ỦY BAN NHÂN DÂN **XÃ LINH THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:122/ QĐ-UBND	*Linh Thông, ngày 10 tháng 9 năm 2024*

QUYẾT ĐỊNH

V/v Ban hành Quy chế quản lý, sử dụng mạng máy tính nội bộ và các thiết bị công nghệ thông tin và bảo đảm an toànthông tin mạng trong hoạt động ứng dụng công nghệ thông tincủa UBND xã Linh Thông

ỦY BAN NHÂN DÂN XÃ LINH THÔNG

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19 tháng 6 năm 2015;Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức Chính quyền địa phương số 47/2019/QH14 ngày 22/11/2019;

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 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính Phủ Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về đảm bảo an toàn Hệ thống mạng nội bộ theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của 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 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 5742/QĐ-UBND ngày 06/9/2024 của huyện Định Hoá về việc 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 trên địa bàn huyện Định Hoá;

Theo đề nghị của công chức Văn phòng – Thông kê

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, sử dụng mạng máy tính nội bộ và các thiết bị công nghệ thông tin và bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của UBND xã Linh Thông.

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

Điều 3. Lãnh đạo UBND xã, Công chức Văn phòng – Thông kê, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND huyện Định Hoá;
- Phòng Văn hóa và Thông tin;
- TT Đảng uỷ;
- TT HĐND;
- Lãnh đạo UBND;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Lưu Viết Viên

UỶ BAN NHÂN DÂN **XÃ LINH THÔNG**	**CỘNGHÒAXÃHỘICHỦNGHĨAVIỆTNAM** **Độclập-Tựdo-Hạnhphúc**

QUYCHẾ

Quản lý, sử dụng mạng máy tính nội bộ và các thiết bị công nghệ thông tin và bảo đảm an toànthông tin mạng trong hoạt động ứng dụng công nghệ thông tincủa UBND xã Linh Thông

(Ban hành theo Quyết đinh số:122 /QĐ-UBND ngày 10/ 9 /2024 của UBND xã Linh Thông)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

1. Quy chế này quy định việc quản lý, sử dụng hệ thống mạng máy tính nội bộ và các thiết bị CNTT tại UBND xã Linh Thông.

2. Áp dụng đối với cán bộ, công chức của xã Linh Thông trong việc quản lý, sử dụng mạng nội bộ (LAN) và mạng Internet.

Điều 2. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Việc áp dụng Quy chế này nhằm xã ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong quá trình ứng dụng CNTT trong hoạt động của đơn vị;

2. Hoạt động ứng dụng CNTT của đơn vị phải tuân thủ theo nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng số 86/2015/QH15 ngày 19/11/2015, cụ thể như sau:

a) Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật; bảo đảm quốc xã, an ninh quốc gia, bí mật nhà nước; giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội;

b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác;

c) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức;

d) Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 3. Giải thích từ ngữ

1. *Mạng* được quy định tại Khoản 2 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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;

2. *An toàn thông tin mạng* được quy định tại Khoản 1 Điều 3 Luật An toàn

thông tin mạng, cụ thể: An toàn thông tin mạng là sự 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;

3. *Hệ thống thông tin* được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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. *Xâm phạm an toàn thông tin mạng* được quy định tại Khoản 6 Điều 3 Luật An toàn thông tin mạng, cụ thể: Xâm phạm an toàn thông tin mạng là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin;

5. *Sự cố an toàn thông tin mạng* được quy định tại Khoản 7 Điều 3 Luật An toàn thông tin mạng, cụ thể: Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng;

6. *Rủi ro an toàn thông tin mạng* được quy định tại Khoản 8 Điều 3 Luật An toàn thông tin mạng, cụ thể: Rủi ro an toàn thông tin mạng là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng;

7. *Phần mềm độc hại* được quy định tại Khoản 11 Điều 3 Luật An toàn thông tin mạng, cụ thể: Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin;

8. *Nguy cơ mất an toàn thông tin mạng* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng;

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015, cụ thể:

a) Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật;

b) Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng;

c) Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin;

d) Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả

mạo, lừa đảo;

đ) Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân;

e) Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

2. Tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point) vào mạng máy tính của cơ quan, đơn vị và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card, wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan, đơn vị;

3. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia; trật tự, an toàn xã hội và lợi ích quốc gia trên mạng; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc…

4. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

5. Tự ý tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

Điều 5.Thống nhất các thuật ngữ sử dụng

1. Thiết bị công nghệ thông tin: Là toàn bộ các thiết bị, máy móc có liên quan đến CNTT như: Máy vi tính (PC, laptop và Server), máy in, máy scan, máy chiếu, ổ cứng, thẻ nhớ (USB), camera, máy ảnh, thiết bị mạng (moden, switch,…), hệ thống cáp mạng.

2. Tài nguyên mạng: Là toàn bộ cácphần mềm dùng chung chạy trên mạng nội bộ của UBND xã gồm: Hệ thống dữ liệu dùng chung của tỉnh, huyện; tài liệu có nội dụng chuyên môn, nghiệp vụ,... được lưu trữ trên máy tính cá nhân (PC).

3. Người sử dụng: Cán bộ, công chức xã Linh Thông sử dụng thiết bị công nghệ thông tin (CNTT) được cấp tài khoản sử dụng gồm; tên người sử dụng (Username) và mật khẩu (Password) để khai thác tài nguyên mạng nội bộ của Xã thông qua mạng LAN, mạng Internet.

4. Quản trị mạng cơ quan: Là công chức được giao nhiệm vụ quản lý hệ thống thiết bị CNTT, duy trì sự hoạt động máy tính nội bộ, hướng dẫn người sử dụng thiết bị CNTT và khai thác tài nguyên phục vụ công tác; xử lý các tình huống khi có sự cố xảy ra để tránh mất an toàn thông tin trên môi trường mạng.

CHƯƠNG II
QUẢN LÝ, SỬ DỤNG MẠNG VÀ THIẾT BỊ CNTT

Điều 6. Quản lý mạng máy tính

Công chức được giao phụ trách quản trị mạng của xã (công chức phụ trách CNTT, chuyển đổi số của đơn vị)có trách nhiệm quản lý trang thiết bị, các ứng dụng phần mềm sử dụng chung để khai thác tài nguyên mạng; trực tiếp theo dõi, giám sát việc sử dụng các dịch vụ mạng máy tính của cơ quan; cấp quyền, phân quyền truycập cho công chức, viên chức một số phần mềm kết nối với máy tính vào mạng máy tính xã để khai thác, sử dụng thông tin phục vụ yêu cầu công tác theo hướng dẫn kỹ thuật của quản trị mạng.

Điều 7.Truy cập mạng, khai thác cơ sở dữ liệu

1. Việc truy cập vào mạng nội bộ phải xuất phát từ yêu cầu phục vụ công tác quản lý, điều hành tác nghiệp của xã.

2. Trường hợp có sự thay đổi vị trí làm việc của công chức, viên chức việc giữ nguyên hoặc thay đổi các tài khoản đã cài đặt trên máy tính phải thông báo đến Quản trị mạng để phối hợp, tiến hành thay đổi.

3. Cá nhân truy cập từ xa vào mạng nội bộ của xã có trách nhiệm bảo mật thông tin, thông số kỹ thuật kết nối mạng. Nghiêm cấm việc cung cấp, tiết lộ để lọt thông tin ra bên ngoài.

4. Khi khai thác, sử dụng các phần mềm như: phần mềm QLVB, hòm thư công vụ*)*, phần mềm quản lý cán bộ công chức, xử lý kiến nghị cử tri,…tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong các trình duyệt.

5. Không truy cập các trang web không biết rõ nguồn gốc; không được xâm nhập trái phép vào các máy trạm của các xã, đơn vị và các máy trạm trong hệ thống của xã, trừ trường hợp được sự thỏa thuận chia sẻ thông tin.

Điều 8. Đảm bảo an toàn, an ninh thông tin

1. Cài đặt phần mềm xã, chống virus, mã độc cho tất cả các máy tính trong mạng nội bộ của cơ quan, đơn vị, thiết lập chế độ cập nhật hàng ngày cho phần mềm này.

