ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 01 /2021/QĐ-UBND	*Hà Tĩnh, ngày 19 tháng 01 năm 2021*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh

ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

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

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

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

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

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

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

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về việc 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;

Căn cứ Thông tư số 12/2019/TT-BTTTT ngày 05 tháng 11 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông về sửa đổi, bổ sung một số điều của Thông tư

số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, 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 tại Văn bản số 38/TTr-STTTT ngày 06 tháng 11 năm 2020, ý kiến thẩm định của Sở Tư pháp tại Văn bản số 494/BC-STP ngày 29 tháng 10 năm 2020.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh.

Điều 2. Quyết định này thay thế Quyết định số 2859/QĐ-UBND ngày 16/9/2013 của Ủy ban nhân dân tỉnh về ban hành Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác các hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh và có hiệu lực thi hành kể từ ngày 01 tháng 02 năm 2021.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Thông tin và Truyền thông, Giám đốc (Thủ trưởng) các sở, ban, ngành cấp tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thành phố, thị xã; Chủ tịch UBND các xã, phường, thị trấn và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- Như Điều 3;
- UBQG về CPĐT;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL-Bộ Tư pháp;
- TTr: Tỉnh ủy, HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- Cổng TTĐT tỉnh;
- Chánh VP, các PVP;
- Trung tâm TT-CB-TH;
- Lưu: VT, VX_1.

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

Lê Ngọc Châu

ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh

(Ban hành kèm theo Quyết định số 01 /2021/QĐ-UBND ngày 19/01/2021 của Ủy ban nhân dân tỉnh Hà Tĩnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh:

Quy chế này quy định về công tác bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh.

2. Đối tượng áp dụng:

Quy chế này áp dụng đối với các sở, ban, ngành, đơn vị thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân các huyện, thành phố, thị xã; các cơ quan Trung ương trên địa bàn tỉnh; Ủy ban nhân dân các xã, phường, thị trấn và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Hà Tĩnh (sau đây gọi tắt là cơ quan, đơn vị); cán bộ, công chức, viên chức, người lao động đang làm việc trong các cơ quan, đơn vị nêu trên.

Điều 2. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị phải tuân thủ theo nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng số 86/2015/QH15 ngày 19/11/2015 (sau đây gọi tắt là Luật An toàn thông tin mạng) và các các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin mạng.

2. Các cơ quan, đơn vị và cán bộ, công chức chịu trách nhiệm trước pháp luật về nội dung thông tin đã chuyển đi trên mạng nội bộ (LAN), mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước và mạng Internet.

3. Kết hợp nhiều biện pháp bảo đảm an toàn thông tin số, nhằm phát hiện và ngăn chặn kịp thời các nguy cơ mất an toàn thông tin.

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.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. An toàn thông tin mạng được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin mạng.

2. Hệ thống thông tin được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng.

3. Xâm phạm an toàn thông tin mạng được quy định tại Khoản 6 Điều 3 Luật An toàn thông tin mạng.

4. Nguy cơ mất an toàn thông tin mạng là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

5. Phần mềm độc hại được quy định tại Khoản 11 Điều 3 Luật An toàn thông tin mạng.

6. Bản ghi nhật ký hệ thống (Logfile) là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

7. Đội ứng cứu, cơ quan Thường trực đội ứng cứu: Là Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh, cơ quan Thường trực đội ứng cứu an toàn thông tin mạng tỉnh Hà Tĩnh do Uỷ ban nhân dân tỉnh quyết định thành lập.

Chương II

NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 4. Bảo vệ thông tin cá nhân

1. Cán bộ, công chức, viên chức, người lao động trong các cơ quan, đơn vị 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 các văn bản pháp luật có liên quan.

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, có trách nhiệm:

a) Tự quản lý và 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, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị; phải thay đổi mật khẩu tài khoản định kỳ hàng tháng/quý.

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.

2. 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, Khoản 3, Khoản 4, Khoản 5 Điều 16; Khoản 1, Khoản 2 Điều 17; Khoản 3 Điều 18; Điều 19 của Luật an toàn thông tin mạng 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 công nghệ thông tin 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.

