

인사이트

ISMS 뜻, 정보보호 관리체계는 무엇을 관리하고 공장은 언제 따로 도입하나

방동걸 (주)웨이스 대표이사

2026년 10월 16일

ISMS는 Information Security Management System의 줄임말로, 보호할 정보자산을 정하고 위험을 평가해 통제를 적용한 뒤, 그 통제가 지켜지는지 주기적으로 점검하고 고쳐 가는 관리 체계입니다. 우리말로로는 정보보호 관리체계라고 부릅니다.

제조 AI 운영체제 VEXPLOR를 만드는 웨이스가 이 글에서 다루는 질문은 「원청사가 보안 증빙을 요구할 때, 공장은 어떤 기록을 평소에 남겨 두어야 하는가」입니다. 방화벽과 백신을 갖춘 공장도 계정 목록이나 권한 변경 이력을 내라는 요청을 받으면 말문이 막히기 쉽습니다. 이 글은 정보보호 관리체계가 무엇을 관리하는지, 보안 장비와 무엇이 다른지, 공장이 관리 시스템을 따로 검토할 시점과 도입 전에 확인할 5가지를 차례로 짚습니다.

01

정보보호 관리체계는 정책에서 점검까지 한 바퀴를 관리합니다

정보보호 관리체계는 장비 하나가 아니라 일의 순서입니다. 정책을 정하고, 지켜야 할 자산을 목록으로 만들고, 위험을 평가해 통제를 고르고, 그 통제가 실제로 지켜졌는지 점검해 고치기까지가 한 바퀴입니다. 이 가운데 정보보호 관리체계의 위험 관리는 지켜야 할 자산의 목록에서 시작합니다.

업무	관리체계가 남기는 기록	기록이 없으면
정책 수립	승인일·개정 이력	문서와 설정이 어긋남
자산 식별	자산 목록·중요도	보호 대상이 빠짐
위험 평가	평가 결과·보호대책	투자 순서를 정하지 못함
계정·권한	발급·변경·회수 이력	퇴사자 계정이 남음
외부자 접속	승인자·허용 기간	열어 둔 접속이 방치됨

업무	관리체계가 남기는 기록	기록이 없으면
사고 대응	탐지·격리·복구 기록	같은 사고가 반복
점검·개선	점검 결과·조치 내역	심사 전에 다시 취합

국내에서 ISMS는 인증 제도의 이름이기도 합니다. 정보통신망법 제47조는 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 정보보호 관리체계라고 정하고, 그 체계가 기준에 맞는지 인증하는 제도를 둡니다. 인증 기준은 과학기술정보통신부와 개인정보보호위원회의 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 별표 7에 있습니다. 관리체계 수립 및 운영 16개와 보호대책 요구사항 64개를 합한 80개 항목이 ISMS 인증 기준이고, 여기에 개인정보 처리 단계별 요구사항 21개를 더한 101개 항목이 ISMS-P 인증 기준입니다.



정보보호 관리체계의 위험 관리는 지켜야 할 자산의 목록에서 시작합니다

인증의 유효기간은 3년이고, 그 기간에도 연 1회 이상 사후심사를 받습니다. 고시는 인증을 신청하기 전에 관리체계를 최소 2개월 이상 운영하도록 정합니다. 심사 직전에 만든 문서만으로는 운영 기록이 되지 못한다는 뜻입니다.

국제 표준으로는 ISO/IEC 27001이 있습니다. 국제표준화기구(ISO)는 이 표준이 정보보호 관리체계가 갖춰야 할 요구사항을 정한다고 설명하고, 표준을 적용한 조직이 인증 절차를 밟을지는 스스로 정할 수 있다고 안내합니다. 현행판은 2022년 10월에 나온 ISO/IEC 27001:2022이고, 인증을 표기할 때도 연도까지 붙인 전체 이름으로 쓰도록 권합니다.

02

보안 장비는 공격을 막고, 정보보호 관리체계는 통제가 지켜졌는지를 봅니다

흔히 보안으로 함께 묶는 도구 셋을 나란히 놓아 봤습니다. 셋 다 필요하지만 답하는 질문이 다릅니다.

도구	답하는 질문	기록 단위
방화벽·백신	이 접속을 막을 것인가	차단·탐지 이벤트
보안관제(SIEM)	지금 공격이 진행 중인가	로그 상관 알림
ISMS 관리 시스템	정한 통제가 지켜졌나	자산·권한·점검 건별

방화벽과 백신은 들어오는 공격을 막는 장비입니다. 보안관제는 여러 장비의 로그를 모아 공격의 흔적을 찾습니다. 정보보호 관리체계는 그보다 한 단계 위에서, 누구에게 어떤 권한을 줄지 정한 규칙이 실제 계정에 맞게 적용됐는지, 위험 평가에서 고른 보호대책이 이행됐는지를 기록으로 확인합니다.

