UỶ BAN NHÂN DÂN **TỈNH SƠN LA**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1856/QĐ- UBND	*Sơn La, ngày 24 tháng 6 năm 2019*

QUYẾT ĐỊNH
Về phê duyệt kế hoạch lựa chọn nhà thầu gói thầu: Xây dựng hệ thống phần mềm phòng, chống mã độc theo mô hình quản trị tập trung
Đơn vị: Sở Thông tin và Truyền thông

CHỦ TỊCH UỶ BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật Đấu thầu số 43/2013/QH13 ngày 26/11/2013;

Căn cứ Nghị định số 63/2014/NĐ-CP ngày 26/6/2014 của Chính phủ về quy định chi tiết thi hành một số điều của Luật Đấu thầu về lựa chọn nhà thầu;

Căn cứ Thông tư số 10/2015/TT-BKHĐT ngày 26/10/2015 của Bộ Kế hoạch và Đầu tư về quy định chi tiết về kế hoạch lựa chọn nhà thầu;

Căn cứ Thông tư số 58/2016/TT-BTC ngày 29/3/2016 của Bộ Tài chính quy định chi tiết sử dụng vốn nhà nước để mua sắm nhằm duy trì hoạt động thường xuyên của cơ quan nhà nước, đơn vị thuộc lực lượng vũ trang nhân dân, đơn vị sự nghiệp công lập, tổ chức chính trị, tổ chức chính trị xã hội, tổ chức chính trị xã hội - nghề nghiệp, tổ chức xã hội, tổ chức xã hội - nghề nghiệp;

Căn cứ Quyết định số 3288/QĐ-UBND ngày 08/12/2018 của UBND tỉnh về việc ban hành quy định về quản lý, điều hành ngân sách địa phương năm 2019; Quyết định số 549/QĐ-UBND ngày 06/3/2019 của Chủ tịch UBND tỉnh về việc bổ sung kinh phí năm 2019, đơn vị: Sở Thông tin và Truyền thông;

Xét đề nghị của Sở Tài chính tại Tờ trình số 394/TTr-STC ngày 12/6/2019; Báo cáo thẩm định số 307/BCTĐ-STC ngày 11/6/2019 của Sở Tài chính về phê duyệt kế hoạch lựa chọn nhà thầu, gói thầu: Xây dựng hệ thống phần mềm phòng, chống mã độc theo mô hình quản trị tập trung; đơn vị: Sở Thông tin và Truyền thông,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt danh mục và kế hoạch lựa chọn nhà thầu gói thầu: Xây dựng hệ thống phần mềm phòng, chống mã độc theo mô hình quản trị tập trung của Sở Thông tin và Truyền thông như sau:

1. Danh mục mua sắm: Theo Phụ lục I kèm theo.

- Tổng dự toán: **1.730.000.000 đồng** *(Bằng chữ: Một tỷ, bảy trăm ba mươi triệu đồng chẵn).*

- Nguồn kinh phí: Quyết định số 549/QĐ-UBND ngày 06/3/2019 của Chủ tịch UBND tỉnh Sơn La.

2. Phê duyệt kế hoạch lựa chọn nhà thầu gói thầu nêu trên với các nội dung chi tiết theo Phụ lục II kèm theo.

Điều 2. Sở Thông tin và Truyền thông có trách nhiệm tổ chức triển khai thực hiện đảm bảo đúng quy định của Luật Ngân sách Nhà nước, Luật Đấu thầu, Nghị định số 63/2014/NĐ-CP ngày 26/6/2014 của Chính phủ, Thông tư số 58/2016/TT-BTC ngày 29/3/2016 của Bộ Tài chính và các chế độ tài chính hiện hành của Nhà nước.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc các Sở: Tài chính, Kế hoạch và Đầu tư; Thông tin và truyền thông; Giám đốc Kho bạc Nhà nước tỉnh và Thủ trưởng các cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Thường trực tỉnh ủy *(B/c)*;
- Thường trực HĐND tỉnh *(B/c)*;
- Chủ tịch UBND tỉnh;
- Các PCT UBND tỉnh;
- Như Điều 3;
- Lưu: VT, KGVX, 15 bản.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Phạm Văn Thủy

Phụ lục 01

KẾ HOẠCH LỰA CHỌN NHÀ THẦU GÓI THẦU: XÂY DỰNG HỆ THỐNG PHẦN MỀM PHÒNG, CHỐNG MÃ ĐỘC THEO MÔ HÌNH QUẢN TRỊ TẬP TRUNG

ĐƠN VỊ: SỞ THÔNG TIN VÀ TRUYỀN THÔNG

(Kèm theo Quyết định số: 1157/QĐ-UBND ngày 11/6/2019 của Chủ tịch UBND tỉnh)

