ỦY BAN NHÂN DÂN TỈNH TUYÊN QUANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1478 /QĐ-UBND	*Tuyên Quang, ngày 04 tháng 12 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh mạng Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH TUYÊN QUANG

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 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 Giám đốc Sở Thông tin và Truyền thông.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP.

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

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các cơ quan đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Cục An toàn thông tin, Bộ TTTT;
- Chủ tịch UBND tỉnh;
- Các Phó Chủ tịch UBND tỉnh;
- Như Điều 3;
- Các sở, ban, ngành;
- Các PCVP UBND tỉnh;
- Ủy ban nhân dân huyện, thành phố;
- Cổng thông tin điện tử tỉnh;
- Lưu VT, TG CNTT 02.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hoàng Việt Phương

ỦY BAN NHÂN DÂN TỈNH TUYÊN QUANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn, an ninh mạng Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP

(Ban hành kèm theo Quyết định số 1478 /QĐ-UBND ngày 04 tháng 12 năm 2023 của Chủ tịch Ủy ban nhân dân tỉnh)

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 các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh (LGSP) bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức;

- Các ứng dụng, dịch vụ hệ thống cung cấp;

- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng:

a) Các đơn vị thuộc Sở Thông tin và Truyền thông; cán bộ, công chức, viên chức thuộc các đơn vị thuộc Sở Thông tin và Truyền thông;

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP;

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP.

Điều 2. Giải thích từ ngữ

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

1. Hệ thống thông tin (HTTT): 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.

2. LGSP: Nền tảng tích hợp và chia sẽ dữ liệu được triển khai ở cấp tỉnh và bộ (*LGSP viết tắt của Local Government Service Platform*) hay Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh, chứa các dịch vụ dùng

chung để chia sẻ dữ liệu giữa các hệ thống thông tin (HTTT) của các cơ quan, đơn vị thuộc phạm vi một Bộ, ngành, địa phương và đóng vai trò trung gian phục vụ kết nối các HTTT trong nội bộ của Bộ, ngành, địa phương với các hệ thống bên ngoài; mô hình kết nối của LGSP theo kiến trúc Chính phủ điện tử của cơ quan cấp Bộ chủ quản hoặc kiến trúc chính quyền điện tử của cơ quan cấp tỉnh chủ quản phù hợp Khung kiến trúc Chính phủ điện tử Việt Nam.

3. NDXP: Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (*NDXP viết tắt của National Data Exchange Platform*) là hạ tầng kết nối, tích hợp, chia sẻ dữ liệu cấp quốc gia, bao gồm hạ tầng kỹ thuật, phần cứng, phần mềm và hoạt động nghiệp vụ hỗ trợ đóng vai trò phục vụ tích hợp, chia sẻ dữ liệu giữa các HTTT lớn (*HTTT quốc gia; cơ sở dữ liệu (CSDL) quốc gia; HTTT có quy mô, phạm vi từ Trung ương đến địa phương*), giữa các HTTT của các cơ quan cấp Bộ, cấp tỉnh khác nhau hoặc giữa các LGSP; mô hình kết nối của NDXP theo Khung kiến trúc Chính phủ điện tử Việt Nam.

4. Cơ sở dữ liệu chuyên ngành là những CSDL của một ngành, lĩnh vực do cơ quan nhà nước quản lý, được tổ chức thành một hoặc nhiều CSDL.

5. Dữ liệu danh mục dùng chung là dữ liệu về các danh mục, bảng mã phân loại do cơ quan nhà nước có thẩm quyền ban hành, được sử dụng chung trong các HTTT, CSDL bảo đảm việc tích hợp, trao đổi, chia sẻ dữ liệu đồng bộ, thống nhất.

6. Trung tâm điều hành - Network Operations Centers (NOC) phải có các khả năng sau: Giám sát và điều khiển hệ thống mạng, điện, điều hòa, phòng cháy và an ninh của Data Center (DC). Sử dụng hệ thống Camera giám sát được kết nối với đầu ghi hình DVR theo dõi hình ảnh bên trong và bên ngoài DC.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

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 LGSP.

2. Nguyên tắc:

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này;

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

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

ii. Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm ATTT Hệ thống được thực hiện một cách tổng thể, đồng bộ,

tập trung trong việc 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

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

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

Giao Sở Thông tin và Truyền thông là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho LGSP; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của LGSP. Tổ chức, tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng:

a) Cán bộ được tuyển dụng vào vị trí việc làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;

b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

2. Trong quá trình làm việc:

a) Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b) Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

c) Có kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: Cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

3. Chấm dứt thay đổi công việc:

a) Cán bộ 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 tổ chức;

b) Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c) 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

Điều 7. Thiết kế an toàn hệ thống thông tin

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

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

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.