인증을 의무로 받아야 하는 곳은 정보통신망법 제47조 제2항이 정합니다. 주요정보통신서비스 제공자, 집적정보통신시설 사업자, 그리고 정보통신서비스 부문 전년도 매출액 100억 원 이상이나 전년도 일일평균 이용자 수 100만 명 이상 등 시행령이 정한 기준에 해당하는 자입니다. 이 의무는 정보통신서비스를 제공하는 사업자에게 걸리므로, 제조기업은 먼저 이 기준에 해당하는지 확인하고, 해당하지 않는다면 인증은 선택입니다. 다만 의무가 아니어도 원청사 보안 점검표가 인증 기준 항목을 바탕으로 질문한다면, 같은 항목에 맞춰 기록을 남겨 두는 편이 대응하기 쉽습니다.

03

공장은 이 4가지 신호가 보일 때 관리 시스템을 따로 검토합니다

아래 4가지 가운데 지금 공장에 해당하는 것이 있다면, 엑셀 대장만으로 버티기보다 정보보호 관리 시스템을 검토해 볼 만합니다.

- 원청사 보안 점검표를 받을 때마다 자료 취합에 몇 주가 든다 — 계정 목록, 권한 부여 이력, 로그 보존 기준, 취약점 조치 내역을 서버와 담당자마다 따로 요청해 모은다면, 평소 업무 기록이 증빙으로 남지 않는다는 뜻입니다.
- 설비 업체에 공용 계정이나 기한 없는 원격 접속을 열어 두었다 — 누가 접속했는지 사람 단위로 남지 않으면 사고가 났을 때 책임 소재를 확인할 수 없습니다.
- 도면·레시피를 누가 조회했는지 기록이 없다 — 파일 서버 공유 폴더에 둔 자료는 내려받은 기록이 남지 않기도 합니다. 그러면 퇴사자의 자료 반출이 의심돼도 근거를 찾기 어렵습니다.

- **담당자가 바뀌면 설정의 이유를 아는 사람이 없다** — 정보보호를 IT 담당자가 겸직한다면, 정책과 설정의 변경 이유가 한 사람의 기억에만 남기 쉽습니다.

04

계정과 권한 기록은 일이 일어나는 순간 남아야 합니다

관리 시스템을 갖추고도 점검 때마다 자료를 다시 모은다면, 기록이 언제 생기는지부터 살펴봐야 합니다.

계정을 발급하고 권한을 바꾸고 퇴사자 계정을 회수한 일을 월말에 대장으로 옮겨 적는다면, 그 사이에 바뀐 권한은 기록에서 빠집니다.

인증 기준도 이 기록을 요구합니다. 별표 7의 접근권한 검토 항목은 계정과 접근권한의 이력을 남기고 주기적으로 검토하라고 정합니다. 퇴직 및 직무변경 관리 항목은 퇴직하거나 직무가 바뀔 때 계정과 접근권한을 회수·조정하는 절차를 요구합니다. 인사 발령과 계정 회수 기록이 함께 남아 있어야 이 항목에 기록으로 답하기 쉽습니다.

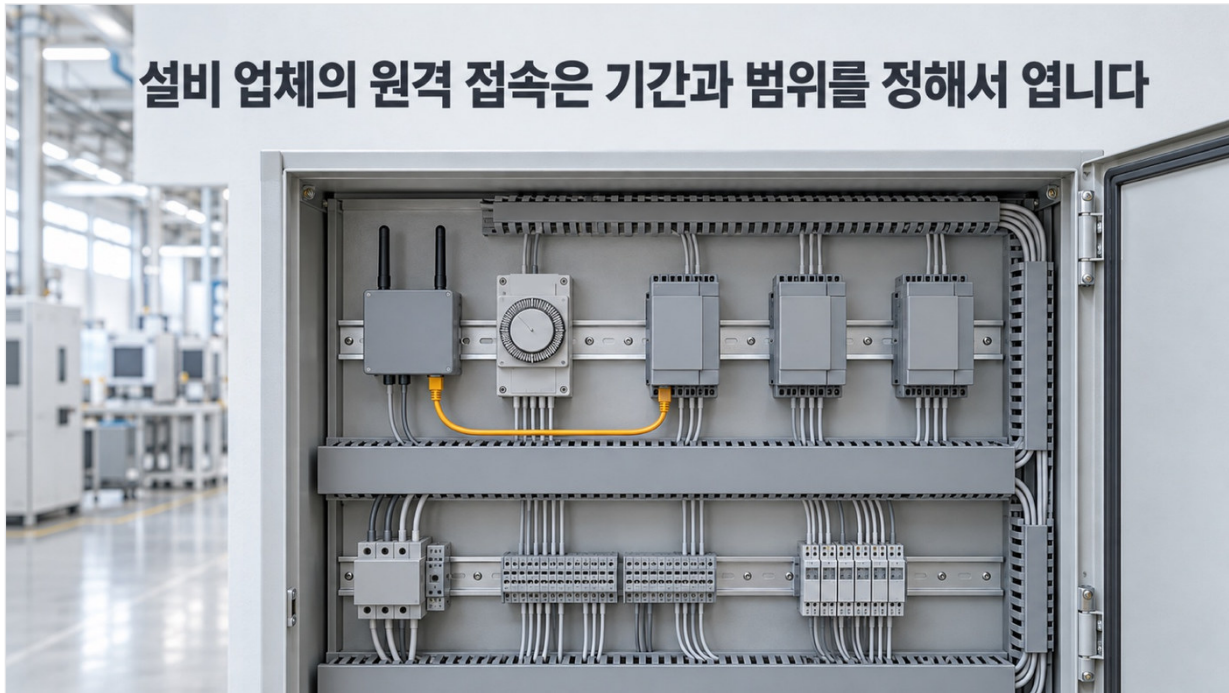
로그는 보존 방법을 미리 정해 둡니다. 접속 기록을 위·변조되지 않게 남기려면 보존 기간과 방법이 사고 전에 정해져 있어야 합니다. 사고가 난 뒤에는 그 이전 기록을 새로 만들 수 없습니다.

