UBND TỈNH SÓC TRĂNG
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

Số: 31 /QĐ-STNMT

Sóc Trăng, ngày 17 tháng 02 năm 2025

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tài nguyên và Môi trường

GIÁM ĐỐC SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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 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 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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 Quyết định số 40/2021/QĐ-UBND ngày 02 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh về việc quy định vị trí, chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tài nguyên và Môi trường tỉnh Sóc Trăng;

Theo đề nghị của Chánh Văn phòng Sở và Giám đốc Trung tâm Công nghệ thông tin tài nguyên và môi trường,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tài nguyên và Môi trường.

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng Sở; Giám đốc Trung tâm Công nghệ thông tin tài nguyên và môi trường, Trưởng các phòng, Thủ trưởng các đơn vị thuộc Sở, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Như Điều 3;
- Sở Thông tin và Truyền thông;
- Công an tỉnh;
- GĐ, các PGĐ;
- Lưu: VT, TTCNTT

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH SÓC TRĂNG

Ngô Thái Chân

UBND TỈNH SÓC TRĂNG
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở tài nguyên và Môi trường
(Ban hành kèm theo Quyết định số 31 /QĐ-STNMT ngày17/02/2025 của Sở Tài nguyên và Môi trường tỉnh Sóc Trăng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung của công tác đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Tài nguyên và Môi trường tỉnh Sóc Trăng (sau đây gọi tắt là Sở TN&MT), bao gồm: công tác xây dựng các quy định quản lý đảm bảo an toàn, an ninh thông tin; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với hệ thống thông tin.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các phòng, đơn vị trực thuộc Sở.

2. Cán bộ, công chức, viên chức đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1, Điều này và những tổ chức, cá nhân có liên quan áp dụng Quy chế này trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại các cơ quan, đơn vị (gọi tắt là người sử dụng).

Điều 3. Giải thích từ ngữ

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

1. *An toàn an ninh mạng* là viết tắt của an toàn thông tin mạng và an ninh mạng; được sử dụng khi nội dung quy định tại Quy chế áp dụng đồng thời quy định của pháp luật về an toàn thông tin mạng và an ninh mạng. An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng. Hệ thống thông tin dùng chung là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng do Bộ Tài nguyên và Môi trường, UBND tỉnh và các cơ quan, đơn vị liên quan triển khai, áp dụng tại đơn vị.

4. *Hệ thống thông tin dùng riêng* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng do Sở Tài nguyên và Môi trường xây dựng, đầu tư, quản lý và triển khai đến các phòng, đơn vị trực thuộc Sở và Chi nhánh Văn phòng Đăng ký Đất đai các huyện, thị xã, thành phố.

5. *Cơ sở dữ liệu* là một tập hợp các dữ liệu, thông tin, văn bản điện tử có liên quan với nhau, chứa thông tin của ngành Tài nguyên và Môi trường, các thông tin thuộc chức năng, nhiệm vụ, quyền hạn của Sở Tài nguyên và Môi trường được lưu trữ trên các thiết bị nhớ, hệ thống máy chủ, máy tính trạm phục vụ, hệ thống thông tin dùng chung để đáp ứng nhu cầu khai thác thông tin của các phòng, đơn vị trực thuộc Sở với mục đích phục vụ công tác chuyên môn Tài nguyên và Môi trường.

6. *Thiết bị xử lý thông tin* là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương tự khác).

7. *Người sử dụng* là cán bộ, công chức, viên chức, người lao động tại các phòng, đơn vị trực thuộc Sở sử dụng máy tính để xử lý công việc.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

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 toàn thông tin trong quá trình quản lý, khai thác, sử dụng đối với hệ thống thông tin dùng chung, hệ thống thông tin dùng riêng của các phòng, đơn vị trực thuộc Sở.

