ỦY BAN NHÂN DÂN **XÃ CON CUÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:458/QĐ-UBND	*Con Cuông, ngày 31 tháng 3 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân tại xã Con Cuông

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ CON CUÔNG

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15 ngày 16 tháng 6 năm 2025;

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 số 116/2025/QH15 ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26 tháng 06 năm 2025;

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

Căn cứ Nghị định số 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 Kế hoạch số 33/KH-UBND ngày 16 tháng 01 năm 2026 của Ủy ban nhân dân tỉnh Nghệ An về triển khai thi hành Luật Bảo vệ dữ liệu cá nhân trên địa bàn tỉnh;

Căn cứ Công văn số 727/CAT-ANM ngày 09 tháng 2 năm 2026 của Công an tỉnh Nghệ An về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Trưởng phòng Văn hóa – Xã hội xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân tại UBND Xã Con Cuông.

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

Chánh Văn phòng HĐND-UBND xã, Trưởng Công an xã, Trưởng các phòng chuyên môn, Thủ trưởng các đơn vị sự nghiệp trực thuộc, toàn thể cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Công an tỉnh (để báo cáo);
- Thường trực Đảng ủy Xã (để báo cáo);
- Thường trực HĐND Xã (để báo cáo);
- Chủ tịch, các PCT UBND xã;
- Lưu: VT, VHXH (Như)

CHỦ TỊCH

U.B.N.D XÃ CON CUÔNG T. NGHỆ AN

Trần Anh Tuấn

ỦY BAN NHÂN DÂN
XÃ CON CUÔNG

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

QUY CHẾ
Bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân tại UBND xã Con Cuông

(Ban hành kèm theo Quyết định số 458/QĐ-UBND ngày 31 tháng 3 năm 2026 của Chủ tịch Trần Anh Tuấn)

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 kỹ thuật, nghiệp vụ nhằm bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân đối với các hệ thống thông tin thuộc quyền quản lý, sử dụng của Ủy ban nhân dân Xã Con Cuông (sau đây gọi tắt là các Hệ thống thông tin).

2. Đối tượng áp dụng:

a) Các phòng, ban, đơn vị trực thuộc, cán bộ, công chức, viên chức và người lao động làm việc tại Ủy ban nhân dân Xã Con Cuông;

b) Cơ quan, tổ chức, cá nhân có kết nối, khai thác, sử dụng các Hệ thống thông tin của Xã;

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, an toàn thông tin mạng và xử lý dữ liệu cá nhân phục vụ hoạt động của Ủy ban nhân dân Xã.

Điều 2. Mục tiêu và nguyên tắc

1. Mục tiêu

a) Bảo vệ thông tin, hệ thống thông tin trên không gian mạng tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng;

b) Bảo vệ quyền và lợi ích hợp pháp của chủ thể dữ liệu cá nhân; bảo đảm việc xử lý dữ liệu cá nhân hợp pháp, minh bạch, đúng mục đích theo quy định của Luật Bảo vệ dữ liệu cá nhân.

2. Nguyên tắc

a) Hoạt động ứng dụng công nghệ thông tin phải gắn kết chặt chẽ với công tác bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân; tuân thủ sự quản lý nhà nước và hướng dẫn chuyên môn của Công an tỉnh và các cơ quan chức năng có thẩm quyền.

b) Việc bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân phải được thực hiện đồng bộ, toàn trình từ khâu thiết kế, mua sắm, lắp đặt, vận hành, bảo trì đến khi ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm,

dữ liệu.

c) Trách nhiệm bảo đảm an toàn thông tin mạng, an ninh mạng và bảo vệ dữ liệu cá nhân gắn liền với trách nhiệm của người đứng đầu cơ quan, Trưởng các phòng chuyên môn và cá nhân cán bộ, công chức trực tiếp vận hành, sử dụng.

d) 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;

đ) Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ nghiêm ngặt theo quy định của pháp luật về bảo vệ bí mật nhà nước. Tuyệt đối không soạn thảo, lưu trữ, truyền đưa tài liệu mang bí mật nhà nước trên máy tính hoặc hệ thống có kết nối mạng Internet.

3. Phạm vi chính sách an toàn thông tin tại Quy chế này bao gồm: Thiết lập chính sách; tổ chức bảo đảm an toàn thông tin; bảo đảm nguồn nhân lực; quản lý thiết kế, xây dựng hệ thống; quản lý vận hành; quản lý rủi ro; kết thúc vận hành, thanh lý; bảo vệ dữ liệu cá nhân.

Điều 3. Những hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng năm 2015, Điều 8 Luật An ninh mạng năm 2018 (hoặc Điều 7 Luật An ninh mạng năm 2025) và Điều 7 Luật Bảo vệ dữ liệu cá nhân.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng (điểm truy cập WIFI cá nhân) vào mạng nội bộ; sử dụng cùng một thiết bị để đồng thời truy cập vào mạng nội bộ và truy cập Internet thông qua kết nối ngoại vi cá nhân (USB 3G/4G/5G, điện thoại di động phát sóng).

3. Tự ý thay đổi cấu hình, gỡ bỏ phần mềm phòng, chống mã độc, các biện pháp bảo đảm an toàn thông tin cài đặt trên thiết bị công vụ; tự ý tháo lắp, thay thế, tráo đổi linh kiện của máy tính cơ quan.

4. Xử lý dữ liệu cá nhân sai mục đích, vượt quá phạm vi thẩm quyền được giao; tiết lộ, chia sẻ, chuyển giao dữ liệu cá nhân cho bên thứ ba khi không có cơ sở pháp lý hoặc không được sự đồng ý của chủ thể dữ liệu.

