ỦY BAN NHÂN DÂN TỈNH QUẢNG BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 13 /2020/QĐ-UBND	*Quảng Bình, ngày 14 tháng 7 năm 2020*

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 tỉnh Quảng Bình

ỦY BAN NHÂN DÂN TỈNH QUẢNG BÌNH

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 An ninh mạng ngày 12 tháng 6 năm 2018;

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 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và 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 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 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 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 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 Tờ trình số 588/TTr-STTTT ngày29 tháng 6 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 tỉnh Quảng Bình.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 24 tháng 7 năm 2020, thay thế Quyết định số 26/2014/QĐ-UBND ngày 21 tháng 10 năm 2014 của Ủy ban nhân dân tỉnh Quảng Bình ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Bình.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành cấp tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố; Chủ tịch Ủy ban nhân dân các xã, phường, thị trấn; Thủ trưởng các cơ quan, đơn vị có tham gia hoạt động tư vấn, cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin và khai thác, sử dụng, kết nối, chia sẻ dữ liệu với các hệ thống thông tin của các cơ quan nhà nước tỉnh Quảng Bình và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL - Bộ Tư pháp;
- Vụ Pháp chế - Bộ Thông tin và Truyền thông;
- TT. Tỉnh ủy;
- TT. HĐND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- UBMTTQVN tỉnh và các tổ chức thành viên;
- CT, PCT UBND tỉnh;
- BCĐ xây dựng CQĐT tỉnh;
- Sở Tư pháp;
- Báo Quảng Bình, Đài PT&TH Quảng Bình;
- VP UBND tỉnh: LĐVP, các phòng, ban, TT;
- Trung tâm Tin học - Công báo tỉnh;
- Lưu: VT, KSTTHC, KGVX.

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

Nguyễn Tiến Hoàng

ỦY BAN NHÂN DÂN TỈNH QUẢNG BÌNH	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 tỉnh Quảng Bình

(Ban hành kèm theo Quyết định số 13 /2020/QĐ-UBND ngày 14 tháng 7 năm 2020 của Ủy ban nhân dân tỉnh Quảng Bình)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Quảng Bình.

Điều 2. Đối tượng áp dụng

1. Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh.

2. Cơ quan chuyên môn, đơn vị trực thuộc Ủy ban nhân dân tỉnh và đơn vị thuộc, trực thuộc; Ủy ban nhân dân huyện, thị xã, thành phố và cơ quan chuyên môn, đơn vị thuộc, trực thuộc; Ủy ban nhân dân xã, phường, thị trấn; các cơ quan, đơn vị, tổ chức khác thuộc hệ thống cơ quan nhà nước của tỉnh.

3. Công an tỉnh, Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh; các doanh nghiệp, đơn vị tư vấn, cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin cho các cơ quan nhà nước của tỉnh; các cơ quan, đơn vị, tổ chức có tham gia hoạt động khai thác, sử dụng, kết nối, chia sẻ dữ liệu với các hệ thống thông tin của các cơ quan nhà nước tỉnh.

4. Cá nhân là cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị, tổ chức nêu tại Khoản 2 Điều này và các cá nhân khác liên quan.

Điều 3. Giải thích từ ngữ

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

1. Các khái niệm *"an toàn thông tin mạng", "mạng", "hệ thống thông tin", "chủ quản hệ thống thông tin", "xâm phạm an toàn thông tin mạng", "sự cố an toàn thông tin mạng", "rủi ro an toàn thông tin mạng", "phần mềm độc hại", "xung đột thông tin", "thông tin cá nhân", "xử lý thông tin cá nhân"* được định nghĩa theo quy định tại các khoản 1, 2, 3, 5, 6, 7, 8, 11, 14, 15 và 17 Điều 3 Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015.

2. Các khái niệm *"tội phạm mạng", "tấn công mạng", "khủng bố mạng", "gián điệp mạng"* được định nghĩa theo quy định tại các khoản 7, 8, 9 và 10 Điều 2 Luật An ninh mạng ngày 12 tháng 6 năm 2018.

3. *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.

4. *Trung tâm dữ liệu điện tử của tỉnh* là nơi tập trung các máy chủ, thiết bị kỹ thuật công nghệ thông tin chuyên dụng với khả năng lưu trữ, xử lý dữ liệu lớn, hệ thống bảo mật an toàn dữ liệu, hệ thống phụ trợ, các hệ thống thông tin, cơ sở dữ liệu dùng chung, chuyên ngành của tỉnh được triển khai theo mô hình điện toán đám mây, tuân theo quy chuẩn, tiêu chuẩn kỹ thuật Việt Nam và quốc tế về Trung tâm dữ liệu, bảo đảm các thiết bị, phần mềm được hoạt động trong môi trường tiêu chuẩn, ổn định, an toàn.