1. Tuân thủ quy định của pháp luật về an toàn thông tin mạng, an ninh mạng; bảo vệ bí mật nhà nước, bí mật công tác, dữ liệu cá nhân; giao dịch điện tử và các quy định khác có liên quan. Trường hợp có văn bản quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

2. Phân cấp, ủy quyền trách nhiệm bảo đảm an toàn an ninh mạng phù hợp với tổ chức bộ máy và phương thức làm việc của Sở Tài nguyên và Môi trường.

3. An toàn an ninh mạng phải gắn liền và hỗ trợ các hoạt động ứng dụng CNTT, giao dịch điện tử, chuyển đổi số của Sở Tài nguyên và Môi trường; hỗ trợ việc sử dụng thiết bị xử lý thông tin để xử lý công việc của cán bộ, công chức, viên chức, người lao động các phòng, đơn vị trực thuộc Sở.

4. Ứng cứu sự cố an toàn an ninh mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn an ninh mạng.

5. Hoạt động ứng dụng CNTT 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 ngày 19/11/2015 (sau đây viết tắt là Luật an toàn thông tin mạng), cụ thể như sau:

a) Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội;

b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác;

c) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức;

d) Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

6. Mỗi cán bộ, công chức, viên chức, người lao động tại các phòng, đơn vị trực thuộc Sở nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp an toàn an ninh mạng.

Điều 5. Các hành vi bị nghiêm cấm trên hệ thống mạng máy tính của Sở

1. Các hành vi bị nghiêm cấm thực hiện theo quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G, điện thoại di động, máy tính bảng).

3. Sử dụng tài nguyên trên hệ thống mạng máy tính của Sở để truyền bá tư tưởng, văn hóa độc hại, đồi trụy, kích động, chống phá các chủ trương, đường lối của Đảng, chính sách và pháp luật của Nhà nước. Lợi dụng hệ thống mạng máy tính của Sở để truyền bá thông tin, quan điểm, thực hiện các hành vi gây hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết đoàn

dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây thù hận, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo.

4. Sử dụng hệ thống mạng máy tính của Sở để truy cập, khai thác, lưu trữ và sử dụng các chương trình giải trí không lành mạnh, các thông tin có nội dung xấu, phát tán vi rút, làm công cụ tấn công hệ thống mạng máy tính của Sở hoặc các mạng khác.

5. Phát tán thư rác, mã độc, thiết lập hệ thống thông tin giả mạo, lừa đảo trong hệ thống mạng máy tính của Sở Tài nguyên và Môi trường; lợi dụng điểm yếu của hệ thống thông tin để tấn công, chiếm quyền điều khiển trái phép đối với hệ thống.

6. Khai thác và sử dụng hệ thống mạng máy tính của Sở vào mục đích kinh doanh, thương mại và cá nhân. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

7. Tự ý gỡ bỏ kết nối, thay đổi thông số thiết lập mạng của các thiết bị công nghệ thông tin liên quan đến hệ thống mạng máy tính của Sở (tên miền, địa chỉ IP,…) gây xung đột tài nguyên.

8. Vi phạm quy định công tác bảo vệ bí mật nhà nước của ngành tài nguyên và môi trường trong quá trình sử dụng hệ thống thông tin, trong đó bao gồm hành vi đánh cắp mật khẩu tài khoản truy cập hệ thống thông tin của người khác hoặc tiết lộ mật khẩu của bản thân cho đối tượng không được phép sử dụng. Tiết lộ tài khoản đăng nhập vào hệ thống mạng qua đường truyền không dây, đấu nối và truy cập trái phép vào hệ thống mạng máy tính của Sở.

Điều 6. Hệ thống thông tin riêng

1. Hệ thống mạng nội bộ (mạng LAN), hệ thống mạng không dây (mạng wifi) phục vụ công tác chuyên môn tại Sở Tài nguyên và Môi trường và các thiết bị công nghệ thông tin tham gia vào hệ thống mạng máy tính của Sở;