3. 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. Quy định bảo vệ hệ thống thông tin

1. Đối với các cơ quan, đơn vị:

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin;

b) Phân công cán bộ, công chức chuyên trách hoặc phụ trách công nghệ thông tin, để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại đơn vị;

c) Thủ trưởng cơ quan, đơn vị tạo điều kiện để cán bộ, công chức chuyên trách hoặc phụ trách công nghệ thông tin học tập, tiếp thu công nghệ, kiến thức an toàn thông tin;

d) Hàng năm, xác định các nhiệm vụ bảo đảm an toàn thông tin hệ thống (mở rộng, nâng cấp trang thiết bị; đào tạo, bồi dưỡng kiến thức công nghệ thông tin, ...), để đề xuất kinh phí đến cơ quan có thẩm quyền hoặc phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả;

đ) Khi xây dựng, nâng cấp, mở rộng hệ thống thông tin, các cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng và phải được Sở Thông tin và Truyền thông có ý kiến trước khi trình cấp có thẩm quyền phê duyệt. Đồng thời cần thực hiện các nội dung sau:

- Phòng đặt thiết bị công nghệ thông tin (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 đảm bảo; 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 phải được cài đặt hệ thống tường lửa (Firewall) để bảo vệ hệ thống mạng LAN. 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 vi-rút.

- Các thiết bị công nghệ thông tin dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong các cơ quan, đơn vị không được phép kết nối mạng internet, phải được kiểm định và bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn. 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 công nghệ thông tin 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.

- 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.

- Ưu tiên việc đảm bảo an toàn thông tin khi thực hiện thuê dịch vụ công nghệ thông tin.

- 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 11, 13 của Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước (sau đây gọi tắt là Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông) và Khoản 5 Điều 1 của Thông tư số 12/2019/TTBTTTT ngày 05/11/2019 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

e) Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, hủy các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin; triển khai các công cụ để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin;

g) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;

h) Thiết lập hệ thống thông tin ghi nhận và lưu vết các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống... Ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký, thời gian lưu trữ các bản ghi nhật ký hệ thống tối thiểu 01 năm;

i) Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập cấu hình lại hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin; kiểm soát quá trình cài đặt trên máy chủ;

k) Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Thủ trưởng đơn vị;

l) Định kỳ hàng tuần sao lưu (backup) thông tin (không lưu đè thông tin, sao lưu dự phòng các thông tin thay đổi), dữ liệu của đơn vị và lưu trữ thông tin sao lưu ở nơi an toàn theo quy định; thường xuyên kiểm tra thông tin, dữ liệu sao lưu để đảm bảo tính sẵn sàng và toàn vẹn;

m) Sử dụng mật khẩu: Đặt cho tài khoản sử dụng ở dạng phức tạp (mật khẩu bao gồm chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt), độ dài tối thiểu 8 ký tự. Không tiết lộ, chia sẻ mật khẩu cho người khác, khi kết thúc công việc hoặc chuyển giao máy tính cho người khác sử dụng phải thoát khỏi tài khoản người dùng.

2. Đối với các đơn vị, doanh nghiệp cung cấp các dịch vụ viễn thông, công nghệ thông tin, Internet cho cơ quan quản lý nhà nước trên địa bàn tỉnh:

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 về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ); Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng 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.

3. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại:

a) Tất cả các máy trạm, máy chủ, các thiết bị công nghệ thông tin trong mạng và hệ thống thông tin phải được cài đặt phần mềm phòng chống vi-rút phù hợp. Các phần mềm phòng chống vi-rút phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc, vi-rút khi sao chép, mở các tập tin.

b) Các cán bộ, công chức, viên chức, người lao động trong cơ quan, đơn vị phải được hướng dẫn về phòng chống phần mềm độc hại, các rủi ro do mã độc gây

ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

c) Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi các tập tin trên các thiết bị lưu trữ di động.

d) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại, vi-rút trên máy chủ, máy trạm, thiết bị công nghệ thông tin như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống vi-rút, mất dữ liệu, những dấu hiệu bất thường khác,… người sử dụng phải giữ nguyên hiện trạng máy tính và thông báo cho cán bộ hoặc bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

đ) Phòng ngừa hư hỏng, sự cố máy tính, hệ thống thông tin qua các sự cố bất khả kháng: Hư hỏng thiết bị đột ngột, chập điện, cháy nổ, lũ lụt, sét đánh, khủng bố, trộm cắp,...