Điều 4. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan, tổ chức.

2. Hoạt động ứng dụng công nghệ thông tin của các cơ quan, tổ chức phải tuân thủ nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 và Điều 41 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.

Điều 5. Các hành vi bị cấm

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng quy định tại Điều 7 Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 và Điều 8 Luật An ninh mạng ngày 12 tháng 6 năm 2018.

2. Các hành vi bị cấm trong quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng quy định tại Điều 5 Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng.

3. Tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point) vào mạng máy tính của cơ quan, tổ chức và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card, wireless USB) trên máy tính có kết nối mạng nội bộ để truy nhập mạng Wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan, tổ chức.

4. Tự ý đăng lên, tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. Yêu cầu chung về quản lý an toàn thông tin mạng

1. Đối với cơ quan, tổ chức:

a) Thực hiện phân loại thông tin do mình sở hữu theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp theo quy định của pháp luật về bảo vệ bí mật nhà nước. Khi sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại;

b) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn mất an toàn thông tin mạng xuất phát từ tần số, kho số, tên miền và địa chỉ Internet của mình. Phối hợp, cung cấp thông tin liên quan đến an toàn tài nguyên viễn thông theo yêu cầu của cơ quan nhà nước có thẩm quyền;

c) Tổ chức các biện pháp bảo vệ hệ thống thông tin, ngăn chặn xung đột thông tin trên mạng thuộc quyền quản lý và phối hợp chặt chẽ với cơ quan nghiệp vụ theo quy định của pháp luật để triển khai các biện pháp ngăn chặn xung đột thông tin trên mạng khi vượt quá thẩm quyền, khả năng;

d) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình. Hợp tác với các cơ quan chức năng xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;

đ) Xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của cơ quan, tổ chức mình. Khi xử lý thông tin cá nhân phải có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý;

e) Phân công, bố trí cán bộ làm công tác chuyên trách về công nghệ thông tin, an toàn thông tin mạng phải có trình độ đào tạo hoặc được bồi dưỡng kiến thức, kỹ năng phù hợp, đáp ứng yêu cầu thực hiện nhiệm vụ;

g) Thường xuyên tuyên truyền, phổ biến, nâng cao nhận thức của cán bộ, công chức, viên chức, người lao động về trách nhiệm bảo đảm an toàn thông tin mạng. Khi tiếp nhận, tuyển dụng nhân sự mới phải quán triệt các quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng. Khi nhân sự chuyển công tác, nghỉ việc, nghỉ theo chế độ phải tổ chức bàn giao, thu hồi tài khoản, quyền truy nhập và tất cả tài sản liên quan tới các hệ thống thông tin của cơ quan, tổ chức.

2. Đối với cá nhân cán bộ, công chức, viên chức, người lao động:

a) Thường xuyên cập nhật và nghiêm túc chấp hành quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng của cơ quan, tổ chức và thực hiện các hướng dẫn, khuyến cáo của bộ phận, cán bộ chuyên trách công nghệ thông tin, an toàn thông tin mạng;

b) Tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng, đồng thời có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý;

c) Khi tham gia quản lý, vận hành mạng máy tính của cơ quan, tổ chức phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin mạng đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp;

d) Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính làm ảnh hưởng đến an toàn thông tin mạng; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin, tài liệu chứa bí mật nhà nước lên hệ thống máy tính có kết nối mạng Internet;

đ) Phải sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin, dữ liệu do các cơ quan nhà nước hoặc tổ chức có thẩm quyền cung cấp, cho phép sử dụng trong trao đổi thông tin, dữ liệu phục vụ công việc; không sử dụng các trang mạng xã hội, dịch vụ thư điện tử, công cụ tiện ích điện tử công cộng để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, tổ chức;

e) Khi phát hiện nguy cơ mất an toàn thông tin mạng hoặc dấu hiệu sự cố an toàn thông tin mạng phải báo cáo kịp thời với cấp trên và bộ phận, cán bộ chuyên trách công nghệ thông tin, an toàn thông tin mạng để xem xét, tham mưu, tổ chức ngăn chặn, xử lý, khắc phục.

