

NGÂN HÀNG TMCP SÀI GÒN – HÀ NỘI



HỒ SƠ YÊU CẦU CHÀO HÀNG

**TRANG BỊ GIẢI PHÁP PHÁT HIỆN VÀ ỨNG PHÓ AN NINH
TRÊN MÁY CHỦ VÀ WORKLOAD (EDR/CWPP)**

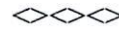
2026



NGÂN HÀNG TMCP
SÀI GÒN - HÀ NỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc



Hà Nội, ngày 21 tháng 10 năm 2026

THƯ MỜI

Kính gửi: Quý Công ty

Ngân hàng TMCP Sài Gòn - Hà Nội có nhu cầu trang bị Giải pháp Phát hiện và Ứng phó An ninh trên Máy chủ và Workload (EDR/CWPP). Trân trọng kính mời quý công ty tham dự gói chào hàng nêu trên.

Quý Công ty có thể tìm hiểu thêm các thông tin cần thiết trong Hồ sơ yêu cầu chào hàng kèm theo.

Hồ sơ chào hàng được gửi tới địa chỉ: Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn Hà Nội, Toà nhà 81 Trần Hưng Đạo, Phường Cửa Nam, TP Hà Nội.

Thời gian nhận hồ sơ: trước 15h00 ngày 26 tháng 10 năm 2026.

Người nhận: Nguyễn Ngọc Cầu – Phòng Đấu thầu - Trung tâm mua sắm.

Điện thoại di động: 0977901188.

Trân trọng kính mời./.

NGÂN HÀNG TMCP SÀI GÒN HÀ NỘI



Nguyễn Anh Thu

PHẦN I CÁC YÊU CẦU VỀ HỒ SƠ CHÀO HÀNG

I. Yêu cầu về Hồ sơ chào hàng

- Hồ sơ chào hàng phải được lập thành 02 bản (**01 bản gốc + 01 bản sao**), đóng trong thùng đựng kín có niêm phong và phải được gửi tới đúng địa điểm trước thời gian quy định trong hồ sơ yêu cầu chào hàng.
- Hồ sơ chào hàng được đóng trong phong bì riêng biệt. Bên ngoài phong bì ghi rõ: Hồ sơ chào hàng: “Trang bị Giải pháp Phát hiện và Ứng phó An ninh trên Máy chủ và Workload (EDR/CWPP).”
- Hồ sơ chào hàng phải có đầy đủ các nội dung sau :
 - o Đơn chào hàng: Phải có chữ ký của người đại diện theo pháp luật của công ty hoặc người được ủy quyền (Có giấy ủy quyền kèm theo);
 - o Bảng chào giá chi tiết (phải chào đầy đủ số lượng, chủng loại, giá trước VAT, giá sau VAT...) theo như Phần III Mục 2 của hồ sơ yêu cầu;
 - o Hiệu lực của Hồ sơ chào hàng tối thiểu **60** ngày kể từ thời điểm 15h00' ngày 26/10/2026;
 - o Đơn vị có tối thiểu 03 năm kinh nghiệm trong việc cung cấp và triển khai giải pháp an toàn bảo mật thông tin. Nhà thầu cung cấp tài liệu chứng minh thời gian kinh nghiệm theo yêu cầu của Hồ sơ yêu cầu chào hàng;
 - o Đơn vị phải có tối thiểu 02 hợp đồng tương tự về cung cấp, triển khai giải pháp bảo vệ điểm cuối (EPP/EDR/XDR) hoặc bảo vệ workload (CWPP), trong đó giá trị của mỗi hợp đồng từ 2 tỷ VND trở lên. Nhà thầu phải cung cấp tài liệu chứng minh gồm bản sao hợp đồng, hóa đơn giá trị gia tăng (VAT) và biên bản nghiệm thu hoặc biên bản bàn giao/thanh lý hợp đồng;
 - o Đơn vị phải có thư hỗ trợ của chính hãng hoặc giấy tờ chứng minh là nhà phân phối, đại lý chính hãng;
 - o Báo cáo tài chính 02 năm gần nhất kiểm toán hoặc bản nộp qua cổng thông tin điện tử đảm bảo doanh thu bình quân trên 10 tỷ VND và có lãi.
 - o Nhân sự triển khai :
 - o Nhà thầu phải bố trí tối thiểu 02 nhân sự chủ chốt, gồm: (i) tối thiểu 01 kỹ sư triển khai có chứng chỉ chuyên môn do chính hãng sản xuất giải pháp được chào cấp, còn hiệu lực; và (ii) 01 cán bộ quản lý dự án có chứng chỉ PMP hoặc PRINCE2 còn hiệu lực.
 - Cung cấp 1 cán bộ quản lý dự án có chứng chỉ PMP hoặc PRINCE2 còn hiệu lực và tối thiểu 01 kỹ sư tham gia triển khai tích hợp và hỗ trợ kỹ thuật; kỹ sư triển khai phải đáp ứng yêu cầu:
 - Có chứng chỉ chuyên môn do chính hãng sản xuất giải pháp được chào cấp, còn hiệu lực.
 - Kỹ sư của hãng, hoặc kỹ sư của nhà thầu được chứng thực bởi hãng.

- Có kinh nghiệm triển khai từ 02 dự án tương tự trở lên với vai trò đầu mối hỗ trợ kỹ thuật và có hợp đồng lao động chính thức còn thời hạn từ 01 năm trở lên.
- Cam kết chấp nhận yêu cầu về kỹ thuật, chất lượng, theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng;
- Cam kết chấp nhận yêu cầu về điều kiện tài chính thương mại theo yêu cầu tại Phần III của Hồ sơ yêu cầu chào hàng;

II. Thời gian và địa điểm nộp Hồ sơ chào hàng

- **Thời gian:** trước 15h00' ngày 26/10./2026.
- **Địa điểm:** Phòng đấu thầu - Trung tâm mua sắm, Ngân hàng TMCP Sài Gòn Hà Nội, tại Toà nhà số 81 Phố Trần Hưng Đạo, Phường Cửa Nam, TP Hà Nội (Liên hệ Nguyễn Ngọc Cầu, Điện thoại: 0977901188).

PHẦN II

YÊU CẦU CỤ THỂ

I. Mục tiêu, Phạm vi gói chào hàng

Với mục đích bổ sung năng lực giám sát – phát hiện – phản ứng sự cố theo thời gian thực trên hệ thống máy chủ ảo hóa và nền tảng đám mây (Kubernetes/OpenShift/AWS), thay thế lớp phòng chống mã độc truyền thống trên máy chủ và tuân thủ quy định của Ngân hàng Nhà nước về an toàn hệ thống thông tin, SHB thực hiện gói chào hàng nhằm lựa chọn nhà thầu có đủ năng lực để trang bị Giải pháp Phát hiện và Ứng phó An ninh trên Máy chủ và Workload (EDR/CWPP).

