Số: 09/QĐ-TTr; 12/1/2022; 16:15:20

UBND TỈNH TÂY NINH
THANH TRA TỈNH

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 tại Thanh tra tỉnh Tây Ninh

(Kèm theo Quyết định số /QĐ-TTr ngày 12 tháng 01 năm 2022 của Thanh tra tỉnh Tây Ninh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc bảo đảm an toàn thông tin (ATTT) mạng trong hoạt động ứng dụng công nghệ thông tin tại Thanh tra tỉnh Tây Ninh.

Điều 2. Đối tượng áp dụng

1. Cơ quan Thanh tra tỉnh Tây Ninh.

2. Công chức, người lao động và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan.

Điều 3. Giải thích từ ngữ

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

1. *Nguy cơ mất ATTT mạng* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái ATTT mạng.

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

Điều 4. Tài nguyên thông tin cần bảo đảm ATTT

Tài nguyên thông tin cần bảo đảm ATTT tại cơ quan bao gồm các thành phần sau đây:

1. Hệ thống hạ tầng kỹ thuật:

a) Thiết bị tính toán, lưu trữ (máy chủ, máy trạm, …);

b) Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hóa, thiết bị lưu trữ dữ liệu di động);

c) Đường truyền dữ liệu, đường truyền Internet;

d) Mạng nội bộ (LAN) và thiết bị kết nối mạng, thiết bị bảo mật, thiết bị phụ trợ;

đ) Thiết bị CNTT kết nối mạng trong cơ quan.

2. Hệ thống thông tin, phần mềm, ứng dụng và cơ sở dữ liệu:

a) Hệ thống thông tin, cơ sở dữ liệu dùng chung (hệ thống thư điện tử, hệ thống phần mềm một cửa và Cổng dịch vụ công, hệ thống phần mềm văn phòng điện tử eGov, phần mềm Họp không giấy, phần mềm quản lý số liệu kinh tế xã hội, phần mềm hỏi đáp trực tuyến, phần mềm đánh giá các chỉ số);

b) Cổng thông tin điện tử của cơ quan;

c) Hệ thống thông tin nghiệp vụ và các cơ sở dữ liệu chuyên ngành.

3. Thông tin, dữ liệu trao đổi, truyền tải, xử lý và lưu trữ trên Trung tâm tích hợp dữ liệu và hạ tầng kỹ thuật của tỉnh.

Điều 5. Nguyên tắc bảo đảm ATTT mạng

1. Bảo đảm ATTT mạng là yêu cầu bắt buộc, có tính xuyên suốt và phải thường xuyên, liên tục được nâng cao, cải tiến trong quá trình:

a) Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu;

b) Thiết kế, xây dựng, vận hành, nâng cấp hoặc hủy bỏ hệ thống thông tin.

2. Cơ quan, cá nhân có trách nhiệm bảo đảm ATTT mạng. Hoạt động ATTT mạng của cơ quan phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

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

4. Xử lý sự cố ATTT phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan và theo quy định của pháp luật.

5. Công chức, người lao động trong cơ quan khi thực hiện nhiệm vụ phải bố trí máy vi tính riêng, nghiêm cấm sử dụng máy tính kết nối Internet và các thiết bị di động thông minh để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định.

6. Phải có phương án tổ chức sao lưu dữ liệu dự phòng dữ liệu của cơ quan. Lãnh đạo các phòng phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

7. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan, đơn vị phải thực hiện việc lưu trữ nhật ký của các hệ thống tại các máy chủ (của hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

8. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 6. Các hành vi bị nghiêm cấm

Theo quy định tại Điều 7 Luật An toàn thông tin mạng.

Chương II

NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 7. Bảo đảm ATTT mức vật lý

1. Bảo đảm ATTT mức vật lý là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động hệ thống.

2. Các biện pháp cơ bản bảo đảm ATTT mức vật lý bao gồm:

a) Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về độ sẵn sàng trong suốt thời gian lắp đặt, sử dụng;

b) Các đường truyền dữ liệu, đường truyền Internet và hệ thống dây dẫn các mạng WAN, LAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của cơ quan;

c) Cá nhân sử dụng thiết bị lưu trữ dữ liệu di động để lưu trữ thông tin, dữ liệu của cơ quan có trách nhiệm bảo vệ thiết bị này và thông tin lưu trên thiết bị, tránh làm mất hoặc lộ, lọt thông tin, dữ liệu;

d) Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan hoặc ngừng sử dụng phải được 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). Khi thanh lý thiết bị thì phải xóa nội dung lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

3. Công chức CNTT có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật; định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 8. Bảo đảm ATTT khi sử dụng máy tính và thiết bị CNTT

