ỦY BAN NHÂN DÂN **THỊ XÃ HOÀI NHƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 59 /KH-UBND	*Hoài Nhơn, ngày 10 tháng 4 năm 2023*

KẾ HOẠCH
Về việc đầu tư bảo đảm an toàn hệ thống thông tin theo cấp độ tại UBND thị xã Hoài Nhơn năm 2023 và năm 2024

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Văn bản số 652/BTTTT-CATTT ngày 28/02/2023 của Bộ Thông tin và Truyền thông về việc hướng dẫn triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023;

Căn cứ Quyết định số 4585/QĐ-UBND ngày 30/12/2022 của UBND tỉnh về việc phê duyệt Kết quả đánh giá, xếp hạng mức độ ứng dụng công nghệ thông tin trong các cơ quan nhà nước trên địa bàn tỉnh Bình Định năm 2022;

Căn cứ Công văn số 315/STTTT-BCVT&CNTT ngày 24/3/2023 của Sở Thông tin và Truyền thông về việc triển khai công tác đảm bảo an toàn thông tin mạng tại các cơ quan, đơn vị;

Thực hiện Quyết định số 22602/QĐ-UBND ngày 22/12/2022 của UBND thị xã Hoài Nhơn về việc giao dự toán ngân sách địa phương năm 2023;

UBND thị xã Hoài Nhơn xây dựng Kế hoạch về việc đầu tư bảo đảm an toàn hệ thống thông tin theo cấp độ tại UBND thị xã Hoài Nhơn năm 2023 và năm 2024, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- 100% hệ thống thông tin thuộc phạm vi quản lý của UBND thị xã, các phòng ban trực thuộc UBND thị xã và UBND các xã, phường được triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

- Không để xảy ra lộ lọt thông tin, dữ liệu cá nhân nghiêm trọng trên các hệ thống thông tin thuộc phạm vi quản lý của UBND thị xã, các phòng ban trực thuộc UBND thị xã và UBND các xã, phường.

2. Yêu cầu

- Triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ cho 100% hệ thống thông tin đang vận hành, cụ thể:

+ Hệ thống mạng nội bộ (Lan) của cơ quan.

+ Hệ thống phần mềm cửa điện tử (VNPT Igate).

+ Hệ thống thông tin tại phòng họp trực tuyến thị xã.

- Bảo vệ thông tin, dữ liệu cá nhân: Định kỳ kiểm tra, rà soát ATTT mạng; Tuyên truyền cho CB, CCVC-NLĐ tham gia chiến dịch rà quét, làm sạch mã độc,… trên không gian mạng.

II. ĐỐI TƯỢNG VÀ THỜI GIAN THỰC HIỆN

1. Tại nhà làm việc của Văn phòng HĐND và UBND, nhà làm việc của các phòng chuyên môn trực thuộc UBND thị xã (Nội vụ, Kinh tế, Tài nguyên - Môi trường, Quản lý đô thị), nhà làm việc tại Bộ phận Tiếp nhận và Trả kết quả của thị xã: Triển khai thực hiện vào quý II năm 2023. (*Có mô hình kèm theo*)

2. Tại nhà làm việc các phòng ban trực thuộc còn lại của UBND thị xã và UBND các xã, phường: Sẽ triển khai thực hiện vào năm 2024.

III. NHIỆM VỤ, GIẢI PHÁP

1. Yêu cầu cơ bản quản lý, bao gồm:

1.1. Thiết lập chính sách an toàn thông tin: Phòng Văn hóa và Thông tin xây dựng kế hoạch và trình UBND thị xã phê duyệt trước khi triển khai thực hiện. Định kỳ 03 năm hoặc khi có thay đổi chính sách ATTT kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

1.2. Tổ chức bảo đảm ATTT: Phòng Văn hóa và Thông tin là đơn vị đầu mối chuyên trách về ATTT. Ngoài ra, cử cán bộ đầu mối phối hợp với Sở Thông tin và Truyền thông, Đội Ứng cứu sự cố ATTT của tỉnh trong công tác hỗ trợ điều phối xử lý sự cố ATTT; Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

1.3. Bảo đảm nguồn nhân lực: Tham mưu UBND thị xã bố trí nguồn nhân lực có chuyên môn phù hợp, phụ trách vận hành hệ thống an toàn, hiệu quả.

1.4. Quản lý thiết kế, xây dựng hệ thống và vận hành hệ thống:

Tham mưu UBND thị xã quy trình quản lý an toàn mạng; chính sách, quy trình quản lý an toàn máy chủ và ứng dụng; chính sách, quy trình quản lý an toàn dữ liệu; chính sách, quy trình quản lý sự cố an toàn thông tin; chính sách, quy trình quản lý an toàn người sử dụng đầu cuối.

