UBND TỈNH SƠN LA **VĂN PHÒNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 97 /QĐ-VPUB	*Sơn La, ngày 19 tháng 8 năm 2025*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng đối với các Hệ thống thông tin của Văn phòng UBND tỉnh

CHÁNH VĂN PHÒNG UỶ BAN NHÂN DÂN TỈNH

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Luật An toàn thông tin mạng 2015;

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ 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 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn Hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 84/2025/QĐ-UBND ngày 16/8/2025 của UBND tỉnh quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Văn phòng UBND tỉnh Sơn La;

Theo đề nghị của Trưởng phòng Tổ chức - Hành chính - Quản trị, Văn phòng UBND tỉnh.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng đối với các Hệ thống thông tin của Văn phòng UBND tỉnh, **gồm 07 Chương, 29 Điều.**

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 63/QĐ-VPUB ngày 24/5/2024 của Chánh Văn phòng Uỷ ban nhân dân tỉnh.

Điều 3. Trưởng phòng Tổ chức - Hành chính - Quản trị; Trưởng các phòng, đơn vị và công chức, viên chức, người lao động thuộc Văn phòng UBND tỉnh chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Chủ tịch UBND tỉnh (b/c);
- Các Phó Chủ tịch UBND tỉnh (b/c);
- Như Điều 3;
- Lưu: VT, TCHCQT, (M3b).

CHÁNH VĂN PHÒNG

CỘNG HOÀ X.H.C.N VIỆT NAM
VĂN PHÒNG UỶ BAN NHÂN DÂN
TỈNH SƠN LA

Trần Bình Minh

UBND TỈNH SƠN LA
VĂN PHÒNG

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

QUY CHẾ
Bảo đảm an toàn, an ninh mạng đối với các Hệ thống thông tin của Văn phòng UBND tỉnh Sơn La

(Ban hành kèm theo Quyết định số: 97 /QĐ-VPUB ngày 19/8/2025 của Văn phòng UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng

1. Quy chế này quy định việc bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin và chuyển đổi số của Văn phòng UBND tỉnh.

2. Đối tượng áp dụng

a) Các phòng, đơn vị trực thuộc Văn phòng; công chức, viên chức, người lao động thuộc Văn phòng UBND tỉnh.

b) Cơ quan, đơn vị, địa phương, tổ chức, doanh nghiệp, cá nhân có kết nối, sử dụng các hệ thống thông tin do Văn phòng quản lý.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và bảo đảm an toàn thông tin mạng phục vụ hoạt động các Hệ thống thông tin của Văn phòng.

Điều 2. Giải thích từ ngữ

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

1. An toàn thông tin mạng là việc bảo vệ thông tin, hệ thống thông tin trên mạng khỏi nguy cơ truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép, nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính sẵn sàng của thông tin.

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.

4. Chủ quản Hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với Hệ thống thông tin.

5. Sự cố ATTT mạng là việc thông tin, Hệ thống mạng nội bộ bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

6. Rủi ro ATTT mạng là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái ATTT mạng.

7. Đánh giá rủi ro ATTT mạng là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, Hệ thống mạng nội bộ.

8. Quản lý rủi ro ATTT mạng là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro ATTT mạng.

Điều 3. Mục tiêu, nguyên tắc bảo đảm ATTT

1. Mục tiêu bảo đảm ATTT: Bảo vệ thông tin, Hệ thống thông tin trên mạng tránh bị truy cập, 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 Hệ thống thông tin.

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm ATTT và Hệ thống thông tin trong phạm vi xử lý công việc theo quy định của pháp luật, cấp có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm ATTT là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu; thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ Hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống thông tin được thực hiện đồng bộ, thống nhất, tập trung đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật ATTT 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 mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi các cài đặt Hệ thống mạng của cơ quan.

3. Tự ý thay đổi, gỡ bỏ biện pháp ATTT cài đặt trên thiết bị CNTT 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.

Điều 5. Phối hợp với cơ quan, tổ chức có thẩm quyền

1. Giao phòng Tổ chức - Hành chính - Quản trị là đầu mối liên hệ, phối hợp Công an tỉnh, Sở Khoa học và Công nghệ, các cơ quan, tổ chức có thẩm quyền quản lý về ATTT trong việc bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin. Đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT của các Hệ thống thông tin.

