ỦY BAN NHÂN DÂN PHƯỜNG NAM GIA NGHĨA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 157/QĐ-UBND	*Nam Gia Nghĩa, ngày 27 tháng 02 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn phường Nam Gia Nghĩa

ỦY BAN NHÂN DÂN PHƯỜNG NAM GIA NGHĨA

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

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 150/2025/NĐ-CP ngày 12 tháng 6 năm 2025 của Chính phủ quy định tổ chức các cơ quan chuyên môn thuộc Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương và Ủy ban nhân dân cấp xã, phường, đặc khu thuộc tỉnh, thành phố trực thuộc trung ương;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 07 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 của Chính phủ ngày 15 tháng 08 năm 2022 quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Chỉ thị số 09/CT-TTg ngày 25 tháng 02 năm 2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 816/QĐ-UBND ngày 26 tháng 8 năm 2025 của Chủ tịch Ủy ban nhân dân tỉnh Lâm Đồng về việc phân công đơn vị chuyên trách về an toàn thông tin mạng của Ủy ban nhân dân tỉnh Lâm Đồng.

Theo đề nghị của Công an phường tại Tờ trình số 42/TTr-CAP ngày 27 tháng 02 năm 2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn phường Nam Gia Nghĩa.

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

Điều 3. Chánh Văn phòng HĐND và UBND phường; Trưởng Công an phường; Thủ trưởng các cơ quan, đơn vị 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 (b/c);
- Thường trực Đảng ủy phường (b/c);
- Thường trực HĐND phường (b/c);
- Chủ tịch, PCT. UBND phường;
- Văn phòng Đảng ủy phường;
- Văn phòng UBND, HĐND phường;
- Trang TTĐT phường (đăng công báo);
- Lưu: VT,CAP.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D PHƯỜNG NAM GIA NGHĨA T. LÂM ĐỒNG

Phan Văn Quốc

ỦY BAN NHÂN DÂN PHƯỜNG NAM GIA NGHĨA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn phường Nam Gia Nghĩa

(Ban hành kèm theo Quyết định số 157/QĐ-UBND ngày 27/02/2026 của Ủy ban nhân dân phường Nam Gia Nghĩa)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Phạm vi điều chỉnh:

Quy chế này quy định về bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin cấp phường.

2. Đối tượng áp dụng:

Các phòng, trung tâm, đơn vị thuộc phường, Thủ trưởng các cơ quan đơn vị thuộc phường, cán bộ, công chức, viên chức, và tổ chức, cá nhân có liên quan đến việc quản lý, vận hành, khai thác hệ thống thông tin cấp phường.

Điều 2. Giải thích từ ngữ

1. An ninh mạng là sự bảo đảm thông tin trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. 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 là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Đối với các hệ thống thông tin chuyên ngành, chủ quản là UBND phường được giao quản lý, vận hành hệ thống đó.

5. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành. Trong trường hợp thuê dịch vụ công nghệ thông tin, đơn vị vận hành là bên cung cấp dịch vụ.

6. Đơn vị chuyên trách về an ninh mạng, an toàn thông tin là đơn vị có chức năng, nhiệm vụ tham mưu, điều phối, giám sát, kiểm tra, đôn đốc và tổ chức thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin trên địa bàn phường.

7. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. Phần mềm mã độc 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.

9. Tài sản công nghệ thông tin bao gồm tài sản thông tin (dữ liệu số), tài sản vật lý (thiết bị phần cứng, vật mang tin) và tài sản phần mềm (hệ điều hành, ứng dụng, mã nguồn).

Điều 3. Nguyên tắc bảo đảm an ninh mạng, an toàn thông tin

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. Bảo đảm an ninh mạng, an toàn thông tin là nhiệm vụ trọng yếu, thường xuyên, liên tục, được ưu tiên trong các kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số và phát triển kinh tế - xã hội của phường.

3. Bảo đảm an toàn hệ thống thông tin theo cấp độ là biện pháp trọng tâm, cốt lõi để bảo vệ hệ thống thông tin. Hoạt động này phải được thực hiện từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ hệ thống.

4. Mọi hệ thống thông tin phải được giám sát an toàn thông tin và có phương án ứng cứu, khắc phục sự cố, duy trì hoạt động giao dịch bình thường, sẵn sàng cho các tình huống khẩn cấp.

