무료 백서

# ISMS-P 취득 백서

정보보호 + 개인정보보호 통합 관리체계 인증 가이드

개인정보 처리단계별 22 개 통제까지 깊이 있게

취득 절차 · 비용 · 결함 사례 · 인증심사원 자격증까지

# 백 지 석

2026

# 머리말 — 이 백서를 시작하며

'P 가 한 글자 더 붙었을 뿐인데 왜 이렇게 차이가 클까.' ISMS 와 ISMS-P 를 비교해 본 사람이라면 한 번쯤 떠올리는 의문입니다. ISMS-P 의 'P'는 단순한 표기가 아니라, 인증 항목 22 개와 한국 기업이 짊어진 가장 무거운 의무 — 개인정보 보호 — 를 가리킵니다.

한국에서 일정 규모 이상의 IT 서비스를 운영한다면 ISMS-P 는 사실상 '선택'이 아닙니다. 정보통신망법은 ISMS·ISMS-P 중 하나의 인증을 의무화하고 있으며, 이커머스·SNS·핀테크처럼 개인정보를 다량 다루는 회사는 ISMS-P 를 '권장'이 아닌 '기본값'으로 받아들이는 추세입니다. 그 배경에는 매년 강화되는 개인정보보호법, 늘어나는 손해배상 소송, 그리고 '정보주체 신뢰'라는 무형 자산의 중요성이 있습니다.

그런데 정작 'P' 영역의 22 개 통제는 한국어 자료에서도 깊게 다루는 곳이 드뭅니다. 수집 동의 화면 하나, 위탁 계약서 한 줄, 처리방침 한 단락에서 결함이 줄줄이 도출되는데도, 그 근거가 어떤 법령·통제와 연결되는지를 전체적으로 짚어주는 자료는 거의 없습니다.

이 백서는 그 빈틈을 메우기 위해 만들었습니다. ISMS-P 102 개 통제 전체를 훑으면서도, 특히 'P' 영역(개인정보 처리단계별 요구사항 22 개)을 한 장 한 장 풀어 설명했습니다. 관리체계·보호대책 같은 일반 ISMS 영역은 압축해서 다루고, 개인정보보호법·정보주체 권리·위탁·국외이전·가명정보처럼 한국형 ISMS-P 에서만 도드라지는 부분에 더 많은 지면을 할애했습니다.

이 백서는 무료입니다. 정보보호 담당자는 물론, 개인정보 보호책임자(CPO)·법무·기획·제품 담당자, 그리고 개인정보를 '한 번이라도 만져야 하는' 모든 분께 도움이 되도록 친절하게 풀어 썼습니다. 잘못된 점이나 보완할 점이 있다면 알려 주시면 다음 판에 반영하겠습니다.

**저자 백지석**

# 목 차

17. ISMS-P 인증심사원 자격증

18. 인증 준비 체크리스트

19. 자주 묻는 질문 (FAQ)

20. 참고자료 및 공식 사이트

# 01. ISMS-P, ‘P’가 가지는 무게

ISMS-P 의 정식 명칭은 ‘정보보호 및 개인정보보호 관리체계 인증’입니다. 영문으로는 ‘Personal information & Information Security Management System’의 약자입니다. 이름이 길어 보이지만 핵심은 명확합니다. 일반적인 정보보안 관리체계(ISMS)에 ‘개인정보(Personal Information)’ 보호 영역을 통합한 한국형 인증입니다.

## ‘P’ 한 글자가 만드는 차이

| 구 분 | ISMS | ISMS-P |
|---|---|---|
| 통제 수 | 80 개 | 102 개 (+22 개) |
| 보호 대상 | 정보 자산 전반 | 정보 자산 + 개인정보 라이프사이클 |
| 근거 법령 | 정보통신망법 제 47 조 | 정보통신망법 + 개인정보보호법 제 32 조의 2 |
| 주관 부처 | 과학기술정보통신부 | 과기정통부 + 개인정보보호위원회 |
| 적합 기업 | B2B SaaS, 인프라 사업자 | 이커머스, SNS, 핀테크, 의료, 교육 등 개인정보 다량 처리 |
| 글로벌 인지도 | 낮음 | 낮음 (국내 인증) |
| 손해배상 시 영향 | ‘적정 보호조치’ 일부 입증 | ‘적정 보호조치’ + ‘개인정보 안전조치’ 동시 입증 |

## 왜 ‘P’가 점점 무거워지는가

한국에서 개인정보 관련 규제는 매년 강화되고 있습니다. 2020 년 ‘데이터 3 법’ 개정으로 가명정보 활용이 가능해졌고, 2023 년 개인정보보호법 전면 개정으로 정보주체 권리가 대폭 확대되었으며, 2024 년에는 가명정보 처리 가이드라인이 비정형 데이터(이미지·음성·영상)까지 확장되었습니다. 한 마디로 ‘P’ 영역의 부담이 매년 커지고 있다는 뜻입니다.

그뿐이 아닙니다. 개인정보 유출 사고가 발생하면 사고 대응 비용·과징금·민사 손해배상이 누적되어 회사가 흔들릴 정도의 타격이 됩니다. 2023 년 개정법은 과징금 상한을 ‘위반행위

관련 매출액의 3%'로 상향했고, 정보주체 한 사람당 '500 만 원 이하의 손해배상'을 청구할 수 있게 했습니다. 100 만 명의 개인정보가 유출된 사고에서 단순 계산으로 5 조 원의 잠재 청구액이 발생할 수 있다는 의미입니다.

**'ISMS-P 는 비싸고 어렵다'는 인식의 배경**

ISMS-P 가 ISMS 보다 비싸고 어렵게 느껴지는 이유는 22 개 통제의 양 때문이 아닙니다. 진짜 부담은 '개인정보 처리의 모든 화면, 모든 동의, 모든 위탁 계약, 모든 파기 절차'를 점검해야 한다는 '면적의 차이'입니다. 22 개 통제 뒤에 80 개 가까운 세부 점검항목이 숨어 있고, 그 각각이 회사의 여러 시스템·문서·계약에 흩어져 있습니다.

# 02. ISMS-P 의 탄생 — ISMS 와 PIMS 의 통합

ISMS-P 는 2018 년 11 월 7 일에 정식 시행된 비교적 새로운 인증 제도입니다. 그러나 이 인증의 뿌리는 20 년 가까이 거슬러 올라갑니다. 한국의 정보보호·개인정보보호 인증 제도가 어떻게 진화해 'ISMS-P 한 우산'으로 통합되었는지 살펴봅니다.

## 20 년의 진화 — 연대표

| 연 도 | 사 건 | 의 미 |
|---|---|---|
| 2002 | ISMS 인증 도입 (정보통신부) | 민간 정보보안 관리체계 인증의 시작 |
| 2010 | PIMS 인증 도입 (방송통신위원회) | 개인정보보호 관리체계 인증 별도 운영 |
| 2013 | PIPL 인증 도입 (행정자치부) | 개인정보보호법 기반 별도 인증 추가 |
| 2014 | G-ISMS 가 ISMS 로 통합 | 공공·민간 정보보안 인증 일원화 |
| 2016 | PIMS 와 PIPL 통합 (KISA 로 일원화) | 개인정보 인증 단일화 |
| 2018-11-07 | ISMS-P 정식 시행 | ISMS + PIMS 통합 인증 출범 |
| 2020 | 데이터 3 법 개정 반영 | 가명정보 처리 영역 강화 |
| 2023-11 | ISMS-P 인증기준 안내서 개정 | 개정 개인정보보호법 반영 (자동화 의사결정 등) |
| 2024-02 | 가명정보 처리 가이드라인 개정 | 비정형 데이터(이미지·음성·영상) 가명처리 반영 |

## 왜 통합이 필요했나

2018 년 통합 이전에는 개인정보를 다루는 IT 서비스 기업이 ISMS 와 PIMS 를 '별도로' 받는 경우가 많았습니다. 두 인증의 통제 70~80%가 겹치는데도 심사·문서·일정·비용을 두 배로 부담하는 비효율이 누적되었고, 정부 입장에서도 두 부처(과기정통부·개인정보위)가 나란히 운영하는 행정 부담이 컸습니다.

