TIÊU CHUẨN ĐÁNH GIÁ VỀ KỸ THUẬT

Gói thầu: PTV/2026-09: Thực hiện kiểm tra, đánh giá ATTT cho các hệ thống điều khiển của Công ty Thủy điện Ialy năm 2026

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	KHÔNG ĐẠT
1	**YÊU CẦU CHUNG**		
1.1	Yêu cầu chung về bảo mật và vận hành	Đáp ứng tất cả các yêu cầu sau đây: - Nhà thầu cam kết bằng văn bản chịu trách nhiệm bảo mật toàn bộ dữ liệu và thông tin của hệ thống trong suốt quá trình thực hiện dịch vụ, không tiết lộ hoặc chia sẻ thông tin cho bất kỳ bên thứ ba nào dưới bất kỳ hình thức nào, đồng thời không cài đặt, không để lại bất kỳ phần mềm, công cụ, mã lệnh, script, agent hoặc thành phần kỹ thuật nào trên hệ thống của Chủ đầu tư. - Nhà thầu có cam kết bằng văn bản: Trong quá trình kiểm tra, đánh giá hệ thống, Nhà thầu phải tuân thủ các quy định sau: + Công tác kiểm tra phải thực hiện trực tiếp tại các Nhà máy Thủy điện, không truy cập từ xa và không kết nối Internet vào hệ thống OT. + Không được kết nối thiết bị cá nhân (laptop, ổ cứng di động) hoặc bất kỳ thiết bị lưu trữ hai chiều nào vào hệ thống OT. + Không được thay đổi Registry, Policy, cấu hình hệ thống, trạng thái thiết bị, không vô hiệu hóa dịch vụ hoặc thực hiện bất kỳ thao tác nào có thể gây treo dịch vụ, gián đoạn điều khiển, đặc biệt đối với luồng dữ liệu điều khiển thời gian thực. + Tuân thủ nguyên tắc không can thiệp hệ thống	Thuộc một trong các trường hợp sau đây: - Nhà thầu không có cam kết bằng văn bản chịu trách nhiệm bảo mật toàn bộ dữ liệu và thông tin của hệ thống trong suốt quá trình thực hiện dịch vụ, không tiết lộ hoặc chia sẻ thông tin cho bất kỳ bên thứ ba nào dưới bất kỳ hình thức nào, đồng thời không cài đặt, không để lại bất kỳ phần mềm, công cụ, mã lệnh, script, agent hoặc thành phần kỹ thuật nào trên hệ thống của Chủ đầu tư. - Nhà thầu không có cam kết bằng văn bản, hoặc có nhưng không đáp ứng một trong các yêu cầu dưới đây trong quá trình kiểm tra, đánh giá hệ thống: + Công tác kiểm tra phải thực hiện trực tiếp tại các Nhà máy Thủy điện, không truy cập từ xa và không kết nối Internet vào hệ thống OT. + Không được kết nối thiết bị cá nhân (laptop, ổ cứng di động) hoặc bất kỳ thiết bị lưu trữ hai chiều nào vào hệ thống OT. + Không được thay đổi Registry, Policy, cấu hình hệ thống, trạng thái thiết bị, không vô hiệu hóa dịch vụ hoặc thực hiện bất kỳ thao tác nào có thể gây treo dịch vụ, gián đoạn điều khiển, đặc biệt đối với luồng dữ liệu điều khiển thời gian thực.