Số TT	Tên gói thầu	Giá gói thầu (1.000 đồng)	Nguồn vốn	Hình thức lựa chọn nhà thầu	Phương thức lựa chọn nhà thầu	Thời gian bắt đầu lựa chọn nhà thầu	Loại hợp đồng	Thời gian thực hiện hợp đồng
	Gói thầu dịch vụ tư vấn		Quyết định số 549/QĐ-UBND ngày 06/3/2019 của UBND tỉnh					
1	Tư vấn lập hồ sơ yêu cầu, đánh giá hồ sơ đề xuất	3.740		Chỉ định thầu rút gọn		Tháng 6 năm 2019	Trọn gói	20 ngày
2	Tư vấn thẩm định hồ sơ yêu cầu, thẩm định kết quả lựa chọn nhà thầu	2.200		Chỉ định thầu rút gọn		Tháng 6 năm 2019	Trọn gói	20 ngày
3	Tư vấn giám sát thi công	13.431		Chỉ định thầu rút gọn		Quý III năm 2019	Trọn gói	Trong thời gian lắp đặt thiết bị
	Mua sắm phần mềm							
4	Hệ thống phần mềm phòng, chống mã độc theo mô hình quản trị tập trung	1.701.200		Chào hàng cạnh tranh thông thường	Một giai đoạn, một túi hồ sơ	Quý III năm 2019	Trọn gói	60 ngày
Tổng cộng: 1.720.571.000 đồng *(Đã bao gồm thuế GTGT,...)*								

Ghi chú: *Yêu cầu chức năng phần mềm phòng, chống mã độc theo mô hình quản trị tập trung, đơn vị: Sở Thông tin và Truyền thông có phụ lục chi tiết kèm theo.*

Phụ lục 02

XÂY DỰNG HỆ THỐNG PHẦN MỀM PHÒNG, CHỐNG MÃ ĐỘC THEO MÔ HÌNH QUẢN TRỊ TẬP TRUNG

ĐƠN VỊ: SỞ THÔNG TIN VÀ TRUYỀN THÔNG

(Kèm theo Quyết định số: 1456/QĐ-UBND ngày 24/6/2019 của Chủ tịch UBND tỉnh)

STT	Danh mục mua sắm	Đơn vị tính	Số lượng
1	**Phần mềm hệ thống phòng, chống mã độc tập trung tại Trung tâm tích hợp dữ liệu** **Administration Console:**Giao diện quản lý tập trung, cùng chính sách quản lý giám sát tương tác với máy trạm. Hệ thống cảm biến mạnh mẽ cho phép xác định máy trạm nào chưa được cập nhật phiên bản mới nhất hay cơ sở dữ liệu mới nhất. **Administration Server:** Phần lõi của gói quản trị được phát triển dựa trên công nghệ tiên tiến, chạy dưới dạng ser- vice ở tầng sâu nhất của hệ thống, tương thích với hệ điều hành từ Windows 2003 trở lên. **Update Server:** Phụ trách việc quản lý và phân phối các gói cập nhật đến các máy trạm, tăng khả năng lưu thông trong việc cập nhật cơ sở dữ liệu với khả năng cập nhật linh hoạt từ bất cứ đâu. **Quản lý tất cả các tiện ích của hệ thống anti-virus từ xa:**Quét virus/ Đặt lịch quét/ Đặt lịch cập nhật từ máy chủ đến từng máy trạm trong hệ thống. Mọi tính năng trên bản End- Point Security đều thao tác được từ bản cài trên Server hoặc máy của Quản Trị Mạng. **Quản lý tài nguyên tiến trình máy tính:** Cải tiến quá trình thay đổi cấu hình của bất kỳ máy trạm nào trong mạng của doanh nghiệp, tập đoàn. Khi muốn thay đổi, cấu hình sẽ được lưu trên server và sẽ được apply ngay sau khi máy trạm sẵn sàng làm việc. **Quản lý thông tin bản quyền trên toàn bộ hệ thống:**Đăng ký, gia hạn, thêm mới bản quyền cho máy trạm **Quản lý hệ thống từ xa:** Chỉ cần có internet là bạn có thể quản lý từ xa dù ở bất cứ nơi đâu Giám sát các luồng dữ liệu theo thời gian thực: liên tục kiểm tra tất cả các dữ liệu ra vào máy tính (Email, Internet, USB....), đẩy lùi những kẻ xâm nhập và chặn đứng những truy vấn trairsi phép, nhằm phát hiện sự bùng nổ mã độc (cùng một lúc nhiễm vào nhiều máy trong mạng) ngay lập tức,từ đó có thể đưa ra chính sách chính sách tùy chỉnh chống lại sự bùng phát đó Cách ly các đối tượng bị nhiễm hay nghi ngờ bị nhiễm: đảm bảo các file nguy hiểm sẽ được mã hóa và cách ly vào khu vực an	Hệ thống	01