Điều 8. Phát triển phần mềm thuê khoán

1. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá an toàn thông tin, 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 thực hiện thử nghiệm và nghiệm thu hệ thống.

4. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

5. 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

Điều 10. Quản lý an toàn mạng

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

a) Bộ phận NOC thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của các thiết bị hệ thống;

b) Giải pháp giám sát hệ thống thông tin tập trung phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thiết bị hệ thống bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của thiết bị hệ thống, bao gồm các thông tin: Trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực.

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

a) Định kỳ hàng tháng hoặc khi có thay đổi cấu hình thiết bị hệ thống, toàn bộ tập tin cấu hình thiết bị hệ thống được sao lưu dự phòng trên thiết bị và hệ thống lưu trữ độc lập;

b) Tệp tin cấu hình của toàn bộ thiết bị hệ thống phải được sao lưu dự phòng theo từng phiên bản khác nhau, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn;

c) Sơ đồ thiết kế hệ thống về logic và vật lý phải được cập nhật khi có sự thay đổi về thiết kế và được sao lưu dự phòng theo từng phiên bản khác nhau, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn;

d) Có thiết bị hoặc thiết lập hệ thống, phân vùng lưu trữ độc lập để lưu trữ tệp tin cấu hình, sơ đồ hệ thống và các dữ liệu khác phục vụ quản lý an toàn mạng; dữ liệu được lưu trữ phải được phân loại và gán nhãn dữ liệu, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn.

3. Truy cập và quản lý cấu hình hệ thống:

a) Chỉ cho phép truy cập, cấu hình thiết bị hệ thống từ vùng mạng quản trị;

b) Truy cập, cấu hình thiết bị hệ thống từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng;

d) Toàn bộ thao tác thay đổi, thiết lập cấu hình thiết bị hệ thống phải được ghi nhật ký hệ thống;

đ) Hệ thống thông tin cấp độ 4 trở lên, khi thực hiện truy cập, cấu hình thiết bị hệ thống phải thông qua hệ thống quản lý tài khoản đặc quyền.

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

5. Hoạt động quản lý an toàn mạng thực hiện theo Quy trình quản lý an toàn mạng, ban hành kèm theo Quy chế này.

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) Bộ phận NOC thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của hệ thống máy chủ và ứng dụng;

b) Tối thiểu các thông tin về hoạt động của máy chủ và ứng dụng, bao gồm các thông tin: Trạng thái (Up/Down), hiệu năng xử lý (CPU, RAM, Storage) và lưu lượng mạng xử lý theo thời gian thực.

2. Truy cập mạng của máy chủ:

a) Tường lửa hệ thống và tường lửa máy chủ phải được thiết lập để quản lý kết nối mạng từ các địa chỉ bên ngoài vào máy chủ theo ứng dụng, dịch vụ máy chủ cung cấp và địa chỉ nguồn truy cập. Các dịch vụ khác, không sử dụng phải vô hiệu hóa và chặn kết nối từ bên ngoài;

b) Tường lửa hệ thống và tường lửa máy chủ phải được thiết lập để quản lý kết nối mạng từ máy chủ đi ra các mạng bên ngoài; chỉ mở truy cập máy chủ theo hướng đi ra đối với các dịch vụ cơ bản như DNS, NTP, các kết nối khác phục vụ cập nhật hệ điều hành và các dịch vụ nghiệp vụ cụ thể mà máy chủ yêu cầu phải kết nối ra bên ngoài.

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

a) Chỉ cho phép truy cập, cấu hình máy chủ từ vùng mạng quản trị; cấu hình ứng dụng từ vùng mạng quản trị hoặc nghiệp vụ;

b) Truy cập, cấu hình máy chủ và ứng dụng từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng.

