Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật mang tính kỹ thuật thuần túy và các yêu cầu khác liên quan đến việc cung cấp dịch vụ (trừ giá). Yêu cầu về kỹ thuật phải được nêu đầy đủ, rõ ràng và cụ thể để làm cơ sở cho nhà thầu lập E-HSDT.

Trong yêu cầu về kỹ thuật không được đưa ra các điều kiện nhằm hạn chế sự tham gia của nhà thầu hoặc nhằm tạo lợi thế cho một hoặc một số nhà thầu gây ra sự cạnh tranh không bình đẳng.

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

Dự án: Trang bị bản quyền phần mềm và đào tạo và đánh giá nhận thức ATTT cho CBCNV toàn EVNSPC

Địa điểm thực hiện dự án: Tổng công ty Điện lực miền Nam, 72 đường Hai Bà Trưng, phường Sài Gòn, Thành phố Hồ Chí Minh

Quy mô dự án:

- *Trang bị bản quyền phần mềm và đào tạo và đánh giá nhận thức ATTT cho CBCNV toàn EVNSPC*

STT	Nội dung yêu cầu	Đơn vị tính	Số lượng	Yêu cầu về cung cấp dịch vụ thuộc gói thầu	Thời gian thực hiện gói thầu	Ghi chú
1	**Khóa đào tạo nhận thức an toàn thông tin (ATTT) bao gồm:** - Đào tạo nhận thức ATTT; - Giả lập Phising Email; - Đánh giá kiểm tra và cải tiến; - Thời gian sử dụng 01 năm, không giới hạn số lần về đào tạo, phising và đánh giá kiểm tra; - Hình thức đào tạo: Trực tuyến; - Số lượng: 508 người.	Gói	01	- Trang bị bản quyền phần mềm và đào tạo và đánh giá nhận thức ATTT cho CBCNV toàn	Trong vòng 45ngày kể từ ngày hợp đồng có hiệu lực, trong đó: - Thời gian cung cấp bản quyền: trong vòng 15 ngày kể từ ngày hợp đồng có hiệu lực. - Thời gian triển khai, đào tạo: trong vòng 30 ngày kể từ ngày hợp đồng có hiệu lực. - Thời gian đánh giá, kiểm tra, cải tiến hệ	*Trang bị bản quyền phần mềm và đào tạo và đánh giá nhận thức ATTT cho CBCNV toàn EVNSPC*

				EVNSPC -Theo quy định tại Chương V	thống: trong vòng 45 ngày kể từ ngày hợp đồng có hiệu lực.	

2. Mục tiêu công việc:

Nâng cao nhận thức bảo mật của CBCNV vận hành hệ thống VTCNTT toàn EVNSPC:

- Xây dựng văn hóa bảo mật mạnh mẽ trong tổ chức.
- Trang bị cho nhân viên vận hành hệ thống VTCNTT kiến thức và kỹ năng cần thiết để nhận diện và ứng phó với các mối đe dọa an ninh mạng.

Đảm bảo tuân thủ các tiêu chuẩn bảo mật quốc tế và yêu cầu pháp luật.

3. Yêu cầu kỹ thuật của gói thầu:

Đáp ứng theo yêu cầu kỹ thuật và tiêu chuẩn đánh giá chi tiết

4. Giải pháp và phương pháp luận:

Không

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Thực hiện đủ các nội dung theo yêu cầu của E-HSMT.

TỔNG CÔNG TY ĐIỆN LỰC MIỀN NAM
CÔNG TY CÔNG NGHỆ THÔNG TIN ĐIỆN LỰC MIỀN NAM

BÁO CÁO KINH TẾ KỸ THUẬT

DỰ ÁN ĐẦU TƯ

TRANG BỊ BẢN QUYỀN PHẦN MỀM VÀ ĐÀO TẠO VÀ ĐÁNH GIÁ NHẬN THỨC ATTT CHO CBCNV TOÀN EVNSPC

TP.Hồ Chí Minh – 08/2025

TỔNG CÔNG TY ĐIỆN LỰC MIỀN NAM
CÔNG TY CÔNG NGHỆ THÔNG TIN ĐIỆN LỰC MIỀN NAM

TP. Hồ Chí Minh, ngày 19 tháng 8 năm 2025

BÁO CÁO KINH TẾ KỸ THUẬT

DỰ ÁN:

TRANG BỊ BẢN QUYỀN PHẦN MỀM VÀ ĐÀO TẠO VÀ ĐÁNH GIÁ NHẬN THỨC ATTT CHO CBCNV TOÀN EVNSPC

TẬP 2 – YÊU CẦU KỸ THUẬT VÀ TIÊU CHUẨN ĐÁNH GIÁ

Tổ xây dựng dự án :

1.Thiết lập : Lai Chiêu Cường
2.Kiểm tra : Nguyễn Hải Nam
3.Chủ nhiệm dự án : Lai Chiêu Cường

GIÁM ĐỐC

M.S.C.N. 0300942001-008 C.T.N.H.H
CHI NHÁNH TỔNG CÔNG TY ĐIỆN LỰC MIỀN NAM TNHH - CÔNG TY CÔNG NGHỆ THÔNG TIN ĐIỆN LỰC MIỀN NAM
TP. HỒ CHÍ MINH

Đặng Nguyên Phương

TỔNG CÔNG TY
ĐIỆN LỰC MIỀN NAM

CÔNG TY CÔNG NGHỆ THÔNG TIN
ĐIỆN LỰC MIỀN NAM

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

BIÊN CHẾ BÁO CÁO KINH TẾ KỸ THUẬT DỰ ÁN "TRANG BỊ BẢN QUYỀN PHẦN MỀM VÀ ĐÀO TẠO VÀ ĐÁNH GIÁ NHẬN THỨC ATTT CHO CBCNV TOÀN EVNSPC"

Dự án đầu tư **"Trang bị bản quyền phần mềm và đào tạo và đánh giá nhận thức ATTT cho CBCNV toàn EVNSPC"** là dự án đầu tư sử dụng vốn SXKD, nhằm trang bị phần mềm đào tạo ATTT nâng cao nhận thức về bảo mật cho CBVNV vận hành hệ thống VTCNTT trong Tổng công ty Điện lực miền Nam đáp ứng yêu cầu của Quyết định 717/EVN-VTCNTT ngày 31/5/2025 về việc ban hành Quy định đảm bảo An ninh mạng và An toàn thông tin trong Tập đoàn Điện lực Việt Nam, có tổng mức đầu tư khoảng 381 triệu VNĐ. Căn cứ theo Khoản 2 Điều 10 của 73/2019/NĐ-CP ngày 05/09/2019, hồ sơ dự án được thiết kế 01 bước.