2. Hệ thống quản lý dữ liệu quan trắc tự động;

3. Hệ thống CSDL đất đai;

4. Hệ thống Công khai thông tin tài nguyên môi trường;

5. Hệ thống CSDL môi trường;

6. Các phần mềm ứng dụng CNTT và cơ sở dữ liệu khác phục vụ công tác chuyên môn.

Chương II

ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 7. Quản lý truy cập

1. Đối với các phòng, đơn vị trực thuộc Sở, người sử dụng có trách nhiệm:

a) Bảo vệ bí mật thông tin tài khoản cá nhân hoặc tài khoản của phòng, đơn vị trực thuộc Sở 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 cá nhân hoặc của phòng, đơn vị trực thuộc Sở;

b) Hệ thống mạng không dây (wifi) của các cơ quan, đơn vị phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây;

c) Đặt mật khẩu đăng nhập, truy cập 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 được thay đổi ít nhất 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng;

d) Các phòng, đơn vị trực thuộc Sở cần rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ;

đ) Khi sử dụng hệ thống thông tin dùng chung người sử dụng phải có ý thức tự bảo vệ thông tin cá nhân của mình; nghiêm cấm việc tiết lộ tài khoản đăng nhập của mình cho người không có thẩm quyền hoặc sử dụng trái phép tài khoản của người khác để truy cập trái phép vào hệ thống thông tin dùng chung;

e) Khi khai thác, sử dụng hệ thống thông tin dùng chung tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ ghi nhớ mật khẩu trong các trình duyệt;

g) Đối với cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác, phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập các hệ thống thông tin dùng chung thu hồi các thiết bị công nghệ thông tin liên quan.

2. Đối với hệ thống thông tin dùng riêng:

a) Bảo đảm mỗi tài khoản của các phòng, đơn vị trực thuộc Sở, người sử dụng truy cập vào hệ thống thông tin là duy nhất;

b) 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;

c) Trong quá trình quản lý, vận hành hệ thống thông tin dùng riêng, các phòng, đơn vị trực thuộc Sở chịu trách nhiệm về những thiệt hại do phía người 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.

Điều 8. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét phần mềm độc hại khi sao chép, mở các tập 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. Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng, diệt virus trên máy tính khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Các máy tính xách tay, thiết bị di động (điện thoại thông minh, máy tính bảng,...) trước khi kết nối vào mạng LAN nội bộ của cơ quan, đơn vị phải bảo đảm đã được cài chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

6. Tất cả các tập tin, thư mục phải được quét virus trước khi sao chép, sử dụng.

7. Máy chủ, máy tính trạm của các phòng, đơn vị trực thuộc Sở chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, phần mềm độc hại trên máy trạm, như: máy hoạt động chậm bất thường, 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; quan trọng nhất là có dấu hiệu mất dữ liệu..., người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng LAN nội bộ và báo trực tiếp cho bộ phận Công nghệ thông tin, cán bộ có trách nhiệm của đơn vị để phối hợp xử lý.

9. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu. Việc sử dụng các thiết bị lưu trữ ngoài, như: ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

Điều 9. Bảo đảm an toàn an ninh mạng đối với hệ thống thông tin, thiết bị xử lý thông tin

1. Bộ phận quản trị hệ thống thông tin, vận hành hệ thống thông tin, chuyên trách an toàn an ninh mạng thực hiện các nhiệm vụ sau:

a) Xác định cấp độ an toàn của hệ thống thông tin (lập hồ sơ đề xuất cấp độ; tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ) và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định từ Điều 13 đến Điều 19 của Nghị định số 85/2016/NĐ-CP; từ Điều 7 đến Điều 10 của Thông tư số 12/2022/TT-BTTTT và khoản 1 Điều 5 của Quy chế này. Việc xác định hệ thống thông tin để xác định cấp độ căn cứ trên nguyên tắc được quy định tại khoản 1 Điều 5 Nghị định 85/2016/NĐ-CP, Điều 7 Thông tư 12/2022/TTBTTTT và các hướng dẫn bổ sung của Bộ Thông tin và Truyền thông (nếu có).

b) Bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia theo quy định từ Điều 12 đến Điều 15 của Luật An ninh mạng, Điều 7 đến Điều 17 của Nghị định số 53/2022/NĐ-CP.