통합의 명분은 명확했습니다. '하나의 회사에서 정보보호와 개인정보 보호는 분리할 수 없다.' 관리체계·정책·위원회·교육 같은 공통 기반은 한 번에 구축하고, 정보 자산의 보호와 개인정보의 라이프사이클을 동일한 인증 우산 아래 다루자는 발상이었습니다. 그렇게 통합된 ISMS-P 는 단순한 '인증 합치기'가 아니라, 한국 정보보안 행정 구조의 일대 정비였습니다.

**ISMS-P 를 받으면 'P 미포함 ISMS'도 자동으로 받는 셈?**

법령상으로는 'ISMS 와 ISMS-P 중 선택'이지만, 실무적으로는 ISMS-P 가 ISMS 의 상위 호환입니다. ISMS-P 인증서를 가지고 있으면 ISMS 의무대상으로서의 의무도 자동 충족됩니다. 따라서 굳이 'ISMS 만' 받을 이유가 거의 없으며, 처음부터 ISMS-P 를 받는 것이 합리적입니다.

# 03. ISMS vs ISMS-P 정확하게 비교한다

두 인증의 차이를 '22 개의 추가 통제'로만 보면 ISMS-P 의 본질을 놓치게 됩니다. 차이는 통제 수가 아니라 '보호 대상'과 '심사 깊이'에 있습니다.

| 관점 | ISMS | ISMS-P |
|---|---|---|
| 보호 대상의 본질 | '회사의 정보 자산' | '회사의 정보 자산' + '정보주체의 개인정보' |
| 심사 시 인터뷰 대상 | 정보보안 담당, 시스템 운영자, 외주사 | 위 + 개인정보 처리자, 마케팅·CS, 법무, CPO |
| 증적의 종류 | 정책·로그·시험 기록 위주 | 위 + 동의 기록, 처리방침 변경 이력, 위탁 계약, 파기 기록 |
| 가장 자주 결함이 나는 곳 | 로그·접근통제·외주 | 수집 동의, 위탁 사항 처리방침, 파기, 정보주체 통지 |
| 담당 조직의 특징 | 정보보안 부서 단독 가능 | 정보보안 + CPO + 법무 + 사업부 협업 필수 |

## 결정 트리 — 우리 회사는 무엇을 받아야 하나

다음 5 가지 질문에 답해 보세요.

1. 회사가 회원가입형 서비스를 운영하는가? (회원 정보 보유)
2. 결제 정보·실명·주민번호·휴대폰번호 등 식별정보를 처리하는가?
3. 마케팅 동의·뉴스레터·푸시 알림 같은 정보주체 동의를 운영하는가?
4. 고객 데이터를 외부 위탁(CRM·콜센터·물류)에 넘기는가?
5. 글로벌 클라우드(AWS·GCP·Azure 등 미국 리전 포함)에 데이터를 저장하는가?

'예'가 2 개 이상이면 ISMS-P 를 권장합니다. '예'가 4 개 이상이면 사실상 ISMS-P 없이는 사업을 안전하게 운영하기 어렵습니다. ISMS 만 받으면 위 5 개 질문 중 하나에서 사고가 나도 '적정 보호조치 이행'의 입증이 부분적이기 때문입니다.

**‘P’를 빼는 비용 vs ‘P’를 추가하는 비용**

ISMS-P 추가 22 개 통제의 컨설팅·심사 비용 증분은 통상 30~50% 수준입니다. 반면 ‘P’를 빼고 운영하다가 개인정보 사고가 났을 때 발생할 수 있는 과징금·소송·평판 손실은 그 100 배 이상이 될 수 있습니다. ‘P’ 추가는 보험료라고 보면 가장 합리적인 보험입니다.

# 04. ISMS-P 의무대상 — 개인정보 처리 관점

정보통신망법 제 47 조 제 2 항은 ISMS·ISMS-P 의무대상을 5 가지로 정의합니다. 이 5 가지 자체는 ISMS 와 동일하지만, '우리 회사가 ISMS 만 받으면 되는가, ISMS-P 를 받아야 하는가'를 결정하는 기준은 '개인정보 처리량과 민감도'입니다.

| 구분 | 기준 | ISMS-P 를 권장하는 이유 |
|---|---|---|
| ① ISP | 정보통신망 서비스 제공자 | 가입자 개인정보·통화기록 등 민감 정보 보유 |
| ② IDC | 집적정보통신시설 사업자 | 다수 고객사의 데이터를 위탁 보관 — 위탁자/수탁자 모두 P 필요 |
| ③ 매출 1,500 억 | 전년 매출 또는 세입 1,500 억 원 이상 | 상급종합병원·대학 포함 — 의료·학적 정보의 민감도 최고 |
| ④ 정보통신 매출 100 억 | 정보통신서비스 매출 100 억 원 이상 | 이커머스·SaaS·플랫폼 — 회원·결제·구매 이력 다량 |
| ⑤ 일평균 100 만 명 | 직전 3 개월 일평균 이용자 100 만 명 | B2C 플랫폼 — 정보주체 수가 곧 책임의 크기 |

## 'ISMS 만 받아도 되는' 케이스가 줄어드는 이유

위 5 개 기준 중 어느 하나라도 해당하면 의무대상이지만, 실제로는 '개인정보를 거의 처리하지 않는' 의무대상은 매우 드뭅니다. 예를 들어 IDC 사업자조차 '직원 인사 정보·고객사 담당자 정보'를 처리하므로 개인정보보호법 적용 대상입니다. 결과적으로 의무대상자 대부분이 ISMS-P 를 선택합니다.

또한 의무대상이 아니더라도 '자율 취득'으로 ISMS-P 를 받는 회사가 빠르게 늘고 있습니다. 공공기관 입찰, 대기업 협력사 등록, B2B 영업, M&A 실사에서 'ISMS-P 보유 여부'가 표준 평가 항목으로 자리잡았기 때문입니다.

## 이행 기한 — 한 번 의무대상이 되면

정보통신망법 시행령은 '의무대상에 해당하게 된 해의 다음 해 8 월 31 일까지 인증을 받아야 한다'고 정하고 있습니다. 인증 준비 기간이 평균 6~9 개월 걸린다는 점을 고려하면, 의무대상이 된 시점부터 즉시 준비를 시작해야 마감을 맞출 수 있습니다.

마감을 놓치면 정보통신망법 제 76 조에 따라 '3,000 만 원 이하의 과태료'가 부과됩니다. 더 큰 리스크는 KISA 가 매년 '미인증 의무대상' 명단을 공공데이터로 공개한다는 점입니다. 회사 이름이 한 번 명단에 오르면 거래처 신뢰도에 직접적인 타격이 갑니다.

**'이용자 100 만 명'의 진짜 의미**

'일평균 100 만 명'은 회원 수 100 만 명이 아닙니다. 직전 3 개월간 매일 평균 100 만 명이 서비스를 '이용'해야 적용됩니다. 즉 회원 1,000 만 명 회사라도 일평균 이용자가 50 만 명이면 이 기준에는 해당하지 않을 수 있습니다. 반대로 회원 50 만 명짜리 라이브 커머스가 매일 100 만 명 이상 들른다면 이 기준이 적용됩니다.

