

ỦY BAN NHÂN DÂN
TỈNH THANH HÓA
Số: ~~1293~~ /2017/QĐ-UBND

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thanh Hóa, ngày 25 tháng 4 năm 2017

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa

ỦY BAN NHÂN DÂN TỈNH THANH HÓA

Căn cứ Luật tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

Căn cứ Luật công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật cơ yếu ngày 26 tháng 11 năm 2011;

Căn cứ Luật ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ, quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ, quy định chi tiết một số điều và biện pháp thi hành Luật ban hành văn bản quy phạm pháp luật;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ, về đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ, về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Thông tư số 27/2011/TT-BTTTT ngày 01/10/2011 của Bộ Thông tin và Truyền thông, quy định về điều phối các hoạt động ứng cứu sự cố mạng internet Việt Nam;

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11 tháng 8 năm 2011 của Bộ Thông tin và Truyền thông, quy định về quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa.

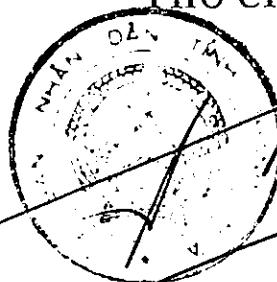
Điều 2. Quyết định này có hiệu lực từ ngày 06 tháng 5 năm 2017.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc các sở, Thủ trưởng các ban, ngành cấp tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố; Giám đốc các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3 (để thực hiện);
- Bộ Thông tin và Truyền thông (để B/cáo);
- Tỉnh ủy, HĐND tỉnh (để B/cáo);
- Chủ tịch, các PCT UBND tỉnh;
- Cục Kiểm tra văn bản-Bộ Tư pháp;
- Công báo;
- Công TTĐT tỉnh;
- Lưu: VT, CNTT(3b).Trung(60).

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



Ngô Văn Tuấn

QUY CHẾ

Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa
(Ban hành kèm theo Quyết định số: 1293 /2017/QĐ-UBND
ngày 25 tháng 4 năm 2017 của Ủy ban nhân dân tỉnh Thanh Hóa)

Chương I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về nội dung đảm bảo an toàn thông tin mạng, bao gồm: Bảo vệ thông tin cá nhân, bảo vệ hệ thống thông tin, giám sát an toàn hệ thống thông tin, ngăn chặn xung đột thông tin trên mạng.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành cấp tỉnh; các đơn vị sự nghiệp công lập trực thuộc UBND tỉnh; UBND các huyện, thị xã, thành phố; UBND các xã, phường, thị trấn trên địa bàn tỉnh (gọi tắt là các cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động (gọi tắt là cán bộ, công chức) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin (CNTT), Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan, đơn vị thuộc khoản 1 Điều này.

4. Khuyến khích các cơ quan, đơn vị khác hoạt động ứng dụng và phát triển CNTT trên địa bàn tỉnh áp dụng quy chế này.

Điều 3. Các nguyên tắc về đảm bảo an toàn thông tin mạng

1. Việc đảm bảo an toàn thông tin mạng phải thực hiện theo đúng quy định tại Điều 4 của Luật an toàn thông tin mạng và hướng dẫn của các cơ quan chuyên môn có thẩm quyền.

2. Các văn bản có nội dung "Mật" trở lên khi gửi, nhận qua mạng phải được thủ trưởng cơ quan, đơn vị cho phép và phải được mã hóa theo quy định của Luật cơ yếu và các văn bản pháp luật liên quan.

3. Việc đảm bảo an toàn thông tin mạng không được làm ảnh hưởng đến các hoạt động bình thường của các cơ quan quản lý nhà nước.

4. Công tác đảm bảo an toàn thông tin mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

Chương II NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 4. Bảo vệ thông tin cá nhân

1. Cán bộ, công chức trong các cơ quan quản lý nhà nước có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại khoản 1, khoản 2 Điều 10; khoản 1, khoản 4 Điều 16; khoản 3 Điều 17; khoản 1 Điều 18 Luật an toàn thông tin mạng và trong các văn bản pháp luật có liên quan.

2. Cán bộ, công chức trong các cơ quan quản lý nhà nước khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của tỉnh phải có trách nhiệm:

a) Tự quản lý và tự chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, mật khẩu, truy cập trái phép vào các phần mềm dùng chung của tỉnh.

b) Ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị, cá nhân được cấp tài khoản phải thực hiện việc đổi mật khẩu.