2. Khi sử dụng các phần mềm dùng chung của tỉnh được cấp tài khoản phải đổi mật khẩu khi được cấp mới, thường xuyên định kỳ thay đổi mật khẩu với mật độ cao.

3. Hạn chế sử dụng chức năng chia sẻ thư mục (Sharing). Khi sử dụng chức năng này thiết lập cơ chế chỉ đọc (Read Only) đối với những thư mục được chia sẻ trong mạng nội bộ. Chỉ sử dụng cơ chế cho phép toàn quyền đọc, ghi (Read, Write) khi thật cần thiết yêu cầu phải sử dụng mật khẩu khi truy cập thư mục chia sẻ và thực hiện thu hồi chức năng này sau khi đã sử dụng xong.

4. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ

nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

Điều 9. Bảo vệ bí mật Nhà nước

1. Không được sử dụng máy tính nối mạng để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nộidung thuộc bí mật nhà nước; cung cấp tin, tài liệuvà đưa thông tin bí mật nhà nước trên mạng.

2. Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kế tnối mạng; tuân thủ Pháp lệnh bảo vệ bí mật Nhà nước và các quy định khác có liên quan của Nhà nước về công tác bảo vệ bí mật nhà nước.

3. Khi sửa chữa, khắc phục các sự cố của máytính dùng soạn thảo văn bản mật, phải báo cáo Lãnh đạo xã và có sự giám sát, quản lý chặt chẽ.

Điều 10. Quyền lợi và trách nhiệm của người sử dụng thiết bị CNTT

1. Người sử dụng tài sản trang thiết bị CNTT có quyền và trách nhiệm trong việc khai thác, bảo quản, sử dụng hiệu quả, không sử dụng vào các mục đích riêng.

2. Trong quá trình làm việc, khi xảy ra sự cố, hư hỏng đối với các thiết bị CNTT phải liên hệ trực tiếp với cán bộ phụ trách CNTT để khắc phục sự cố.

3. Việc sử dụng trang thiết bị CNTT phải tuân thủ các quy định sau:

- Không tự ý tháo,lắp máy tính các thiết bị CNTT.

- Không cài đặt các phần mềm,chương trình kh ichưa rõ nguồn gốc và chưa được sự nhất trí của người có thẩm quyền.

- Không để nước, vật dụng dễ cháy nổ gần thiết bị CNTT.

- Bảo quản các thiết bị CNTT trong xã làm việc, thường xuyên lau chùi, vệ sinh thiết bị.

- Không tắt, khởi động máy tính đột ngột bằng công tắc cứng, rút nguồn điện đột ngột.

- Không cho người ngoài cơ quan sử dụng các thiết bị CNTT của cơ quan.

- Không tự ý vận chuyển các thiết bị CNTT ra khỏi cơ quan khi chưa được sự cho phép của Lãnh đạo xã.

Điều 11. Quyền lợi và trách nhiệm của người sử dụng dịch vụ mạng

1. Người sử dụng được cấp quyền sử dụng các phần mềm nghiệp vụ trong mạng máy tính nội bộ của cơ quan và phải bảo vệ quyền truy cập của mình.

2. Việc sử dụng mật khẩu đối với các phần mềm nghiệp vụl à bắt buộc, cán bộ công chức chịu trách nhiệm về tài khoản mình được cấp.

3. Khi kết thúc làm việc với các phần mềm nghiệp vụ trong mạng, nhất thiết phải thực hiện thao tác thoát khỏi ứng dụng hoặc dịch vụ mạng trước khi rời khỏi máy, không được để máy trong tình trạng đang truy cập vào ứng dụng khi mình vắng mặt, nhằm tránh trường hợp bị lợi dụng tài khoản tên đăng kí và mật khẩu.

4. Trong quá trình làm việc, khi xảy ra sự cố đối với các ứng dụng nghiệp vụ chạy trên mạng, phải liên hệ trực tiếp với quản trị mạng để khắc phục sự cố.

5. Nghiêm cấm các hành vi sau đây:

- Sử dụng tên đăng kí và mật khẩu của người khác khi không đượcủy quyền, cho phép.

- Tự ý tìm cách thâm nhập và đọc những tài liệu nằm ngoài phạm vi được phép của mình.

