THIRD-PARTY / OUTSOURCED DEVELOPMENT POLICY

Chính sách Phát triển Thuê ngoài và Bên thứ ba

Trust, but Verify • Same Bar as Internal • Clean Offboarding

Tổ chức / Organization	AI Biết Tuốt
Chủ sở hữu / Document Owner	Head of Procurement/Vendor Management, phối hợp Head of Engineering
Phê duyệt / Approved by	Engineering Governance Council
Ngày hiệu lực / Effective Date	17/09/2026
Phiên bản / Version	1.0
Chu kỳ rà soát / Review Cycle	Hằng năm, hoặc ngay khi có thay đổi đáng kể về khung pháp lý/chuẩn bảo mật liên quan đến vendor
Tài liệu cấp trên / Parent Documents	Engineering Constitution v1.0 (Tầng 1); Software Development Governance Policy v1.0 (Tầng 2)
Phân loại / Classification	INTERNAL

SAMPLE DOCUMENT

A. Kiểm soát tài liệu

DOCUMENT CONTROL

Phiên bản	Ngày	Người soạn	Mô tả thay đổi
1.0	17/09/2026	Head of Procurement/Vendor Management	Ban hành lần đầu

B. Mục lục nội dung

CONTENTS

- 1. Mục đích
- 2. Phạm vi áp dụng
- 3. Liên kết với Engineering Constitution
- 4. Định nghĩa
- 5. Yêu cầu bắt buộc
- 6. Vai trò và trách nhiệm
- 7. Đo lường tuân thủ
- 8. Cơ chế ngoại lệ
- 9. Không tuân thủ
- 10. Chủ sở hữu tài liệu và chu kỳ rà soát
- 11. Tài liệu liên quan
- 12. Phê duyệt

1. Mục đích

Chính sách này quy định cụ thể các yêu cầu bắt buộc khi tổ chức thuê ngoài (outsource), hợp tác với nhà thầu (contractor), hoặc sử dụng bất kỳ bên thứ ba nào để thực hiện một phần hoặc toàn bộ công việc phát triển, bảo trì, kiểm thử phần mềm. Mục tiêu là đảm bảo phần mềm do bên thứ ba phát triển đạt cùng một mức độ bảo mật, chất lượng và khả năng kiểm soát như phần mềm do đội ngũ nội bộ phát triển — **không có ngoại lệ "vì là hàng thuê ngoài"**.

Chính sách này là bản mở rộng chi tiết của Điều 5.11 (Phát triển thuê ngoài và bên thứ ba) trong Software Development Governance Policy (SDGP) — tài liệu Tầng 2 "mẹ" của khung quản trị. Các nội dung về SDLC, vai trò chung, cơ chế ngoại lệ và không tuân thủ đã được quy định tại SDGP không được lặp lại ở đây mà được dẫn chiếu trực tiếp.

2. Phạm vi áp dụng

Áp dụng cho mọi trường hợp một bên không phải nhân viên nội bộ — nhà thầu độc lập, công ty gia công phần mềm (outsourcing vendor), đối tác offshore/nearshore, freelancer, thực tập sinh thuê ngoài qua bên thứ ba — tham gia vào bất kỳ khâu nào của vòng đời phát triển phần mềm của tổ chức: viết code, thiết kế kiến trúc, kiểm thử, vận hành hạ tầng, hoặc tư vấn kỹ thuật có quyền truy cập hệ thống/mã nguồn/dữ liệu của tổ chức. Áp dụng cho cả trường hợp vendor thuê lại nhà thầu phụ (sub-processor/fourth party) để thực hiện một phần công việc.

Không áp dụng cho việc mua sắm phần mềm đóng gói (COTS) không có tùy biến mã nguồn. Việc sử dụng thư viện/mã nguồn mở, kể cả khi do vendor đưa vào sản phẩm bàn giao, áp dụng theo Open-Source Software Policy song song với chính sách này (xem Điều 5.4 và Điều 11).

