ỦY BAN NHÂN DÂN TỈNH TÂY NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2273 /QĐ-UBND	*Tây Ninh, ngày 18 tháng 10 năm 2019*

QUYẾT ĐỊNH

Phê duyệt Kế hoạch triển khai thực hiện Chỉ thị 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH

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

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Chỉ thị 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 54/TTr-STTTT ngày 12 tháng 9 năm 2019,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt kèm theo Quyết định này Kế hoạch triển khai thực hiện Chỉ thị 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

Điều 2. Sở Thông tin và Truyền thông có trách nhiệm triển khai, theo dõi tiến độ thực hiện kế hoạch đã được phê duyệt theo đúng quy định.

Điều 3. Chánh Văn phòng Đoàn ĐBQH, HĐND và UBND tỉnh, Thủ trưởng các sở, ban, ngành có liên quan, Chủ tịch Ủy ban nhân dân các huyện, thành phố chịu trách nhiệm thi hành Quyết định này kể từ ngày ký./.

Nơi nhận:
- Như Điều 3;
- CT, các PCT.UBND tỉnh;
- CVP;
- Phòng VHXH,TTHCC;
- Lưu VT, VP.Đoàn ĐBQH, HĐND,UBND tỉnh.

5

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thanh Ngọc

ỦY BAN NHÂN DÂN TỈNH TÂY NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

KẾ HOẠCH

Triển khai thực hiện Chỉ thị 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam

(Ban hành kèm theo Quyết định số 2273/QĐ-UBND ngày 18./.10/2019 của Chủ tịch Ủy ban nhân dân tỉnh)

Thực hiện Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Ủy ban nhân dân tỉnh ban hành Kế hoạch thực hiện Chỉ thị số 14/CT-TTg ngày 07/6/2019, cụ thể như sau:

I. MỤC TIÊU

1. Mục tiêu chung

- Quán triệt, triển khai thực hiện nghiêm túc Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ nhằm tạo sự chuyển biến, nâng cao năng lực, nhận thức và trách nhiệm của cán bộ, công chức, viên chức và nhân dân trên địa bàn tỉnh về an toàn, an ninh mạng.

- Tăng cường phối hợp giữa các cơ quan, tổ chức, doanh nghiệp về bảo đảm an toàn, an ninh mạng; triển khai các hoạt động giám sát, đánh giá, bảo vệ các hệ thống thông tin của tỉnh bảo đảm khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ.

- Đe dọa mất an toàn thông tin trên mạng, sẵn sàng các giải pháp phòng ngừa và ứng phó khi có sự cố về an toàn, an ninh mạng, góp phần cải thiện Chỉ số an toàn, an ninh thông tin toàn cầu - Global Cybersecurity Index (GCI) của Việt Nam.

2. Mục tiêu cụ thể

- Tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng đến 100% cán bộ, công chức, viên chức toàn tỉnh. Đảm bảo 100% các đơn vị có cán bộ chuyên trách CNTT được đào tạo chuyên sâu về an toàn, an ninh thông tin.

- 100% cơ quan nhà nước được áp dụng phương án an toàn thông tin phù hợp, triển khai chuẩn hóa cấp độ an toàn của các hệ thống thông tin và tổ chức thực hiện nghiêm túc Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác các hệ thống thông tin đang sử dụng.

- 100% các hệ thống thông tin dùng chung, các hệ thống mạng LAN, máy chủ, máy trạm của các Sở, Ban, ngành cấp tỉnh, UBND cấp huyện; UBND cấp xã và mạng chuyên dùng của các cơ quan nhà nước được trang bị giải pháp an toàn, bảo mật nhằm bảo đảm an toàn thông tin trên môi trường mạng.

- 100% cổng, trang thông tin điện tử của các cơ quan nhà nước được giám sát, sẵn sàng các biện pháp phòng ngừa, ngăn chặn tấn công gây mất an toàn thông tin và có phương án khắc phục sự cố đảm bảo hệ thống hoạt động liên tục 24/24h..

- Tăng cường năng lực cho cơ quan chuyên trách về an toàn thông tin và mạng lưới ứng cứu sự cố mạng máy tính của các cơ quan nhà nước trên địa bàn tỉnh.