Theo đó, Hồ sơ dự án có biên chế hồ sơ thành 02 tập như sau:

- Tập 1 : Thuyết minh Báo cáo kinh tế kỹ thuật
- **Tập 2: Yêu cầu kỹ thuật và Tiêu chuẩn đánh giá**

TẬP 2 – YÊU CẦU KỸ THUẬT VÀ TIÊU CHUẨN ĐÁNH GIÁ

MỤC LỤC

I. Yêu cầu về kỹ thuật

1. Giới thiệu chung

- **Nội dung:**
  - **Phần mềm đào tạo nhận thức an toàn thông tin (ATTT) bao gồm:** Đào tạo nhận thức ATTT; Giả lập Phising Email; Đánh giá kiểm tra và cải tiến với cho 508 Cán bộ nhân viên EVNSPC trong thời gian sử dụng 01 năm theo hình thức học trực tuyến.
  - Để nhằm mục đích nâng cao nhận thức bảo mật của toàn bộ nhân viên: Xây dựng văn hóa bảo mật mạnh mẽ trong tổ chức; trang bị cho nhân viên kiến thức và kỹ năng cần thiết để nhận diện và ứng phó với các mối đe dọa an ninh mạng và đảm bảo tuân thủ các tiêu chuẩn bảo mật quốc tế và yêu cầu pháp luật.
  - Lợi ích của phần mềm đào tạo nhận thức an toàn thông tin (ATTT):
    - Tăng cường khả năng kiểm soát: Nhân viên nhận diện tốt hơn các mối đe dọa và hành động đúng đắn để giảm thiểu rủi ro.
    - Giảm thiểu rủi ro sự cố bảo mật: Tránh được các cuộc tấn công như phishing hoặc ransomware nhờ nâng cao nhận thức.
    - Nâng cao hiệu quả hoạt động: Nhân viên làm việc an toàn hơn, giảm nguy cơ làm gián đoạn hoạt động kinh doanh.
    - Bảo vệ dữ liệu quan trọng: Đảm bảo dữ liệu nhạy cảm được bảo vệ khỏi truy cập trái phép.
    - Cải thiện hình ảnh tổ chức: Thể hiện sự chuyên nghiệp và cam kết bảo mật thông tin cho khách hàng và đối tác.
- **Địa điểm thực hiện**: Văn phòng Tổng công ty Điện lực miền Nam – 72 Hai Bà Trưng, Phường Sài Gòn Thành phố Hồ Chí Minh.

- **Quy mô**:

STT	Hạng mục thuê	Đơn vị tính	Số lượng
1	Khóa đào tạo nhận thức an toàn thông tin (ATTT) bao gồm: - Đào tạo nhận thức ATTT; - Giả lập Phising Email; - Đánh giá kiểm tra và cải tiến; - Thời gian sử dụng 01 năm, không giới hạn số lần về đào tạo, phising và đánh giá kiểm tra; - Hình thức đào tạo: Trực tuyến; - Số lượng: 508 người.	Gói	01

2. Yêu cầu kỹ thuật

a. Yêu cầu về kỹ thuật chung:

STT	Tên hàng hóa hoặc dịch vụ liên quan	Yêu cầu
I.	**Yêu cầu năng lực**	
1	Đáp ứng chứng chỉ về An toàn thông tin	Đáp ứng chứng nhận về hệ thống quản lý an toàn thông tin (ISMS) theo tiêu chuẩn quốc tế ISO/IEC **27001:2022**
2	Đáp ứng về chứng chỉ Hệ thống Quản lý Dịch vụ (SMS).	Đáp ứng chứng nhận về quản lý dịch vụ công nghệ thông tin (ITSM) **ISO/IEC 20000**
II.	**Yêu cầu kỹ thuật chung**	
1	Bản quyền phần mềm đào tạo nhận thức an toàn thông tin	**Đăng nhập theo tài khoản được cấp:** cung cấp tài khoản quản trị hệ thống ứng dụng bao gồm tên đăng nhập và mật khẩu để quản trị viên tự do quản lý toàn bộ ứng dụng.
2		**Đường đi của quản trị viên trong hệ thống** o Tạo các chiến dịch nâng cao nhận thức với nhiều ngôn ngữ Anh/ Việt/ Hoa o Tạo các chiến dịch kiểm tra trắc nghiệm o Tạo các chiến dịch mô phỏng lừa đảo o Phối hợp hoặc thay đổi thứ tự các chiến dịch để sáng tạo ra được nhiều phương pháp nâng cao nhận thức hiệu quả hơn, thú vị hơn.
3		**Phân hệ kiến thức:**

		○ Nhận thức bảo mật – Lý thuyết: Tất cả những kiến thức an toàn thông tin cần có dành cho người dùng Internet ○ Kiểm tra trắc nghiệm – Thực hành: Dựa trên những kiến thức từ khoá đào tạo nhận thức bảo mật ○ Mô phỏng chiến dịch lừa đảo – Thực hành như thật: Phân chia theo đặc thù ngành nghề, phòng ban, hành vi.
4		**Chiến dịch nâng cao nhận thức**: được hiển thị dưới Animation Video/Interactive Learning (video hoạt hình hoá bằng các nhân vật theo đó là các tính năng nổi bật của phương pháp tương tác thú vị, tăng khả năng tiếp thu)
5		**Kiểm tra trắc nghiệm:** Được hiển thị dưới dạng danh sách các câu hỏi trắc nghiệm được quản lý khéo léo bằng tính năng chống gian lận bằng hình thức chọn câu hỏi ngẫu nhiên nhằm đảm bảo rằng học viên sẽ không thể sao chép lẫn nhau khi tham gia, đảm bảo kết quả đầu ra chất lượng nhất
6		**Mô phỏng lừa đảo:** Là hệ thống mô phỏng như thật các thao tác mà kẻ xấu thao tác để lừa đảo, nhắm vào một hoặc nhiều tệp khách hàng nhất định và sau đó gửi hàng loạt các email giả mạo như thật từ trang web đến đường link, từ tên người gửi đến email người nhận. Giả mạo hoàn toàn nội dung bên trong email nhằm lừa đảo nhiều người nhất có thể.
7		**Thông báo & gợi ý:** tự động gửi email thông báo đến học viên khi có khoá học và bài kiểm tra, thông báo tới học viên thời gian bắt đầu và kết thúc khoá học cũng như đốc thúc học viên tham gia khoá học và bài kiểm tra khi cần thiết.