# 05. 개인정보보호법과 ISMS-P 의 매핑

ISMS-P 의 'P' 영역 22 개 통제는 '개인정보보호법(이하 '개보법')'의 핵심 의무를 거의 그대로 통제로 옮겨 놓은 것입니다. 즉 ISMS-P 는 '개보법 준수의 통제판'이라고 봐도 무방합니다. 이 절은 주요 법 조항과 통제의 매핑을 정리합니다.

| 개인정보보호법 조항 | 주요 의무 | 매핑되는 ISMS-P 통제 |
|---|---|---|
| 제 15 조 (수집·이용) | 수집 동의, 최소 수집, 처리 목적 명시 | 3.1.1 ~ 3.1.4 (수집) |
| 제 17 조 (제공) | 제 3 자 제공 동의, 제공 목적 명시 | 3.3.1, 3.3.2 (제공) |
| 제 18 조 (목적 외 이용·제공) | 수집 목적 외 이용·제공 제한 | 3.2.1, 3.2.2 (보유·이용) |
| 제 22 조 (동의 방법) | 선택적 동의, 항목별 분리 동의 | 3.1.1 (수집 동의) |
| 제 23 조 (민감정보) | 사상·신념·건강 등 민감정보 별도 동의 | 3.1.3 (민감정보·고유식별정보) |
| 제 24 조 (고유식별정보) | 주민번호 등 고유식별정보 처리 제한 | 3.1.3 (민감정보·고유식별정보) |
| 제 25 조 (영상정보처리기기) | CCTV 설치·운영 제한 | 3.1.5 (영상정보처리기기) |
| 제 26 조 (위탁) | 위탁사 보안 조치, 처리방침 공개 | 3.3.2 (위탁), 2.3.1 (외부자 보안) |
| 제 27 조 (영업양도) | 영업양도·합병 시 통지 | 3.3.3 (영업의 양도) |
| 제 28 조의 2 (가명정보) | 가명정보 처리, 결합·재식별 금지 | 3.2.5 (가명정보 처리) |
| 제 28 조의 8 (국외이전) | 국외이전 동의, 보호조치 | 3.3.2 (제공·위탁) |
| 제 30 조 (처리방침) | 개인정보 처리방침 작성·공개 | 3.5.1 (처리방침 공개) |
| 제 31 조 (CPO) | 개인정보 보호책임자 지정 | 1.1.2 (조직 구성) |
| 제 35~37 조 (정보주체 권리) | 열람·정정·삭제·처리정지·이전 | 3.5.2 (정보주체 권리) |

| | | |
|---|---|---|
| 제 39 조의 6<br>(자동화 결정) | 자동화된 의사결정<br>거부·설명 요구권 | 3.2.6 (자동화된 의사결정) |

**개보법이 바뀌면 ISMS-P 도 바뀐다**

ISMS-P 인증기준은 '법령 개정에 따라 주기적으로 갱신'됩니다. 2023 년 개보법 전면 개정에 따라 '자동화된 의사결정에 관한 정보주체 권리' 같은 신설 통제가 들어갔고, 2024 년 가명정보 가이드라인 개정에 따라 비정형 데이터 처리 부분이 보강되었습니다. 인증을 운영 중인 회사는 매년 KISA 공지의 '인증기준 개정 이력'을 확인해야 합니다.

# 06. 인증기준 102 개 한 장으로 보기

ISMS-P 인증기준은 3 개 영역, 21 개 분야, 102 개 통제, 약 317 개 세부 점검항목으로 구성됩니다. 전체 구조를 한 장에 정리합니다.

| 영 역 | 분야 수 | 통제 수 | 세부 점검 | 비 중 |
|---|---|---|---|---|
| 1. 관리체계 수립 및 운영 | 4 | 16 | 약 42 | 관리·거버넌스 |
| 2. 보호대책 요구사항 | 12 | 64 | 약 195 | 관리적·물리적·기술적 |
| 3. 개인정보 처리단계별 요구사항 | 5 | 22 | 약 80 | 개인정보 라이프사이클 |
| 합 계 | 21 | 102 | 약 317 | — |

## 영역별 무게중심

영역별로 심사관이 가장 신경 쓰는 '무게중심'이 다릅니다. 준비 시 우선순위를 정할 때 참고하세요.

- 1.관리체계 (16 개) — 경영진 의지·CISO/CPO 지정·위원회 운영. '체계가 살아 있는가'를 보여주는 영역
- 2.보호대책 (64 개) — 가장 양이 많고 결함도 가장 많이 도출. 접근통제·암호화·로그·외주가 핵심
- 3.개인정보 처리단계 (22 개) — 양은 적지만 결함률 1 위. 동의 화면 한 줄로 다수 결함이 나오는 영역

**'22 개'가 가장 부담스러운 이유**

1·2 영역의 결함은 '기술 도입·정책 보완'으로 비교적 빠르게 해결되지만, 3 영역 결함은 '서비스 화면을 고치고, 약관을 다시 받고, 처리방침을 재공시'해야 하는 경우가 많아 사업 일정에 직접 영향을 줍니다. 그래서 ISMS-P 준비에서 3 영역을 '가장 먼저, 가장 깊게' 점검해야 합니다.

# 07. 1. 관리체계 수립·운영 (16 개) 핵심 포인트

관리체계 영역은 '회사가 ISMS-P 를 어떻게 운영하는가'의 골격입니다. PDCA 사이클(계획-실행-점검-개선)에 따라 4 개 분야로 나뉩니다.

| 분야 | 통제 수 | 주 요 통 제 |
|---|---|---|
| 1.1 관리체계 기반 마련 | 6 | 경영진 참여, CISO·CPO 지정, 조직 구성, 범위 설정, 정책 수립, 자원 할당 |
| 1.2 위험관리 | 4 | 정보자산 식별, 현황 분석, 위험 평가, 보호대책 선정·이행계획 |
| 1.3 관리체계 운영 | 3 | 보호대책 구현, 보호대책 공유, 운영 현황 관리 |
| 1.4 관리체계 점검 및 개선 | 3 | 법적 요구사항 준수 검토, 관리체계 점검(내부심사), 관리체계 개선 |

## ISMS-P 관점에서 특별히 챙겨야 할 것

- CPO(개인정보 보호책임자) 지정 — 임원급 지정 필수. 개보법 제 31 조에 따라 신고도 함께 (1.1.2)
- 정보보호 + 개인정보보호 위원회 — 두 위원회를 따로 둘지, 통합할지 결정. 통합 시 안건 비율을 명확히
- 정보자산 식별에서 '개인정보 자산'을 별도 분류 — 개인정보 항목·보유기간·저장 위치 모두 식별
- 위험평가에서 '개인정보 영향평가(PIA)' 결과를 반영 — 공공기관은 의무, 민간도 권장

**CISO 와 CPO 를 한 사람이 겸임해도 되나**

법령상 가능합니다. 다만 회사 규모가 크거나 개인정보 처리량이 많은 경우 분리 지정을 권장합니다. 심사관은 '겸임 시 의사결정의 충돌 가능성을 어떻게 관리하는가'를 묻습니다. 작은 회사라면 겸임 + '분기별 외부 자문' 같은 보완 통제를 SoA 에 명시하면 됩니다.

# 08. 2. 보호대책 요구사항 (64 개) 핵심 포인트

보호대책 영역은 12 개 분야 64 개 통제로 구성됩니다. 양이 가장 많지만 '일반적인 정보보안 통제'와 겹치는 부분이 많아 기존 ISMS·ISO 27001 운영 회사라면 부담이 크지 않습니다.

| 분야 | 통제 수 | ISMS-P 관점의 핵심 |
|---|---|---|
| 2.1 정책·조직·자산관리 | 3 | 개인정보 자산을 별도 분류·라벨링 |
| 2.2 인적보안 | 6 | 주요 직무자(개인정보 취급자) 별도 관리·교육 |
| 2.3 외부자 보안 | 4 | 위탁사·재위탁사 점검, 클라우드 위탁 별도 |
| 2.4 물리보안 | 7 | 개인정보 처리시스템 보호구역 분리 |
| 2.5 인증 및 권한 관리 | 6 | 개인정보 취급자 권한 최소화·정기 검토 |
| 2.6 접근 통제 | 7 | 개인정보 처리시스템 접근통제 강화 (망분리 등) |
| 2.7 암호화 적용 | 2 | 개인정보 저장·전송 시 암호화 (안전성 확보조치 기준) |
| 2.8 정보시스템 도입·개발 보안 | 6 | 개인정보 처리 시스템 개발·시험 분리 |
| 2.9 시스템·서비스 운영관리 | 7 | 접속기록(로그) 1 년 이상 안전 보관 |
| 2.10 시스템·서비스 보안관리 | 9 | 보안 패치, 클라우드 보안, 악성코드 통제 |
| 2.11 사고 예방 및 대응 | 5 | 개인정보 유출 사고 신고 절차 (24 시간/72 시간) |
| 2.12 재해복구 | 2 | 개인정보 처리시스템 RTO·RPO 측정 |

## '개인정보 안전성 확보조치 기준' 고시와 매핑

2 영역의 기술적 통제 상당수는 '개인정보의 안전성 확보조치 기준 고시(개인정보보호위원회)'와 직접 연결됩니다. 이 고시는 개인정보 처리자가 반드시 지켜야 하는 '기술적·관리적·물리적' 안전조치를 정의합니다. ISMS-P 심사에서는 이 고시 위반이 곧 통제 결함입니다.