05

정보보호 관리체계가 공장 설비와 만나는 두 지점

사무실 PC와 서버만 목록에 올리면 공장의 정보보호는 절반에서 멈춥니다. 생산 설비와 만나는 두 지점은 따로 봐야 합니다.

- **설비 자산 목록** — PLC, HMI, SCADA, 산업용 네트워크 장비도 정보자산입니다. 제조사, 모델, 펌웨어 버전, 설치 위치, 중요도가 서버와 같은 목록에 있어야 어떤 제어기에 취약점 공지가 나와도 영향 범위를 바로 확인할 수 있습니다.
- **원격 유지보수 접속** — 인증 기준의 원격접근 통제 항목은 원격 접속을 허용할 때 책임자 승인, 접근 단말 지정, 허용 범위와 기간 설정, 강화된 인증 같은 보호대책을 요구합니다. 설비 업체의 원격 접속은 기간과 범위를 정해서 엽니다. 정한 기간이 끝나면 닫습니다.



설비 업체의 원격 접속은 기간과 범위를 정해서 엽니다

패치는 공장에서 더 따져 봐야 할 일입니다. 생산 설비는 재부팅이 곧 가동 중단이라 사무용 PC처럼 바로 패치하기 어렵습니다. 인증 기준의 패치관리 항목도 최신 패치를 적용하되, 서비스 영향을 검토해 적용이 어려우면 별도의 보완대책을 마련해 이행하라고 정합니다. 패치하지 못한 설비는 그 이유와 보완대책을 기록으로 남겨 두는 것까지가 관리체계의 일입니다.

06

정보보호 관리체계는 4단계로 넓혀 가는 편이 안전합니다

인증 기준 80개 항목을 처음부터 한꺼번에 맞추려 하면 검직 담당자가 감당하기 어렵습니다. 앞 단계 기록이 정확해야 다음 단계도 의미가 있으니, 아래 순서로 넓혀 가기를 권합니다.

단계	커는 범위	다음으로 넘어갈 기준
1단계	IT·설비 자산 목록	중요도가 모두 매겨짐
2단계	계정·권한·외부자 접속	공용 계정이 없어짐
3단계	로그 보존·사고 대응	대응 절차가 문서화됨
4단계	점검·중방·인증 준비	점검이 조회로 끝남

1단계만 자리 잡아도 「우리 공장에 제어기가 몇 대 있고 펌웨어 버전이 무엇인가」라는 물음에 목록으로 답할

수 있습니다. 2단계부터는 인사·설비·구매 담당자도 계정 회수와 외부자 승인을 맡으므로 승인자와 처리 기한도 이때 정합니다.

