

Số: 1576 /QĐ-UBND

Cà Mau, ngày 26 tháng 10 năm 2013

QUYẾT ĐỊNH
Về việc phê duyệt Kế hoạch Đảm bảo an toàn thông tin số
trong hoạt động cơ quan Nhà nước năm 2014

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức HĐND và UBND ngày 26/11/2003;

Căn cứ Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển an toàn thông tin số Quốc gia đến năm 2020;

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 bảo đảm an toàn thông tin số;

Căn cứ Công văn số 1943/BTTTT-CNTT ngày 04/7/2013 của Bộ Thông tin và Truyền thông về việc hướng dẫn xây dựng kế hoạch phát triển và ứng dụng công nghệ thông tin năm 2014;

Xét đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 77/TTr-STTTT ngày 18/10/2013,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Kế hoạch Đảm bảo an toàn thông tin số trong hoạt động cơ quan Nhà nước năm 2014 (kèm theo Kế hoạch số 35/KH-STTTT ngày 18/10/2013 của Sở Thông tin và Truyền thông).

Điều 2. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các ngành có liên quan tổ chức triển khai thực hiện, hướng dẫn, đôn đốc và kiểm tra việc thực hiện Kế hoạch này.

Điều 3. Chánh Văn phòng UBND tỉnh, Giám đốc các Sở: Thông tin và Truyền thông, Kế hoạch và Đầu tư, Tài chính; Chủ tịch UBND các huyện, thành phố Cà Mau và Thủ trưởng các sở, ngành, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này.

Quyết định này có hiệu lực thi hành kể từ ngày ký./.

Nơi nhận:

- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- PVP (H.Hùng);
- CVVX (T);
- Công TTTĐT;
- Trung tâm Công báo;
- Lưu: VT, Mi54/10.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Nguyễn Tiến Hải

KẾ HOẠCH

Đảm bảo an toàn thông tin số trong hoạt động cơ quan Nhà nước năm 2014

I. TÌNH HÌNH THỰC HIỆN AN TOÀN THÔNG TIN (ATTT) SỐ NĂM 2013

1. Hạ tầng kỹ thuật

Hiện nay, cơ sở hạ tầng CNTT tại các cơ quan nhà nước về cơ bản đã đáp ứng được các yêu cầu để triển khai các ứng dụng CNTT của Chính phủ và kế hoạch của tỉnh; 100% Sở, ban, ngành, UBND huyện, TP.Cà Mau đã có trang thông tin điện tử, góp phần quan trọng trong công tác chỉ đạo, điều hành của UBND tỉnh, các ngành và địa phương. Tuy nhiên, công tác đảm bảo an toàn, an ninh thông tin tại các ngành, các cấp trên địa bàn tỉnh còn rất thấp, cụ thể: số đơn vị có trang bị hệ thống tường lửa đúng chuẩn để bảo vệ hệ thống mạng LAN đạt 5%, tỷ lệ máy tính có phần mềm chống virus bản quyền chỉ đạt 10%, số còn lại 90% máy tính (trên 2.500 máy trong các cơ quan Đảng, Nhà nước, Đoàn thể) chỉ sử dụng phần mềm chống virus miễn phí hoặc không cài phần mềm chống virus nên nguy cơ mất an toàn thông tin, lộ bí mật nhà nước là rất cao.

2. Nguồn nhân lực bảo đảm ATTT

- Hàng năm Sở Thông tin và Truyền thông tổ chức trên 10 lớp tập huấn về quản trị mạng cho hơn 200 cán bộ, công chức, viên chức phụ trách CNTT trong các cơ quan nhà nước. Tuy nhiên, năm 2013 mới bắt đầu tổ chức các khóa đào tạo về đảm bảo an toàn an ninh và bảo mật mạng máy tính.

- Tỉnh có 02 cơ sở của 02 trường đại học đặt trên địa bàn tỉnh đã có chuyên ngành đào tạo CNTT, góp phần cung cấp và phát triển nguồn nhân lực CNTT đáng kể.

- Nguồn nhân lực CNTT đang làm việc tại các cơ quan cấp tỉnh và cấp huyện trên 1.613 người (trên đại học 3 người, đại học 129 người, cao đẳng và trung cấp 106 người, còn lại đều có trình độ sơ cấp phụ trách CNTT). Nhưng nguồn lực bảo đảm ATTT trên toàn tỉnh không quá 50 người.