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

3. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định tại khoản 2, 3, 4, 5 Điều 16; khoản 1, 2 Điều 17; khoản 3 Điều 18; Điều 19 của Luật an toàn thông tin và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi cán bộ, công chức, viên chức đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các thiết bị CNTT liên quan; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

4. Sở Thông tin và Truyền thông thực hiện công tác quản lý nhà nước về bảo vệ thông tin cá nhân trên mạng theo các nội dung quy định tại Điều 20 của Luật an toàn thông tin mạng.

Điều 5. Bảo vệ hệ thống thông tin mạng

1. Đối với các cơ quan, đơn vị:

Thực hiện việc phân loại thông tin, phân loại cấp độ an toàn cho hệ thống thông tin thuộc quyền quản lý theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp, cụ thể:

a) Việc phân loại thông tin được thực hiện theo các quy định tại Điều 9 Luật an toàn thông tin mạng và khoản 1, Điều 6 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

b) Việc quản lý gửi thông tin trên mạng phải tuân thủ theo các nội dung quy định tại Điều 10 Luật an toàn thông tin mạng và các quy định sau:

- Việc trao đổi văn bản, tài liệu điện tử của cơ quan (kể cả tài liệu tham khảo) chỉ thực hiện trên hệ thống phần mềm quản lý văn bản và hồ sơ công việc đã được triển khai hoặc sử dụng hệ thống thư điện tử công vụ của tỉnh hoặc trên các phần mềm ứng dụng của nội bộ ngành chuyên giao ứng dụng.

- Khi phát hành và gửi qua mạng các văn bản của các cơ quan quản lý nhà nước phải được thực hiện ký số trước khi gửi.

c) Việc phân loại cấp độ an toàn cho hệ thống thông tin được thực hiện theo các quy định tại Điều 21 Luật an toàn thông tin mạng; khoản 2 Điều 6; các Điều 7, 8, 9, 10, 11 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

d) Nội dung bảo vệ hệ thống thông tin được thực hiện theo các quy định tại các Điều 22, 23 Luật an toàn thông tin mạng và trong Chương IV Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ. Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật CNTT, các hệ thống thông tin của cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng và phải được Sở Thông tin và Truyền thông thẩm định trước khi trình cấp có thẩm quyền phê duyệt và tuân thủ các quy định sau:

- Phòng đặt thiết bị CNTT (đối với các cơ quan, đơn vị đang quản lý, vận hành các hệ thống thông tin, cơ sở dữ liệu của tỉnh) phải đảm bảo các điều kiện đáp ứng các yêu cầu cơ bản (được bố trí ở khu vực có điều kiện an ninh tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có nguồn điện dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy, quy trình làm việc trong khu vực an toàn bảo mật). Phải thiết lập cơ chế bảo vệ mạng nội bộ, đảm bảo an toàn thông tin khi có kết nối với mạng ngoài bằng các công cụ, thiết bị bảo vệ (tường lửa, hệ thống chống xâm nhập trái phép, hệ thống giám sát, cảnh báo sớm).

- Hệ thống mạng nội bộ (mạng LAN) của các cơ quan, đơn vị được tổ chức theo hướng sử dụng máy chủ để quản lý các máy trạm trong hệ thống mạng, không sử dụng mô hình mạng ngang hàng (không có máy chủ quản lý). Các máy chủ, máy trạm, hệ thống lưu trữ nội bộ, thiết bị mạng, mạng không dây (wifi) phải được bảo vệ bởi mật khẩu an toàn. Tất cả các máy tính tại các cơ quan, đơn vị phải được cài đặt các phần mềm bảo vệ, phòng chống virus.

- Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong các cơ quan, đơn vị phải được bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn; không được kết nối vào mạng LAN của đơn vị. Đặc biệt là không được sử dụng máy tính đã nối mạng Internet đánh máy, in, sao tài liệu mật. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu (password) cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin.

- Khi thực hiện di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, thông tin thuộc danh mục bí mật Nhà nước phải được tổ chức quản lý, giám sát chặt chẽ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

- Khi xây dựng, nâng cấp mở rộng các hệ thống thông tin phải có nội dung, giải pháp kỹ thuật đảm bảo an toàn thông tin cho các hệ thống thông tin; cập nhật kịp thời các bản vá lỗ hổng bảo mật từ nhà cung cấp, nhà sản xuất cho các hệ thống thông tin, cơ sở dữ liệu; có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn để sẵn sàng phục hồi cơ sở dữ liệu khi xảy ra sự cố an toàn thông tin mạng.

