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

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

Số: 1430 /TTĐTHL-ĐT
V/v mời báo giá khóa đào tạo tập huấn về An toàn thông tin và An ninh mạng

Hà Nội, ngày 30 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 tổ chức khóa đào tạo tập huấn về An toàn thông tin và An ninh mạng *(Chi tiết tại phụ lục kèm theo)*.

Kính mời các Công ty quan tâm gửi báo giá khóa đào tạo trên để làm cơ sở xem xét.

Thời gian tiếp nhận: Trước 16h00 ngày 01/8/2025.

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, Hà Nội.

- Người liên hệ: Bà Tạ Thu Trang, số điện thoại: 0906.655.623

Mong nhận được sự hợp tác của Quý công ty.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VT, ĐT (02b).

GIÁM ĐỐC

M.S.C.N:0100108624-014-C.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 1430 /TTĐTHL-ĐT ngày 30 tháng 7 năm 2025)

Stt	Yêu cầu	Số lượng	ĐVT	Đơn giá VNĐ	Thành tiền
1	Chi phí đào tạo: Khóa đào tạo tập huấn về An toàn thông tin và An ninh mạng **1. Thời lượng đào tạo:** 03 ngày (có cả ngày nghỉ cuối tuần). **2. Thời gian thực hiện:** Từ cuối tháng 8/2025 **3. Qui mô lớp học:** 03 lớp, 30-50 người/lớp. **4. Hình thức, địa điểm học:** Học trực tiếp tại 03 khu vực: Hà Nội, Đà Nẵng, TP Hồ Chí Minh. **5. Nội dung khóa học:** Chuyên đề 1 1. Giới thiệu tổng quan - Bối cảnh an ninh mạng – toàn cầu, APAC, Việt Nam. - Phân tích các sự cố nổi bật 2024–nửa đầu 2025. 2. Xu hướng & mối đe doạ tiềm ẩn năm 2025 - AI + tội phạm mạng, deepfake, phishing. - IoT & mối đe dọa mới. - Ransomware, APT, leak dữ liệu. - Case study: các cuộc tấn công gần đây. 3. Khung pháp lý hiện hành - Phân tích Luật 2018: quyền, nghĩa vụ, biện pháp. - Diễn giải Nghị định 53/2022. - Vai trò lực lượng chuyên trách, cấp quản lý & DN. - Bài tập tình huống pháp lý – đối phó sự cố, xử lý nội dung vi phạm. 4: Updates & chính sách mới - Tầm nhìn & nội dung Luật An ninh mạng 2025. - Cam kết quốc tế, liên minh ứng phó. - Ảnh hưởng đến doanh nghiệp: compliance, chuẩn hóa, cập nhật tiêu chuẩn. Chuyên đề 2 1: Các khái niệm cơ bản về An toàn thông tin - Định nghĩa quan trọng: + An toàn thông tin (Information Security) + An ninh mạng (Cybersecurity) + Bảo mật (Confidentiality), Toàn vẹn (Integrity), Sẵn sàng (Availability) – Tam giác CIA + Xác thực (Authentication), Ủy quyền	1	gói		

	(Authorization), Non-repudiation - Phân biệt ATTT và AT mạng - Nguyên tắc bảo mật 5 yếu tố: Chính sách – Con người – Quy trình – Công nghệ – Giám sát - Các chuẩn thông dụng: ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls Thảo luận nhóm: "Nếu mất tính sẵn sàng trong hệ thống ERP sẽ ảnh hưởng gì?" 2: Rủi ro & nguy cơ mất ATTT trong doanh nghiệp hiện nay - Các dạng mối đe dọa phổ biến: Mối đe dọa từ bên ngoài: ▪ Phishing, Social Engineering ▪ Ransomware, Malware tấn công vào hệ thống máy chủ ▪ DDoS & APT (Advanced Persistent Threat) -Mối đe dọa từ bên trong: ▪ Nhân viên lạm dụng quyền ▪ Sai sót do thiếu nhận thức -Top rủi ro hiện nay tại Việt Nam: - Rò rỉ dữ liệu khách hàng (CRM, ERP) - Tấn công vào hạ tầng đám mây - Lợi dụng AI để tạo deepfake, phishing nâng cao - Chi phí trung bình cho sự cố bảo mật & tác động đến uy tín - Quy trình đánh giá rủi ro theo ISO 27005 -Thảo luận và thực hành - Sự cố ransomware tại một ngân hàng Việt Nam – phân tích nguyên nhân và hậu quả - Demo tấn công ransomeware vào hạ tầng ảo hóa VMware 3: Các mô hình triển khai an toàn thông tin trong doanh nghiệp - Mô hình truyền thống vs Mô hình hiện đại - Perimeter Security → Zero Trust Architecture - 3 mô hình triển khai ATTT phổ biến: - Tập trung (Centralized) – Tất cả bảo mật tại trung tâm - Phân tán (Decentralized) – Tại từng bộ phận - Kết hợp (Hybrid) – Phù hợp doanh nghiệp lớn - Các thành phần chính trong kiến trúc bảo mật doanh nghiệp: - Firewall, IDS/IPS, Endpoint Protection				