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

a) Khi có thay đổi, cập nhật cấu hình, mã nguồn ứng dụng, toàn bộ tập tin cấu hình, mã nguồn ứng dụng phải được sao lưu dự phòng trên thiết bị và hệ thống lưu trữ độc lập;

b) Thực hiện lưu trạng thái ảnh của hệ điều hành ảo hóa (take snapshot) tại thời điểm trước và sau khi cập nhật máy chủ và ứng dụng;

c) Định kỳ hàng tháng lưu trữ ảnh của hệ điều hành máy chủ trên thiết bị và hệ thống lưu trữ độc lập.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng:

a) Trước khi cài đặt hệ điều hành, dịch vụ, phần mềm trên hệ thống chính phải thực hiện cài đặt trên môi trường thử nghiệm để đánh giá mức độ an toàn, ổn định;

b) Dịch vụ, phần mềm trên máy chủ ứng dụng không phục vụ hoạt động của máy chủ theo chức năng phải gỡ bỏ;

c) Thực hiện lưu trạng thái ảnh của hệ điều hành ảo hóa (take snapshot) tại thời điểm trước và sau khi gỡ bỏ dịch vụ, phần mềm;

d) Xóa sạch dữ liệu của hệ điều hành, dịch vụ, phần mềm sau khi được gỡ bỏ.

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

a) Máy chủ hệ thống phải được kiểm tra, đánh giá và xử lý các điểm yếu an toàn thông tin; không còn tồn tại điểm yếu mở mức trung bình trở lên, trước khi kết nối vào hệ thống;

b) Máy chủ phải được cấu hình tối ưu và tăng cường bảo mật trước khi kết nối vào hệ thống;

c) Khi gỡ bỏ máy chủ khỏi hệ thống, toàn bộ chính sách bảo mật, cấu hình hệ thống phải được gỡ bỏ;

d) Toàn bộ dữ liệu, hệ điều hành máy chủ phải được xóa bỏ trước khi gỡ bỏ máy chủ 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.

8. Hoạt động quản lý an toàn máy chủ và ứng dụng thực hiện theo Quy trình quản lý an toàn máy chủ và ứng dụng, ban hành kèm theo Quy chế này.

Điều 12. Quản lý an toàn dữ liệu

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

a) Toàn bộ cơ sở dữ liệu, dữ liệu nghiệp vụ của hệ thống khi lưu trữ trên thiết bị và hệ thống lưu trữ độc lập phải được mã hóa và kèm theo mã kiểm tra tính toàn vẹn;

b) Dữ liệu được sao lưu dự phòng theo từng phiên bản và có nhật ký ghi lại thông tin dữ liệu sau mỗi lần thực hiện sao lưu, dự phòng;

c) Độ dài của khóa bí mật dùng để mã hóa dữ liệu tối thiểu 128 bit.

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

a) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu hệ thống (tệp tin cấu hình, ảnh hệ điều hành,…) được quản lý bởi bộ phận NOC;

b) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu nghiệp vụ (tệp tin dữ liệu, cơ sở dữ liệu,…) được quản lý bởi bộ phận nghiệp vụ tương ứng;

c) Thông tin khóa bí mật phải được lưu trữ mã hóa, kèm theo mã kiểm tra tính toàn vẹn trên thiết bị và hệ thống lưu trữ độc lập;

d) Chỉ có bộ phận/cán bộ có chức năng có quyền quản lý và truy cập khóa bí mật;

đ) Thông tin mỗi khóa bí mật phải có thông tin nhật ký quản lý, cán bộ quản lý tại mỗi thời điểm.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu không được sử dụng không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Thông tin và Truyền thông công bố.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ phải được mã hóa đáp ứng yêu cầu ở trên.

5. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ phải được đồng bộ theo thời gian thực.

6. Định kỳ hàng tháng 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) theo Quy trình tại điểm 5 Điều này.

7. Hoạt động quản lý an toàn dữ liệu thực hiện theo Quy trình quản lý an toàn dữ liệu, ban hành kèm theo Quy chế này.

Điều 13. Quản lý an toàn thiết bị đầu cuối

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối:

a) Thiết bị đầu cuối (máy trạm và thiết bị ngoại vi) của cán bộ thuộc tổ chức khi kết nối vào mạng nghiệp vụ phải được quản lý truy cập theo địa chỉ IP và địa chỉ MAC;

b) Trạng thái hoạt động (UP/DOWN) của thiết bị đầu cuối phải được quản lý bởi hệ thống quản lý truy cập lớp mạng tập trung;

c) Ngăn chặn toàn bộ các thiết bị đầu cuối chưa được quản lý kết nối vào mạng nghiệp vụ.

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa:

a) Chỉ cho phép truy cập, sử dụng thiết bị đầu cuối từ bên ngoài hệ thống phải thông qua kết nối VPN;

b) Tất cả truy cập từ các thiết bị đầu cuối từ các mạng khác nhau trong hệ thống phải được kiểm soát truy cập bởi tường lửa lớp mạng;

c) Mọi máy trạm trong mạng phải thiết lập chức năng tường lửa của hệ điều hành;

đ) Mọi máy trạm trong mạng phải cài đặt phần mềm phòng chống mã độc trước khi kết nối vào hệ thống.

