ỦY BAN NHÂN DÂN TỈNH THỪA THIÊN HUẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2409/QĐ-UBND	*Thừa Thiên Huế, ngày 13 tháng 11 năm 2014*

QUYẾT ĐỊNH

Phê duyệt Đề án xây dựng và áp dụng hệ thống quản lý an toàn thông tin theo tiêu chuẩn TCVN ISO/IEC 27001:2009 tại Trung tâm Thông tin dữ liệu - Sở Thông tin và Truyền thông và Trung tâm Tin học hành chính - Văn phòng UBND tỉnh

ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức Hội đồng nhân dân và Uỷ ban nhân dân ngày 26 tháng 11 năm 2003;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/06/2006;

Căn cứ Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về việc Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 102/2009/NĐ-CP ngày 06/11/2009 của Chính phủ về Quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;

Căn cứ Quyết định số 246/2005/QĐ-TTg ngày 06/10/2005 của Thủ tướng Chính phủ phê duyệt Chiến lược phát triển công nghệ thông tin và truyền thông Việt Nam đến năm 2010 và định hướng đến năm 2020;

Căn cứ Quyết định số 1419/QĐ-UBND ngày 10/6/2007 của UBND tỉnh Thừa Thiên Huế về việc phê duyệt Quy hoạch phát triển công nghệ thông tin tỉnh Thừa Thiên Huế đến năm năm 2020;

Căn cứ Kế hoạch 53/KH-UBND ngày 13/7/2011 của UBND tỉnh Thừa Thiên Huế về Xây dựng Thừa Thiên Huế thành tỉnh mạnh về Công nghệ thông tin - Truyền thông;

Căn cứ Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Chỉ thị số 17/CT-UBND ngày 06/5/2014 của UBND Tỉnh Thừa Thiên Huế về tăng cường công tác đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Thừa Thiên Huế;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền Thông tại Tờ trình số 752/TTr-STTTT ngày 22 tháng 10 năm 2014,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Đề án "Xây dựng và áp dụng hệ thống quản lý an toàn thông tin theo tiêu chuẩn TCVN ISO/IEC 27001:2009 tại Trung tâm Thông tin dữ liệu điện tử - Sở Thông tin và Truyền thông và Trung tâm Tin học hành chính - Văn phòng UBND tỉnh" (gọi tắt là Đề án) với những nội dung chủ yếu sau:

I. MỤC TIÊU

Triển khai và áp dụng thành công hệ thống an toàn thông tin theo tiêu chuẩn ISO/IEC 27001:2005 tại Trung tâm Thông tin dữ liệu điện tử - Sở Thông tin và Truyền thông và Trung tâm Tin học hành chính – Văn phòng UBND tỉnh đạt chứng chỉ của tổ chức chứng nhận được công nhận bởi UKAS thông qua việc vận hành thành công hệ thống quản lý an toàn thông tin phù hợp với tiêu chuẩn ISO/IEC 27001:2013, các mục tiêu sẽ đạt được bao gồm:

- Đảm bảo tính bảo mật, tính toàn vẹn, tính sẵn sàng của các tài sản thông tin số.

- Nâng cao nhận thức của toàn thể thành viên trong hai Trung tâm về an toàn thông tin, từ đó, có những chính sách điều hành phù hợp nhằm đảm bảo an ninh thông tin trong hệ thống.

- Đảm bảo hệ thống được theo dõi, vận hành đáng tin cậy, các sự cố nếu xuất hiện sẽ được phát hiện sớm và khắc phục kịp thời.

- Giảm thiểu tác động của các rủi ro, chi phí bảo trì và vận hành hệ thống.

- Tạo niềm tin cho các cơ quan nhà nước và khách hàng.

- Tạo được khung cho các hoạt động tổ chức một cách có hệ thống về an toàn thông tin số.

- Cấp độ tổ chức: sự cam kết.

- Cấp độ pháp luật: sự tuân thủ.

- Cấp độ điều hành: quản lý rủi ro.

- Cấp độ thương mại: sự tớn nhiệm và tin cậy.

- Cấp độ tài chính: tiết kiệm chi phí.