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	**KHÔNG ĐẠT**
		(Zero-Impact). Tuyệt đối không cài đặt, triển khai hoặc thực thi bất kỳ phần mềm, công cụ hunting, tool/script, agent nào trực tiếp trên các máy chủ, máy trạm vận hành và máy giao diện HMI. + Nhà thầu chỉ được thực hiện các thao tác kỹ thuật sau khi đã xây dựng kế hoạch khôi phục nguyên trạng (Rollback) và được Chủ đầu tư đồng ý; mọi thao tác phải thực hiện thông qua máy trung gian dưới sự kiểm soát quyền truy cập đặc quyền và giám sát của Chủ quản hệ thống. - Nhà thầu có cam kết không có hành vi tự ý kết nối thiết bị lưu trữ hai chiều hoặc thực cài đặt Script/Tool lên hệ thống khi chưa có sự chấp thuận của Chủ đầu tư.	+ Tuân thủ nguyên tắc không can thiệp hệ thống (Zero-Impact). Tuyệt đối không cài đặt, triển khai hoặc thực thi bất kỳ phần mềm, công cụ hunting, tool/script, agent nào trực tiếp trên các máy chủ, máy trạm vận hành và máy giao diện HMI. + Nhà thầu chỉ được thực hiện các thao tác kỹ thuật sau khi đã xây dựng kế hoạch khôi phục nguyên trạng (Rollback) và được Chủ đầu tư đồng ý; mọi thao tác phải thực hiện thông qua máy trung gian dưới sự kiểm soát quyền truy cập đặc quyền và giám sát của Chủ quản hệ thống. - Nhà thầu không có cam kết không có hành vi tự ý kết nối thiết bị lưu trữ hai chiều hoặc thực cài đặt Script/Tool lên hệ thống khi chưa có sự chấp thuận của Chủ đầu tư.
1.2	Yêu cầu về năng lực tổ chức cung cấp dịch vụ	Có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trong đó có đăng ký dịch vụ: Cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng.	Không có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, hoặc có mà trong đó không có đăng ký dịch vụ: Cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng.
2	**YÊU CẦU KỸ THUẬT CHI TIẾT**		
2.1	Đánh giá cấu hình	Nhà thầu có đề xuất kỹ thuật về nội dung "Đánh giá cấu hình" hoặc có cam kết đáp ứng yêu cầu kỹ thuật của E-HSMT (tham chiếu Mục "3.2.1. Đánh giá cấu hình:" tại tập tin đính kèm Chương V).	Thuộc một trong các trường hợp sau đây: - Nhà thầu không có đề xuất kỹ thuật về nội dung "Đánh giá cấu hình", và cũng không có cam kết "Đánh giá cấu hình"; - Nhà thầu không có đề xuất kỹ thuật về nội dung "Đánh giá cấu hình" hoặc có cam kết "Đánh giá cấu

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	KHÔNG ĐẠT
			hình" nhưng không đáp ứng yêu cầu về kỹ thuật của E-HSMT (tham chiếu Mục "3.2.1. Đánh giá cấu hình:" tại tập tin đính kèm Chương V).
2.2	Kiểm tra mã độc và lỗ hổng bảo mật	Đề xuất kỹ thuật của nhà thầu đáp ứng tất cả các yêu cầu sau đây: - Sử dụng công cụ chuyên dụng (phần mềm rà quét chỉ được chạy từ bên trong thiết bị) để phát hiện mã độc, Rootkit, các kỹ thuật tấn công nâng cao (Memory Injection, DLL Hijacking) mà không được phép cài đặt phần mềm lên các máy tính của hệ thống OT. - Các mẫu mã độc, hoặc nghi ngờ là mã độc phải được lưu lại như một phần của báo cáo, việc chuyển các mẫu này ra ngoài phải đảm bảo thực hiện bằng các thiết bị truyền dữ liệu một chiều (Data Diode/Unidirectional Gateway). - Thực hiện rà soát và dò quét lỗ hổng bảo mật bằng các công cụ chuyên dụng theo chuẩn CVE nhằm phát hiện điểm yếu trên hệ điều hành, phần mềm ứng dụng, firmware cũng như toàn bộ môi trường IT và các giao thức OT đặc thù như Modbus, DNP3, IEC-104. - Thực hiện cập nhật các bản vá lỗi (Hotfix/Service Pack) cho hệ điều hành và thiết bị mà hãng đã phát hành miễn phí sau khi đã kiểm tra tính tương thích trong môi trường cô lập có kiểm soát. - Thực hiện Backup cấu hình và dữ liệu hệ thống trước khi tiến hành cập nhật để đảm bảo khả năng khôi phục nguyên trạng (Rollback) nếu xảy ra lỗi.	