5. Thực hiện phương châm "4 tại chỗ" trong ứng cứu sự cố: chỉ huy tại chỗ, lực lượng tại chỗ, phương tiện tại chỗ và hậu cần tại chỗ. Ứng cứu sự cố trước hết phải được thực hiện bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

6. Có sự phối hợp chặt chẽ, thống nhất, phân định rõ trách nhiệm giữa các cơ quan, đơn vị dưới sự chỉ đạo, điều phối của UBND phường và sự tham mưu, hướng dẫn của Công an phường.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 8 Luật An ninh mạng.

2. Các hành vi bị nghiêm cấm về an toàn thông tin quy định tại Điều 7 Luật An toàn thông tin.

3. Hành vi nghiêm cấm khác về an ninh mạng, an toàn thông tin theo quy định của pháp luật.

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Bảo đảm an ninh mạng, an toàn thông tin khi sử dụng máy tính, thiết bị ngoại vi và phần mềm

1. Máy tính và các thiết bị ngoại vi tại các cơ quan, đơn vị phải được cài đặt hệ điều hành, phần mềm ứng dụng có bản quyền hoặc sử dụng phần mềm mã nguồn mở hợp pháp, có nguồn gốc rõ ràng.

2. Chỉ cài đặt các phần mềm nằm trong danh mục được phép sử dụng do cơ quan có thẩm quyền ban hành (nếu có). Nghiêm cấm việc tự ý cài đặt các phần mềm không rõ nguồn gốc, phần mềm bẻ khóa, các phần mềm không phục vụ công tác chuyên môn hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

3. Tất cả các máy tính phải được cài đặt phần mềm phòng, chống mã độc và được thiết lập chế độ cập nhật tự động cơ sở dữ liệu nhận dạng mã độc. Người sử dụng có trách nhiệm thường xuyên rà quét mã độc đối với máy tính và các thiết bị lưu trữ di động (USB, ổ cứng ngoài) trước khi sử dụng.

4. Khi phát hiện máy tính có dấu hiệu bất thường (hoạt động chậm, tự động mở các cửa sổ lạ, mất dữ liệu, nhận được cảnh báo từ phần mềm diệt virus), người sử dụng phải ngay lập tức ngắt kết nối mạng của máy tính đó và báo cáo cho bộ phận chuyên trách công nghệ thông tin của đơn vị để được hỗ trợ, xử lý kịp thời.

5. Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, tệp đính kèm hoặc liên kết trong thư điện tử không rõ nguồn gốc, có dấu hiệu đáng ngờ; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

6. Người sử dụng phải khóa màn hình máy tính (sử dụng tính năng có sẵn của hệ điều hành) khi rời khỏi vị trí làm việc và tắt hoàn toàn máy tính khi hết giờ làm việc.

Điều 6. Quản lý trang thiết bị công nghệ thông tin, an toàn, an ninh thông tin

1. Quản lý trang thiết bị công nghệ thông tin

a) Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.

b) Quy định việc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

c) Trang thiết bị công nghệ thông tin có lưu trữ bí mật nhà nước, bí mật công tác, bí mật nội bộ khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

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

đ) Các đơn vị có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

2. Quản lý an ninh mạng, an toàn thông tin

a) Các đơn vị phải xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng, an toàn thông tin đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an ninh mạng, an toàn thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

b) Các đơn vị phải thường xuyên tổ chức quán triệt các quy định về an ninh mạng, an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an ninh mạng, an toàn thông tin của từng cá nhân trong đơn vị.

c) Các đơn vị phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

d) Khi cá nhân chấm dứt hoặc thay đổi công việc, cơ quan đơn vị phải:

- Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

- Lập biên bản bàn giao tài sản công nghệ thông tin.

- Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

3. Việc kết nối thiết bị thuộc sở hữu cá nhân (máy tính xách tay, điện thoại thông minh, máy tính bảng…) vào mạng nội bộ của cơ quan, đơn vị để xử lý công việc phải được sự đồng ý của lãnh đạo đơn vị và phải tuân thủ các quy định về bảo đảm an ninh mạng, an toàn thông tin được quy định tại quy chế này; chịu sự giám sát của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

4. Hệ thống mạng không dây (Wi-Fi) tại các cơ quan, đơn vị phải được cấu hình bảo mật, sử dụng các giao thức mã hóa mạnh (như WPA2/WPA3), đặt mật khẩu phức tạp và thay đổi định kỳ. Mạng Wi-Fi dành cho khách phải được thiết lập riêng biệt, tách biệt hoàn toàn với mạng nội bộ.