- 내부 관리계획 수립 (관리적 안전조치)

- 접근권한 관리 (개인정보 취급자별 권한 부여·변경·말소 기록 3 년 보관)
- 접근통제 (안전한 인증수단, 외부 인터넷망 차단, 망분리)
- 개인정보의 암호화 (저장·전송 시 안전한 암호 알고리즘)
- 접속기록의 보관·점검 (1 년 이상 보관, 월 1 회 이상 점검)
- 악성프로그램 등 방지 (백신·패치)
- 물리적 안전조치 (출입통제·잠금장치)
- 재해·재난 대비 안전조치 (백업·복구)

**'5 만 명 vs 100 만 명' — 안전조치 기준이 달라진다**

안전성 확보조치 기준은 '처리하는 정보주체 수'에 따라 적용 강도가 다릅니다. 100 만 명 이상이면 '망분리 의무화', '접속기록 2 년 보관' 등 상위 기준이 적용됩니다. 회사가 어느 등급에 해당하는지 정확히 산정해 SoA·정책서에 반영해야 합니다.

# 09. 3. 개인정보 처리단계별 요구사항 (22 개) 완전 해부

이 백서의 '심장'입니다. ISMS-P 를 ISMS 와 구분 짓는 22 개 통제를 5 개 분야로 나누어 한 항목 한 항목 풀어 봅니다. 각 통제는 개보법 조항과 직접 매핑되며, 실무에서 가장 자주 결함이 도출되는 영역이기도 합니다.

## 3.1 개인정보 수집 시 보호조치 (5 개)

'처음 받을 때 잘 받아야 한다.' 수집 단계의 결함은 회원가입 화면·가입 약관·앱 권한 요청 화면 등 사용자가 직접 보는 곳에서 발생하므로 결함이 곧바로 회사 평판에 영향을 줍니다.

| 통제 | 내 용 | 심사 포인트 |
|---|---|---|
| 3.1.1 개인정보 수집·이용 | 수집 항목·이용 목적·보유 기간 동의 | 필수·선택 분리, 항목별 별도 동의 |
| 3.1.2 개인정보의 수집 제한 | 최소 수집 원칙 | '필요 최소' 항목만 수집하는지, 미사용 항목 즉시 삭제 |
| 3.1.3 주민번호 처리 제한·민감정보·고유식별정보 | 주민번호 처리 법적 근거 + 별도 동의 | 주민번호 대체수단(i-PIN, 휴대폰 본인인증) 제공 |
| 3.1.4 만 14 세 미만 아동의 개인정보 | 법정대리인 동의 | 법정대리인 확인 절차 (이메일·휴대폰·신용카드) |
| 3.1.5 영상정보처리기기 | CCTV 설치·운영 안내, 보관 기준 | 안내판 설치, 30 일 이내 자동삭제 |

**■ 3.1 영역에서 가장 자주 발생하는 결함**

- 필수 항목과 선택 항목이 한 화면에 묶여 '체크박스 1 개'로 동의를 받는 경우
- 수집·이용 목적이 '서비스 제공' 같은 추상적 표현으로만 기재됨
- 주민번호 입력란이 있지만 i-PIN 등 대체수단이 함께 제공되지 않음
- 만 14 세 미만 회원가입 시 법정대리인 동의 절차가 '이름만 입력' 수준
- CCTV 안내판이 '일부 출입구에만' 설치됨

## 3.2 개인정보 보유·이용 시 보호조치 (5 개)

'받은 다음 어떻게 쓰는가'의 단계입니다. 가명정보 처리, 자동화 의사결정 같은 최신 트렌드 통제가 들어 있어 매년 갱신되는 영역입니다.

| 통제 | 내 용 | 심사 포인트 |
|---|---|---|
| 3.2.1 개인정보 현황 관리 | 개인정보 처리 현황·항목·흐름 관리 | 개인정보 처리 흐름도(데이터 라이프사이클 다이어그램) |
| 3.2.2 개인정보 품질보장 | 정확성·최신성 유지 | 주기적 정합성 점검, 정보주체 정정 요청 처리 |
| 3.2.3 이용자 단말기 접근 보호 | 앱의 단말기 접근 권한 관리 | 꼭 필요한 권한만 요청, 거부 시에도 일부 기능 제공 |
| 3.2.4 개인정보 목적 외 이용·제공 | 수집 목적 외 사용 금지 | 마케팅·통계·연구 목적 활용 시 별도 동의 또는 가명처리 |
| 3.2.5 가명정보 처리 | 가명처리·결합·재식별 방지 | 가명처리 절차서, 추가정보 분리 보관, 결합 신청 |

## 3.3 개인정보 제공 시 보호조치 (3 개)

'남에게 넘길 때'의 통제입니다. 위탁·재위탁·국외이전·영업양도 — 모두 이 단계에 들어갑니다. 결함이 가장 많은 영역 중 하나이며, 위반 시 과징금이 가장 큰 영역이기도 합니다.

| 통제 | 내 용 | 심사 포인트 |
|---|---|---|
| 3.3.1 개인정보 제 3 자 제공 | 제 3 자 제공 동의, 제공 항목·목적·보유기간 | 제공받는 자 '특정'되어야 함 ('~ 등' 금지) |
| 3.3.2 업무 위탁에 따른 정보주체 고지 | 위탁 시 처리방침 공개·통지 | 재위탁 사전 승인, 처리방침 즉시 갱신 |
| 3.3.3 영업의 양도 등에 따른 개인정보 이전 | 영업양도·합병 시 정보주체 통지 | 이전 사실·이전받는 자·연락처 사전 통지 |

**■ 3.3 영역의 '단골 결함'**

- 수탁사 일부가 위탁자 동의 없이 재위탁한 경우

- 처리방침의 위탁 사항에 일부 수탁사·업무가 누락된 경우
- 수탁사 변경 후 처리방침이 즉시 갱신되지 않은 경우
- 제공 동의 시 '제공받는 자'를 '제휴사 등' 형태로 포괄적으로만 안내
- 영업양도 시 정보주체 통지가 누락되거나 시점이 늦어진 경우

## 3.4 개인정보 파기 시 보호조치 (2 개)

'끝맺음을 잘 해야 한다.' 보유기간이 지났는데도 데이터가 남아 있는 사례가 매우 흔하며, 이는 즉시 결함입니다.

| 통제 | 내 용 | 심사 포인트 |
|---|---|---|
| 3.4.1 개인정보의 파기 | 보유기간 만료 시 지체 없이 파기 | 파기 기록(일시·항목·방법·담당자) 보관 |
| 3.4.2 처리목적 달성 후 보유 시 조치 | 법령 의무로 보관 시 분리 보관 | 별도 DB·접근권한 분리, 활용 금지 명시 |

## 3.5 정보주체 권리보호 (2 개)

개보법이 정보주체에게 부여하는 권리를 회사가 어떻게 보장하는지 보는 영역입니다. 2023 년 개정법으로 '이전권'과 '자동화된 의사결정 거부·설명 요구권'이 추가되어 통제 범위가 넓어졌습니다.

| 통제 | 내 용 | 심사 포인트 |
|---|---|---|
| 3.5.1 개인정보 처리방침 공개 | 처리방침 작성·공개·갱신 | 홈페이지 첫 화면 한 클릭 접근, 변경 이력 보관 |
| 3.5.2 정보주체 권리보장 | 열람·정정·삭제·처리정지·이전·자동화 결정 거부 | 신청 절차·답변 기한(10 일) 준수, 거부 시 사유 통지 |

**'처리방침'은 ISMS-P 심사의 '얼굴'**

심사관이 회사의 개인정보 운영 수준을 판단할 때 가장 먼저 확인하는 문서가 '개인정보 처리방침'입니다. 처리방침에 적힌 항목·목적·보관기간·위탁 내용이 실제 운영과 일치하지 않으면 곧바로 결함이 됩니다. 처리방침은 '마케팅 문구'가 아니라 '선언과 약속'이라는 점을 잊지 마세요.