Nhà thầu không đề xuất về nội dung "Kiểm tra mã độc và lỗ hổng bảo mật"; hoặc có đề xuất nhưng thuộc một trong các trường hợp sau đây: - Không sử dụng công cụ chuyên dụng (phần mềm rà quét chỉ được chạy từ bên trong thiết bị) để phát hiện mã độc, Rootkit, các kỹ thuật tấn công nâng cao (Memory Injection, DLL Hijacking); hoặc sử dụng công cụ chuyên dụng cài đặt phần mềm lên các máy tính của hệ thống OT. - Các mẫu mã độc, hoặc nghi ngờ là mã độc không được lưu lại như một phần của báo cáo; hoặc việc chuyển các mẫu này ra ngoài không đảm bảo thực hiện bằng các thiết bị truyền dữ liệu một chiều (Data Diode/Unidirectional Gateway). - Thực hiện rà soát và dò quét lỗ hổng bảo mật bằng các công cụ chuyên dụng không theo chuẩn CVE nhằm phát hiện điểm yếu trên hệ điều hành, phần mềm ứng dụng, firmware cũng như toàn bộ môi trường IT và các giao thức OT đặc thù như Modbus, DNP3, IEC-104. - Không thực hiện cập nhật các bản vá lỗi (Hotfix/Service Pack) cho hệ điều hành và thiết bị mà hãng đã phát hành miễn phí sau khi đã kiểm tra tính tương thích trong môi trường cô lập có kiểm soát. - Không thực hiện Backup cấu hình và dữ liệu hệ thống trước khi tiến hành cập nhật để đảm bảo khả năng khôi phục nguyên trạng (Rollback) nếu xảy ra lỗi.

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	**KHÔNG ĐẠT**
2.3	Kiểm thử xâm nhập có kiểm soát	Đề xuất kỹ thuật của nhà thầu đáp ứng tất cả các yêu cầu về kỹ thuật sau đây: - Kiểm thử xâm nhập (Pentest), thực hiện các kịch bản tấn công giả lập không xâm lấn (Black-box, Gray-box) để chứng minh lỗ hổng mà không gây hại cho hệ thống. - Giám sát sự cố, triển khai giải pháp giám sát và phát hiện xâm nhập SIEM tạm thời để thu thập và phân tích nhật ký (log) trên đường truyền nhằm phát hiện các hành vi bất thường hoặc tấn công APT.	Nhà thầu không đề xuất về nội dung "Kiểm thử xâm nhập có kiểm soát"; hoặc có đề xuất nhưng thuộc một trong các trường hợp sau đây: - Không kiểm thử xâm nhập (Pentest); hoặc không thực hiện các kịch bản tấn công giả lập không xâm lấn (Black-box, Gray-box) để chứng minh lỗ hổng mà không gây hại cho hệ thống. - Không giám sát sự cố; hoặc không triển khai giải pháp giám sát và phát hiện xâm nhập SIEM tạm thời để thu thập và phân tích nhật ký (log) trên đường truyền nhằm phát hiện các hành vi bất thường hoặc tấn công APT.
2.4	Kiểm thử xâm nhập và dấu vết tấn công	Đề xuất kỹ thuật của nhà thầu đáp ứng tất cả các yêu cầu về kỹ thuật sau đây: - Thực hiện kiểm thử xâm nhập từ bên trong để đánh giá khả năng phòng thủ của hệ thống khi có tác nhân nội bộ hoặc mã độc lây lan. - Rà soát toàn diện các kết nối và tiến trình lạ đang chạy ngầm trong mạng OT để triệt tiêu mọi nguy cơ tiềm ẩn.	Nhà thầu không đề xuất về nội dung "Kiểm thử xâm nhập và dấu vết tấn công"; hoặc có đề xuất nhưng thuộc một trong các trường hợp sau đây: - Không thực hiện kiểm thử xâm nhập từ bên trong để đánh giá khả năng phòng thủ của hệ thống khi có tác nhân nội bộ hoặc mã độc lây lan. - Không rà soát toàn diện các kết nối và tiến trình lạ đang chạy ngầm trong mạng OT để triệt tiêu mọi nguy cơ tiềm ẩn.