3. Liên kết với Engineering Constitution

TRACEABILITY TO THE 10 PRINCIPLES

#	Nguyên tắc Constitution	Cách TPODP thể hiện
2	Security and Privacy by Design	Đánh giá bảo mật vendor bắt buộc trước khi ký hợp đồng; truy cập tối thiểu, có thời hạn, phân tầng theo rủi ro
3	Quality Is Everyone's Responsibility	Code/artifact vendor giao phải qua đúng gate chất lượng và bảo mật như code nội bộ, không ngoại lệ
4	Segregation of Duties	Vendor không tự phê duyệt/merge sản phẩm của chính mình; review độc lập bởi nội bộ
8	Evidence over Opinion	Đánh giá vendor, giám sát định kỳ và offboarding đều phải có bằng chứng bằng văn bản, không dựa trên cam kết miệng

4. Định nghĩa

- **Nhà cung cấp phát triển phần mềm (Software Development Vendor):** tổ chức hoặc cá nhân bên ngoài được thuê để thực hiện công việc phát triển/bảo trì/kiểm thử phần mềm cho tổ chức.

- **Đánh giá bảo mật nhà cung cấp (Vendor Security Assessment/Due Diligence):** quá trình thẩm định năng lực bảo mật, quy trình phát triển và mức độ tuân thủ của vendor trước khi ký hợp đồng.
- **Phân tầng nhà cung cấp (Vendor Tiering):** việc xếp hạng vendor theo mức độ rủi ro (ví dụ Tier 1 — Trọng yếu, Tier 2 — Cao, Tier 3 — Thấp) dựa trên mức độ nhạy cảm của dữ liệu/hệ thống mà vendor được tiếp cận, làm cơ sở xác định độ sâu đánh giá, kiểm soát truy cập và tần suất giám sát.
- **Nguyên tắc đặc quyền tối thiểu (Principle of Least Privilege):** chỉ cấp cho nhân sự bên thứ ba đúng mức truy cập cần thiết để hoàn thành công việc được giao, không hơn.
- **Nhà thầu phụ/bên thứ tư (Sub-processor/Fourth Party):** bất kỳ bên nào mà vendor thuê lại (subcontract) để thực hiện một phần công việc đã cam kết với tổ chức.
- **SBOM (Software Bill of Materials):** danh mục kê khai đầy đủ các thành phần cấu thành một sản phẩm phần mềm, bao gồm cả thư viện/mã nguồn mở, phục vụ việc rà soát lỗ hổng và giấy phép.
- **Lưu trữ mã nguồn qua bên thứ ba (Source Code Escrow):** thỏa thuận trong đó một bản sao mã nguồn và tài liệu liên quan được lưu giữ bởi một bên trung lập, chỉ được giải phóng cho tổ chức trong các trường hợp đã thỏa thuận trước (vendor phá sản, ngừng hoạt động, hoặc vi phạm nghiêm trọng nghĩa vụ hỗ trợ).
- **Chuyển giao tri thức (Knowledge Transfer):** quá trình vendor bàn giao lại toàn bộ hiểu biết, tài liệu, quyết định thiết kế liên quan đến sản phẩm đã phát triển cho đội ngũ nội bộ.
- **Offboarding nhà cung cấp:** toàn bộ quy trình chấm dứt quan hệ hợp tác kỹ thuật với vendor, bao gồm thu hồi quyền truy cập và xác nhận bàn giao.

5. Yêu cầu bắt buộc

MANDATORY REQUIREMENTS

5.1 Đánh giá bảo mật và năng lực nhà cung cấp trước khi ký hợp đồng

Trước khi ký bất kỳ hợp đồng phát triển phần mềm nào, bộ phận phụ trách (Procurement/Vendor Management phối hợp Engineering và Security) **PHẢI** thực hiện đánh giá bảo mật và năng lực (vendor security assessment/due diligence), đồng thời xếp hạng vendor vào một tầng rủi ro (Vendor Tiering) làm cơ sở cho các kiểm soát ở các điều tiếp theo:

