ỦY BAN NHÂN DÂN **PHƯỜNG PHÙ LIỄN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:1139/QĐ-UBND	*Phù Liễn, ngày 16 tháng 04 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng phường Phù Liễn

ỦY BAN NHÂN DÂN PHƯỜNG PHÙ LIỄN

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

Căn cứ Nghị định số 42/2022/NĐ-CP ngày 24/6/2016 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Thông tư số 11/2015/TT-BTTTT ngày 05/5/2015 của Bộ Thông tin và Truyền thông về Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp; Thông tư số 17/2021/TT-BTTTT ngày 30/11/2021 của Bộ Thông tin và Truyền thông về việc sửa đổi, bổ sung một số điều Thông tư số 11/2015/TT-BTTTT ngày 05 tháng 5 năm 2015 của Bộ Thông tin và Truyền thông Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 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 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về 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,

QUYẾT ĐỊNH:

Điều 1. Ban hành theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin trong ứng dụng công nghệ thông tin tại phường Phù Liễn.

Điều 2. Quyết định này thay thế các quy định trước đây về công tác an toàn, an ninh thông tin trong ứng dụng công nghệ thông tin tại phường Phù Liễn. Quyết định này có hiệu lực từ kể từ ngày ký.

Điều 3. Giám đốc Trung tâm Phục vụ hành chính công, Thủ trưởng các phòng ban; các cơ quan, đơn vị, công chức, viên chức, người lao động thuộc Uỷ ban nhân dân Phường Phù Liễn và các cá nhân liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- CT, các PCT UBND phường;
- Như Điều 3;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Phạm Văn Diện

QUY CHẾ

Bảo đảm an toàn, an ninh thông tin mạng phường Phù Liễn

(Ban hành kèm theo Quyết định số ….1139…/QĐ-UBND ngày 16 tháng 04 năm 2026 của Ủy ban nhân dân phường Phù Liễn)

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 biện pháp, chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin các hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan của phường Phù Liễn bao gồm: Hệ thống mạng tại máy tính tại Trung tâm hành chính, Trung tâm phục vụ hành chính công và các phần mềm ứng dụng khác.

2. Đối tượng áp dụng

a) Các phòng, ban , đơn vị thuộc phường Phù Liễn.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các hệ thống thông tin của phường Phù Liễn

Điều 2. Giải thích từ ngữ

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

1. *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.

2. *Mạng* 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.

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. *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.

5. *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.

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

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của Hệ thống mạng nội bộ trung tâm hành chính phường.

2. Nguyên tắc

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

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

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

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

c) Việc bảo đảm an toàn Hệ thống mạng nội bộ trung tâm hành chính được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

3. Phạm vi chính sách an toàn thông tin

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

a) Thiết lập chính sách an toàn thông tin.

b) Tổ chức bảo đảm an toàn thông tin.

c) Bảo đảm nguồn nhân lực.

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

e) Quản lý vận hành hệ thống.

Điều 4. Những hành vi nghiêm cấm

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

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

Điều 5. Tổ chức bảo đảm an toàn thông tin

1. Trách nhiệm của Trung tâm Phục vụ hành chính công

a) Thực hiện trách nhiệm của đơn vị vận hành hệ thống và đơn vị chuyên trách về an toàn thông tin theo quy định tại Điều 21 và Điều 22, 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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về 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.

b) Chỉ đạo, tổ chức, thực hiện quản lý; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật, triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

c) Là đầu mối liên hệ, phối hợp với Sở Khoa học và Công nghệ, Công an thành phố 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.

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

Điều 6. Bảo đảm nguồn nhân lực

1. Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ

Điều kiện tuyển dụng cán bộ: Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng. Có bằng tốt nghiệp Đại học trở lên thuộc một trong các nhóm ngành: Máy tính; Công nghệ thông tin …. Có chứng chỉ bồi dưỡng nghiệp vụ quản lý nhà nước ngạch chuyên viên hoặc tương đương trở lên;

2. Quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

a) Cán bộ chuyên trách an toàn thông tin phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

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

c) Các cơ quan địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ công nghệ thông tin của Phường 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.

3. Trung tâm Phục vụ hành chính công có trách nhiệm xây dựng kế hoạch và định kỳ hằng năm tổ chức đào tạo, phổ biến tuyên truyền nâng cao nhận thức về an toàn thông tin cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

4. Với người sử dụng trong quá trình làm việc

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

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

- Cá nhân, tổ 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 thiết bị.

5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:

a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức.

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

c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật các thông tin liên quan gây mất ATTT sau khi nghỉ việc.