2.5	Thiết bị và công cụ hỗ trợ	Nhà thầu có đề xuất thiết bị và công cụ hỗ trợ đáp ứng tất các yêu cầu kỹ thuật sau đây: - Thiết bị do nhà thầu đề xuất đáp ứng yêu cầu kỹ thuật của E-HSMT (tham chiếu Mục "3.3.1. Thiết bị:" thuộc Mục "3.3. Yêu cầu thiết bị và công cụ hỗ trợ:" tại tập tin đính kèm Chương V);	Thuộc một trong các trường hợp sau đây: - Không đề xuất thiết bị để thực hiện gói thầu; - Không đề xuất công cụ hỗ trợ để thực hiện gói thầu; - Thiết bị do nhà thầu đề xuất không đáp ứng yêu cầu kỹ thuật của E-HSMT (tham chiếu Mục "3.3.1. Thiết bị:"

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	**KHÔNG ĐẠT**
		- Công cụ hỗ trợ do nhà thầu đề xuất đáp ứng yêu cầu kỹ thuật của E-HSMT (tham chiếu Mục "3.3.2. Công cụ:" thuộc Mục "3.3. Yêu cầu thiết bị và công cụ hỗ trợ:" tại tập tin đính kèm Chương V).	thuộc Mục "3.3. Yêu cầu thiết bị và công cụ hỗ trợ:" tại tập tin đính kèm Chương V); - Công cụ hỗ trợ do nhà thầu đề xuất không đáp ứng yêu cầu kỹ thuật của E-HSMT (tham chiếu Mục "3.3.2. Công cụ:" thuộc Mục "3.3. Yêu cầu thiết bị và công cụ hỗ trợ:" tại tập tin đính kèm Chương V).
3	**GIẢI PHÁP VÀ PHƯƠNG PHÁP LUẬN**		
3.1	Phương pháp luận tổng thể	Nhà thầu có đề xuất Giải pháp và phương pháp luận đáp ứng tất cả các yêu cầu sau đây: - Phương pháp luận tổng thể: Phương pháp luận thực hiện được xây dựng trên cơ sở hợp nhất các tiêu chuẩn an toàn thông tin và an ninh hệ thống điều khiển công nghiệp nghiêm ngặt, bao gồm: TCVN 14423:2025, NIST SP 800-82 (Bảo mật hệ thống điều khiển công nghiệp), IEC 62443 cùng các chuẩn kiểm thử chuyên dụng như PTES/OSSTMM đối với hoạt động kiểm thử có kiểm soát; - Tiêu chuẩn và khung tham chiếu: Toàn bộ quá trình đánh giá phải được đối soát và thực hiện theo các khung tiêu chuẩn quốc tế và trong nước mới nhất như: TCVN 14423:2025, IEC 62443, NIST Cybersecurity Framework (CSF), ISO/IEC 27001 và ISO/IEC 27002; - Quy trình triển khai: Hoạt động đánh giá được thực hiện theo quy trình 06 giai đoạn, bao gồm: Chuẩn bị → Thu thập thông tin → Phân tích lỗ hổng → Kiểm thử khai thác có kiểm soát → Khắc phục/Cập	Nhà thầu không đề xuất Giải pháp và phương pháp luận; hoặc có đề xuất nhưng thuộc một trong các trường hợp sau đây: - Phương pháp luận tổng thể: Phương pháp luận thực hiện không được xây dựng trên cơ sở hợp nhất các tiêu chuẩn an toàn thông tin và an ninh hệ thống điều khiển công nghiệp nghiêm ngặt, bao gồm: TCVN 14423:2025, NIST SP 800-82 (Bảo mật hệ thống điều khiển công nghiệp), IEC 62443 cùng các chuẩn kiểm thử chuyên dụng như PTES/OSSTMM đối với hoạt động kiểm thử có kiểm soát; - Tiêu chuẩn và khung tham chiếu: Toàn bộ quá trình đánh giá không được đối soát và thực hiện theo các khung tiêu chuẩn quốc tế và trong nước mới nhất như: TCVN 14423:2025, IEC 62443, NIST Cybersecurity Framework (CSF), ISO/IEC 27001 và ISO/IEC 27002; - Quy trình triển khai: Hoạt động đánh giá không được thực hiện theo quy trình 06 giai đoạn, bao gồm: Chuẩn bị → Thu thập thông tin → Phân tích lỗ hổng

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	**KHÔNG ĐẠT**