- Tổ chức phân quyền truy cập cho các đối tượng người dùng tham gia vận hành, khai thác các hệ thống thông tin đúng quy trình, chặt chẽ gắn với trách nhiệm của từng tổ chức, cá nhân để đảm bảo an toàn thông tin mạng cho các hệ thống thông tin cơ quan, đơn vị đang quản lý, vận hành.

- Các cơ quan, đơn vị, cá nhân tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về đảm bảo an toàn thông tin mạng trên mạng truyền số liệu chuyên dùng được quy định tại các Điều 10, 11, 12 của Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và truyền thông.

2. Đối với các đơn vị, doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, Internet cho cơ quan quản lý nhà nước tỉnh Thanh Hóa:

Thực hiện các nội dung liên quan đến hoạt động bảo đảm an toàn thông tin mạng theo Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Điều 7, Điều 9, Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và Truyền thông và các quy định sau:

a) Thực hiện các quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của các cơ quan, đơn vị. Áp dụng và tổ chức thực hiện các biện pháp ngăn chặn việc gửi thông tin vi phạm quy định của pháp luật khi nhận được thông báo của cơ quan, đơn vị. Cung cấp các điều kiện kỹ thuật và nghiệp vụ cần thiết để thực hiện nhiệm vụ, bảo đảm an toàn thông tin mạng theo yêu cầu của cơ quan nhà nước có thẩm quyền.

b) Phải có hệ thống lọc phần mềm độc hại trong quá trình thực hiện các dịch vụ gửi, nhận, lưu trữ thông tin trên hệ thống của mình; có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền; quản lý, phối hợp ngăn chặn mất an toàn thông tin mạng xuất phát từ tài nguyên Internet, từ khách hàng của mình; phối hợp, kết nối định tuyến để đảm bảo hệ thống máy chủ có tên miền quốc gia Việt Nam hoạt động an toàn, ổn định.

Điều 6. Giám sát an toàn hệ thống thông tin mạng

1. Đối với các cơ quan, đơn vị:

Tổ chức thực hiện việc giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trực tiếp quản lý. Nội dung và đối tượng giám sát thực hiện theo quy định tại các khoản 1, 2 Điều 24 của Luật an toàn thông tin mạng; đồng thời, thực việc lưu trữ nhật ký tình trạng hoạt động của các hệ thống thông tin tại các máy chủ trong thời gian ít nhất là 30 ngày để phục vụ các công tác đảm bảo an toàn thông tin mạng.

2. Đối với các doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, Internet có trách nhiệm thực hiện theo quy định tại khoản 3 Điều 24 của Luật an

toàn thông tin mạng.

Điều 7. Ngăn chặn xung đột thông tin trên mạng

1. Đối với các cơ quan, đơn vị là chủ quản trực tiếp các hệ thống thông tin:

a) Các cơ quan, đơn vị trong phạm vi quyền hạn của mình có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật an toàn thông tin mạng; khoản 1 Điều 8; khoản 1, Điều 9; các khoản 3, 4, 5, Điều 12; các khoản 1, 2, Điều 14 và Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ và các quy định sau:

- Phải thực hiện các biện pháp bảo vệ hệ thống thông tin của mình quản lý, không để các phần tử xấu lợi dụng hệ thống thông tin để thâm nhập, truy cập trái phép vào các Trung tâm đang quản lý các hệ thống thông tin, cơ sở dữ liệu của tỉnh.

- Quản lý chặt chẽ các tài khoản đã cung cấp cho người dùng trong cơ quan, đơn vị.

b) Cán bộ, công chức của các cơ quan, đơn vị có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật an toàn thông tin mạng; khoản 1 Điều 7; các khoản 4, 5 Điều 12 và Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ.

2. Sở Thông tin và Truyền thông.

Chủ trì, phối hợp với các đơn vị liên quan của Bộ Thông tin và Truyền thông và các cơ quan nghiệp vụ, các ngành, đơn vị liên quan để tham mưu và tổ chức thực hiện các giải pháp ngăn chặn xung đột thông tin trên mạng theo các nội dung được quy định tại các khoản 2, 3 Điều 6; các khoản 2, 3 Điều 9; khoản 3 Điều 14; các khoản 1, 3 Điều 15 và các Điều 16, 17, 18 của Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ và các quy định sau:

a) Chủ trì, phối hợp với các đơn vị liên quan thực hiện ngăn chặn xung đột thông tin trên mạng bao gồm giám sát, phát hiện, cảnh báo, xác định nguồn gốc và khắc phục xung đột thông tin trên mạng.

b) Chủ trì, phối hợp với các cơ quan nghiệp vụ tổ chức triển khai các phương án bảo vệ các hệ thống thông tin trong phạm vi quản lý; sẵn sàng huy động lực lượng, phương tiện tham gia hoạt động ngăn chặn xung đột thông tin trên mạng, thuộc phạm vi quản lý theo quy định của pháp luật.