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống:

b) Máy trạm phải được cấu hình tối ưu và tăng cường bảo mật trước khi kết nối vào hệ thống;

c) Toàn bộ dữ liệu, hệ điều hành máy trạm phải được xóa bỏ trước khi gỡ bỏ máy chủ khỏi hệ thống.

4. Hoạt động quản lý an toàn thiết bị đầu cuối thực hiện theo Quy trình quản lý an toàn thiết bị đầu cuối, ban hành kèm theo Quy chế này.

Điều 14. Quản lý phòng chống phần mềm độc hại

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động:

a) Máy tính, máy chủ và thiết bị di động phải được cập nhật phần mềm phòng chống mã độc trước khi kết nối vào hệ thống;

b) Phần mềm phòng, chống mã độc trên máy tính, máy chủ và thiết bị di động phải được thiết lập chế độ tự động cập nhật dấu hiệu mã độc từ nhà cung cấp và chế độ bảo vệ theo thời gian thực;

c) Triển khai giải pháp phòng, chống mã độc có chức năng quản lý tập trung.

2. Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng:

a) Phần mềm trước khi cài đặt trên máy tính, thiết bị di động phải được kiểm tra mã độc;

b) Phần mềm trước khi cài đặt trên máy tính, thiết bị di động phải xác thực nguồn gốc từ nhà sản xuất theo mã kiểm tra tính toàn vẹn;

c) Phần mềm sau khi cài đặt phải được xử lý điểm yếu an toàn thông tin và cập nhật lên phiên bản mới nhất;

d) Hệ thống phải được trang bị giải pháp kỹ thuật để quản lý và ngăn chặn truy cập đến các trang thông tin độc hại trên mạng.

3. Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động phải thực hiện qua kênh kết nối an toàn sử dụng giao thức mã hóa, xác thực không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Thông tin và Truyền thông công bố.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ 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.

5. Hoạt động quản lý phòng chống phần mềm độc hại thực hiện theo Quy trình quản lý phòng chống phần mềm độc hại, ban hành kèm theo Quy chế này.

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

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

a) Bộ phận NOC thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của các thành phần của hệ thống giám sát;

b) Giải pháp giám sát hệ thống thông tin tập trung phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thành phần của hệ thống giám sát bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của các thành phần của hệ thống giám sát, bao gồm các thông tin: Trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực;

2. Đối tượng giám sát bao gồm tối thiểu bao gồm: Thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ.

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 chỉ được thực hiện từ vùng mạng quản trị; trường hợp truy cập và quản trị từ mạng bên ngoài thì phải thông qua kênh kết nối VPN.

5. Loại thông tin cần được giám sát bao gồm tối thiểu các loại sau: Thông tin giám sát lớp mạng, lớp máy chủ, lớp ứng dụng, cơ sở dữ liệu và thiết bị đầu cuối.

6. Lưu trữ và bảo vệ thông tin giám sát phải được lưu trữ tập trung đầy đủ các loại thông tin tại khoản 5 Điều này theo thời gian thực.

7. Toàn bộ thành phần trong hệ thống giám sát, máy chủ, thiết bị hệ thống và ứng dụng phải được đồng bộ thời gian.

8. Bộ phận SOC thực hiện giám sát giám sát an toàn hệ thống thông tin 24/7 để thực hiện theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.

9. Việc tổ chức hoạt động giám sát thực hiện theo Quy trình Quảng lý giám sát an toàn hệ thống thông tin, ban hành theo Quy chế này.

Điều 16. Quản lý điểm yếu an toàn thông tin

1. Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: Thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng,

dịch vụ và các thành phần khác trong hệ thống nếu có.

2. Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định:

a) Sở Thông tin và Truyền thông, đơn vị vận hành HTTT định kỳ ngày 01 lần truy cập và cập nhật thông tin về điểm yếu an toàn thông tin được cung cấp bởi tối thiểu 02 tổ chức trong nước và quốc tế;

b) Điểm yếu an toàn thông tin được phân nhóm theo mức độ nghiêm trọng (Critical, High, Medium, Low);

c) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Critical đơn vị vận hành HTTT phải xử lý trong vòng 03 giờ;

d) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Critical đơn vị vận hành HTTT phải xử lý trong vòng 03 giờ;

đ) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Medium đơn vị vận hành HTTT phải xử lý trong vòng 24 giờ.

3. Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin:

a) Bên cung cấp phần mềm, giải pháp, ứng dụng phải có trách nhiệm hỗ trợ xử lý điểm yếu an toàn thông tin theo yêu cầu của bên sử dụng;

b) Đơn vị vận hành HTTT là đầu mối phối hợp xử lý điểm yếu an toàn thông tin từ các nhóm chuyên gia, bên cung cấp dịch vụ.

4. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

5. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

6. Khi phát hiện điểm yếu an toàn thông tin tồn tại trong hệ thống thực hiện theo Quy trình Quản lý điểm yếu an toàn thông tin, ban hành theo Quy chế này.

Điều 17. Quản lý sự cố an toàn thông tin

1. Xây dựng phương án quản lý sự cố an toàn thông tin bao gồm các nội dung sau:

a) Phân nhóm sự cố an toàn thông tin 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 an toàn thông tin mạng quốc gia; xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin

mạng, ứng phó sự cố an toàn thông tin mạng;

b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;

c) Kế hoạch ứng phó sự cố an toàn thông tin mạng;

d) Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

đ) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường;

e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;

g) Cơ chế 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 an toàn thông tin.

3. Phương án Quản lý sự cố an toàn thông tin phải được ban hành cùng Quy chế bảo đảm an toàn thông tin trước khi đưa hệ thống vào vận hành, khai thác.

4. Định kỳ hàng năm tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

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

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

a) Người sử dụng đầu cuối phải tuân thủ các quy định của pháp luật và quy định tại Quy chế này khi truy cập, sử dụng tài nguyên nội bộ;

b) Không truy cập từ xa vào trực tiếp các máy tính trong mạng nội bộ của đơn vị. Trường hợp, người sử dụng cần truy cập từ xa thì phải truy cập gián tiếp qua giao thức mạng an toàn, có hỗ trợ mã hóa bảo mật thông tin như VPN;

c) Không kết nối các thiết bị lưu trữ di động của khách bên ngoài vào các máy tính để bàn của đơn vị. Trường hợp, người sử dụng cần thiết phải kết nối các thiết bị lưu trữ di động của khách bên ngoài thì phải đề nghị và được bộ phận chuyên trách kiểm tra an toàn thông tin trước khi thực hiện.

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

a) Không truy cập trang thông tin theo đường link, mở tệp tin đính kèm từ những thư điện tử lần đầu tiên nhận được, không rõ nguồn gửi hoặc nghi ngờ có thể gây hại. Trường hợp, người sử dụng cần thiết phải truy cập hoặc mở tệp tin đính kèm thì đề nghị bộ phận chuyên trách kiểm tra an toàn thông tin trước khi truy cập hoặc mở tệp tin;

b) Không truy cập các trang thông tin không rõ nguồn gốc hoặc có nội dung độc hại;

c) Thiết bị di động của người sử dụng được kết nối vào mạng không dây công cộng của đơn vị nhưng không kết nối thiết bị di động vào mạng ngang hàng với mạng máy tính để bàn của cán bộ. Trường hợp, người sử dụng cần thiết phải kết

nối vào mạng ngang hàng thì phải đề nghị bộ phận chuyên trách kiểm tra an toàn thông tin cho thiết bị di động trước khi thực hiện;

d) Thiết bị di động khi kết nối vào mạng nội bộ của đơn vị phải được quản lý truy cập ra các vùng mạng khác của hệ thống và mạng Internet;

đ) Thiết bị di động phải được quản lý cấp phát DHCP theo địa chỉ MAC (trừ các thiết bị kết nối vào mạng không dây công cộng).

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

a) Đặt mật khẩu cho các tài khoản của hệ điều hành theo quy tắc: tối thiểu 08 ký tự; bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt. Định kỳ 03 tháng thay đổi mật khẩu;

b) Khóa máy tính và các thiết bị có tính năng tương tự máy tính khi tạm thời rời khỏi vị trí làm việc. Đóng các phiên làm việc của ứng dụng khi đã hoàn tất, trừ khi đã có cơ chế bảo vệ thích hợp;

c) Không tự ý thay đổi cấu hình thiết bị đã được thiết lập, việc thay đổi phải thông báo đến bộ phận chuyên trách.

4. Hoạt động quản lý an toàn người sử dụng đầu cuối thực hiện theo Quy trình Quản lý an toàn người sử dụng đầu cuối, ban hành kèm theo Quy chế này.

Điều 19. Quản lý rủi ro an toàn thông tin

1. Hệ thống phải được xây dựng phương án Quản lý rủi ro an toàn thông tin.

2. Phương án Quản lý an toàn thông tin phải được ban hành cùng Quy chế bảo đảm an toàn thông tin trước khi đưa hệ thống vào vận hành, khai thác.

