VĂN BẢN PHÁP LUẬT KHÁC

ỦY BAN NHÂN DÂN XÃ PHONG NHA

ỦY BAN NHÂN DÂN **XÃ PHONG NHA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 990/QĐ-CT	*Phong Nha, ngày 09 tháng 12 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống thông tin nội bộ UBND xã Phong Nha tỉnh Quảng Trị

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ PHONG NHA

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006; Luật An toàn thông tin mạng ngày 19/11/2015; Luật An ninh mạng ngày 12/6/2018;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng Công nghệ thông tin trong hoạt động của cơ quan nhà nước; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ; Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng; Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 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 13/2020/QĐ-UBND ngày 14/7/2020 của UBND tỉnh Quảng Bình ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Quảng Bình;

Xét đề nghị của Chánh Văn phòng HĐND-UBND xã Phong Nha.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống thông tin nội bộ UBND xã Phong Nha tỉnh Quảng Trị.

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

Điều 3. Chánh Văn phòng HĐND-UBND xã, các Trưởng phòng, Trung tâm

phục vụ hành chính công xã và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

CHỦ TỊCH

Phan Hải Hà

ỦY BAN NHÂN DÂN XÃ PHONG NHA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn, an ninh mạng Hệ thống thông tin nội bộ UBND xã Phong Nha tỉnh Quảng Trị

(Ban hành kèm theo Quyết định số 1000/QĐ-CT ngày 09 tháng 12 năm 2025 của Chủ tịch UBND xã Phong Nha tỉnh Quảng Trị)

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 các Hệ thống thông tin của UBND xã Phong Nha tỉnh Quảng Trị (sau đây gọi tắt là các Hệ thống thông tin).

2. Đối tượng áp dụng

a) Các bộ phận, cán bộ, công chức, viên chức của UBND xã Phong Nha, tỉnh Quảng Trị.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các Hệ thống thông tin.

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

Điều 2. 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 các Hệ thống thông tin.

2. Nguyên tắc

a) Cơ quan, tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng 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, an ninh mạng được thực hiện xuyên suốt, toàn trình trong khâu mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

c) Việc bảo đảm an toàn Hệ thống thông tin 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.

d) Trách nhiệm bảo đảm an toàn thông tin mạng và an ninh mạng gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

đ) Trường hợp có quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

e) Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

3. Phạm vi chính sách an toàn thông tin

Phạm vi Chính sách an toàn thông tin tại Quy chế này bao gồm:

a) Thiết lập chính sách an toàn thông tin.

b) Tổ chức bảo đảm an toàn thông tin.

c) Bảo đảm nguồn nhân lực.

d) Quản lý thiết kế, xây dựng hệ thống.

e) Quản lý vận hành hệ thống.

f) Quản lý rủi ro an toàn thông tin.

g) Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

Điều 3. Những hành vi nghiêm cấm

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

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

Điều 4. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

a) UBND xã Phong Nha tỉnh Quảng Trị là đầu mối liên hệ, phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh và các cơ quan, tổ chức có thẩm quyền

quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn thông tin, an ninh mạng cho các Hệ thống thông tin của UBND xã Phong Nha tỉnh Quảng Trị.

b) Giao Chuyên viên Công nghệ thông tin làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin đối với các Hệ thống thông tin của UBND xã Phong Nha tỉnh Quảng Trị.

2. Giao Chuyên viên Công nghệ thông tin tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

Điều 5. Bảo đảm nguồn nhân lực

1. Cán bộ được tuyển dụng, bố trí vào vị trí làm về an toàn thông tin có trình độ, năng lực về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng được lồng ghép trong quy trình tuyển dụng cán bộ, công chức và điều kiện tuyển dụng cán bộ, công chức.

2. Xây dựng kế hoạch và định kỳ hằng năm tổ chức đào tạo hoặc tham gia đào tạo về an toàn thông tin cho 03 nhóm đối tượng bao gồm: Cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

3. Trách nhiệm bảo đảm an toàn thông tin cho cán bộ quản lý và vận hành hệ thống.

a) Cán bộ chuyên trách 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.

b) Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

c) Các bộ phận, 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.

d) 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. Phân quyền sử dụng tài khoản quản trị theo chức năng nhiệm vụ của cá nhân trong công tác vận hành quản trị hệ thống.