Điều 4. Phân công trách nhiệm và phối hợp quản lý an toàn thông tin, an ninh mạng

1. Phòng Văn hóa – Xã hội và Ủy ban nhân dân Xã là bộ phận chuyên trách về an toàn thông tin của cơ quan, có trách nhiệm:

a) Tham mưu Chủ tịch Ủy ban nhân dân Xã xây dựng, triển khai các kế hoạch ứng dụng công nghệ thông tin; lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin trình cấp có thẩm quyền phê duyệt. Quản lý danh mục thiết bị công nghệ thông tin; cấp phát, thu hồi quyền truy cập mạng và tài khoản nội bộ của cán bộ, công chức, viên chức, người lao động.

b) Quản trị mạng nội bộ (LAN), thiết bị mạng (Router, Switch, thiết bị phát sóng không dây); tổ chức cài đặt, cập nhật phần mềm phòng, chống mã độc cho toàn bộ máy tính công vụ; thực hiện sao lưu dự phòng định kỳ cấu hình

mạng và dữ liệu nghiệp vụ quan trọng.

c) Làm đầu mối tiếp nhận, xử lý các sự cố kỹ thuật công nghệ thông tin (hỏng hóc phần cứng, lỗi kết nối mạng) và các sự cố an toàn thông tin mạng thông thường. Đối với các sự cố phức tạp, vượt khả năng xử lý, chủ trì cô lập hệ thống, phối hợp với Công an xã bảo vệ hiện trường và báo cáo ngay cơ quan cấp trên để được hướng dẫn, điều phối ứng cứu.

d) Đôn đốc, hướng dẫn cán bộ, công chức, viên chức, người lao động tuân thủ các quy định tại Quy chế này; tổng hợp, báo cáo định kỳ hoặc đột xuất về công tác bảo đảm an toàn thông tin mạng theo yêu cầu của Lãnh đạo Ủy ban nhân dân xã và cơ quan có thẩm quyền.

2. Công an xã là lực lượng nòng cốt, chuyên trách trong công tác bảo vệ an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng và bảo vệ dữ liệu cá nhân tại cơ quan, có trách nhiệm:

a) Tham mưu Chủ tịch Ủy ban nhân dân Xã thực hiện công tác quản lý nhà nước về an ninh mạng; chủ trì phòng ngừa, phát hiện, đấu tranh và phối hợp điều tra, xử lý các hành vi vi phạm pháp luật về an ninh mạng, lộ mất bí mật nhà nước và vi phạm quy định về bảo vệ dữ liệu cá nhân tại địa bàn xã theo thẩm quyền.

b) Làm đầu mối thường trực liên hệ với cơ quan chuyên trách bảo vệ an ninh mạng cấp trên; báo cáo khẩn cấp và phối hợp trực tiếp với Công an tỉnh điều tra, xử lý khi phát hiện các sự cố tấn công mạng có chủ đích, xâm nhập hệ thống trái phép, đánh cắp dữ liệu mang tính chất phức tạp hoặc có dấu hiệu tội phạm hình sự.

3. Trách nhiệm phối hợp

Phòng Văn hóa – Xã hội và UBND xã phối hợp chặt chẽ với Công an xã trong việc trao đổi thông tin, kiểm tra nội bộ và tham mưu tổ chức lực lượng tham gia các hoạt động diễn tập, đánh giá an toàn thông tin, an ninh mạng khi có yêu cầu, chỉ đạo của Ủy ban nhân dân tỉnh và Công an tỉnh.

Điều 5. Bảo đảm nguồn nhân lực và trách nhiệm của người sử dụng

1. Cán bộ được tuyển dụng, bố trí vào vị trí làm về an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân phải có trình độ, năng lực về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí và điều kiện tuyển dụng.

2. Định kỳ hằng năm tổ chức hoặc tham gia đào tạo, tập huấn về an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân cho: Cán bộ chuyên trách công nghệ thông tin; Cán bộ quản lý; Người sử dụng trực tiếp (Trung tâm phục vụ hành chính công, tư pháp, địa chính, chính sách Xã hội...).

3. Trách nhiệm bảo đảm an toàn thông tin đối với cán bộ/đơn vị quản lý và vận hành hệ thống:

a) Thiết lập cơ chế kiểm soát, giám sát mạng không dây; bắt buộc xác thực và mã hóa để bảo vệ truy cập;

b) Tổ chức quản lý định danh đối với tất cả người dùng tham gia sử

dụng hệ thống thông tin;

c) Tài khoản quản trị hệ thống phải tách biệt với tài khoản truy nhập của người sử dụng thông thường và được giao đích danh cá nhân làm công tác quản trị.

4. Trách nhiệm của người sử dụng:

a) Có trách nhiệm đảm bảo an toàn thông tin và bảo vệ dữ liệu cá nhân đối với từng vị trí công việc;

b) Chỉ truy cập vào các trang, cổng thông tin điện tử, ứng dụng trực tuyến phục vụ công việc; không truy cập, mở các đường dẫn, thư điện tử không rõ nguồn gốc;

c) Có trách nhiệm bảo mật tài khoản; đặt mật khẩu với độ phức tạp cao (có độ dài tối thiểu 08 ký tự, bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt); bắt buộc thay đổi mật khẩu tối thiểu 03 tháng/lần và đăng xuất tài khoản khi không sử dụng;

d) Không được in ấn, chụp ảnh màn hình, sao chép dữ liệu cá nhân nhạy cảm, tài liệu nội bộ mang ra khỏi cơ quan khi không có sự cho phép bằng văn bản của người có thẩm quyền;

đ) Khóa màn hình máy tính khi tạm thời rời khỏi vị trí làm việc; tắt máy tính, ngắt nguồn điện khi kết thúc làm việc.

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

a) Phải bàn giao, thu hồi thông tin lưu trữ trên các thiết bị, phần cứng, phần mềm thuộc sở hữu của cơ quan;

b) Đơn vị, cán bộ chuyên trách phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống và quyền truy cập dữ liệu cá nhân;

c) Đối với cán bộ trực tiếp xử lý dữ liệu cá nhân nhạy cảm, Lãnh đạo phụ trách phải lập biên bản bàn giao, cam kết bảo mật và xác nhận đã xóa toàn bộ dữ liệu cá nhân trên thiết bị cá nhân (nếu có).

