

Tuyên Quang, ngày 31 tháng 12 năm 2022

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng của Sở Nội vụ

GIÁM ĐỐC SỞ NỘI VỤ

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 01 tháng 7 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 Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về việc phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

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 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 17/2014/QĐ-UBND ngày 21 tháng 10 năm 2014 của Ủy ban nhân dân tỉnh ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Tuyên Quang;

Căn cứ Quyết định số 469/QĐ-UBND ngày 25 tháng 7 năm 2022 của Ủy ban nhân dân tỉnh về việc phê duyệt Kiến trúc Chính quyền điện tử tỉnh Tuyên Quang, phiên bản 2.0;

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, an ninh thông tin mạng của Sở Nội vụ.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế Quyết định số 98/QĐ-SNV ngày 27/12/2014 của Sở Nội vụ ban hành Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Nội vụ tỉnh Tuyên Quang.

Điều 3. Chánh Văn phòng sở, Người đứng đầu các cơ quan, đơn vị thuộc và trực thuộc Sở và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- UBND tỉnh (báo cáo);
- Sở Nội vụ;
- Như Điều 3 (thực hiện);
- Các cơ quan, đơn vị thuộc và trực thuộc Sở;
- Lưu: VT, VP.

GIÁM ĐỐC



Vũ Quang Thắng

**QUY CHẾ****BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG CỦA SỞ NỘI VỤ**
(Ban hành kèm theo Quyết định số 240/QĐ-SNV ngày 31 tháng 12 năm 2022
của Sở Nội vụ)**Chương I**
QUY ĐỊNH CHUNG**Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng**

1. Phạm vi điều chỉnh: Quy chế này quy định về bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động của Sở Nội vụ và các cơ quan, đơn vị thuộc và trực thuộc Sở.

2. Đối tượng áp dụng:

- Các cơ quan, đơn vị thuộc và trực thuộc Sở Nội vụ (sau đây gọi là cơ quan, đơn vị) và công chức, viên chức và người lao động thuộc các cơ quan, đơn vị.
- Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Sở Nội vụ.
- Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho Sở Nội vụ.

Điều 2. Giải thích từ ngữ

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

- An toàn thông tin mạng* là sự bảo vệ thông tin số và các 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 thông tin mạng* là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.
- Bảo đảm an toàn thông tin 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 của hệ thống;
- Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian;

5. *Hệ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng;

6. *Trang thông tin điện tử* là trang thông tin hoặc tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin;

7. *Cổng thông tin điện tử* là điểm truy nhập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin;

8. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Các cơ quan, đơn vị có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của cơ quan, đơn vị mình; xác định rõ quyền hạn, trách nhiệm của từng cá nhân đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

3. Công chức, viên chức, người lao động trong các cơ quan, đơn vị có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của nhà nước và của Sở Nội vụ.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước lĩnh vực Nội vụ phải được bảo vệ theo quy định của Nhà nước, quy định của Sở Nội vụ về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

5. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng 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/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 5. Quản lý thiết bị công nghệ thông tin

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng thiết bị công nghệ thông tin.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ thiết bị công nghệ thông tin trong các trường hợp như: Mang ra khỏi cơ quan, thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

3. Thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, cơ quan, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, cơ quan, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên thiết bị công nghệ thông tin đó.

4. 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 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).

Điều 6. Quản lý công chức, viên chức, người lao động

1. Các cơ quan, đơn vị sau khi tuyển dụng, tiếp nhận nhân sự mới, cơ quan, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin tại cơ quan, đơn vị.

2. Các cơ quan, đơn vị phải thường xuyên quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin của từng cá nhân.

3. Các cơ quan, đơn vị phải thực hiện quản lý, báo cáo quản trị hệ thống thông tin cấp mới, thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do cơ quan, đơn vị quản lý.