I. Mục tiêu của gói chào hàng

Mục tiêu của gói thầu này nhằm lựa chọn nhà thầu có đầy đủ năng lực để thực hiện các công việc thuộc gói chào hàng, cụ thể như sau:

1. Cung cấp bản quyền Giải pháp Phát hiện và Ứng phó An ninh trên Máy chủ và Workload (EDR/CWPP) cho tối thiểu 1.500 máy chủ ảo hóa Windows/Linux và 200 node Kubernetes/OpenShift/AWS, thời hạn 12 tháng, đáp ứng đúng và đầy đủ các yêu cầu của SHB.
2. Triển khai, cấu hình và tích hợp hai chiều giải pháp với hệ thống giám sát an ninh tập trung (SIEM/SOC) của SHB; thay thế phần mềm phòng chống mã độc truyền thống trên các máy chủ trong phạm vi.
3. Đào tạo chuyên gia công nghệ cho cán bộ vận hành của SHB.
4. Cung cấp dịch vụ hỗ trợ kỹ thuật 24/7 trong 12 tháng nhằm đảm bảo hệ thống được vận hành ổn định, xử lý kịp thời các sự cố phát sinh và giảm thiểu ảnh hưởng đến hoạt động của SHB:
 - Thời gian hỗ trợ kỹ thuật: 24 giờ/ngày và 7 ngày/tuần;
 - Thời gian phản hồi: tối đa 30 phút kể từ thời điểm nhận được thông báo sự cố;
 - Thời gian đưa ra giải pháp khắc phục hoặc giải pháp tạm thời: tối đa 04 giờ kể từ thời điểm nhận được thông báo sự cố.

II. Phạm vi của gói chào hàng

Nhà thầu cần thực hiện đầy đủ các công việc sau :

- Cung cấp bản quyền bảo vệ máy chủ (EPP/EDR) cho tối thiểu 1.500 máy chủ ảo hóa Windows Server/Linux tại Trung tâm dữ liệu chính của SHB, thời hạn 12 tháng;
- Cung cấp bản quyền bảo vệ workload đám mây và container (CWPP) cho tối thiểu 200 node Kubernetes/OpenShift/AWS, thời hạn 12 tháng;
- Khảo sát, thiết kế và cài đặt agent theo lộ trình phân kỳ, bảo đảm không gián đoạn các ứng dụng đang vận hành;
- Tích hợp hai chiều với hệ thống SIEM/SOC của SHB: đẩy cảnh báo, sự cố và dữ liệu hành vi về SIEM; tiếp nhận lệnh phản ứng từ SOC;
- Xây dựng chính sách bảo vệ, ngoại lệ và playbook phản ứng sự cố phù hợp với từng nhóm máy chủ và cụm Kubernetes; kiểm thử chức năng trước khi nghiệm thu;

- Đào tạo chuyển giao công nghệ cho tối thiểu 05 cán bộ vận hành của SHB, thời lượng tối thiểu 03 ngày, có tài liệu đào tạo và giấy chứng nhận hoàn thành;
- Cung cấp dịch vụ hỗ trợ kỹ thuật 24/7 trong 12 tháng kể từ ngày hai bên ký Biên bản nghiệm thu tổng thể; cung cấp các bản cập nhật agent, bản vá và cập nhật tri thức phát hiện theo chính sách hỗ trợ của hãng;
- Bàn giao đầy đủ bản quyền, tài liệu kỹ thuật, hướng dẫn vận hành và các chứng từ xác nhận quyền sử dụng dịch vụ hỗ trợ chính hãng đứng tên SHB.
- Bảng dưới đây liệt kê phạm vi cung cấp hàng hóa và dịch vụ:

STT	Mã hàng hóa	Mô tả hàng hóa	Đơn vị	SL
Danh mục bản quyền phần mềm				
1	Nhà thầu ghi mã SKU của hãng	Bản quyền bảo vệ máy chủ (EPP/EDR) cho máy chủ ảo hóa Windows Server/Linux, thời hạn 12 tháng, đã bao gồm hỗ trợ kỹ thuật 24/7 của hãng	Bản quyền	1.500
2	Nhà thầu ghi mã SKU của hãng	Bản quyền bảo vệ workload đám mây và container (CWPP) cho node Kubernetes/OpenShift/AWS, thời hạn 12 tháng, đã bao gồm hỗ trợ kỹ thuật 24/7 của hãng	Bản quyền	200
Danh mục dịch vụ				
1	—	Dịch vụ triển khai, cài đặt, cấu hình, tích hợp SIEM/SOC, kiểm thử và đào tạo chuyển giao công nghệ	Gói	01

II. Yêu cầu kỹ thuật

1. Yêu cầu chung

Nhà thầu phải cung cấp đầy đủ hàng hóa và dịch vụ trong bản liệt kê phạm vi cung cấp hàng hóa và dịch vụ được nêu tại Mục tiêu phạm vi gói chào hàng, đáp ứng tối thiểu các yêu cầu sau:

- Giải pháp Phát hiện và Ứng phó An ninh trên Máy chủ và Workload (EDR/CWPP) phải là sản phẩm của một trong các hãng CrowdStrike, SentinelOne hoặc Palo Alto Networks — là các giải pháp đã được thử nghiệm thực tế tại SHB theo chủ trương đã được phê duyệt tại Tờ trình số 82/26/TTr-ATBMCN — và đáp ứng các yêu cầu tại Bảng chấm kỹ thuật;
- Giải pháp được quản trị tập trung trên nền tảng đám mây của hãng theo mô hình một agent và một giao diện quản trị; SHB không đầu tư thiết bị phần cứng trong phạm vi gói chào hàng này. Nhà thầu nêu rõ sơ đồ kiến trúc, vùng lưu trữ dữ liệu của nền tảng và danh mục module/bản quyền được chào;
- Bản quyền phần mềm đầy đủ cho tối thiểu 1.500 máy chủ và 200 node, thời hạn 12 tháng, đã bao gồm cập nhật phiên bản, bản vá, cập nhật tri thức phát hiện và hỗ trợ kỹ thuật 24/7 của hãng; bản quyền được cấp đích danh cho SHB. Trường hợp hãng cấp phép theo đơn vị khác (vCPU, pod, cluster), nhà thầu quy đổi và ghi rõ số lượng tương đương;

- Mọi tính năng nhà thầu tuyên bố đáp ứng phải nằm trong gói bản quyền được chào; tính năng thuộc module hoặc bản quyền bổ sung phải được liệt kê và tính giá trong Bảng chào giá;
- Sản phẩm phải là chính hãng, có nguồn gốc rõ ràng, hợp pháp; phiên bản phần mềm được chào là phiên bản đang được hãng hỗ trợ tại thời điểm đóng thầu;
- Thư hỗ trợ của chính hãng đối với giải pháp cung cấp trong phạm vi yêu cầu chào hàng này.