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

1. Khi triển khai đầu tư, thiết lập, nâng cấp, mở rộng hệ thống thông tin, Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã có trách nhiệm chủ trì, phối hợp với các cơ quan, đơn vị tư vấn xây dựng tài liệu mô tả trình Chủ tịch Ủy ban nhân dân xã phê duyệt, bao gồm các nội dung sau:

a) Quy mô, phạm vi, đối tượng sử dụng, khai thác và quản lý hệ thống thông tin;

b) Thiết kế kiến trúc và các thành phần của hệ thống thông tin;

c) Phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;

d) Phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

2. Trong quá trình triển khai hoặc vận hành, khi có sự thay đổi về thiết kế hệ thống, Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã có trách nhiệm đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn thông tin đã đặt ra; kịp thời tham mưu, trình Chủ tịch Ủy ban nhân dân xã xem xét, phê duyệt phương án điều chỉnh.

Điều 7. Phát triển phần mềm thuê khoán

1. Hợp đồng ký kết phải có các điều khoản ràng buộc chặt chẽ đối với đơn vị phát triển phần mềm về cam kết bảo mật thông tin, bảo vệ bí mật nhà nước và bảo vệ dữ liệu cá nhân người dùng theo đúng quy định của pháp luật.

2. Đơn vị phát triển phần mềm có trách nhiệm bàn giao toàn bộ mã nguồn, tài liệu thiết kế, tài liệu hướng dẫn quản trị, sử dụng và tài khoản quản trị cấp cao nhất (Super Admin) cho Ủy ban nhân dân xã sau khi nghiệm thu, đưa vào sử dụng.

3. Đơn vị phát triển phần mềm có trách nhiệm xây dựng kế hoạch, nội dung thử nghiệm hệ thống, gửi Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã thẩm định, trình Chủ tịch Ủy ban nhân dân Xã phê duyệt trước khi thực hiện. Phần mềm thuê khoán phải được kiểm thử tính năng và kiểm thử an toàn thông tin trên môi trường thử nghiệm độc lập trước khi bàn giao và đưa vào sử dụng.

4. Phần mềm phải được rà quét lỗ hổng bảo mật, kiểm tra và đánh giá an toàn thông tin (do đơn vị chuyên môn cấp tỉnh hoặc tổ chức đánh giá độc lập thực hiện) trước khi đưa vào vận hành, khai thác chính thức trên hệ thống mạng của cơ quan.

5. Giao Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã làm đầu mối phối hợp với đơn vị phát triển phần mềm và các cơ quan chuyên môn cấp trên để triển khai thực hiện các bước kiểm thử, đánh giá an toàn thông tin và nghiệm thu hệ thống.

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

Điều 8. Quản lý an toàn vật lý, môi trường và an toàn mạng

1. Quản lý an toàn vật lý và môi trường đặt thiết bị:

a) Thiết bị mạng lõi, máy chủ, thiết bị lưu trữ (nếu có) phải được đặt tại phòng hoặc khu vực an toàn, có khóa bảo vệ; được trang bị hệ thống phòng cháy, chữa cháy, thiết bị làm mát và bộ lưu điện dự phòng (UPS).

b) Tuyệt đối không cho phép cơ quan, tổ chức, cá nhân không có chức năng, nhiệm vụ tự ý tiếp cận khu vực đặt thiết bị mạng trung tâm của cơ quan.

2. Quản lý, vận hành hoạt động bình thường của hệ thống 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: Lưu giữ sơ đồ logic và vật lý của hệ thống mạng; tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng và thiết bị nhằm bảo đảm an toàn, bảo mật.

b) Sử dụng thiết bị tường lửa (Firewall) hoặc bộ định tuyến (Router) để kiểm soát truy cập từ bên ngoài; phân chia hệ thống mạng nội bộ của cơ quan tách biệt với mạng không dây dành cho khách (Guest WIFI); bảo đảm lưu trữ nhật ký hoạt động của hệ thống (log), lỗi và sự kiện an toàn thông tin tối thiểu 03 tháng; thực hiện kết nối, gửi nhật ký hệ thống về hệ thống giám sát tập trung của Công an tỉnh (nếu có yêu cầu kỹ thuật).

c) Thiết lập, cấu hình đầy đủ các tính năng an toàn 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. Phối hợp với cơ quan chuyên môn cấp trên hoặc sử dụng các công cụ hợp lệ để dò tìm, phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các kết nối, thiết bị cài đặt bất hợp pháp vào mạng nội bộ.

d) Xác định và ghi rõ các tính năng an toàn, yêu cầu bảo mật dữ liệu trong các hợp đồng, thỏa thuận cung cấp dịch vụ mạng, đường truyền với bên thứ ba (nhà cung cấp dịch vụ viễn thông).

đ) Đối với mạng không dây (WIFI): Phải thiết lập chuẩn mã hóa an toàn và định kỳ ít nhất 03 tháng/lần thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

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

a) Căn cứ điều kiện thực tế, trang bị phương án dự phòng đường truyền mạng, thiết bị mạng để đảm bảo tính sẵn sàng, không làm gián đoạn hoạt động điều hành của Ủy ban nhân dân Xã.

b) Triển khai phương tiện lưu trữ độc lập để sao lưu định kỳ các thông tin cấu hình thiết bị mạng, thông tin kết nối, định danh người dùng nhằm phục vụ công tác khôi phục nhanh chóng sau khi xảy ra sự cố.

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

a) Cán bộ, công chức, người lao động truy cập, khai thác thông tin mạng theo đúng trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, tuyệt đối không tự ý cung cấp thông tin, tài nguyên nội bộ ra bên ngoài.

b) Đơn vị/Cán bộ quản lý, vận hành có trách nhiệm theo dõi, phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn quyền hạn; tiến hành ngăn chặn, thu hồi, khóa quyền truy cập đối với các tài khoản, thiết bị vi phạm.

c) Các thiết bị mạng, thiết bị đầu cuối phải được cấu hình tối ưu, tăng cường bảo mật (cứng hóa) và tắt các dịch vụ không cần thiết trước khi đưa vào vận hành, khai thác.

d) Việc kết nối thiết bị đầu cuối mới của người sử dụng vào hệ thống mạng nội bộ phải tuân thủ quy trình, được sự đồng ý và giám sát cấu hình trực tiếp của Phòng Văn hóa - Xã hội và UBND Xã.