3. Thực hiện đánh giá và xây dựng phương án xử lý rủi ro cho hệ thống trước khi đưa vào vận hành, khai thác.

4. Thực hiện đánh giá và quản lý rủi ro an toàn thông tin cho hệ thống theo Quy trình Quản lý rủi ro an toàn thông tin, được ban hành kèm theo Quy chế này.

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

1. Yêu cầu đối với việc thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin:

a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành 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 bên ngoài sửa chữa, bảo hành;

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi;

c) Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin thực hiện theo Khoản 1, điều này.

Chương IV:
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 21. Xây dựng và công bố

1. Quy chế này được tổ chức/bộ phận được ủy quyền trình Chủ quản hệ thống thông tin thông qua trước khi công bố áp dụng.

2. Quy chế này được công bố trước khi áp dụng.

3. Tổ chức tuyên truyền, phổ biến Quy chế này cho toàn bộ cán bộ trong tổ chức.

Điều 22. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế này.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

Chương V:
TỔ CHỨC THỰC HIỆN

Điều 23. Trách nhiệm của Sở Thông tin và Truyền thông

1. Đơn vị chuyên trách là Sở Thông tin và Truyền thông có trách nhiệm thực hiện nhiệm vụ quy định tại Điều 16, Quy chế quản lý, vận hành và khai thác Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP.

2. Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin.

Điều 24. Trách nhiệm quản lý của các cơ quan, đơn vị trên địa bàn tỉnh

1. Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Thực hiện theo Quy định tại Điều 17, Quy chế quản lý, vận hành và khai thác Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP.

3. Thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin.

4. Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin, báo cáo chủ quản hệ thống thông tin Điều chỉnh nếu cần thiết.

5. Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

QUY TRÌNH QUẢN LÝ ĐIỂM YẾU AN TOÀN THÔNG TIN

(Ban hành kèm theo Quy chế Bảo đảm an toàn, an ninh mạng Nền tảng chung tích hợp chia sẻ các hệ thống thông tin quy mô cấp tỉnh LGSP)

1. Mục đích

- Quy trình quản lý điểm yếu an toàn thông tin nhằm giảm thiểu rủi ro xuất phát từ việc khai thác các điểm an toàn thông tin tồn tại trong thiết bị hệ thống, máy chủ và ứng dụng trong hệ thống thông tin thuộc phạm vi quản lý của Sở Thông tin và Truyền thông.

- Hướng dẫn chi tiết việc thực hiện Quy trình Quản lý an toàn mạng theo quy định tại **Điều 16** Quy chế này.

2. Phạm vi áp dụng

Quy trình này được áp dụng đối với hệ thống thông tin thuộc phạm vi quản lý của Sở Thông tin và Truyền thông nhằm bảo đảm an toàn thông tin mạng.

3. Tài liệu viện dẫn

- Quy chế bảo đảm an toàn thông tin

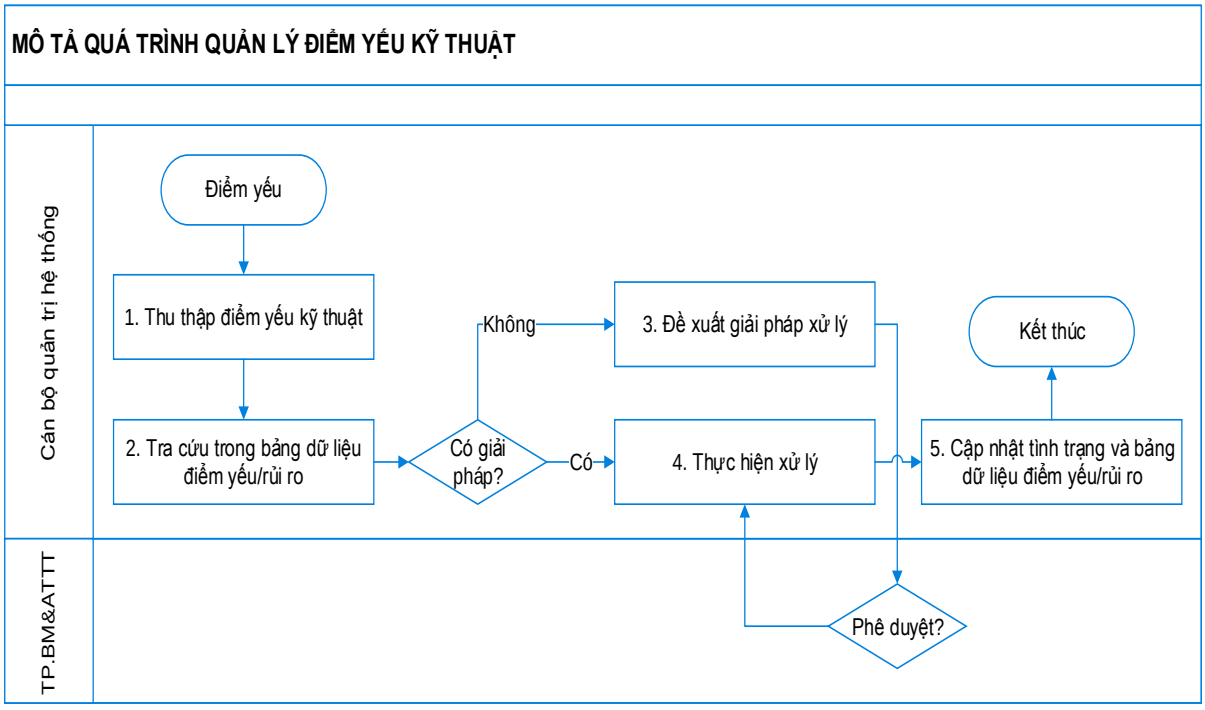
- Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