2. Yêu cầu về kỹ thuật đối với danh mục hàng hóa và dịch vụ

Danh mục hàng hóa và dịch vụ phải chào được nêu trong bảng dưới đây. Yêu cầu kỹ thuật chi tiết của giải pháp được quy định tại BẢNG CHẤM KỸ THUẬT của hồ sơ này; nhà thầu kê khai mức độ đáp ứng theo đúng thứ tự và cây đánh số của bảng đó, kèm tài liệu chứng minh đính kèm dưới dạng tệp hoàn chỉnh.

STT	Danh mục hàng hóa	Mô tả hàng hóa (cấu hình, kích thước, tiêu chuẩn kỹ thuật, tốc độ ..)	SL	Đơn vị tính
I	Bản quyền giải pháp bảo vệ máy chủ (EPP/EDR)			
1	Bản quyền EPP/EDR cho máy chủ	Quản trị tập trung trên nền tảng đám mây của hãng; đáp ứng các Mục I–VI và Mục VIII của Bảng chấm kỹ thuật	1.500	Bản quyền
II	Bản quyền giải pháp bảo vệ workload đám mây và container (CWPP)			
1	Bản quyền CWPP cho node Kubernetes/OpenShift/AWS	Dùng chung agent hoặc console với hạng mục I; đáp ứng Mục VII của Bảng chấm kỹ thuật	200	Bản quyền
III	Dịch vụ triển khai, đào tạo			
1	Dịch vụ triển khai, tích hợp và đào tạo	Theo Mục 3, 4 Phần II của hồ sơ này	01	Gói

3. Nhân sự triển khai và tổ chức thực hiện

01 cán bộ quản lý dự án có chứng chỉ PMP hoặc PRINCE2 còn hiệu lực và tối thiểu 01 kỹ sư triển khai có chứng chỉ chuyên môn do chính hãng sản xuất giải pháp được chào cấp, còn hiệu lực.

- Kinh nghiệm: đã triển khai dự án tương tự tại vị trí đảm nhiệm trong dự án này; hồ sơ mỗi nhân sự gồm lý lịch chuyên môn, chứng chỉ, hợp đồng lao động và xác nhận đóng bảo hiểm xã hội.
- Nhà thầu phải cam kết các nhân sự trong danh sách nêu trên sẽ triển khai trực tiếp cho dự án này. Trường hợp có sự thay đổi nhân sự triển khai, nhà thầu phải gửi thông báo chính thức tới SHB, cam kết nhân sự thay thế có trình độ tương đương và phải được chấp thuận của SHB.

III. Yêu cầu triển khai

1. Yêu cầu chung:

- Hệ thống được triển khai và bàn giao theo phương thức trọn gói. Nhà thầu đóng vai trò chủ trì và phối hợp với hãng sản xuất để thực hiện cài đặt, cấu hình và tích hợp các thành phần của giải pháp, đáp ứng theo yêu cầu của SHB;
- Thời gian hoàn thành: tối đa 16 tuần kể từ ngày ký hợp đồng, theo lộ trình:
 - Bàn giao bản quyền cho 1.500 máy chủ và 200 node: tối đa 04 tuần;
 - Hoàn thành khảo sát, thiết kế, triển khai đợt đầu và tích hợp SIEM/SOC: tối đa 08 tuần;
 - Hoàn thành triển khai toàn bộ phạm vi, nghiệm thu và Golive hệ thống: tối đa 16 tuần.
- Phương pháp luận triển khai: nhà thầu phải đề xuất phương pháp luận, quy trình triển khai và kế hoạch triển khai phân kỳ chi tiết (môi trường thử nghiệm trước, môi trường sản xuất sau), mỗi đợt có tiêu chí nghiệm thu và phương án quay lui;
- Địa điểm triển khai: Trung tâm dữ liệu chính của SHB tại Hà Nội và các môi trường đám mây của SHB;
- Trong suốt quá trình triển khai phải có sự tham gia của cán bộ SHB;
- Yêu cầu về bảo mật thông tin: cam kết không tiết lộ, sao chép, sử dụng bất cứ thông tin liên quan đến hệ thống, cơ sở dữ liệu, dữ liệu, hệ thống ứng dụng và các thông tin khác liên quan đến việc triển khai gói chào hàng này dưới bất kỳ hình thức nào;

2. Các yêu cầu cụ thể:

2.1. Khảo sát và thiết kế

- Khảo sát hiện trạng máy chủ ảo hóa, phần mềm phòng chống mã độc đang sử dụng, các cụm Kubernetes/OpenShift/AWS và hệ thống SIEM/SOC của SHB; lập thiết kế chi tiết trình SHB phê duyệt trước khi triển khai;

2.2. Cài đặt, cấu hình và tích hợp

- Cài đặt agent hàng loạt từ xa trên máy chủ Windows Server/Linux; triển khai sensor trên các cụm Kubernetes/OpenShift/AWS theo đúng phương thức nêu tại Mục VII Bảng chấm kỹ thuật;
- Cấu hình chính sách bảo vệ theo nhóm máy chủ, ban đầu ở chế độ giám sát, chuyển sang chế độ ngăn chặn sau khi hoàn tất tinh chỉnh ngoại lệ và được SHB chấp thuận;
- Tích hợp hai chiều với hệ thống SIEM/SOC của SHB; xây dựng playbook phản ứng cho các kịch bản: mã độc mã hóa dữ liệu, mã độc fileless, khai thác lỗ hổng, hành vi bất thường trong container;
- Gỡ bỏ phần mềm phòng chống mã độc truyền thống trên các máy chủ đã chuyển đổi sau khi SHB xác nhận; bảo đảm agent không làm gián đoạn và không ảnh hưởng đáng kể tới hiệu năng của máy chủ ứng dụng, cơ sở dữ liệu trọng yếu.