Điều 7. Bảo vệ bí mật nhà nước trên không gian mạng

1. Nghiêm cấm việc soạn thảo, lưu trữ, xử lý, gửi, nhận thông tin, tài liệu thuộc phạm vi bí mật nhà nước trên các máy tính, thiết bị có kết nối mạng Internet, mạng viễn thông, mạng máy tính nội bộ không đáp ứng yêu cầu bảo mật.

2. Các cơ quan, đơn vị có xử lý thông tin bí mật nhà nước phải bố trí máy tính, máy in và các thiết bị ngoại vi được tách biệt hoàn toàn về mặt vật lý với mạng Internet và các mạng máy tính khác để phục vụ riêng cho việc soạn thảo, lưu trữ, in ấn tài liệu bí mật nhà nước.

3. Việc truyền đưa thông tin thuộc bí mật nhà nước qua không gian mạng phải được mã hóa bằng sản phẩm mật mã của Ban Cơ yếu Chính phủ và tuân thủ tuyệt đối các quy định của pháp luật về bảo vệ bí mật nhà nước và pháp luật về cơ yếu.

4. Các thiết bị lưu trữ di động (USB, ổ cứng ngoài) dùng để sao chép, lưu trữ tài liệu bí mật nhà nước phải được quản lý chặt chẽ, sử dụng riêng và áp dụng các biện pháp mã hóa để bảo vệ dữ liệu.

Điều 8. Quản lý tài khoản và mật khẩu truy cập

1. Tài khoản truy cập các hệ thống thông tin của phường được cấp cho từng cá nhân và chỉ dùng để thực hiện các nhiệm vụ theo quyền hạn được phân công. Nghiêm cấm việc sử dụng chung tài khoản, chia sẻ thông tin tài khoản và mật khẩu cho người khác.

2. Mật khẩu truy cập phải được đặt theo quy tắc an toàn: có độ dài tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt (như @, #, !...). Người sử dụng phải thay đổi mật khẩu định kỳ tối thiểu 03 tháng một lần hoặc ngay khi có yêu cầu từ quản trị hệ thống hoặc khi nghi ngờ bị lộ, lọt.

3. Không sử dụng tính năng lưu mật khẩu tự động trên các trình duyệt web đối với các hệ thống thông tin quan trọng. Phải đăng xuất khỏi các hệ thống thông tin khi không còn sử dụng.

4. Khi cán bộ, công chức, viên chức và người lao động chuyển công tác, thôi việc hoặc thay đổi vị trí công việc, bộ phận chuyên trách công nghệ thông tin của đơn vị có trách nhiệm thu hồi hoặc vô hiệu hóa tất cả các tài khoản truy cập đã cấp cho cá nhân đó trong vòng 24 giờ.

Chương III

BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 9. Phân loại và xác định cấp độ an toàn hệ thống thông tin

1. Tất cả các hệ thống thông tin do các cơ quan, đơn vị trong phường quản lý, vận hành phải được phân loại và xác định cấp độ an toàn hệ thống thông tin để áp dụng các biện pháp quản lý và kỹ thuật tương ứng nhằm bảo vệ hệ thống thông tin.

2. Việc phân loại cấp độ an toàn hệ thống thông tin được thực hiện theo 5 cấp độ, từ cấp độ 1 đến cấp độ 5, dựa trên các tiêu chí quy định từ Điều 7 đến Điều 11 của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ.

3. Chủ quản hệ thống thông tin có trách nhiệm chủ trì, chỉ đạo đơn vị vận hành hệ thống thông tin thực hiện việc xác định và đề xuất cấp độ an toàn cho các hệ thống thông tin thuộc phạm vi quản lý của mình.

Điều 10. Lập hồ sơ đề xuất cấp độ

Đơn vị vận hành hệ thống thông tin có trách nhiệm lập hồ sơ đề xuất cấp độ theo quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ, bao gồm tài liệu mô tả tổng quan, thiết kế hệ thống, thuyết minh đề xuất cấp độ và thuyết minh phương án bảo đảm an toàn thông tin.

Điều 11. Phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt

1. Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo đơn vị vận hành xây dựng và triển khai đầy đủ phương án bảo đảm an toàn thông tin đã được phê duyệt trong hồ sơ đề xuất cấp độ.