1.5. Xây dựng phương án Quản lý rủi ro an toàn thông tin.

1.6. Xây dựng phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

2. Yêu cầu cơ bản về kỹ thuật, bao gồm:

2.1. Bảo đảm an toàn mạng:

- Thiết kế hệ thống: Thiết kế các vùng mạng trong hệ thống theo chức năng. Phương án thiết kế bảo đảm: Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn; Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập; Có phương án dự phòng cho các thiết bị mạng chính.

- Kiểm soát truy cập từ bên ngoài, bên trong mạng.

- Nhật ký hệ thống: Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu có); Sử dụng thời gian trên máy chủ để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát.

- Phòng chống xâm nhập: Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ và vùng máy chủ nội bộ; Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures).

- Bảo vệ thiết bị hệ thống: Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa; Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa.

2.2. Bảo đảm an toàn máy chủ:

- Xác thực: Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ; Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng); Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng.

- Kiểm soát truy cập: Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa; Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng.

- Nhật ký hệ thống: Ghi nhật ký hệ thống; Đồng bộ thời gian giữa máy chủ với máy chủ thời gian; Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng.

- Phòng chống xâm nhập: Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ; Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ; Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng; Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.

- Phòng chống phần mềm độc hại: Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt.

- Xử lý máy chủ khi chuyển giao: Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2.3. Bảo đảm an toàn ứng dụng:

- Xác thực: Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng; Lưu trữ có mã hóa thông tin xác thực hệ thống; Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng; Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.

- Kiểm soát truy cập: Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa; Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng; Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa.

- Nhật ký hệ thống: Ghi nhật ký hệ thống; Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng.

2.4. Bảo đảm an toàn dữ liệu:

- Bảo mật dữ liệu: Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

- Sao lưu dự phòng: Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Bảo vệ thông tin, dữ liệu cá nhân

- Định kỳ phối hợp kiểm tra, rà soát ATTT mạng.

- Tham mưu UBND thị xã bố trí kinh phí đầu tư mua sắm trang bị các thiết bị tường lửa (*có chức năng lưu trữ log*) và phần mềm diệt virut có bản quyền để bảo vệ an toàn hệ thống mạng của UBND thị xã, các phòng ban trực thuộc UBND thị xã, UBND các xã, phường và thông tin dữ liệu cá nhân của người sử dụng. Trong đó, quan tâm mua sắm phần mềm diệt virut bản quyền cho các máy tính thường xuyên sử dụng để ký số, ban hành văn bản điện tử, máy tính tham gia hệ thống đấu thầu qua mạng và kết nối các cơ sở dữ liệu quốc gia,…

- Tuyên truyền cho cán bộ, CCVC-NLĐ tham gia chiến dịch rà quét, làm sạch mã độc,… trên không gian mạng.

IV. KINH PHÍ THỰC HIỆN

Từ nguồn ngân sách hỗ trợ của tỉnh, ngân sách của thị xã, ngân sách của UBND các xã, phường và các nguồn vốn hợp pháp khác, cụ thể:

- Kinh phí đầu tư tại nhà làm việc Văn phòng HĐND và UBND thị xã, nhà làm việc của các phòng chuyên môn trực thuộc UBND thị xã (Nội vụ, Tài nguyên – Môi trường, Quản lý đô thị, Kinh tế) và nhà làm việc tại Bộ phận Tiếp nhận và Trả kết quả thị xã; Số tiền: 839.453.226 đồng. (Bằng chữ: Tám trăm ba mươi chín triệu, bốn trăm năm mươi ba nghìn, hai trăm hai mươi sáu đồng). Trong đó, kinh phí đầu tư: 836.942.400 đồng, kinh phí tư vấn thiết kế: 2.510.826 đồng. (*Có Bảng dự trù kinh phí kèm theo*)

- Năm 2024, tiếp tục tham mưu UBND thị xã bố trí kinh phí đầu tư hệ thống tường lửa đảm bảo An toàn thông tin (phần còn lại).

V. TỔ CHỨC THỰC HIỆN

1. Phòng Văn hóa và Thông tin

- Giao Phòng Văn hóa và Thông tin chủ trì, phối hợp với các cơ quan, UBND các xã, phường triển khai thực hiện theo Kế hoạch.

- Phối hợp lập đề cương và dự toán chi tiết đầu tư hệ thống tường lửa bảo đảm ATTT theo cấp độ trình Sở Thông tin và Truyền thông thẩm định và UBND thị xã phê duyệt kinh phí.

- Tổ chức tuyên truyền, hướng dẫn các cơ quan nhà nước thực hiện đảm bảo hệ thống thông tin theo cấp độ; tổ chức kiểm tra, đánh giá ATTT tại các cơ quan nhà nước, xã, phường.