IV. BÀN GIAO, NGHIỆM THU

1. Bàn giao

Nhà thầu có trách nhiệm bàn giao các hạng mục chính sau:

- Toàn bộ hạng mục cung cấp phải đáp ứng các yêu cầu kỹ thuật tại Bảng chấm kỹ thuật của hồ sơ này;
- Lập Biên bản bàn giao về số lượng bản quyền, module và danh sách máy chủ, node đã được bảo vệ; bàn giao giấy chứng nhận bản quyền, tài khoản quản trị và thông tin đăng ký dịch vụ hỗ trợ của hãng đứng tên SHB;

- Các tài liệu theo yêu cầu:
 - Kế hoạch triển khai chi tiết; tài liệu kiến trúc và thiết kế hệ thống;
 - Tài liệu cài đặt, cấu hình chính sách; kịch bản và kết quả kiểm thử;
 - Playbook phản ứng sự cố và tài liệu tích hợp SIEM/SOC;
 - Tài liệu quy trình, hướng dẫn vận hành và phân quyền quản trị hệ thống;
- Các nội dung liên quan khác (nếu có).

2. Nghiệm thu

- Trước khi nghiệm thu, hai bên thực hiện kiểm thử chức năng theo Bảng chấm kỹ thuật và kiểm thử tích hợp với hệ thống SIEM/SOC; kết quả được lập thành biên bản có chữ ký của hai bên;
- Hệ thống được đưa vào vận hành chính thức sau khi hoàn thành triển khai toàn bộ phạm vi, đáp ứng đúng, đầy đủ các yêu cầu của SHB và được SHB xác nhận bằng Biên bản bàn giao và Biên bản nghiệm thu tổng thể.

3. Các yêu cầu chung

- Cung cấp dịch vụ bảo hành, hỗ trợ kỹ thuật đối với giải pháp do nhà thầu cung cấp, với cam kết chất lượng dịch vụ theo đúng chính sách của hãng sản xuất;
- Nhà thầu phải nêu rõ các nội dung về bảo hành và hỗ trợ kỹ thuật, bao gồm cả các đề xuất với Bên mời thầu về chế độ bảo hành và hỗ trợ kỹ thuật;
- Nhà thầu phải có bộ phận hỗ trợ kỹ thuật tại Hà Nội; nêu rõ chế độ sau bán hàng của hãng sản xuất cũng như khả năng đáp ứng của nhà thầu.

4. Bảo hành

- Thời gian bảo hành: 12 tháng kể từ thời điểm ký Biên bản nghiệm thu tổng thể; mọi chi phí liên quan đến bảo hành thuộc trách nhiệm của nhà thầu;
- Nội dung bảo hành bao gồm những công việc cụ thể sau:
 - Khắc phục và xử lý các lỗi phát sinh trong quá trình hoạt động của giải pháp, kể cả lỗi do agent gây ảnh hưởng tới máy chủ;
 - Cam kết bằng văn bản của người đại diện theo pháp luật của nhà thầu về thời gian xử lý sự cố: phản hồi tối đa 30 phút, đưa ra giải pháp khắc phục hoặc giải pháp tạm thời tối đa 04 giờ;
 - Thông báo cho SHB các vấn đề liên quan đến bản vá lỗi, cập nhật và phiên bản mới của agent; cung cấp và cài đặt các bản cập nhật theo tiêu chuẩn của hãng nếu được SHB chấp nhận;
- Trong bảng chào giá, nhà thầu chào thêm đơn giá gia hạn bản quyền và hỗ trợ kỹ thuật cho năm thứ 2 và năm thứ 3 (không tính vào giá đánh giá) để SHB tham khảo khi gia hạn.

5. Hỗ trợ kỹ thuật theo tiêu chuẩn chính hãng

- Nhà thầu có trách nhiệm phối hợp với SHB hỗ trợ khai thác sử dụng hệ thống, hướng dẫn cán bộ kỹ thuật của SHB các tính năng của hệ thống khi SHB yêu cầu;
- Nhà thầu phải cam kết hỗ trợ kỹ thuật 24/7 theo tiêu chuẩn chính hãng trong thời gian hiệu lực bản quyền;
- Nhà thầu phải nêu rõ phương pháp tổ chức hỗ trợ kỹ thuật (tổ chức nhân sự, phương pháp liên lạc, quy trình xử lý yêu cầu hỗ trợ kỹ thuật);
- Chất lượng dịch vụ theo đúng chính sách tuyên bố từ hãng sản xuất.

PHẦN III

YÊU CẦU VỀ TÀI CHÍNH THƯƠNG MẠI

1. Yêu cầu về thương mại

1.1. Đồng tiền chào giá: Việt Nam đồng.

1.2. Đồng tiền thanh toán: Việt Nam đồng.

1.3. Phương thức thanh toán: Chuyển khoản vào tài khoản của nhà thầu.

1.4. Điều kiện thanh toán

- Bên mua tạm ứng cho bên bán 30% giá trị hợp đồng kể từ ngày 2 bên ký hợp đồng và cung cấp cho bên bán hồ sơ sau :
 - Bảo lãnh tạm ứng bằng giá trị tạm ứng (nếu nhà thầu thực hiện tạm ứng)
 - Bảo đảm thực hiện hợp đồng có giá trị bằng 10% tổng giá trị hợp đồng.
 - Đề nghị tạm ứng.
- Bên Mua thanh toán cho Bên Bán 100 % (có khấu trừ 30% giá trị tạm ứng) tổng giá trị hợp đồng trong vòng 07 (bảy) ngày làm việc kể từ ngày Bên Bán bàn giao cho bên mua các giấy tờ, tài liệu sau :
 - Biên bản nghiệm thu tổng thể;
 - Giấy đề nghị thanh toán;
 - Hóa đơn tài chính hợp lệ.
 - Các giấy tờ tài liệu liên quan khác (nếu có).

2. Bảng chào giá chi tiết

Nhà thầu trình bày bảng chào giá chi tiết như sau

STT	Tên sản phẩm	ĐVT	Số lượng	Đơn giá (VNĐ)	Thành tiền (VNĐ)	Tiến độ cung cấp
1	Bản quyền bảo vệ máy chủ (EPP/EDR) cho tối thiểu 1.500 máy chủ, thời hạn 12 tháng (nêu rõ hãng, tên thương mại, gói bản quyền và các module đi kèm)	Bản quyền	1.500			Tối đa 04 tuần
2	Bản quyền bảo vệ workload đám mây và container (CWPP) cho tối thiểu 200 node, thời hạn 12 tháng (nêu rõ hãng, gói bản quyền, đơn vị cấp phép)	Bản quyền	200			Tối đa 04 tuần
3	Dịch vụ triển khai, cài đặt, cấu hình, tích hợp SIEM/SOC, kiểm thử và đào tạo chuyển giao công nghệ	Trọn gói	1			Tối đa 16 tuần
	Tổng cộng					

	Thuế VAT	
	Tổng giá trị đã bao gồm VAT	

3. Điều kiện xem xét lựa chọn nhà thầu

Nhà thầu được xem xét lựa chọn là đơn vị cung cấp khi đáp ứng các yêu cầu sau:

- Đáp ứng yêu cầu về năng lực kinh nghiệm, kỹ thuật.
- Có giá chào cạnh tranh nhất.

