Phụ lục

NỘI DUNG ĐÀO TẠO, BỒI DƯỠNG (dự kiến 1 buổi)

(Đính kèm Kế hoạch số 5423/KH-SGDĐT ngày 05 tháng 12 năm 2025 của Sở Giáo dục và Đào tạo)

Mục tiêu	Nội dung chính	Phương pháp	Thời lượng (Phút)
Phần I: Khai mạc & Bối cảnh (Tầm quan trọng)	1.1. Giới thiệu & Mục tiêu	Giới thiệu Trainer, mục tiêu khóa học.	10
	1.2. Bối cảnh & Sự cần thiết	Thảo luận mở: Dùng danh sách thuật ngữ để khởi động. Trình bày xu hướng số hóa, thách thức từ AI, Máy tính lượng tử, và các Case Study Ransomware, Thất thoát dữ liệu tại Việt Nam.	35
	1.3. Cơ sở Pháp lý	Tóm tắt các tiêu chuẩn, quy định quốc tế (GDPR, NIST CSF) và trong nước (Luật ATTT mạng, NĐ 85) mà tổ chức cần tuân thủ. Lưu ý: Chỉ tập trung vào những điều người dùng cuối cần biết.	15
	Kiểm tra nhanh (Q&A)	Đặt câu hỏi nhanh về các thuật ngữ và sự kiện đã học.	5
Phần II: Các mối đe dọa & Thuật ngữ cơ bản (Hiểu rõ rủi ro)	2.1. Yếu tố Con người & Tấn công Phishing/Social Engineering	Phân tích quy trình tấn công Phishing và Social Engineering. Bài tập tương tác: Cho ví dụ email giả mạo và yêu cầu học viên nhận diện.	30
	2.2. Malware và Rủi ro thiết bị/mạng	Phân loại các loại mã độc phổ biến (Ransomware, Trojan, Spyware) và cách nhận biết máy tính bị nhiễm. Thảo luận về rủi ro khi sử dụng Wi-Fi công cộng và BYOD (thiết bị cá nhân).	30
	2.3. Quy tắc Vàng về Mật khẩu & Đa yếu tố	Thực hành: Hướng dẫn tạo mật khẩu mạnh theo khuyến nghị mới (dài, là cụm từ). Giải thích nguyên tắc MFA/2FA và lý do cần sử dụng.	25
Phần III: Phòng vệ, Phát hiện và Phục hồi (Trách	3.1. Khung NIST CSF 2.0 và Trách nhiệm cá nhân	Áp dụng mô hình Identify - Protect - Detect - Respond - Recover (Nhận diện - Phòng vệ - Phát hiện - Phản ứng - Phục hồi) cho hành vi cá nhân:	35

Mục tiêu	Nội dung chính	Phương pháp	Thời lượng (Phút)
nhiệm cá nhân theo NIST CSF)		- Protect: Các biện pháp phòng vệ (chống Phishing, cập nhật phần mềm, sử dụng VPN/chỉ mạng công ty). - Detect/Respond: Dấu hiệu phát hiện và quy trình báo cáo sự cố (người/bộ phận cần liên hệ ngay lập tức). - Recover: Nguyên tắc Sao lưu dự phòng 3-2-1.	
Phần IV: Tổng kết & Tài nguyên hỗ trợ	4.1. Giới thiệu Giải pháp hỗ	Giới thiệu các dịch vụ và công cụ mà tổ chức đang sử dụng (hoặc có thể sử dụng) như VNPT SmartIR, DNS Protect, MSS để củng cố niềm tin về hệ thống phòng thủ. Lưu ý: Giới thiệu ngắn gọn, không đi sâu vào kỹ thuật.	20
	4.2. Hoạt động Nhóm/Case Study cuối khóa	Yêu cầu học viên thảo luận nhanh (10 phút) để giải quyết một tình huống ATTT thực tế (ví dụ: Bạn nhận được email yêu cầu chuyển tiền gấp từ CEO, bạn sẽ làm gì?).	25
	4.3. Tổng kết & Kiểm tra cuối khóa	Tổng hợp các điểm chính. (Tùy chọn) 10 câu hỏi trắc nghiệm kiến thức.	10
	Tổng thời lượng thực tế:		**240 phút (4 giờ)**