3. Tình hình triển khai các dự án, nhiệm vụ đầu tư đảm bảo ATTT

- Việc đảm bảo an toàn thông tin (ATTT) số trong các cơ quan, đơn vị trên địa bàn tỉnh hiện nay hầu như chưa xây dựng hệ thống bảo mật, các phần mềm, phần cứng ATTT chưa được quan tâm đầu tư. Trong các dự án ứng dụng Công nghệ thông tin, các chủ đầu tư chưa quan tâm đến giải pháp kỹ thuật, giải pháp hành chính để đảm bảo an toàn, an ninh thông tin.

- Sở Thông tin và Truyền thông đang khẩn trương triển khai dự án “Xây dựng hệ thống an ninh mạng và bảo mật máy tính”, dự kiến hoàn thành trong năm 2013.

II. NỘI DUNG KẾ HOẠCH NĂM 2014

1. Đảm bảo an toàn thông tin số cho cơ sở hạ tầng thông tin

- Các hệ thống thông tin dùng chung của tỉnh, Cổng thông tin điện tử, hệ thống Hội nghị truyền hình trực tuyến, hệ thống mạng Truyền số liệu chuyên dùng, hệ thống thư điện tử tỉnh, hệ thống điều hành tác nghiệp đều được kiểm tra, đánh giá tổng thể khả năng đảm bảo an toàn thông tin số; đảm bảo vận hành an toàn, ổn định và thông suốt.

- Chuẩn hóa hệ thống mạng của các sở, ban, ngành tỉnh, uỷ ban nhân dân các huyện, thành phố theo hướng khai thác hiệu quả sử dụng nhưng vẫn bảo đảm tốt nhất an toàn thông tin số phù hợp với khả năng tài chính tỉnh và quy mô của hệ thống.

- Áp dụng quy trình quản lý an ninh, an toàn hạ tầng kỹ thuật tại các đơn vị bao gồm:

+ Các giải pháp bảo vệ nhằm ngăn chặn và phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu; theo dõi phòng ngừa thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại ra khỏi hệ thống;

+ Áp dụng các công nghệ xác thực, cơ chế quản lý quyền truy cập và cơ chế ghi biên bản hoạt động của hệ thống để quản lý và kiểm tra việc truy cập mạng;

+ Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ và máy trạm;

+ Các quy trình quản lý an toàn hạ tầng kỹ thuật khác.

2. Đảm bảo an toàn thông tin số cho hệ thống cơ sở dữ liệu

- Quản lý hệ thống thư điện tử: Rà soát, bổ sung, hoàn thiện quy định về đảm bảo an ninh thông tin trong việc sử dụng hệ thống thư điện tử trong hoạt động của các cơ quan Nhà nước.

- Trang bị hệ thống các phần mềm bảo mật, phần mềm diệt virus, mã độc hại đủ mạnh, có bản quyền để triển khai và khuyến khích các đơn vị áp dụng.

- Áp dụng quy trình đảm bảo an toàn dữ liệu tại các đơn vị, bao gồm:

+ Đảm bảo an toàn cơ sở dữ liệu đã được số hóa tại các đơn vị, từng bước đầu tư hệ thống số hoá thông tin ở các đơn vị chưa có.

+ Giám sát các khâu tạo lập, xử lý và hủy bỏ dữ liệu;

- Đẩy mạnh đầu tư trang thiết bị:

+ Trang bị các thiết bị tường lửa, thiết bị chống, phát hiện truy cập trái phép vào hệ thống Mạng truyền số liệu chuyên dùng, hệ thống Cổng thông tin điện tử, hệ thống Hội nghị truyền hình trực tuyến, hệ thống thư điện tử.

+ Trang bị các thiết bị chuyên dùng cho Bộ phận ứng cứu sự cố máy tính của tỉnh, đảm bảo đầy đủ các điều kiện để tác nghiệp trong các trường hợp khẩn cấp.