Điều 9. Quản lý an toàn máy chủ và phần mềm ứng dụng

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

dịch vụ (nếu có):

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, tệp tin nhật ký hoạt động (log) của hệ thống để kịp thời phát hiện và xử lý sự cố;

c) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp; loại bỏ các dịch vụ, phần mềm không còn nhu cầu sử dụng; thống kê và quản lý thời hạn bản quyền phần mềm phục vụ cho việc gia hạn.

2. Truy cập mạng và quản trị máy chủ:

a) Phải thay đổi các tài khoản, mật khẩu mặc định ngay trước khi đưa hệ điều hành, phần mềm, máy chủ vào sử dụng; thiết lập cấu hình tường lửa để kiểm soát các cổng dịch vụ từ bên trong ra cũng như từ bên ngoài vào hệ thống.

b) Phân quyền quản lý truy cập chặt chẽ cho người sử dụng trên máy chủ.

c) Toàn bộ máy chủ không được kết nối trực tiếp với mạng Internet, ngoại trừ các hệ thống bắt buộc phải có giao tiếp mạng (như hệ thống phục vụ truy cập Internet, cung cấp giao diện dịch vụ công, thư điện tử hoặc cập nhật bản vá lỗi).

3. Tối ưu và tăng cường bảo mật (cứng hóa) hệ thống máy chủ trước khi đưa vào vận hành, khai thác:

a) Sử dụng hệ điều hành và các phiên bản phần mềm an toàn, tin cậy;

b) Vô hiệu hóa hoặc gỡ bỏ tất cả các dịch vụ, giao thức kết nối không cần thiết;

c) Thiết lập kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Ngăn chặn mọi truy cập trái phép từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các địa chỉ IP và người dùng tin cậy.

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

Triển khai phương tiện lưu trữ độc lập với hệ thống lưu trữ trên máy chủ để sao lưu dự phòng. Định kỳ thực hiện sao lưu các dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản sao hệ điều hành máy chủ (image), cơ sở dữ liệu và dữ liệu thông tin nghiệp vụ.

5. Cài đặt, gỡ bỏ phần mềm trên hệ thống máy chủ và máy tính làm việc: Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã chịu trách nhiệm cài đặt các phần mềm nghiệp vụ, phần mềm bảo mật cho máy tính phục vụ công việc. Cán bộ, công chức, người lao động không được tự ý can thiệp (thay đổi cấu hình, gỡ bỏ...) vào các phần mềm đã cài đặt trên thiết bị khi chưa được sự đồng ý của bộ phận chuyên trách.

Điều 10. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với việc mã hóa và phân loại dữ liệu:

a) Ủy ban nhân dân xã áp dụng các phương thức mã hóa dữ liệu thích hợp theo tiêu chuẩn quốc gia hoặc các giải pháp do cơ quan nhà nước có thẩm quyền cung cấp (như chứng thư số của Ban Cơ yếu Chính phủ) để bảo vệ thông tin, đặc biệt là các tài liệu nội bộ và dữ liệu cá nhân nhạy cảm.

b) Cán bộ, công chức, viên chức có trách nhiệm phân loại thông tin, dữ liệu theo mức độ nhạy cảm và tầm quan trọng để áp dụng các biện pháp quản lý, bảo vệ tương ứng theo quy định của pháp luật.

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

a) Các thông tin, tài liệu mang tính chất nội bộ, dữ liệu cá nhân nhạy cảm phải được mã hóa hoặc đặt mật khẩu bảo vệ trước khi trao đổi, truyền nhận qua môi trường mạng máy tính (thư điện tử công vụ, phần mềm quản lý văn bản).

b) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ; quản lý, kiểm soát chặt chẽ Trang/cổng thông tin điện tử của Xã nhằm phòng ngừa việc xâm nhập, thay đổi nội dung hoặc khai thác bất hợp pháp thông tin của tổ chức, cá nhân.

3. Sao lưu dự phòng, phục hồi và hủy bỏ dữ liệu:

a) Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã có trách nhiệm lập danh mục các cơ sở dữ liệu, phần mềm và dữ liệu nghiệp vụ cần được sao lưu; quy định rõ phương pháp và chu kỳ sao lưu (tần suất sao lưu).

b) Việc sao lưu dự phòng phải được thực hiện định kỳ và lưu trữ trên phương tiện vật lý độc lập (như ổ cứng di động, máy chủ sao lưu chuyên dụng) đặt tại khu vực an toàn. Định kỳ kiểm tra dữ liệu sao lưu để đảm bảo khả năng phục hồi nhanh chóng khi hệ thống gặp sự cố (hỏng phần cứng, nhiễm mã độc tống tiền).

c) Khi tiêu hủy phương tiện lưu trữ hoặc hủy bỏ dữ liệu cá nhân đã hết thời hạn lưu trữ theo quy định, phải áp dụng các biện pháp kỹ thuật xóa bỏ vĩnh viễn, bảo đảm dữ liệu không thể phục hồi dưới mọi hình thức, quá trình tiêu hủy phải có sự giám sát của bộ phận chuyên trách.

4. Nguyên tắc xử lý và bảo vệ dữ liệu cá nhân đối với cán bộ, công chức:

a) Việc thu thập dữ liệu cá nhân của công dân qua các thủ tục hành chính, hồ sơ chuyên môn phải tuân thủ nguyên tắc: Chỉ thu thập những dữ liệu thực sự cần thiết, đúng mục đích và đúng thẩm quyền được pháp luật quy định.

b) Dữ liệu cá nhân (đặc biệt là thông tin về lý lịch tư pháp, tình trạng sức khỏe, thông tin tài chính, dân tộc...) thu thập qua Trung tâm phục vụ hành chính công hoặc các phòng chuyên môn phải được lưu trữ an toàn, phân quyền truy cập nghiêm ngặt. Chỉ cán bộ, công chức được phân công trực tiếp giải quyết hồ sơ mới được quyền tiếp cận, xử lý.

c) Tuyệt đối nghiêm cấm hành vi tự ý sao chép, cung cấp, chia sẻ hoặc phát tán dữ liệu cá nhân cho bên thứ ba (kể cả trên các ứng dụng nhắn tin, mạng Xã hội) khi không có yêu cầu bằng văn bản của cơ quan nhà nước có thẩm quyền hoặc chưa được sự đồng ý hợp pháp của chủ thể dữ liệu.