2. Tham gia các hoạt động, công tác bảo đảm ATTT khi có yêu cầu của cấp có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

a) Công chức, viên chức được tuyển dụng vào vị trí về ATTT có trình độ, chuyên ngành về lĩnh vực CNTT, ATTT, phù hợp với vị trí tuyển dụng, vị trí việc làm.

b) Có quy định, quy trình tuyển dụng công chức và điều kiện tuyển dụng công chức.

2. Xây dựng kế hoạch và định kỳ hàng năm tổ chức đào tạo về ATTT cho 03 nhóm đối tượng bao gồm: công chức, viên chức kỹ thuật, công chức, viên chức quản lý và người sử dụng trong Hệ thống.

3. Trong quá trình làm việc

a) Trách nhiệm bảo đảm ATTT cho người sử dụng, công chức, viên chức quản lý và vận hành Hệ thống thông tin

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT theo từng vị trí công việc.

+ Được phổ biến, quán triệt thường xuyên các quy định về ATTT để nâng cao nhận thức và trách nhiệm bảo đảm ATTT

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với công chức, viên chức quản lý và vận hành Hệ thống:

+ Công chức, viên chức quản lý và vận hành Hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới Hệ thống thông tin.

+ Công chức, viên chức quản lý và vận hành Hệ thống phải tổ chức quản lý định danh đối với người dùng tham gia sử dụng Hệ thống thông tin.

+ Các cơ quan, đơn vị và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của Hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên Hệ thống.

4. Chấm dứt thay đổi công việc

a) Công chức, viên chức chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác *(nếu có)* thuộc sở hữu của cơ quan, đơn vị.

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị Hệ thống sau khi thôi việc.

c) Công chức, viên chức nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 7. Thiết kế an toàn Hệ thống thông tin

1. Xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành Hệ thống thông tin.

2. Xây dựng tài liệu mô tả thiết kế và các thành phần của Hệ thống thông tin.

3. Xây dựng tài liệu mô tả phương án bảo đảm ATTT theo cấp độ.

4. Xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với Hệ thống.

6. Xây dựng phương án quản lý và bảo vệ hồ sơ thiết kế.

7. Có bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế Hệ thống thông tin, các biện pháp bảo đảm ATTT trước khi triển khai thực hiện.

Điều 8. Phát triển phần mềm thuê khoán

1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Các nhà phát triển cung cấp mã nguồn phần mềm.

3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Phần mềm thuê khoán phải được kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng.

Điều 9. Thử nghiệm và nghiệm thu Hệ thống

1. Thực hiện thử nghiệm và nghiệm thu Hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu Hệ thống.

3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu Hệ thống.

4.Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản Hệ thống thông tin trước khi đưa vào sử dụng.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 10. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của Hệ thống

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn.

g) Triển khai Hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

a) Triển khai Hệ thống, phương tiện lưu trữ độc lập với Hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại, nhóm thông tin được dán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình Hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b) Triển khai Hệ thống, phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng.

3. Truy cập và quản lý cấu hình Hệ thống

a) Công chức, viên chức quản lý, vận hành truy cập, khai thác thông tin tại Trung tâm dữ liệu theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Công chức, viên chức quản lý, vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập Hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị Hệ thống *(cứng hóa)* trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào Hệ thống mạng; truy nhập và quản lý cấu hình Hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật *(cứng hóa)* trong Hệ thống và thực hiện quy trình trước khi đưa Hệ thống vào vận hành khai thác.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của Hệ thống máy chủ và dịch vụ

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ: Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào Hệ thống.

3. Truy cập và quản trị máy chủ và ứng dụng

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị CNTT không phải máy tính ngoại trừ các Hệ thống bắt buộc phải có giao tiếp với Internet *(các Hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công)* không được kết nối Internet.

4. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Triển khai Hệ thống, phương tiện lưu trữ độc lập với Hệ thống lưu trữ trên các máy chủ dịch vụ 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 sau: tập tin cấu hình Hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên Hệ thống máy chủ và ứng dụng: Công chức, viên chức phụ trách CNTT chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính *(thay đổi, gỡ bỏ…)* khi chưa được sự đồng ý của bộ phận CNTT của đơn vị.

6. Kết nối và gỡ bỏ Hệ thống máy chủ và dịch vụ khỏi Hệ thống.

7. Cấu hình tối ưu và tăng cường bảo mật *(cứng hóa)* cho Hệ thống máy chủ trước khi đưa vào vận hành, khai thác

a) Sử dụng hệ điều hành bảo đảm ATTT.