II. NHIỆM VỤ VÀ GIẢI PHÁP CHỦ YẾU

1. Hoàn thiện hệ thống các văn bản về an toàn, an ninh thông tin

a. Rà soát cơ chế, chính sách, hành lang pháp lý về an toàn thông tin mạng, an ninh mạng, tội phạm mạng, bảo vệ trẻ em trên môi trường mạng.

b. Hoàn thiện cơ chế, chính sách, xây dựng chiến lược, quy hoạch, kế hoạch phát triển an toàn thông tin mạng; phát triển nguồn nhân lực an toàn, an ninh mạng; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng.

c. Xây dựng và ban hành văn bản nâng cao hiệu quả hoạt động của Cơ quan chuyên trách và mạng lưới đảm bảo an toàn thông tin trên địa bàn.

2. Tuyên truyền, nâng cao nhận thức về an toàn, an ninh mạng

a. Tổ chức quán triệt và thực hiện có hiệu quả Luật An toàn thông tin mạng; Luật An ninh mạng; các văn bản của Chính phủ, Kế hoạch của tỉnh về an toàn, an ninh mạng; nâng cao nhận thức, trách nhiệm cho đội ngũ cán bộ, công chức, viên chức về công tác an toàn, an ninh mạng.

b. Thực hiện tuyên truyền trên các phương tiện thông tin đại chúng như Báo Tây Ninh, Đài Phát thanh - Truyền hình tỉnh, hệ thống Đài truyền thanh các cấp và trên cổng, trang thông tin điện tử nhằm nâng cao nhận thức về an toàn, an ninh thông tin cho người dân, doanh nghiệp.

c. Nâng cao nhận thức về an toàn an ninh thông tin cho các cán bộ phụ trách CNTT, CBCCVC theo Quyết định 893/QĐ-TTg phê duyệt Đề án tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin (ATTT) đến năm 2020.

3. Hạ tầng bảo đảm an toàn, an ninh thông tin mạng

a. Đầu tư nâng cấp hệ thống trang thiết bị lưu trữ dữ liệu, sao lưu dự phòng cho các máy chủ và máy trạm, sao lưu dữ liệu cho các hệ thống phần

mềm dùng chung như phần mềm điều hành tác nghiệp, hệ thống một cửa điện tử, cơ sở dữ liệu chuyên ngành,... đảm bảo an toàn dữ liệu ở mức cao nhất cho các hệ thống.

b. Nâng cao năng lực, cơ sở vật chất cho cơ quan chuyên trách an toàn thông tin của tỉnh; đầu tư trang bị các thiết bị chuyên dùng cho Đội ứng cứu sự cố an toàn thông tin của tỉnh, bảo đảm đủ điều kiện tác nghiệp trong các trường hợp khẩn cấp có thể gây sự cố nghiêm trọng hay khủng bố mạng.

4. Triển khai các ứng dụng phòng ngừa

a. Triển khai các biện pháp đảm bảo an toàn thiết bị, hạ tầng viễn thông, CNTT trong đấu thầu, mua sắm, đặc biệt là các thiết bị quan trọng. Riêng các dự án về CNTT khi xây dựng bắt buộc phải có cấu phần mua sắm giải pháp phòng, chống mã độc, bảo đảm tuân thủ đúng quy định của pháp luật.

b. Kiểm tra, rà soát các lỗ hổng bảo mật, an toàn thông tin trên Cổng thông tin điện tử, trang thông tin điện tử các cơ quan nhà nước trên địa bàn tỉnh; phối hợp triển khai trong các cơ quan Đảng; xây dựng các giải pháp và tổ chức khắc phục lỗ hổng, điểm yếu có rủi ro gây mất an toàn thông tin.

c. Triển khai các giải pháp đảm bảo an toàn thông tin cho các dịch vụ cung cấp trên Cổng thông tin điện tử tỉnh, cổng/trang thông tin điện tử các cơ quan nhà nước; hệ thống thư điện tử của tỉnh; phần mềm quản lý điều hành của tỉnh, huyện; hệ thống một cửa điện tử của các cơ quan nhà nước.

d. Chuẩn hóa hệ thống mạng của các cơ quan nhà nước theo hướng khai thác hiệu quả sử dụng nhưng vẫn bảo đảm mật, an toàn thông tin phù hợp với khả năng tài chính và quy mô của hệ thống.