Điều 11. Quản lý an toàn thiết bị đầu cuối

1. Thông tin về thiết bị đầu cuối (máy tính, máy in, thiết bị thông minh) kết nối vào hệ thống mạng nội bộ của Ủy ban nhân dân xã phải được Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã lập danh mục quản lý và cập nhật thường

xuyên thông qua địa chỉ MAC, địa chỉ IP.

2. Việc cài đặt mới, kết nối, thay đổi vị trí hoặc gỡ bỏ thiết bị đầu cuối ra khỏi hệ thống mạng nội bộ phải được sự đồng ý của Lãnh đạo Ủy ban nhân dân Xã và thực hiện dưới sự kiểm tra, giám sát của Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã nhằm bảo đảm an toàn hệ thống.

3. Quản lý việc truy cập và điều khiển thiết bị đầu cuối từ xa:

a) Hạn chế việc cài đặt, sử dụng các phần mềm hỗ trợ điều khiển thiết bị đầu cuối từ xa trên máy tính công vụ;

b) Trường hợp bắt buộc phải sử dụng để khắc phục sự cố kỹ thuật, phải áp dụng cơ chế xác thực an toàn. Cán bộ, công chức sử dụng thiết bị có trách nhiệm giám sát trực tiếp quá trình thực hiện, ngắt kết nối và đóng phần mềm ngay sau khi hoàn thành công việc; tuyệt đối không thiết lập chế độ duy trì hoạt động ngầm đối với các phần mềm điều khiển từ xa trên thiết bị.

4. Quản lý thiết bị đầu cuối trong quá trình bảo hành, sửa chữa:

Khi đưa thiết bị đầu cuối ra ngoài cơ quan để bảo hành, sửa chữa, Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã chủ trì, phối hợp với cán bộ, công chức sử dụng thiết bị tháo rời phương tiện lưu trữ dữ liệu để quản lý tại cơ quan. Trường hợp không thể tháo rời phương tiện lưu trữ, phải thực hiện sao lưu và áp dụng các biện pháp kỹ thuật tiêu hủy toàn bộ tài liệu công vụ, dữ liệu cá nhân trên thiết bị nhằm phòng ngừa nguy cơ lộ mất thông tin, bí mật nhà nước.

Điều 12. Quản lý phòng, chống phần mềm độc hại

1. Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã có trách nhiệm cài đặt phần mềm phòng, chống mã độc trên toàn bộ máy tính công vụ của cơ quan; thiết lập cấu hình cập nhật cơ sở dữ liệu tự động và tự động quét mã độc khi kết nối thiết bị ngoại vi, sao chép hoặc mở tệp tin.

2. Cán bộ, công chức, viên chức, người lao động khi trao đổi văn bản điện tử qua hệ thống thư điện tử, phần mềm dùng chung phải sử dụng các định dạng tệp tin an toàn theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước (như: .txt, .docx, .pdf); tuyệt đối không gửi, nhận và mở các tệp tin có định dạng thực thi nguy hiểm (như: .exe, .bat, .com).

3. Nghiêm cấm cán bộ, công chức tự ý cài đặt phần mềm không rõ nguồn gốc, vô hiệu hóa hoặc gỡ bỏ phần mềm phòng, chống mã độc trên thiết bị công vụ khi chưa có sự đồng ý của Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã.

4. Toàn bộ máy tính công vụ phải được cấu hình vô hiệu hóa tính năng tự động thực thi (AutoPlay) đối với các thiết bị lưu trữ di động. Mọi tệp tin, phần mềm ứng dụng và phương tiện lưu trữ ngoại vi (USB, ổ cứng ngoài) phải được quét mã độc trước khi sao chép, cài đặt và đưa vào sử dụng.

5. Khi phát hiện thiết bị có dấu hiệu lây nhiễm mã độc (máy hoạt động chậm bất thường, có cảnh báo từ phần mềm bảo mật, dữ liệu bị mã hóa hoặc mất mát), người sử dụng phải lập tức ngắt kết nối thiết bị khỏi mạng nội bộ và báo cáo Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã để tiến hành cô lập, 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. Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã chủ trì thực hiện kiểm tra, rà quét phần mềm độc hại trên toàn bộ hệ thống mạng và thiết bị đầu cuối định kỳ hằng năm hoặc rà quét đột xuất khi có cảnh báo về chiến dịch tấn công mã độc từ cơ quan chức năng có thẩm quyền.

Điều 13. Quản lý giám sát an toàn hệ thống thông tin

1. Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã chủ trì, phối hợp với cơ quan chức năng cấp trên thực hiện cấu hình, kết nối và chia sẻ dữ liệu, gửi nhật ký hệ thống (log) từ các thiết bị mạng, thiết bị bảo mật, máy chủ (nếu có) và thiết bị đầu cuối thuộc hệ thống thông tin của Ủy ban nhân dân xã về hệ thống giám sát trung tâm của tỉnh theo quy định.

2. Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã thực hiện theo dõi, giám sát thường xuyên tình trạng hoạt động của thiết bị mạng, đường truyền và nhật ký truy cập nhằm phát hiện sớm các dấu hiệu bất thường, các kết nối trái phép hoặc hành vi tấn công, xâm nhập hệ thống mạng nội bộ.

3. Khi phát hiện dấu hiệu tấn công mạng hoặc nhận được cảnh báo từ hệ thống giám sát trung tâm của cơ quan cấp trên, Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã khẩn trương kiểm tra, xác minh, áp dụng ngay các biện pháp kỹ thuật cô lập thiết bị để ngăn chặn sự cố, đồng thời báo cáo cơ quan có thẩm quyền để phối hợp, hỗ trợ xử lý.