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động *(log)* của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào Hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

đ) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

Điều 12. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa

a) Đơn vị xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

5. Sao lưu dự phòng và khôi phục dữ liệu *(tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ)*.

6. Cập nhật đồng bộ thông tin, dữ liệu giữa Hệ thống sao lưu dự phòng chính và Hệ thống phụ.

7. Định kỳ hoặc khi có thay đổi cấu hình trên Hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình Hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên Hệ thống *(nếu có)*.

Điều 13. Quản lý an toàn thiết bị đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Thông tin về thiết bị đầu cuối *(tên, chủng loại, địa chỉ MAC, địa chỉ IP)* phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào Hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong Hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 14. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc có bản quyền. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Văn bản điện tử gửi qua hệ thống thư điện tử phải sử dụng định dạng theo danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: .txt, .doc, .odt, .pdf hoặc các định dạng khác theo quy định; không được gửi tệp thực thi (.com, .bat, .exe, …).

3. Cán bộ, công chức, viên chức, người lao động thuộc Sở phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm *(ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…)*, người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

5. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có tồn tại phần mềm độc hại, bảo đảm tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

6. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn Hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên Hệ thống.

Điều 15. Quản lý giám sát an toàn Hệ thống thông tin

Chính sách, quy trình quản lý giám sát an toàn Hệ thống thông tin bao gồm:

1. Quản lý, vận hành hoạt động bình thường của Hệ thống giám sát.

2. Đối tượng giám sát bao gồm: thiết bị Hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong Hệ thống *(nếu có)*.

3. Kết nối và gửi nhật ký Hệ thống từ đối tượng giám sát về Hệ thống giám sát.

4. Truy cập và quản trị Hệ thống giám sát.

5. Loại thông tin cần được giám sát.

6. Lưu trữ và bảo vệ thông tin giám sát *(nhật ký Hệ thống)*.

7. Đồng bộ thời gian giữa Hệ thống giám sát và thiết bị được giám sát.

8. Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên Hệ thống thông tin.

9. Bố trí nguồn lực và tổ chức giám sát an toàn Hệ thống thông tin 24/7.

Điều 16. Quản lý điểm yếu ATTT

Chính sách, quy trình quản lý điểm yếu ATTT bao gồm:

1. Bộ phận cung cấp, xây dựng Hệ thống và bộ phận chuyên trách về ATTT thực hiện

a) Quản lý thông tin điểm yếu ATTT đối với từng thành phần có trong Hệ thống *(hệ điều hành, máy chủ, ứng dụng, dịch vụ…)*; phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Báo cáo kịp thời Lãnh đạo Văn phòng và bộ phận chuyên trách về ATTT ngay khi phát hiện điểm yếu ATTT ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu ATTT theo chỉ đạo. Việc xử lý điểm yếu ATTT phải bảo đảm không giảm ảnh hưởng, gián đoạn hoạt động của Hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu ATTT chưa được khắc phục và phương án khôi phục Hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Bộ phận chuyên trách về ATTT phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT đối với các điểm yếu khi cần thiết.

2. Định kỳ 02 năm kiểm tra, đánh giá điểm yếu ATTT toàn Hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu ATTT khi có thông tin hoặc nhận được cảnh báo về điểm yếu ATTT đối với thành phần cụ thể trong Hệ thống.

3. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập Hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và điểm a, b, c khoản 3 Điều 12 Thông tư 12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông *(nay là Bộ Khoa học và Công nghệ)* 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.

Điều 17. Quản lý sự cố ATTT

1. Phân nhóm sự cố ATTT mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về Hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia; xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng, ứng phó sự cố ATTT mạng.

2. Xây dựng quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05/2017/QĐ-TTg.

3. Xây dựng và triển khai kế hoạch ứng phó sự cố ATTT theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

4. Giám sát, phát hiện và cảnh báo sự cố ATTT

a) Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố ATTT, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh báo sớm về nguy cơ mất ATTT trong Hệ thống.

b) Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên

trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào Hệ thống thông tin của cơ quan, đơn vị; phối hợp tích cực trong quá trình giải quyết và khắc phục sự cố.

5. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố ATTT; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến Hệ thống.

6. Tổ chức diễn tập phương án xử lý sự cố ATTT theo chỉ đạo của cấp có thẩm quyền và khi cần thiết.

Điều 18. Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Quản lý truy cập, sử dụng tài nguyên nội bộ

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT.

c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào Hệ thống.