Điều 6. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ thực hiện theo quy định tại Điều 4, Điều 5 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

2. Đơn vị chuyên trách về an toàn thông tin:

a) Sở Thông tin và Truyền thông là đơn vị chuyên trách về an toàn thông tin mạng của tỉnh.

b) Đơn vị chuyên trách về công nghệ thông tin tại các cơ quan, đơn vị đồng thời là đơn vị chuyên trách về an toàn thông tin của các cơ quan, đơn vị. Trong trường hợp chưa có đơn vị chuyên trách về công nghệ thông tin thì giao cho bộ phận có chuyên môn về công nghệ thông tin, trong đó cán bộ chuyên trách công nghệ thông tin chịu trách nhiệm chính.

3. Thẩm quyền xác định cấp độ an toàn hệ thống thông tin:

a) Đơn vị lập hồ sơ đề xuất cấp độ:

- Đối với các hệ thống thông tin thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ;

- Đối với các hệ thống thông tin thuê dịch vụ, đơn vị chủ trì thuê dịch vụ lập hồ sơ đề xuất cấp độ;

- Đối với các hệ thống thông tin đang trong giai đoạn triển khai, đơn vị chủ trì triển khai lập hồ sơ đề xuất cấp độ;

- Đối với các hệ thống thông tin đang vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

b) Thẩm quyền thẩm định và phê duyệt cấp độ theo quy định tại Điều 12 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

4. Trình tự, thủ tục xác định cấp độ hệ thống thông tin:

a) Việc xác định, phân loại hệ thống thông tin theo quy định tại Điều 4 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ (sau đây gọi tắt là Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông).

b) Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

d) Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

e) Trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 13, Điều 14 Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Điều 14, Điều 15, Điều 16 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

5. Phương án bảo đảm an toàn hệ thống thông tin:

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác.

b) Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Đơn vị/bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

Điều 7. 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. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định hoạt động giám sát an toàn hệ thống thông tin; thực hiện 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, công nghệ thông tin, Internet có trách nhiệm thực hiện theo quy định tại Khoản 3 Điều 24 của Luật An toàn thông tin mạng.

Điều 8. Xây dựng nội quy bảo đảm an toàn thông tin nội bộ

Trên cơ sở quy chế này và văn bản liên quan, các cơ quan, đơn vị ban hành nội quy đảm bảo an toàn thông tin nội bộ tại cơ quan, đơn vị mình trong đó quy định rõ các vấn đề cơ bản sau:

1. Phân công cụ thể cán bộ, công chức chuyên trách công nghệ thông tin, số điện thoại liên hệ khi có sự cố về an toàn thông tin.

2. Phân công cán bộ, công chức chịu trách nhiệm quản lý máy tính để dự thảo các văn bản, tài liệu có tính mật; việc sử dụng và vận hành máy tính này, đảm bảo tuân thủ các quy định của pháp luật về bảo mật và an toàn thông tin.

3. Thiết lập quy tắc vào ra, quản lý phòng máy chủ; quy tắc cài đặt phần mềm lên máy chủ, máy tính trạm.

4. Quy tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị…).

5. Kiểm tra, rà soát và khắc phục sự cố an toàn của hệ thống thông tin sử dụng các biện pháp trong Điều 4, Điều 5 của Quy chế này.

6. Quy tắc quản lý bảo đảm an toàn hệ thống thông tin tại đơn vị; đảm bảo tính toàn vẹn, tính tin cậy, tính thống nhất và tính sẵn sàng của dữ liệu trong quản lý và vận hành trao đổi thông tin.