đ. Thực hiện đồng bộ các biện pháp phòng, chống mã độc, bảo vệ 100% máy trạm, thiết bị đầu cuối liên quan tại các sở, ban ngành, UBND các huyện.

e. Nâng cấp, bảo trì hệ thống lưu trữ, hệ thống giám sát an toàn thông tin, hệ thống máy chủ nhằm duy trì hoạt động thường xuyên của trung tâm tích hợp dữ liệu tỉnh; đảm bảo an toàn thông tin mạng.

g. Sửa đổi, bổ sung các quy định, quy chế vận hành hoạt động và triển khai ứng dụng CNTT trong hoạt động của cơ quan nhà nước, tổ chức thực hiện đồng bộ, đúng quy định đảm bảo an toàn, an ninh thông tin.

h. Áp dụng quy trình quản lý 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 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;

- Áp dụng quy trình sao lưu, dự phòng (backup) dữ liệu, bảo đảm an toàn dữ liệu, đầu tư các thiết bị lưu trữ dữ liệu an toàn từ tỉnh đến các Sở, Ban, ngành, UBND các huyện, thành phố;

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

5. Triển khai các nội dung xử lý sự cố

a. Hướng dẫn các đơn vị xây dựng hồ sơ an toàn thông tin theo cấp độ.

b. Kiện toàn Đội Ứng phó sự cố an toàn thông tin của tỉnh. Nâng cao kỹ năng và hiệu quả hoạt động của đội ứng cứu sự cố an toàn thông tin mạng, tập trung phòng, chống, phát hiện xâm nhập trái phép và tấn công từ chối dịch vụ. Tổ chức diễn tập đảm bảo an toàn thông tin mạng, phòng chống tấn công mạng vào các hệ thống thông tin của tỉnh Tây Ninh

c. Định kỳ hàng năm thực hiện kiểm tra, đánh giá mức độ an toàn, an ninh thông tin trong các cơ quan nhà nước trong tỉnh; nghiên cứu đề xuất nhiều giải pháp tăng cường bảo đảm an toàn, an ninh thông tin cho các hạ tầng và hệ thống thông tin triển khai ứng dụng tại tỉnh. Lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện việc giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ các hệ thống thông tin trọng yếu của tỉnh; lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật.

d. Tổ chức kiểm thử đánh giá mức bảo mật đối với các hệ thống thông tin dùng chung, các hệ thống quan trọng để xây dựng giải pháp bảo mật tối ưu, phù hợp. Triển khai các phương pháp bảo vệ sau xử lý sự cố

đ. Triển khai hệ thống giám sát và phòng, chống tấn công mạng đối với các hệ thống thông tin của các cơ quan, đơn vị để quản lý, giám sát tập trung tại Trung tâm giám sát điều hành tập trung của tỉnh.

e. Tổ chức Hội thảo về an toàn thông tin mạng cấp tỉnh;

6. Đào tạo nguồn nhân lực

a. Phổ biến, đào tạo, tập huấn nâng cao nhận thức an toàn thông tin cho cán bộ, công chức, viên chức các cơ quan nhà nước, cơ quan Đảng trên địa bàn

tỉnh. Hỗ trợ cán bộ chuyên trách CNTT tham gia các lớp tập huấn chuyên ngành về an toàn thông tin do các bộ, ngành Trung ương tổ chức.

b. Đào tạo vận hành hệ thống an toàn thông tin cho 100% đội ngũ cán bộ chuyên trách CNTT cấp tỉnh, cấp huyện. Tổ chức thực hiện chương trình đào tạo nâng cao trình độ chuyên môn, nghiệp vụ cho cán bộ thực hiện nhiệm vụ chuyên trách CNTT cấp xã; hình thành đội ngũ cán bộ chuyên trách an toàn thông tin từ cấp tỉnh đến cấp xã. Đào tạo nâng cao nhận thức an toàn thông tin cho lãnh đạo CNTT (CIO) các cấp.

c. Đào tạo ngắn hạn về an toàn thông cho đội ngũ chuyên trách CNTT cấp tỉnh, cấp huyện, ưu tiên cho nhân lực quản lý, vận hành các hệ thống thông tin trọng yếu của tỉnh.