c) Phối hợp với các cơ quan nghiệp vụ triển khai và đôn đốc thực hiện các kế hoạch, biện pháp ngăn chặn xung đột thông tin trên mạng; xử lý, khắc phục các vụ việc liên quan đến xung đột thông tin trên mạng thuộc phạm vi quản lý theo quy định của pháp luật.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet cho các cơ quan quản lý nhà nước tỉnh Thanh Hóa trong phạm vi quyền hạn của mình có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1, Điều 28; khoản 1, Điều 29 Luật an toàn thông tin mạng và các quy định tại khoản 5 Điều 12; Điều 28 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 8. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức quán triệt, nâng cao nhận thức cho cán bộ, công chức về đảm bảo an toàn thông tin mạng; tổ chức triển khai thực hiện Quy chế này và các văn bản pháp luật liên quan đến công tác đảm bảo an toàn thông tin mạng; có trách nhiệm tổ chức, quản lý các hệ thống thông tin, cơ sở dữ liệu quan trọng của cơ quan, đơn vị mình; chịu trách nhiệm trước UBND tỉnh và trước pháp luật trong công tác đảm bảo an toàn thông tin mạng của cơ quan, đơn vị thuộc phạm vi quản lý.

2. Xây dựng và ban hành quy chế, quy định về đảm bảo an toàn thông tin mạng; phương án thực hiện bảo vệ hệ thống thông tin do cơ quan, đơn vị quản lý theo hướng dẫn của Sở Thông tin và Truyền thông.

Cơ quan, đơn vị được giao quản lý, vận hành các hệ thống thông tin, cơ sở dữ liệu của tỉnh xây dựng các quy định, phương án phù hợp để đảm bảo an toàn thông tin mạng trong quá trình quản lý, vận hành và sử dụng các dịch vụ.

3. Tổ chức triển khai thực hiện các hoạt động đảm bảo an toàn thông tin mạng trong cơ quan, đơn vị mình theo các nội dung đảm bảo an toàn thông tin mạng đã nêu trong Chương II của quy chế này. Phối hợp với Sở thông tin và Truyền thông và các đơn vị có liên quan trong việc triển khai các giải pháp, biện pháp đảm bảo an ninh, an toàn thông tin mạng trong cơ quan, đơn vị.

4. Bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị CNTT để tăng cường năng lực đảm bảo an toàn thông tin mạng của cơ quan, đơn vị theo quy định của nhà nước.

5. Xây dựng và tổ chức tập huấn, bồi dưỡng kiến thức về an toàn thông tin mạng cho cán bộ, công chức, viên chức trong cơ quan, đơn vị. Tạo điều kiện cho cán bộ chuyên trách về CNTT có môi trường làm việc phù hợp để thực hiện nhiệm vụ đảm bảo an toàn thông tin mạng của cơ quan, đơn vị và được tham dự đầy đủ các khóa đào tạo, bồi dưỡng, diễn tập nâng cao kiến thức, nghiệp vụ về an toàn thông tin mạng.

6. Phối hợp với các cơ quan chức năng và tạo điều kiện thuận lợi trong hoạt động kiểm tra về công tác an toàn thông tin mạng tại cơ quan, đơn vị.

7. Chủ tịch UBND cấp huyện có trách nhiệm chỉ đạo UBND cấp xã thuộc phạm vi quản lý tổ chức triển khai thực hiện quy chế này.

8. Định kỳ trước ngày 15/10 hàng năm, báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị; gửi về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND tỉnh.

Điều 9. Trách nhiệm của Sở Thông tin và Truyền thông

1. Chủ trì tham mưu cho UBND tỉnh, Chủ tịch UBND tỉnh ban hành các văn bản chỉ đạo, các chương trình, kế hoạch để tổ chức thực hiện tốt nhiệm vụ đảm bảo an toàn thông tin mạng trong các cơ quan, đơn vị trên địa bàn tỉnh. Chịu trách nhiệm trước UBND tỉnh về công tác đảm bảo an toàn thông tin mạng

trong hoạt động của các cơ quan, đơn vị trên địa bàn tỉnh.