4. Với người sử dụng

a) Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT.

b) Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

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; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc.

d) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu với người khác. Đặt mật khẩu với độ an toàn cao và thay đổi mật khẩu tối thiểu 03 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng. Thực hiện các biện pháp mã hóa đối với các tài khoản, mật khẩu được lưu trữ trên thiết bị.

e) Khóa máy tính khi tạm thời rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc, trong tối đa 05 ngày làm việc:

a) Cán bộ nghỉ 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 thuộc sở hữu của tổ chức.

- Quy định đối với viên chức nghỉ hoặc thay đổi công việc:

+ Xác định rõ trách nhiệm của viên chức, người lao động và các bên liên quan về hệ thống thông tin;

+ Làm biên bản bàn giao tài sản với viên chức;

+ Thu hồi quyền truy cập các hệ thống thông tin khi nghỉ việc, điều chuyển công việc, việc thu hồi quyền truy cập phải được thực hiện trong vòng 24 giờ kể từ khi có quyết định nghỉ việc hoặc có quyết định điều chuyển công việc chính thức;

+ Thay đổi quyền truy cập hệ thống thông tin của viên chức cho phù hợp với công việc được điều chuyển.

- Quy định về ATTT quản lý nguồn nhân lực đối tác:

+ Yêu cầu đối tác bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc.

+ Thu hồi quyền truy cập hệ thống thông tin đã được cấp cho đối tác ngay sau khi kết thúc công việc. Thực hiện loại bỏ các thông tin của UBND xã trên các thiết bị của đối tác trước khi hoàn trả.

+ Thay đổi các khóa, mật khẩu nhận bàn giao từ đối tác.

b) Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

- Quy định đối với viên chức nghỉ hoặc thay đổi công việc:

+ Xác định rõ trách nhiệm của viên chức và các bên liên quan về hệ thống thông tin;

+ Làm biên bản bàn giao tài sản với nhân viên;

+ Thu hồi quyền truy cập các hệ thống thông tin khi nghỉ việc, điều chuyển công việc, việc thu hồi quyền truy cập phải được thực hiện trong vòng 24 giờ kể từ khi có quyết định nghỉ việc hoặc có quyết định điều chuyển công việc chính thức;

+ Thay đổi quyền truy cập hệ thống thông tin của viên chức cho phù hợp với công việc được điều chuyển.

- Quy định về ATTT quản lý nguồn nhân lực đối tác:

+ Yêu cầu đối tác bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc;

+ Thu hồi quyền truy cập hệ thống thông tin đã được cấp cho đối tác ngay sau khi kết thúc công việc. Thực hiện loại bỏ các thông tin của UBND xã trên các thiết bị của đối tác trước khi hoàn trả;

+ Thay đổi các khóa, mật khẩu nhận bàn giao từ đối tác.

CHƯƠNG II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 6. Thiết kế, xây dựng hệ thống thông tin

Khi thực hiện triển khai đầu tư, nâng cấp, mở rộng hệ thống hệ thống thông tin, cần thực hiện xây dựng các tài liệu mô tả các yêu cầu sau:

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

3. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

4. Xây dựng các tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

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 7. Thử nghiệm và nghiệm thu hệ thống

1. Khi phát triển phần mềm nội bộ, đối với các hệ thống thông tin theo yêu cầu bắt buộc phải kiểm thử theo quy định của pháp luật, trước khi đưa vào sử dụng phải kiểm thử để đảm bảo an toàn thông tin.

2. Các hệ thống hạ tầng kỹ thuật khác phải tuân thủ vận hành thử, nghiệm thu trước khi đưa vào sử dụng, đơn vị chủ trì có trách nhiệm phối hợp với đơn vị tư vấn triển khai và các tổ chức, cá nhân liên quan tổ chức vận hành thử và nghiệm thu.

3. Hồ sơ phục vụ kiểm định hệ thống thông tin (HTTT) bao gồm:

- Văn bản đề nghị kiểm định, phiếu đăng ký kiểm định.

- Tài liệu ma trận lưu vết yêu cầu (RTM).

- Tài liệu đặc tả yêu cầu người dùng (URD).

- Tài liệu đặc tả yêu cầu phần mềm (SRS).