8		Hệ thống báo cáo được thiết kế để hỗ trợ tổ chức theo dõi tiến độ, đo lường hiệu quả, và cải thiện nhận thức bảo mật của nhân viên một cách liên tục: 1. **Báo cáo tổng quan các chỉ số quan trọng** như tổng số tài khoản tham gia chương trình đào tạo, các chiến dịch phishing, Điểm số nhận thức bảo mật tổng thể, Tỷ lệ hoàn thành và tham gia, Hiệu quả phishing,…. 2. **Báo cáo tổng quan theo phòng ban (Departments General Report):** Xếp hạng nhận thức bảo mật theo phòng ban; Hiệu suất đào tạo; Hiệu quả phishing; Báo cáo chi tiết theo tháng. 3. **Báo cáo chi tiết (Detail Report):** Kết quả nhận thức bảo mật từng tài khoản; Tỷ lệ hoàn thành bài học; Tỷ lệ vượt bài kiểm tra; Danh sách chưa hoàn thành. 4. **Báo cáo phishing (Phishing By Department):** Tỷ lệ bị phishing qua mỗi chiến dịch (Số lượng gửi phishing, số lượng mở nội dung, số lượng nhấn vào đường dẫn liên kết, số lượng điền thông tin….) ;
9		**Xuất báo cáo theo các định dạng**: Excel và PDF
10		**Nền tảng cloud-native, hỗ trợ multi-tenant**
11		**MICROLEARNING giải pháp đào tạo nhận thức súc tích và thực tiễn**
12		**AI phân tích hành vi và kết quả học tập để đề xuất nội dung phù hợp nhất với từng người học**
13		**Nội dung khóa học:** • **Tổng quan về an ninh mạng** o Giới thiệu khái niệm cơ bản về an ninh mạng, tầm quan trọng của việc bảo vệ thông tin cá nhân và tổ chức trong môi trường số. o Nêu bật các loại mối đe dọa phổ biến và cách

		nhận biết để phòng tránh. • **Quản lý mật khẩu và an toàn trực tuyến** o Hướng dẫn tạo và quản lý mật khẩu mạnh, an toàn, phù hợp với thực tế sử dụng. o Trang bị kỹ năng bảo vệ tài khoản email, trình duyệt web, và nhận biết các liên kết độc hại. o Giảm thiểu nguy cơ bị tấn công thông qua email phishing hoặc các trang web giả mạo. • **Bảo mật thiết bị cá nhân và văn phòng** o Cung cấp các biện pháp bảo mật cần thiết để bảo vệ thiết bị cá nhân như máy tính, điện thoại, và phần mềm trước các mối đe dọa mạng. o Đảm bảo an toàn thông tin trong môi trường văn phòng và khi làm việc từ xa, bao gồm quản lý quyền truy cập và sao lưu dữ liệu. • **Nhận diện và phòng ngừa các mối đe dọa** o Phân tích các hình thức tấn công lừa đảo (phishing) và giả mạo phổ biến, giúp nhân viên nhận biết và ứng phó kịp thời. o Hiểu rõ cách hoạt động của các phần mềm độc hại như virus, ransomware, và mã độc, từ đó áp dụng các biện pháp phòng ngừa hiệu quả. • **An toàn trong điện toán và dữ liệu** o Trình bày các nguyên tắc bảo vệ dữ liệu và quyền truy cập, giúp nhân viên xử lý thông tin an toàn trên môi trường số. o Áp dụng các phương pháp mã hóa và bảo mật tiên tiến để bảo vệ thông tin nhạy cảm • **Kỹ năng ứng phó sự cố** o Trang bị các chiến lược phản ứng khi xảy ra sự cố an ninh mạng, từ phát hiện sớm đến phục hồi hệ thống. o Hướng dẫn quy trình báo cáo và xử lý sự cố để giảm thiểu thiệt hại. • **Lời khuyên và thực hành bảo mật** o Chia sẻ các mẹo bảo mật thực tiễn, phù hợp với từng tình huống làm việc cụ thể. o Xây dựng thói quen tốt để bảo vệ thông tin cá

		nhân và tổ chức trong suốt quá trình làm việc.

b. Yêu cầu về kỹ thuật cụ thể

STT	Tiêu chí kỹ thuật	Yêu cầu chi tiết
Yêu cầu đào tạo trực tuyến: có các bài học tối thiểu, hoặc nội dung tương đương như bên dưới, yêu cầu liệt kê các bài học hiện ứng dụng đang có sẵn.		
1	Bảo vệ máy tính cá nhân	-An toàn khi làm việc tại nhà -Bảo vệ thiết bị di động -Mang thiết bị cá nhân tới nơi làm việc
2	Bảo mật thư điện tử và tin nhắn cá nhân	-Bảo vệ email -Bảo vệ bản thân khỏi các cuộc tấn công lừa đảo -Lừa đảo qua thư điện tử doanh nghiệp
3	Lừa đảo Social Engineering và Phishing	-Bảo vệ email -Bảo vệ bản thân khỏi các cuộc tấn công lừa đảo -Lừa đảo qua thư điện tử doanh nghiệp -Một số kỹ thuật tấn công lừa đảo
4	Sử dụng và quản lý mật khẩu	-Phương pháp bảo vệ mật khẩu -Các công cụ và mẹo bảo mật mật khẩu
5	Không gian làm việc an toàn	-Bảo mật chốn công sở -Cẩn trọng với wifi công cộng -An toàn khi làm việc tại nhà
6	Nguy cơ, bảo mật khi sử dụng wifi công cộng	Cẩn trọng với wifi công cộng
7	Sử dụng điện thoại thông minh an toàn	Bảo vệ thiết bị di động, smart devides
8	Theo dõi thông tin, hành vi cá nhân trên mạng xã hội và môi trường Internet	-An toàn trực tuyến cho trẻ em và gia đình. -Sử dụng internet an toàn
9	Lướt web an toàn	Sử dụng internet an toàn