1. Bảo đảm an toàn cho máy tính, thiết bị công nghệ thông tin và an toàn dữ liệu.

Cá nhân sử dụng máy tính để xử lý công việc tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do cơ quan, đơn vị có thẩm quyền ban hành (nếu có) trên máy tính được cơ quan cấp cho mình;

b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm trước khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình; trước khi cài đặt, kết nối phần mềm ứng dụng vào hạ tầng mạng nội bộ, hạ tầng Trung tâm tích hợp dữ liệu cần thực hiện hiện kiểm tra để phòng, tránh phần mềm độc hại;

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần

mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...), phải ngắt kết nối giữa máy với mạng nội bộ và báo trực tiếp cho bộ phận chuyên trách về CNTT để được xử lý kịp thời;

d) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động;

đ) Máy tính cá nhân phải được cài đặt mật khẩu và thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan;

e) Phải sử dụng hộp thư điện tử công vụ của tỉnh có tên miền: @tayninh.gov.vn hoặc hộp thư điện tử có tên miền đặc thù theo quy định của ngành nhưng phải đảm bảo tính an toàn, bảo mật khi trao đổi trên môi trường mạng trong quá trình thực hiện nhiệm vụ công vụ;

g) Báo cáo và phải được lãnh đạo cơ quan đồng ý, cho phép trước khi mang máy tính, thiết bị CNTT có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các Điểm a, b, c, d, đ, e, g của Khoản này và chịu sự giám sát của bộ phận chuyên trách về CNTT của cơ quan.

2. Tài khoản truy nhập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó;

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc, cơ quan quản lý cá nhân đó phải thông báo để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin; tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị;

c) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !) và khuyến khích thay đổi mật khẩu ít nhất 03 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ cache và cookie trong trình duyệt trên máy tính;

d) Tạm dừng quyền sử dụng đối với tài khoản đã được đăng ký trên hệ thống nhưng không làm việc trong hệ thống từ 30 ngày trở lên.

Điều 9. Bảo đảm ATTT đối với mạng máy tính

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức

năng cơ bản, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý giám sát bởi các hệ thống các thiết bị mạng, thiết bị bảo mật.

Căn cứ điều kiện, yêu cầu thực tế về bảo mật dữ liệu cơ quan chủ động triển khai xây dựng mô hình, giải pháp an toàn bảo mật, bao gồm các biện pháp kỹ thuật như sau:

a) Bước 1: Kiểm soát truy nhập từ bên ngoài mạng *(sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL/TLS, VPN);*

b) Bước 2: Kiểm soát truy nhập từ bên trong mạng (quản lý các thiết bị đầu cuối, máy tính người sử dụng kết nối vào hệ thống mạng; giám sát, phát hiện và ngăn chặn truy nhập từ bên trong mạng đến các địa chỉ Internet bị cấm truy nhập);

c) Bước 3: Phòng, chống xâm nhập và phần mềm độc hại, bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ; có khả năng tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công. Vô hiệu hóa tất cả các dịch vụ không cần thiết tại từng vùng mạng;

d) Bước 4: Cấu hình chức năng xác thực trên các thiết bị kết nối mạng để xác thực người sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

đ) Bước 5: Mạng không dây phải có cơ chế bảo toàn tính toàn vẹn và bí mật của thông tin được truyền đưa trên môi trường mạng, có hướng dẫn bảo đảm ATTT dành cho các thiết bị đầu cuối khi kết nối vào mạng; được thiết lập các tham số: tên, nhận dạng dịch vụ (SSID), mật khẩu, cấp phép truy nhập đối với địa chỉ vật lý (MAC address), mã hóa dữ liệu. Thường xuyên thay đổi mật khẩu. Các điểm truy nhập không dây phải được bảo vệ, tránh bị tiếp cận trái phép;

e) Bước 6: Hệ thống máy chủ phải có chức năng tự động cập nhật bản ghi nhật ký hệ thống trong khoảng thời gian nhất định (tối thiểu là 03 tháng), lưu trữ thông tin kết nối mạng, quá trình đăng nhập vào máy chủ, các thao tác cấu hình hệ thống, lỗi phát sinh trong quá trình hoạt động và các thông tin liên quan về ATTT để phục vụ công tác khắc phục sự cố và điều tra về ATTT khi xảy ra. Xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN), mạng truyền số liệu chuyên dùng của tỉnh có trách nhiệm:

a) Bảo đảm ATTT đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào hệ thống mạng diện rộng, mạng truyền số liệu chuyên dùng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Sở Thông tin và Truyền thông để xử lý;

b) Phối hợp với Sở Thông tin và Truyền thông rà soát đánh giá tính hợp lệ cấu hình địa chỉ IP kết nối mạng diện rộng, mạng truyền số liệu chuyên dùng

trong quá trình vận hành và sử dụng các hệ thống thông tin, máy chủ, thiết bị CNTT của mình có kết nối với hệ thống mạng diện rộng;