Điều 7. Quản lý đăng nhập, truy nhập hệ thống thông tin

1. Đối với cơ quan, tổ chức chủ quản hệ thống thông tin:

a) Tổ chức cấp tài khoản truy nhập hệ thống thông tin phù hợp với mục đích, yêu cầu, nhiệm vụ quản trị, khai thác, sử dụng hệ thống; bảo đảm tài khoản của mỗi cơ quan, tổ chức, cá nhân đăng nhập, truy nhập vào hệ thống là duy nhất;

b) Thiết lập mật khẩu tài khoản đăng nhập, truy nhập quản trị máy chủ, thiết bị mạng, hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải thay đổi ít nhất 03 tháng/lần. Không đặt chế độ tự động ghi nhớ mật khẩu trên các trình duyệt của máy chủ hệ thống trong mọi trường hợp;

c) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản;

d) Hệ thống mạng không dây (Wifi) nội bộ phải được đặt mật khẩu khi truy nhập và có phương pháp hạn chế người dùng truy nhập, giám sát, điều khiển truy nhập mạng không dây;

đ) Cơ quan, tổ chức quản lý, vận hành các hệ thống thông tin dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người khai thác, sử dụng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

2. Đối với cá nhân người quản trị, khai thác, sử dụng hệ thống thông tin:

a) Thiết lập mật mã truy nhập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả máy chủ, máy trạm;

b) Bảo vệ bí mật thông tin tài khoản của cá nhân hoặc tài khoản của cơ quan, tổ chức khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản. Không được cho người khác sử dụng tài khoản của cá nhân hoặc của cơ quan, tổ chức;

c) Thiết lập mật khẩu đăng nhập, truy nhập khai thác, sử dụng hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải thay đổi ít nhất 03 tháng/lần. Không đặt chế độ tự động ghi nhớ mật khẩu đăng nhập, truy nhập khai thác, sử dụng hệ thống thông tin trên các trình duyệt của máy tính trong mọi trường hợp.

Điều 8. Quản lý vận hành hệ thống thông tin

1. Hệ thống thông tin phải được chạy vận hành thử nghiệm và kiểm tra an toàn thông tin trước khi đưa vào sử dụng; phải có tài liệu hướng dẫn sử dụng, quy trình vận hành và thủ tục vận hành, quy trình quản lý sự cố liên quan đến an toàn thông tin; phải có các văn bản xác định vai trò, trách nhiệm của từng cá nhân trong quá trình vận hành và sử dụng.

2. Quản lý nhật ký quá trình vận hành hệ thống thông tin:

a) Cơ quan, tổ chức phải tổ chức thực hiện việc ghi nhật ký trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống thông tin được ghi nhận và lưu giữ. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết;

b) Các sự kiện tối thiểu phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy nhập hệ thống;

c) Cơ quan, tổ chức thường xuyên theo dõi bản ghi nhật ký của hệ thống thông tin và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro an toàn thông tin mạng và mức độ nghiêm trọng các rủi ro đó.

3. Quản lý vận hành đối với trung tâm dữ liệu, phòng máy chủ.

a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, thiết bị cảm biến, giám sát an toàn thông tin, thiết bị phòng chống tấn công mạng phải đặt trong trung tâm dữ liệu hoặc phòng máy chủ và được thiết lập, thực hiện các cơ chế, biện pháp kiểm soát truy nhập, kết nối vật lý, bảo vệ, theo dõi phát hiện xâm nhập phù hợp;

b) Trung tâm dữ liệu, phòng máy chủ phải được trang bị hệ thống lưu điện, hệ thống phát điện dự phòng, hệ thống làm mát, điều hòa không khí, độ ẩm, hệ thống cảnh báo nguồn điện, hệ thống chống sét lan truyền, hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp bảo đảm tiêu chuẩn, quy chuẩn kỹ thuật và tương xứng với quy mô, tính chất, yêu cầu phục vụ;

c) Cơ quan, tổ chức quản lý trung tâm dữ liệu điện tử, phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc và cử cán bộ thường xuyên giám sát thiết bị, hạ tầng tại trung tâm dữ liệu điện tử, phòng máy chủ. Việc vào, ra trung tâm dữ liệu, phòng máy chủ phải được kiểm soát bằng nhật ký hoặc thiết bị bảo vệ (mật khẩu, quẹt thẻ, sinh trắc học) nếu đã có đầy đủ công nghệ.

Điều 9. Phòng, chống phần mềm độc hại

1. Tất cả máy chủ, máy trạm của cơ quan, tổ chức phải được trang bị phần mềm phòng, chống phần mềm độc hại có bản quyền và đã được cơ quan chức năng khuyến cáo sử dụng. Phần mềm phòng, chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật và chế độ tự động quét phần mềm độc hại khi sao chép, mở các tệp tin.

2. Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Cá nhân không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan, tổ chức.

4. Tất cả các máy tính của cơ quan, tổ chức phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp tin trên các thiết bị lưu trữ di động kết nối vào.

5. Máy tính xách tay, thiết bị di động (máy tính bảng, điện thoại thông minh, thiết bị có phần mềm hệ điều hành) trước khi kết nối vào mạng nội bộ (LAN) của cơ quan, tổ chức phải bảo đảm đã được cài đặt phần mềm phòng, chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

6. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, tổ chức; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và không phục vụ công việc.

7. Khi kết nối từ xa vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa. Khuyến khích sử dụng mạng diện rộng của tỉnh (được thiết lập trên nền tảng mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước) để truy nhập, khai thác các hệ thống thông tin dùng chung của tỉnh.

8. Tất cả các tệp tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng, truyền đưa, trao đổi.

9. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: hoạt động chậm bất thường, có cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau, nhất là có dấu hiệu bị thay đổi, mất dữ liệu, người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng nội bộ (LAN), mạng diện rộng (WAN), mạng Internet và báo cáo, thông báo trực tiếp cho cán bộ chuyên trách công nghệ thông tin, an toàn thông tin mạng hoặc bộ phận có trách nhiệm của cơ quan, tổ chức để xử lý.

10. Sở Thông tin và Truyền thông tham mưu Ủy ban nhân dân tỉnh xây dựng, quản lý, vận hành hệ thống phòng, chống phần mềm độc hại tập trung cho các máy chủ, máy trạm của các cơ quan nhà nước tỉnh.

Điều 10. Sao lưu dữ liệu dự phòng

1. Cơ quan, tổ chức chủ quản hệ thống thông tin có trách nhiệm:

a) Xác định danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi dữ liệu hệ thống từ dữ liệu sao lưu; ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi dữ liệu, phần mềm;

b) Tổ chức lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và thường xuyên kiểm tra, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

2. Cơ quan, tổ chức và cá nhân người khai thác, sử dụng hệ thống thông tin và dữ liệu:

a) Lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ đối với các dữ liệu quan trọng, tối thiểu mỗi tháng một lần; trường hợp cần thiết phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng ký số chứng thực;

b) Việc sao lưu dữ liệu dự phòng phải bảo đảm tính đầy đủ, toàn vẹn, và tin cậy. Sau khi sao lưu phải tổ chức lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài phù hợp, bảo đảm tính bảo mật và sẵn sàng cho việc phục hồi dữ liệu khi cần thiết.

Điều 11. Bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Các hoạt động liên quan đến xây dựng, nâng cấp, mở rộng, quản lý, vận hành hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng. Cơ quan, tổ chức chủ quản hệ thống thông tin phải xây dựng, triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng và tổ

chức giám sát, kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý.

2. Công tác quản lý, hướng dẫn và tổ chức thực hiện việc xác định cấp độ và phương án bảo đảm an toàn thông tin mạng; thẩm định, phê duyệt hồ sơ đề xuất cấp độ; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; giám sát an toàn hệ thống thông tin; xây dựng kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng; kiểm tra, đánh giá an toàn thông tin mạng; báo cáo, chia sẻ thông tin theo quy định tại 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, 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 và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Sở Thông tin và Truyền thông tham mưu Ủy ban nhân dân tỉnh tổ chức thực hiện xác định cấp độ, phương án bảo đảm an toàn thông tin mạng, giám sát, kiểm tra, đánh giá an toàn thông tin đối với mạng diện rộng (WAN), các hệ thống thông tin tại Trung tâm dữ liệu điện tử của tỉnh và xây dựng, triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng của tỉnh.