2. Phòng Tài chính - Kế hoạch

- Tham mưu, đề xuất UBND thị xã kinh phí mua sắm thiết bị - đảm bảo ATTT (đã bố trí kinh phí đầu năm 2023 tại Quyết định số 22602/QĐ-UBND của UBND thị xã) và hướng dẫn cho các cơ quan, UBND các xã, phường thực hiện đảm bảo theo quy định pháp luật.

3. Văn phòng HĐND và UBND thị xã

- Phối hợp, tổ chức lắp đặt, vận hành hiệu quả Hệ thống Tường lửa đảm bảo an toàn thông tin hệ thống mạng tại UBND thị xã Hoài Nhơn.

- Thường xuyên kiểm tra, phối hợp với Phòng Văn hóa và Thông tin đề nghị thay thế các thiết bị hư hỏng trong quá trình vận hành hệ thống.

4. Các phòng, ban trực thuộc UBND thị xã có liên quan

- Bố trí nhân lực, tổ chức vận hành hiệu quả Hệ thống tường lửa của cơ quan sau khi được bàn giao.

- Thường xuyên kiểm tra, báo cáo các sự cố của hệ thống về UBND thị xã (qua phòng Văn hóa và Thông tin) để phối hợp xử lý.

5. UBND các xã, phường

Chủ động xây dựng kế hoạch tổ chức bố trí nguồn nhân lực, nguồn kinh phí triển khai thực hiện theo Kế hoạch này vào năm 2024.

Yêu cầu Thủ trưởng các cơ quan, UBND các xã, phường căn cứ nội dung Kế hoạch nghiêm túc triển khai thực hiện./.

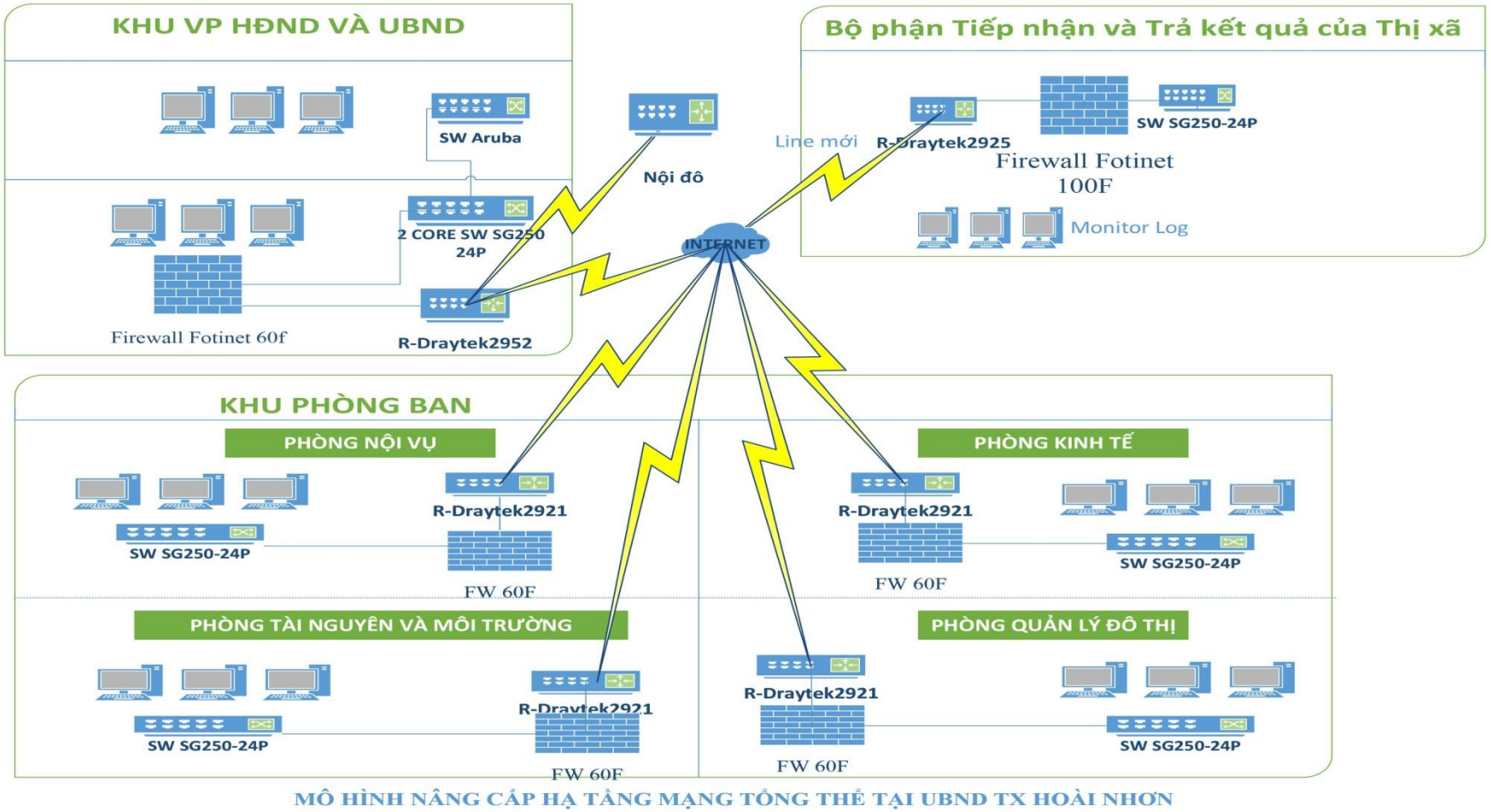
Nơi nhận:
- Sở TT&TT; (Báo cáo)
- TT Thị ủy; (Báo cáo)
- TT HĐND thị xã; (Báo cáo)
- CT và các PCT UBND thị xã; (Báo cáo)
- Các phòng ban trực thuộc UBND thị xã; (Phối hợp)
- UBND các xã, phường; (Phối hợp)
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trần Hữu Thảo