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

a) Xác định rõ trách nhiệm của công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 7. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an toàn thông tin khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính được cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin.

b) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) 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; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

2. Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính

a) Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), 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.

b) Các cơ quan, đơn vị tham gia kết nối, sử dụng hệ thống mạng của Sở Nội vụ có trách nhiệm bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về phòng Văn phòng Sở để xử lý; không được tiết lộ phương thức (tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) để truy nhập vào hệ thống mạng cho tổ chức, cá nhân khác; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

c) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn mạng 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 các cơ quan, đơn vị.

3. Quản lý tài khoản truy cập

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. Các hệ thống thông tin dùng chung của Sở sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá **03** ngày làm việc cơ quan, đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

c) 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 hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

d) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

đ) Việc quản lý tài khoản thư điện tử của Sở Nội vụ theo quy định của quy chế quản lý, sử dụng hệ thống thư điện tử tỉnh Tuyên Quang (*Quyết định số 12/2013/QĐ-UBND* ngày 20/07/2013 của UBND tỉnh).

4. Bảo đảm an toàn thông tin mức ứng dụng

a) Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: Cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần

mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

5. Bảo đảm an toàn thông tin mức dữ liệu

a) Các cơ quan, đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: Thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động.

b) Các cơ quan, đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy tính để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản.

c) Cơ quan, đơn vị bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

d) Các cơ quan, đơn vị phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

đ) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 8. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

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

2. Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

3. 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 Điều 10, Thông tư số 12/2022/TT-BTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác theo quy định (nếu có).

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

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

Điều 9. 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, đơn vị chủ quản 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 cơ quan, đơn vị thuộc và trực thuộc Sở 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 đảm bảo 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 10. Giám sát an toàn thông tin mạng

1. Lãnh đạo Sở phụ trách công nghệ thông tin chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý/ HTTT được giao quản lý giám sát theo quy định.

2. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

Điều 11. Kiểm tra, đánh giá an toàn thông tin

1. Văn phòng Sở chủ trì thực hiện việc kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các HTTT của Sở theo quy định tại Điều 12, Thông tư số 12/2022/TT-BTTTT.
2. Văn phòng Sở là đơn vị chủ trì thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

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

1. Đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở đưa ra phương án xử lý.

2. Thực hiện quy trình xử lý sự cố, lỗ hổng và phương án, giải pháp kỹ thuật bảo đảm an toàn thông tin, an ninh mạng ban hành theo Quyết định số 97/QĐ-SNV ngày 27/12/2016 của Sở Nội vụ và các phương án hướng dẫn của các cơ quan chuyên môn về an toàn thông tin.

Điều 13. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

Các cơ quan, đơn vị phải thường xuyên tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến công chức, viên chức, người lao động tại cơ quan, đơn vị.

Chương III TỔ CHỨC THỰC HIỆN

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

1. Thực hiện các trách nhiệm được giao tại Quy chế này.
2. Tổ chức triển khai thực hiện Quy chế này tại cơ quan, đơn vị.
3. Thực hiện việc quản lý thiết bị công nghệ thông tin và công chức, viên chức, người lao động theo Điều 5 và Điều 6 của Quy chế này.
4. Đối với các đơn vị thuộc Sở: Phối hợp với Văn phòng Sở bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Sở và các hệ thống thông tin do đơn vị quản lý, vận hành.

Điều 15. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin/Lãnh đạo Sở phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 16. Trách nhiệm cá nhân

1. Người đứng đầu các cơ quan, đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến tới từng công chức, viên chức, người lao động của cơ quan, đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại cơ quan, đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Sở về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của cơ quan, đơn vị do không tổ chức, chỉ đạo, kiểm tra công chức, viên chức, người lao động của cơ quan, đơn vị thực hiện đúng quy định.

2. Công chức, viên chức, người lao động các cơ quan, đơn vị thuộc và trực thuộc Sở và các đơn vị khác thuộc đối tượng áp dụng của quy định có trách nhiệm: Tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành do không tuân thủ Quy chế.

Điều 17. Trách nhiệm thi hành

1. Người đứng đầu các cơ quan, đơn vị có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức, người lao động của cơ quan, đơn vị thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh về Văn phòng Sở để tổng hợp, trình Giám đốc sở xem xét, sửa đổi, bổ sung quy chế./