2. Các phòng, đơn vị trực thuộc Sở không thuộc phạm vi khoản 1 Điều này và sử dụng bị thiết bị xử lý thông tin cá nhân tại đơn vị có trách nhiệm:

a) Bảo đảm an toàn an ninh mạng cho máy tính của người sử dụng thuộc đơn vị: sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn; cài đặt phần mềm phòng, diệt mã độc và cập nhật thường xuyên mẫu nhận diện mã độc.

b) Bảo đảm an toàn an ninh mạng cho thiết bị mạng, thiết bị an ninh mạng sử dụng tại đơn vị: không sử dụng thiết bị không còn được hỗ trợ khắc phục lỗ hổng bảo mật; thực hiện khắc phục lỗ hổng bảo mật ngay khi nhận được cảnh báo, hướng dẫn từ cơ quan chức năng; thay đổi mật khẩu mặc định và giữ bí mật mật khẩu quản trị thiết bị.

Điều 10. Bảo đảm an toàn trong xây dựng hệ thống thông tin

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng theo quy định tại Nghị định số 85/2016/NĐCP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Nghị định số 85/2016/NĐ-CP) và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐCP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Thông tư số 12/2022/TT-BTTTT).

2. Nhiệm vụ quản lý về hướng dẫn xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng; tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 12/2022/TT-BTTTT.

3. Cơ quan, đơn vị chủ quản hệ thống thông tin phải tổ chức kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý.

4. Cán bộ chuyên trách về an toàn an ninh thông tin phối hợp với Sở Thông tin và Truyền thông tổ chức kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin do Sở Thông tin và Truyền thông phê duyệt hồ sơ đề xuất cấp độ; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin.

Điều 11. Bảo đảm an toàn thông tin tham gia kết nối với Trung tâm tích hợp dữ liệu của tỉnh

1. Xây dựng phương án bảo đảm an toàn thông tin mạng khi tham gia kết nối với Trung tâm tích hợp dữ liệu của tỉnh; bảo đảm an toàn và thuận lợi đối với quá trình quản lý và sử dụng các dịch vụ.

2. Các phòng, đơn vị trực thuộc Sở đặt dữ liệu hoặc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh phải tuân thủ các chính sách an toàn thông tin mạng liên quan đến việc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh.

3. Các phòng, đơn vị trực thuộc Sở khi kết nối vào Trung tâm tích hợp dữ liệu phải bảo vệ thiết bị đầu cuối của mình, chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và truy cập trái phép vào Trung tâm tích hợp dữ liệu của tỉnh.

Điều 12. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố

đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Các phòng, đơn vị trực thuộc Sở có liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác bảo đảm an toàn thông tin, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Điều 13. Bảo đảm an toàn với hệ thống thông tin riêng

1. Đối với hệ thống thông tin riêng phải bố trí phòng máy chủ độc lập, phân công bộ phận chuyên trách hoặc cán bộ chuyên trách CNTT trực tiếp quản lý. Áp dụng các biện pháp và kiểm soát ra vào thích hợp.

2. Phòng máy chủ phải đảm bảo các điều kiện cho những thiết bị đặt trong đó hoạt động ổn định, các điều kiện tối thiểu, gồm: 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 dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy hướng dẫn làm việc trong khu vực an toàn bảo mật.

3. Thiết lập cơ chế bảo vệ mạng nội bộ bảo đảm an toàn thông tin khi có kết nối mạng nội bộ với mạng ngoài, như: Internet, mạng cơ quan khác; cần sử dụng hệ thống bảo vệ mạng nội bộ, như: hệ thống tường lửa, hệ thống chống xâm nhập trái phép...

4. Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động và quản lý hạ tầng kỹ thuật, hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy cập trái phép.

5. Kiểm soát chặt chẽ việc cài đặt các phần mềm lên các máy chủ và máy trạm, đảm bảo tuân thủ quy định quản lý an toàn, an ninh thông tin của cơ quan, đơn vị và các quy định khác có liên quan.