- Đưa những dữ liệu chứa virus làm thay đổi hệ thống, các chương trìnhgây nghẽn mạch đường truyền.

- Sử dụng hệ thống mạng để tiết lộ thông tin ra bên ngoài.

Điều 12. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Phân công bộ phận chuyên trách về an toàn thông tin:

Giao công chức phụ trách về CNTT của xã đồng thời là bộ phận chuyên trách về an toàn thông tin.

Cán bộ, công chức được giao là đầu mối, liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền, liên quan tham mưu các biện pháp quản lý, vận hành và bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy định an toàn thông tin của cơ quan có thẩm quyền cụ thể:

1.1. UBND xã Linh Thông

- Người đại diện: Lưu Viết Viên; Chức vụ: Chủ tịch UBND xã

- Thông tin liên hệ: Hoàng Văn Trinh, Công chức Văn phòng - Thống kê.

-Số điện thoại: 0943912986.

Thư điện tử: Trinhhv.dinhhoa@thainguyen.gov.vn

1.2.UBND tỉnh Thái Nguyên

- Người liên hệ/bộ phận: Trung tâm Công nghệ Thông tin Sở Thông tin và Truyền thông tỉnh Thái Nguyên

- Số điện thoại: 0208.3501.260

- Email: ict@thainguyen.gov.vn

a) UBND tỉnh Thái Nguyên giao Sở Thông tin và Truyền thông là đầu mối liên hệ, phối hợp với các cơ quan, đơn vị có thẩm quyền quản lý về ATTT.

b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn

- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

2. Trách nhiệm của bộ phận chuyên trách về an toàn thông tin:

a. Là đầu mối liên hệ, tiếp nhận, phối hợp với các cơ quan, tổ chức (có thẩm quyền quản lý về an toàn thông tin) trong công tác đảm bảo an toàn thông tin, hỗ trợ điều phối xử lý sự cố an toàn thông tin;

b. Là đầu mối liên hệ, phối hợp với Thông tin và Truyền thông và 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 các Hệ thống Thông tin do đơn vị triển khai;

c. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền;

d. Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ Xã;

đ. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả;

e. Phối hợp chặt chẽ với Phòng Văn hoá và Thông tin huyện, Công an huyện, Sở Thông tin và Truyền thông tỉnh và các đơn vị liên quan trong công tác xã ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng;

f. Định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Phòng Văn hoá và Thông tin huyện, Sở Thông tin và Truyền thông (theo hướng dẫn của cơ quan có thẩm quyền).

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

Điều 13.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.

6. Có 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 an toàn thông tin trước khi triển khai thực hiện.

Điều 14. 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.

5. Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh

giá an toàn thông tin cho phần mềm.

6. Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

Điều 15. 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 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 IV
BẢO ĐẢM AN TOÀN THÔNG TIN TRONGQUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 16. Quản lý an toàn mạng

1. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

2. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 03 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.

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

a. Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy tính 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 xã chống xâm nhập giữa các vùng mạng quan trọng.

h. Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

i. Triển khai phương án cảnh báo thời gian thực trực tiếp đến người

quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

4. Cập nhật, sao lưu dự xã 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 tính để sao lưu dự xã; 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 xã các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b. Triển khai phương án dự xã cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự xã phải đáp ứng theo quy mô hoạt động của hệ thống.

c. Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d. Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

5. Truy cập và quản lý cấu hình hệ thống

a. Cán bộ quản lý, vận hành truy cập, khai thác thông tin tạihệ thống 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, 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 cấp có thẩm quyền 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.

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

7. 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; xã chống xâm nhập giữa các vùng mạng; Xã chống phần mềm độc hại trên môi trường mạng;

8. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng;

9. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế xã chống vi rút tin học, thư rác cho những hệ thống xung yếu và máy tính trong hệ thống;

10. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy;

11. Đối với các thiết bị mạng chính

a. Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét (do nhà cung cấp thực hiện): một cho đường cung cấp điện và một cho đường mạng nội bộ (LAN);

b. Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin học của cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security);

c. Tường lửa (firewall): Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu vào, ra và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS);

12. Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự xã;

13. Có biện pháp bảo vệ, dự xã, xã chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.

Điều 17. Quản lý xã chống phần mềm độc hại

1. Tất cả các máy tính phải được trang bị phần mềm xã chống mã độc. Các phần mềm xã 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 cơ quan phải được hướng dẫn về xã 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 xã 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 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.