- Tài liệu thiết kế tổng thể/kiến trúc phần mềm (HLD/SAD).

- Tài liệu thiết kế chi tiết (LLD).

- Tài liệu mô tả sản phẩm (PRD).

- Tài liệu hướng dẫn sử dụng (UM).

- Tài liệu hướng dẫn cài đặt (IG).

- Tài liệu hướng dẫn vận hành, quản trị (OA).

- Tài liệu định cỡ.

- Tài liệu kế hoạch kiểm thử phần mềm (Test plan).

- Tài liệu Kịch bản và test script chức năng (mô tả các tình huống, kịch bản, dữ liệu mẫu, kết quả kiểm thử, ...).

- Bộ cài đặt HTTT.

- Bộ cài đặt phần mềm/thư viện đặc thù liên quan đến HTTT.

- Link lưu trữ bộ cài đặt/ thư viện HTTT trên các công cụ như SCM, Jenkins, Nexus, SonarQube.

- Link lưu trữ tài liệu trên các hệ thống lưu trữ tài liệu KMS, Jira...

- Thoả thuận SLA.

- Tài liệu phục vụ kiểm định ATTT:

+ Hồ sơ đề xuất cấp độ (hoặc hồ sơ đề xuất cấp độ dự kiến).

+ Mã nguồn của phiên bản đem đi kiểm định ATTT dưới dạng bản điện tử. Mã nguồn cung cấp cần khớp với phiên bản đem đi kiểm định ATTT và đã loại bỏ các phần mã nguồn thừa. Trường hợp không cung cấp mã nguồn, trong văn bản đề nghị kiểm định, Lãnh đạo đơn vị cần xác nhận về việc không cung cấp mã nguồn và hoàn toàn chịu trách nhiệm khi phát hiện các điểm yếu, lỗ hổng có nguồn gốc từ mã nguồn.

+ Bản đóng gói đã được cài đặt trên môi trưởng kiểm thử.

+ Các tài khoản có khả năng truy cập ứng dụng (ví dụ tài khoản khách, người dùng hỗ trợ, quản trị ứng dụng và các tài khoản khác nếu có).

+ Thông tin các máy chủ (IP, phiên bản hệ điều hành, tài khoản có đặc quyền administrator/root).

+ Thiết lập kết nối theo yêu cầu.

+ Các thông tin khác (nếu cần).

- Các tài liệu khác (nếu có).

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 sau khi đưa vào sử dụng.

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

a) Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

b) Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt.

4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

a) Bên triển khai xây dựng kế hoạch, nội dung đánh giá, kiểm tra hệ thống theo quy định, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện kiểm tra, đánh giá an toàn thông tin.

b) Hệ thống phải được thực hiện kiểm tra, đánh giá an toàn thông tin trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt.

5. Trong quá trình thực hiện thử nghiệm và nghiệm thu hệ thống, giao cho bộ phận chuyên trách an toàn thông tin mạng là đầu mối phối hợp với đơn vị phát triển để triển khai thực hiện.

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

Điều 9. Quản lý an toàn hạ tầng mạng

1. Quản lý, vận hành hoạt động bình thường của hạ tầng mạng.

a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các nguy cơ, rủi ro và duy trì an toàn cho các máy tính, ứng dụng sử dụng mạng:

- Có sơ đồ logic và vật lý về hệ thống mạng, tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

- Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy cập từ bên ngoài

mạng và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

c) Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp.

d) Mạng không dây (WIFI), thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

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

- Phải có phương án dự phòng đường truyền mạng, thiết bị mạng để đảm bảo tính sẵn sàng đáp ứng yêu cầu hoạt động của hệ thống mạng.

- Triển khai hệ thống/phương tiện lưu trữ độc lập để lưu trữ các thông tin cấu hình thiết bị mạng, kết nối, định danh trong mạng để khôi phục sau khi xảy ra sự cố.

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin 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) Cán bộ quản lý, nhân viên 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 cho cán bộ quản lý 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 10. Quản lý an toàn mạng

1. Công chức, người lao động trong cơ quan khi sử dụng máy tính trong nội bộ không được tự ý thay đổi địa chỉ IP và địa chỉ Default gateway đã được mặc định.