10	Phòng chống phần mềm độc hại	Tổng quan về mạng và phần mềm độc hại
11	Những hiểu nhầm thường thấy trong việc đảm bảo ATTT	An ninh mạng là gì? những thói quen xấu và một số hình thức tấn công mạng phổ biến
12	Xử lý các sự cố bảo mật	Xử lý các sự cố bảo mật: Khóa học đưa ra các hành vi sai phổ biến mà người dùng dễ mắc phải và đưa ra một vài cách giải quyết
13	Các chỉ dẫn căn bản và thiết thực về ATTT dành cho người dùng cuối	Toàn bộ khoá học về đào tạo nhận thức ATTT đều là kiến thức cơ bản mà người dùng cuối cần phải có.
14	Các chỉ dẫn căn bản và thiết thực về ATTT dành cho lãnh đạo	Toàn bộ khoá học. Đây là khoá học dành cho mọi người khi sử dụng Internet, nên tất cả mọi thành viên trong doanh nghiệp đều cần nắm. Và khoá đào tạo này cũng cần cho các cấp lãnh đạo
15	Cho phép bổ sung nội dung tùy chỉnh của Khách hàng (Video/file đào tạo)	Cho phép bổ sung nội dung tùy chỉnh của Khách hàng (Video/file đào tạo)
Yêu cầu đánh giá sau đào tạo: Cho phép bổ sung, tuy chỉnh các câu hỏi kiểm tra sau đào tạo. Yêu cầu cung cấp thêm các thông tin sau:		
16	Số lượng câu hỏi về nhận thức an toàn thông tin có sẵn trong ngân hàng câu hỏi.	Bộ câu hỏi 210 câu, bao quát kiến thức về ATTT dành cho tất cả học viên
	Phương thức đánh giá sau đào tạo (trắc nghiệm, bài tập tình huống, demo/thực hành,...)	- Đáp ứng câu hỏi trắc nghiệm. - Demo giả lập phishing/ thực hành
Yêu cầu về chiến dịch tấn công lừa đảo (Phishing)		

17	Phạm vi dịch vụ sẽ bao gồm không giới hạn số lượng các cuộc tấn công thử nghiệm trong thời gian cung cấp dịch vụ.	Đáp ứng được các thể loại: + Phishing Link + Attachment + Data Entry + Spear Phishing + QR Code
18	Giả lập tấn công web	Giả lập tấn công web bằng cách lây nhiễm mã độc khi người dùng click vào link trên website. (Đường dẫn website)
19	Gửi email chứa mã độc tới một hoặc nhiều nạn nhân cùng một lúc.	Thực hiện các tình huống gửi email có chứa đính kèm mã độc tới một nạn nhân có chủ đích hoặc nhiều nạn nhân cùng một lúc.
20	Cho phép lựa chọn Mức độ khó (Difficulty) cho đợt kiểm tra.	Cho phép quản trị viên lựa chọn Mức độ khó (Difficulty) cho đợt kiểm tra để đánh giá năng lực của học viên.
21	Cho phép sử dụng nhiều Email Template (nhiều mẫu phishing) trong cùng 01đợt kiểm tra/chiến dịch	Cho phép sử dụng nhiều Email Template (nhiều mẫu phishing) trong cùng 01đợt kiểm tra/chiến dịch
22	Cho phép sử dụng 1 email bất kỳ trong 508 học viên để sử dụng để gởi (sender) trong đợt kiểm tra/chiến dịch	Cho phép giả mạo 1 email bất kỳ trong 508 học viên đã mua để gởi (sender) trong đợt kiểm tra/chiến dịch. Trừ trường hợp Email của học viên đó có áp dụng các cơ chế chống giả mạo, đối với trường hợp này sẽ ưu tiên sử dụng domain Email gần giống với chỉ định của khách hàng.
23	Tạo email Phishing bằng AI	Áp dụng AI trong việc tạo email Phishing, giúp việc tạo chiến dịch trở nên hiệu quả và nhanh chóng
Yêu cầu về báo cáo		
24	Cung cấp báo cáo tổng quát và chi tiết về đào tạo	- Cung cấp báo cáo tổng quát và chi tiết về đào tạo (thời gian học, số bài đã học,điểm số)

		- Cung cấp báo cáo kết quả đánh giá sau đào tạo, kết quả đạt hay không đạt theo các định dạng: Excel và PDF
25	Cung cấp báo cáo kết quả đánh giá sau đào tạo	Cung cấp cho người quản trị được báo cáo kết quả đánh giá sau đào tạo của các người dùng khi tham gia khóa học.
26	Cung cấp báo cáo chi tiết đối với mỗi loại giả lập tấn công	Cung cấp báo cáo chi tiết đối với mỗi loại giả lập tấn công như: thống kê hành vi người dùng đã thực hiện, chưa thực hiện, các ảnh hưởng mất an toàn thông tin (nếu có).
Yêu cầu về cấu hình		
27	Lựa chọn và thiết lập lịch cho đào tạo	Quản trị viện có thể lựa chọn và thiết lập lịch cho việc đào tạo
28	Lựa chọn và thiết lập lịch cho tấn công xâm nhập	Quản trị viên có thể lựa chọn và thiết lập lịch cho các bài học tấn công xâm nhập
29	Cho phép nhập/thay thế danh sách người dùng được đào tạo	- Có thể tự nhập danh sách người dùng được đào tạo theo định dạng file csv/xls. - Trường hợp thay thế, hệ thống sẽ tính là 1 người dùng mới
30	Lựa chọn nhóm người dùng/nhóm đối tượng được áp dụng các khóa đào tạo	Lựa chọn danh sách các bài đào tạo và nhóm đối tượng phù hợp áp dụng cho khóa đào tạo
31	Tự động nhắc nhở người dùng về lịch đào tạo	Hệ thống sẽ tự động nhắc nhở người dùng về lịch đào tạo
Yêu cầu về đào tạo		
32	Đào tạo quản trị và vận hành hệ thống	Đào tạo quản trị và vận hành hệ thống
	Đào tạo chỉnh sửa (customize) giao diện, chức năng ứng dụng	Đào tạo chỉnh sửa (customize), giao diện, chức năng của ứng dụng trong khả năng hiện có của sản phẩm phù hợp với yêu cầu của người quản trị.
	Đào tạo người sử dụng cuối	Đào tạo, hướng dẫn sử dụng cho người sử dụng cuối sử dụng chương trình.