- Cấp độ con người: cải tiến nhận thức cán bộ, viên chức.

- Nhận biết được tất cả mối nguy về an toàn thông tin.

- Là cơ sở cho các hoạt động cải tiến hệ thống an toàn thông tin.

- Các bên quan tâm tin tưởng hơn trong việc quan hệ và cung cấp các dịch vụ của đơn vị khi có chứng nhận.

II. NỘI DUNG VÀ GIẢI PHÁP THỰC HIỆN

1. Nội dung:

- Khảo sát phân tích hiện trạng và lập kế hoạch thực hiện.

- Thiết kế hệ thống.

- Triển khai và áp dụng đánh giá nội bộ.

- Đánh giá chứng nhận.

2. Giải pháp thực hiện:

- Lựa chọn đơn vị tư vấn đủ năng lực để tư vấn cho Trung tâm Thông tin dữ liệu điện tử và Trung tâm Tin học hành chính xây dựng và áp dụng hệ thống quản lý an ninh thông tin theo tiêu chuẩn ISO 27001: :2009.

- Lựa chọn nhân sự tham gia xây dựng và áp dụng ISO 27001: do hệ thống quản lý theo tiêu chuẩn ISO 27001 liên quan đến các phạm vi, gồm:

+ Chính sách an ninh;

+ An ninh tổ chức;

+ Quản lý tài sản;

+ An ninh nguồn nhân lực;

+ An ninh vật lý và môi trường;

+ Quản lý vận hành và truyền thông;

+ Kiểm soát truy cập;

+ Tiếp nhận, phát triển và duy trì hệ thống thông tin;

+ Quản lý sự cố, sự tuân thủ.

Mỗi lĩnh vực lại có thể liên quan đến một hay nhiều bộ phận của các Trung tâm nên cần phải lựa chọn nhân sự tham gia xây dựng và triển khai là điều quan trọng để tiếp tục duy trì và vận hành sau này.

III. LỢI ÍCH MANG LẠI

1. Lợi ích trực tiếp

- Giảm thiểu chi phí sửa chữa, bảo trì thiết bị và vận hành hệ thống: quá trình áp dụng sẽ áp các chính sách để kiểm soát việc vận hành tránh được việc tự các đặt các phần mềm không rõ nguồn gốc có thể dẫn đến lỗi phần mềm, hệ điều hành mất thời gian bảo trì, cài đặt lại…

- Các quá trình được tối ưu hóa, được quản lý và kiểm soát một cách có hệ thống: khi xây dựng hệ thống quản lý theo tiêu chuẩn này, các Trung tâm có điều kiện rà soát và tối ưu hóa các quá trình vận hành và tác nghiệp, giúp cán bộ quản lý được chuỗi các quá trình từ đó nâng cao nghiệp vụ quản lý và điều hành.

- Phát hiện được các lỗ hổng của hệ thống thông qua quá trình phân tích và đánh giá rủi ro.

- Phát hiện trước được các nguy cơ có thể xảy ra gây thất thoát, tổn thất cho đơn vị: quá trình này phối hợp với việc phát hiện lỗ hổng ở trên sẽ đánh giá và nhận biết các rủi ro có thể có đối với tài sản thông tin của đơn vị từ đó đề xuất biện pháp kiểm soát thích hợp.

- Đảm bảo duy trì được tính liên tục trong hoạt động chính: từ việc phân tích hệ thống và đánh giá rủi ro, nhiều hoạt động có thể có những nguy cơ gây gián đoạn như: cháy nổ, mất tài liệu, hư hỏng server, bị nhiễm virus, … do đó đơn

vị xây dựng biện pháp nhằm giảm thiểu những vấn đề trên và đảm bảo hoạt động liên tục 24/7.

- Tài sản thông tin của doanh nghiệp được bảo vệ.

- Hệ thống quản lý cũng cung cấp cho đơn vị phương pháp giải quyết các vấn đề an toàn thông tin khi gặp phải, đảm bảo giải quyết nhanh chóng, hiệu quả.

- Tăng sự tin cậy và nhận thức của các bên quan tâm: hệ thống được một bên thứ ba độc lập đánh giá và cấp giấy chứng nhận là một bằng chứng khách quan để tạo lòng tin cho các bên quan tâm.