4. Cán bộ, công chức được giao chuyên trách công nghệ thông tin, an toàn thông tin mạng có trách nhiệm tham gia các chương trình đào tạo, tập huấn, bồi dưỡng và diễn tập thực chiến về giám sát, cảnh báo, ứng cứu sự cố an toàn thông tin do Công an tỉnh và các cơ quan chức năng cấp trên tổ chức hằng năm.

5. Chủ tịch Ủy ban nhân dân Xã chỉ đạo công tác giám sát an toàn thông tin tại cơ quan; bảo đảm duy trì các điều kiện kỹ thuật và nguồn lực cần thiết để hoạt động giám sát được diễn ra liên tục, hiệu quả và không làm gián đoạn công tác chuyên môn.

Điều 14. Quản lý điểm yếu an toàn thông tin

1. Trách nhiệm của Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã:

a) Quản lý, theo dõi thông tin về các điểm yếu, lỗ hổng bảo mật đối với từng thành phần của hệ thống thông tin (hệ điều hành, phần mềm ứng dụng, thiết bị mạng); phân loại mức độ nguy hiểm và có phương án, quy trình xử lý phù hợp.

b) Báo cáo kịp thời Lãnh đạo Ủy ban nhân dân Xã khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng; thực hiện cảnh báo và tổ chức khắc phục theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm gián đoạn hoạt động bình thường của hệ thống.

c) Triển khai phương án xử lý tạm thời (cô lập kết nối, tạm dừng dịch vụ)

đối với các điểm yếu chưa thể khắc phục triệt để và chuẩn bị sẵn sàng phương án khôi phục hệ thống phòng trường hợp việc xử lý thất bại.

d) Chủ động phối hợp với cơ quan chuyên môn cấp trên, tổ chức, doanh nghiệp cung cấp dịch vụ công nghệ thông tin để được hỗ trợ trong việc khắc phục, vá lỗ hổng bảo mật khi cần thiết.

2. Mọi thành phần thiết bị, phần mềm của hệ thống thông tin phải được kiểm tra, rà quét và xử lý điểm yếu an toàn thông tin trước khi đưa vào vận hành, khai thác chính thức.

3. Định kỳ hằng năm, Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã phối hợp với các cơ quan chức năng tiến hành kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống; khẩn trương thực hiện quy trình xử lý, vá lỗi ngay khi nhận được thông tin hoặc cảnh báo về lỗ hổng bảo mật từ các cơ quan có thẩm quyền.

4. Hoạt động kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu và thử nghiệm xâm nhập hệ thống được thực hiện tuân thủ theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ và Điều 11 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

Điều 15. Quản lý sự cố an toàn thông tin

1. Việc phân nhóm sự cố an toàn thông tin mạng được thực hiện theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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. Giao Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã chủ trì tham mưu xây dựng phương án tiếp nhận, phát hiện, phân loại, xử lý ban đầu và ứng phó sự cố an toàn thông tin mạng tại cơ quan.

2. Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã tham mưu xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng bảo đảm tuân thủ quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg.

3. 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.

4. Xây dựng và triển khai phương án giám sát, phát hiện, cảnh báo sự cố an toàn thông tin trong quy trình ứng cứu nhằm khắc phục kịp thời sự cố. Khi cần thiết để phục vụ công tác khắc phục sự cố, Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã báo cáo Chủ tịch Ủy ban nhân dân Xã xem xét, quyết định việc ngưng hoạt động một phần hoặc toàn bộ hệ thống thông tin của cơ quan; phối hợp với các cơ quan chức năng điều tra nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo Ủy ban nhân dân Xã và cơ quan cấp trên.

5. Phối hợp trong công tác hỗ trợ, điều phối xử lý sự cố an toàn thông tin: Tùy thuộc vào mức độ của sự cố, Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã phối hợp với Công an Xã khẩn trương liên hệ, báo cáo Đội Ứng cứu sự cố an

toàn thông tin mạng tỉnh và các cơ quan, đơn vị có liên quan để được hướng dẫn xử lý, hỗ trợ ứng cứu đối với các sự cố tấn công mạng, sự cố lộ lọt dữ liệu.

Điều 16. Quản lý an toàn người sử dụng đầu cuối

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

a) Cán bộ, công chức, viên chức, người lao động (sau đây gọi chung là người sử dụng) khi truy cập, sử dụng tài nguyên nội bộ, mạng Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của Ủy ban nhân dân Xã.

b) Việc cài đặt, kết nối máy tính, thiết bị đầu cuối vào hệ thống mạng cơ quan phải được thực hiện theo đúng hướng dẫn, quy trình và dưới sự giám sát của Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã.

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

d) Không sử dụng các thiết bị máy tính thuộc sở hữu cá nhân (máy tính xách tay, thiết bị di động thông minh) để kết nối vào mạng nội bộ hoặc xử lý thông tin, tài liệu công vụ nếu chưa được phép. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

đ) Khi sử dụng các thiết bị lưu trữ ngoài (ổ cứng di động, thẻ nhớ, thiết bị lưu trữ USB), người sử dụng bắt buộc phải quét mã độc trước khi đọc hoặc sao chép dữ liệu.

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

a) Người sử dụng phải 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 chức năng, nhiệm vụ và quyền hạn được giao.

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

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng, người sử dụng phải báo cáo ngay với Lãnh đạo phụ trách trực tiếp và Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã để kịp thời ngăn chặn và xử lý.

d) Người sử dụng có trách nhiệm tham gia các chương trình đào tạo, hội nghị, tập huấn về an toàn thông tin mạng do cấp trên hoặc cơ quan tổ chức.

Điều 17. Bảo đảm an toàn thông tin cho hệ thống camera giám sát

1. Hệ thống camera giám sát phải được thiết lập biện pháp kiểm soát truy cập an toàn. Bắt buộc thay đổi mật khẩu mặc định của nhà sản xuất ngay khi thiết lập; định kỳ thực hiện cập nhật, thay đổi mật khẩu tài khoản quản trị cấp cao nhất theo quy định về an toàn thông tin.