Yêu cầu về tài liệu		
33	Tài liệu hướng dẫn vân hành và quản trị hệ thống	Tài liệu hướng dẫn vân hành và quản trị hệ thống
	Tài liệu hướng dẫn sử dụng hệ thống đối với nhân sự đào tạo	Tài liệu hướng dẫn sử dụng hệ thống đối với nhân sự đào tạo
Yêu cầu về khắc phục sự cố		
34	Bảo đảm sẵn sàng hoạt động 24/7.	Hệ thống phải bảo đảm sẵn sàng hoạt động liên tục 24/7 phục vụ đào tạo người dùng cuối.
35	Hỗ trợ xử lý sự cố 24/7	Hỗ trợ xử lý sự cố 24/7 qua điện thoại, email, tin nhắn đa phương tiện.
36	Đảm bảo hiệu suất của phần mềm luôn sẵn sàng khi nhiều 508 người truy cập cùng 1 lúc.	Đảm bảo hiệu suất của phần mềm luôn sẵn sàng khi nhiều 508 người truy cập cùng một lúc.
37	Cam kết khắc phục sự cố trong thời gian sớm nhất.	Cam kết khắc phục sự cố: chậm nhất là 04 giờ. Đối với những lỗi phát sinh chưa rõ nguyên nhân, sau khi khắc phục lỗi, sự cố. Nhà thầu có trách nhiệm tìm hiểu nguyên nhân và phản hồi cho khách hàng khoảng thời gian sớm nhất.
38	Cam kết phần mềm không chứa mã độc hại, không có backdoor, hardcode... gây ảnh hưởng đến An toàn thông tin cho khách hàng	Cam kết phần mềm không chứa mã độc hại, không có backdoor, hardcode,… có thể bị tấn công khai thác, đánh cắp dữ liệu, gây mất an toàn cho phần mềm và hệ thống Công nghệ thông tin Khách hàng.
	Bảo đảm tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng..	Có các biện pháp bảo đảm tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.

	Khắc phục hoàn toàn các lỗ hổng bảo mật của sản phẩm phần mềm (bao gồm phần mềm, cơ sở dữ liệu và các cấu phần khác của sản phẩm phần mềm) trước khi đưa vào sử dụng dựa trên kết quả đánh giá bảo mật và trong thời gian khách hàng sử dụng	Khắc phục hoàn toàn các lỗ hổng bảo mật của sản phẩm phần mềm (bao gồm phần mềm, cơ sở dữ liệu và các cấu phần khác của sản phẩm phần mềm) trước khi đưa vào sử dụng dựa trên kết quả đánh giá bảo mật và trong thời gian khách hàng sử dụng.
39	Bộ tài liệu chứng nhận kiểm thử bảo mật ứng dụng	Cung cấp tài liệu chứng nhận kiểm thử bảo mật ứng dụng đối với hệ thống gồm kiểm thử xâm nhập (pentest) và kiểm tra rà soát mã nguồn.
	Chứng nhận kiểm thử bảo mật cho môi trường Cloud .	Cung cấp tài liệu chứng nhận kiểm thử bảo mật đối với môi trường Cloud được triển khai.

II. Tiêu chuẩn đánh giá

1. Tiêu chuẩn đánh giá

Tiêu chuẩn đánh giá về kỹ thuật: Phương pháp đánh giá **Đạt/ Không đạt.**

Theo đó:

- Đánh giá về kỹ thuật được kết luận **Đạt** khi **tất cả** đặc tính, thông số kỹ thuật của hàng hóa đáp ứng Đạt yêu cầu của HSMT.
- Đánh giá về kỹ thuật được kết luận **Không Đạt** khi có từ **Một** trở lên đặc tính, thông số kỹ thuật của hàng hóa không đáp ứng (Không Đạt) yêu cầu của HSMT.

2. Tiêu chí đánh giá yêu cầu về kỹ thuật chung

STT	Nội dung	Mô tả cụ thể	Tiêu chuẩn đánh giá		
			Đạt	**Chấp nhận được**	**Không đạt**
	I. Yêu cầu về năng lực				
1	Đáp ứng chứng chỉ về An toàn thông tin	Đáp ứng chứng nhận về hệ thống quản lý an toàn thông tin (ISMS) theo tiêu chuẩn quốc tế ISO/IEC **27001:2022**	Nhà thầu cung cấp tài liệu chứng minh (Viện dẫn chương, trang, mục tham chiếu)		Nhà thầu không cung cấp được tài liệu chứng minh (Viện dẫn chương, trang, mục

					tham chiếu)
2	Đáp ứng về chứng chỉ *Hệ thống Quản lý Dịch vụ (SMS).*	Đáp ứng chứng nhận về quản lý dịch vụ công nghệ thông tin (ITSM) **ISO/IEC 20000**	Nhà thầu cung cấp tài liệu chứng minh (Viện dẫn chương, trang, mục tham chiếu)		Nhà thầu không cung cấp được tài liệu chứng minh (Viện dẫn chương, trang, mục tham chiếu)
	II. Yêu cầu kỹ thuật chung				
1	Bản quyền phần mềm đào tạo nhận thức an toàn thông tin (ATTT)	**Đăng nhập theo tài khoản được cấp:** cung cấp tài khoản quản trị hệ thống ứng dụng bao gồm tên đăng nhập và mật khẩu để quản trị viên tự do quản lý toàn bộ ứng dụng.	Như yêu cầu.		Không như yêu cầu.
2		**Đường đi của quản trị viên trong hệ thống**	Như yêu cầu.		Không như yêu cầu.

