YÊU CẦU	TÍNH ĐÁP ỨNG
1. Yêu cầu	
a) Công khai, minh bạch, không hạn chế truy cập và tiếp cận thông tin;	- Thông tin về tài sản đấu giá, giá khởi điểm, bước giá, thời gian – hình thức đấu giá, điều kiện tham gia và kết quả đấu giá được công bố đầy đủ, kịp thời và chính xác trên hệ thống. - Người tham gia đấu giá có thể truy cập hệ thống mọi lúc, mọi nơi thông qua môi trường Internet, không bị hạn chế bởi địa lý hay đối tượng, trừ các trường hợp hạn chế theo quy định của pháp luật. - Quy trình đấu giá, lịch sử trả giá và kết quả trúng đấu giá được ghi nhận, lưu trữ và hiển thị rõ ràng, cho phép kiểm tra, đối chiếu khi cần thiết. Checklist kỹ thuật: - Có Public pages cho danh mục/cuộc đấu giá/hồ sơ công khai. - Có API read-only công khai không yêu cầu login cho dữ liệu công khai. - Khả năng hỗ trợ: hỗ trợ mobile, tiêu chuẩn WCAG (Web Content Accessibility Guidelines) cơ bản (phông chữ, tương phản, bàn phím…)
b) Thời gian trên Cổng Đấu giá tài sản quốc gia, trang thông tin đấu giá trực tuyến là thời gian thực và thời gian chuẩn theo tiêu chuẩn quốc tế (GMT) trong đấu giá trực tuyến;	- Thời gian hiển thị trên trang là thời gian thực đảm bảo công bằng, minh bạch cho tất cả người tham gia đấu giá, tránh tranh chấp phát sinh do chênh lệch thời gian hiển thị hoặc sai lệch đồng hồ hệ thống. - Không dựa vào giờ máy người dùng để quyết định hợp lệ/không hợp lệ. Checklist kỹ thuật: - Có cơ chế đồng bộ thời gian (NTP) cho toàn bộ node (app, worker, DB, message broker…) - Tất cả timestamp trong DB ở UTC, có quy ước rõ ràng. - Màn hình phiên đấu giá hiển thị "Giờ hệ thống" (server time) và mốc đóng/mở rõ ràng. - Log có timestamp UTC; đối soát được giữa các thành phần (correlation id).
c) Hoạt động ổn định, liên tục và phải bảo đảm an toàn hệ thống thông tin;	- Áp dụng các biện pháp bảo mật kỹ thuật như xác thực người dùng, phân quyền truy cập, mã hóa dữ liệu, giám sát và phát hiện xâm nhập để ngăn chặn truy cập trái phép, phá hoại hệ thống. - Hạn chế tối đa tình trạng gián đoạn, lỗi kỹ thuật hoặc ngừng hoạt động, đặc biệt trong các thời điểm mở và kết thúc phiên đấu giá. Checklist kỹ thuật hoạt động ổn định, liên tục: - Triển khai tối thiểu 2 instance BE (active-active) sau load balancer. - DB có HA/replication; backup định kỳ; có kế hoạch khôi phục. - Cache/queue (nếu có) cũng cần HA. - Tách các tác vụ nặng (gửi mail/SMS/telegram, tạo biên bản, xuất báo cáo) sang worker. - Realtime channel: SignalR để đẩy sự kiện giá. Nếu realtime rớt: fallback polling theo chu kỳ ngắn. Mọi lệnh "trả giá" phải idempotent/có mã giao dịch. *(SignalR Core là một thư viện mã nguồn mở của Microsoft, cho phép thêm chức năng thời gian thực vào các ứng dụng web một cách dễ dàng. "Thời gian thực" ở đây có nghĩa là server có thể đẩy (push) nội dung xuống client ngay lập tức khi có dữ liệu mới, thay vì client phải liên tục gửi yêu cầu (polling) lên server để kiểm tra xem có gì mới hay không)* Checklist nghiệm thu liên quan ATTT: - Có SLA nội bộ (ví dụ uptime/tháng), có dashboard đo. - Có backup/restore test định kỳ. - Có giám sát, log tập trung, cảnh báo (email/telegram nội bộ). - Có kịch bản DR (disaster recovery) tối thiểu: RPO/RTO mục tiêu.

