

## 상호 비밀유지계약서

**참고용 템플릿입니다.** 이 문서는 계약을 체결하기 전에 잠재 고객이 당사의 표준 조건을 검토할 수 있도록 자리표시자 (placeholder)와 함께 제공됩니다. 이 문서는 법적 조언이 아니며, 양 당사자가 내용을 채우고 날짜를 기재한 뒤 서명하기 전까지는 구속력을 갖지 않습니다. 체결된 계약이 각 계약건을 규율합니다.

이 상호 비밀유지계약(이하 “계약”)은 [날짜]을 기준으로 다음 당사자 간에 체결됩니다:

[고객 이름], [관할권]에 등록된 회사로, 등록 번호는 [회사 번호], 등록 사무소는 [고객 주소]에 소재한 회사 (이하 “고객”); 그리고

VAVELIO LTD, 잉글랜드와 웨일즈에 등록된 회사로, 등록 번호 16558123, 등록 사무소는 128 City Road, London, EC1V 2NX에 소재한 회사 (이하 “Vavelio”);

각각을 “당사자”라 하고, 함께 “당사자들”이라고 합니다.

### 1. 목적

당사자들은 데이터센터 인프라, 글로벌 네트워크, 보안 아키텍처의 설계, 구축, 운영과 관련된 잠재적 업무 관계를 논의하고자 합니다 (이하 “목적”).

### 2. 비밀정보

“비밀정보”란 본 계약일 이전 또는 이후에, 어느 한 당사자 (이하 “공개자”)가 상대방(이하 “수령자”)에게 목적과 관련하여 어떤 형태로든 공개하는 모든 정보를 의미하며, 기술 설계, 아키텍처, 보안 구성, 사업 계획, 고객 정보, 가격, 재무 정보를 포함합니다. 구두로 공개된 정보는 공개 당시 비밀로 식별되고 14일 이내에 서면으로 확인된 경우에만 비밀정보로 간주됩니다.

제한 없이, 모든 아키텍처 문서, 서비스 설계, 그리고 목적과 관련된 모든 것은 고도로 기밀입니다.

이 계약은 비밀유지에 관한 관습법(common law) 및 Trade Secrets (Enforcement, etc.) Regulations 2018 (SI 2018/597)에 따른 당사자들의 의무를 보완하며 제한하지 않습니다. 단, 비밀정보가 영업비밀(trade secret)을 구성하는 범위에 한합니다.

### 3. 수령자의 의무

수령자는 다음을 준수해야 합니다:

- 모든 비밀정보를 비밀로 유지하고 제3자에게 공개하지 않을 것;
- 비밀정보를 목적을 위해서만 사용할 것;
- 필요한 직원과 계약자로서 최소한 이 계약만큼 보호적인 의무에 구속된 자에게만 공개할 것; 그리고
- 자신의 동급 중요도의 비밀정보에 적용하는 것과 동일한 수준의 주의로 보호할 것. 어떠한 경우에도 합리적인 주의 미만으로 보호해서는 안 됩니다.

## 4. 제외 사항

비밀정보는 다음에 해당하는 정보를 포함하지 않습니다:

- 본 계약 위반 없이 이미 공개되었거나 공개되는 정보;
- 공개 이전에 비밀유지 의무 없이 수령자가 적법하게 보유하고 있던 정보;
- 비밀유지 의무 없이 제3자로부터 수령한 정보; 또는
- 수령자가 비밀정보를 사용하지 않고 독자적으로 개발한 정보.

수령자는 법률, 법원 명령, 또는 관할 규제기관이 요구하는 범위 내에서 비밀정보를 공개할 수 있습니다. 단, 법적으로 허용되는 경우 공개자에게 즉시 통지하고 공개 범위를 요구된 수준으로 제한해야 합니다.

## 5. 공개 금지

고객은 Vavelio의 사전 서면 동의 없이 — 웹사이트, 마케팅 자료, 또는 공개 포럼에서 — Vavelio와 협력하고 있다는 사실을 공개해서는 안 됩니다. 비밀정보를 공개하지 않는 한, 지인 간 대화에서의 사적인 언급은 허용됩니다.