7. Quy trình xử lý các sự cố ảnh hưởng đến an toàn hệ thống tại đơn vị.

8. Chế độ báo cáo tổng hợp tình hình an toàn của hệ thống thông tin.

Điều 9. Ngăn chặn xung đột thông tin trên mạng

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

a) Quản lý chặt chẽ các tài khoản đã cung cấp cho người dùng và hệ thống thông tin do 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.

b) Thực hiện các nội dung ngăn chặn xung đột thông tin trên mạng trong phạm vi và thẩm quyền theo quy định.

2. Sở Thông tin và Truyền thông:

a) Chủ trì, phối hợp với các đơn vị liên quan của Bộ Thông tin và Truyền thông, các cơ quan, đơn vị có liên quan để tham mưu xây dựng và triển khai các kế hoạch, phương án bảo vệ hệ thống thông tin; sẵn sàng huy động lực lượng, phương tiện tham gia thực hiện các nội dung ngăn chặn xung đột thông tin trên mạng trong phạm vi quản lý.

b) Xử lý, khắc phục các vụ việc liên quan đến xung đột thông tin trên mạng thuộc phạm vi quản lý theo quy định pháp luật.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin, Internet cho các cơ quan nhà nước tỉnh có trách nhiệm ngăn chặn xung đột thông tin trên mạng trong phạm vi thẩm quyền theo quy định pháp luật.

Điều 10. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm an toàn thông tin mạng trên địa bàn tỉnh

1. Quy trình xử lý khẩn cấp:

Khi phát hiện hệ thống có nguy cơ mất an toàn thông tin như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung Cổng/Trang thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan,… thực hiện các bước cơ bản:

a) Bước 1: Ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị;

b) Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

c) Bước 3: Khôi phục lại hệ thống, hoặc sử dụng hệ thống dự phòng và chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động;

d) Bước 4: Tổng hợp, báo cáo sự cố và nội dung khắc phục gửi về Đội ứng cứu để tổng hợp.

2. Trách nhiệm phối hợp trong ứng cứu sự cố:

a) Đơn vị vận hành hệ thống thông tin:

- Thực hiện các bước khắc phục sự cố theo Khoản 1 điều này.

- Các sự cố vượt quá khả năng xử lý, đơn vị thông báo đến Đội ứng cứu để hỗ trợ khắc phục và thực hiện báo cáo sự cố mạng theo mẫu số 03 ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

- Tổng hợp, báo cáo Đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng (Sở Thông tin và Truyền thông) theo định kỳ 06 tháng một lần và báo cáo đột xuất khi có yêu cầu.

b) Đội ứng cứu:

- Tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin của đơn vị.

- Phản hồi cho đơn vị, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Thẩm tra, xác minh và phân loại sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh hướng giải quyết trong trường hợp vượt thẩm quyền.

- Chủ động hỗ trợ ngay đơn vị cần ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình, cử cán bộ kỹ thuật của Đội có mặt tại đơn vị báo sự cố để

phối hợp, hướng dẫn, ghi nhận giải quyết sự cố, trong trường hợp sự cố phức tạp, nguy cơ cao về an toàn thông tin mà không thể hướng dẫn, trao đổi qua điện thoại, email với đơn vị bị sự cố.

- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Ban chỉ đạo xây dựng Chính quyền điện tử tỉnh; đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm hoặc vượt khả năng xử lý của mình.

- Tổng hợp, báo cáo Cơ quan điều phối quốc gia theo quy định và báo cáo đột xuất khi có yêu cầu.

c) Sở Thông tin và Truyền thông báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông thông qua Cục An toàn thông tin, để được hỗ trợ khắc phục các sự cố vượt quá khả năng xử lý của địa phương.

Điều 11. Mua sắm, trang bị máy tính, thiết bị công nghệ thông tin có liên quan đến an toàn thông tin mạng

Trong quá trình mua sắm trang thiết bị cho hệ thống, các cơ quan, đơn vị cần tuân thủ quy định tại Thông tư số 47/2016/TT-BTTTT ngày 26/12/2016 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết về ưu tiên đầu tư mua sắm sản phẩm, dịch vụ công nghệ thông tin sản xuất trong nước sử dụng nguồn vốn ngân sách nhà nước và các quy định khác về bảo đảm an toàn thông tin mạng.