STT	Danh mục mua sắm	Đơn vị tính	Số lượng
	toàn, tránh tình trạng lây nhiễm toàn hệ thống. **Hệ thống cập nhật tự động thông minh:** Toàn bộ máy trạm trong hệ thống được cập nhật tập trung trên một server, giúp giảm băng thông đường truyền với cơ chế cập nhật dữ liệu nhanh chóng 1 phút/lần **Tạo nhóm và quản lý máy trạm theo nhóm:** Đơn giản hóa mọi việc nhưng vẫn đảm bảo việc quản lý được hệ thống sâu hơn. Điều khiển từ xa tới máy trạm: khi có sự xảy ra người quản trị có thể điều khiển nhiều máy cùng một lúc mà không phải đi trực tiếp đến từng máy Client. **Xây dựng chính sách cho các máy trạm:** Giám sát thời gian truy cập Internet, nội dung truy cập...giảm băng thông cho đường truyền, hạn chế được thời gian rảnh rỗi của nhân viên Thiết lập lịch quét/Cập nhật virus cho nhóm hoặc cho các máy trạm trên hệ thống: đảm bảo quá trình tự động hóa việc quét, diệt, cập nhật virus cho các nhóm và client theo lịch đã được định sẵn. Đa dạng hình thức cảnh báo: cảnh báo tại máy chủ, cảnh báo bằng email, cảnh báo bằng tin nhắn điện thoai. đảm bảo doanh nghiệp kịp thời ứng cứu hệ thống khi có cảnh báo. **Thông kê, báo cáo rõ ràng đầy đủ:** Hệ thống tự động thống kê các báo cáo hàng tuần về tình hình các máy trạm nhiễm virus trên toàn hệ thống. Từ đó người người quản trị sẽ xác định được cấp độ an toàn của hệ thống dựa trên số lượng máy nhiễm virus, thời gian bị nhiễm, thời gian cập nhật .v.v. Giúp hệ thống luôn được giám sát 24/24. Gửi dữ liệu báo cáo tổng hợp về Trung tâm Giám sát không gian mạng Quốc gia thuộc Bộ Thông tin và Truyền Thông **Bản quyền phần mềm:** 02 năm		
2	**Phần mềm phòng, chống mã độc cho máy trạm** **Hệ thống nhận dạng - Odin Engine :** Trang bị hàng trăm cảm biến nhận dạng cực kì thông minh, tăng tốc độ phân tích và phản ứng với mã độc. **Hệ thống cảnh báo - Realtime (Valkyrie):** Hệ thống bảo vệ thời gian thực có sức mạng kiểm soát, giám sát các hành vi trên máy tính vô cùng tối ưu. **Hệ thống bảo vệ - Sona Engine:** Công nghệ bảo vệ các tiến trình, dễ dàng cách ly và loại bỏ lập tức các loại mã độc **Hệ thống phòng chống xâm nhập - IPS:** Giám sát và quản lý lưu lượng gói, từ đó đưa ra quyết định có chủ ý, sau đó xác định đó có phải là một hành động hợp pháp hay không.	Bộ	2002