4. Thuật ngữ và định nghĩa

- Điểm yếu an toàn thông tin (information security vulnerability): Lỗi tồn tại trên sản phẩm phần cứng, phần mềm, dịch vụ hoặc hệ thống trong quá trình phát triển, cài đặt và thiết lập, có thể gây ra nguy cơ mất an toàn cho hệ thống thông tin khi bị tin tặc khai thác.

5. Nội dung quy trình

5.1. Lưu đồ



5.2. Thông số tổng hợp

Thông số	Mô tả	Yêu cầu
Đầu vào	Điểm yếu an toàn thông tin	Bảo đảm xác định đầy đủ điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ và ứng dụng.
Đầu ra	Điểm yếu an toàn thông tin được xử lý	Đáp ứng mục tiêu quản lý điểm yếu an toàn thông tin.
Chỉ tiêu đánh giá	Số điểm yếu an toàn thông tin được xử lý.	Hệ thống không còn tồn tại điểm yếu ở mức độ trung bình trở lên.
Quy trình liên quan	Quy trình Quản lý rủi ro Quy trình Quản lý sự cố ATTT	Tương thích với các yêu cầu của quá trình liên quan

5.3. Diễn giải

Bước 1: Thu thập điểm yếu kỹ thuật

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
1	Cán bộ quản trị hệ thống nhận thông báo điểm yếu an toàn thông tin của hệ thống đang quản lý từ những nguồn chính thức.	Các điểm yếu kỹ thuật được lập danh sách và thông báo	Cán bộ quản trị hệ thống	Việc thu thập các điểm yếu kỹ thuật được thu thập qua các nguồn sau: - Thực hiện quét điểm yếu kỹ thuật định kỳ 1 lần/năm vào Quý 4. - Từ đánh giá/ kiểm soát: Cán bộ đánh giá/ kiểm soát ghi nhận và thông báo tới cán bộ quản trị hệ thống theo Mô tả quá trình Quản lý sự kiện/sự cố BMTT. - Nhà cung cấp: Cán bộ quản trị thực hiện kiểm tra các khuyến nghị của nhà sản xuất liên quan đến các điểm yếu kỹ thuật định kỳ 6 tháng/lần. - Thông báo từ các tổ chức có uy tín (NCSC,VNCERT/CC).

Bước 2. Tra cứu trong bảng dữ liệu điểm yếu/rủi ro

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
1	Tham khảo kho dữ liệu về điểm yếu và các bài học: Cán bộ tiếp nhận có trách nhiệm tra cứu database điểm yếu an toàn thông tin.	Giải pháp xử lý rủi ro (nếu có)	Cán bộ quản trị hệ thống	Database quản lý điểm yếu an toàn thông tin lưu thông tin về các điểm yếu an toàn thông tin đã từng xảy ra (người thông báo, bộ phận thông báo, ngày thông báo, giải pháp xử lý, …) cho các điểm yếu từ mức Trung bình trở lên (tham khảo Mô tả quá trình Quản lý rủi ro). Nếu trong database điểm yếu an toàn thông tin có điểm yếu tương tự và xử lý thành công thì thực hiện hành động xử lý. Nếu chưa có hoặc điểm yếu an toàn thông tin được xử lý không thành công, cán bộ quản trị hệ thống đề xuất giải pháp xử lý theo các bước phía sau.