2. Phương án bảo đảm an toàn thông tin phải đáp ứng các yêu cầu về quản lý, kỹ thuật tương ứng với cấp độ đã được phê duyệt, bao gồm các nội dung chính theo quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ và các điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia quy định từ Điều 8 đến Điều 12 Nghị định số 53/2022/NĐ-CP (nếu thuộc danh mục).

3. Công an phường có trách nhiệm hướng dẫn, đôn đốc, kiểm tra việc triển khai phương án bảo đảm an toàn thông tin tại các cơ quan, đơn vị.

Chương IV

GIÁM SÁT, CẢNH BÁO, ỨNG CỨU SỰ CỐ VÀ KIỂM TRA, ĐÁNH GIÁ

Điều 12. Giám sát an ninh mạng, an toàn thông tin

1. Tất cả các hệ thống thông tin từ cấp độ 3 trở lên phải được giám sát an toàn thông tin thường xuyên, liên tục 24/7. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với Công an phường tổ chức thực hiện việc giám sát hệ thống thông tin theo Điều 15 của Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ và Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông.

2. Các cơ quan, đơn vị là chủ quản hệ thống thông tin có trách nhiệm triển khai hệ thống giám sát an toàn thông tin cho các hệ thống thuộc phạm vi quản lý (có thể tự triển khai hoặc thuê dịch vụ chuyên nghiệp).

3. Các hệ thống thông tin của các cơ quan, đơn vị phải được kết nối, chia sẻ thông tin, dữ liệu giám sát về Trung tâm Giám sát an toàn, an ninh tập trung (SOC) của tỉnh để thực hiện giám sát tập trung, phân tích, cảnh báo sớm các

nguy cơ, mối đe dọa trên toàn phường và kết nối, chia sẻ kết quả giám sát về Trung tâm an ninh mạng quốc gia (thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an).

4. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, việc giám sát an ninh mạng thực hiện theo quy định tại Điều 14 Luật An ninh mạng.

Điều 13. Tiếp nhận, báo cáo và phân loại sự cố

1. Quy trình báo cáo sự cố được thực hiện thống nhất trên toàn phường nhằm đảm bảo thông tin được xử lý nhanh chóng, kịp thời.

2. Khi phát hiện sự cố, đơn vị vận hành hệ thống thông tin có trách nhiệm thực hiện các bước sau theo quy định tại Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông:

a) Thông báo sự cố: Chậm nhất 05 ngày kể từ khi phát hiện sự cố, phải gửi "Thông báo sự cố" (nội dung theo điểm a khoản 3 Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông đến đồng thời: Chủ quản hệ thống thông tin và Đơn vị chuyên trách của phường (Công an phường).

b) Báo cáo ban đầu: Trong trường hợp sự cố có nguy cơ lan rộng, ảnh hưởng nghiêm trọng hoặc vượt quá khả năng xử lý của đơn vị, phải ngay lập tức lập "Báo cáo ban đầu sự cố" (sử dụng Mẫu số 03 tại Phụ lục I Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông) gửi chủ quản hệ thống thông tin và Đơn vị chuyên trách của phường (Công an phường) để yêu cầu hỗ trợ, điều phối.

c) Báo cáo kết thúc: Sau khi xử lý xong sự cố, trong vòng 05 ngày, phải hoàn thiện "Báo cáo kết thúc ứng phó sự cố" (sử dụng Mẫu số 04 tại Phụ lục I Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông) gửi các cơ quan đã nhận báo cáo trước đó.

Điều 14. Ứng cứu sự cố an toàn hệ thống tin

1. Đội ứng cứu sự cố an toàn thông tin mạng phường có vai trò là đầu mối điều phối các hoạt động ứng cứu sự cố trên toàn phường.

2. Nguyên tắc ứng cứu sự cố

Ưu tiên xử lý tại chỗ bằng lực lượng của chủ quản hệ thống thông tin. Khi sự cố vượt quá khả năng, chủ quản hệ thống thông tin phải báo cáo ngay cho Đội ứng cứu sự cố an toàn thông tin mạng phường để kích hoạt cơ chế điều phối.