	- SIEM, DLP, IAM (Identity & Access Management) - Mô hình quản lý sự cố (Incident Response Plan) -Thảo luận 4: Tổng quan về SOC & thành phần trong SOC - SOC là gì? - Trung tâm điều hành an ninh (Security Operation Center) - Vai trò: Giám sát, phát hiện, phản ứng, điều tra - Chức năng chính của SOC: - Monitoring & Detection – Giám sát 24/7 - Incident Response – Xử lý sự cố - Threat Intelligence – Phân tích mối đe dọa - Compliance – Đảm bảo tuân thủ luật & tiêu chuẩn - Các thành phần công nghệ trong SOC: - EDR - XDR - SIEM: Splunk, QRadar, ELK - SOAR: Tự động hóa xử lý sự cố - UEBA: Phân tích hành vi người dùng - Threat Intel Platform - Nhân sự trong SOC: - Level 1: Analyst – Giám sát sự kiện - Level 2: Incident Responder – Điều tra, xử lý - Level 3: Threat Hunter – Săn tìm mối đe dọa - SOC Manager: Quản trị, chiến lược - Mô hình SOC: - In-house SOC - Managed SOC (MSSP) - Hybrid SOC Demo thực tế: - Giới thiệu dashboard SIEM (Splunk hoặc ELK) - Ví dụ xử lý cảnh báo từ Firewall → phân tích log → tạo Incident Ticket -Thảo luận nhóm: - Giả lập sự cố Phishing → xử lý theo quy trình SOC -Chuyên đề 3 1: Quản trị an ninh mạng theo ISO 27001 & NIST mới nhất - ISO/IEC 27001:2022 (phiên bản mới nhất)				

	- 11 điều khoản chính, 4 nhóm điều khiển mới - Tích hợp quản trị rủi ro và bảo mật trong chiến lược kinh doanh - Các bước triển khai ISO 27001 trong thực tế doanh nghiệp - NIST Cybersecurity Framework (CSF) 2.0 – 2024 Update - 6 chức năng chính: Identify – Protect – Detect – Respond – Recover – Govern - Cách áp dụng NIST để đánh giá maturity level - So sánh ISO & NIST: Khi nào dùng ISO, khi nào dùng NIST? - Vai trò của lãnh đạo: - Thiết lập governance structure cho an ninh mạng - Gắn KPI bảo mật vào quản trị doanh nghiệp -Thảo luận: Doanh nghiệp bạn đang ở mức maturity nào (theo NIST)? 2: Chiến lược an ninh mạng cho lãnh đạo -Tại sao cần chiến lược? - 80% doanh nghiệp bị tấn công nghiêm trọng do thiếu chiến lược bảo mật dài hạn - Các thành phần của chiến lược an ninh mạng: - Đánh giá rủi ro & phân tích GAP (theo ISO 27005/NIST) - Xác định tầm nhìn & mục tiêu bảo mật - Thiết lập mô hình quản trị (Governance Model) - Lộ trình đầu tư & ngân sách bảo mật (CAPEX/OPEX) - Chính sách bảo mật & đào tạo nhân sự - Tích hợp an ninh mạng vào chiến lược chuyển đổi số - Báo cáo ATTT cho Hội đồng quản trị – phải thể hiện gì? Thảo luận 3: Quy trình Ứng cứu sự cố (Incident Response) chuẩn NIST - 6 giai đoạn IRP theo NIST SP 800-61 Rev.2: - Preparation – Xây dựng kế hoạch IR, phân công vai trò - Detection & Analysis – Xác định sự cố, phân loại mức độ - Containment – Ngăn chặn lan rộng - Eradication – Loại bỏ nguyên nhân gốc				

	- Recovery – Khôi phục hệ thống an toàn - Lessons Learned – Báo cáo, cải tiến chính sách - Vai trò của lãnh đạo trong mỗi giai đoạn: - Kích hoạt IR Team & phê duyệt nguồn lực - Ra quyết định pháp lý, truyền thông, tài chính - Đàm phán với cơ quan quản lý nhà nước - Demo: Sơ đồ quy trình IR + Dashboard giám sát 4: Workshop mô phỏng & quản trị khủng hoảng - Kịch bản 1: Tấn công ransomware vào ERP – Có trả tiền chuộc hay không? - Kịch bản 2: Lộ dữ liệu 10.000 khách hàng – Xử lý truyền thông và báo cáo nhà nước - Kịch bản 3: Website thương mại điện tử bị DDoS trong mùa cao điểm -Thảo luận: - Chia nhóm lãnh đạo → Ra quyết định trong 20 phút → Trình bày giải pháp - Học bài học thực tế từ các vụ việc lớn (Colonial Pipeline, Vietcombank phishing…) **6. Tài liệu:** 1 bản cứng/học viên **7. Yêu cầu giáo viên**: - 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 an toàn thông tin, bảo mật; - 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; - Tối thiểu 1 giáo viên là cán bộ Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Bộ Công An (A05) trực tiếp giảng dạy. **8. Hồ sơ năng lực của nhà cung cấp**				
Giá …………………… bằng chữ:…………………………………………………….. **Giá trên là giá trọn gói đã bao gồm thuế VAT (nếu có) và các chi phí khác liên quan**					