- Tăng lợi thế, nâng cao uy tín trong cạnh tranh, đấu thầu: hiện nay rất nhiều đơn vị khi mời thầu có đưa vào nội dung doanh nghiệp dự thầu đã xây dựng và áp dụng ISMS và đã đạt chứng chỉ ISO/IEC 27001 do một tổ chức chứng nhận được quốc tế công nhận.

- Việc áp dụng và cải tiến liên tục các quá trình sẽ giúp cho đội ngũ IT làm việc bài bản hơn, khoa học hơn và ứng phó được với các tình huống khẩn cấp.

- Chứng minh được quản lý chuyên nghiệp và ứng phó tốt khi xảy ra sự cố, thảm họa.

- Chứng minh đáp ứng yêu cầu tiêu chuẩn, tuân thủ yêu cầu pháp luật.

2. Lợi ích gián tiếp

- Việc áp dụng các biện pháp kiểm soát sẽ càng ngày càng được cải thiện và bổ sung do nhận thức trong hệ thống này cũng ngày một rõ hơn và lớn lên theo thời gian.

- Với các quá trình được xây dựng thành văn bản, sẽ tạo ra sự minh bạch, rõ ràng trong cách thức và trình tự thực hiện cũng như là trách nhiệm và quyền hạn được định rõ, từ đó các cá nhân tự giác thực hiệc các công việc được giao và cũng là cơ sở để xử lý các hành vi vi phạm do vô tình hay cố ý.

- Các kế hoạch và công tác quản lý được cải tiến liên tục.

- Giấy chứng nhận cho hệ thống phù hợp với ISO/IEC 27001 là cơ sở tăng cường niềm tin cho các cơ quan, đơn vị và đối tác là một trong những công cụ cạnh tranh trong ngành.

- Góp phần đảm bảo an toàn an ninh thông tin trong ngành theo định hướng của Chính phủ.

IV. KINH PHÍ THỰC HIỆN

1. Kinh phí dự kiến thực hiện:

- Nguồn kinh phí: Ngân sách tỉnh.

- Tổng mức kinh phí thực hiện tạm tính: **297.000.000 đồng** (*Hai trăm chín mươi bảy triệu đồng*). Giao Sở Thông tin và Truyền thông lập dự toán, gửi Sở Tài chính thẩm định trình UBND tỉnh phê duyệt.

2. Thời gian thực hiện:

Từ năm 2014 đến năm 2015.

V. TỔ CHỨC THỰC HIỆN:

1. Sở Thông tin và Truyền Thông: chủ trì, phối hợp các cơ quan liên quan theo dõi việc triển khai thực hiện Đề án, định kỳ hàng tháng tổng hợp báo cáo kết quả thực hiện cho UBND tỉnh; đảm bảo việc thực hiện Đề án theo đúng lộ trình xây dựng và áp dụng chứng nhận ISO 27001.

2. Trung tâm Thông tin dữ liệu điện tử, Trung tâm Tin học hành chính phối hợp với đơn vị triển khai để đảm bảo hai Trung tâm tâm xây dựng và áp dụng hệ thống quản lý an toàn thông tin theo tiêu chuẩn TCVN ISO/IEC 27001:2009.

3. Sở Tài chính bố trí kinh phí để đảm bảo cho các đơn vị triển khai Đề án đúng tiến độ và đạt hiệu quả.

4. Văn phòng UBND tỉnh chủ trì theo dõi, đôn đốc các đơn vị liên quan trong quá trình triển khai thực hiện Đề án, kịp thời tham mưu UBND tỉnh chỉ đạo thực hiện, kiểm tra, giám sát, giải quyết các vướng mắc phát sinh.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền Thông, Sở Tài chính; Thủ trưởng các cơ quan liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- CT và các PCT UBND tỉnh;
- TT.EDIC - Sở TTTT;
- TT.THHC-VPUBND tỉnh;
- VP: CVP, P.CVP Đ.N.Tân;
- Lưu: VT, DL.

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

Phan Ngọc Thọ