Bước 3. Đề xuất giải pháp xử lý

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
1	Đề xuất cách thức xử lý: Cán bộ phụ trách quản lý điểm yếu an toàn thông tin xây dựng giải pháp xử lý điểm yếu an toàn thông tin đối với những hệ thống có quyền hạn và trách nhiệm xử lý.	Giải pháp xử lý rủi ro dạng đề xuất.	Cán bộ quản trị hệ thống	Tra cứu hướng dẫn xử lý điểm yếu từ hãng cung cấp sản phẩm, giải pháp. Đề nghị hỗ trợ từ các cơ quan, tổ chức hoặc các doanh nghiệp bảo mật trong nước tư vấn, hướng dẫn. Sau khi giải pháp xử lý được xây dựng, cán bộ phụ trách quản lý điểm yếu an toàn thông tin trình lên cho lãnh đạo Phòng phụ trách lĩnh vực BM&ATTT.

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
2	Phê duyệt cách thức xử lý	Giải pháp xử lý rủi ro được duyệt.	Đại diện lãnh đạo Phòng phụ trách lĩnh vực BM&ATTT	Đại diện lãnh đạo Phòng phụ trách lĩnh vực BM&ATTT xem xét giải pháp xử lý điểm yếu được trình lên: - Trường hợp cách thức xử lý điểm yếu không được chấp nhận, cán bộ tiếp nhận phải xây dựng lại giải pháp xử lý điểm yếu (quay lại **bước 3**). - Trường hợp cách thức xử lý điểm yếu được chấp nhận, chuyển sang **bước 4** (Thực hiện giải pháp xử lý điểm yếu). Cần thông tin việc phê duyệt cho cán bộ phụ trách BM&ATTT.

Bước 4. Thực hiện xử lý

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
1	Thực hiện sao lưu, dự phòng	Dữ liệu được sao lưu, dự phòng trước khi xử lý điểm yếu.	Cán bộ quản trị hệ thống	- Đối với máy chủ, trước khi thực hiện xử lý mã độc, toàn bộ dữ liệu, tệp tin cấu hình, ảnh hệ điều hành (nếu là máy ảo) phải sao lưu, dự phòng. - Đối với máy trạm, người sử dụng thực hiện sao lưu dự phòng những dữ liệu quan trọng có trên máy tính của mình.
2	Xử lý điểm yếu trên môi trường thử nghiệm	Thử nghiệm phương án xử lý điểm yếu	Cán bộ quản trị hệ thống	Thực hiện xử lý điểm yếu trong môi trường thử nghiệm, bảo đảm việc xử lý điểm yếu không ảnh hưởng đến hệ thống đang cung cấp dịch vụ.
3	Xử lý điểm yếu trên môi trường thực	Điểm yếu được xử lý	Cán bộ quản trị hệ thống	Trường hợp thử nghiệm thành công ở bước 2, thực hiện xử lý điểm yếu trong môi trường đang

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
				cung cấp dịch vụ.

Bước 5. Cập nhật tình trạng và bảng dữ liệu điểm yếu/rủi ro

STT	Hoạt động	Sản phẩm	Người thực hiện	Hướng dẫn chi tiết
1	Thực hiện báo cáo	Báo cáo xử lý điểm yếu kỹ thuật	Cán bộ quản trị hệ thống	Sau khi thực hiện xử lý các điểm yếu kỹ thuật cán bộ quản trị hệ thống phải báo cáo tới Lãnh đạo Phòng phụ trách lĩnh vực BM&ATTT
2	Cập nhật bảng quản lý rủi ro	Bảng rủi ro	Cán bộ phụ trách BMTT	Cập nhật thông tin tình trạng điểm yếu và các rủi ro sau xử lý vào bảng quản lý rủi ro của tổ chức.

6. Hồ sơ

STT	Tên hồ sơ	Mã biểu mẫu	Người lập	Hình thức lưu	Thời hạn lưu giữ (năm)	Mức độ quan trọng
1	Danh sách điểm yếu kỹ thuật	N/A	Cán bộ quản trị hệ thống	SOFT	3 năm	INF-SOFT-HIGH
2	Giải pháp xử lý rủi ro	N/A	Cán bộ quản trị hệ thống			
3	Các hồ sơ khác trong quá trình xử lý rủi ro (báo cáo,…)	N/A	Cán bộ quản trị hệ thống			
4	Bảng rủi ro	N/A	Cán bộ phụ trách BMTT			