III. TỔ CHỨC THỰC HIỆN

1 Các Sở, ban, ngành và UBND các huyện, thành phố

- Chủ trì, phối hợp với các ngành liên quan thực hiện các nội dung tại Điểm a, d, đ, g, h Mục 4 Phần II của Kế hoạch.

- Tổ chức sử dụng có hiệu quả các hạ tầng thiết bị, hệ thống thông tin đã triển khai tại cơ quan, đơn vị.

- Quán triệt nguyên tắc Thủ trưởng cơ quan các Sở, Ban, ngành; Chủ tịch UBND huyện, thành phố trên địa bàn tỉnh Tây Ninh chịu trách nhiệm trước UBND tỉnh, Chủ tịch UBND tỉnh nếu để xảy ra mất an toàn, an ninh mạng, lộ lọt bí mật nhà nước tại cơ quan, đơn vị mình quản lý.

- Sử dụng và quản lý khóa bí mật (USB token) của chữ ký số, dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, chứng thư số, các giải pháp mã hóa của Ban Cơ yếu Chính phủ theo đúng quy định.

- Kịp thời cung cấp thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác trong lĩnh vực an toàn, an ninh mạng phục vụ việc đánh giá, xếp hạng chỉ số GCI của ITU.

- Căn cứ Kế hoạch này, xây dựng Kế hoạch thực hiện Chỉ thị số 14/CT-TTg của cơ quan, đơn vị, địa phương; tổ chức triển khai các nhiệm vụ và giải pháp theo sự chỉ đạo, điều hành của UBND tỉnh và hướng dẫn của Sở Thông tin và Truyền thông, đảm bảo sự thống nhất, chất lượng và hiệu quả trong triển khai thực hiện.

- Kịp thời thông tin, báo cáo về Sở Thông tin và Truyền thông để phối hợp xử lý, khắc phục sự cố.

- Thông báo về Sở Thông tin và Truyền thông khi có thay đổi nhân sự đầu mối thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng

2. Sở Thông tin và Truyền thông

- Chủ trì phối hợp với Công an tỉnh, các Sở, Ban, ngành; UBND các huyện, thành phố triển khai thực hiện các nhiệm vụ, giải pháp tại Điểm a, b Mục 1; Mục 2; Mục 3; Điểm b, c, d, đ, e, Mục 4; Mục 5; Mục 6 Phần II của Kế hoạch.

- Tham mưu giúp UBND tỉnh đôn đốc, kiểm tra các đơn vị trong quá trình triển khai thực hiện Kế hoạch này. Tổng hợp kết quả thực hiện và những vướng mắc trong quá trình triển khai Kế hoạch để báo cáo, đề xuất UBND tỉnh điều chỉnh cho phù hợp.

- Hằng năm, tổng hợp chung nhu cầu vốn đầu tư và vốn sự nghiệp chi cho hoạt động bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh trong Kế hoạch ứng dụng CNTT, xây dựng Chính quyền điện tử của tỉnh để thực hiện nhiệm vụ. Phối hợp với Sở Kế hoạch và Đầu tư, Sở Tài chính xây dựng dự toán kinh phí các chương trình, dự án, hạng mục về bảo đảm an toàn, an ninh mạng trình UBND tỉnh xem xét phê duyệt.

3. Công an tỉnh

- Chủ trì, phối hợp với các ngành liên quan thực hiện các nội dung tại Điểm c Mục 1.