## 6. 고객 정보의 판매 또는 공유 금지

Vavelio는 고객 정보를 제3자에게 판매, 대여, 또는 공유하지 않습니다. 고객 정보는 본 계약에 따른 서비스를 제공하는 목적으로만 사용됩니다. 개인 데이터는 영국 일반 데이터 보호 규정(UK GDPR) 및 Data Protection Act 2018에 따라 처리됩니다.

## 7. 위반 및 보상

본 계약을 위반할 경우, 위반하지 않은 당사자는 관할 법원이 결정한 손해배상을 받을 권리가 있습니다.

별도로, 그리고 법적 의무가 아닌 Vavelio 자체 원칙의 문제로서, Vavelio가 가장 먼저 선호하는 방식은 책임 인정의 표시로 고객에게 고객 월 비용의 두 배에 해당하는 보상을 제공하는 것입니다. 이는 전적으로 Vavelio의 결정입니다. Vavelio가 그러한 보상을 제공하지 않기로 하는 경우, Vavelio는 고객이 이 문제를 공개하고 그에 따라 Vavelio를 평가할 것을 권장합니다. 고객이 그렇게 하는 경우, Vavelio는 결정에 동의하지 않은 이유를 설명하는 자체 성명서를 기꺼이 게시할 것입니다. 제공되는 보상은 고객의 선택에 따라 (a) 향후 서비스에 대한 크레딧, (b) 지급액 환불, 또는 (c) 컨설팅 시간 중 하나로 지급됩니다.

## 8. 인력 및 보안 심사

고객의 직원 또는 계약자는 본 계약(또는 이에 상응하는 비밀유지 서약)에 서명하고 Vavelio가 해당 인물의 신원을 통보받기 전까지 Vavelio에 관한 어떠한 정보에도 접근할 수 없습니다.

계약 건이 물리적 데이터센터 건설과 관련된 경우, Vavelio 관련 구역에 배정된 모든 인력에 대해 심리 또는 정신 적합성 평가가 의무화됩니다. 고객 관련 구역의 경우, 그러한 평가 여부는 전적으로 고객의 판단에 맡깁니다. 모든 평가는 개인의 사전 동의를 받고 적용 가능한 데이터 보호법에 따라 실시되어야 합니다.

모든 Vavelio 관련 구역의 출입 통제는 전적으로 Vavelio가 관리합니다. 해당 구역에 접근해야 하는 사람은 접근이 허용되기 전에 먼저 Vavelio에 등록하고 Vavelio가 요구하는 모든 정보를 제공해야 합니다. 이 구역의 출입은 카드 ID, 지문 스캔, 홍채 스캔의 세 단계 보안으로 보호됩니다. 이 구역에 대한 모든 출입은 카메라로 모니터링됩니다. 신호 차단 장치와 승인되지 않은 전자 기기는 금지됩니다. 입구의 금속 탐지 스캐너는 금속이 감지되면 출입을 차단하며, 금속이 없어질 때까지 출입은 차단된 상태로 유지됩니다.

출입 통제를 위해 수집된 모든 생체 인식 데이터는 암호화된 형태로 고객의 데이터베이스에 저장됩니다. Vavelio는 데이터에 직접 접근할 수 없으며, 오직 Vavelio의 소프트웨어를 통해서만 암호화된 데이터를 검증합니다 — 원본 생체 인식 데이터는 절대 검증하지 않으며, 엄격히 읽기 전용으로만 검증합니다. 각 장치는 자체 테이블에만 접근할 수 있으며, Vavelio는 생체 인식 데이터를 자체적으로 보유하지 않습니다.

고객은 평가를 거부할 권리가 있으며, 이 경우 고객은 웹사이트에 설명된 인계 절차에 따라 파트너십을 해소할 수 있습니다 ([vavel.io/independence](https://vavel.io/independence) 참조).

Vavelio가 고객의 특정 인력이 Vavelio의 인프라 보안에 실질적인 위협이 된다고 합리적으로 판단하는 경우, Vavelio는 해당 판단의 근거를 서면으로 고객에게 설명하고, 해당 인력의 Vavelio 인프라에 대한 모든 접근 권한의 즉각적인 철회를 요구할 수 있습니다.

고객이 Vavelio의 판단이 틀렸다는 것을 입증하는 문서 또는 증거를 제공하지 않으면서 해당 판단에 동의하지 않는 경우, Vavelio는 본 계약 및 고객과의 관련 관계를 해소하고 웹사이트에 설명된 표준 인계 절차를 따를 권리가 있습니다 ([vavel.io/independence](https://vavel.io/independence) 참조).