NGÂN HÀNG TMCP SÀI GÒN – HÀ NỘI



Nguyễn Anh Thu

BẢNG CHẤM NĂNG LỰC KINH NGHIỆM

STT	Nội dung	Yêu cầu cụ thể	Điểm tối đa	Điểm tối thiểu
1	Kinh nghiệm	Đơn vị có tối thiểu 03 năm kinh nghiệm trong việc cung cấp và triển khai giải pháp an toàn bảo mật thông tin. Nhà thầu cung cấp tài liệu chứng minh thời gian kinh nghiệm theo yêu cầu của Hồ sơ yêu cầu chào hàng;	10	10
2	Hợp đồng tương tự	Đơn vị phải có tối thiểu 02 hợp đồng tương tự về cung cấp, triển khai giải pháp bảo vệ điểm cuối (EPP/EDR/XDR) hoặc bảo vệ workload (CWPP), trong đó giá trị của mỗi hợp đồng từ 2 tỷ VND trở lên. Nhà thầu phải cung cấp tài liệu chứng minh gồm bản sao hợp đồng, hóa đơn giá trị gia tăng (VAT) và biên bản nghiệm thu hoặc biên bản bàn giao/thanh lý hợp đồng;	40	
	Có từ 3 hợp đồng trở lên		40	
	Có 2 hợp đồng		30	30
	Có 1 hợp đồng		10	
	Không có hợp đồng		0	
3	Thư hỗ trợ của hãng	Đơn vị phải có thư hỗ trợ của chính hãng hoặc giấy tờ chứng minh là nhà phân phối, đại lý chính hãng;	20	20
4	Đội ngũ nhân sự triển khai	Cung cấp danh sách nhân sự triển	10	10
5	Tình hình tài chính	Báo cáo tài chính 02 năm gần nhất kiểm toán hoặc bản nộp qua cổng thông tin điện tử đảm bảo doanh thu bình quân trên 10 tỷ VND và có lãi.	10	10
6	Các cam kết	Cam kết chấp nhận yêu cầu về kỹ thuật, chất lượng, theo yêu cầu tại Phần II của Hồ sơ yêu cầu chào hàng Cam kết chấp nhận yêu cầu về điều kiện tài chính thương mại theo yêu cầu tại Phần III của Hồ sơ yêu cầu chào hàng.	10	10
	Tổng cộng		100	90

Nhà thầu được đánh giá đáp ứng năng lực kinh nghiệm khi tổng điểm đánh giá tối thiểu đạt 90 điểm và phải đáp ứng các yêu cầu điểm tối thiểu của bảng trên.

BẢNG CHẤM KỸ THUẬT

STT	Nội dung yêu cầu	Tối thiểu	Tối đa
I	KIẾN TRÚC VÀ NỀN TẢNG		
1	Agent và kết nối: Agent nhẹ, không ảnh hưởng hiệu năng thiết bị, không cần khởi động lại sau khi cài đặt. Giao tiếp giữa agent và hệ thống quản trị trên Cloud được mã hóa theo giao thức TLS. Cập nhật/nâng cấp agent từ xa qua hệ thống quản trị tập trung; thiết lập cập nhật theo lịch và phân tán.	10	10
2	Nền tảng hợp nhất, định hướng XDR: Giải pháp cloud-native, có khả năng mở rộng linh hoạt; kiến trúc 01 agent – 01 console quản trị duy nhất cho tất cả chức năng trên nền tảng thống nhất, quản lý tập trung từ dịch vụ đám mây của hãng. Kiến trúc cho phép quản lý tập trung tất cả máy trạm, thiết bị; phần mềm bảo mật đầu cuối; chính sách bảo mật; theo dõi giám sát và tự động phản ứng; quản lý hàng trăm nghìn thiết bị trong môi trường phức tạp, đa dạng, nhiều địa điểm, chi nhánh. Có khả năng tương quan dữ liệu giữa nhiều nguồn (Endpoint, Network, Cloud, Identity) để phát hiện sự cố bảo mật.	10	10
3	Hệ điều hành và nền tảng hỗ trợ: Agent hỗ trợ cài đặt trên các hệ điều hành máy trạm và máy chủ.	5	10
3.1	Mức tối thiểu: Windows 10, 11; Windows Server 2016, 2019, 2022, 2025; macOS (tối thiểu 03 phiên bản gần nhất); Linux: CentOS, Debian, Oracle Linux, Red Hat Enterprise Linux, SUSE, Ubuntu.	5	
3.2	Mức tối đa: đáp ứng mức tối thiểu và hỗ trợ thêm: Windows 7, 8.1; Windows Server 2008 R2, 2012 R2 (hệ thống legacy)		10
4	Đánh giá độc lập: Là giải pháp nằm trong nhóm dẫn đầu (Leaders) được một trong các tổ chức nghiên cứu và tư vấn công nghệ chuyên nghiệp như Gartner, Forrester, IDC hoặc tương đương trực tiếp đánh giá trong vòng 04 năm gần nhất. Giải pháp có kết quả kiểm tra của đơn vị kiểm thử độc lập trong thời gian gần đây (không quá 02 năm).	5	5
II	PHÒNG CHỐNG MÃ ĐỘC VÀ BẢO VỆ ENDPOINT (EPP)		
1	NGAV – chống mã độc đa lớp: Phát hiện và ngăn chặn mã độc đã biết (known) và chưa biết (unknown) bằng Machine Learning, AI, phân tích hành vi; bảo vệ thời gian thực (real-time) và quét theo yêu cầu/thủ công; xử	15	15