3. Thực hiện áp dụng các biện pháp kỹ thuật cần thiết bảo đảm ATTT trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau:

a) Có hệ thống tường lửa và hệ thống bảo vệ kiểm soát truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu ra , vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS);

b) Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp;

c) Không mở trang tin hoặc ứng dụng Internet trên máy tính chứa dữ liệu quan trọng hoặc có khả năng tiếp cận các dữ liệu, ứng dụng quan trọng; chỉ thiết lập kết nối Internet cho các máy chủ và thiết bị CNTT cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; thiết bị cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

Điều 10. Kiểm tra, khắc phục sự cố ATTT

1. Trách nhiệm phối hợp với các cơ quan, đơn vị chuyên trách về CNTT, ATTT của tỉnh:

a) Rà soát, đánh giá và xác định các sự cố ATTT, các rủi ro ATTT có thể xảy ra với từng thành phần hệ thống thông tin trong phạm vi quản lý của mình. Trên cơ sở đó, xây dựng và phê duyệt các phương án ứng cứu, xử lý sự cố phù hợp với các rủi ro ATTT có thể xảy ra;

b) Chuẩn bị sẵn sàng các biện pháp, phương tiện kỹ thuật để phục vụ cho triển khai các phương án ứng cứu đã được xây dựng;

c) Xây dựng và ban hành các hướng dẫn, quy trình xử lý sự cố ATTT đối với từng đối tượng người sử dụng cụ thể trong hệ thống thông tin theo hướng dẫn của Sở Thông tin và Truyền thông;

d) Thông báo công khai các phương án liên lạc với bộ phận xử lý sự cố cho toàn bộ cá nhân liên quan hệ thống thông tin đang quản lý;

đ) Thường xuyên kiểm tra, rà soát tính sẵn sàng của các phương án ứng cứu sự cố; thực hiện đúng các hướng dẫn, quy trình xử lý sự cố ATTT.

2. Khi có sự cố hoặc nguy cơ mất ATTT, lãnh đạo Thanh tra tỉnh thực hiện:

a) Chỉ đạo xác định nguyên nhân sự cố, có biện pháp khắc phục kịp thời, hạn chế thiệt hại;

b) Trường hợp gặp sự cố nghiêm trọng ở mức độ cao, khẩn cấp (hệ thống bị gián đoạn dịch vụ; dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; hệ thống bị mất quyền điều khiển) hoặc chủ quản hệ thống không đủ khả năng tự kiểm soát, xử lý được sự cố thì phải phối hợp chặt

chẽ với Đội ứng cứu sự cố ATTT mạng của tỉnh và cung cấp đầy đủ thông tin sự cố để được hướng dẫn, hỗ trợ cụ thể;

c) Chuẩn bị nội dung báo cáo sự cố, bao gồm:

Tên, địa chỉ Đơn vị vận hành hệ thống thông tin; chủ quản hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;

Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;

Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;

Đơn vị cung cấp dịch vụ hạ tầng kỹ thuật;

Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;

Kết quả ứng cứu sự cố ban đầu;

Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có);

Bản cập nhật mới nhất của tài liệu mô tả các thành phần hệ thống thông tin, bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin (trong trường hợp sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin quan trọng khác).

Điều 11. Giám sát an toàn hệ thống thông tin mạng

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

Điều 12. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm ATTT số trên địa bàn tỉnh

1. Quy trình xử lý khẩn cấp:

Khi phát hiện hệ thống có nguy cơ mất ATTT như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng (trang) thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan thực hiện các bước cơ bản như sau:

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

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

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

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

2. Nguyên tắc phối hợp trong ứng cứu sự cố:

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

Các sự cố vượt quá khả năng xử lý, cơ quan thông báo đến Đội ứng cứu để hỗ trợ khắc phục và thực hiện báo cáo sự cố mạng.

Tổng hợp, báo cáo đơn vị chuyên trách CNTT (Sở Thông tin và Truyền thông) theo định kỳ 06 tháng một lần và báo cáo đột xuất khi có yêu cầu;

Chương III
TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của công chức, người lao động trong cơ quan

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm ATTT.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay đến công chức chuyên trách CNTT của cơ quan.

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

4. Công chức chuyên trách CNTT:

a) Theo nhiệm vụ được lãnh cơ quan chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin tại cơ quan;

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

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

Điều 14. Tổ chức thực hiện

Văn phòng, các phòng nghiệp vụ có trách nhiệm thực hiện theo đúng quy chế này.

Báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

Trong quá trình thực hiện nếu phát hiện những điểm chưa phù hợp các phòng nghiệp vụ, cá nhân có liên quan kiến nghị với công chức Công nghệ thông tin xem xét hoàn chỉnh nhằm đảm bảo hoạt động thông suốt, hiệu quả, an toàn, an ninh thông./.