6. Việc truy cập vào hệ thống mạng máy tính phải xuất phát từ yêu cầu phục vụ cho việc quản lý, điều hành và công tác chuyên môn của Sở.

7. Trong trường hợp có sự thay đổi chỗ làm việc của cán bộ, công chức viên chức trong các phòng, đơn vị trực thuộc Sở việc giữ nguyên hoặc thay đổi các thông tin người sử dụng đã cài từ trước phải được thông báo cho cán bộ chuyên trách về công nghệ thông tin, an toàn thông tin để phối hợp thực hiện.

8. Đối với các nút mạng đấu nối từ hệ thống mạng máy tính của Sở với máy tính trạm phục vụ của cán bộ, công chức, viên chức trong các phòng, đơn vị trực thuộc Sở thì các cá nhân có trách nhiệm trực tiếp quản lý, bảo quản và sử dụng.

9. Đối với các nút mạng và máy tính nối mạng có nhiều người sử dụng thì mỗi người dùng phải có trách nhiệm bảo quản, sử dụng và giữ bí mật tài khoản

của mình (account) bao gồm: Tên người sử dụng (Username); Mật khẩu đăng nhập vào hệ thống mạng (Password).

10. Việc truy cập vào hệ thống mạng thông qua hệ thống truy cập từ xa, các cá nhân, phòng, đơn vị trực thuộc Sở có trách nhiệm bảo mật các thông số kỹ thuật kết nối vào hệ thống mạng. Nghiêm cấm việc cung cấp, để lộ các thông tin này cho người khác.

11. Hệ thống mạng nội bộ (mạng LAN) phải đáp ứng các yêu cầu sau:

a) Phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi phòng, đơn vị trực thuộc Sở truy cập và kiểm soát truy cập giữa các vùng mạng bằng phân quyền truy cập, khai thác và sử dụng.

b) Cài đặt các bản cập nhật, vá lỗi cho hệ điều hành máy chủ, máy trạm và tường lửa để khắc phục kịp thời các điểm yếu nghiêm trọng.

d) Che giấu và tránh truy cập trực tiếp các địa chỉ mạng bên trong từ bên ngoài (Internet, hạ tầng truyền thông thống nhất ngành tài nguyên và môi trường).

12. Hệ hệ thống mạng không dây (mạng wifi) phải đáp ứng các điều kiện tối thiểu sau:

a) Thiết bị phần cứng phải có chứng nhận Wi-Fi (chứng nhận của Liên minh Wi-Fi (www.wi-fi.org) cho sản phẩm đạt tiêu chuẩn 802.11).

b) Áp dụng mã hoá dữ liệu truyền nhận sử dụng thuật toán mã hoá an toàn.

c) Người dùng mạng không dây phải được cung cấp tài khoản truy cập mới có thể truy cập được và xác thực qua kênh mã hoá.

d) Các điểm truy cập không dây (thiết bị phát sóng làm cầu nối giữa mạng có dây và không dây) của đơn vị được bảo vệ tránh bị xâm nhập, truy cập trái phép.

13. Việc truy cập vào hệ thống mạng qua đường truyền không dây của các thiết bị di động (laptop, mobile phone…) chỉ phục vụ cho các đối tượng trong nội bộ cơ quan Sở. Trong trường hợp cần phục vụ Hội nghị, Hội thảo, Bộ phận Công nghệ thông tin thiết lập hệ thống kết nối đường truyền không dây riêng tách rời hệ thống mạng của Sở. Thông tin trao đổi thông qua hệ thống kết nối đường truyền không dây phải được bảo mật và cấp tài khoản truy cập.

14. Đối với truy cập từ xa vào hệ thống mạng nội bộ (mạng LAN):

a) Máy tính dùng để kết nối tới mạng của đơn vị phải được đảm bảo an toàn theo quy định tại Điều 9.

b) Kết nối truy cập từ xa phải sử dụng mã hoá kênh truyền theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định.

c) Hạn chế truy cập từ xa vào mạng nội bộ từ những điểm truy cập Internet công cộng.