	lý khi phát hiện mã độc như chặn/loại bỏ tiến trình, cách ly file; giám sát hành vi tiến trình lạ và loại bỏ khi có hành vi độc hại; tự động cập nhật tri thức phát hiện tấn công mới không cần can thiệp thủ công; bảo vệ khi endpoint mất kết nối Internet; lập lịch dò quét cho các hệ thống máy tính được bảo vệ; kiểm tra và ngăn chặn mã độc trên các định dạng file: PE, ELF, DMG, Office, script.		
2	Chống tấn công nâng cao và khai thác lỗ hổng: Ngăn chặn theo thời gian thực các cuộc tấn công fileless, malware-free, zero-day; phát hiện hành vi bất thường, IOA và ánh xạ với TTP theo MITRE ATT&CK (C&C, Reconnaissance, Lateral Movement...); phòng chống tấn công khai thác lỗ hổng/điểm yếu của ứng dụng và hệ điều hành. Đáp ứng tối thiểu 2/3 điều kiện sau: (i) ngăn chặn khai thác lỗ hổng dựa trên kỹ thuật khai thác (techniques) cho cả Windows, macOS, Linux và cho phép tạo ngoại lệ cho một process cụ thể với một kỹ thuật cụ thể; (ii) ngăn chặn khai thác lỗ hổng ở mức OS kernel; (iii) ngăn chặn các hình thức Reverse Shell, Cryptominers, Dylib Hijacking, Container Escaping, Brute Force, DLL Hijacking, Browser Exploits.	15	15
3	Phòng chống ransomware: Phòng chống hiệu quả mã độc mã hóa dữ liệu (ransomware) dựa trên phân tích hành vi hoặc cơ chế tương đương.	10	10
4	Chính sách bảo vệ và tự bảo vệ agent: Agent có cơ chế tự bảo vệ: chống gỡ bỏ, chống tắt tiến trình; chỉ quản trị viên mới được gỡ bỏ từ xa hoặc khi cung cấp khóa. Quản lý, cập nhật, triển khai chính sách/rule, cấu hình từ xa khác nhau theo nhóm endpoint.	5	10
4.1	Mức tối thiểu: đáp ứng đầy đủ các nội dung trên.	5	
4.2	Mức tối đa: đáp ứng mức tối thiểu và đồng thời: (i) có sẵn và cho phép tạo mới security profiles, tối thiểu gồm Malware profile, Exploit profile, Restriction profile (giới hạn kết nối mạng, tệp tin, thiết bị gắn ngoài, ổ đĩa); (ii) ngăn chặn truy nhập vào file, thư mục chia sẻ, registry key/value cần bảo vệ và ngăn chặn tiến trình, dịch vụ thực thi hành vi nguy hại.		10
5	Host Firewall và Device Control: Host Firewall: kiểm soát kết nối mạng vào/ra endpoint dựa trên source IP, destination IP, source port, destination port, service/protocol. Device Control: quản lý thiết bị ngoại vi theo một hoặc nhiều tham số (loại, kiểu, mã nhà sản xuất, định danh/số hiệu thiết bị); kiểm soát kết nối thiết bị lưu trữ ngoại vi, thiết bị plug-and-play; kiểm soát	5	5

	quyền read/write file từ thiết bị ngoại vi; áp dụng chính sách theo nhóm máy tính.		
III	THREAT INTELLIGENCE		
1	Threat Intelligence tích hợp: Tích hợp sẵn nguồn Threat Intelligence của hãng, cập nhật trực tuyến, tự động để phát hiện và ngăn chặn kết nối tới địa chỉ độc hại (IP/Domain). Cho phép bổ sung nhận diện mã độc/mối đe dọa như hash, IP, domain. Tự động thực thi, phân tích mẫu trong sandbox và hiển thị verdict trên giao diện giải pháp.	5	5
IV	THU THẬP DỮ LIỆU VÀ HIỂN THỊ ENDPOINT		
1	Telemetry endpoint đầy đủ: Thu thập dữ liệu trên endpoint: (i) tập tin: tạo mới, ghi, truy cập, mở, đổi tên, xóa; đường dẫn đầy đủ trước và sau khi sửa đổi; hash SHA256, MD5 sau khi sửa đổi; (ii) tiến trình: PID tiến trình cha, PID tiến trình, đường dẫn đầy đủ, đối số dòng lệnh, hash SHA256/MD5, thông tin chứng chỉ và chữ ký; (iii) registry: tạo, sửa đổi, xóa, đổi tên key; registry path, tên value/key bị thay đổi, dữ liệu value bị thay đổi; (iv) DNS request và UDP response.	5	5
2	Host inventory và quản lý lỗ hổng: Hiển thị đầy đủ thông tin endpoint, tối thiểu: Applications, Browser extension, Disks, System Information, OS Patch Installed, Users, Autoruns; hiển thị các lỗ hổng bảo mật trên endpoint.	5	5
V	PHÁT HIỆN, ĐIỀU TRA VÀ THREAT HUNTING		
1	Cơ chế phát hiện: Phát hiện tấn công dựa trên IOC (IP, hash, domain, signature...), BIOC/IOA (hành vi trên máy tính, hệ thống mạng) và tương quan (correlation) từ nhiều nguồn kết hợp; liên kết chiến thuật, kỹ thuật MITRE ATT&CK cho từng cảnh báo; cho phép định nghĩa rule BIOC/IOA dựa trên network, process, file, registry activity; quản trị viên có thể sao chép và sửa đổi các rule BIOC/IOA có sẵn trên hệ thống.	10	10
2	Điều tra sự cố: Trực quan hóa các cảnh báo, phát hiện dưới dạng sơ đồ; xem các tiến trình, sự kiện dẫn đến cảnh báo với mô hình trực quan, có khả năng tương tác (di chuyển, mở rộng, thay đổi) phục vụ điều tra; dữ liệu phân tích có thể bao gồm lớp mạng, môi trường đám mây, bên thứ ba. Xây dựng timeline chi tiết cho mỗi sự kiện an ninh (trước và trong quá trình xảy	5	5