Điều 18. 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 hàng 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 19. Quản lý điểm yếu an toàn hệ thống thông tin

1. Bộ phận 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, 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/Cán bộ quản lý 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 giám 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;

đ. 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. 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;

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 và Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của 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;

Điều 20. Quản lý an toàn dữ liệu

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

a. Đơn vị phải 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. Sao lưu dự xã và khôi phục dữ liệu (tần suất sao lưu dự xã, 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).

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

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

7. Có cơ chế sao lưu dữ liệu dự xã, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy tính công vụ được sao lưu thông qua hệ thống sao lưu dữ liệu.

8. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự xã: tập tin cấu hình hệ thống, bản dự xã hệ điều hành máy tính, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

9. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

10. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn;

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

1. 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 virus trước khi đọc hoặc sao chép dữ liệu.

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

3. Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Công chức được giao về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa; theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc; cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

7. 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.

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.

8. 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 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.

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

10. Đối với cán bộ, công chức thay đổi công tác hoặc nghỉ chế độ:

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi tài khoản, đóng tài khoản và 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) của tổ chức;

b) Có quy trình và thực hiện vô hiệu hóa tấ tcả 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.

Điều 22. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin:

a. Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan như: máy tính trạm bị nhiễm phần mềm độc hại, phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi;

b. Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 (một) cá nhân hoặc xãbị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 xã;

c. Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như: một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa,…) bị hư hỏng;

d. Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin:

Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a. Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quanquản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông tỉnh quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3;

b. Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3;

c. Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông tỉnh và thực hiện

tiếp Bước 4;

d. Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông tỉnh và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ. Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan xã TRUNG HỘIphải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông tỉnh để được hướng dẫn, hỗ trợ.

3. Bộ phận chuyên trách về an toàn thông tin có trách nhiệm (công chức được giao phụ trách)

a. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP 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. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

c. Phối hợp với các đơn vị chức năng xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg;

d. Phối hợp với các đơn vị chuyên trách về an toàn thông tin đưa ra cảnh bảo sớm về nguy cơ mất an toàn thông tin trong hệ thống.

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

f. 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; 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;

g. Quyết định toàn diện về mặt kỹ thuật trong quá trình khắc phục sự cố về an toàn thông tin; hỗ trợ, phối hợp và hướng dẫn các cán bộ, công chức khác trong đơn vị khắc phục sự cố mất an toàn thông tin; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về an toàn thông tin; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo;

h. 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; 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.

4. Trách nhiệm của người dùng:

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về an toàn thông tin của cơ quan khi phát hiện các sự cố gây mất an toàn thông tin trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

Điều 23. Quản lý truy cập

1. Đối với các cá nhân có trách nhiệm:

a. Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị;

b. Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng;

c. Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả hệ thống máy tính của người sử dụng;

d. Hệ thống mạng không dây (wifi) của xã phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây;

đ. Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống, thiết bị mạng, máy tính, các ứng dụng;

e. Các đơn vị cần rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.

2. Đối với các hệ thống thông tin

a. Bảo đảm mỗi tài khoản của cá nhân truy cập vào hệ thống thông tin là duy nhất;

b. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản;

c. Đơn vị quản lý, vận hành các hệ thống dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người dùng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

Điều 24. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Cán bộ, công chức thực hiện việc ghi nhật ký trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết;

2. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống;

3. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 25. Sao lưu dữ liệu dự phòng

a. Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng. Khi lưu trữ, trao đổi thông tin, dữ liệu quan trọng phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự xã;

b. Phải lập kế hoạch và thực hiện sao lưu dữ liệu dự xã định kỳ ít nhất một lần trong tháng các dữ liệu quan trọng, bao gồm: cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh, các tập tin dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (như: đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

Điều 26. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Trường hợp hệ thống phải kết thúc vận hành, khai thác, thanh lý, hủy bỏ, Bộ phận được giao vận hành hệ thống tham mưu lãnh đạo xã phương án thực hiện. Trong đó cần làm rõ:

a) Lý do kết thúc vận hành, khai thác, thanh lý, hủy bỏ và phương án thay thế (nếu có).