2. Thực hiện vai trò, nhiệm vụ của cơ quan chuyên trách, giúp UBND tỉnh thực hiện quản lý nhà nước về đảm bảo an toàn thông tin mạng trên địa bàn tỉnh:

a) Ban hành đầy đủ và kịp thời các văn bản hướng dẫn cho các cơ quan, đơn vị về đảm bảo an toàn thông tin mạng theo các nội dung chỉ đạo của Bộ Thông tin và Truyền thông và của UBND tỉnh. Hướng dẫn các cơ quan, đơn vị xây dựng quy chế, quy định về đảm bảo an toàn thông tin mạng, phương án thực hiện bảo vệ hệ thống thông tin.

b) Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn thông tin mạng; tiếp nhận thông tin, hỗ trợ kỹ thuật và tham gia xử lý các sự cố về an toàn thông tin mạng cho các cơ quan, đơn vị. Tổ chức thực hiện các hoạt động điều phối, ứng cứu sự cố máy tính trên địa bàn tỉnh và các nhiệm vụ được quy định tại khoản 2 Điều 7 của Quy chế này.

c) Hàng năm, lập kế hoạch và tổ chức đào tạo, tập huấn, bồi dưỡng kiến thức về an toàn thông tin mạng cho cán bộ chuyên trách về CNTT của các cơ quan, đơn vị.

d) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan thành lập đoàn kiểm tra liên ngành và tổ chức kiểm tra, giám sát việc thực hiện đảm bảo an toàn thông tin mạng tại các cơ quan, đơn vị của tỉnh, tại các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet trên địa bàn tỉnh để kịp thời phát hiện, xử lý các hành vi vi phạm an toàn thông tin mạng.

đ) Hàng năm, xây dựng kế hoạch và tổ chức các hội nghị, hội thảo chuyên đề về an toàn thông tin mạng để tiếp tục nâng cao nhận thức về an toàn thông tin mạng cho các cơ quan, đơn vị, doanh nghiệp và người dân trên địa bàn tỉnh.

e) Tổng hợp báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, UBND tỉnh và thông báo các cơ quan, đơn vị có liên quan.

3. Phối hợp, hợp tác với Cục An toàn thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các tổ chức, đơn vị liên quan trong các hoạt động liên quan đến công tác đảm bảo an toàn thông tin mạng.

Điều 10. Trách nhiệm của Công an tỉnh

1. Chủ động triển khai các biện pháp, công tác nghiệp vụ phòng ngừa, phát hiện, đấu tranh ngăn chặn hoạt động xâm hại đến an toàn thông tin mạng trong các cơ quan, đơn vị.

2. Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan thanh tra, kiểm tra, xử lý vi phạm về an toàn thông tin mạng trên địa bàn tỉnh.

Điều 11. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và Internet cho các cơ quan quản lý nhà nước tỉnh Thanh Hóa

1. Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về an ninh mạng và an toàn thông tin và các nội dung quy định tại Quy chế này.

2. Phối hợp với Sở Thông tin và Truyền thông để tham gia các hoạt động

điều phối, ứng cứu, khắc phục sự cố thông tin đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác dịch vụ.

Điều 12. Trách nhiệm của cán bộ, công chức tại các cơ quan, đơn vị

1. Cán bộ chuyên trách CNTT hoặc cán bộ được cơ quan, đơn vị giao phụ trách CNTT:

a) Tham mưu cho lãnh đạo cơ quan, đơn vị xây dựng quy chế, quy định về đảm bảo an toàn thông tin mạng cho hệ thống thông tin của cơ quan, đơn vị. Tham mưu xây dựng kế hoạch và tổ chức thực hiện các biện pháp đảm bảo an toàn thông tin mạng để quản lý vận hành các hệ thống thông tin.

b) Chủ động phối hợp và tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn thông tin mạng.

c) Tham gia đầy đủ các khóa đào tạo về đảm bảo an toàn thông tin mạng do các cơ quan chuyên môn tổ chức.

2. Trách nhiệm của cán bộ, công chức tham gia sử dụng và khai thác thông tin mạng:

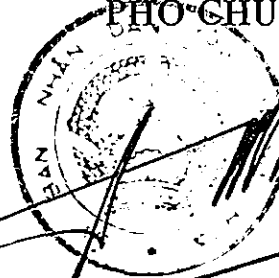
a) Thực hiện các nội dung đã được quy định tại quy chế này; các quy chế, nội quy của cơ quan, đơn vị và các quy định khác của pháp luật về an toàn thông tin mạng trong quá trình sử dụng, khai thác thông tin mạng.

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho lãnh đạo đơn vị để có giải pháp ngăn chặn, xử lý kịp thời.

Điều 13. Điều khoản thi hành

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh; các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét sửa đổi, bổ sung cho phù hợp./.

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



Ngô Văn Tuấn