	ra sự cố), tối thiểu gồm: command line, file hash, process, parent/child process, DLLs, username, network activity.		
3	Threat hunting: Tìm kiếm và xem dữ liệu thô (process, file, network, registry, event log, hash, IP, script...) trên toàn bộ endpoint và workload (máy chủ, container).	5	10
3.1	Mức tối thiểu: tìm kiếm bằng ngôn ngữ truy vấn (query language); lưu và tái sử dụng truy vấn.	5	
3.2	Mức tối đa: đáp ứng mức tối thiểu và đồng thời: (i) tìm kiếm bằng ngôn ngữ tự nhiên qua AI; (ii) có khả năng mở rộng tìm kiếm trên dữ liệu nguồn bên thứ ba khi nâng cấp lên XDR.		10
VI	PHẢN ỨNG VÀ XỬ LÝ SỰ CỐ		
1	Hành động phản ứng: Cô lập (isolate) endpoint khỏi hệ thống mạng thủ công hoặc tự động theo chính sách; cung cấp sẵn hành động xử lý: tắt endpoint, kill process, xóa thư mục/file, cách ly file theo yêu cầu quản trị viên; thu thập file từ endpoint phục vụ điều tra; hỗ trợ định nghĩa bổ sung hành động phản ứng.	5	15
1.1	Mức tối thiểu: đáp ứng đầy đủ các nội dung trên.	5	
1.2	Mức tối đa: đáp ứng mức tối thiểu và đồng thời: (i) dump memory của endpoint; (ii) tìm và xóa nhanh file độc hại trên toàn bộ (hoặc danh sách xác định) endpoint; (iii) thu thập thông tin điều tra: Browser History, File Access, Process Execution, Command History, Remote Access, Memory Collections.		15
2	Phản hồi trực tiếp từ xa (Live Response): Kết nối trực tiếp tới terminal của endpoint để điều tra, xử lý sự cố; thực thi script mẫu có sẵn hoặc script/command tùy chỉnh (PowerShell, Bash, Python hoặc tương đương) qua live terminal, bằng giao diện dòng lệnh hoặc giao diện đồ họa.	5	5
VII	BẢO VỆ WORKLOAD (CWPP): MÁY CHỦ, CLOUD, CONTAINER, KUBERNETES		
1	Runtime protection cho container và Kubernetes: Bảo vệ, phát hiện và ngăn chặn tấn công/khai thác lỗ hổng/hành vi nguy hại runtime cho host (worker node) và container; phát hiện và ngăn chặn malware trong container; phát hiện, ngăn chặn Crypto miners, Reverse shell, process dùng cho lateral movement; phát hiện process bất thường. Triển khai: sensor dạng DaemonSet hoặc tương đương (01 agent/pod trên mỗi worker node), thiết	15	15

	lập được tài nguyên (CPU/RAM) cho container agent trong file triển khai (YAML/Helm); hỗ trợ tối thiểu EKS, AKS, GKE, Red Hat OpenShift, Kubernetes upstream, HCS (CEE); tự động triển khai khi có node mới trong cluster; xem được các container đang hoạt động trên từng worker node; quản lý trên cùng console với EDR.		
2	Bảo vệ workload máy chủ (VM cloud và on-prem): Bảo vệ máy chủ Windows Server/Linux chạy trên VM cloud (AWS, Azure, GCP) và hạ tầng ảo hóa on-prem bằng cùng agent và console với EDR, hỗ trợ kiến trúc x86_64 và ARM64; hỗ trợ workload tạm thời (auto-scaling, golden image) – tự đăng ký/hủy đăng ký agent khi instance được tạo/xóa.	5	10
2.1	Mức tối thiểu: đáp ứng đầy đủ các nội dung trên.	5	
2.2	Mức tối đa: đáp ứng mức tối thiểu và đồng thời: (i) giám sát toàn vẹn tệp tin (File Integrity Monitoring – FIM) cho file, thư mục, registry quan trọng trên máy chủ; (ii) kiểm soát ứng dụng (application allowlisting/blocklisting) trên máy chủ.		10
3	Posture và khả năng quan sát Kubernetes (KSPM), mở rộng CSPM: Giám sát, bảo đảm tuân thủ cho Kubernetes, container theo CIS Docker, CIS Kubernetes; theo dõi, thống kê số lượng, trạng thái (create, update, delete) của node, container, pod trong môi trường Kubernetes.	5	10
3.1	Mức tối thiểu: đáp ứng đầy đủ các nội dung trên.	5	
3.2	Mức tối đa: đáp ứng mức tối thiểu và có khả năng mở rộng (kích hoạt license, không đổi console) đánh giá cấu hình sai của tài khoản cloud (CSPM) trên AWS, Azure, GCP theo CIS Benchmark.		10
VIII	QUẢN TRỊ VÀ TÍCH HỢP		
1	Xác thực và phân quyền: Portal quản trị hỗ trợ xác thực 2FA, yếu tố xác thực đăng nhập như OTP; hỗ trợ SSO và tích hợp với các hệ thống xác thực; quản lý, phân quyền tài khoản quản trị, vận hành viên và kiểm soát truy cập theo vai trò (RBAC).	5	5
2	Dashboard, báo cáo, cảnh báo: Cung cấp sẵn dashboard quản trị và tùy biến theo nhu cầu; mẫu báo cáo trực quan, gửi báo cáo định kỳ, xuất PDF, CSV; gửi cảnh báo qua syslog, email, Slack, Microsoft Teams.	5	5
3	API và tích hợp SIEM/SOAR: Tích hợp với SIEM (Splunk, QRadar...) để đẩy alert, incident; tích hợp với SOAR để điều phối, tự động hóa xử lý sự	5	5

	cố; cung cấp RESTful API cho phép thực thi đầy đủ chức năng quản trị, giám sát, phản ứng sự cố từ xa.		
IX	NHÂN SỰ TRIỂN KHAI		
1	Quản lý dự án: Nhà thầu bố trí 01 cán bộ quản lý dự án có chứng chỉ PMP hoặc PRINCE2 còn hiệu lực.	5	5
2	Kỹ sư triển khai: Nhà thầu bố trí tối thiểu 01 kỹ sư triển khai tích hợp và hỗ trợ kỹ thuật tốt nghiệp đại học trở lên chuyên ngành công nghệ thông tin, an toàn thông tin, điện tử viễn thông hoặc tương đương; có chứng chỉ chuyên môn cấp độ quản trị/triển khai (administrator/engineer) trở lên do chính hãng sản xuất giải pháp được chào cấp (ví dụ: CrowdStrike CCFA, Palo Alto Networks XDR Engineer, SentinelOne Administrator hoặc tương đương), còn hiệu lực tại thời điểm đóng thầu, kèm mã số/đường dẫn tra cứu trực tuyến; là kỹ sư của hãng hoặc kỹ sư của nhà thầu được hãng chứng thực; có kinh nghiệm triển khai từ 02 dự án tương tự trở lên với vai trò đầu mối hỗ trợ kỹ thuật và có hợp đồng lao động chính thức còn thời hạn từ 01 năm trở lên.	5	5
Tổng điểm		175	210

Nhà thầu được đánh giá đáp ứng năng lực kỹ thuật khi tổng điểm đánh giá tối thiểu đạt 175/210 điểm và phải đáp ứng các yêu cầu điểm tối thiểu của bảng trên.