Điều 12. Ứng cứu sự cố an toàn thông tin mạng

1. Phân loại mức độ sự cố an toàn thông tin mạng:

a) Sự cố mức độ thấp (thông thường): sự cố gây ảnh hưởng đến 01 (một) hoặc một vài cá nhân đơn lẻ và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, tổ chức như: máy tính cá nhân bị nhiễm phần mềm độc hại hoặc hư hỏng phần cứng; phần mềm hệ điều hành, các phần mềm ứng dụng, tiện ích cài đặt trên máy tính cá nhân phát sinh lỗi;

b) Sự cố mức độ trung bình: sự cố ảnh hưởng đến một nhóm lớn người khai thác, sử dụng nhưng vẫn chưa gây gián đoạn hay đình trệ hoạt động chính của cơ quan, tổ chức như: hệ thống mạng của 01 (một) phòng, ban, đơn vị thuộc cơ quan, tổ chức bị ngưng hoạt động; phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 (một) phòng, ban đơn vị thuộc cơ quan, tổ chức;

c) Sự cố mức độ cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan, tổ chức như: ứng dụng quản lý văn bản và điều hành, một cửa điện tử, thông tin báo cáo của toàn cơ quan, tổ chức bị ngưng hoạt động; một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tệp tin chung) bị hư hỏng;

d) Sự cố có tính chất nghiêm trọng: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, tổ chức như toàn bộ hệ thống thiết bị công nghệ thông tin ngừng hoạt động; hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung; hoặc sự cố có một hoặc nhiều tính chất sau: có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính, lấy cắp dữ liệu; có thể gây thiệt hại lớn cho các hệ thống thông tin quan trọng của tỉnh như: Trung tâm dữ liệu điện tử, Cổng thông tin điện tử, Cổng dịch vụ công và hệ thống thông tin một cửa điện tử, hệ thống quản lý văn bản và điều hành, hệ thống thông tin báo cáo, hệ thống thư điện tử công vụ và các hệ thống thông tin, cơ sở dữ liệu chuyên ngành của sở, ban, ngành, địa phương, đòi hỏi sự tham gia phối hợp của nhiều cơ quan, tổ chức trong tỉnh và cần có sự hỗ trợ của các cơ quan, đơn vị chuyên trách quốc gia để giải quyết.

2. Khi có nguy cơ mất an toàn thông tin mạng hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ thấp thì cơ quan, tổ chức chỉ đạo bộ phận, cán bộ chuyên trách công nghệ thông tin, an toàn thông tin mạng phối hợp với cá nhân bị ảnh hưởng thực hiện tự ngăn chặn, xử lý, khắc phục hoặc liên hệ với đơn vị cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin, đơn vị triển khai ứng dụng phần mềm để được tư vấn, hỗ trợ ngăn chặn, xử lý, khắc phục.

3. Khi có nguy cơ mất an toàn thông tin mạng hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ trung bình trở lên, hoặc gặp nguy cơ, sự cố thông thường mà cơ quan, tổ chức xét thấy không có khả năng tự ngăn chặn, xử lý được thì thực hiện thông báo hoặc báo cáo cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh để tổ chức điều phối, hỗ trợ ứng cứu.

4. Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh thực hiện nhiệm vụ theo quy chế hoạt động do Ủy ban nhân dân tỉnh ban hành và theo hướng dẫn tại 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.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 13. Tổ chức thực hiện

1. Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh trực tiếp chỉ đạo 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 và thực hiện chức năng Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của tỉnh.

2. Sở Thông tin và Truyền thông có trách nhiệm:

a) Tham mưu, giúp Uỷ ban nhân dân tỉnh, Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh tổ chức triển khai, hướng dẫn, đôn đốc, kiểm tra việc thực hiện

Quy chế này; tổng hợp, thực hiện chế độ báo cáo định kỳ, đột xuất về tình hình, kết quả công tác bảo đảm an toàn thông tin mạng cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, tổ chức có liên quan theo quy định;

b) Tham mưu Ủy ban nhân dân tỉnh xây dựng, đầu tư, nâng cấp các chính sách, giải pháp, hạ tầng kỹ thuật, công nghệ phục vụ quản lý, vận hành và bảo đảm an toàn thông tin mạng cho Trung tâm dữ liệu điện tử, mạng diện rộng (WAN) và các hệ thống thông tin dùng chung của tỉnh;

c) Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, tổ chức để triển khai công tác an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định;

d) Xây dựng và triển khai các chương trình đào tạo, bồi dưỡng, tập huấn, diễn tập, các hội nghị, hội thảo tuyên truyền, phổ biến, cập nhật kiến thức, kỹ năng an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh; thường xuyên cập nhật thông tin, thông báo cho các cơ quan, tổ chức biết và có biện pháp phòng ngừa, ngăn chặn các rủi ro, nguy cơ mất an toàn thông tin do phần mềm độc hại, xung đột thông tin, tấn công mạng gây ra;

đ) Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy định nội bộ và thực hiện việc bảo đảm an toàn thông tin mạng cho hệ thống thông tin theo quy định; chủ trì, phối hợp với các cơ quan, tổ chức liên quan thanh tra, kiểm tra, kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trên địa bàn tỉnh;

e) Thực hiện chức năng Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của tỉnh. Tham mưu UBND tỉnh thành lập và ban hành Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh. Tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC).