2. Quản lý truy cập mạng và tài nguyên trên Internet

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

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất ATTT mạng phải báo cáo Lãnh đạo Sở chỉ đạo bộ phận phụ trách CNTT của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

3. Cài đặt và sử dụng máy tính an toàn.

Điều 19. Quản lý rủi ro ATTT

1. Xác định mức rủi ro.

2. Quy trình đánh giá và quản lý rủi ro.

3. Biện pháp kiểm soát rủi ro.

Điều 20. Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ

1. Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên Hệ thống với sự xác

nhận của đơn vị chủ quản Hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ Hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của Hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản Hệ thống thông tin thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

2. Đối với các Hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

3. Quy định về xử lý và hủy bỏ phương tiện lưu trữ điện tử

a) Thiết bị CNTT có chứa dữ liệu *(máy tính, thiết bị lưu trữ,* ...) khi bị hỏng phải được công chức, viên chức chuyên trách về CNTT kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra khỏi cơ quan, đơn vị sửa chữa, bảo hành.

b) Trước khi tiến hành thanh lý, loại bỏ thiết bị CNTT cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

Chương IV
KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 21. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá

a) Đơn vị chuyên trách ATTT.

b) Bộ Công an.

4. 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 nhiệm vụ kiểm tra, đánh giá.

5. 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.

Điều 22. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin; Kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

c) Kiểm tra các nội dung khác tại quy chế.

2. Hoạt động kiểm tra về an toàn thông tin do Chuyên viên CNTT thực hiện tại các phòng, đơn vị thuộc công tác ứng dụng CNTT hàng năm, theo kế hoạch được phê duyệt.

Chương V

BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 23. Chế độ báo cáo: Theo quy định tại Điều 13, Điều 14 Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

Chương VI

TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 24. Đơn vị vận hành

1. Thực hiện theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP; Quy chế này và các nhiệm vụ do chủ quản Hệ thống thông tin phân công.

2. Chỉ đạo các phòng, đơn vị tổ chức, thực hiện 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 ATTT trong tất cả các công đoạn liên quan đến Hệ thống thông tin.

Điều 25. Trách nhiệm của cán bộ, công chức, viên chức, người lao động tại các phòng, đơn vị trực thuộc Văn phòng và các tổ chức, cá nhân có liên quan tham gia sử dụng Hệ thống

1. Thực hiện nghiêm túc các quy định về bảo đảm an toàn, an ninh thông tin tại Quy chế này.

2. Chịu trách nhiệm về các vi phạm làm mất ATTT mạng do không tuân thủ Quy chế này và các quy định của pháp luật.

3. Tham gia các chương trình đào tạo, tập huấn về ATTT mạng do cấp có thẩm quyền tổ chức.

Điều 26. Trách nhiệm của bộ phận chuyên trách về ATTT

Chuyên viên CNTT thực thi nhiệm vụ làm đầu mối tiếp nhận thông tin về sự cố, phối hợp với các phòng, đơn vị chủ trì xây dựng Hệ thống chỉ đạo bên cung cấp dịch vụ bảo đảm ATTT và ứng cứu sự cố ATTT mạng theo các quy định tại Quy chế này.

Điều 27. Trách nhiệm của đơn vị cung cấp dịch vụ

1. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; thiết kế, thiết lập Hệ thống đáp ứng các yêu cầu kỹ thuật theo tiêu chuẩn TCVN 11930:2017.

2. Quản lý, vận hành, bảo đảm ATTT cho các thành phần Hệ thống thuộc phạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

3. Phối hợp cung cấp nội dung với Chuyên viên CNTT cung cấp thông tin về số liệu báo cáo định kỳ, đột xuất *(Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo ATTT và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về ATTT)* đảm bảo đúng thời gian theo quy định.

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 28. Xây dựng và công bố

1. Chính sách được thông qua và công bố công khai trước khi áp dụng.

2. Tổ chức tuyên truyền, phổ biến cho toàn thể công chức, viên chức, người lao động trong cơ quan để triển khai thực hiện.

Điều 29. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm ATTT kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Trong quá trình thực hiện, nếu có phát sinh, vướng mắc, các phòng, đơn vị phản ánh kịp thời về Phòng Tổ chức - Hành chính - Quản trị để tổng hợp, báo cáo Lãnh đạo Văn phòng xem xét, điều chỉnh, bổ sung Quy chế cho phù hợp./.