		○ Tạo các chiến dịch nâng cao nhận thức với nhiều ngôn ngữ Anh/ Việt/ Hoa ○ Tạo các chiến dịch kiểm tra trắc nghiệm ○ Tạo các chiến dịch mô phỏng lừa đảo ○ Phối hợp hoặc thay đổi thứ tự các chiến dịch để sáng tạo ra được nhiều phương pháp nâng cao nhận thức hiệu quả hơn, thú vị hơn.			
3		**Phân hệ kiến thức:** ○ Nhận thức bảo mật – Lý thuyết: Tất cả những kiến thức an toàn thông tin cần có dành cho người dùng Internet ○ Kiểm tra trắc nghiệm – Thực hành: Dựa trên những kiến thức từ khoá đào tạo nhận thức bảo mật ○ Mô phỏng chiến dịch lừa đảo – Thực hành như thật: Phân chia theo đặc thù ngành nghề, phòng ban, hành vi.	Như yêu cầu.		Không như yêu cầu.

4		**Chiến dịch nâng cao nhận thức**: được hiển thị dưới Animation Video/Interactive Learning (video hoạt hình hoá bằng các nhân vật theo đó là các tính năng nổi bật của phương pháp tương tác thú vị, tăng khả năng tiếp thu)	Như yêu cầu.		Không như yêu cầu.
5		**Kiểm tra trắc nghiệm:** Được hiển thị dưới dạng danh sách các câu hỏi trắc nghiệm được quản lý khéo léo bằng tính năng chống gian lận bằng hình thức chọn câu hỏi ngẫu nhiên nhằm đảm bảo rằng học viên sẽ không thể sao chép lẫn nhau khi tham gia, đảm bảo kết quả đầu ra chất lượng nhất	Như yêu cầu.		Không như yêu cầu.
6		**Mô phỏng lừa đảo:** Là hệ thống mô phỏng như thật các thao tác mà kẻ xấu thao tác để lừa đảo, nhắm vào một hoặc nhiều tệp khách hàng nhất định và sau đó gửi hàng loạt các email giả mạo như thật từ trang web đến đường link, từ tên người gửi đến email người nhận. Giả mạo hoàn toàn nội	Như yêu cầu.		Không như yêu cầu.

		dung bên trong email nhằm lừa đảo nhiều người nhất có thể.			
7		**Thông báo & gợi ý:** tự động gửi email thông báo đến học viên khi có khoá học và bài kiểm tra, thông báo tới học viên thời gian bắt đầu và kết thúc khoá học cũng như đốc thúc học viên tham gia khoá học và bài kiểm tra khi cần thiết.	Như yêu cầu.		Không như yêu cầu.
8		Hệ thống báo cáo được thiết kế để hỗ trợ tổ chức theo dõi tiến độ, đo lường hiệu quả, và cải thiện nhận thức bảo mật của nhân viên một cách liên tục: 1. **Báo cáo tổng quan các chỉ số quan trọng** như tổng số tài khoản tham gia chương trình đào tạo, các chiến dịch phishing, Điểm số nhận thức bảo mật tổng thể, Tỷ lệ hoàn thành và tham gia, Hiệu quả phishing,…. 2. **Báo cáo tổng quan theo phòng ban (Departments General Report):** Xếp hạng	Như yêu cầu.		Không như yêu cầu.

		nhận thức bảo mật theo phòng ban; Hiệu suất đào tạo; Hiệu quả phishing; Báo cáo chi tiết theo tháng. 3. **Báo cáo chi tiết (Detail Report):** Kết quả nhận thức bảo mật từng tài khoản; Tỷ lệ hoàn thành bài học; Tỷ lệ vượt bài kiểm tra; Danh sách chưa hoàn thành. 4. **Báo cáo phishing (Phishing By Department):** Tỷ lệ bị phishing qua mỗi chiến dịch (Số lượng gửi phishing, số lượng mở nội dung, số lượng nhấn vào đường dẫn liên kết, số lượng điền thông tin….) ;			
9		**Xuất báo cáo theo các định dạng**: Excel và PDF	Như yêu cầu.		Không như yêu cầu.
10		**Nền tảng cloud-native, hỗ trợ multi-tenant**	Như yêu cầu.		Không như yêu cầu.
11		**MICROLEARNING giải pháp đào tạo nhận thức súc tích và thực tiễn**	Như yêu cầu.		Không như yêu cầu.

12		**AI phân tích hành vi và kết quả học tập để đề xuất nội dung phù hợp nhất với từng người học**	Như yêu cầu.		Không như yêu cầu.
13		**Nội dung khóa học:** • **Tổng quan về an ninh mạng** o Giới thiệu khái niệm cơ bản về an ninh mạng, tầm quan trọng của việc bảo vệ thông tin cá nhân và tổ chức trong môi trường số. o Nêu bật các loại mối đe dọa phổ biến và cách nhận biết để phòng tránh. • **Quản lý mật khẩu và an toàn trực tuyến** o Hướng dẫn tạo và quản lý mật khẩu mạnh, an toàn, phù hợp với thực tế sử dụng. o Trang bị kỹ năng bảo vệ tài khoản email, trình duyệt web, và nhận biết các liên kết độc hại. o Giảm thiểu nguy cơ bị tấn công thông qua email phishing hoặc các trang web giả mạo. • **Bảo mật thiết bị cá nhân và văn phòng** o Cung cấp các biện pháp bảo mật cần thiết để bảo vệ thiết bị cá nhân như máy tính, điện thoại, và phần mềm	Như yêu cầu.		Không như yêu cầu.

		trước các mối đe dọa mạng. o Đảm bảo an toàn thông tin trong môi trường văn phòng và khi làm việc từ xa, bao gồm quản lý quyền truy cập và sao lưu dữ liệu. • **Nhận diện và phòng ngừa các mối đe dọa** o Phân tích các hình thức tấn công lừa đảo (phishing) và giả mạo phổ biến, giúp nhân viên nhận biết và ứng phó kịp thời. o Hiểu rõ cách hoạt động của các phần mềm độc hại như virus, ransomware, và mã độc, từ đó áp dụng các biện pháp phòng ngừa hiệu quả. • **An toàn trong điện toán và dữ liệu** o Trình bày các nguyên tắc bảo vệ dữ liệu và quyền truy cập, giúp nhân viên xử lý thông tin an toàn trên môi trường số. o Áp dụng các phương pháp mã hóa và bảo mật tiên tiến để bảo vệ thông tin nhạy cảm • **Kỹ năng ứng phó sự cố** o Trang bị các chiến lược phản ứng khi xảy ra sự cố an ninh mạng, từ phát hiện			

		sớm đến phục hồi hệ thống. ○ Hướng dẫn quy trình báo cáo và xử lý sự cố để giảm thiểu thiệt hại. • **Lời khuyên và thực hành bảo mật** ○ Chia sẻ các mẹo bảo mật thực tiễn, phù hợp với từng tình huống làm việc cụ thể. ○ Xây dựng thói quen tốt để bảo vệ thông tin cá nhân và tổ chức trong suốt quá trình làm việc.			

