TỔNG CÔNG TY QUẢN LÝ BAY VIỆT NAM
**TRUNG TÂM ĐÀO TẠO - HUẤN LUYỆN NGHIỆP VỤ QUẢN LÝ BAY**

Số: 1345 /TTĐTHL-ĐT
V/v mời báo giá gói đào tạo chuyên gia bảo mật của Cisco

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

*Hà Nội, ngày 21 tháng 7 năm 2025*

Kính gửi: Quý công ty

Trung tâm Đào tạo - Huấn luyện nghiệp vụ Quản lý bay (Trung tâm Đào tạo - Huấn luyện) có nhu cầu mời báo giá gói đào tạo chuyên gia bảo mật của Cisco (Chi tiết tại phụ lục kèm theo).

Kính mời các Công ty quan tâm gửi báo giá gói dịch vụ trên để làm cơ sở xem xét.

Thời gian tiếp nhận: Trước 14h00 ngày 23/7/2025.

Hình thức gửi báo giá: Bản cứng (đóng dấu đỏ).

Địa chỉ nhận báo giá:

- Trung tâm Đào tạo - Huấn luyện nghiệp vụ Quản lý bay; Số 5 ngõ 200 đường Nguyễn Sơn, Phường Bồ Đề, TP Hà Nội.

- Người liên hệ: Bà Nguyễn Thị Hồng Minh; Số điện thoại: 0916712008

Mong nhận được sự hợp tác của Quý công ty.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Lưu: VT, ĐT (hm02b).

**GIÁM ĐỐC**

M.S.C.N: 0100108624 - C.T.T.N.H.H - TRUNG TÂM ĐÀO TẠO-HUẤN LUYỆN NGHIỆP VỤ QUẢN LÝ BAY - CHI NHÁNH TỔNG CÔNG TY QUẢN LÝ BAY VIỆT NAM - CÔNG TY TNHH - THÀNH PHỐ HÀ NỘI

**Nguyễn Đình Tuấn**

# Phụ lục

*(Kèm theo Văn bản số: 1345/TTĐTHL-ĐT ngày 21 tháng 7 năm 2025)*

| Stt | Yêu cầu | Số lượng | ĐVT | Đơn giá VNĐ | Thành tiền |
|---|---|---|---|---|---|
| 1 | Chi phí đào tạo:<br>**1. Thông tin chung các khoá học về đào tạo chuyên gia bảo mật của Cisco:**<br>**1.1 Chuyên gia bảo mật mạng CCNP Security (Cisco Certified Network Professional Security)**<br>a. Tên khoá học: Chuyên gia bảo mật mạng CCNP Security (Cisco Certified Network Professional Security):<br>b. Thời lượng đào tạo: 5 ngày<br>c. Thời gian thực hiện: dự kiến Quý III/2025<br>d. Quy mô lớp học: 01 lớp, dự kiến 20 người.<br>e. Hình thức đào tạo: Trực tuyến<br>f. Nội dung đào tạo:<br>Module 1: Giới thiệu về dòng sản phẩm Cisco ASA<br>- Giới thiệu về các tính năng của sản phẩm ASA<br>- Giới thiệu về các dòng sản phẩm ASA<br>Module 2: Thực thi các chức năng kết nối cơ bản và quản lý thiết bị<br>- Bắt đầu với ASA và Cisco ASDM<br>- Cấu hình cho các interface và định tuyến tĩnh<br>- Cấu hình các tính năng cơ bản để quản lý thiết bị<br>- Cấu hình quản lý truy nhập<br>Module 3: Triển khai các tính năng điều khiển truy cập trên ASA<br>- Cấu hình điều khiển truy nhập cơ bản<br>- Sử dụng Cisco ASA Modular<br>- Điều chỉnh tính năng Stateful Inspection cơ bản<br>- Cấu hình các chính sách lớp ứng dụng<br>- Cấu hình điều khiển truy nhập nâng cao<br>- Cấu hình giới hạn tài nguyên<br>- Cấu hình chính sách người dùng<br>Module 4: Triển khai các tính năng tích hợp trên Cisco ASA | 1 | gói | | |

