지털 정보만을 대상으로 한 것이 아니다. 온도에 민감한 상품, 예를 들면 식품이나 의약품과 같은 제품들은 무단 접근, 훼손, 손실 또는 도난의 위험에 직면하고 있기에, 중요한 자산을 보호하기 위해 적절한 물리적 보안 조치가 필요하며, 이를 위해 ISO27001 표준에 따라 보안 가이드라인을 작성하였다.

시설의 중요한 부분, 특히 냉동고나 창고와 같은 중요한 자원 주변에는 격리되고 보안 경계가 구축되어야 한다. 이 경계를 넘어서는 모든 접근은 통제되어야 하며, 이를 위해 RFID 카드 같은 인증 방식을 사용하여 인증된 사용자만이 해당 구역에 접근할 수 있도록 해야 한다. 또한, 보안을 위한 모니터링도 필수적이다. 실시간 모니터링 데이터를 효과적으로 수집하고 관리하기 위해 클라우드 통합 모니터링 솔루션을 도입하는 것이 바람직하다. 예를 들어, 보안 카메라를 설치하여 창고나 냉동고의 상황을 실시간으로 확인하고, 이 정보를 클라우드 서비스와 연동하여 필요한 경우 언제든지 원격으로도 접근할 수 있게 하는 것을 권고한다.

환경적 위험 요소도 고려되어야 한다. 예를 들어 창고 내의 전력 공급 중단이 발생했을 때, 백업 발전기를 자동으로 가동시켜 냉동고나 다른 중요한 시설의 전력 공급을 지속적으로 유지하는 것이 중요하다. 또한, 물 새김이나 화재 같은 위험 상황을 대비하여 적절한 탐지 시스템과 대응 계획을 마련하는 것도 필요하다.

화물트럭, 운송수단 및 저장고에 설치된 데이터 전송, 저장 및 처리 기기는 안전하게 관리되고 보호되어야 한다. 이러한 장비는 물리적으로 안전한 위치에 배치되며, 추가적인 물리적 보호 장치를 포함해야 한다.

물리보안 이행지침		
영역	세부 항목	이행 지침
출입통제 (ISO27001 A.11.1.5, ISO27001 A.11.1.2)	물리적 보안 경계	중요 시설 주변에는 격리 및 보안 경계가 필요하다. 창고 입구에는 보안 표지판과 바리케이드를 설치하여 무단 접근을 방지한다.
	물리적 출입	허가받은 사용자만이 보안 경계 내부로 접근해야 한다. 기사와 직원에게 RFID 카드를 제공하여 인증된 사용자만 창고에 접근할 수 있도록 한다.
물리적 분리	물리적 보안	클라우드 통합 모니터링 솔루션을 도입하여 중앙에서

및 보니터링 (ISO27001 A.11.2.1, ISO27001 A.11.1.4)	모니터링	모니터링 데이터를 관리한다. 보안 카메라의 실시간 영상을 클라우드 서비스에 연동하여 원격으로도 확인할 수 있게 한다.
	물리적 및 환경적 위협에 대한 보호	빠른 대응이 가능하도록 백업 발전기와 물 새김 탐지 시스템 등을 준비한다. 창고의 전력 공급이 중단될 경우, 백업 발전기가 자동으로 작동하여 냉동고의 전력을 지속적으로 공급하도록 설정한다.
장비 및 이동 수단 내 데이터 기기 보안 (ISO27001 A.11.1.3, ISO27001 A.11.2.6)		
	저장고	저장고 내부에 설치된 데이터 전송 및 저장 장치는 도난 방지를 위해 바닥에나 벽에 고정된다. 장치 주변에는 보안 잠금 장치나 보안 울타리가 설치되어 무단 접근을 방지한다. 추가적으로, 장비의 물리적 보호를 위해 감시 카메라나 물리적 방어 장벽이 설치될 수 있다.
	기타 기기	무선 데이터 전송 장치나 기타 휴대 가능한 기기는 강화 플라스틱 또는 금속 케이스로 보호받아야 한다. 장치의 고정 및 잠금 장치는 무단 접근 및 제거를 방지하기 위해 필요하다. 장치가 움직이거나 이동될 경우, 센서가 반응하여 경보가 울리도록 설정될 수 있다.

5. 기술적 보안

기술적 보안은 정보 자산의 무결성, 기밀성, 가용성을 보장하는 데 필수적이다. 시대가 발전함에 따라 새로운 위협이 지속적으로 등장하고 있기 때문에 이러한 위협을 예방하고 대응하기 위한 체계적인 접근 방식이 필요하다. 본 가이드라인은 국제 표준인 ISO 27002, 27017, 27018의 권장 사항을 바탕으로 구축되☝으며, 조직의 IT 환경에서의 다양한 위협에 대응하는 방법을 제시한다.

기술적 보안은 모든 조직에 있어 핵심적인 요소로, 정보의 무결성, 기밀성, 및 가용성을 보장하는 역할을 한다. 사용자 장치의 보안 설정, 특힌 보안 패치 및 업데이트, 비밀번호 정책, 화면 잠금 등의 보안 관련 조치가 필수적이다. 그리고 관리자나 특권을 갖는 사용자의 접근 권한은 신중하게 관리되어야 하며, 해당 권한의 사용은 로깅되어야 한다.

데이터 접근은 업무에 근거하여 제한되며, 이러한 제한은 안전한 인증, 다중 인증 방식을 통해 강화될 수 있다. 소스 코드 역시 중요한 자산이기 때문에, 저장소 보안 및 안전한 코딩 원칙을 준수하여 SQL 인젝션과 같은 공격으로부터 보호해야 한다. 외부 개발된 소프트웨어나 서비스는 내부 보안 표준에 따라 검토 및 수정된 후 사용되어야 한다.