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông, các cơ quan, đơn vị có liên quan thực hiện nhiệm vụ kiểm tra, đánh giá toàn diện về hiện trạng, đánh giá phân loại các nhóm nguy cơ, mức độ rủi ro, thiệt hại từ các sự cố an toàn thông tin; dự báo xu hướng phát triển của tội phạm công nghệ cao và đề xuất hệ thống giải pháp thực thi hiệu quả việc bảo đảm an toàn thông tin mạng trong toàn tỉnh hàng năm và giai đoạn.

- Thường xuyên nắm tình hình không gian mạng trên địa bàn tỉnh, phát hiện, đấu tranh, xử lý nghiêm các đối tượng vi phạm Luật An ninh mạng, tập trung phối hợp phát hiện các lỗ hổng bảo mật, lộ lọt thông tin bí mật của các cơ quan Đảng, Nhà nước, hệ thống chính trị.

- Chủ trì, phối hợp với các cơ quan liên quan tiếp tục hoàn thiện các văn bản hướng dẫn thực hiện về an ninh mạng, tội phạm mạng và bảo vệ dữ liệu cá nhân trên môi trường mạng.

- Đẩy mạnh công tác tuyên truyền, phổ biến pháp luật; thường xuyên thông báo, cảnh báo cho các cơ quan nhà nước, người dân và doanh nghiệp về phương thức, thủ đoạn mới của các loại tội phạm gây mất an toàn, an ninh thông tin để có biện pháp phòng ngừa, đấu tranh, ngăn chặn.

- Tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin thuộc lĩnh vực do Công an tỉnh chịu trách nhiệm quản lý.

- Phối hợp chặt chẽ với Sở Thông tin và Truyền thông trong hoạt động thẩm định, phê duyệt hồ sơ cấp độ và bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng của tỉnh.

4. Bộ Chỉ huy Quân sự tỉnh

- Tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin thuộc lĩnh vực do đơn vị chịu trách nhiệm quản lý.

- Phối hợp chặt chẽ với Sở Thông tin và Truyền thông trong hoạt động thẩm định, phê duyệt hồ sơ cấp độ và bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng của tỉnh.

5. Văn phòng Đoàn ĐBQH, HĐND và UBND tỉnh

- Chủ trì, phối hợp Sở Thông tin và Truyền thông xây dựng kế hoạch đẩy mạnh chương trình cải cách hành chính trên cơ sở phát triển ứng dụng CNTT, đảm bảo an toàn thông tin trong hoạt động quản lý và điều hành của các cơ quan nhà nước.

6. Sở Kế hoạch và Đầu tư, Sở Tài chính

- Tham mưu cho UBND tỉnh ưu tiên bố trí vốn đầu tư phát triển, vốn chi sự nghiệp thường xuyên hằng năm cho các Sở, Ban, ngành, UBND huyện, thành phố để triển khai hoạt động bảo đảm an toàn, an ninh mạng.

- Trong quá trình thẩm định, cân đối nguồn vốn cho các dự án Công nghệ thông tin, bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin (trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ).

7. Sở Giáo dục và Đào tạo

- Chỉ đạo, định hướng, hướng dẫn các cơ sở đào tạo, đơn vị trực thuộc xây dựng kế hoạch đào tạo nhân lực an toàn, an ninh mạng đáp ứng nhu cầu của tỉnh.

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông đẩy mạnh triển khai các chương trình tuyên truyền, phổ biến, nâng cao nhận thức về an toàn, an ninh mạng trong các cơ sở đào tạo.

8. Sở Khoa học và Công nghệ

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông, Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và các sở, ngành liên quan công bố và hướng dẫn các tiêu chuẩn, quy chuẩn kỹ thuật trong lĩnh vực an toàn thông tin mạng.

- Chủ trì, phối hợp với các cơ quan, đơn vị, địa phương kết nối các chương trình, nhiệm vụ khoa học và công nghệ, khuyến khích, đẩy mạnh các đề tài khoa học liên quan đến an toàn, an ninh thông tin, sớm đưa các sản phẩm đề tài khoa trong lĩnh vực an toàn, an ninh thông tin vào ứng dụng trong các cơ quan nhà nước.