b) Phương án xử lý xóa bỏ các thông tin, dữ liệu: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối, phương tiện lưu trữ chứa thông tin, dữ liệu cần xóa. Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung cần đề xuất xử lý, các thư mục chứa dữ liệu sao lưu cần xóa dữ liệu…, phương thức xóa bỏ thông tin, dữ liệu, bảo đảm thông tin, dữ liệu được xóa hoàn toàn, không thể khôi phục trên các máy chủ, thiết bị, phương tiện lưu trữ.

c) Phương án gỡ bỏ các phần mềm, ứng dụng hoặc dịch vụ có liên quan: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối có cài đặt

phần mềm, ứng dụng hoặc dịch vụ có liên quan đến hệ thống cần thực hiện gỡ bỏ.Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung đề xuất xử lý, phương thức xử lý bảo đảm phần mềm, ứng dụng, dịch vụ được xóa hoàn toàn, không thể phục hồi trên các máy chủ, thiết bị mạng, thiết bị đầu cuối có liên quan.

d) Danh mục các máy chủ, thiết bị mạng, thiết bị đầu cuối, thiết bị lưu trữ cần thanh lý (nếu có), làm rõ phương án thanh lý. Các máy tính công vụ, thiết bị mang, thiết bị đầu cuối, thiết bị lưu trữ cần được xử lý xóa bỏ thông tin, dữ liệu, gỡ bỏ phầnmềm, ứng dụng, dịch vụ trước khi tiến hành thanh lý.

2. Trình tự, thủ tục thực hiện: Sau khi được sự đồng ý bằng văn bản của cơ quan có thẩm quyền, lãnh đạo đơn vị thực hiện thanh lý, hủy bỏ hệ thống theo đúng các quy định tại Điều 29, Điều 30 Nghị định số 151/2017/NĐ-CP ngày 26/12/2017 của Chính phủ quy định chi tiết một số điềucủa Luật quản lý, sử dụng tài sản công.

Điều 27.Quản lý rủi ro an toàn thông tin

1. Thiếtbị CNTT phải đặt tên và dán nhãn theo đúng quy định.

2. Đơn vị vận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị CNTT hàng quý.

3. Đơn vị vận hành đề xuất mua thêm thiết bị CNTT và các thiết bị phụ trợ khác trong trường hợp thiết bị hết bảo hành bị hỏng. Thiết bị được trang bị phải tuân theo các tiêu chuẩn (theo yêu cầu của từng hệ thống).

4. Đối với thiết bị hỏng còn bảo hành, đơn vị vận hành, khai thác yêu cầu đơn vị cung cấp sửa chữa. Thiết bị hỏng đã hết bảo hành, đơn vị vận hành báo cáo cơ quan quản lý về phương án sửa chữa.

5. Trường hợp thiết bị hỏng là thiết bị quan trọng (máy tính công vụ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị tường lửa), đơn vị vận hành phải báo cáo ngay về cơ quan quản lý để có biện pháp khắc phục nhanh.

CHƯƠNGV
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 28. Chế độ báo cáo

1. Báo cáo định kỳ

Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại Thông tư số 12/2022/TT-BTTTT của 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, cụ thể như sau:

- Tình hình an toàn thông tin của hệ thống thông tin trong kỳ báo cáo;

- Tiến độ triển khai, áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

- Hiệu quả áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ

sơ xác định cấp độ đã được phê duyệt;

- Đề xuất thay đổi cấp độ, phương án bảo đảm an toàn hệ thống thông tin (nếu có);

- Nội dung khác phục vụ công tác bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Báo cáo đột xuất

Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

CHƯƠNG VI
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 29. Trách nhiệm của xã Linh Thông

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin (UBND tỉnh) phân công;

2. Lãnh đạo xã Linh Thông có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND tỉnh, UBND huyện trong công tác bảo đảm an toàn thông tin mạng của địa phương;

3. Phân công công chức bảo đảm an toàn thông tin mạng của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ về an toàn thông tin mạng; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin mạng đối với các vị trí cần tuyển dụng hoặc phân công;

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả;

5. Phối hợp chặt chẽ với các đơn vị liên quan trong công tác xã ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng;

6. Định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Phòng Văn hoá và Thông tin huyện, Sở Thông tin và Truyền thông tỉnh (theo hướng dẫn của cơ quan có thẩm quyền).