3. Đảm bảo an toàn an ninh cho các ứng dụng công nghệ thông tin

- Tuyên truyền, hướng dẫn người dân và doanh nghiệp sử dụng các dịch vụ hành chính công an toàn, tin cậy được tích hợp trên hệ thống Cổng thông tin điện tử tỉnh, các trang thông tin điện tử thành viên. Có các biện pháp đảm bảo an toàn thông tin, an ninh khi người dân và doanh nghiệp tham gia khai thác và sử dụng các dịch vụ công.

- Các ứng dụng về chính phủ điện tử và thương mại điện tử đều được đảm bảo an toàn thông tin ở mức cao nhất trong quá trình cung cấp các dịch vụ trực tuyến cho người dân.

- Từng bước xây dựng và đưa vào sử dụng hệ thống chứng thư số chữ ký số phục vụ các cơ quan, doanh nghiệp và người dân khi có nhu cầu. Đảm bảo tính xác thực và an toàn trong công tác điều hành, chỉ đạo của tỉnh và các giao dịch điện tử.

- Phối hợp với các đơn vị ngoài tỉnh phát triển các sản phẩm, giải pháp, quy trình, công nghệ đảm bảo an toàn thông tin số. Ưu tiên phát triển các sản phẩm, giải pháp phần mềm sử dụng mã nguồn mở, ban hành các quy trình về an toàn thông tin số theo những tiêu chuẩn quy định của Nhà nước đã ban hành.

4. Đào tạo, xây dựng nhân lực về an toàn thông tin số

- Triển khai thành lập Bộ phận ứng cứu sự cố máy tính (CSIRT) trực thuộc Sở Thông tin và Truyền thông.

- Đảm bảo 100% các đơn vị có bộ phận chuyên trách và cán bộ chuyên trách công nghệ thông tin được đào tạo cơ bản về an toàn an ninh thông tin.

- Bảo đảm 100% cán bộ chuyên trách an ninh, an toàn hệ thống của tỉnh và các đơn vị được đào tạo và cấp chứng chỉ theo chuẩn quốc tế về an ninh mạng và bảo mật máy tính.

III. GIẢI PHÁP

1. Về tài chính

- Bố trí kinh phí ngân sách tỉnh và các nguồn kinh phí hợp pháp khác để: đảm bảo an toàn thông tin số cho các hệ thống thông tin quan trọng của tỉnh; đầu tư các sản phẩm về an ninh, an toàn hệ thống dùng chung cho toàn tỉnh; triển khai hoặc nâng cấp hệ thống theo các mô hình điểm để nhân rộng trên địa bàn tỉnh.

- Tăng cường tìm kiếm, tranh thủ các nguồn vốn hỗ trợ của Trung ương và các dự án tài trợ của nước ngoài, đặc biệt là các dự án liên quan đến chính phủ

điện tử, an toàn bảo mật.

- Đối với việc bảo đảm an ninh thông tin cho các doanh nghiệp, các tổ chức khác, sử dụng nguồn vốn tự có của các doanh nghiệp và người dân.

2. Về triển khai

- Đẩy mạnh tuyên truyền sâu rộng cho tổ chức, người dân trên địa bàn tỉnh hiểu rõ về an toàn thông tin số. Phổ cập, nâng cao nhận thức của cán bộ, công chức trong bộ máy hành chính nhà nước, trước hết là lãnh đạo các cấp, các ngành về vai trò, vị trí và trách nhiệm của người đứng đầu cơ quan đơn vị, đảm bảo an toàn thông tin số trong các hoạt động của đơn vị mình.

- Tăng cường hợp tác giữa các tổ chức trong và ngoài nước trong việc bảo vệ cơ sở hạ tầng thông tin quốc gia, thiết lập mạng lưới theo dõi và cảnh báo sớm, điều phối ngăn chặn các cuộc tấn công.

- Phối hợp giữa các đơn vị tư vấn, chuyên gia an toàn thông tin số tiến hành thường xuyên rà quét các lỗ hổng trong hệ thống thông tin quan trọng của tỉnh, sẵn sàng ứng phó với những sự cố liên quan tới mất an toàn thông tin số.

- Thành lập Bộ phận ứng cứu sự cố máy tính nhằm ứng cứu sự cố máy tính của tỉnh và bộ phận này liên kết với các trung tâm của các tỉnh, thành khác thành một mạng lưới trên toàn quốc nhằm phối hợp, ứng phó kịp thời khi xảy ra các sự cố mất an toàn thông tin số.