Điều 14. Bảo đảm an toàn dữ liệu, cơ sở dữ liệu và phần mềm ứng dụng công nghệ thông tin

1. Các hệ thống phần mềm ứng dụng, cơ sở dữ liệu phải có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn đồng thời phải thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi khi có sự cố an toàn thông tin mạng xảy ra.

2. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã.

3. Quản lý chặt chẽ các thiết bị tin học lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền. Trước khi thanh lý các máy tính, thiết bị công nghệ thông tin trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

4. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

5. Phần mềm hệ quản trị cơ sở dữ liệu phải được thiết lập cơ chế tự động cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

6. Bảo đảm an toàn cho Cổng/Trang thông tin điện tử của đơn vị trong quá trình quản lý, khai thác và cung cấp thông tin phải thường xuyên theo dõi, cập nhật phiên bản vá lỗi nhằm tránh các lỗi đã được công bố; thiết lập và cấu hình hệ thống máy chủ cài đặt Cổng/Trang thông tin điện tử an toàn giảm thiểu khả năng bị tin tặc tấn công. Tổ chức mô hình mạng hợp lý cũng như thiết lập các hệ thống phòng thủ quan trọng như tường lửa (firewall), thiết bị phát hiện, phòng, chống xâm nhập.

7. Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong các phòng, đơn vị trực thuộc Sở 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 cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền.

Điều 15. Phát triển nguồn nhân lực an toàn thông tin

1. Cán bộ chuyên trách về công nghệ thông tin, an toàn thông tin được tạo điều kiện trang bị các thiết bị tin học, phương tiện kỹ thuật làm việc phù hợp với chuyên môn; tham dự đầy đủ các khóa đào tạo và bồi dưỡng kiến thức, nghiệp vụ cho cán bộ quản lý, kỹ thuật về an toàn thông tin mạng.

2. Các phòng, đơn vị trực thuộc Sở xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại đơn vị mình gửi Văn phòng Sở tổng hợp, xây dựng trình Lãnh đạo Sở phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Sở và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

3. Các phòng, đơn vị trực thuộc Sở phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị mình.

4. Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin xây dựng, tham mưu trình Lãnh đạo Sở kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng và triển khai thực hiện các nội dung theo kế hoạch đã được phê duyệt.

5. Khuyến khích các phòng, đơn vị trực thuộc Sở liên kết với tổ chức, cá nhân, doanh nghiệp CNTT uy tín mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng.

Điều 16. Sao lưu dữ liệu dự phòng

1. Đối với các phòng, đơn vị trực thuộc Sở và người sử dụng:

a) Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng. Khi lưu trữ, trao đổi thông tin, dữ liệu quan trọng phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

b) Phải lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ ít nhất một lần trong tháng đối với các dữ liệu quan trọng, bao gồm: cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng, như: các tập tin văn bản, hình ảnh, các tập tin dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

c) Đảm bảo an toàn dữ liệu ở ổ đĩa, thư mục dùng chung trên hệ thống mạng Sở Tài nguyên và Môi trường: Định kỳ hàng tháng, nghiêm túc việc thực hiện soạn thảo, in ấn tài liệu mật; không lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật của nhà nước trên máy tính kết nối mạng Internet, mạng cục bộ Sở Tài nguyên và Môi trường (dữ liệu trên máy tính cá nhân, ổ đĩa mạng, thư mục dùng chung); sắp xếp, dọn dẹp dữ liệu, sao lưu dữ liệu, tổng hợp cơ sở dữ liệu văn bản, công văn đi, công văn đến trên hệ thống

máy chủ để quản lý tập trung, thuận tiện cho công tác tra cứu, tìm kiếm các văn bản phục vụ công tác chuyên môn tại Sở.

2. Đối với bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin các hệ thống thông tin:

a) Có trách nhiệm ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu.

b) Xây dựng 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 hệ thống từ dữ liệu sao lưu.