| | | | | | |
|---|---|---|---|---|---|
| | - Triển khai NAT<br>- Cấu hình các tính năng hoạt động trong suốt trên ASA<br>Module 5: Triển khai các tính năng ảo hóa và sẵn sàng cao trên Cisco ASA<br>- Triển khai các tính năng ảo hóa<br>- Triển khai các tính năng redundant<br>- Triển khai các tính năng sẵn sàng nâng cao Active/Standby Failover<br>Module 6: Tích hợp thêm các modular bảo mật trên Cisco ASA<br>- Giới thiệu về khả năng tích hợp modular<br>- Tích hợp modular AIP-SSM và AIP-SSC<br>- Tích hợp modular CSC-SSM<br>Module 7: Giới thiệu về cơ chế phát hiện và phòng chống xâm nhập, phần mềm Cisco IPS và các thiết bị hỗ trợ<br>- Đánh giá cơ chế phát hiện và phòng chống xâm nhập<br>- Lựa chọn phần mềm Cisco IPS, phần cứng và các ứng dụng hỗ trợ<br>- Đánh giá các phương pháp phân tích lưu lượng mạng IPS, các khả năng lẩn tránh và các biện pháp đối phó<br>- Lựa chọn kiến trúc mạng IPS và triển khai IDS<br>Module 8: Lắp đặt và vận hành các bộ cảm biến Cisco IPS<br>- Tích hợp bộ cảm biến Cisco IPS vào mạng<br>- Thực hiện khởi tạo cấu hình cho các bộ cảm biến<br>- Quản lý các thiết bị Cisco IPS<br>Module 9: Áp dụng các chính sách bảo mật Cisco IPS<br>- Cấu hình phân tích lưu lượng cơ bản<br>- Thực thi Cisco IPS Signatures và Responses<br>- Cấu hình Cisco IPS Signature Engines và Signature Database<br>- Triển khai quá trình hoạt động Anomaly-Based<br>Module 10: Tối ưu hóa việc phân tích lưu lượng và đáp ứng cho môi trường mạng<br>- Tùy chính phân tích lưu lượng<br>- Quản lý False Positives và Fal Negatives<br>- Nâng cao chất lượng Alarm và Response<br>Module 11: Quản lý và phân tích các sự kiện<br>- Lắp đặt và tích hợp Cisco IPS Manager Express với các bộ cảm biến Cisco IPS<br>- Quản lý và nghiên cứu các sự kiện sử dụng Cisco IPS Manager Express | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | - Sử dụng Cisco IME Reporting và Notifications<br>- Tích hợp Cisco IPS với Cisco Security Manager và Cisco Sercurity MARS<br>- Sử dụng Cisco IntelliShield Database và các dịch vụ<br>Module 12: Triển khai các giải pháp ảo hóa, độ tin cậy và hiệu năng cao<br>- Sử dụng các bộ cám biến ảo Cisco IPS<br>- Triển khai Cisco IPS cho hiệu năng và độ tin cậy cao<br>Module 13: Cấu hình và vận hành phần cứng Cisco IPS<br>- Cấu hình và vận hành các module Cisco ASA AIP-SSM và AIP-SSC-5<br>- Cấu hình và vận hành các midule Cisco ISR IPS AIM và IPS NME<br>- Cấu hình và vận hành Cisco IDSM-2<br>Module 14: Tổng quan về kiến trúc và công nghệ ASA<br>- Vai trò của VPN và khả năng hỗ trợ của ASA<br>- Cấu hình các chính sách, kế thừa và các thuộc tính<br>Module 15: Giải pháp Cisco Clientless Remote-Access VPN<br>- Triển khai giải pháp Clientless SSL VPN<br>- Các thiết lập nâng cao Clientless SSL VPN<br>- Tùy chỉnh Clientless Portal<br>- Xác thực và cấp quyền nâng cao trong Clientless SSL VPN<br>- Tính sẵn sàng và hiệu năng của Clientless SSL<br>Module 16: Giải pháp Cisco AnyConnect Remote-Access VPN<br>- Triển khai giải pháp AnyConnect Remote-Access VPN<br>- Xác thực và cấp quyền nâng cao trong AnyConnect VPNs<br>- Triển khai và quản lý nâng cao cho AnyConnect Client<br>- Cấp phép trong AnyConnect sử dụng AAA and DAPs<br>- Hiệu năng và tính sẵn sàng