ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 256 /KH-UBND	*Hà Tĩnh, ngày 03 tháng 8 năm 2018*

KẾ HOẠCH

Bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước tỉnh Hà Tĩnh giai đoạn 2018 - 2020

I. CĂN CỨ PHÁP LÝ

Luật An toàn thông tin mạng ngày;

Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư về tăng cường công tác bảo đảm an toàn thông tin mạng;

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;

Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

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;

Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an ninh và an toàn thông tin mạng trong tình hình mới;

Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

II. MỤC TIÊU

1. Mục tiêu chung

- Tạo sự chuyển biến sâu sắc trong nhận thức của cán bộ, công chức, viên chức và Nhân dân về tầm quan trọng của công tác đảm bảo an toàn thông tin mạng.

- Bảo đảm an toàn thông tin mạng của các cơ quan nhà nước trong toàn tỉnh, có 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 thông tin mạng.

- Nâng cao năng lực chuyên môn về an toàn, an ninh thông tin cho cán bộ chuyên trách CNTT toàn tỉnh.

2. Mục tiêu cụ thể đến năm 2020

- 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 của các sở, ban, ngành cấp tỉnh, UBND cấp huyện 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 24/24.

- 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.

III. NHIỆM VỤ

1. Hoàn thiện hệ thống các văn bản về an toàn thông tin trên địa bàn

- Rà soát, ban hành các quy định, quy chế về bảo đảm an toàn thông tin mạng trên địa bàn tỉnh; các kế hoạch, phương án ứng phó sự cố an toàn thông tin mạng.

- Xây dựng, ban hành một số chính sách đặc thù đối với chuyên gia, cán bộ có trình độ cao trực tiếp thực hiện nhiệm vụ chuyên trách về an toàn thông tin, ứng cứu sự cố và bảo đảm an toàn thông tin mạng của tỉnh.

- 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 thông tin mạng

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

- Thực hiện tuyên truyền trên các phương tiện thông tin đại chúng như Báo Hà Tĩnh, 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 thông tin cho người dân, doanh nghiệp.

3. Hạ tầng bảo đảm an toàn thông tin mạng

- 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 đến 2025.

- Đầu tư nâng cao 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.

- 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

- 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.

- 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.

- 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.

- 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.

- 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, thành phố, thị xã theo Công văn số 4163/UBND-KGVX1 ngày 13/7/2018 của UBND tỉnh về việc thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

- 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, ngành, huyện, thị xã;

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

5. Triển khai các nội dung xử lý sự cố

- Tổ chức thực hiện xác định cấp độ an toàn các hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh theo Công văn số 4163/UBND-KGVX1 ngày 13/7/2018 của UBND tỉnh về việc thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

- 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 hệ thống giám sát và phòng, chống tấn công mạng trên tại các đơn vị, quản lý tập trung tại cơ quan Chuyên trách an toàn thông tin của tỉnh.

- 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.

- Triển khai các phương pháp bảo vệ sau xử lý sự cố.

6. Đào tạo nguồn nhân lực ATTT

- 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.

- 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.

- 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.

IV. GIẢI PHÁP

1. Chỉ đạo điều hành

- Ban Chỉ đạo CNTT tỉnh, Ban Chỉ đạo CNTT các huyện, thành phố, thị xã tăng cường công tác chỉ đạo bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên địa bàn.

- Tiếp tục hoàn thiện bộ máy quản lý nhà nước về an toàn thông tin mạng từ cấp tỉnh đến cấp xã, trong đó chú trọng nâng cao năng lực, trình độ chuyên môn nghiệp vụ cho đội ngũ cán bộ làm nhiệm vụ quản trị an toàn thông tin, ứng cứu sự cố mạng máy tính; nâng cao vai trò, trách nhiệm của đơn vị chuyên trách ứng cứu sự cố mạng máy tính của tỉnh.

- Đưa an toàn thông tin trở thành tiêu chí đánh giá trong chỉ số cải cách hành chính (phần hiện đại hóa); gắn trách nhiệm của người đứng đầu các cơ quan, đơn vị với việc bảo đảm an toàn thông tin.

2. Giải pháp về tài chính

- Tranh thủ sự hỗ trợ từ các bộ, ngành Trung ương, chương trình quốc gia về CNTT và nguồn vốn ODA; tăng cường huy động các nguồn vốn xã hội hóa và thực hiện việc thuê các dịch vụ CNTT.