d) Bảo đảm an toàn, bảo mật thông tin của người tham gia đấu giá, tài khoản truy cập;	Áp dụng các biện pháp xác thực và quản lý tài khoản chặt chẽ, như mật khẩu mạnh, xác thực đa yếu tố (nếu có), phân quyền truy cập rõ ràng để ngăn chặn việc sử dụng trái phép tài khoản. Checklist nghiệm thu - Có tài liệu phân loại dữ liệu (data classification) và ma trận quyền. - Có log đăng nhập/đăng xuất/thao tác nhạy cảm. - Có cơ chế thu hồi phiên, logout mọi thiết bị, reset mật khẩu an toàn.
đ) Đáp ứng các yêu cầu về hạ tầng kỹ thuật, tiêu chuẩn công nghệ thông tin để kết nối, tích hợp và chia sẻ dữ liệu thông qua nền tảng tích hợp, chia sẻ dữ liệu;	Hệ thống có khả năng kết nối, tích hợp với các hệ thống thông tin, cơ sở dữ liệu khác thông qua nền tảng tích hợp, chia sẻ dữ liệu, phục vụ công tác quản lý, giám sát và khai thác thông tin. Checklist nghiệm thu: - Có tài liệu API (OpenAPI/Swagger). - Có cơ chế hàng đợi/sự kiện (nếu cần realtime liên thông). - Có kiểm soát truy cập theo đối tác, nhật ký gọi API.
e) Đáp ứng yêu cầu về hạ tầng kỹ thuật, cơ sở vật chất và đội ngũ nhân sự cần thiết cho việc vận hành Cổng Đấu giá tài sản quốc gia, trang thông tin đấu giá trực tuyến.	- Có hạ tầng kỹ thuật, trang thiết bị và hệ thống công nghệ thông tin phù hợp, đáp ứng yêu cầu vận hành liên tục, khả năng mở rộng và bảo đảm an toàn, an ninh thông tin. - Có đội ngũ nhân sự chuyên môn về công nghệ thông tin, quản trị hệ thống và nghiệp vụ đấu giá, đủ năng lực để vận hành, bảo trì, xử lý sự cố và nâng cấp hệ thống khi cần thiết. - DC đạt tiêu chuẩn Tier3 (Hệ thống có khả năng vận hành liên tục, dự phòng đầy đủ). Phân tách môi trường: dev/test/staging/prod. Có Hệ thống sao lưu, lưu trữ log, giám sát. Checklist nghiệm thu: - Có quy trình vận hành chuẩn: incident, change management, backup/restore. - Có kịch bản xử lý sự cố trong phiên đấu giá (mạng, quá tải, lỗi realtime…). - Có nhật ký vận hành & báo cáo định kỳ.
2. Điều kiện	
a) Đạt cấp độ 3 theo quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ;	Cam Kết đạt mức độ 3. Các vùng mạng được thiết kế như sau: - Phân vùng mạng Core o Là vùng gồm các thiết bị switch L3 Juniper Ex4300, Cisco Switch 2960 , Firewall Palo Alto PA 3260, Cisco ASA 5540 kết nối trực tiếp với nhau thực hiện truyền tải dữ liệu giữa các vùng mạng bên trong và ngoài VTT. Các thiết bị trên được đặt tại phòng máy chủ VTT. - Phân vùng mạng máy chủ VNPT Nghệ An - Là vùng mạng vận hành các thiết bị mạng, máy chủ cung cấp các ứng dụng, dịch vụ phục vụ công tác ĐHSXKD (CSS, CƯỚC, OMS, …). Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị tường lửa cho CSDL. - Phân vùng mạng máy chủ cung cấp dịch vụ cho Khách hàng (DMZ) o Là vùng mạng vận hành các thiết bị mạng, máy chủ cung cấp các dịch vụ ra ngoài internet phục vụ Khách hàng như Web Hosting, Email Hosting và các dịch vụ khác. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam - Phân vùng mạng đối tác o Là vùng mạng gồm các thiết bị Router kết nối tới các đơn vị ngoài VTT - Phân vùng mạng người dùng điều hành sản xuất kinh doanh o Là phân vùng mạng thuộc cấp 3, được chia nhỏ thành các vùng mạng nhỏ hơn dựa vào vị trí địa lý (Thành phố, Huyện) và chức năng của đơn vị; bao gồm các thiết bị mạng có dây, máy tính các nhân, máy in, … được cán bộ công nahan viên của tất cả các phòng chức năng và đơn vị trực thuộc sử dụng, tham gia vào mạng ĐHSXKD. - Phân vùng mạng quản lý thiết bị o Là vùng mạng phục vụ công tác quản trị hệ thống, các hệ thống quản lý – điều khiển thiết bị Việc bảo mật hệ thống do thiết bị Firewall cứng đảm nhiệm: Firewall Palo Alto PA 3260, Cisco ASA 5540. Tất cả truy cập tới máy chủ dịch vụ đều