Điều 12. Mạng truyền số liệu chuyên dùng

1. Các cơ quan, đơn vị sử dụng mạng truyền số liệu chuyên dùng trong việc trao đổi thông tin, truy cập internet, liên thông văn bản trên phần mềm quản lý văn bản và điều hành tác nghiệp và thực hiện các quy định của Quyết định số 58/2019/QĐ-UBND ngày 25/11/2019 của Ủy ban nhân dân tỉnh ban hành Quy chế quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng cấp II trên địa bàn tỉnh Hà Tĩnh nhằm đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị.

2. Đối với các cơ quan, đơn vị đã được kết nối sử dụng mạng truyền số liệu chuyên dùng nhưng vẫn kết nối sử dụng thêm đường truyền công cộng để truy cập internet khi xảy ra sự cố mất an toàn thông tin liên quan đến sử dụng mạng internet công cộng thì thủ trưởng cơ quan đó chịu trách nhiệm đến sự cố mất an toàn thông tin tại cơ quan, đơn vị.

3. Các cơ quan, đơn vị sử dụng mạng truyền số liệu chuyên dùng thông báo sự cố đường truyền về Sở Thông tin và Truyền thông để được hỗ trợ khắc phục kịp thời.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh

1. Đảm nhiệm chức năng Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của tỉnh.

2. Thực hiện trách nhiệm, quyền hạn được quy định tại Khoản 2 Điều 5 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban

hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

3. Chỉ đạo, tổ chức thực hiện, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh.

Điều 14. Trách nhiệm của các cơ quan, đơn vị

1. Cơ quan nhà nước có bị sự cố về an toàn thông tin, thực hiện theo nội dung quy định tại Khoản 1 Điều 42 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ.

2. Báo cáo định kỳ hàng năm hoặc đột xuất theo yêu cầu về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

3. Tuân thủ và bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin, đảm bảo an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo hướng dẫn của Sở Thông tin và Truyền thông theo quy định của Quy chế này và các quy định khác của pháp luật có liên quan.

4. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm và quyền hạn của từng cơ quan.

5. Xác định và trình cấp có thẩm quyền phê duyệt cấp độ hệ thống thông tin của cơ quan, đơn vị.

6. Khi được kiểm tra công tác đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị cử cán bộ có chuyên môn về công nghệ thông tin tham gia đoàn kiểm tra.

Điều 15. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác đảm bảo an toàn thông tin mạng trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo an toàn cho các hệ thống thông tin cấp tỉnh.

2. Xây dựng và triển khai các kế hoạch, chương trình, dự án đầu tư, đào tạo về an toàn thông tin trong ứng dụng công nghệ thông tin trên địa bàn tỉnh.

3. Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn tỉnh; cảnh báo các vấn đề về an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh.

4. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước trên địa bàn tỉnh; xử lý các vấn đề liên quan sự cố mạng truyền số liệu chuyên dùng.

5. Hướng dẫn, hỗ trợ sao lưu dự phòng các thông tin, cơ sở dữ liệu của các cơ quan nhà nước đảm bảo an toàn.

6. Hướng dẫn, giám sát các đơn vị xây dựng quy chế và thực hiện việc đảm bảo an toàn cho hệ thống thông tin theo quy định; hướng dẫn các cơ quan về khung báo cáo; định kỳ tổng hợp báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông về công tác an toàn thông tin mạngtrên địa bàn tỉnh.

7. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền trên các phương tiện truyền thông đại chúng về công tác bảo đảm an toàn thông tin.

8. Hàng năm, tổ chức đào tạo chuyên sâu về an toàn thông tin mạng cho cán bộ, công chức chuyên trách công nghệ thông tin, đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị.

9. Tham mưu xây dựng kế hoạch hàng năm, chủ trì, phối hợp với Công an tỉnh và các đơn vị có liên quan tổ chức kiểm tra định kỳ đảm bảo an toàn thông tin mạng, hệ thống thông tin theo cấp độ của các cơ quan, đơn vị.