- **Tier 3 — Thấp:** vendor chỉ tiếp cận mã nguồn không nhạy cảm, không có dữ liệu thật. Đánh giá cơ bản (bảng câu hỏi bảo mật, kiểm tra tham chiếu).
- **Tier 2 — Cao:** vendor tiếp cận môi trường staging hoặc dữ liệu đã được ẩn danh hóa. Đánh giá đầy đủ, yêu cầu bằng chứng bảo mật cụ thể (chính sách nội bộ, kết quả kiểm thử bảo mật gần nhất).
- **Tier 1 — Trọng yếu:** vendor tiếp cận hệ thống production, dữ liệu khách hàng, dữ liệu cá nhân, hoặc phát triển các module cốt lõi. Bắt buộc có báo cáo **SOC 2 Type 2** (đánh giá hiệu quả vận hành kiểm soát trong một giai đoạn quan sát, không chấp nhận báo cáo Type 1 vốn chỉ đánh giá thiết kế tại một thời điểm) hoặc chứng nhận ISO/IEC 27001 còn hiệu lực, kèm khảo sát bảo mật chi tiết và quyền audit trực tiếp trước khi ký.

Báo cáo SOC 2 hoặc chứng nhận ISO/IEC 27001 do vendor cung cấp **KHÔNG** được mặc nhiên chấp nhận — đội ngũ đánh giá PHẢI xem xét phạm vi (scope), thời hạn hiệu lực và các ngoại lệ (exceptions) nêu trong báo cáo. Đối với vendor Tier 1, tổ chức **NÊN** yêu cầu vendor cung cấp SBOM cho các sản phẩm/công cụ nội bộ mà vendor sẽ dùng để phát triển, nhằm sàng lọc rủi ro chuỗi cung ứng từ sớm. Kết quả đánh giá và tầng rủi ro được gán PHẢI lưu trữ bằng văn bản và là điều kiện tiên quyết để ký hợp đồng.

Tổ chức **NÊN** tránh phụ thuộc quá mức vào một vendor duy nhất cho các module phần mềm cốt lõi (concentration risk) — mức độ phụ thuộc chấp nhận được do Engineering Governance Council xác định theo từng giai đoạn, và được xem xét lại trong quá trình giám sát định kỳ tại Điều 5.6.

5.2 Điều khoản hợp đồng bắt buộc

Mọi hợp đồng phát triển phần mềm với bên thứ ba PHẢI bao gồm tối thiểu các điều khoản sau:

- **Cam kết bảo mật:** vendor cam kết tuân thủ yêu cầu bảo mật tối thiểu tương đương chính sách bảo mật nội bộ, bao gồm tuân theo Secure Software Development Policy đối với mọi mã nguồn được giao.
- **Quyền sở hữu trí tuệ (IP Ownership):** toàn bộ mã nguồn, tài liệu thiết kế và sản phẩm bàn giao thuộc quyền sở hữu của tổ chức ngay khi được tạo ra/bàn giao, trừ khi có thỏa thuận khác bằng văn bản; vendor không được tái sử dụng/tái phân phối cho bên khác.
- **Quyền audit (Audit Rights):** tổ chức có quyền yêu cầu audit định kỳ hoặc đột xuất đối với quy trình phát triển, môi trường bảo mật và việc tuân thủ hợp đồng của vendor.
- **Kiểm soát nhà thầu phụ (Sub-processor Control):** vendor **KHÔNG ĐƯỢC PHÉP** thuê lại bên thứ tư (sub-processor) để thực hiện công việc đã cam kết nếu chưa được tổ chức phê duyệt bằng văn bản; mọi sub-processor được phê duyệt vẫn phải đáp ứng cùng yêu cầu bảo mật tại Điều 5.1 tương ứng với tầng rủi ro của công việc được giao.
- **Lưu trữ mã nguồn qua bên thứ ba (Source Code Escrow):** đối với vendor Tier 1 phát triển module cốt lõi, hợp đồng **NÊN** quy định thỏa thuận escrow mã nguồn với một bên trung lập, nhằm đảm bảo tính

liên tục nếu vendor phá sản, ngừng hoạt động hoặc vi phạm nghiêm trọng nghĩa vụ hỗ trợ.