# 10. 위탁 · 제 3 자 제공 · 국외이전 완벽 정리

ISMS-P 결함 중 절반 가까이가 이 세 가지 — 위탁, 제 3 자 제공, 국외이전 — 영역에서 나옵니다. 용어가 비슷해 헷갈리지만 법적 의미는 완전히 다릅니다. 표 하나로 정리합니다.

| 구 분 | 성 격 | 동 의 | 처리방침 공개 |
|---|---|---|---|
| 업무 위탁 | 회사 '대신' 처리 (CRM, 콜센터, 물류) | 별도 동의 불요 (단, 마케팅 위탁은 동의 필요) | '위탁 사항'으로 공개 의무 |
| 제 3 자 제공 | 독립적인 제 3 자가 '자기 목적'으로 사용 (제휴사, 공동마케팅) | 별도 동의 필수 | '제 3 자 제공 사항'으로 공개 |
| 국외 이전 | 국외로 제공·위탁·보관 | 별도 동의 필수 (예외 7 가지 있음) | '국외이전 사항'으로 공개 |

## 위탁 — '우리 일을 대신 해주는 곳'

수탁사는 위탁자(우리 회사)의 '대리인' 격입니다. 그래서 별도 동의를 받지 않고도 위탁이 가능하지만, 그 대신 위탁자가 수탁사를 '끝까지 관리'해야 하는 책임을 집니다.

- 위탁 계약서에 9 가지 필수 사항 포함 (개보법 시행령 제 28 조)
- 수탁사에 대한 정기 점검·교육 — 연 1 회 이상 권장
- 재위탁 시 위탁자의 사전 서면 동의 — 가장 자주 결함
- 처리방침에 '위탁받는 자 + 위탁 업무 내용' 공개
- 수탁사 변경 시 처리방침 즉시 갱신 — 지연 시 결함

## 제 3 자 제공 — '남에게 넘기는 것'

제 3 자는 자기 목적으로 정보를 사용합니다. 그래서 정보주체에게 '반드시 별도 동의'를 받아야 합니다. 동의 화면에서 '제공받는 자'를 명확히 특정해야 하며 '제휴사 등' 같은 포괄 표현은 결함입니다.

- 제 3 자 제공 동의 시 5 가지 고지 사항 (제공받는 자, 목적, 항목, 보유기간, 거부권·불이익)
- 제공받는 자가 변경되면 재동의 필수
- 제공 기록(누구에게, 언제, 어떤 항목을 줬는지) 보관

## 국외이전 — '대한민국 밖으로 나가는 것'

개보법 제 28 조의 8 은 개인정보의 국외이전을 원칙적으로 금지하며, 7 가지 예외 중 하나에 해당해야 가능합니다. 글로벌 클라우드(AWS·GCP·Azure)의 미국·일본 리전을 사용하는 것도 국외이전에 해당할 수 있어, 한국 기업 대부분이 영향을 받습니다.

**■ 국외이전이 가능한 7 가지 경우 (제 28 조의 8 제 1 항)**

1. 정보주체로부터 국외이전에 관한 별도 동의를 받은 경우
2. 법률·조약·국제협정에 특별한 규정이 있는 경우
3. 정보주체와의 계약 체결·이행을 위해 위탁·보관이 필요한 경우 (계약 내용 또는 처리방침에 공개 시)
4. 이전받는 자가 '개인정보보호 인증'을 받은 경우
5. 이전 대상국이 '적정 보호 수준' 인증을 받은 경우 (개인정보위 고시)
6. 정보주체의 명백한 이익을 위해 필요한 경우
7. 국가안전보장 등 공익적 사유

**■ 국외이전 동의 시 5 가지 고지 사항**

- 이전받는 자의 성명·연락처
- 이전되는 항목

- 이전되는 국가, 시기, 방법
- 이전받는 자의 이용 목적·보유 기간
- 이전을 거부하는 방법·절차·거부의 효과

**글로벌 클라우드를 쓰는 모든 회사의 숙제**

AWS Seoul 리전을 쓰면 '국내 보관'이지만, 동시에 사용하는 CloudFront·Route 53·SES 같은 서비스는 글로벌 인프라이므로 국외이전에 해당할 수 있습니다. '우리는 한국 리전이라 괜찮다'는 착각이 가장 자주 결함을 만듭니다. 처리방침에 '이용 인프라가 글로벌 분산되어 있음'을 정확히 기재하고, AWS GDPR/Personal Information Protection 부속서 같은 계약을 함께 챙기세요.

# 11. 가명정보 · 자동화 의사결정 · 마이데이터 (2024 업데이트)

최근 5 년간 한국 개인정보 환경에서 가장 큰 변화를 만든 세 가지 키워드 — 가명정보, 자동화된 의사결정, 마이데이터 — 를 ISMS-P 관점에서 정리합니다.

## 가명정보 (Pseudonymized Data)

가명정보는 '추가 정보를 사용하지 않고는 특정 개인을 알아볼 수 없도록 처리한 정보'입니다. 2020 년 데이터 3 법 개정으로 등장했고, 통계 작성·과학적 연구·공익적 기록 보존 등 '목적이 정해진 경우'에 한해 정보주체 동의 없이 처리·결합이 가능합니다.

**■ ISMS-P 통제 3.2.5 에서 점검하는 것**

- 가명처리 절차서·기록 — 어떤 항목을 어떻게 가명화했는가
- 추가 정보(매핑 키)의 분리 보관과 접근통제
- 결합 신청 — 가명정보 결합은 '결합전문기관'을 통해서만
- 재식별 시도 금지 — 위반 시 형사처벌
- 비정형 데이터 가명처리(2024 추가) — 이미지·음성·영상의 식별 위험성 검토

## 자동화된 의사결정 (Automated Decision-Making)

AI·머신러닝이 개인의 권리·의무에 중대한 영향을 미치는 결정(예: 신용평가, 채용 서류 자동 탈락, 보험 인수 거부)을 내리는 경우, 정보주체에게 다음 권리가 부여됩니다.

- 거부할 권리 — 자동화된 의사결정 적용을 거부하고 '사람의 검토' 요구
- 설명 요구권 — 결정의 기준·이유·결과에 대한 설명 요구
- 이의 제기권 — 결정 결과에 이의를 제기하고 재검토 요구

ISMS-P 통제 3.2.6 은 회사가 이러한 권리를 보장하는 절차를 갖추고 있는지 점검합니다. AI 모델을 도입한 회사라면 '우리 모델이 자동화된 의사결정에 해당하는가'를 가장 먼저 판단해야 합니다.

## 마이데이터 (개인정보 이전 요구권)

정보주체가 자기 정보를 '다른 사업자에게 이전해 달라'고 요구할 수 있는 권리입니다. 금융 분야는 이미 시행 중이며, 2024 년 시행령 개정으로 전 분야 마이데이터로 확장될 예정입니다. ISMS-P 관점에서는 다음과 같은 통제가 추가됩니다.

- 이전 가능한 항목·형식의 표준화 (구조화된 데이터)
- 이전 요청 처리 절차 — 신원 확인, 이전 방법, 처리 기한
- 이전 기록 — 누구에게, 어떤 항목을, 언제 이전했는가
- 이전 시 보안 조치 — API 인증·암호화

**'우리 회사도 마이데이터 사업자가 되는가'**

마이데이터의 적용 대상은 시행령 개정에 따라 분야별·단계적으로 확대됩니다. 모든 회사가 '마이데이터 사업자'가 되는 것은 아니지만, '이전 요구를 받는 측'으로서 정보주체의 이전 요구에 대응할 의무가 있습니다. 회원 정보가 표준 형식으로 추출 가능한지 시스템 차원에서 미리 점검해 두세요.