3. Khi nhận được yêu cầu điều phối, Đội ứng cứu sự cố an toàn thông tin mạng có thẩm quyền:

a) Chủ trì, điều hành, phân công nhiệm vụ cho các thành viên Đội ứng cứu sự cố an toàn thông tin mạng phường và các cơ quan, đơn vị liên quan.

b) Yêu cầu các đơn vị cung cấp dịch vụ viễn thông, Internet trên địa bàn phối hợp ngăn chặn nguồn tấn công, lọc lưu lượng độc hại.

c) Là đầu mối liên lạc, phối hợp với Công an tỉnh, Trung tâm An ninh mạng quốc gia và các cơ quan Trung ương trong các trường hợp cần thiết.

d) Quyết định các phương án ứng phó, khắc phục sự cố theo quy định tại Điều 17 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ.

4. Kế hoạch ứng phó sự cố bảo đảm an ninh mạng, an toàn thông tin

Các cơ quan, đơn vị thực hiện kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý và tổ chức triển khai kế hoạch sau khi phê duyệt.

Điều 15. Kiểm tra, đánh giá an toàn thông tin

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Hoạt động kiểm tra, đánh giá an ninh mạng, an toàn thông tin được thực hiện định kỳ hoặc đột xuất nhằm xác định thực trạng, phát hiện các điểm yếu, lỗ hổng bảo mật và đánh giá sự tuân thủ các quy định.

4. Việc kiểm tra, đánh giá được thực hiện 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:

a) Hàng năm đối với hệ thống thông tin cấp độ 3 và 4;

b) 06 tháng một lần đối với hệ thống thông tin cấp độ 5.

5. Trình tự, thủ tục kiểm tra:

Việc kiểm tra đột xuất được thực hiện theo trình tự, thủ tục quy định tại Điều 16 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ. Đơn vị chuyên trách về an toàn thông tin mạng có trách nhiệm thông báo kế hoạch kiểm tra, thành lập đoàn kiểm tra, lập biên bản và thông báo kết quả kiểm tra cho đơn vị được kiểm tra.

6. Các cơ quan, đơn vị được kiểm tra có trách nhiệm phối hợp, cung cấp thông tin, tài liệu và tạo điều kiện cần thiết cho đoàn kiểm tra hoàn thành nhiệm vụ.

Điều 16. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng, an toàn thông tin

1. Các cơ quan, đơn vị xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại đơn vị mình gửi Công an phường tổng hợp để đề xuất Công an tỉnh.

2. Các cơ quan, đơn vị tham gia đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an ninh mạng, an toàn thông tin các đơn vị trực thuộc; tham gia đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị.

3. Các cơ quan, đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an ninh mạng, an toàn thông tin đến toàn thể cán bộ, công chức, viên chức và người lao động tại đơn vị.

Chương V

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC, CÁ NHÂN

Điều 17. Trách nhiệm của Công an phường

Với vai trò là đơn vị chuyên trách về an toàn thông tin mạng của Ủy ban nhân dân phường, Công an phường chịu trách nhiệm trước Ủy ban nhân dân phường, Chủ tịch Ủy ban nhân dân phường và có các nhiệm vụ, quyền hạn sau:

1. Tham mưu và quản lý nhà nước:

a) Chủ trì tham mưu, giúp Ủy ban nhân dân phường thực hiện công tác quản lý nhà nước về an ninh mạng, an toàn thông tin trên địa bàn.

b) Xây dựng, trình Ủy ban nhân dân phường ban hành và tổ chức thực hiện các kế hoạch, chương trình, đề án của phường về an ninh mạng, an toàn thông tin.

2. Giám sát và cảnh báo:

a) Tổ chức giám sát tập trung, phân tích, cảnh báo sớm các nguy cơ, mối đe dọa an ninh mạng, an toàn thông tin.

b) Phối hợp với cơ quan chủ quản hệ thống trong bảo đảm an ninh mạng, an toàn thông tin cho hạ tầng kỹ thuật của Trung tâm dữ liệu phường.

c) Phối hợp với Công an tỉnh, các cơ quan chức năng xử lý thông tin vi phạm pháp luật trên không gian mạng.

d) Phối hợp tổ chức triển khai kết nối, chia sẻ thông tin giám sát, cảnh báo với Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

3. Ứng cứu sự cố an toàn thông tin mạng:

Phối hợp tổ chức triển khai hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của phường, kết nối với hệ thống phương án ứng cứu quốc gia.