- **Chuyển dữ liệu xuyên biên giới:** nếu vendor ở nước ngoài (offshore) và có khả năng tiếp cận dữ liệu cá nhân của người dùng Việt Nam, hợp đồng PHẢI quy định rõ trách nhiệm tuân thủ quy định hiện hành về bảo vệ dữ liệu cá nhân khi chuyển dữ liệu ra nước ngoài (Nghị định 13/2023/NĐ-CP), bao gồm việc phối hợp lập hồ sơ đánh giá tác động khi thuộc trường hợp bắt buộc theo quy định.
- **Nghĩa vụ bảo mật dữ liệu:** vendor cam kết bảo vệ dữ liệu theo đúng phân loại dữ liệu của tổ chức, không sao chép/lưu trữ dữ liệu ngoài phạm vi cần thiết.
- **Nghĩa vụ tuân theo chính sách của bên thuê:** vendor cam kết tuân thủ Secure Software Development Policy, Software Quality Policy và Open-Source Software Policy (nếu có sử dụng mã nguồn mở) trong toàn bộ quá trình thực hiện công việc.
- **Nghĩa vụ thông báo sự cố:** theo quy định tại Điều 5.7.

5.3 Quản lý truy cập cho nhân sự bên thứ ba

- Áp dụng nguyên tắc đặc quyền tối thiểu: nhân sự vendor chỉ được cấp quyền truy cập đúng phạm vi hệ thống/mã nguồn/môi trường cần thiết cho công việc được giao.
- Mỗi nhân sự vendor PHẢI được cấp tài khoản cá nhân riêng biệt, định danh rõ ràng — **KHÔNG ĐƯỢC PHÉP** dùng tài khoản dùng chung (shared account) hoặc tài khoản mượn của nhân viên nội bộ.
- Mọi tài khoản cấp cho vendor PHẢI có thời hạn (time-bound), gắn với thời gian hợp đồng hoặc từng giai đoạn công việc, và PHẢI được rà soát định kỳ.
- Xác thực đa yếu tố (MFA) là bắt buộc đối với mọi tài khoản truy cập cấp cho nhân sự bên thứ ba, không có ngoại lệ.
- Đối với vendor Tier 1 hoặc dự án tiếp cận dữ liệu/hệ thống nhạy cảm, tổ chức **NÊN** yêu cầu nhân sự vendor phát triển thông qua môi trường ảo hóa do tổ chức cấp và kiểm soát (VDI/cloud workspace), hạn chế việc mã nguồn hoặc dữ liệu bị sao chép ra thiết bị cá nhân của vendor.
- Quyền truy cập PHẢI được thu hồi ngay khi nhân sự vendor kết thúc công việc, đổi vai trò, hoặc khi hợp đồng chấm dứt — không chờ đến chu kỳ rà soát định kỳ tiếp theo. Đối với các hệ thống do tổ chức trực tiếp quản lý (IAM/SSO, kho mã nguồn, công cụ quản lý dự án), việc thu hồi PHẢI hoàn tất trong cùng ngày làm việc.

5.4 Review và kiểm soát chất lượng/bảo mật đối với sản phẩm bàn giao

- Mọi mã nguồn, cấu hình hạ tầng (infrastructure as code) hoặc artifact khác do bên thứ ba giao PHẢI đi qua đúng quy trình code review và các security/quality gate tự động (SAST, dependency scanning, kiểm thử) như áp dụng cho mã nguồn nội bộ, theo Secure Software Development Policy và Software Quality Policy. **KHÔNG CÓ** ngoại lệ "vì đây là mã do vendor viết" đối với bất kỳ gate bắt buộc nào trong pipeline.
- Người review và người phê duyệt merge PHẢI là nhân sự nội bộ hoặc người được ủy quyền chính thức của tổ chức — vendor không được tự phê duyệt/merge sản phẩm của chính mình (Segregation of Duties, xem SDGP Điều 5.4).
- Nếu vendor sử dụng thư viện/thành phần mã nguồn mở trong sản phẩm bàn giao, thành phần đó vẫn PHẢI tuân thủ đầy đủ Open-Source Software Policy như khi đội nội bộ tự sử dụng; đối với sản phẩm Tier 1, vendor **NÊN** cung cấp SBOM kèm theo mỗi lần bàn giao để phục vụ rà soát lỗ hổng và giấy phép mã nguồn mở.