2. Không được tự ý lắp đặt thiết bị thu, phát sóng Wifi (Access Point Router Wifi) vào mạng khi chưa thống nhất với cán bộ phụ trách công nghệ thông tin.

3. Thiết bị không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; Sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố.

4. Không cung cấp mật khẩu của các thiết bị phát sóng Wifi trong mạng nội bộ ra bên ngoài, trừ các đoàn trực tiếp đến làm việc tại đơn vị.

5. Việc sử dụng mạng riêng ảo (VPN- Vitual Private Network) khi có nhu cầu cần làm việc từ xa, bắt buộc phải đặt mật khẩu với độ an toàn cao theo quy định của Khoản 7, điều 10 và thay đổi mật khẩu tối thiểu 03 tháng/lần.

6. Hạn chế tối đa sử dụng chức năng chia sẻ tài nguyên trên các máy tính cá nhân(sharing), trừ máy in. Trường hợp cần thiết sử dụng chức năng này, bắt buộc phải thiết lập mật khẩu và thực hiện việc thu hồi chức năng này khi sử dụng xong.

7. Không tự ý cắm usb khi máy tính đã nhiễm virut.

8. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

9. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; kiểm soát truy cập từ bên trong mạng; kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; phòng chống phần mềm độc hại trên môi trường mạng.

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.

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

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

- 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 công nghệ thông tin 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 Đơn vị/bộ phận chuyên trách về công nghệ thông tin của đơn vị 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 công nghệ thông tin của đơn vị.

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

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

7. Các máy chủ trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.

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.

e) 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;

a) Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

b) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

c) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

d) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

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.

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.

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

a) 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, dữ liệu, thông tin nghiệp vụ và các thông tin,

dữ liệu quan trọng khác trên hệ thống (nếu có).

b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.

c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

Điều 13. Quản lý an toàn thiết bị đầu cuối

1. Quy định về quản lý truy cập, sử dụng tài nguyên nội bộ

a) Cán bộ chuyên trách công nghệ thông tin có trách nhiệm quản lý các thiết bị công nghệ thông tin phục vụ công việc, hoạt động chung của UBND xã.

b) Công chức, viên chức, người lao động có trách nhiệm sử dụng và bảo quản các thiết bị công nghệ thông tin được cấp để phục vụ công việc hàng ngày.

c) Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu, tài liệu khi thay đổi mục đích sử dụng hoặc thanh lý, phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi.

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

đ) Người sử dụng được cấp tài khoản truy cập hệ thống khi có yêu cầu của lãnh đạo phòng, dưới sự giám sát, phân quyền của cán bộ chuyên trách.

e) Cài đặt tường lửa cá nhân để chặn các truy cập từ bên ngoài trái với quy định của cơ quan;

g) Cấu hình máy tính cá nhân chỉ được phép truy cập các thư mục lưu trữ dữ liệu của mình, không truy cập các thư mục lưu trữ dữ liệu của cá nhân khác trên máy tính dùng chung;

h) Sử dụng chức năng mã hóa dữ liệu, khóa thư mục để đề phòng trường hợp dữ liệu bị đánh cắp;

i) Hiển thị đầy đủ phần mở rộng của tập tin để không kích hoạt nhầm tập tin thực thi mà tập tin đó có thể là phần mềm có hại hoặc có chứa mã độc.

Điều 14. Phân nhóm sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

a) Hệ thống thông tin bị sự cố là hệ thống thông tin của UBND xã Phong Nha, các bộ phận thuộc UBND xã Phong Nha và bị một trong số các sự cố sau: 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; 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;...

b) Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý sự cố.

2. Sự cố an toàn thông tin thường gặp:

a) Sự cố do bị tấn công mạng;

b) Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, hosting,...;

c) Sự cố do lỗi của người quản trị, vận hành hệ thống, ...;

Điều 15. Quy trình ứng cứu sự cố an toàn thông tin mạng

Bước 1: Thông báo sự cố

Công chức, viên chức, người lao động tại các phòng, ban thuộc UBND xã Phong Nha, khi gặp sự cố trong quá trình sử dụng máy tính có kết nối mạng thực hiện thông báo ngay cho bộ phận đầu mối/cán bộ chuyên trách/bán chuyên trách công nghệ thông tin tại đơn vị (Bộ phận ứng cứu sự cố).