b) Bảo đảm việc mỗi cá nhân, tổ chức được đăng ký duy nhất một tài khoản tham gia đấu giá, trả giá;	- Sử dụng tính duy nhất theo tài khoản, số điện thoai, email (Thêm hình ảnh trùng)
c) Bảo đảm việc tham gia trả giá, hiển thị giá đã trả bằng mã số riêng của người tham gia đấu giá;	Với Bảo vệ bí mật danh tính, Tránh áp lực, thông đồng, can thiệp ngoài hệ thống, nhưng vẫn phải truy vết được khi cần: Hệ thống tự động sinh mã trả giá cho mỗi lượt trả giá (Ko hiển thị tên hay thông tin của ng trả giá - chỉ hiển thị mã số riêng cho lượt đấu giá đó) (Hệ thống nội bộ: mã số vẫn ánh xạ được với tài khoản thật (phục vụ công tác xác định người thắng đấu giá))
d) Hiển thị công khai thời điểm đăng ký tham gia đấu giá, thời điểm truy cập tài khoản tham dự phiên đấu giá, thời điểm bắt đầu và kết thúc phiên đấu giá;	Hệ thống hiển thị công khai: - Thời điểm đăng ký tham gia đấu giá - Thời điểm truy cập tài khoản tham dự phiên đấu giá - Thời điểm bắt đầu và kết thúc phiên đấu giá - Thời gian hiển thị thống nhất dựa trên thời gian hệ thống, không phụ thuộc máy người dùng
đ) Hiển thị công khai, trung thực các lần trả giá, giá đã trả của người tham gia đấu giá theo mã số riêng, giá trả cao nhất; ghi lại và truy xuất được toàn bộ thông tin của cuộc đấu giá, phiên đấu giá;	Đáp ứng theo yêu cầu: - Hệ thống phải đã hiển thị: Toàn bộ các lần trả giá hợp lệ bao gồm: mã số người trả, mức giá, giá cao nhất tại từng thời điểm. - Các tài khoản đấu giá cũng như tài khoản Admin không thể sửa/xóa/làm sai lệch lịch sử. - Hệ thống có ghi log đầy đủ (kể cả các lượt trả giá không hợp lệ), truy xuất lại được toàn bộ diễn biến phiên đấu giá sau khi kết thúc.
e) Hiển thị liên tục giá khởi điểm của tài sản đấu giá, mức giá cao nhất đã trả đối với phương thức trả giá lên và mức giá bằng giá khởi điểm hoặc giá đã giảm thấp nhất đối với phương thức đặt giá xuống trong	Hệ thống hiển thị liên tục, realtime: - Giá khởi điểm - Mức giá cao nhất đã trả (Đấu giá lên) - Các lượt đấu giá hợp lệ gần nhất.
g) Bảo đảm người tham gia đấu giá không thể nộp hồ sơ tham gia đấu giá sau thời điểm kết thúc nộp hồ sơ và không thể thực hiện việc trả giá sau thời điểm kết thúc cuộc đấu giá.	Hệ thống tự động khóa: - Chức năng đăng ký, điểm danh khi hết hạn phiên đấu giá - Chức năng trả giá khi kết thúc phiên Khóa ở mức hệ thống, không chỉ giao diện mọi yêu cầu gửi sau thời điểm kết thúc đều bị từ chối - Hệ thống có log ghi nhận