5.5 Quy trình offboarding khi kết thúc hợp đồng/dự án

Khi hợp đồng hoặc dự án với vendor kết thúc (dù đúng hạn hay chấm dứt sớm), PHẢI thực hiện đầy đủ:

1. Thu hồi toàn bộ quyền truy cập của mọi tài khoản liên quan đến vendor (hệ thống, mã nguồn, hạ tầng, công cụ cộng tác) ngay trong ngày làm việc kết thúc hợp đồng.
2. Xác nhận bằng văn bản việc chuyển giao tri thức (knowledge transfer) — tài liệu thiết kế, quyết định kỹ thuật quan trọng (ADR nếu có), hướng dẫn vận hành — cho đội ngũ nội bộ tiếp nhận.
3. Xác nhận bàn giao đầy đủ mã nguồn và tài liệu liên quan vào hệ thống quản lý mã nguồn/tài liệu chính thức của tổ chức.
4. Yêu cầu vendor xác nhận bằng văn bản rằng không giữ lại bất kỳ bản sao dữ liệu, mã nguồn hoặc thông tin nội bộ nào ngoài phạm vi được phép sau khi kết thúc hợp đồng.
5. Lưu trữ toàn bộ hồ sơ offboarding làm bằng chứng tuân thủ.

5.6 Giám sát định kỳ trong suốt vòng đời hợp đồng

Việc đánh giá vendor **KHÔNG** dừng lại ở thời điểm ký hợp đồng. Trong suốt thời gian hợp tác, tổ chức PHẢI giám sát định kỳ, với tần suất tương xứng tầng rủi ro (Điều 5.1):

- Hiệu năng thực hiện công việc (chất lượng sản phẩm, tiến độ, số lượng lỗi/sự cố phát sinh).
- Mức độ tuân thủ các điều khoản bảo mật và quy trình đã cam kết trong hợp đồng.
- Hiệu lực của các chứng nhận/báo cáo (SOC 2 Type 2, ISO/IEC 27001...) mà vendor đã cung cấp, để phát hiện kịp thời khi hết hạn hoặc bị thu hồi.
- Mức độ phụ thuộc (concentration risk) và rủi ro phát sinh từ nhà thầu phụ mà vendor sử dụng.

Việc giám sát rủi ro chuỗi cung ứng nên tham chiếu nhóm kiểm soát về quan hệ nhà cung cấp tại ISO/IEC 27001:2022 Annex A (control 5.19 đến 5.22) và các nguyên tắc quản trị rủi ro chuỗi cung ứng an ninh mạng (C-SCRM) theo NIST SP 800-161. Kết quả giám sát PHẢI được lưu trữ bằng văn bản.

5.7 Thông báo sự cố bảo mật liên quan đến vendor

Hợp đồng PHẢI quy định rõ thời hạn tối đa vendor phải thông báo cho tổ chức khi phát hiện sự cố bảo mật liên quan đến hệ thống, mã nguồn hoặc dữ liệu của tổ chức mà vendor đang xử lý, kể cả sự cố xảy ra tại nhà thầu phụ của vendor. Khi nhận được thông báo, sự cố PHẢI được xử lý theo đúng cơ chế ứng phó sự cố và không tuân thủ đã quy định tại SDGP, Điều 9.

> **Lưu ý:** Mục 5 trên đây không lặp lại SDLC, vai trò chung, cơ chế ngoại lệ và không tuân thủ đã có ở SDGP — xem Điều 8 và Điều 9 của TPODP để dẫn chiếu ngược lại SDGP thay vì viết lại.