데이터 관리 측면에서는 민감한 정보는 마스킹 되어야 하며, 데이터 유출 방지 솔루션을 도입하여 외부로의 무단 전송을 차단해야 한다. 중요 정보는 암호화된 상태로 정기적으로 백업되며, 이 백업된 데이터의 복원 가능성은 정기적으로 테스트되어야 한다.

시스템의 모든 활동은 로깅되어 보안 사건에 대한 조사와 분석이 가능하도록 해야 하며, 실시간 모니터링 도구를 통해 시스템 활동을 지속적으로 감시한다. 네트워크 보안에 있어서는 조직의 내부 네트워크를 방화벽, 침입 탐지 및 예방 시스템, VPN 등을 활용하여 외부 위협으로부터 보호하는 것이 중요하다. 또한, 민감한 정보를 다루는 네트워크 영역은 다른 네트워크로부터 분리하여 추가적인 보안을 제공한다.

기술적 보안 이행지침		
영역	세부 항목	이행 지침
인증관리 (ISO27002 6.2.1, ISO27001 A.9.2.2, ISO27001 A.9.1.2, ISO27002 9.4.2)	사용자 엔드포인트	기업 직원의 모든 디바이스에 MDM (Mobile Device Management) 솔루션을 도입하여 원격으로 보안 정책을 강제하고 장치를 관리한다.
	특권 접근 권한	관리자 권한은 최소한의 직원만이 받을 수 있으며, 권한 부여에 앞서 내부 승인 프로세스를 통과해야 한다.

	정보 접근 제한	역할 기반 접근 제어 (RBAC)를 구현하여 각 직원의 역할에 따라 데이터 접근 권한을 설정한다.
소프트웨어 및 소스코드 관리 (ISO27001 A.9.4.5, ISO27017 9.4.1, ISO27001 A.14.2.8, ISO27002 14.2.7)	소스 코드에 대한 접근	GitLab 또는 GitHub 와 같은 소스 코드 관리 시스템을 사용하며, 각 접근은 계정 기반으로 로깅되어 추적된다.
	안전한 코딩	기업 개발자에게 OWASP Top 10 및 다른 보안 취약성에 대한 교육을 제공한다.
	보안 테스트	모든 코드 변경 사항은 자동화된 보안 테스트를 거친 후 배포된다.
	외부 개발	외부에서 개발된 코드는 기업 보안 팀에 의해 검토 및 테스트가 이루어지기 전까지 실제 환경에 배포되지 않는다.
데이터 관리 (ISO27018 PII.3.1, ISO27001 A.13.2.3, ISO27002 12.3.1)	데이터 마스킹	사용자 개인 정보가 시스템에 저장되거나 전송될 때, 실제 값을 숨기기 위해 토큰화 및 데이터 마스킹 도구를 사용한다.
	데이터 유출 방지	DLP 솔루션을 도입하여 중요 데이터의 외부로의 유출을 감지하고 차단한다.
	정보 백업	모든 중요 데이터는 암호화된 형태로 AWS S3, Google Cloud Storage 또는 유사한 서비스에 주기적으로 백업된다.
모니터링 (ISO27001 A.12.4.1, ISO27001 A.12.4.3)	로깅	모든 로그는 ELK Stack (Elasticsearch, Logstash, Kibana) 또는 유사한 솔루션을 사용하여 중앙화되어 저장 및 분석된다.
	모니터링 활동	기업은 SIEM (Security Information and Event Management) 솔루션을 도입하여 비정상적 활동을 실시간으로 감지한다.
네트워크 관리 (ISO27002 13.1.2, ISO27001 A.13.1.3, ISO27001 A.13.2.3)	네트워크 보안	모든 네트워크 트래픽은 WAF (Web Application Firewall)와 IDS/IPS 시스템을 통해 필터링된다.
	네트워크 분리	민감한 데이터를 처리하는 서버는 별도의 VLAN 에 위치시켜 다른 네트워크와 격리된다.
	암호화 사용	모든 네트워크 통신은 TLS 를 사용하여 암호화된다.
실시간 위치 및 상태 모니터링 (ISO27002 12.4.1,	장비 및 제품 위치 모니터링	GPS 기반의 위치 추적 시스템을 사용하여 모든 차량과 장비의 실시간 위치 정보를 중앙 데이터베이스에 기록한다. 모든 로그는 암호화되어 저장되며, 접근은 제한적으로 관리된다.
ISO27002 13.1.2, ISO27002 12.4.3)	위치기반 경보 시스템	자원이 지정된 경로나 지역을 벗어나면 중앙 관리 시스템에 경보가 발생한다. 경보는 SMS, 이메일 또는 모바일 앱을 통해 담당자에게 즉시 전송된다.
	상태 모니터링	각 제품에 설치된 센서들은 실시간 정보를 수집하고 중앙 데이터베이스에 전송한다. 보안 상태는 설정된 임계치와 비교되어 경보가 필요한 경우 중앙 시스템에서 자동으로 알림을 전송한다.

모바일 앱 및 웹 인터페이스 (ISO27017 9.5.1, ISO27002 14.3.1, ISO27002 12.3.1)	실시간 대시보드	관리자나 담당자는 웹 인터페이스나 모바일 앱을 통해 모든 장비의 실시간 위치와 상태를 확인할 수 있다. 액세스는 개인별로 제한되며, 각 사용자는 그에 맞는 권한을 부여받아야 한다.
	리포팅 및 분석 도구	과거 데이터를 기반으로 다양한 분석을 수행할 수 있는 도구를 제공한다. 중앙 데이터베이스에서는 주기적으로 백업을 수행하며, 백업 데이터는 암호화되어 저장된다