- Tăng cường kiểm tra, giám sát đối với các dự án về CNTT, an toàn thông tin nhằm đảm bảo tính hiệu quả của quá trình đầu tư và phát huy tối đa hiệu quả khai thác các nguồn vốn.

- Hàng năm, cân đối, bố trí nguồn ngân sách của tỉnh cho công tác đảm bảo an toàn thông tin mạng theo từng nội dung công việc cụ thể.

3. Giải pháp môi trường chính sách

- Tiếp tục tổ chức thực hiện có hiệu quả Luật An toàn thông tin mạng; 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; Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016-2020; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại.

- Tổ chức thực hiện hiệu quả cơ chế, chính sách hiện hành về ứng dụng và phát triển CNTT trên địa bàn tỉnh, trong đó chú trọng các nội dung về bảo đảm an toàn thông tin. Xây dựng, ban hành một số quy định trong việc quản lý, sử dụng chuyên gia và nhân lực trình độ cao về an toàn thông tin.

- Hoàn thiện các văn bản quy định về thuê dịch vụ CNTT; quy trình thử nghiệm, vận hành thử và nghiệm thu, công nhận đảm bảo an toàn đối với các hệ thống thông tin dùng chung trên địa bàn.

4. Các giải pháp khác

- Đổi mới công tác tuyên truyền, tăng cường tuyên truyền trực tuyến, trực quan, phát huy hiệu quả các cổng/ trang thông tin điện tử, hệ thống truyền thanh cơ sở.

- Đẩy mạnh nghiên cứu khoa học, áp dụng công nghệ mới trong việc bảo đảm an toàn thông tin, ưu tiên các đề tài nghiên cứu khoa học về bảo đảm an toàn thông tin, đặc biệt là bảo đảm an toàn thông tin trong các cơ quan nhà nước.

- Tăng cường hiệu quả hoạt động của Ban Chỉ đạo CNTT các cấp và đội ngũ CIO, cán bộ chuyên trách CNTT, chuyên trách an toàn thông tin trong các cơ quan nhà nước.

- Đổi mới mô hình tổ chức và triển khai hệ thống ứng cứu, xử lý sự cố theo hướng tinh gọn, đồng bộ, hiệu quả và thiết thực.

V. TỔ CHỨC THỰC HIỆN

1. Ban Chỉ đạo CNTT tỉnh

Phối hợp với Ban chỉ đạo CNTT các cơ quan Đảng, tăng cường công tác chỉ đạo, giám sát, kiểm tra về an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan nhà nước, cơ quan Đảng trên địa bàn tỉnh.

2. Sở Thông tin và truyền thông

- Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức triển khai thực hiện Kế hoạch; hướng dẫn, theo dõi, kiểm tra, đôn đốc việc triển khai Kế hoạch này; định kỳ tổng hợp, báo cáo UBND tỉnh, Ban Chỉ đạo CNTT tỉnh.

- Tổ chức đào tạo, bồi dưỡng cập nhật kiến thức, nâng cao năng lực về an toàn thông tin cho đội ngũ CIO, cán bộ chuyên trách CNTT, cán bộ thuộc Đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Hướng dẫn, theo dõi, kiểm tra, đôn đốc việc triển khai các chương trình, dự án ứng dụng CNTT, bảo đảm về an toàn thông tin.

- Chủ trì quản lý, quản trị, vận hành và bảo đảm an toàn thông tin đối với Cổng thông tin điện tử của tỉnh. Chỉ đạo Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của tỉnh thường xuyên theo dõi, giám sát các hệ thống thông

tin của các cơ quan nhà nước trong tỉnh, bảo đảm hỗ trợ, xử lý kịp thời các sự cố phát sinh.

- Phối hợp với các cơ quan liên quan tham mưu cho UBND tỉnh thu hút nguồn lực và các nguồn hỗ trợ từ Trung ương để thực hiện thành công Kế hoạch.

3. Văn phòng UBND tỉnh

- Bảo đảm an toàn thông tin cho các hệ thống dùng chung của tỉnh đang được Văn phòng UBND tỉnh quản lý, vận hành.

- Triển khai ứng dụng chữ ký số chuyên dùng trong các cơ quan nhà nước trên địa bàn tỉnh theo Kế hoạch số 336/KH-UBND ngày 19/8/2014 của UBND tỉnh, đảm bảo thời gian, lộ trình thực hiện.