của AnyConnect<br>Module 17: Cisco Secure Desktop<br>- Cisco Secure Desktop<br>Module 18: Giải pháp Cisco Ipsec Remote-Access Client<br>- Triển khai và quản lý Cisco VPN Client<br>Module 19: Giải pháp Cisco Easy VPN<br>- Triển khai giải pháp Easy VPN<br>- Xác thực và cấp phép trong Easy VPN<br>- Xác thực nâng cao trong Easy VPN | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | - Tính sẵn sàng và hiệu năng cho Easy VPN<br>- Hoạt động Easy VPN sử dụng ASA 5505 như một thành phần client hardware<br>Module 20: Giải pháp Cisco Ipsec Site-to-Site VPN<br>- Triển khai IPSec Site-to-Site VPNs<br>- Các chiến lược đảm bảo hiệu năng và tính sẵn sàng cao cho Performance Ipsec Site-to-Site VPN<br>**1.2 Khóa đào tạo bảo mật hệ thống mạng với giãi pháp IPS thế hệ mới của Cisco -Cisco SSFIPS (Securing Networks with Cisco Firepower Next-Generation IPS SSFIPS):**<br>a. Tên khoá học: Khóa đào tạo bảo mật hệ thống mạng với giãi pháp IPS thế hệ mới cùa Cisco -Cisco SSFIPS (Securing Networks with Cisco Firepower Next-Generation IPS SSFIPS):<br>b. Thời lượng đào tạo: 4 ngày<br>c. Thời gian thực hiện: dự kiến Quý III/2025<br>d. Quy mô lớp học: 01 lớp, dự kiến 18-20 người.<br>e. Hình thức đào tạo: Trực tuyến<br>f. Nội dung đào tạo:<br>- Cisco Firepower Threat Defense Overview<br>- Cisco Firepower NGFW Device Configuration<br>- Cisco Firepower NGFW Traffic Control<br>- Cisco Firepower Discovery<br>- Implementing Access Control Policies<br>- Security Intelligence<br>- File Control and Advanced Malware Protection<br>- Next-Generation Intrusion Prevention Systems<br>- Network Analysis Policies<br>- Detailed Analysis Techniques<br>- Detailed Analysis Techniques (cont.)<br>- Cisco Firepower Platform Integration<br>- Alerting and Correlation Policies<br>- System Administration<br>- Cisco Firepower Troubleshooting<br>Lab outline<br>- Initial Configuration<br>o FMC configuration<br>o Network Object creation and Variable Set | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | o Security Zones<br>o Basic Access Control<br>o Device registration<br>o Platform settings<br>- Network Configuration<br>o Interface, Routes and NAT<br>- Threat Configuration<br>o Network Discovery policy<br>o Malware & File policy<br>o Decryption policy<br>o Intrusion/Network Analysis policy<br>- Access Control<br>o Access Control Policy Settings<br>o Rules<br>o Encrypted Visibility Engine<br>- Advanced Lab<br>o CSDAC in FMC<br>o Packet-Tracer in Firewall Threat Defense<br>o Threat Protection & AttackIQ<br>**2. Tài liệu khoá học:** Tài liệu bằng bản mềm.<br>**3. Yêu cầu giáo viên:**<br>- Có bằng đại học trở lên một trong các chuyên ngành: CNTT, hệ thống thông tin, khoa học máy tính, toán – tin ứng dụng, an toàn thông tin, điện tử, truyền thông, điện tử viễn thông, mạng máy tính và truyền thông dữ liệu.<br>- Có kinh nghiệm tối thiểu 05 năm tham gia giảng dạy về CNTT hoặc tối thiểu 01 hợp đồng đào tạo với vai trò là giáo viên về nội dung của khoá học mà giáo viên sẽ tham gia giảng dạy.<br>**4. Hồ sơ năng lực của nhà cung cấp** | | | | |
| | **Giá: ..... (Bằng chữ:.....)**<br>Giá trên là giá trọn gói đã bao gồm thuế, phí, lệ phí (nếu có) và các chi phí liên quan | | | | |