3. Tiêu chí đánh giá yêu cầu về kỹ thuật cụ thể

STT	Tiêu chí kỹ thuật	Yêu cầu chi tiết	Tiêu chuẩn đánh giá		
			Đạt	Chấp nhận đươc	Không đạt
Yêu cầu đào tạo trực tuyến: có các bài học tối thiểu, hoặc nội dung tương đương như bên dưới, yêu cầu liệt kê các bài học hiện ứng dụng đang có sẵn.					
1	Bảo vệ máy tính cá nhân	-An toàn khi làm việc tại nhà -Bảo vệ thiết bị di động -Mang thiết bị cá nhân tới nơi làm việc	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
2	Bảo mật thư điện tử và tin nhắn cá nhân	-Bảo vệ email -Bảo vệ bản thân khỏi các cuộc tấn công lừa đảo -Lừa đảo qua thư điện tử doanh nghiệp	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

3	Lừa đảo Social Engineering và Phishing	-Bảo vệ email -Bảo vệ bản thân khỏi các cuộc tấn công lừa đảo -Lừa đảo qua thư điện tử doanh nghiệp -Một số kỹ thuật tấn công lừa đảo	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
4	Sử dụng và quản lý mật khẩu	-Phương pháp bảo vệ mật khẩu -Các công cụ và mẹo bảo mật mật khẩu	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
5	Không gian làm việc an toàn	-Bảo mật chốn công sở -Cẩn trọng với wifi công cộng -An toàn khi làm việc tại nhà	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
6	Nguy cơ, bảo mật khi sử dụng wifi công cộng	Cẩn trọng với wifi công cộng	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

7	Sử dụng điện thoại thông minh an toàn	Bảo vệ thiết bị di động, smart devides	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
8	Theo dõi thông tin, hành vi cá nhân trên mạng xã hội và môi trường Internet	-An toàn trực tuyến cho trẻ em và gia đình. -Sử dụng internet an toàn	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
9	Lướt web an toàn	Sử dụng internet an toàn	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
10	Phòng chống phần mềm độc hại	Tổng quan về mạng và phần mềm độc hại	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

11	Những hiểu nhầm thường thấy trong việc đảm bảo ATTT	An ninh mạng là gì? những thói quen xấu và một số hình thức tấn công mạng phổ biến	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
12	Xử lý các sự cố bảo mật	Xử lý các sự cố bảo mật: Khóa học đưa ra các hành vi sai phổ biến mà người dùng dễ mắc phải và đưa ra một vài cách giải quyết	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
13	Các chỉ dẫn căn bản và thiết thực về ATTT dành cho người dùng cuối	Toàn bộ khoá học về đào tạo nhận thức ATTT đều là kiến thức cơ bản mà người dùng cuối cần phải có.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
14	Các chỉ dẫn căn bản và thiết thực về ATTT dành cho lãnh đạo	Toàn bộ khoá học. Đây là khoá học dành cho mọi người khi sử dụng Internet, nên tất cả mọi thành viên trong doanh nghiệp đều cần nắm. Và khoá đào tạo này cũng cần cho các cấp lãnh đạo	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

15	Cho phép bổ sung nội dung tùy chỉnh của Khách hàng (Video/file đào tạo)	Cho phép bổ sung nội dung tùy chỉnh của Khách hàng (Video/file đào tạo)	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
Yêu cầu đánh giá sau đào tạo: Cho phép bổ sung, tuy chỉnh các câu hỏi kiểm tra sau đào tạo. Yêu cầu cung cấp thêm các thông tin sau:					
16	Số lượng câu hỏi về nhận thức an toàn thông tin có sẵn trong ngân hàng câu hỏi.	Bộ câu hỏi 210 câu, bao quát kiến thức về ATTT dành cho tất cả học viên	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
	Phương thức đánh giá sau đào tạo (trắc nghiệm, bài tập tình huống, demo/thực hành,...)	- Đáp ứng câu hỏi trắc nghiệm. - Demo giả lập phishing/ thực hành	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
Yêu cầu về chiến dịch tấn công lừa đảo (Phishing)					

17	Phạm vi dịch vụ sẽ bao gồm không giới hạn số lượng các cuộc tấn công thử nghiệm trong thời gian cung cấp dịch vụ.	Đáp ứng được các thể loại: + Phishing Link + Attachment + Data Entry + Spear Phishing + QR Code	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
18	Giả lập tấn công web	Giả lập tấn công web bằng cách lây nhiễm mã độc khi người dùng click vào link trên website. (Đường dẫn website)	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
19	Gửi email chứa mã độc tới một hoặc nhiều nạn nhân cùng một lúc.	Thực hiện các tình huống gửi email có chứa đính kèm mã độc tới một nạn nhân có chủ đích hoặc nhiều nạn nhân cùng một lúc.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
20	Cho phép lựa chọn Mức độ khó (Difficulty) cho đợt kiểm tra.	Cho phép quản trị viên lựa chọn Mức độ khó (Difficulty) cho đợt kiểm tra để đánh giá năng lực của học viên.	Như yêu cầu. Viện dẫn chương,		Không như yêu cầu. Không viện dẫn chương,

			trang, mục tham chiếu		trang, mục tham chiếu
21	Cho phép sử dụng nhiều Email Template (nhiều mẫu phishing) trong cùng 01đợt kiểm tra/chiến dịch	Cho phép sử dụng nhiều Email Template (nhiều mẫu phishing) trong cùng 01đợt kiểm tra/chiến dịch	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
22	Cho phép sử dụng 1 email bất kỳ trong 508 học viên để sử dụng để gởi (sender) trong đợt kiểm tra/chiến dịch	Cho phép giả mạo 1 email bất kỳ trong 508 học viên đã mua để gởi (sender) trong đợt kiểm tra/chiến dịch. Trừ trường hợp Email của học viên đó có áp dụng các cơ chế chống giả mạo, đối với trường hợp này sẽ ưu tiên sử dụng domain Email gần giống với chỉ định của khách hàng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
23	Tạo email Phishing bằng AI	Áp dụng AI trong việc tạo email Phishing, giúp việc tạo chiến dịch trở nên hiệu quả và nhanh chóng	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
Yêu cầu về báo cáo					