4. Phòng, chống tội phạm và vi phạm pháp luật:

a) Phối hợp với Công an tỉnh, các cơ quan chức năng trong công tác phòng, chống tấn công mạng, gián điệp mạng, khủng bố mạng, phòng, chống mã độc và các loại tội phạm sử dụng công nghệ cao. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao.

b) Điều tra, xử lý các hành vi vi phạm pháp luật về an ninh mạng, an toàn thông tin theo thẩm quyền.

c) Chủ trì triển khai các biện pháp bảo đảm an toàn thông tin cá nhân trên mạng và bảo vệ trẻ em trên không gian mạng.

5. Hướng dẫn và báo cáo:

a) Phối hợp, hướng dẫn nghiệp vụ về bảo đảm an ninh mạng, an toàn thông tin; hỗ trợ giải quyết sự cố khi có yêu cầu. Hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ và triển khai thực hiện việc bảo đảm an ninh mạng, an toàn thông tin cho hệ thống thông tin theo quy định của Nhà nước.

b) Tổng hợp tình hình và định kỳ báo cáo Công an tỉnh, và các cơ quan, đơn vị có liên quan về công tác bảo đảm an ninh mạng, an toàn thông tin trên địa bàn.

Điều 18. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị là chủ quản hệ thống thông tin chịu trách nhiệm toàn diện trước Ủy ban nhân dân phường và trước pháp luật về công tác bảo đảm an ninh mạng, an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý của mình.

2. Trực tiếp chỉ đạo và phụ trách công tác bảo đảm an ninh mạng, an toàn thông tin trong hoạt động của cơ quan, đơn vị.

3. Phân công bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng, an toàn thông tin; bố trí đủ nguồn lực (nhân sự, kinh phí, trang thiết bị) để triển khai các nhiệm vụ bảo đảm an ninh mạng, an toàn thông tin.

4. Trình cấp có thẩm quyền phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin; chỉ đạo xây dựng và ban hành phương án bảo đảm an toàn thông tin tương ứng với cấp độ được duyệt và tổ chức triển khai thực hiện.

5. Ban hành và tổ chức thực hiện quy chế nội bộ về bảo đảm an ninh mạng, an toàn thông tin tại cơ quan, đơn vị mình.

6. Chỉ đạo, tổ chức thực hiện việc kiểm tra, đánh giá, quản lý rủi ro an toàn thông tin định kỳ theo quy định.

7. Phối hợp chặt chẽ với Công an phường và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh mạng, an toàn thông tin.

8. 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 ninh mạng, an toàn thông tin kịp thời, nhanh chóng và đạt hiệu quả.

9. Định kỳ hằng năm (trước ngày 15/11) báo cáo tình hình an ninh mạng, an toàn thông tin của cơ quan gửi Công an phường tổng hợp, báo cáo Ủy ban nhân dân phường.

Điều 19. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Trách nhiệm của các cơ quan, đơn vị được cấp có thẩm quyền giao vận hành hệ thống thông tin:

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

b) Thực hiện bảo vệ hệ thống thông tin theo Quy chế này, các quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin.

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng, an toàn thông tin, báo cáo Ủy ban nhân dân phường điều chỉnh nếu cần thiết.

d) Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của Ủy ban nhân dân phường hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

đ) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Công an tỉnh trong công tác bảo đảm an ninh mạng, an toàn thông tin.

e) Kịp thời thông báo sự cố an ninh mạng, an toàn thông tin và phối hợp ứng cứu xử lý sự cố an ninh mạng, an toàn thông tin với các cơ quan, đơn vị liên quan.

2. Trường hợp hệ thống thông tin do các cơ quan thực hiện đầu tư: Cơ quan chủ đầu tư đóng vai trò là đơn vị vận hành hệ thống thông tin thực hiện các quy định tại khoản 1 Điều này.

3. Trường hợp hệ thống thông tin do các cơ quan thực hiện thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Đơn vị cung cấp dịch vụ đóng vai trò là đơn vị vận hành hệ thống thông tin, có trách nhiệm thực hiện các quy định tại khoản 1 Điều này; phối hợp chặt chẽ với cơ quan chủ trì thuê dịch vụ trong quá trình thực hiện; tổng hợp báo cáo Ủy ban nhân dân phường hoặc cơ quan nhà nước có thẩm quyền thông qua đơn vị chủ trì thuê dịch vụ.