# 12. 취득 절차 — 신청부터 인증서까지

ISMS-P 인증 취득은 4 단계로 진행됩니다. ISMS 와 절차 자체는 동일하지만, 심사 깊이와 일수가 다릅니다.

| 단계 | 주요 활동 | 산출물 | 소요 기간 |
|---|---|---|---|
| ① 신청 | 공문, 신청서, 운영명세서 제출 | 신청 접수증 | 1~2 주 |
| ② 계약 | 수수료 산정, 계약 체결 | 계약서, 수수료 납입 | 2~3 주 |
| ③ 예비점검 | 심사팀장 사전 방문 점검 | 사전 결함 리스트 | 1~2 주 |
| ④ 본 심사 | 문서·인터뷰·시스템 심사 | 심사보고서·결함보고서 | ISMS-P 7~10 일 |
| ⑤ 보완조치 | 결함 시정·증빙 제출 | 보완조치내역서 | 30~40 일 |
| ⑥ 인증의결 | KISA 인증위원회 심의 | 인증서 발급 | 2~4 주 |

## ISMS 와 다른 점

- 본 심사 일수가 ISMS(통상 5 일) 대비 2~4 일 더 길다 (개인정보 처리시스템 점검 시간)
- 심사팀에 '개인정보 분야 심사원'이 별도 포함됨
- 인터뷰 대상이 정보보호팀 외에 CPO·법무·CS·마케팅까지 확장
- 처리방침·동의 화면 등 정보주체 접점 자료를 별도 검증
- 법령 준수 검토(법적 요구사항 매핑)에 개보법 비중이 압도적

**'신청 시점'이 가장 중요한 결정**

ISMS-P 는 '최소 2 개월 운영 증적'이 필수입니다. 정책 문서를 만든 직후 신청하면 거절됩니다. 권장은 '운영 시작 후 3 개월 시점'에 신청하는 것입니다. 의무대상 마감(다음 해 8 월 31 일)에 쫓겨 무리하게 일정을 당기면 결함이 폭증해 오히려 인증이 늦어집니다.

# 13. 비용은 얼마나 드는가

ISMS-P 인증 비용은 '심사 수수료'만 보면 1,000~1,800 만 원 수준이지만, 컨설팅·구축·운영을 모두 포함한 '진짜 총비용'은 그보다 훨씬 큽니다. 회사 규모·범위·기존 보안 수준에 따라 달라지지만, 다음 4 개 카테고리로 보면 의사결정에 충분합니다.

| 비용 항목 | 범위 | 전형적 금액 |
|---|---|---|
| ① 심사 수수료 | 심사기관 직접 납부 (인건비 + 직접경비) | ISMS-P 1,000~1,800 만 원<br>(간편인증 600~1,100 만 원) |
| ② 컨설팅 비용 | 사전 준비, 위험평가, 문서화, 예비점검 지원 | 5,000 만 원 ~ 1 억 5,000 만 원 |
| ③ 시스템 구축 | DLP, 접근통제, 로그관리, 망분리, 암호화 솔루션 | 3,000 만 원 ~ 수억 원 |
| ④ 내부 인건비·간접비 | 담당자 투입, 교육비, 부대비용 | 프로젝트당 3,000 만 원 이상 |

## ISMS 와 비용 차이

ISMS 와 비교했을 때 ISMS-P 의 추가 비용은 통상 30~50% 수준입니다. 그 차이는 다음 영역에서 발생합니다.

- 컨설팅 — 개인정보 처리 흐름도, 처리방침 검토, 위탁 계약 정비 (+1,500 만~3,000 만 원)
- 시스템 — 망분리, 가명처리 도구, 동의관리 시스템(CMP) 도입 (+1,000 만 원~억대)
- 심사 수수료 — ISMS-P 가 ISMS 보다 약 200~400 만 원 더 비쌈

## 정부 지원사업 — 적극 활용해야 할 자원

KISA·과기정통부·개인정보위는 매년 다양한 ISMS-P 관련 지원사업을 운영합니다.

- '정보보호 인증 컨설팅 지원사업' — 매출 800 억 원 미만 중소·중견기업 컨설팅비 50~70% 지원

- ‘개인정보 영향평가(PIA) 지원’ — 공공기관·대용량 처리 기관 영향평가 비용 지원
- ‘CISO·CPO 교육비 지원’ — 책임자 교육 이수비 일부 지원
- ‘중소기업 정보보호 솔루션 도입 지원’ — 보안 솔루션 도입 비용 일부 지원

지원사업은 매년 공고 일정·예산이 다르므로, KISA 홈페이지의 ‘기업지원’ 메뉴와 개인정보위의 ‘기업지원’ 메뉴를 1~2 월에 반드시 확인하세요.

# 14. 기간은 얼마나 걸리는가

'준비 시작'부터 '인증서 수령'까지 ISMS-P 는 평균 7~9 개월이 소요됩니다. ISMS 보다 1~2 개월 더 길게 잡는 것이 안전합니다. 22 개 추가 통제의 운영 증적을 쌓는 데 시간이 더 필요하기 때문입니다.

| 월차 | 주요 활동 | 마일스톤 |
|---|---|---|
| M1 | 착수, 인증범위 확정, 컨설팅사 선정, 갭 분석 | 범위 명세서, 갭 분석 보고서 |
| M2 | 현황 분석, 개인정보 흐름도 작성, 위험평가 | 흐름도, 위험평가 보고서 |
| M3 | 정책·지침 수립, 처리방침 정비, 동의 화면 개선 | 정책서 v1.0, 처리방침 v2.0 |
| M4 | 통제 구현, 위탁 계약 정비, 동의관리 시스템 구축 | 보호대책 운영 시작 |
| M5 | 운영 증적 누적, 보안교육·CPO 교육 실시 | 교육 이수 기록 |
| M6 | 예비점검, 결함 보완, 내부심사 | 예비점검 보고서 |
| M7 | 인증 신청, 본 심사 (7~10 일) | 심사·결함 보고서 |
| M8 | 결함 보완, 보완조치 제출 | 보완조치내역서 |
| M9 | 인증위원회 의결, 인증서 발급 | 인증서 ✦ |

## ISMS-P 일정에서 가장 시간이 걸리는 구간

- M3 처리방침 정비 — 법무·기획·CS·마케팅 부서 협의로 2~4 주가 걸리는 경우 흔함
- M4 위탁 계약 정비 — 수십 개의 수탁사 계약을 일괄 갱신해야 함
- M4 동의관리 — 회원가입·앱 권한 화면 개선은 개발 일정과 충돌할 수 있음
- M5 운영 증적 — 최소 2 개월, 권장 3 개월 이상 누적 필요

**'서비스 개편과 인증을 동시에'는 매우 어렵다**

ISMS-P 준비 중 회사가 큰 서비스 개편(앱 리뉴얼·홈페이지 리뉴얼)을 진행하면 일정이 크게 흔들립니다. 처리방침·동의 화면이 두 번 바뀌고, 운영 증적이 무효화되는 경우가 많습니다. 인증

준비를 시작하면 최소 6 개월간 '큰 서비스 개편 동결(Code Freeze for Privacy)'을 권장합니다.

# 15. 사후관리 — 사후심사와 갱신심사

ISMS-P 인증서의 유효기간은 발급일로부터 3 년입니다. 매년 사후심사, 3 년 차에 갱신심사를 받아야 인증이 유지됩니다.

| 연차 | 심사 종류 | 주요 점검 | 수수료 수준 |
|---|---|---|---|
| 1 년차 | 최초심사 | 전 통제 102 개 | 100% (기준) |
| 2 년차 | 사후심사 | 운영 적정성, 변경사항, 결함 후속조치 | 약 50~70% |
| 3 년차 | 사후심사 | 운영 적정성, 변경사항, 결함 후속조치 | 약 50~70% |
| 4 년차 | 갱신심사 | 전 통제 재심사 (최초 수준) | 약 80~100% |

## 사후심사에서 ISMS-P 가 특히 주목하는 것

- 지난 1 년간 처리방침 변경 이력 — 변경 사유와 정보주체 통지
- 지난 1 년간 신규 도입한 시스템·서비스의 개인정보 영향평가
- 지난 1 년간 위탁사 변경 이력과 처리방침 갱신
- 지난 1 년간 정보주체 권리 행사 처리 기록 (열람·정정·삭제 요청 건수와 처리)
- 지난 1 년간 개인정보 유출·침해 사고 발생 여부와 신고 절차

이 다섯 가지가 '기록으로 남아 있지 않으면' 사후심사에서 결함이 도출됩니다. 즉 ISMS-P 는 단순한 '인증 받음'이 아니라, '기록의 누적'이 핵심입니다.

# 16. 개인정보 분야 결함 사례 TOP 10

KISA 의 연도별 결함 통계와 컨설팅 현장의 경험을 바탕으로, ISMS-P 심사에서 'P 영역'에서 가장 자주 도출되는 결함 10 가지를 추렸습니다. 인증 준비 시 우선적으로 점검해야 할 '단골 결함'입니다.

- **TOP 1. 처리방침과 실제 운영의 불일치**

  처리방침에 적힌 수집 항목·보유기간·위탁 사항이 실제와 다른 경우. 가장 흔한 결함이며, 한 번 도출되면 비슷한 결함이 줄줄이 추가 도출됩니다.