24	Cung cấp báo cáo tổng quát và chi tiết về đào tạo	- Cung cấp báo cáo tổng quát và chi tiết về đào tạo (thời gian học, số bài đã học,điểm số) - Cung cấp báo cáo kết quả đánh giá sau đào tạo, kết quả đạt hay không đạt theo các định dạng: Excel và PDF	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
25	Cung cấp báo cáo kết quả đánh giá sau đào tạo	Cung cấp cho người quản trị được báo cáo kết quả đánh giá sau đào tạo của các người dùng khi tham gia khóa học.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
26	Cung cấp báo cáo chi tiết đối với mỗi loại giả lập tấn công	Cung cấp báo cáo chi tiết đối với mỗi loại giả lập tấn công như: thống kê hành vi người dùng đã thực hiện, chưa thực hiện, các ảnh hưởng mất an toàn thông tin (nếu có).	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
Yêu cầu về cấu hình					
27	Lựa chọn và thiết lập lịch cho đào tạo	Quản trị viện có thể lựa chọn và thiết lập lịch cho việc đào tạo	Như yêu cầu. Viện dẫn chương,		Không như yêu cầu. Không viện dẫn chương,

			trang, mục tham chiếu		trang, mục tham chiếu
28	Lựa chọn và thiết lập lịch cho tấn công xâm nhập	Quản trị viên có thể lựa chọn và thiết lập lịch cho các bài học tấn công xâm nhập	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
29	Cho phép nhập/thay thế danh sách người dùng được đào tạo	- Có thể tự nhập danh sách người dùng được đào tạo theo định dạng file csv/xls. - Trường hợp thay thế, hệ thống sẽ tính là 1 người dùng mới	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
30	Lựa chọn nhóm người dùng/nhóm đối tượng được áp dụng các khóa đào tạo	Lựa chọn danh sách các bài đào tạo và nhóm đối tượng phù hợp áp dụng cho khóa đào tạo	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
31	Tự động nhắc nhở người dùng về lịch đào tạo	Hệ thống sẽ tự động nhắc nhở người dùng về lịch đào tạo	Như yêu cầu. Viện dẫn chương,		Không như yêu cầu. Không viện dẫn chương,

			trang, mục tham chiếu		trang, mục tham chiếu
Yêu cầu về đào tạo					
32	Đào tạo quản trị và vận hành hệ thống	Đào tạo quản trị và vận hành hệ thống	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
	Đào tạo chỉnh sửa (customize) giao diện, chức năng ứng dụng	Đào tạo chỉnh sửa (customize), giao diện, chức năng của ứng dụng trong khả năng hiện có của sản phẩm phù hợp với yêu cầu của người quản trị.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
	Đào tạo người sử dụng cuối	Đào tạo, hướng dẫn sử dụng cho người sử dụng cuối sử dụng chương trình.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
Yêu cầu về tài liệu					

33	Tài liệu hướng dẫn vân hành và quản trị hệ thống	Tài liệu hướng dẫn vân hành và quản trị hệ thống	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
	Tài liệu hướng dẫn sử dụng hệ thống đối với nhân sự đào tạo	Tài liệu hướng dẫn sử dụng hệ thống đối với nhân sự đào tạo	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
Yêu cầu về khắc phục sự cố					
34	Bảo đảm sẵn sàng hoạt động 24/7.	Hệ thống phải bảo đảm sẵn sàng hoạt động liên tục 24/7 phục vụ đào tạo người dùng cuối.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
35	Hỗ trợ xử lý sự cố 24/7	Hỗ trợ xử lý sự cố 24/7 qua điện thoại, email, tin nhắn đa phương tiện.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

36	Đảm bảo hiệu suất của phần mềm luôn sẵn sàng khi nhiều 508 người truy cập cùng 1 lúc.	Đảm bảo hiệu suất của phần mềm luôn sẵn sàng khi nhiều 508 người truy cập cùng một lúc.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
37	Cam kết khắc phục sự cố trong thời gian sớm nhất.	Cam kết khắc phục sự cố: chậm nhất là 04 giờ. Đối với những lỗi phát sinh chưa rõ nguyên nhân, sau khi khắc phục lỗi, sự cố. Nhà thầu có trách nhiệm tìm hiểu nguyên nhân và phản hồi cho khách hàng khoảng thời gian sớm nhất.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
38	Cam kết phần mềm không chứa mã độc hại, không có backdoor, hardcode... gây ảnh hưởng đến An toàn thông tin cho khách hàng	Cam kết phần mềm không chứa mã độc hại, không có backdoor, hardcode,… có thể bị tấn công khai thác, đánh cắp dữ liệu, gây mất an toàn cho phần mềm và hệ thống Công nghệ thông tin Khách hàng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
	Bảo đảm tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng..	Có các biện pháp bảo đảm tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu

	Khắc phục hoàn toàn các lỗ hổng bảo mật của sản phẩm phần mềm (bao gồm phần mềm, cơ sở dữ liệu và các cấu phần khác của sản phẩm phần mềm) trước khi đưa vào sử dụng dựa trên kết quả đánh giá bảo mật và trong thời gian khách hàng sử dụng	Khắc phục hoàn toàn các lỗ hổng bảo mật của sản phẩm phần mềm (bao gồm phần mềm, cơ sở dữ liệu và các cấu phần khác của sản phẩm phần mềm) trước khi đưa vào sử dụng dựa trên kết quả đánh giá bảo mật và trong thời gian khách hàng sử dụng.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
39	Bộ tài liệu chứng nhận kiểm thử bảo mật ứng dụng	Cung cấp tài liệu chứng nhận kiểm thử bảo mật ứng dụng đối với hệ thống gồm kiểm thử xâm nhập (pentest) và kiểm tra rà soát mã nguồn.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu
	Chứng nhận kiểm thử bảo mật cho môi trường Cloud .	Cung cấp tài liệu chứng nhận kiểm thử bảo mật đối với môi trường Cloud được triển khai.	Như yêu cầu. Viện dẫn chương, trang, mục tham chiếu		Không như yêu cầu. Không viện dẫn chương, trang, mục tham chiếu