2. Việc cấp phát, quản lý tài khoản truy cập hệ thống camera phải căn cứ trên chức năng, nhiệm vụ và thẩm quyền của từng cá nhân, bộ phận. Nghiêm cấm mọi hành vi tự ý chia sẻ thông tin tài khoản, sao chép, trích xuất hoặc phát tán dữ liệu hình ảnh, video từ hệ thống camera ra bên ngoài khi chưa có sự chấp

thuận của người có thẩm quyền.

3. Dữ liệu hình ảnh thu thập từ hệ thống camera giám sát là tài sản thông tin của cơ quan. Việc khai thác, sử dụng dữ liệu này chỉ được thực hiện đúng mục đích, phục vụ công tác quản lý điều hành, bảo đảm an ninh trật tự hoặc cung cấp cho cơ quan nhà nước có thẩm quyền khi có yêu cầu theo quy định của pháp luật.

4. Quá trình đầu tư, mua sắm, lắp đặt hoặc nâng cấp hệ thống, thiết bị camera giám sát phải bảo đảm đầy đủ chứng nhận xuất xứ và tiêu chuẩn chất lượng. Tuyệt đối không đưa vào sử dụng các loại thiết bị đã bị cơ quan chức năng có thẩm quyền đưa ra cảnh báo rủi ro về an toàn thông tin mạng.

5. Về mặt kỹ thuật, hệ thống camera giám sát phải được quy hoạch và thiết lập thành một phân vùng mạng (VLAN) độc lập, tách biệt với mạng nội bộ (LAN) làm việc của cán bộ, công chức để ngăn chặn nguy cơ xâm nhập, lây nhiễm mã độc chéo.

6. Việc triển khai, vận hành hệ thống camera giám sát phải tuân thủ các tiêu chuẩn, quy chuẩn và yêu cầu về an toàn thông tin mạng do cơ quan nhà nước có thẩm quyền ban hành.

Điều 18. 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 thông tin, Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã có trách nhiệm chủ trì thực hiện kiểm tra, đánh giá để bảo đảm an toàn thông tin, không làm rò rỉ, thất thoát dữ liệu.

2. Việc xử lý thông tin, dữ liệu trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ, thanh lý thiết bị phải được thực hiện theo phương án kỹ thuật an toàn (tiêu hủy dữ liệu) và phải được Chủ tịch Ủy ban nhân dân xã phê duyệt trước khi thực hiện.

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

Điều 19. Nội dung, hình thức và thẩm quyền 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 các biện pháp bảo đảm an toàn hệ thống thông tin đang được áp dụng tại cơ quan;

c) Đánh giá, phát hiện mã độc, lỗ hổng, điểm yếu và thử nghiệm xâm nhập hệ thống (nếu có yêu cầu từ cơ quan chuyên môn);

d) Các nội dung kiểm tra, đánh giá khác do cơ quan có thẩm quyền quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch hằng năm của Ủy ban nhân dân Xã hoặc của cơ quan quản lý cấp trên;

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) Cơ quan chuyên trách về an toàn thông tin mạng, an ninh mạng cấp tỉnh (Công an tỉnh);

b) Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Nghệ An;

c) Chủ tịch Ủy ban nhân dân Xã.

4. Đơn vị chủ trì thực hiện:

Đơn vị chủ trì kiểm tra, đánh giá là tổ chức, bộ phận được cấp có thẩm quyền (quy định tại khoản 3 Điều này) giao nhiệm vụ hoặc đơn vị chuyên môn độc lập được Ủy ban nhân dân Xã thuê để thực hiện nhiệm vụ rà quét, đánh giá.

5. Đối tượng kiểm tra, đánh giá:

Đối tượng chịu sự kiểm tra, đánh giá là các phòng, ban, bộ phận chuyên môn và toàn thể cán bộ, công chức, viên chức, người lao động thuộc Ủy ban nhân dân Xã có tham gia vận hành, khai thác và sử dụng hệ thống thông tin.

Điều 20. Kiểm tra việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc lập hồ sơ, xác định cấp độ an toàn hệ thống thông tin và tiến độ triển khai phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt; đánh giá hiệu quả thực tế của các biện pháp kỹ thuật, quản lý đang áp dụng;

b) Kiểm tra công tác theo dõi, giám sát an toàn thông tin mạng, an ninh mạng và sự sẵn sàng trong việc ứng phó, ứng cứu sự cố;

c) Kiểm tra việc chấp hành các nội dung khác tại Quy chế này đối với các bộ phận và từng cán bộ, công chức, viên chức, người lao động.

2. Thẩm quyền kiểm tra

a) Cơ quan quản lý nhà nước, cơ quan chuyên trách cấp trên (Công an tỉnh) thực hiện thanh tra, kiểm tra định kỳ hoặc đột xuất theo thẩm quyền quản lý ngành, lĩnh vực.

b) Ủy ban nhân dân Xã tự tổ chức kiểm tra việc tuân thủ Quy chế trong phạm vi nội bộ cơ quan.

3. Tổ chức thực hiện kiểm tra nội bộ:

a) Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã chủ trì, phối hợp với Công an xã tham mưu xây dựng kế hoạch và tổ chức thực hiện công tác tự kiểm tra an toàn thông tin, an ninh mạng tại các phòng, ban, bộ phận trực thuộc định kỳ hằng năm.

b) Hoạt động tự kiểm tra về an toàn thông tin, an ninh mạng có thể được lồng ghép trong chương trình kiểm tra công tác cải cách hành chính, kiểm tra ứng dụng công nghệ thông tin hằng năm theo kế hoạch được Chủ tịch Ủy ban nhân dân xã phê duyệt.