Điều 20. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Chấp hành Quy chế này, quy chế nội bộ của cơ quan và các quy định của pháp luật về an ninh mạng, an toàn thông tin. Chịu trách nhiệm bảo đảm an ninh mạng, an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm an ninh mạng, an toàn thông tin cho tài khoản, các thiết bị mà mình được giao sử dụng;

c) Khi phát hiện sự cố mất an ninh mạng, an toàn thông tin phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách công nghệ thông tin hoặc phụ trách an toàn thông tin của cơ quan để kịp thời ngăn chặn, xử lý;

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn về an ninh mạng, an toàn thông tin do Ủy ban nhân dân phường chỉ đạo hoặc cơ quan chuyên trách về an ninh mạng, an toàn thông tin tổ chức.

2. Trách nhiệm của cán bộ phụ trách công nghệ thông tin/an toàn thông tin:

Ngoài các quy định tại khoản 1 Điều này, cán bộ phụ trách công nghệ thông tin, an toàn thông tin có trách nhiệm:

a) Chủ trì tham mưu với lãnh đạo cơ quan thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến an ninh mạng, an toàn thông tin:

b) Tham mưu lãnh đạo cơ quan ban hành các quy định nội bộ và triển khai các giải pháp kỹ thuật bảo đảm an ninh mạng, an toàn thông tin;

c) Trực tiếp thiết lập hoặc tham mưu các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin;

d) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay thủ trưởng cơ quan các sự cố mất an ninh mạng, an toàn thông tin và mức độ nghiêm trọng của các sự cố đó;

đ) Phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an ninh mạng, an toàn thông tin.

Điều 21. Kinh phí thực hiện

1. Kinh phí bảo đảm an ninh mạng, an toàn thông tin được bố trí từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Căn cứ vào kế hoạch hằng năm, Công an phường có trách nhiệm phối hợp các đơn vị liên quan xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an ninh mạng, an toàn thông tin cho Ủy ban nhân dân phường; kịp thời tham mưu Ủy ban nhân dân phường bổ sung kinh phí ngoài dự toán khi phát sinh sự cố khẩn cấp, bảo đảm hệ thống nhanh chóng được khắc phục.

Điều 22. Chế độ, nội dung báo cáo

Các đơn vị báo cáo tình hình an ninh mạng, an toàn thông tin trước ngày 15/11 hằng năm cho Ủy ban nhân dân phường (qua Công an phường) như sau:

1. Báo cáo năm

a) Nội dung báo cáo:

- Việc thực hiện bảo đảm an ninh mạng, an toàn thông tin theo quy định tại Quy chế này;

- Các nội dung chỉnh sửa, bổ sung quy chế bảo đảm an ninh mạng, an toàn thông tin của đơn vị (nếu có).

b) Thời hạn gửi báo cáo: Trước ngày 15 tháng 11.

2. Báo cáo đột xuất

a) Các sự cố mất an ninh mạng, an toàn thông tin:

- Thời hạn gửi báo cáo: Trong thời gian 24 giờ kể từ thời điểm vụ việc được phát hiện;

- Nội dung vụ, việc;

- Thời gian, địa điểm phát sinh vụ, việc;

- Nguyên nhân xảy ra vụ, việc (nếu có);

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống thông tin và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan;

- Các biện pháp đơn vị đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro;

- Kiến nghị, đề xuất (nếu có).

b) Các trường hợp đột xuất khác theo yêu cầu của Ủy ban nhân dân phường.

Điều 23. Trách nhiệm thi hành.

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

2. Công an phường chủ trì, phối hợp với các cơ quan, đơn vị, địa phương triển khai thực hiện Quy chế này.

3. Thủ trưởng các cơ quan, trung tâm thuộc phường, Thủ trưởng các cơ quan đơn vị có trách nhiệm triển khai thực hiện, phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức, người lao động trong cơ quan, đơn vị Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế tại đơn vị; chịu trách nhiệm trước pháp luật và trước Ủy ban nhân dân phường về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của cơ quan, đơn vị.

4. Tổ chức, cá nhân vi phạm Quy chế này tùy mức độ sẽ bị xử lý theo quy định của pháp luật; là căn cứ đánh giá hoàn thành nhiệm vụ của người đứng đầu.

5. Các văn bản quy phạm pháp luật dẫn chiếu để áp dụng tại Quy chế này được sửa đổi, bổ sung hoặc thay thế bằng văn bản mới thì áp dụng theo các văn bản sửa đổi, bổ sung hoặc thay thế.

6. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, các đơn vị gửi về Công an phường để tổng hợp, báo cáo Ủy ban nhân dân phường xem xét, quyết định./.