3. Công an tỉnh có trách nhiệm:

a) Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan xây dựng kế hoạch, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin, môi trường mạng gây phương hại đến an ninh quốc gia, lợi ích quốc gia, an ninh, trật tự, an toàn xã hội trên địa bàn tỉnh;

b) Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về công tác bảo đảm an toàn thông tin mạng;

c) Điều tra và xử lý các tổ chức, cá nhân vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

4. Sở Kế hoạch và Đầu tư, Sở Tài chính có trách nhiệm chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, tổ chức rà soát, cân đối, tham mưu Ủy ban nhân dân tỉnh bảo đảm nguồn kinh phí triển khai công tác bảo đảm an toàn thông tin mạng cho Trung tâm dữ liệu điện tử, mạng diện rộng (WAN), các hệ thống thông tin dùng chung của tỉnh, hệ thống thông tin của sở, ban, ngành, địa phương và xây dựng, duy trì, phát triển hệ thống phòng, chống phần mềm độc hại tập trung của tỉnh.

5. Các cơ quan, tổ chức có trách nhiệm:

a) Tổ chức quán triệt, thực hiện Quy chế này; tổng hợp, thực hiện chế độ báo cáo định kỳ, đột xuất theo hướng dẫn của Sở Thông tin và Truyền thông về tình hình, kết quả công tác bảo đảm an toàn thông tin mạng tại cơ quan, tổ chức;

b) Phân công bộ phận hoặc cán bộ chuyên trách bảo đảm an toàn thông tin mạng của cơ quan, tổ chức; tạo điều kiện để các cán bộ phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ kiến thức, kỹ năng về an toàn thông tin mạng;

c) Ban hành và tổ chức thực hiện quy định, quy chế nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật liên quan; thực hiện xác định cấp độ an toàn thông tin mạng và phương án bảo đảm an toàn cho hệ thống thông tin do cơ quan, tổ chức quản lý theo quy định;

d) Phối hợp, cung cấp thông tin và tạo điều kiện cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các đơn vị liên quan triển khai công tác kiểm tra, hỗ trợ ngăn chặn, xử lý, khắc phục nguy cơ, sự cố an toàn thông tin mạng kịp thời, nhanh chóng, hiệu quả;

đ) Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, tổ chức liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

6. Các doanh nghiệp, đơn vị tư vấn, cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin cho các cơ quan nhà nước tỉnh có trách nhiệm:

a) Tư vấn, cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin đáp ứng yêu cầu, tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin theo quy định của Bộ Thông tin và Truyền thông và quy định của pháp luật liên quan;

b) Tư vấn, hỗ trợ các cơ quan, tổ chức ngăn chặn, xử lý, khắc phục hậu quả các nguy cơ mất an toàn thông tin mạng hoặc sự cố an toàn thông tin mạng liên quan đến sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin do mình tư vấn, cung cấp. Tham gia, phối hợp các hoạt động ứng cứu, khắc phục sự cố an toàn thông tin mạng khi có yêu cầu, điều phối của Ủy ban nhân dân tỉnh, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và cơ quan, tổ chức khác có thẩm quyền.

7. Cơ quan, đơn vị, tổ chức và cá nhân có tham gia hoạt động khai thác, sử dụng, kết nối, chia sẻ dữ liệu với các hệ thống thông tin của các cơ quan nhà nước tỉnh có trách nhiệm tuân thủ Quy chế này và các quy định của pháp luật liên quan.

Điều 14. Trách nhiệm thi hành

1. Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh; Thủ trưởng các sở, ban, ngành cấp tỉnh; Chủ tịch Ủy ban nhân dân cấp huyện; Chủ tịch Ủy ban nhân dân cấp xã; Thủ trưởng các cơ quan, đơn vị có tham gia hoạt động tư vấn, cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin và khai thác, sử dụng, kết nối, chia sẻ dữ liệu với các hệ thống thông tin của các cơ quan nhà nước tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành các quy định tại Quy chế này.

2. Trong quá trình triển khai thực hiện Quy chế, nếu có vấn đề phát sinh, vướng mắc, các cơ quan, đơn vị, tổ chức, cá nhân phản ánh với Ủy ban nhân dân tỉnh (thông qua Sở Thông tin và Truyền thông) để xem xét, sửa đổi, bổ sung./.

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

Nguyễn Tiến Hoàng