- Đầu tư mua sắm trang thiết bị, kiện toàn, củng cố, giao nhiệm vụ cụ thể cho các đơn vị hữu quan hiện có; xây dựng cơ chế, tạo điều kiện cho các Trung tâm công nghệ thông tin của các trường đại học, cao đẳng, của các hội nghề nghiệp và các doanh nghiệp công nghệ thông tin trên địa bàn tham gia cung cấp dịch vụ và bảo đảm kỹ thuật về an toàn và bảo mật.

3. Về tổ chức thực hiện

- Rà soát, hoàn thiện bộ máy quản lý nhà nước về an toàn thông tin số từ các sở, ban, ngành tỉnh, ủy ban nhân dân các huyện, thành phố trong đó chú trọng nâng cao năng lực các cơ quan quản lý chuyên trách về an toàn thông tin số. Tăng cường các hoạt động dự báo, kiểm soát, phát hiện tấn công, cảnh báo sớm, ngăn chặn kịp thời và khắc phục sự cố khi có các cuộc tấn công. Tổ chức đánh giá định kỳ và công bố các báo cáo hàng năm về năng lực đảm bảo an toàn thông tin số đối với các hệ thống thông tin quan trọng của tỉnh.

- Các sở, ban, ngành tỉnh các huyện, thành phố có trách nhiệm bố trí đủ cán bộ chuyên trách về công nghệ thông tin, phù hợp với kế hoạch ứng dụng công nghệ thông tin và bảo đảm an ninh, an toàn thông tin số tại đơn vị mình.

4. Giải pháp môi trường chính sách

- Rà soát và hoàn thiện các văn bản quy phạm pháp luật, cơ chế và chính sách của Nhà nước, tạo môi trường thuận lợi để đảm bảo an toàn thông tin số, đáp ứng các yêu cầu về hội nhập toàn diện kinh tế quốc tế, thúc đẩy hợp tác và cạnh tranh lành mạnh giữa các doanh nghiệp.

- Kiến nghị cơ quan có thẩm quyền ban hành các chính sách ưu đãi cho cán bộ chuyên trách CNTT ở các cấp.

- Nghiên cứu về thể chế, cơ chế, giải pháp mới phù hợp với đặc điểm kinh tế xã hội của tỉnh để thực hiện có hiệu quả an toàn thông tin số tại các cơ quan, doanh nghiệp và người dân trên địa bàn tỉnh.

IV. KINH PHÍ THỰC HIỆN

- Tổng kinh dự kiến triển khai các dự án, nhiệm vụ năm 2014, sử dụng nguồn vốn sự nghiệp trong kế hoạch khoảng: 6.000.000.000 đồng (Bằng chữ: Sáu tỷ đồng chẵn).

(Phụ lục kèm theo)

V. TỔ CHỨC THỰC HIỆN

1. Trách nhiệm của Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với Sở Kế hoạch và Đầu tư, Sở Tài chính và các cơ quan có liên quan xây dựng kế hoạch, cân đối mức ngân sách bố trí cho kế hoạch hàng năm; tranh thủ các nguồn kinh phí hỗ trợ từ Trung ương và nước ngoài về ứng dụng công nghệ thông tin trong hoạt động của các cơ quan Nhà nước thuộc tỉnh, trình UBND tỉnh phê duyệt. Điều phối triển khai thực hiện kế hoạch, ưu tiên các dự án về an toàn bảo mật tại các đơn vị trên địa bàn tỉnh.

- Chủ trì, phối hợp với các cơ quan có liên quan nghiên cứu, đề xuất xây dựng các cơ chế, chính sách hỗ trợ, khuyến khích các hoạt động nghiên cứu phát triển các biện pháp và ứng dụng đảm bảo an toàn thông tin số trình UBND tỉnh xem xét, quyết định.

2. Sở Thông tin và Truyền thông đề nghị các đơn vị có liên quan phối hợp thực hiện tốt Kế hoạch này, cụ thể như:

2.1. Sở Kế hoạch và Đầu tư

- Cân đối và đưa vào kế hoạch của tỉnh các kế hoạch 5 năm và hàng năm về ứng dụng công nghệ thông tin, các dự án về an toàn bảo mật mạng máy tính, thông tin số.