Bước 2: Tiếp nhận sự cố

Bộ phận ứng cứu sự cố tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp, .

Bước 3: Xác minh/xác nhận sự cố

Bộ phận ứng cứu sự cố triển khai tiến hành Xác minh/xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xảy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);

- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);

- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);

- Và địa điểm xảy ra sự cố.

Bước 4: Phân loại sự cố

Bộ phận ứng cứu sự cố có trách nhiệm phân loại sự cố:

- Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, hosting,.;

- Sự cố do lỗi của người quản trị, vận hành hệ thống;

- Sự cố do bị tấn công mạng nhưng trên phạm vi 01 máy tính, có thể khắc phục.

- Sự cố về tấn công thay đổi giao diện (deface);

- Sự cố về tấn công lừa đảo (phishing);

- Sự cố về tấn công phát tán mã độc (malware);

- Sự cố về tấn công từ chối dịch vụ (DoS/DDoS);

- Sự cố có yếu tố nước ngoài (hợp tác quốc tế);

- Sự cố tấn công khác.

Bước 5: Báo cáo lãnh đạo, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự Bộ phận ứng cứu sự cố có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành xử lý.

- Trường hợp sự cố được phân loại thông thường thì Bộ phận ứng cứu sự cố báo cho các bên liên quan để tiếp tục triển khai theo phương án ứng cứu sự cố an toàn thông tin mạng thông thường theo quy trình ứng cứu sự cố thông thường của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017; báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng tỉnh để phối hợp xử lý.

- Trường hợp sự cố được phân loại nghiêm trọng thì gửi báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng tỉnh về sự cố nghiêm trọng để có phương án ứng cứu; và tổ chức ứng cứu, xử lý sự cố: các đơn vị tham gia lực lượng ứng cứu; nguồn lực cần thiết để ứng cứu sự cố; dự kiến triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp và thực hiện tiếp các bước tiếp theo quy định tại Điều 14 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.

Bước 6: Phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh: Thu thập thông tin phục vụ phân tích sự cố; Phân tích sự cố; Xử lý sự cố; Khôi phục, kiểm tra, báo cáo, tổng kết, đánh giá.

Điều 16. Kế hoạch ứng phó sự cố an toàn thông tin mạng

1. Điều kiện, nguyên tắc, phương châm ứng phó sự cố

a) Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin (ATTT) mạng.

b) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

c) Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan, đơn vị, ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

d) Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của hệ thống thông tin đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.

e) Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

f) Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố.

2. Các bộ phận vận hành, quản lý hệ thống thông tin cần thực hiện thường xuyên việc đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm cả đơn vị đã ký hợp đồng cung cấp dịch vụ nếu có).

3. Triển khai các nội dung phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin.

4. Các bộ phận quản lý, vận hành hệ thống thông tin tổ chức triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố theo quy định.

5. Đầu tư trang thiết bị bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố: Căn cứ điều kiện, tình hình thực tế tại đơn vị từ đó chủ động trang bị thiết bị, công cụ, phương tiện cần thiết để phục vụ ứng phó sự cố ATTT mạng; chuẩn bị các điều kiện bảo đảm, sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

Điều 17. Quản lý giám sát an toàn hệ thống thông tin

1. Công chức, viên chức và người lao động khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho cán bộ chuyên trách/bán chuyên trách của các đơn vị để kịp thời xử lý.

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

3. Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

Điều 18. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm phải được trang bị phần mềm phòng chống mã độc. 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. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) ….

3. Các cán bộ, công chức trong đơn vị 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. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Khi phát hiện ra bất kỳ dấu hiện 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.

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

7. Định kỳ hằng 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.

Điều 19. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

4. Định kỳ hằng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9 Thông tư số 31/2017/TT-BTTTT.

5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

Điều 20. Quản lý điểm yếu an toàn thông tin

1. Cán bộ chuyên trách về an toàn thông tin có trách nhiệm:

a) Quản lý thông tin điểm yếu an toàn thông tin 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 Lãnh đạo UBND xã Phong Nha tỉnh Quảng Trị ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin 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 an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Có trách nhiệm 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 đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện 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.

3. Định kỳ hằng 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.

4. 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 và Điều 11 Thông tư số 12/2022/TT-BTTTT.