TỈNH
JNG TÂM
ỊCH VỤ
GIÁ TÀI SẢN

An toàn thông tin cấp độ

Hệ thống thông tin cấp độ 3:

Căn cứ Điều 9 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

(1) Tiêu chí 1: Hệ thống thông tin xử lí thông tin bí mật nhà nước hoặc hệ thống phục vụ quốc phòng, an ninh khi bị phá hoại sẽ làm tổn hại tới quốc phòng, an ninh quốc gia.

(2) Tiêu chí 2: Hệ thống thông tin phục vụ người dân, doanh nghiệp thuộc một trong các loại hình như sau:

- Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 3 trở lên theo quy định của pháp luật;
- Cung cấp dịch vụ trực tuyến thuộc danh mục dịch vụ kinh doanh có điều kiện (theo quy định của Luật Đầu tư năm 2020);
- Cung cấp dịch vụ trực tuyến khác có xử lí thông tin riêng, thông tin cá nhân của từ 10.000 người sử dụng trở lên.

(3) Tiêu chí 3: Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi một ngành, một tỉnh hoặc một số tỉnh.

Ví dụ: Trung tâm dữ liệu cấp bộ, cấp tỉnh; Nền tảng tích hợp, chia sẻ dữ liệu cấp Bộ, cấp tỉnh; Mạng truyền số liệu chuyên dùng cấp II tại các địa phương…

(4) Tiêu chí 4: Hệ thống thông tin điều khiển công nghiệp trực tiếp phục vụ Điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp II, cấp III hoặc cấp IV theo phân cấp của pháp luật về xây dựng.

Hệ thống đấu giá trực tuyến là hệ thống phục vụ người dân, doanh nghiệp, cung cấp dịch vụ trực tuyến thuộc lĩnh vực kinh doanh có điều kiện, đồng thời xử lý thông tin cá nhân và thông tin nghiệp vụ của người tham gia đấu giá.

Nhóm tiêu chí	Tiêu chí chi tiết	Yêu cầu pháp lý (Cấp độ 3)	Cách hệ thống đáp ứng	Minh chứng / Tài liệu
A. Kiểm soát truy cập	Xác thực, phân quyền người dùng	Người dùng được xác thực, phân quyền rõ ràng	Đăng nhập tài khoản, phân quyền theo vai trò	Sơ đồ RBAC, log đăng nhập
B. Bảo mật dữ liệu	Bảo mật dữ liệu khi truyền và lưu trữ	Bảo vệ thông tin cá nhân, dữ liệu nghiệp vụ	HTTPS, băm mật khẩu, phân quyền DB	Cấu hình TLS, chính sách mật khẩu
C. Ghi log & giám sát	Ghi nhận hành vi người dùng	Có log truy vết, không chỉnh sửa	Log đăng nhập, trả giá, thao tác quản trị	Mẫu log hệ thống
D. Phòng chống tấn công	Ngăn chặn tấn công phổ biến	Có biện pháp ATTT mức ứng dụng/hạ tầng	Validate input, rate limit, firewall	Mô tả kỹ thuật bảo mật
E. Đảm bảo sẵn sàng	Sao lưu, khôi phục, liên tục dịch vụ	Hạn chế gián đoạn, có phương án khôi phục	Backup định kỳ, giám sát hệ thống	Kế hoạch backup/restore
F. Quản lý & vận hành	Quy trình, nhân sự ATTT	Có phân công, quy trình xử lý sự cố	Phân công quản trị, quy trình vận hành	Quyết định phân công, SOP