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

Điều 17. Quản lý, diễn tập, ứng phó sự cố

1. Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin tham mưu Lãnh đạo Sở bố trí cán bộ tham gia diễn tập và ứng phó sự cố an toàn thông tin mạng theo kế hoạch của Bộ Tài nguyên và Môi trường, UBND tỉnh cùng các cơ quan, đơn vị liên quan.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra, như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền trực tiếp quản lý của đơn vị thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc các hệ thống được triển khai tập trung tại Trung tâm tích hợp dữ liệu tỉnh thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo mẫu số 03 của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Trưởng Bộ Thông tin và Truyền thông (sau đây viết tắt là Thông tư số 20/2017/TT-BTTTT) và thực hiện tiếp Bước 4.

d) Bước 4: Phối hợp với Sở Thông tin và Truyền thông, Tổ ứng cứu an toàn thông tin mạng của tỉnh và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 04 của Thông tư số 20/2017/TT-BTTTT, lãnh đạo cơ quan, đơn

vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

3. Trường hợp có sự cố nghiêm trọng, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 18. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. 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 7 Thông tư số 12/2022/TT-BTTTT.

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 .

c) Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP .

d) Trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 13, Điều 14 Nghị định số 85/2016/NĐ-CP và Điều 6, Điều 7, Điều 8, Điều 9, Điều 10 Thông tư số 12/2022/TT-BTTTT.

2. 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 12/2022/TTBTTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin mạng của Bộ Tài nguyên và Môi trường, UBND tỉnh, chính sách an toàn thông tin mạng khác (nếu có).

b) Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin tham mưu Lãnh đạo Sở 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) Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin tham mưu Lãnh đạo Sở chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

Điều 19. Giám sát an toàn thông tin mạng

1. Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin tham mưu Lãnh đạo Sở chỉ đạo, triển khai thực hiện việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Sở Thông tin và Truyền thông và các đơn vị chức năng của Bộ Thông tin và Truyền thông, Bộ Tài nguyên và Môi trường giám sát theo quy định.

2. 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/TTBTTTT ngày 15/11/2017 của Bộ Trưởng Bộ Thông tin và Truyền thông và các quy định khác của Bộ Tài nguyên và Môi trường.

3. Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin tham mưu Lãnh đạo Sở cử 01 lãnh đạo đơn vị và 01 cán bộ (hoặc 01 đơn vị trực thuộc) làm đầu mối giám sát an toàn thông tin mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Cục Chuyển đổi số và Thông tin dữ liệu Tài nguyên Môi trường - Bộ Tài nguyên và Môi trường, Sở Thông tin và Truyền thông trong các hoạt động giám sát an toàn thông tin tại đơn vị.

Điều 20. Kiểm tra, đánh giá an toàn thông tin

1. Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin phối hợp Sở Thông tin và Truyền thông thực hiện kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ trên địa bàn tỉnh theo quy định tại Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 12 Thông tư số 12/2022/TT-BTTTT.

Điều 21. Quản lý hạ tầng kỹ thuật, trang thiết bị CNTT

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng hạ tầng kỹ thuật, trang thiết bị CNTT. Các thiết bị CNTT được giao cho đơn vị, cá nhân nào sử dụng và khai thác thì đơn vị, cá nhân đó phải có trách nhiệm bảo quản và thường xuyên làm vệ sinh thiết bị.

2. Người sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng ngoài, băng từ …) để lưu thông tin thuộc phạm vi bảo vệ có trách nhiệm bảo vệ các thiết bị này và thông tin trên thiết bị, tránh làm mất, lộ thông tin. Nghiêm cấm sử dụng các thiết bị do cá nhân tự trang bị để lưu giữ các thông tin bí mật ngành tài nguyên và môi trường, bí mật của Nhà nước. Khi kết nối vào các máy trạm trong hệ thống mạng máy tính của Sở, tuân thủ các biện pháp phòng chống virus, phải thực hiện quét và diệt virus trên các thiết bị lưu trữ dữ liệu di động này tránh để virus phát tán sang các máy tính trạm trong hệ thống mạng máy tính của Sở. Khi có nghi ngờ máy vi tính bị nhiễm virus phải ngắt máy vi tính ra khỏi hệ thống mạng của Sở và thông báo cho bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin kịp thời phối hợp xử lý.