- **TOP 2. 필수·선택 동의 미분리**

  회원가입 시 필수 동의와 선택 동의가 한 체크박스로 묶여 있어 정보주체가 '선택권'을 행사할 수 없는 경우. 개인정보위 시정명령 단골 사항입니다.

- **TOP 3. 위탁사 처리방침 미공개·재위탁 미동의**

  처리방침에 일부 수탁사가 누락되거나, 수탁사가 재위탁한 사실을 위탁자가 모르는 경우. 클라우드 위탁에서 특히 자주 발생합니다.

- **TOP 4. 국외이전 동의·고지 부족**

  글로벌 클라우드·해외 분석 도구 사용 시 국외이전 동의와 5 가지 고지 사항이 누락되는 경우. '우리는 한국 리전이라 괜찮다'는 착각이 결함으로 이어집니다.

- **TOP 5. 만 14 세 미만 법정대리인 동의 부실**

  법정대리인 확인 절차가 '이름만 입력' 수준이거나 아예 없는 경우. 13 세 이하 회원이 가입 가능한 서비스에서 자주 도출됩니다.

- **TOP 6. 주민번호 처리 법적 근거 미확보·대체수단 미제공**

법령상 근거 없이 주민번호를 수집하거나, 수집하더라도 i-PIN 같은 대체수단을 제공하지 않은 경우.

### ▸ TOP 7. 보유기간 만료 데이터 미파기

보유기간이 지났는데 데이터가 운영 DB 에 남아 있거나, 분리 보관 없이 활용 가능한 상태로 방치된 경우. 파기 정책은 있지만 자동화가 안 된 회사에서 흔합니다.

### ▸ TOP 8. 정보주체 권리 행사 절차 미흡

열람·정정·삭제 요청을 받을 창구가 없거나, 요청 후 10 일 이내 답변이 이루어지지 않는 경우. '이메일로만 받는다'는 회사가 의외로 많습니다.

### ▸ TOP 9. 접속기록·개인정보 처리 로그 보관 미흡

안전성 확보조치 기준상 접속기록은 1 년 이상 보관해야 하나, 실제로는 6 개월만 보관하거나 위·변조 가능한 상태로 방치된 경우.

### ▸ TOP 10. 개인정보 영향평가(PIA) 미실시

공공기관 또는 대용량 개인정보 처리시스템 신규 구축 시 PIA 가 의무인데도 미실시한 경우. 결함 외에 별도 행정처분 대상이기도 합니다.

**'P' 영역 결함의 공통점**

TOP 10 결함의 공통점은 '정책·약관·처리방침에는 적혀 있는데, 실제 화면·계약·운영이 따라가지 않는다'는 것입니다. '선언과 운영의 일치'를 매년 점검하는 것이 ISMS-P 유지의 핵심입니다.

# 17. ISMS-P 인증심사원 자격증

회사 내부에 ISMS-P 인증심사원 자격을 가진 직원이 한 명만 있어도 인증 준비·운영의 부담이 절반 가까이 줄어듭니다. 또한 보안 컨설팅·심사 분야의 핵심 자격증으로, 정보보안 직군의 커리어 패스에서 가장 가치 있는 자격증 중 하나로 꼽힙니다.

## 자격 요건

- 4 년제 대학 졸업 이상 또는 동등 학력
- 정보보호 경력 1 년 이상 (필수)
- 개인정보보호 경력 1 년 이상 (필수)
- 정보보호·개인정보보호·정보기술 경력 합산 6 년 이상

## 취득 절차

1. 응시 자격 서류 검토 (KISA)
2. 필기시험 — 객관식 + 단답형
3. 양성과정 (KISA 주관, 5 일) — 필기 합격자만 수강
4. 실기 평가 — 모의 심사 시나리오
5. 자격 부여 — 통과자에게 'ISMS-P 인증심사원' 자격 부여

## 난이도와 합격률

ISMS-P 인증심사원 자격검정은 정보보안 분야 자격증 중 '가장 어려운 시험'으로 꼽힙니다. 합격률은 5% 미만으로 알려져 있고, 시험 범위가 정보보안 + 개보법·정보통신망법 + 안전성 확보조치 기준 + 심사 실무까지 매우 광범위합니다. 응시 전 6 개월 이상의 집중 학습이 권장됩니다.

### 내부에 자격자가 있으면 무엇이 좋은가

인증심사원 자격자는 사내 '예비 심사'를 직접 수행할 수 있어 외부 컨설팅 의존도를 크게 낮출 수 있습니다. 또한 인증기관과의 커뮤니케이션이 매끄러워지고, 사후심사 결함 대응도 빨라집니다.

정보보안팀에 한 명, CPO 팀에 한 명, 두 명만 있어도 인증 운영이 훨씬 수월해집니다.

# 18. 인증 준비 체크리스트

본 심사 전 반드시 점검해야 할 항목을 영역별로 정리했습니다. 일반 ISMS 영역은 압축하고, 'P' 영역에 가중치를 두었습니다.

### [조직과 거버넌스]

- ☐ 최고경영자가 정보보호 + 개인정보보호 의지를 공식 문서로 표명했는가
- ☐ CISO 와 CPO 를 임원급으로 지정하고 신고를 완료했는가
- ☐ 정보보호 위원회·개인정보보호 위원회가 정기 개최되는가
- ☐ 조직도와 직무기술서에 정보보호·개인정보 책임이 명시되어 있는가

### [수집 단계 (3.1)]

- ☐ 회원가입 화면의 필수·선택 동의가 분리되어 있는가
- ☐ 동의 시 수집 항목·이용 목적·보유 기간이 모두 표시되는가
- ☐ 민감정보·고유식별정보의 별도 동의가 분리되어 있는가
- ☐ 주민번호 입력란이 있다면 i-PIN 등 대체수단이 함께 제공되는가
- ☐ 만 14 세 미만 가입 시 법정대리인 확인 절차가 작동하는가
- ☐ CCTV 설치 위치마다 안내판이 부착되어 있는가

### [보유·이용 단계 (3.2)]

- ☐ 개인정보 처리 흐름도가 작성되어 있고 최신 상태인가
- ☐ 수집 목적 외 이용 시 별도 동의 또는 가명처리 절차가 있는가
- ☐ 앱이 요구하는 단말 권한이 '꼭 필요한 것'으로 최소화되어 있는가
- ☐ 가명처리를 한다면 절차서·기록·추가정보 분리 보관이 운영되는가
- ☐ AI 모델이 자동화된 의사결정에 해당하면 권리 보장 절차가 있는가

**[제공 단계 (3.3)]**

- □ 제 3 자 제공 동의에서 '제공받는 자'가 '특정'되어 있는가
- □ 위탁 계약서에 9 가지 필수 사항이 모두 포함되어 있는가
- □ 수탁사 재위탁 시 위탁자의 사전 서면 동의를 받는가
- □ 수탁사 변경 시 처리방침이 즉시 갱신되는가
- □ 국외이전 시 5 가지 고지 사항이 동의 화면에 표시되는가
- □ 글로벌 클라우드 사용 사실이 처리방침에 정확히 기재되어 있는가

**[파기 단계 (3.4)]**

- □ 보유기간 만료 데이터의 자동 파기 또는 분리 보관이 작동하는가
- □ 파기 기록(일시·항목·방법·담당자)이 보관되는가
- □ 법령 의무로 보관하는 데이터가 별도 DB·권한으로 분리되어 있는가

**[정보주체 권리 (3.5)]**

- □ 처리방침이 홈페이지 첫 화면에서 한 클릭으로 접근되는가
- □ 처리방침 변경 이력이 보관되어 있는가
- □ 열람·정정·삭제·처리정지·이전 요청 창구가 있는가
- □ 요청 후 10 일 이내 답변·처리가 이루어지는가
- □ 거부 시 사유 통지와 이의 제기 절차가 있는가

**[기술적 안전조치 (안전성 확보조치 기준)]**

- □ 관리자 계정에 다중 인증(MFA)이 적용되어 있는가
- □ 개인정보 처리시스템 접속기록이 1 년(또는 2 년) 이상 보관되는가
- □ 접속기록을 월 1 회 이상 점검하고 그 기록이 있는가
- □ 개인정보 저장·전송 시 암호화가 모두 적용되는가

- □ 개인정보 처리시스템과 일반 시스템의 망분리가 적용되는가
- □ 악성코드 방지·보안 패치 정기 적용 기록이 있는가

**[사고 대응]**

- □ 개인정보 유출 사고 신고 절차(24 시간/72 시간)가 매뉴얼화되어 있는가
- □ 최근 1 년 이내 사고 대응 모의훈련을 실시했는가
- □ 정보주체에게 통지하는 5 가지 고지 사항이 정의되어 있는가

# 19. 자주 묻는 질문 (FAQ)

### Q1. ISMS 만 받고 ISMS-P 는 안 받아도 되나요?

법적으로는 의무대상이라도 ISMS·ISMS-P 중 '하나'만 받으면 충분합니다. 다만 회원가입형 서비스, 결제 처리, 마케팅 동의 등을 운영한다면 사실상 ISMS-P 가 필요합니다. ISMS 만 받으면 사고 발생 시 '개인정보 안전조치 이행'의 입증이 부분적이어서 손해배상·과징금 부담이 커집니다.