Mẫu số 1
ĐƠN CHÀO HÀNG

_____, ngày ____ tháng ____ năm ____

Kính gửi: Ngân hàng thương mại cổ phần Sài Gòn - Hà Nội

Sau khi nghiên cứu Hồ sơ yêu cầu chào hàng mà chúng tôi đã nhận được, chúng tôi, ____ [*Ghi tên bên chào hàng*], cam kết thực hiện gói chào hàng ____ [*Ghi tên gói chào hàng*] theo đúng yêu cầu của Hồ sơ yêu cầu chào hàng với tổng số tiền là ____ [*Ghi giá trị bằng số, bằng chữ và đồng tiền chào giá*]⁽¹⁾ cùng với biểu giá kèm theo. Thời gian thực hiện hợp đồng là ____ [*Ghi thời gian thực hiện tất cả các công việc theo yêu cầu của gói chào hàng*].

Chúng tôi đồng ý với các điều kiện tài chính thương mại theo hồ sơ yêu cầu chào hàng.

Nếu Hồ sơ chào hàng của chúng tôi được chấp nhận, chúng tôi cam kết cung cấp hàng hóa theo đúng nội dung đã nêu trong bảng chào giá và trong thỏa thuận hợp đồng.

Hồ sơ Chào hàng này có hiệu lực trong thời gian ____ ngày, kể từ ____ giờ, ngày ____ tháng ____ năm ____ [*Ghi thời điểm hết hạn nộp HSCH*].

Đại diện hợp pháp của bên chào hàng⁽²⁾
[*Ghi tên, chức danh, ký tên và đóng dấu⁽³⁾*]

Ghi chú:

- (1) Trường hợp đại diện theo pháp luật của bên chào hàng ủy quyền cho cấp dưới ký đơn chào giá thì phải gửi kèm theo Giấy ủy quyền theo Mẫu số 2 Phần này. Trường hợp tại Điều lệ công ty, Quyết định thành lập chi nhánh hoặc tại các tài liệu khác liên quan có phân công trách nhiệm cho cấp dưới ký đơn chào hàng thì phải gửi kèm theo bản chụp các văn bản, tài liệu này (không cần lập Giấy ủy quyền theo Mẫu số 2 Phần này). Trước khi ký kết hợp đồng, bên chào hàng được lựa chọn phải trình chủ đầu tư bản chụp được chứng thực của các văn bản, tài liệu này. Trường hợp phát hiện thông tin kê khai ban đầu là không chính xác thì bên chào hàng bị coi là vi phạm Luật Đấu thầu.

Mẫu số 2

GIẤY ỦY QUYỀN ⁽¹⁾

Hôm nay, ngày ____ tháng ____ năm ____, tại ____

Tôi là ____ [*Ghi tên, số CMND hoặc số hộ chiếu, chức danh của người đại diện theo pháp luật của bên chào hàng*], là người đại diện theo pháp luật của ____ [*Ghi tên bên chào hàng*] có địa chỉ tại ____ [*Ghi địa chỉ của bên chào hàng*] bằng văn bản này ủy quyền cho ____ [*Ghi tên, số CMND hoặc số hộ chiếu, chức danh của người được ủy quyền*] thực hiện các công việc sau đây trong quá trình tham gia chào hàng gói chào hàng ____ [*Ghi tên gói chào hàng*] thuộc dự án ____ [*Ghi tên dự án*] do ____ [*Ghi tên bên mời chào hàng*] tổ chức:

[- Ký đơn chào giá;

- Ký các văn bản, tài liệu để giao dịch với bên mời chào hàng trong quá trình tham gia chào hàng, kể cả văn bản đề nghị làm rõ HSYCCH và văn bản giải trình, làm rõ HSYCCH

- Tham gia quá trình thương thảo, hoàn thiện hợp đồng;

- Ký đơn kiến nghị trong trường hợp bên chào hàng có kiến nghị;

- Ký kết hợp đồng với chủ đầu tư nếu được lựa chọn.] ⁽²⁾

Người được ủy quyền nêu trên chỉ thực hiện các công việc trong phạm vi ủy quyền với tư cách là đại diện hợp pháp của ____ [*Ghi tên bên chào hàng*]. ____ [*Ghi tên bên chào hàng*] chịu trách nhiệm hoàn toàn về những công việc do ____ [*Ghi tên người được ủy quyền*] thực hiện trong phạm vi ủy quyền.

Giấy ủy quyền có hiệu lực kể từ ngày ____ đến ngày ____ ⁽³⁾. Giấy ủy quyền này được lập thành ____ bản có giá trị pháp lý như nhau, người ủy quyền giữ ____ bản, người được ủy quyền giữ ____ bản.

Người được ủy quyền

[Ghi tên, chức danh, ký tên và đóng dấu (nếu có)]

Người ủy quyền

[Ghi tên người đại diện theo pháp luật của bên chào hàng, chức danh, ký tên và đóng dấu]

Ghi chú:

(1) Trường hợp ủy quyền thì bản gốc giấy ủy quyền phải được gửi cho bên mời chào hàng cùng với đơn dự thầu theo hồ sơ yêu cầu chào hàng. Việc ủy quyền của người đại diện theo pháp luật của bên chào hàng cho cấp phó, cấp dưới, giám đốc chi nhánh, người đứng đầu văn phòng đại diện của bên chào hàng để thay mặt cho người đại diện theo pháp luật của bên chào hàng thực hiện một hoặc các nội dung công việc nêu trên đây. Việc sử dụng con dấu trong trường hợp được ủy quyền có thể là dấu của bên chào hàng hoặc dấu của đơn vị mà cá nhân liên quan được ủy quyền. Người được ủy quyền không được tiếp tục ủy quyền cho người khác.

(2) Phạm vi ủy quyền bao gồm một hoặc nhiều công việc nêu trên.

(3) Ghi ngày có hiệu lực và ngày hết hiệu lực của giấy ủy quyền phù hợp với quá trình tham gia chào giá.

Mẫu số 3
HỢP ĐỒNG TƯƠNG TỰ DO BÊN CHÀO HÀNG THỰC HIỆN ⁽¹⁾

_____, ngày ____ tháng ____ năm ____

Tên bên chào hàng: _____ *[Ghi tên đầy đủ của bên chào hàng]*
 Thông tin về từng hợp đồng, mỗi hợp đồng cần đảm bảo các thông tin sau đây :

STT	Tên hợp đồng	Số hợp đồng	Ngày tháng HĐ	Giá trị HĐ	Tên chủ đầu tư	Mô tả tính chất tương tự
1						
2						
3						
4						
5						
6						
7						
8						

Đại diện hợp pháp của bên chào hàng
[Ghi tên, chức danh, ký tên và đóng dấu]