Điều 30. Trách nhiệm

1. Trách nhiệm của cán bộ, công chức phụ trách quản lý vận hành hệ thống và an toàn thông tin mạng tại xã Linh Thông:

a. Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị;

b. Tham mưu cho lãnh đạo UBND xã ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c. Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d. Phối hợp với các tổ chức, cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin;

đ. 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;

e. Phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin;

2. Trách nhiệm của cán bộ, công chức thuộc xã Linh Thông:

a. Nghiêm túc chấp hành các quy định tại quy chế này 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. Khi tham gia vận hành mạng máy tính của cơ quan phải nghiêm chỉnh chấp hành chế độ bảo mật, an ninh, an toàn thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin có nội dung "mật", "tối mật" và "tuyệt mật" lên hệ thông máy tính có kết nối mạng Internet;

c. Trong trao đổi thông tin, dữ liệu phục vụ công việc, cán bộ, công chức phải sử dụng hệ thống thông tin do cơ quan có thẩm quyền triển khai như: hệ thông thư điện tử tỉnh (@thainguyen.gov.vn); hệ thống quản lý văn bản và điều hành. Mỗi cán bộ, công chức không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,... để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, đơn vị;

d. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và công chức chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý;

đ. Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do cơ quan hoặc Sở Thông tin và Truyền thông tỉnh tổ chức;

e. Đối với cán bộ, công chức trong cơ quan vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật, xử phạt hành chính, bồi thường thiệt hại hoặc bị truy cứu trách nhiệm hình sự theo quy định hiện hành.

3. Cán bộ, công chức trong cơ quan phải tham gia các hoạt động, công tác bảo đảm an toàn thông tin do các đơnvị có thẩm quyền tổ chức. Tham gia phổ biến, tuyên truyền, quán triệt các văn bản, quy định về an toàn thông tin nhằm

nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức do lãnh đạo xã thực hiện hoặc cơ quan có chức năng vền an toàn bảo mật thông tin tổ chức...

4. Đối với các cơ quan, địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống mạng LAN 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.

CHƯƠNG VII
ĐIỀU KHOẢN THI HÀNH

Điều 31.Tổ chức thực hiện

Lãnh đạoxã, cán bộ, công chức thuộc UBND xã Linh Thông căn cứ các quy định trên triển khai thực hiện.Trong quá trình thực hiện có vấn đề phát sinh, vướng mắc cần kịp thời báo cáo lãnh đạo UBND xã để giải quyết.

Điều 32. Xử lývi phạm

Các hành vi vi phạm quy định tại Quy chế này, tùy theo mức độ vi phạm mà bị xử lý theo các quy định của pháp luật hoặc quy định khen thưởng, kỷ luật của cơ quan.

Điều 33. Rà soát, sửa đổi, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi về chính sách ATTT, lãnh đạo đơn vị và các bộ phận liên quan có trách nhiệm kiểm tra tính phù hợp của Quy chế này và thực hiện rà soát, cập nhật bổ sung đảm bảo đúng với quy định của pháp luật.

2. Trong quá trình thực hiện Quy chế này, nếu có vướng mắc hoặc phát sinh mới, đề nghị bộ phận phụ trách CNTT có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo nhà trường theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

Điều 34.Hiệu lực thực hiện

1. Quy chế này có hiệu lực từ ngàyký. Trong quá trình thực hiện sẽ có sửa đổi, bổ sung cho phù hợp với thực tế.

2. Bộ phận chuyên môn (công chức phụ trách) có trách nhiệm tổng hợp những ý kiến đóng góp và đề xuất điều chỉnh, bổ sung nếu cần thiết.

3. Việc sửa đổi, bổ sung Quy chế này do UBND xã Linh Thông quyết định theo đề xuất của cán bộ, công chức được giao phụ trách./.