

Số: /QĐ-SNV

Quảng Bình, ngày tháng 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 Sở Nội vụ tỉnh Quảng Bình

GIÁM ĐỐC SỞ NỘI VỤ TỈNH QUẢNG BÌNH

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 Quyết định số 24/2015/QĐ-UBND ngày 15/7/2015 của UBND tỉnh Quảng Bình về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Nội vụ tỉnh Quảng Bình;

Căn cứ Quyết định số 13/2020/QĐ-UBND ngày 14/7/2020 của UBND tỉnh Quảng Bình 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;

Theo đề nghị của Chánh Văn phòng Sở.

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 Sở Nội vụ tỉnh Quảng Bình, kể từ ngày ký quyết định.

Điều 2. Chánh Văn phòng, trưởng các đơn vị thuộc, trực thuộc Sở và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- UBND tỉnh (b/cáo);
- Sở Thông tin và Truyền thông;
- Lãnh đạo Sở;
- Như Điều 2;
- Lưu: VT, VP.

GIÁM ĐỐC

Trần Đình Dinh

QUY CHẾ

Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Nội vụ tỉnh Quảng Bình

(Ban hành kèm theo Quyết định số /QĐ-SNV ngày tháng năm 2020 của Sở Nội vụ 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 đơn vị thuộc, trực thuộc Sở Nội vụ tỉnh Quảng Bình.

Điều 2. Đối tượng áp dụng

1. Các đơn vị thuộc, trực thuộc Sở Nội vụ.
2. Cá nhân là công chức, viên chức, người lao động của cơ quan, đơn vị thuộc, trực thuộc Sở 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 Sở.

2. Hoạt động ứng dụng công nghệ thông tin của Sở phải tuân thủ nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 41 Nghị định số 64/2007/NĐ-CP.

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 và Điều 8 Luật An ninh mạng.

2. Tự ý lắp đặt các thiết bị thu, phát sóng Wifi (Access Point) vào mạng máy tính của Sở khi chưa được phê duyệt của Lãnh đạo Sở.

3. 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 các đơn vị thuộc, trực thuộc Sở

a) 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; 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;

đ) Xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của cơ quan 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) Thường xuyên tuyên truyền, phổ biến, nâng cao nhận thức của 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 chuyên 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.

2. Đối với cá nhân 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 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 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 truy cập vào các liên kết lạ không rõ về nội dung; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để truy cập 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;

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 đối với người quản trị, sử dụng hệ thống thông tin

1. 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.

2. Bảo vệ bí mật thông tin tài khoản của cá nhân hoặc tài khoản của cơ quan khi được phân công quản lý, đồng thời phải thay đổi ngay mật khẩu tài

khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, sử dụng và bảo vệ mật khẩu của tài khoản. Không được cho người khác sử dụng tài khoản của cá nhân hoặc của cơ quan.

3. 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. Phòng, chống phần mềm độc hại

1. Tất cả máy chủ, máy trạm 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.

4. Tất cả các máy tính 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 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; 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 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.

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 hoặc bộ phận có trách nhiệm của cơ quan để xử lý.

Điều 9. Sao lưu dữ liệu dự phòng

1. Văn phòng Sở 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 phục hồi dữ liệu; 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. Các đơn vị và cá nhân sử dụng hệ thống thông tin:

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 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 10. 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 Sở 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 hoạt động chính của Sở như: Hệ thống mạng của 01 (một) đơn vị thuộc, trực thuộc Sở bị ngưng hoạt động; phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 (một) đơn vị;

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 Sở như: Ứng dụng quản lý văn bản và điều hành, một cửa điện tử, thư điện tử công vụ... của toàn Sở bị ngưng hoạt động; một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến... 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 Sở 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.

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 Văn phòng Sở chỉ đạo bộ phận phụ trách công nghệ thông tin phối hợp với đơn vị, cá nhân bị ảnh hưởng tự xử lý, khắc phục hoặc liên hệ với đơn vị cung cấp sản phẩm, dịch vụ viễn thông, Internet, 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 hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ trung bình trở lên, xét thấy không có khả năng tự xử lý được thì Văn phòng Sở báo cáo lãnh đạo Sở và thông báo cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh để tổ chức điều phối, hỗ trợ ứng cứu.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 11. Tổ chức thực hiện

1. Thủ trưởng các đơn vị thuộc, trực thuộc Sở có trách nhiệm:

Tổ chức quán triệt, thực hiện Quy chế này; 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, gửi về Sở Nội vụ (qua Văn phòng);

Phân công bộ phận hoặc cán bộ chuyên trách bảo đảm an toàn thông tin mạng của cơ quan, đơn vị; 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.

2. Văn phòng Sở có trách nhiệm:

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 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;

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

Theo dõi, tổng hợp và báo cáo định kỳ theo quy định.

Trong quá trình triển khai thực hiện Quy chế, nếu có vấn đề phát sinh, vướng mắc, các đơn vị, cá nhân phản hồi với Văn phòng Sở để tổng hợp, báo cáo Giám đốc Sở xem xét, sửa đổi, bổ sung./.