## 9. 가상 데이터센터 접근

어느 누구도 루트 접근(root access)이나 사용자 인터페이스를 통해서든 데이터센터 노드에 접근할 수 없습니다. 고객은 지정된 엔지니어에게 모든 작업을 요청할 수 있으며, 해당 엔지니어는 자동 확장(autoscaling)을 포함한 작업을 API 게이트웨이를 통해 배포합니다.

직접 접근이 필요한 예외적인 상황에서 Vavelio는 카드 ID 또는 가상 ID를 발급합니다. 이러한 접근에는 엔지니어가 노드 로그인 시점에 현장에 있어야 합니다. 모든 직접 접근은 임시적이며 삼십(30)분으로 제한되고, 이후 자동으로 해제됩니다. 그러한 접근 중 엔지니어는 읽기 전용 접근 권한만 가지며 관리자 접근 권한은 절대 갖지 않습니다.

VINS, VNTP, VDNS를 포함한 모든 Vavelio 제품은 고객의 관할권 밖에서 완전히 운영됩니다.

모든 접근은 Vavelio의 접근 포털인 Kratos를 통해 엄격히 모니터링되며, 사건(case)과 계급(rank) 체계를 갖춘 군사 등급 접근 시스템을 재현합니다. Vavelio가 직원 ID가 오용되었거나 사칭자에 의해 사용되었다고 판단하는 경우, Vavelio는 해당 인물을 완전히 차단하고 새로운 ID 발급을 거부할 수 있습니다.

고객은 자체 애플리케이션 또는 요구사항을 위해 구축된 모든 가상 머신에 대해 직접 관리자 접근 권한을 가집니다. 단, 해당 머신이 Vavelio 관련 서비스가 아닌 경우에 한합니다.

고객은 이러한 가상 머신에 대한 외부 접근을 허용할 수 있습니다. 네트워크 스캐닝 솔루션은 엄격히 금지되며 즉시 차단되고, 가상 머신이 일시적으로 차단될 수 있습니다.

고객이 제3자 벤더에게 자체 가상 머신에 대한 접근 권한을 부여하는 경우, 고객은 벤더의 행위에 대한 모든 책임을 집니다.

제3자 벤더의 모든 로그인은 Vavelio의 PAM 솔루션을 통해 제공되어야 합니다. 원격 데스크톱 소프트웨어, 또는 관련 원격 접속 소프트웨어의 사용은 금지됩니다. Vavelio가 이러한 소프트웨어의 사용을 발견하는 경우, Vavelio는 고객이 상황에 대한 설명을 제공할 때까지 접근을 완전히 차단할 수 있습니다. 모든 서비스는 중단 없이 계속 실행됩니다. 차단되는 것은 접근뿐입니다.

## 10. 계약 기간

이 계약은 당사자들의 업무 관계가 지속되는 전체 기간 — 고객이 Vavelio의 고객으로 있는 한 — 효력을 유지합니다. 관계 종료 후에도 영업비밀을 구성하는 정보에 관한 의무는 무기한 계속됩니다.

11. 정보의 반환

공개자의 서면 요청 또는 본 계약의 종료 시, 수령자는 모든 비밀정보를 지체 없이 반환하거나 파기하고 이를 서면으로 확인해야 합니다.

12. 라이선스 또는 보증 없음

명시적으로 규정된 경우를 제외하고 어떠한 라이선스 또는 기타 권리도 부여되지 않습니다. 비밀정보는 어떠한 종류의 진술이나 보증 없이 “있는 그대로(as is)” 제공됩니다.

13. 진행 의무 없음

이 계약의 어떤 조항도 어느 한쪽 당사자에게 추가 계약 또는 거래를 체결할 의무를 부과하지 않습니다.

14. 준거법

이 계약은 잉글랜드와 웨일즈의 법률에 따라 규율되고 해석됩니다. 당사자들은 잉글랜드와 웨일즈 법원의 전속 관할권에 따르기로 합의합니다. 당사자가 아닌 자는 Contracts (Rights of Third Parties) Act 1999에 따라 이 계약의 어떤 조항도 집행할 권리가 없습니다.

15. 서명

고객 대리 서명

서명

이름 및 직함

날짜

Vavelio LTD 대리 서명

서명

이름 및 직함

날짜