Điều 21. Quản lý an toàn người sử dụng đầu cuối

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 an toàn thông tin 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 an toàn thông tin.

c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

d) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, thiết bị di động thông minh) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích riêng. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

e) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét mã độc trước khi đọc hoặc sao chép dữ liệu.

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 an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) 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 an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

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

Điều 22. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

1. Khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống phải được bộ phận chuyên trách an toàn thông tin thực hiện kiểm tra, đánh giá bảo đảm an toàn thông tin.

2. Quá trình xử lý thông tin trên hệ thống phải được thực hiện khi thay đổi mục đích sử dụng hoặc gỡ bỏ theo phương án kỹ thuật được lãnh đạo UBND xã Phong Nha tỉnh Quảng Trị phê duyệt.

CHƯƠNG IV
KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN

Điều 23. 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 của tỉnh;

b) Đội ứng cứu sự cố an toàn thông tin mạng tỉnh;

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 24. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro

a) Nhận biết tài sản thông qua xác định và thu thập thông tin đầy đủ về tài sản của mình đang quản lý, đặc biệt là các thông tin liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản. Đánh giá các nguy cơ, điểm yếu đối với tài sản đó, từ đó có thể đánh giá xem mỗi tài sản khi gặp rủi ro thì sẽ gây ra hậu quả, mức độ ảnh hưởng thế nào đối với cơ quan, tổ chức

b) Phân loại nhóm các điểm yếu: Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu an toàn thông tin trong hệ thống; Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: Không có quy định về sử dụng mật khẩu an toàn; không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố, không có quy định về bảo đảm an toàn thông tin phía người sử dụng.v.v.; Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: Không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công.v.v.; Nhóm các điểm yếu khác liên quan đến các nguy cơ mất an toàn thông tin từ bên thứ ba.

c) Phân loại các mối đe dọa: Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật.

d) Đánh giá hậu quả và khả năng xảy ra sự cố, xác định mức rủi ro bao gồm các mức thấp, trung bình, cao, rất cao, cực cao.

2. Quy trình đánh giá và quản lý rủi ro bao gồm 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý rủi ro; (4) Chấp nhận rủi ro và 02 quá trình cần thực hiện song song: Truyền thông và tư vấn rủi ro, Giám sát và soát xét rủi ro.

3. Biện pháp kiểm soát rủi ro được thực hiện theo yêu cầu an toàn cơ bản trong Hồ sơ đề xuất cấp độ của Hệ thống thông tin được cấp có thẩm quyền phê duyệt.

CHƯƠNG V
TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG

Điều 25. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) Xây dựng phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;

b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng

đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý;

c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng;

d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ trực tuyến, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác;

đ) Triển khai kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

2. Người đứng đầu cơ quan, đơn vị có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

3. Lực lượng bảo vệ an ninh mạng của UBND xã Phong Nha tỉnh Quảng Trị.

CHƯƠNG VI
TỔ CHỨC THỰC HIỆN

Điều 26. Tổ chức triển khai Quy chế

1. Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

2. Các tổ chức, đơn vị thuộc UBND xã, đơn vị sự nghiệp trực thuộc UBND xã tổ chức phổ biến, quán triệt và triển khai thực hiện Quy chế này.

Điều 27. Xây dựng, rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi Quy chế bảo đảm an toàn thông tin không còn phù hợp với tình hình thực tế thì tiến hành rà soát, cập nhật, bổ sung, ban hành Quy chế mới. Quy chế được thông qua Lãnh đạo UBND xã, các phòng, đơn vị trực thuộc trước khi công bố áp dụng.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các phòng đơn vị trực thuộc phản ánh kịp thời về UBND xã Phong Nha tỉnh Quảng Trị (qua Văn phòng UBND xã) để xem xét, bổ sung, sửa đổi.

Điều 28. Bộ phận chuyên trách về an toàn thông tin

1. Giao cán bộ quản trị mạng là công chức Văn phòng UBND xã là bộ phận chuyên trách về ATTT cho hệ thống.

2. Văn phòng UBND xã chủ trì, phối hợp với các tổ chức, đơn vị thuộc UBND xã và đơn vị trực thuộc UBND xã tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo chỉ đạo của Chủ tịch UBND xã Phong Nha tỉnh Quảng Trị./.