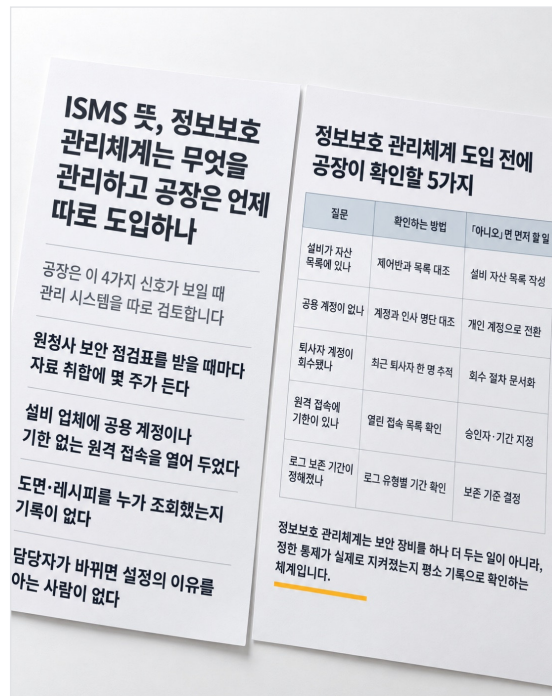
07

정보보호 관리체계 도입 전에 공장이 확인할 5가지

질문	확인하는 방법	「아니오」면 먼저 할 일
설비가 자산 목록에 있나	제어반과 목록 대조	설비 자산 목록 작성
공용 계정이 없나	계정과 인사 명단 대조	개인 계정으로 전환
퇴사자 계정이 회수됐나	최근 퇴사자 한 명 추적	회수 절차 문서화
원격 접속에 기한이 있나	열린 접속 목록 확인	승인자·기간 지정
로그 보존 기간이 정해졌나	로그 유형별 기간 확인	보존 기준 결정

세 번째 질문부터 확인하는 편이 좋습니다. 최근에 퇴사한 직원 한 명을 골라 메일, 업무 시스템, 파일 서버, 설비 접속 계정이 언제 회수됐는지 따라가 보면, 시스템에 옮겨야 할 절차와 아직 정해지지 않은 절차가 드러납니다. 첫 번째 질문도 미리 봐 뒀야 합니다. 제어반에 있는 장비가 목록에 없으면, 그 장비는 위험 평가에서도 빠집니다.

웨이스가 VEXPLOR에서 정보보호 관리 기능을 ERP·MES와 같은 플랫폼 안에 두는 이유도 여기에 있습니다. VEXPLOR ISMS는 보안 정책을 접근제어 규칙으로 내려 업무 화면의 동작을 정하고, 계정 생명주기를 인사 정보와 연결해 퇴직 처리 때 권한이 회수되도록 설계돼 있습니다. 감사 로그는 추가만 가능하고 수정·삭제가 되지 않는 구조로 남고, PLC·SCADA·HMI 같은 설비 자산은 설비 마스터와 연결된 목록에서 펌웨어 버전과 최근 점검일을 함께 관리하도록 설계돼 있습니다. 인증 기준 항목에 시스템 기록을 증빙으로 연결하는 점검 기능도 설계돼 있지만, 인증 취득 여부는 심사 기관이 판단하며 이 기능이 취득을 보장하지는 않습니다. 백신, 방화벽·침입방지 장비, 대규모 로그의 장기 저장 인프라는 이 솔루션의 범위가 아니고, 24시간 관제가 필요하다면 전문 관제 서비스와 함께 검토해야 합니다. 기능 목록과 따르는 표준은 [VEXPLOR ISMS 솔루션 페이지](#)에 정리해 두었습니다.



이 글을 한 장으로 요약하면 이렇습니다 — 관리 시스템을 따로 검토할 신호 4가지와 도입 전에 확인할 5가지

정보보호 관리체계는 보안 장비를 하나 더 두는 일이 아니라, 정한 통제가 실제로 지켜졌는지 평소 기록으로 확인하는 체계입니다. 원청사 점검표 앞에서 자료 취합부터 시작하는 공장이라면, 최근 퇴사자 한 명의 계정 회수 기록을 따라가 보는 것이 첫 단계입니다.

WACE(웨이스)는 공장이 스스로 판단하고 멈추지 않게 하는 제조 AI 운영체제 VEXPLOR를 만드는 회사다.

08

함께 읽어보세요

- [WMS 뜻, 창고관리시스템은 무엇을 관리하고 공장은 언제 따로 도입하나](#)
- [경영진이 AI 도입을 결정하면 보안 걱정은 설계 요건이 됩니다 — 구축 업체에 확인할 5가지](#)
- [웨이스는 대기업 협력사 공장에 VEXPLOR를 구축할 때 공장 데이터를 어디에 두는가](#)



원문	blog.vexplor.com/post/what-is-isms-information-security-management-system
발행	2026년 10월 16일 · 방동걸 (주)웨이스 대표이사
회사	주식회사 웨이스 (WACE Inc.) · 대표이사 방동걸 · 사업자등록번호 439-87-02852
주소	(18462) 경기 화성시 동탄구 동탄영천로 150, 에이동(A동) 1332·1333·1334·1335호 (영천동, 실리콘엘리동탄)
연락처	전화 070-4730-0629 · contact@wace.me
홈페이지	wace.me · linkedin.com/company/wace-inc



원문



홈페이지



링크드인