9. Sở Nội vụ

- Phối hợp Sở Thông tin và Truyền thông xây dựng kế hoạch đào tạo, bồi dưỡng đội ngũ lãnh đạo, đội ngũ CBCC các cấp trong tỉnh về đảm bảo an toàn thông tin trong hoạt động các cơ quan nhà nước.

10. Sở Lao động - Thương binh và Xã hội

- Chủ trì hướng dẫn pháp luật về bảo vệ trẻ em trên môi trường mạng.

- Tăng cường công tác tuyên truyền, thực thi, cơ chế tương tác, công cụ, phương tiện để bảo vệ trẻ em trên môi trường mạng.

11. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP)

- Thiết lập, kiện toàn đầu mối đơn vị chuyên trách an toàn thông tin mạng trực thuộc để bảo vệ hệ thống, khách hàng của mình; tham gia hỗ trợ các cơ quan, tổ chức trong tỉnh giám sát, bảo vệ, kiểm tra, đánh giá an toàn thông tin mạng dưới sự điều phối của Sở Thông tin và Truyền thông.

Yêu cầu Thủ trưởng các cơ quan, đơn vị, địa phương chỉ đạo tổ chức triển khai thực hiện nghiêm túc Kế hoạch này; trong quá trình thực hiện nếu có vướng mắc, khó khăn, các cơ quan, đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBNB tỉnh xem xét, quyết định./.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thanh Ngọc

DANH MỤC
CÁC NHIỆM VỤ TRIỂN KHAI THỰC HIỆN
(Ban hành kèm theo Quyết định số 2273/QĐ-UBND, ngày 18 /10/2019 của UBND tỉnh Tây Ninh)

STT	Tên nhiệm vụ	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian thực hiện
I	**Hoàn thiện hệ thống các văn bản về an toàn, an ninh thông tin mạng**			
1	Rà soát, hoàn thiện cơ chế, chính sách, hành lang pháp lý về an toàn thông tin mạng, an ninh mạng, tội phạm mạng, bảo vệ trẻ em trên môi trường mạng	Sở Thông tin và Truyền thông; Công an tỉnh	Các Sở, Ban, ngành; UBND các huyện, thành phố	Thường xuyên hàng năm
2	Hoàn thiện cơ chế, chính sách, xây dựng chiến lược, quy hoạch, kế hoạch phát triển an toàn thông tin mạng; phát triển nguồn nhân lực an toàn, an ninh mạng; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng	Sở Thông tin và Truyền thông	Các Sở, Ban, ngành; UBND các huyện, thành phố	Thường xuyên hàng năm
3	Rà soát, sửa đổi quy chế phối hợp giữa Công an tỉnh và Sở Thông tin và Truyền thông về hoạt động đảm bảo an toàn, an ninh mạng	Công an tỉnh	Sở Thông tin và Truyền thông	2019-2020
II	**Tuyên truyền, nâng cao nhận thức về an toàn, an ninh thông tin mạng**			
1	Quán triệt và đẩy mạnh công tác tuyên truyền Luật An toàn thông tin mạng; Luật An ninh mạng; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ; Kế hoạch này và các văn	Đài PTTH tỉnh; Báo Tây Ninh; các Sở, Ban, ngành; UBND các huyện,		Thường xuyên hàng năm