STT	Danh mục mua sắm	Đơn vị tính	Số lượng
	Hệ thống update: Update theo cơ chế incremental, tự động thảo luận với server để giảm băng thông truyền tải **Chế độ bảo vệ máy trạm một cách toàn diện:** Bảo vệ tập tin: tự động quét các tập tin khi bạn truy cập.Những file riêng lẻ, những danh sách và ổ đĩa sẽ được chỉ định trong việc quét virus. Người dùng có thể giới hạn việc quét những vùng quan trọng của hệ điều hành và những ứng dụng chạy lúc khởi động để bảo vệ việc phòng chống virus được tập trung vào những yếu điểm nhất của hệ thống. Bảo vệ Email: Quét mail dựa trên giao thức POP3, IMAP, SMTP trong bất kỳ chương trình nào, cung cấp các plug-in cho Micro- soft Outlook và Microsoft Outlook Express Bảo vệ Internet : Tất cả các dữ liệu vào ra sẽ được quét để kiểm tra virus trong thời gian thực, đảm bảo những dữ liệu bị nhiễm sẽ không được lưu vào máy. Chương trình ngăn chặn những đoạn mã nguy hiểm không cho người dùng thực thi trên web, chặn đứng cửa sổ pop-up và quảng cáo. Bảo vệ thông minh: Giám sát những hoạt động của tất cả các tiến trình đang được thực thi trong RAM và thông báo cho người dùng những tiến trình nguy hiểm đáng nghi, ngăn ngừa những thay đổi có hại đến hệ thống và phục hồi hệ thống. Bảo vệ các thông tin cá nhân (mật khẩu, số tài khoản): Chương trình sẽ phát hiện thông điệp lừa đảo và vô hiệu hóa đường dẫn. **Chế độ quét virus:** Tốc độ quét nhanh, quét sâu vào hệ thống, xử lý chính xác nhằm ngăn chặn và tiêu diệt virus. Quét được nhiều tác vụ cùng 1 lúc, có nhiều chế độ thiết lập quét cho bạn tùy chọn: Quét theo từng vùng,Quét theo lịch,Quét theo kiểu file...Phát hiện và diệt các packer, hay các trình bảo vệ khác để chống lại sự phát hiện của chương trình đối với các dòng virus sử dụng công nghệ root- kit chiếm quyền điều khiển máy tính. **Phát hiện mã độc mạnh mẽ, dễ dàng cách ly và loại bỏ:**Công nghệ phân tích và phản ứng mã độc thông minh. Khi hệ thống bị nhiễm virus hay đoạn mã lạ, chương trình sẽ tự đưa ra những khả năng trong hệ thống có thể bị tấn công, từ đó đưa ra cảnh báo hay chính sách chặn các lỗ hổng để mã độc không thể xâm nhập gây hại cho máy tính và hệ thống. **Quản lý truy cập trang web:** Hỗ trợ người dùng chủ động CHO PHÉP hay CẤM vào các trang web. **Khôi phục các tập tin bị nhiễm mã độc:** Các dữ liệu khi bị		

STT	Danh mục mua sắm	Đơn vị tính	Số lượng
	nhận nhầm là mã độc hoặc nhiễm nặng không thể khôi phục được thì sẽ được cách ly đưa vào vùng tin tưởng, đề phòng trường hợp người dùng muốn sử dụng lại, đảm bảo không bị mất dữ liệu trong hệ thống **Phòng chống xâm nhập trái phép:** Cho phép "nắm" lấy bất cứ lưu lượng nào của các gói tin mạng và đưa ra quyết định có chủ ý – xác định đây có phải là một cuộc tấn công hay một sự sử dụng hợp pháp – sau đó thực hiện hành động thích hợp để hoàn thành tác vụ một cách trọn vẹn. Kết quả cuối cùng là một nhu cầu có hạn định cho các giải pháp phát hiện hay giám sát thâm nhập một khi tất cả những gì liên quan đến mối đe doạ đều bị ngăn chặn. **Chức năng remote từ xa:** Hỗ trợ trong việc xử lý các sự cố về virus, đem lại hiệu quả tối đa và tốt nhất cho người sử dụng nhận được **Chế độ cập nhật tự động, thông minh:** Khi có bất kì sự cố về an ninh (phát hiện một virus mới có mức độ nguy hiểm cao) hệ thống Update Center tự động gửi gói cập nhật ngay về máy tính người dùng mà không cần đợi người dùng update sản phẩm. Hệ thống update này có kiến trúc thiết kế rất tốt và chính là một công nghệ update mà thường thấy ở các hãng lớn như Oracle, Microsoft. **Quản lý truy cập cá nhân:** Chức năng này giúp người quản trị dễ dàng quản lý việc truy cập website của máy trạm, từ đó sẽ hạn chế việc truy cập vào các trang web không phục vụ công việc như game, phim... trong giờ làm việc và các web có chứa mã độc, gây ảnh hưởng đến đường truyền mạng của hệ thống, cũng như tiến độ công việc. Tích hợp các công cụ lựa chọn (cho phép hoặc không cho phép): Chỉnh sửa Registry; Chỉnh sửa Folder Option; Sử dụng Task Manager; Bật, tắt chế độ cập nhật Windows; Hiện thư mục ẩn; Gọi hộp thoại Run; Mở Control Panel. **Phát hiện các loại rootkit cao cấp:** Cho phép dò tìm file, tiến trình, driver ẩn, tìm kiếm những đoạn mã bị hook hoạt động ở chế độ người dùng (user mode) hay ở chế độ cấp hệ thống (kernel mode). **Bản quyền phần mềm:** 02 năm		