		nhật bản vá → Hậu kiểm; - Mỗi giai đoạn phải được mô tả chi tiết về phương pháp thực hiện, thiết bị và công cụ sử dụng, đồng thời xác định rõ phương án xử lý rủi ro trước khi triển khai.	→ Kiểm thử khai thác có kiểm soát → Khắc phục/Cập nhật bản vá → Hậu kiểm; - Mỗi giai đoạn không được mô tả chi tiết về phương pháp thực hiện, thiết bị và công cụ sử dụng; hoặc không xác định rõ phương án xử lý rủi ro trước khi triển khai.
3.2	Kế hoạch công tác	Nhà thầu có đề xuất kế hoạch công tác đáp ứng tất cả các yêu cầu kỹ thuật sau đây: - Nhà thầu phải xây dựng kế hoạch công tác chi tiết, xác định rõ phạm vi công việc, danh mục hạng mục mục tiêu và mốc thời gian hoàn thành cho từng giai đoạn triển khai; - Thiết lập lộ trình triển khai cụ thể theo từng bước, xác định rõ danh mục thiết bị hỗ trợ, công cụ kỹ thuật chuyên dụng và giải pháp kỹ thuật phù hợp với đặc thù của môi trường mạng OT; - Phân bổ đội ngũ chuyên gia có năng lực và kinh nghiệm phù hợp, bao gồm các nhân sự có trình độ tương đương nhân sự chủ chốt, nhằm bảo đảm tiến độ thực hiện, chất lượng kỹ thuật và an toàn cho hệ thống trong suốt quá trình triển khai; - Phương án kỹ thuật phải bảo đảm hệ thống OT duy trì hoạt động ổn định, an toàn và liên tục, không gây gián đoạn đến hoạt động vận hành trong toàn bộ quá trình đánh giá; - Thiết lập cơ chế kiểm soát chặt chẽ luồng trao đổi dữ liệu giữa môi trường IT và OT; đồng thời triển khai các biện pháp phòng vệ chủ động nhằm phát hiện,	Nhà thầu không đề xuất kế hoạch công tác; hoặc có đề xuất nhưng thuộc một trong các trường hợp sau đây: - Nhà thầu không xây dựng kế hoạch công tác chi tiết, xác định rõ phạm vi công việc, danh mục hạng mục mục tiêu và mốc thời gian hoàn thành cho từng giai đoạn triển khai; - Không thiết lập lộ trình triển khai cụ thể theo từng bước; hoặc không xác định rõ danh mục thiết bị hỗ trợ, công cụ kỹ thuật chuyên dụng và giải pháp kỹ thuật phù hợp với đặc thù của môi trường mạng OT; - Không phân bổ đội ngũ chuyên gia có năng lực và kinh nghiệm phù hợp, bao gồm các nhân sự có trình độ tương đương nhân sự chủ chốt, nhằm bảo đảm tiến độ thực hiện, chất lượng kỹ thuật và an toàn cho hệ thống trong suốt quá trình triển khai; - Phương án kỹ thuật không bảo đảm hệ thống OT duy trì hoạt động ổn định, an toàn và liên tục; hoặc phương án kỹ thuật gây gián đoạn đến hoạt động vận hành trong toàn bộ quá trình đánh giá; - Không thiết lập cơ chế kiểm soát chặt chẽ luồng trao đổi dữ liệu giữa môi trường IT và OT; hoặc không triển khai các biện pháp phòng vệ chủ động nhằm phát hiện,

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	**KHÔNG ĐẠT**
		ngăn chặn và giảm thiểu các mối đe dọa từ bên ngoài đối với mạng điều khiển công nghiệp; - Thiết lập quy trình thông tin liên lạc và phối hợp rõ ràng với Chủ đầu tư; kịp thời thông báo, báo cáo và đề xuất phương án xử lý khi phát hiện lỗ hổng nghiêm trọng hoặc các sự cố bất thường trong hệ thống.	ngăn chặn và giảm thiểu các mối đe dọa từ bên ngoài đối với mạng điều khiển công nghiệp; - Không thiết lập quy trình thông tin liên lạc và phối hợp rõ ràng với Chủ đầu tư; hoặc không kịp thời thông báo, báo cáo và đề xuất phương án xử lý khi phát hiện lỗ hổng nghiêm trọng hoặc các sự cố bất thường trong hệ thống.