	bản của Chính phủ, của tỉnh về an toàn, an ninh mạng nhằm nâng cao nhận thức về an toàn, an ninh thông tin mạng cho cán bộ, công chức và người dân, doanh nghiệp	thành phố		
2	Đổi mới phương thức tuyên truyền, xây dựng chuyên mục riêng hoặc lồng ghép với chuyên mục về lĩnh vực Công nghệ thông tin, các nội dung về an toàn, an ninh mạng	Đài PTTH tỉnh	Các Sở, Ban, ngành; UBND các huyện, thành phố	Thường xuyên hàng năm
3	Tổ chức Hội thảo về an toàn thông tin mạng cấp tỉnh; diễn tập bảo đảm an toàn thông tin và ứng cứu sự cố mạng	Sở Thông tin và Truyền thông	Công an tỉnh; các Sở, Ban, ngành; UBND các huyện, thành phố	Thường xuyên hàng năm
III	**Hạ tầng bảo đảm an toàn, an ninh thông tin mạng**			
1	Rà soát, đầu tư bổ sung trang thiết bị lưu trữ dữ liệu, sao lưu dự phòng cho các máy chủ và máy trạm, sao lưu dữ liệu cho các hệ thống phần mềm dùng chung	Sở Thông tin và Truyền thông	Sở Kế hoạch và Đầu tư; Sở Tài chính;	Thường xuyên hàng năm
2	Đầu tư trang bị các thiết bị chuyên dùng cho Đội ứng cứu sự cố an toàn thông tin của tỉnh	Sở Thông tin và Truyền thông	Sở Kế hoạch và Đầu tư; Sở Tài chính	Thường xuyên hàng năm
3	Nâng cấp, bảo trì hệ thống lưu trữ, hệ thống giám sát an toàn thông tin, hệ thống máy chủ nhằm duy trì hoạt động thường xuyên của trung tâm tích hợp dữ liệu tỉnh; đảm bảo an toàn thông tin mạng	Sở Thông tin và Truyền thông	Sở Kế hoạch và Đầu tư; Sở Tài chính	2019-2020 và thường xuyên hàng năm

IV	**Triển khai các ứng dụng phòng ngừa**			
1	Triển khai thực hiện thuê dịch vụ kiểm tra, rà soát các lỗ hổng bảo mật, an toàn thông tin trên Cổng thông tin điện tử, trang thông tin điện tử các cơ quan nhà nước trên địa bàn tỉnh	Sở Thông tin và Truyền thông	Sở Kế hoạch và Đầu tư; Sở Tài chính; các đơn vị có liên quan	2019-2020
2	Triển khai giải pháp thuê dịch vụ bảo vệ Website phòng chống tấn công xâm nhập và tấn công DDoS cho Cổng thông tin điện tử tỉnh, cổng/trang thông tin điện tử các cơ quan nhà nước; hệ thống thư điện tử của tỉnh; Cổng dịch vụ công, hệ thống Một cửa điện tử; hệ thống Quản lý văn bản và điều hành của tỉnh …	Sở Thông tin và Truyền thông	Sở Kế hoạch và Đầu tư; Sở Tài chính; các đơn vị có liên quan	2019-2020 và thường xuyên hàng năm
V	**Triển khai các nội dung xử lý sự cố an toàn, an ninh thông tin mạng**			
1	Lựa chọn tổ chức, doanh nghiệp có đủ năng lực cung cấp dịch vụ giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ các hệ thống thông tin trọng yếu của tỉnh; tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu	Sở Thông tin và Truyền thông	Sở Kế hoạch và Đầu tư; Sở Tài chính; các đơn vị liên quan	2019-2020 và thường xuyên hàng năm
2	Thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng,bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện	Các Sở, Ban, ngành; UBND các huyện, thành phố	Sở Thông tin và Truyền thông	2019-2020 và thường xuyên hàng năm

3	Thông báo thông tin đầu mối thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng	Các Sở, Ban, ngành; UBND các huyện, thành phố	Sở Thông tin và Truyền thông	Trước ngày 15/12/2019 và khi có sự thay đổi về thông tin đầu mối
VI	**Đào tạo nguồn nhân lực**			
1	Đào tạo vận hành hệ thống an toàn thông tin; nâng cao trình độ chuyên môn, nghiệp vụ cho cán bộ thực hiện nhiệm vụ chuyên trách CNTT cấp xã; lãnh đạo CNTT (CIO) các cấp	Sở Thông tin và Truyền thông	Sở Nội vụ; các Sở, Ban, ngành; UBND các huyện, thành phố	Thường xuyên hàng năm
2	Đào tạo ngắn hạn về an toàn thông tin trong nước và Quốc tế cho đội ngũ chuyên trách CNTT cấp tỉnh, cấp huyện, ưu tiên cho hệ thống thông tin trọng yếu của tỉnh.	Sở Thông tin và Truyền thông	Sở Nội vụ; các Sở, Ban, ngành; UBND các huyện, thành phố	Thường xuyên hàng năm