- Tranh thủ các nguồn vốn từ trung ương và tài trợ của nước ngoài cho các dự án ứng dụng công nghệ thông tin, đặc biệt là các dự án về đảm bảo an toàn thông tin số trên địa bàn tỉnh.

2.2. Sở Tài chính

- Ưu tiên bố trí kinh phí cho các đề án, dự án an toàn an ninh thông tin trên địa bàn tỉnh theo kế hoạch hàng năm đã được cấp có thẩm quyền phê duyệt.

- Hướng dẫn các đơn vị bố trí kinh phí cho ứng dụng công nghệ thông tin, an toàn bảo mật theo kế hoạch của tỉnh.

2.3. Các sở, ban, ngành tỉnh; UBND huyện, thành phố Cà Mau

Phối hợp với Sở Thông tin và Truyền thông thực hiện có hiệu quả kế

hoạch này và đồng bộ với kế hoạch phát triển kinh tế - xã hội của tỉnh, của ngành và của từng huyện, thành phố.

Trên đây là Kế hoạch đảm bảo an toàn thông tin số trong hoạt động cơ quan nhà nước tỉnh Cà Mau năm 2014 trên địa bàn tỉnh Cà Mau.

Nơi nhận:

- UBND tỉnh;
- Đ/c Nguyễn Tiến Hải, PCTUBND tỉnh (B/cáo)
- Sở Kế hoạch và Đầu tư;
- Sở Tài chính;
- Sở, ban, ngành tỉnh;
- UBND các huyện, thành phố;
- Lưu: VT, PKHTC.

GIÁM ĐỐC



Võ Quốc Việt



(Kèm theo Kế hoạch Số 35/KH-STTT ngày 18/10/2013 của Sở Thông tin và Truyền thông)

TT	Tên dự án, nhiệm vụ	Mục tiêu, quy mô	Thời gian thực hiện	Đơn vị chủ trì	Dự kiến tổng kinh phí (triệu đồng)	Nội dung/hạng mục công việc năm 2014	Dự kiến kinh phí năm 2014 (triệu đồng)	
							NS địa phương	Nguồn khác
I	Các dự án sử dụng vốn đầu tư theo Quyết định số 1599/QĐ-UBND ngày 06/11/2012, Sở Thông tin và Truyền thông đề xuất điều chỉnh sử dụng vốn sự nghiệp (năm 2014: 5.000 triệu đồng)							
1	Đầu tư phần cứng, phần mềm bảo đảm an toàn, bảo mật thông tin số tại các đơn vị cấp tỉnh, cấp huyện (Công Thông tin điện tử, và các công thành phần ; VIC; các phần mềm chuyên dùng v.v...).	Các cơ quan nhà nước các cấp	2013 - 2015	Sở TT&TT	4.500	Đầu tư các phần cứng, phần mềm bảo đảm an toàn, bảo mật thông tin tại các đơn vị	3.000	
2	Đầu tư trang thiết bị nghiên cứu của bộ phận ứng cứu sự cố máy tính	Ứng phó khi xảy ra các sự cố mất an toàn thông tin số	2013 - 2015	Sở TT&TT	3.000	Đầu tư trang thiết bị nghiên cứu của bộ phận ứng cứu sự cố máy tính	2.000	
Tổng cộng					7.500		5.000	
II	Các nhiệm vụ sử dụng vốn sự nghiệp (năm 2014: 1.000 triệu đồng)							
1	Duy trì và mở rộng hệ thống chứng thư số, và chữ ký số các cơ quan cấp tỉnh, cấp huyện	31 đơn vị quản lý nhà nước	2013-2015	Sở TT&TT	1.500	Duy trì hệ thống chứng thư số, và chữ ký số các cơ quan cấp tỉnh, cấp huyện	500	
2	Đào tạo, tập huấn an toàn an ninh thông tin và bảo mật máy tính từ cơ bản đến chuyên sâu	31 đơn vị quản lý nhà nước	2014 -2015	Sở TT&TT	1.000	Đào tạo, tập huấn an toàn an ninh thông tin và bảo mật máy tính từ cơ bản đến chuyên sâu	500	
Tổng cộng					2.500		1.000	