MÔ HÌNH NÂNG CẤP HẠ TẦNG MẠNG TỔNG THỂ TẠI UBND THỊ XÃ

(Kèm theo Kế hoạch số /KH-UBND ngày / /2023 của UBND thị xã Hoài Nhơn)



MÔ HÌNH NÂNG CẤP HẠ TẦNG MẠNG TỔNG THỂ TẠI UBND TX HOÀI NHƠN

BẢNG DỰ TRÙ KINH PHÍ THỰC HIỆN TẠI UBND THỊ XÃ NĂM 2023

(Kèm theo Kế hoạch số /KH-UBND ngày / /2023 của UBND thị xã Hoài Nhơn)

STT	Tên thiết bị	Đơn vị tính	Số lượng	Đơn giá	Tổng tiền	Ghi chú
1	**Thiết bị chuyển mạch Switch Cisco** CBS250-24T-4G-EU- 1Gb Switch Cisco Switch Cisco Business 250 24 port 10/100/1000, 4 port 1G SFP uplink	Cái	7	19,440,000	136,080,000	
2	**Thiết bị tường lửa Firewall Fortinet** Firewall Fortinet FG-100F-BDL-950-36 - 22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media). - 4 SFP ports, 2x 10G SFP+ FortiLinks, dual power supplies redundancy. - Max managed FortiAPs (Total / Tunnel) 128 / 64. - VPN support. - Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM): 3 Year	Cái	1	198,640,000	198,640,000	
3	**Thiết bị tường lửa Firewall Fortinet** FG-60F-BDL-950-12 FortiGate-60F	Cái	5	59,452,000	297,260,000	
4	**Convert 1Gb**	Cái	1	3,654,000	3,654,000	

5	**Router DrayTek 2952**	Cái	1	13,138,000	13,138,000	
6	**Dây nhảy Cat6 UTP AMP**	Sợi	8	165,300	1,322,400	
7	**Cáp Commscope CAT6**	Thùng	1	4,038,000	4,038,000	
8	**Vật tư phụ (keo, nhãn,…)**		1	870,000	870,000	
9	**Nẹp nhựa nhỏ**	mét	200	26,100	5,220,000	
10	**Phần mền phân tích log tập trung Eventlog analyzer premium**	năm	1	118,000,000	118,000,000	
11	**HP Z2 G9 Workstation, core i5, 256 SSD, 32Gb ram, 2Tb HDD**	Cái	1	58,720,000	58,720,000	
	Tổng tiền				**836,942,400**	

BẢNG KINH PHÍ TƯ VẤN THIẾT KẾ

(Kèm theo Kế hoạch số /KH-UBND ngày / /2023 của UBND thị xã Hoài Nhơn)

STT	Tên chi phí tư vấn	Tổng giá trị tư vấn (Gtv)	Tổng tiền
1	Chi phí Lập Hồ sơ mời thầu/Hồ sơ đề xuất	0,1% x Tổng dự toán thiết bị (Gtb)	836,942
2	Chi phí thẩm định Hồ sơ đề xuất	0,05 x Tổng dự toán thiết bị (Gtb)	418,471
3	Chi phí đánh giá Hồ sơ dự thầu	0,1% x Tổng dự toán thiết bị (Gtb)	836,942
4	Chi phí thẩm định Kết quả lựa chọn nhà thầu	0,05 x Tổng dự toán thiết bị (Gtb)	418,471
Tổng cộng			**2,510,826**