4. Sở Nội vụ

- Phối hợp với Sở Thông tin và Truyền thông nghiên cứu đưa nội dung về an toàn thông tin vào một tiêu chí thành phần, tại tiêu chí "Ứng dụng công nghệ, thông tin", phần "Hiện đại hóa nền hành chính" trong Bộ chỉ số đánh giá cải cách hành chính tại các sở, ban ngành; UBND cấp huyện và UBND cấp xã trên địa bàn tỉnh Hà Tĩnh; Bộ chỉ số đánh giá cải cách hành chính của các cơ quan Trung ương đóng trên địa bàn.

- Phối hợp với Trường Chính trị Trần phú đưa nội dung đào tạo về CNTT và an toàn thông tin vào một chuyên đề của lớp bồi dưỡng chương trình quản lý nhà nước ngạch chuyên viên chính và chuyên viên; Kế hoạch đào tạo, bồi dưỡng hàng năm cho cán bộ, công chức, viên chức trên toàn tỉnh.

5. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh

- Phối hợp với Sở Thông tin và Truyền thông, tăng cường công tác tuyên truyền, phổ biến pháp luật và xử lý tội phạm trong lĩnh vực CNTT, truyền thông.

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông tổ chức kiểm tra, đánh giá thực trạng an toàn, an ninh thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh; phát hiện, đấu tranh, ngăn chặn mọi âm mưu, thủ đoạn hoạt động sử dụng không gian mạng của các thế lực thù địch, tội phạm mạng nhằm xâm phạm an ninh quốc gia, trật tự an toàn xã hội và gây mất an toàn thông tin mạng. Điều tra, xử lý kịp thời các các vi phạm về an ninh, an toàn thông tin mạng.

- 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 thông tin để có biện pháp phòng ngừa, đấu tranh, ngăn chặn.

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

Ưu tiên bố trí ngân sách cho các chương trình, dự án, hạng mục đầu tư cho công tác đảm bảo an toàn thông tin theo Kế hoạch.

7. Báo Hà Tĩnh, Đài Phát thanh và Truyền hình tỉnh

Thực hiện tuyên truyền, đăng phát và đưa tin về các hoạt động đảm bảo an toàn thông tin nhằm nâng cao nhận thức về an toàn thông tin mạng.

8. Các sở, ban, ngành cấp tỉnh; UBND các huyện, thành phố, thị xã

- Xây dựng, ban hành các quy chế nội bộ về đảm bảo an toàn thông tin tại các đơn vị, địa phương. Tăng cường công tác tuyên truyền nâng cao nhận thức về

an toàn thông tin mạng cho cán bộ, công chức, viên chức, người dân và doanh nghiệp trên địa bàn, thuộc phạm vi quản lý.

- Chủ động thực hiện các biện pháp bảo đảm an toàn thông tin cho các hệ thống thông tin đang triển khai, ứng dụng tại đơn vị mình. Phối hợp kịp thời với Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của tỉnh trong việc giám sát, phòng ngừa và xử lý các sự cố về an toàn thông tin.

- Chủ động bố trí kinh phí tăng cường cơ sở hạ tầng đảm bảo an toàn thông tin, thiết bị tường lửa, phần mềm chống mã độc, rà soát kiểm ra lỗ hỗng bảo mật, an ninh trên các dịch vụ công trực tuyến, cổng/trang thông tin điện tử của các đơn vị, địa phương; tạo điều kiện cho cán bộ tham dự các lớp đào tạo về an toàn thông tin.

9. Các Doanh nghiệp cung cấp dịch vụ viễn thông, internet

Có trách nhiệm phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác bảo đảm an toàn thông tin mạng đối với hạ tầng viễn thông, internet; phối hợp với các đơn vị liên quan kiểm tra, phát hiện các vị phạm an toàn thông tin mạng.

Yêu cầu Thủ trưởng các cơ quan, đơn vị, địa phương 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 về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, xử lý./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- TT Tỉnh ủy, TT HĐND Tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- BCĐ CNTT tỉnh, BCĐ CNTT cơ quan Đảng;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- Chánh, Phó VP UBND tỉnh;
- Cổng TTĐT tỉnh, Trung tâm CB-TH;
- Lưu: VT, KGVX.

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

Đặng Quốc Vinh