3. Nghiêm cấm tự ý tháo, lắp, sửa chữa hoặc thay thế các linh kiện, thiết bị công nghệ thông tin thuộc tài nguyên mạng máy tính của Sở đã được bàn giao

để quản lý và sử dụng. Trong trường hợp có sự cố, hỏng hóc xảy ra thì cá nhân, đơn vị quản lý, sử dụng thiết bị phải thông báo cho Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin để kịp thời phối hợp xử lý, tiến hành tách rời và cô lập thiết bị khỏi hệ thống mạng máy tính của Sở.

4. Trang thiết bị CNTT có lưu trữ dữ liệu quan trọng khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu, loại bỏ triệt để khi chuyển đổi mục đích sử dụng các thiết bị đã lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật của nhà nước (ổ cứng di động, ổ cứng máy vi tính cho, tặng các cơ quan, đơn vị, các xã nông thôn mới ....) đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị CNTT đó.

5. Trang thiết bị CNTT có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 22. Trách nhiệm của các phòng, đơn vị trực thuộc Sở

1. Lãnh đạo các phòng, đơn vị trực thuộc Sở có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Lãnh đạo Sở về việc bảo đảm an toàn thông tin trong quản lý, khai thác và sử dụng hệ thống thông tin dùng chung, hệ thống thông tin dùng riêng, hệ thống mạng nội bộ, hoạt động ứng dụng công nghệ thông tin triển khai tại đơn vị.

2. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

3. Phối hợp chặt chẽ với Bộ phận chuyên trách về công nghệ thông tin, an toàn thông tin, Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

4. Thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng trong quản lý, khai thác và sử dụng hệ thống thông tin dùng chung, hệ thống thông tin dùng riêng, hệ thống mạng nội bộ, hoạt động ứng dụng công nghệ thông tin của từng cá nhân trong đơn vị.

5. Có trách nhiệm quản lý và sử dụng tài khoản, quyền truy cập các hệ thống thông tin dùng chung, hệ thống mạng nội bộ, hoạt động ứng dụng công nghệ thông tin và tất cả các tài sản liên quan tới hệ thống thông tin dùng chung.

Điều 23. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin, an toàn thông tin và chuyển đổi số:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình;

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các tổ chức, cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các các phòng, đơn vị trực thuộc Sở:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Khi tham gia vận hành mạng máy tính của cơ quan, đơn vị phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm 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; 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 có nội dung “mật”, “tối mật” và “tuyệt mật” lên hệ thống máy tính có kết nối mạng Internet;

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ, công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai, như: hệ thống thư điện tử tỉnh Sóc Trăng (@soctrang.gov.vn) hoặc hệ thống thư điện tử của bộ, ngành, lĩnh vực; hệ thống quản lý văn bản và điều hành. Mỗi cán bộ, công chức, viên chức và người lao động không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,… để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, đơn vị;

d) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

đ) Tham gia các chương trình đào tạo, hội nghị tập huấn về an toàn thông tin mạng do các cơ quan, đơn vị chuyên trách an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

3. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản CNTT được giao.

b) Lập biên bản bàn giao tài sản CNTT.

c) Bàn giao tài khoản, quyền truy cập hệ thống thông tin dùng chung, hệ thống thông tin dùng riêng, hệ thống mạng nội bộ, hoạt động ứng dụng công nghệ thông tin.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 24. Khen thưởng và xử lý vi phạm

1. Hàng năm, Trung tâm Công nghệ thông tin TNMT phối hợp với Văn phòng Sở căn cứ kết quả kiểm tra, đánh giá công tác bảo đảm an toàn thông tin mạng của các phòng, đơn vị trực thuộc Sở đề xuất Lãnh đạo Sở xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 25. Tổ chức thực hiện

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng, đơn vị trực thuộc Sở kịp thời báo cáo về Trung tâm Công nghệ thông tin TNMT tổng hợp, trình Lãnh đạo Sở xem xét, giải quyết.