Điều 21. Quản lý rủi ro an toàn thông tin

1. Xác định và đánh giá mức độ rủi ro:

Phòng Văn hóa - Xã hội và Ủy ban nhân dân Xã chủ trì, phối hợp với Công an Xã định kỳ tổ chức đánh giá rủi ro đối với hệ thống thông tin của cơ quan, bao gồm các nội dung sau:

a) Thống kê, nhận biết các tài sản thông tin, hạ tầng thiết bị đang quản lý; xác định đặc điểm, vị trí lưu trữ, mức độ quan trọng và giá trị đặc thù của từng tài sản để làm cơ sở phân tích hậu quả nếu xảy ra sự cố.

b) Nhận diện và phân loại các điểm yếu, lỗ hổng thành các nhóm:

- Nhóm điểm yếu liên quan đến tồn tại lỗ hổng an toàn thông tin nội tại trong hệ thống thiết bị, phần mềm;

- Nhóm điểm yếu do thiếu hụt các biện pháp quản lý (không có quy định sử dụng mật khẩu an toàn, không mã hóa dữ liệu, thiếu quy trình xử lý sự cố, thiếu quy định ràng buộc người sử dụng);

- Nhóm điểm yếu do thiếu hụt các biện pháp kỹ thuật bảo vệ (thiếu hệ thống phòng, chống xâm nhập; mã độc).

c) Phân loại các mối đe dọa:

- Nhóm mối đe dọa khai thác các lỗ hổng, điểm yếu tồn tại trong hệ thống;

- Nhóm mối đe dọa phát sinh từ việc thiếu hụt các biện pháp quản lý và biện pháp kỹ thuật;

- Nhóm mối đe dọa, nguy cơ mất an toàn thông tin xuất phát từ các nhà cung cấp dịch vụ, bên thứ ba.

d) Đánh giá hậu quả, khả năng xảy ra sự cố và xác định mức độ rủi ro đối với hệ thống thông tin theo các mức: thấp, trung bình, cao, rất cao và cực cao.

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

Hoạt động quản lý rủi ro phải được thực hiện định kỳ hằng năm hoặc khi có sự thay đổi, nâng cấp lớn về hạ tầng công nghệ thông tin. Quá trình thực hiện bảo đảm tuân thủ 04 bước cơ bản: thiết lập bối cảnh; đánh giá rủi ro; xử lý rủi ro; chấp nhận rủi ro. Trong quá trình thực hiện, phải duy trì song song hoạt động truyền thông, tư vấn rủi ro và giám sát, soát xét liên tục.

3. Triển khai biện pháp kiểm soát rủi ro:

Các biện pháp kiểm soát, xử lý rủi ro phải được triển khai bám sát phương án bảo đảm an toàn thông tin đã được phê duyệt trong Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin của Ủy ban nhân dân xã và tuân thủ các hướng dẫn nghiệp vụ chuyên môn của Công an tỉnh.

Chương V
TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG

Điều 22. 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 đối với hệ thống thông tin và các thông tin, tài liệu, dữ liệu cá nhân được soạn thảo, lưu trữ, truyền đưa trên hệ thống; bảo đảm sử dụng các sản phẩm, dịch vụ an ninh mạng đáp ứng tiêu chuẩn kỹ thuật theo quy định;

c) Tổ chức bồi dưỡng kiến thức, kỹ năng an ninh mạng cho cán bộ, công chức, người hoạt động không chuyên trách; chú trọng nâng cao năng lực nhận diện, phòng, chống các thủ đoạn tấn công mạng, lừa đảo trực tuyến và các hành vi giả mạo bằng công nghệ trí tuệ nhân tạo (AI/Deepfake);

d) Bảo vệ an ninh mạng và dữ liệu trong hoạt động cung cấp dịch vụ công trực tuyến, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân; đặc biệt chú trọng các biện pháp hỗ trợ, bảo vệ an toàn thông tin cho các nhóm đối tượng yếu thế (người cao tuổi, trẻ em, người yếu thế trong Xã hội) khi tham gia giao dịch điện tử với chính quyền Xã;

đ) Triển khai tự 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 và lộ lọt dữ liệu.

2. Chủ tịch Ủy ban nhân dân xã có trách nhiệm chỉ đạo, tổ chức triển khai toàn diện các hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

3. Lực lượng bảo vệ an ninh mạng của Ủy ban nhân dân Xã do Công an xã làm nòng cốt, có sự tham gia phối hợp chặt chẽ của Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã nhằm bảo đảm sự thống nhất trong quản lý nhà nước về an ninh mạng tại cơ sở.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 23. Tổ chức thực hiện và rà soát, sửa đổi Quy chế

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

2. Trách nhiệm rà soát, cập nhật và sửa đổi Quy chế:

a) Định kỳ 03 năm hoặc khi có sự thay đổi của các văn bản quy phạm pháp luật cấp trên liên quan, Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã chủ trì, phối hợp với Công an xã tiến hành rà soát, đánh giá tính phù hợp và tham mưu cập nhật, bổ sung Quy chế.

b) Trong quá trình triển khai thực hiện, nếu có vấn đề phát sinh hoặc vướng mắc, các tổ chức, cá nhân phản ánh kịp thời về Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã để tổng hợp, phối hợp với Công an xã báo cáo Chủ tịch Ủy ban nhân dân xã xem xét, điều chỉnh cho phù hợp.

3. Mọi nội dung sửa đổi, bổ sung Quy chế phải được Chủ tịch Ủy ban nhân dân Xã phê duyệt thông qua trước khi công bố áp dụng.

Điều 24. Kinh phí thực hiện, khen thưởng và xử lý vi phạm

1. Hằng năm, Phòng Văn hóa - Xã hội và Ủy ban nhân dân xã có trách nhiệm lập dự toán kinh phí phục vụ công tác bảo đảm an toàn thông tin, an ninh mạng trình Chủ tịch Ủy ban nhân dân xã phê duyệt để triển khai thực hiện. Bảo

đảm tỷ lệ kinh phí chi cho các sản phẩm, giải pháp và dịch vụ an toàn thông tin mạng, an ninh mạng đạt tối thiểu 15% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hằng năm của cơ quan.

2. Tập thể, cá nhân có thành tích xuất sắc trong công tác bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân được xem xét biểu dương, khen thưởng theo quy định.

3. Cán bộ, công chức vi phạm các quy định tại Quy chế này, tùy theo tính chất, mức độ vi phạm và hậu quả gây ra sẽ bị xem xét xử lý kỷ luật, bồi thường thiệt hại hoặc bị đề nghị xử lý theo quy định của pháp luật.