Điều 16. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an toàn thông tin mạng trong cơ quan nhà nước.

2. Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan tổ chức kiểm tra về an toàn thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo quy định của pháp luật.

3. Cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị; điều tra và xử lý các trường hợp vi phạm các quy định về an toàn thông tin mạng theo thẩm quyền.

4. Kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin theo đúng quy định của pháp luật.

5. Thực hiện quản lý công tác an toàn hệ thống thông tin thuộc Công an tỉnh.

Điều 17. Trách nhiệm của Bộ Chỉ huy quân sự tỉnh

1. Tham mưu với Ủy ban nhân dân tỉnh; phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các thế lực thù địch trong và ngoài nước lợi dung không gian mạng, hệ thống thông tin xâm phạm độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ theo chức năng, nhiệm vụ được giao.

2. Chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan tổ chức kiểm tra về an toàn thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm pháp luật về an toàn thông tin trong lĩnh vực quân sự quốc phòng.

Điều 18. Trách nhiệm của Sở Tài chính

Hàng năm, căn cứ khả năng cân đối ngân sách và chế độ, tiêu chuẩn, định mức do Nhà nước ban hành, phối hợp với các đơn vị liên quan tham mưu Ủy ban nhân dân tỉnh bố trí kinh phí triển khai thực hiện nhiệm vụ về bảo đảm an toàn thông tin mạng.

Điều 19. Trách nhiệm của Sở Kế hoạch và Đầu tư

Chủ trì, phối hợp các đơn vị liên quan tham mưu Ủy ban nhân dân tỉnh trình Hội đồng nhân dân tỉnh thông qua việc phân bổ kế hoạch vốn trung hạn theo giai đoạn và hằng năm thực hiện các dự án về bảo đảm an toàn thông tin.

Điều 20. Trách nhiệm Đội ứng cứu

1. Tham mưu các văn bản hướng dẫn, cảnh báo nguy cơ mất an toàn thông tin cho các cơ quan, đơn vị.

2. Phối hợp với Cục An toàn thông tin và các đơn vị có liên quan trong thực hiện nhiệm vụ đảm bảo an toàn thông tin mạng.

3. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

4. Tổ chức thực hiện các biện pháp bảo đảm an toàn thông tin trên mạng máy tính của các cơ quan nhà nước trên địa bàn tỉnh; hỗ trợ kỹ thuật cho các đơn vị trong việc ngăn chặn, phòng ngừa và khắc phục sự cố liên quan đến an toàn thông tin trên mạng máy tính.

5. Cơ quan Thường trực Đội ứng cứu chịu trách nhiệm vận hành Trung tâm giám sát, điều hành an toàn, an ninh mạng của tỉnh.

Điều 21. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin và Internet cho các cơ quan nhà nước trên địa bàn tỉnh

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 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 sử dụng dịch vụ.

3. Thực hiện các quy định về bảo đảm an toàn thông tin mạng tại Luật An toàn thông tin mạng và các văn bản liên quan.

Điều 22. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay đến cán bộ, công chức chuyên trách công nghệ thông tin của đơn vị.

3. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và an toàn thông tin.

4. Cán bộ, công chức chuyên trách công nghệ thông tin:

a) Theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin tại cơ quan, đơn vị;

b) Hướng dẫn, hỗ trợ người dùng tại cơ quan, đơn vị giải pháp phòng, chống vi rút máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro;

c) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an toàn thông tin; tham gia khắc phục các sự cố mất an toàn thông tin.

Điều 23. Trách nhiệm của tổ chức, cá nhân bên ngoài khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan Nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng công nghệ thông tin trên địa bàn tỉnh chịu sự thanh tra, kiểm tra của các cơ quan Nhà nước có thẩm quyền về lĩnh vực an toàn thông tin mạng.

Điều 24. Điều khoản thi hành

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố, thị xã và các tổ chức, cá nhân có liên quan triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung; các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông tổng hợp, trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

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

Lê Ngọc Châu