6. Vai trò và trách nhiệm

Vai trò	Trách nhiệm chính
Head of Procurement/Vendor Management	Chủ trì đánh giá bảo mật và xếp tầng rủi ro vendor, đàm phán điều khoản hợp đồng, giám sát định kỳ, chủ sở hữu tài liệu
Head of Engineering	Xác nhận yêu cầu kỹ thuật/bảo mật trong đánh giá vendor, đảm bảo code/artifact vendor qua đúng gate nội bộ
Security Team	Thực hiện/thẩm định đánh giá bảo mật vendor, xem xét báo cáo SOC 2 Type 2/ISO 27001, xử lý thông báo sự cố từ vendor
Project/Engineering Lead phụ trách vendor	Quản lý truy cập nhân sự vendor hằng ngày, thực hiện review sản phẩm bàn giao, thực hiện offboarding
Legal/Pháp chế	Soạn thảo và rà soát điều khoản hợp đồng (Điều 5.2), bao gồm IP, audit rights, escrow, chuyển dữ liệu xuyên biên giới

7. Đo lường tuân thủ

- Tỷ lệ hợp đồng vendor mới có đầy đủ hồ sơ đánh giá bảo mật và xếp tầng rủi ro trước khi ký (mục tiêu: 100%).
- Tỷ lệ tài khoản vendor đang hoạt động có bật MFA và còn trong thời hạn hợp đồng (mục tiêu: 100%).
- Thời gian trung bình từ khi hợp đồng kết thúc đến khi thu hồi toàn bộ quyền truy cập trên hệ thống do tổ chức quản lý (mục tiêu: trong ngày làm việc kết thúc hợp đồng).
- Tỷ lệ hồ sơ offboarding có đầy đủ xác nhận bàn giao và cam kết không giữ lại dữ liệu.
- Số lần giám sát định kỳ đã thực hiện so với kế hoạch đã cam kết theo tầng rủi ro của từng vendor.

8. Cơ chế ngoại lệ

Áp dụng theo đúng cơ chế ngoại lệ tại SDGP, Điều 8. Mọi ngoại lệ đối với yêu cầu của TPODP (ví dụ rút ngắn thời gian đánh giá bảo mật do áp lực tiến độ) PHẢI được phê duyệt bằng văn bản theo đúng quy trình đó, có thời hạn xác định và đánh giá rủi ro đi kèm.

9. Không tuân thủ

Áp dụng theo đúng cơ chế xử lý không tuân thủ tại SDGP, Điều 9. Riêng đối với vi phạm nghiêm trọng của bên thứ ba (ví dụ: dùng tài khoản dùng chung trái phép, thuê nhà thầu phụ chưa được phê duyệt, không thông báo sự cố bảo mật đúng hạn), tổ chức bảo lưu quyền xử lý theo điều khoản hợp đồng đã ký, bao gồm cả việc chấm dứt hợp đồng trước hạn.

10. Chủ sở hữu tài liệu và chu kỳ rà soát

Document Owner: Head of Procurement/Vendor Management, phối hợp Head of Engineering. Rà soát hằng năm hoặc ngay khi có thay đổi đáng kể về khung pháp lý/chuẩn bảo mật liên quan đến vendor.

11. Tài liệu liên quan

- Engineering Constitution v1.0 (Tầng 1)
- Software Development Governance Policy v1.0 (SDGP, Tầng 2) — đặc biệt Điều 5.4, 5.11, 8, 9
- Secure Software Development Policy (Tầng 2)
- Software Quality Policy (Tầng 2)
- Open-Source Software Policy (Tầng 2)

> *"Tin tưởng, nhưng phải xác minh. Sản phẩm do bên thứ ba tạo ra mang cùng trách nhiệm, đi qua cùng cánh cổng kiểm soát, và khi hợp tác kết thúc — không để lại khoảng trống nào."*

12. Phê duyệt

Vai trò	Họ tên	Chữ ký	Ngày
Head of Procurement/Vendor Management			
Head of Engineering			
Engineering Governance Council (Chủ tọa)			