### Q2. 처리방침과 약관(이용약관)이 다른 건가요?

다릅니다. 약관은 '회사와 이용자 간 계약 조건'이고, 처리방침은 '개인정보 처리에 대한 회사의 선언'입니다. 약관에 동의했다고 처리방침이 자동으로 동의되는 것이 아니며, 처리방침은 '동의 대상'이 아니라 '공개 의무' 대상입니다.

### Q3. AWS·GCP 를 쓰면 무조건 국외이전인가요?

'저장 리전'이 한국이면 국외이전이 아닙니다. 그러나 AWS 의 IAM·CloudTrail·SES 같은 글로벌 서비스는 미국 본사를 거치므로 국외이전에 해당할 수 있습니다. 또한 백업·재해복구가 다른 리전으로 자동 복제된다면 그 시점부터 국외이전입니다. 클라우드 아키텍처 전체를 '데이터 흐름' 관점에서 점검하세요.

### Q4. 마케팅 동의를 '기본 체크'로 받을 수 있나요?

절대 안 됩니다. 마케팅·광고 등 '선택 동의'는 '기본값으로 체크되지 않은 상태'에서 정보주체가 능동적으로 체크해야 유효합니다. 다크 패턴(어두운 색·작은 글씨·숨김 처리)은 동의를 무효로 만듭니다. 이 부분은 개인정보위 행정처분 단골 사항입니다.

### Q5. CPO 가 반드시 임원이어야 하나요?

법령은 '사업주 또는 대표자, 또는 개인정보 처리에 관한 업무를 총괄해서 수행하는 자'로 규정하고 있어, 반드시 등기 임원일 필요는 없습니다. 다만 실질적 '의사결정 권한'이 있는

직급이어야 하며, 심사관은 CPO 가 위원회 안건을 직접 결정할 수 있는 위치에 있는지 확인합니다.

### Q6. 외국 본사가 있고 한국 지사인 경우 어떻게 하나요?

한국 지사가 '개인정보 처리자'의 지위라면 한국 법인 명의로 ISMS-P 를 받아야 합니다. 본사 시스템을 사용하더라도 그 흐름이 '국외이전'으로 분류되어 처리방침·동의에 반영되어야 합니다. 국내 거래처의 신뢰를 위해서도 본사 인증서 대신 한국 법인 명의 ISMS-P 를 권장합니다.

### Q7. ISMS-P 를 받은 후에도 개인정보 사고가 나면 책임이 면제되나요?

면제되지 않습니다. 그러나 '적정 보호조치 + 개인정보 안전조치를 이행하고 있었다'는 강력한 정황 증거가 됩니다. 과징금 산정 시 '위반자의 노력'이 감경 사유로 작용하고, 손해배상 소송에서도 고의·중과실 추정을 막는 데 도움이 됩니다.

### Q8. 개인정보 영향평가(PIA)와 ISMS-P 는 무엇이 다른가요?

PIA 는 '새 시스템·서비스 도입 전'에 개인정보 위험을 사전 분석하는 절차이고, ISMS-P 는 '운영 중인 관리체계'를 검증하는 인증입니다. 공공기관·대용량 처리기관은 PIA 가 법적 의무이며, ISMS-P 심사 시 PIA 결과를 위험평가 입력으로 활용해야 합니다. 한 마디로 PIA 는 '기획', ISMS-P 는 '운영'입니다.

### Q9. 스타트업도 ISMS-P 를 받을 수 있나요?

받을 수 있습니다. 의무대상이 아니라면 2024 년부터 시행된 '간편인증제'를 활용하면 통제 수가 절반 가까이 줄어들고 수수료도 600~1,100 만 원으로 인하됩니다. B2B SaaS·핀테크·헬스케어 분야 스타트업이 영업 자격으로 ISMS-P 를 받는 사례가 빠르게 늘고 있습니다.

### Q10. ISO 27701(개인정보 관리체계 국제표준)과 ISMS-P 는 어떻게 다른가요?

ISO 27701 은 ISO 27001 기반의 '개인정보 관리체계 확장 표준'이며 글로벌 인증입니다.

ISMS-P 는 한국형 통합 인증입니다. 통제 수준은 비슷하지만 법적 매핑이 다릅니다(ISMS-P 는 개보법 매핑, ISO 27701 은 GDPR 매핑이 강합니다). 글로벌 영업이 본격적이라면 두 인증을 함께 받는 것이 효과적입니다.

# 20. 참고자료 및 공식 사이트

## 공식 사이트

| 기관/사이트 | 주소 | 용도 |
|---|---|---|
| KISA ISMS-P 누리집 | isms.kisa.or.kr | 제도 안내, 신청서, 인증기준 안내서 |
| ISMS-P 누리집(별도) | isms-p.or.kr | 심사기관 통합 안내, 자격검정 |
| 개인정보 포털 | privacy.go.kr | 처리방침 작성 가이드, 영향평가 가이드 |
| 개인정보보호위원회 | pipc.go.kr | 법령 해설, 가명정보 가이드라인, 행정처분 사례 |
| 국가법령정보센터 | law.go.kr | 개인정보보호법·정보통신망법 원문 |
| KAIT 정보보호 인증 | isms.kait.or.kr | 한국정보통신진흥협회 심사기관 |
| OPA 정보보호 인증 | opa.or.kr | 개인정보보호협회 심사기관 |

## 주요 법령·고시

- 개인정보보호법 (2023.3.14. 개정, 2024.3.15. 시행)
- 개인정보보호법 시행령
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47 조
- 개인정보의 안전성 확보조치 기준 (개인정보보호위원회 고시)
- 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시
- ISMS-P 인증기준 안내서 (최신본 2023.11)
- 가명정보 처리 가이드라인 (2024.2 개정)

## 추천 KISA·개보위 자료

- ISMS-P 인증기준 안내서 — 102 개 통제별 점검 가이드
- ISMS-P 결함 사례집 — 연도별 통계와 사례
- ISMS·ISMS-P 간편인증제 안내서
- 개인정보 처리방침 작성 지침
- 개인정보 영향평가(PIA) 수행 안내서
- 기업을 위한 개인정보보호 가이드라인
- 위탁자·수탁자가 알아야 할 개인정보보호
- 국외이전 가이드라인

# 맺음말

이 백서를 끝까지 읽으셨다면 ISMS-P 가 '22 개의 통제'만이 아니라 '회사와 정보주체 사이의 약속'이라는 점을 느끼셨을 겁니다. 개인정보를 받고, 쓰고, 넘기고, 버리고, 권리를 보장하는 모든 단계에서 회사가 무엇을 '선언'했고 그 선언을 '지키고 있는지'를 검증하는 인증입니다.

개인정보를 다루는 일은 점점 더 어려워지고 있습니다. 법은 매년 강화되고, 기술은 빠르게 변하고, 정보주체의 기대 수준은 계속 올라갑니다. 그러나 '약속을 지키는 회사'는 어떤 변화에도 무너지지 않습니다. ISMS-P 는 그 약속을 시스템화하는 가장 좋은 도구입니다. 이 백서가 그 시스템을 만드는 첫 번째 지도가 되기를 바랍니다.

**— 백 지 석 —**