3.3	Phê duyệt phương án thi công	Nhà thầu có đề xuất hoặc có cam kết về phê duyệt phương án thi công đáp ứng yêu cầu kỹ thuật của EHSMT (tham chiếu Mục **"4.3. Phê duyệt phương án thi công:"** tại tập tin đính kèm Chương V).	Nhà thầu không có đề xuất và cũng không có cam kết về phê duyệt phương án thi công đáp ứng yêu cầu kỹ thuật của E-HSMT (tham chiếu Mục **"4.3. Phê duyệt phương án thi công:"** tại tập tin đính kèm Chương V).
4	**TIẾN ĐỘ, KIỂM TRA VÀ NGHIỆM THU DỊCH VỤ**		
4.1	Tiến độ	Nhà thầu đề xuất tổng thời gian thực hiện dịch vụ không quá 15 ngày.	Nhà thầu đề xuất tổng thời gian thực hiện dịch vụ quá 15 ngày.
4.2	Kiểm tra, nghiệm thu sản phẩm:	Nhà thầu có đề xuất hoặc có cam kết về "Quy định về kiểm tra, nghiệm thu sản phẩm" đáp ứng yêu cầu của EHSMT (tham chiếu Mục **"5. Quy định về kiểm tra, nghiệm thu sản phẩm"** của tập tin Yêu cầu kỹ thuật đính kèm chương V của E-HSMT).	Nhà thầu không có đề xuất và cũng không có cam kết về "Quy định về kiểm tra, nghiệm thu sản phẩm"; hoặc có đề xuất (hoặc cam kết) nhưng không đáp ứng yêu cầu của E-HSMT (tham chiếu Mục **"5. Quy định về kiểm tra, nghiệm thu sản phẩm"** của tập tin Yêu cầu kỹ thuật đính kèm chương V của E-HSMT).
5	**UY TÍN CỦA NHÀ THẦU**		
5.1	Kết quả thực hiện hợp đồng của nhà thầu theo quy định tại Điều 19 và Điều 20 của Nghị định số 214/2025/NĐ-CP	Nhà thầu không có vi phạm.	Nhà thầu thuộc danh sách Tổ chức, cá nhân vi phạm (còn trong thời gian hiệu lực xử phạt và trong phạm vi áp dụng xử phạt) đã đăng tải trên hệ thống đấu thầu quốc gia.

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	
		ĐẠT	KHÔNG ĐẠT
	KẾT LUẬN		
	ĐẠT	**E-HSDT được đánh giá là đạt yêu cầu về kỹ thuật khi tất cả các tiêu chuẩn được đánh giá là đạt.**	
	KHÔNG ĐẠT		**E-HSDT không đạt một trong các tiêu chuẩn thì được đánh giá là không đạt và không được xem xét, đánh giá bước tiếp theo.**