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

Điều 7. Quản lý thiết kế, xây dựng hệ thống thông tin

1. Khi xây dựng mới và đưa hệ thống thông tin vào vận hành, đơn vị quản lý hệ thống thông tin có trách nhiệm:

a) Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

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

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

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

2. Khi có thay đổi thiết kế, nâng cấp hệ thống thông tin, đơn vị quản lý hệ thống phải đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

Điều 8. Phát triển phần mềm thuê khoán

1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Các nhà phát triển phải cung cấp mã nguồn phần mềm.

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

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

5. UBND phường tùy theo từng hợp đồng thuê khoán phần mềm, chỉ định bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

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

Điều 9. Quản lý an toàn mạng

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

a) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn bảo mật.

b) 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.

c) Mạng không dây (WIFI) cần thiết lập các thông số an toàn và định kỳ ít nhất 6 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

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

Triển khai các hệ thống/phương án lưu trữ độc lập để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ

bản sau: tập tin cấu hình hệ thống, firmware các thiết bị mạng (firewall, router, switch, access point ...).

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

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

Điều 10. Quản lý an toàn máy chủ và ứng dụng

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

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

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

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

- Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ

Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

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

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

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

Triển khai hệ thống/phương án lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

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

- Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận công nghệ thông tin của đơn vị.

- Đơn vị chuyên môn của cơ quan, đơn vị khác chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc của đơn vị mình.

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

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

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

e) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

Điều 11. Quản lý an toàn dữ liệu

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

a) Đơn vị vận hành hệ thống chủ trì, phối hợp với đơn vị tư vấn xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

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

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

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

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

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

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

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

5. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ.

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

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

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

a) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có). Bản sao lưu được lưu trữ tối thiểu thành 02 bản và được lưu trữ ở hai địa chỉ khác nhau.

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

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

Điều 12. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin

a) Mức 0 (không): sự cố không gây ảnh hưởng có hại tức thời đến hoạt động và dữ liệu của hệ thống. Tuy nhiên, cần phân tích và báo cáo lại để tránh phát sinh những sự cố khác trong tương lai.

b) Mức 1 (thấp): sự cố gây ảnh hưởng tới các hệ thống nói chung, gây ảnh hưởng nhỏ hoặc không đáng kể đến hoạt động của hệ thống hoặc dữ liệu của hệ thống, gây ra những tác động không đáng kể cho đơn vị hoặc cho xã hội.

c) Mức 2 (trung bình): sự cố gây ảnh hưởng tới các hệ thống quan trọng hoặc thông thường, gây ảnh hưởng đáng kể đến hoạt động hoặc dữ liệu của hệ thống, hoặc gây ra những tác động đáng kể cho đơn vị hoặc cho xã hội.

d) Mức 3 (nghiêm trọng): sự cố xảy ra đối với các hệ thống đặc biệt quan trọng hoặc các hệ thống quan trọng, gây ảnh hưởng nghiêm trọng đến hoạt động của hệ thống, bao gồm việc ngừng hoạt động trong một thời gian dài hoặc thiệt hại nghiêm trọng đến dữ liệu của hệ thống; hoặc gây đến những tác động nghiêm trọng cho đơn vị hoặc cho xã hội.

đ) Mức 4 (đặc biệt nghiêm trọng): sự cố xảy ra đối với các hệ thống đặc biệt quan trọng, làm tê liệt hoạt động của hệ thống hoặc thiệt hại rất nghiêm trọng tới dữ liệu của hệ thống; gây nên những tác động đặc biệt nghiêm trọng hoặc làm ảnh hưởng lớn tới trật tự xã hội, lợi ích công cộng, đe dọa nghiêm trọng tới an ninh, quốc phòng của đất nước.

2. Đơn vị, cá nhân vận hành hệ thống thông tin khi phát hiện, tiếp nhận, xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng, có trách nhiệm:

a) Khi phát hiện sự cố: Tổ chức theo dõi, ghi chép và tập hợp các thông tin liên quan đến sự cố và tổ chức thông báo hoặc báo cáo sự cố. Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử (có ký tên và đóng dấu hoặc chữ ký số của người có thẩm quyền).

b) Khi tiếp nhận thông báo sự cố: Phản hồi ngay cho tổ chức, cá nhân gửi thông báo sự cố để xác nhận thông tin;

c) Xác minh sự cố và xử lý ban đầu: Chủ trì, phối hợp với đơn vị chịu trách nhiệm bảo đảm an toàn thông tin (nếu có), đơn vị chuyên trách về ứng cứu sự cố

liên quan và các doanh nghiệp viễn thông, Internet (ISP) để tiến hành phân tích, xác minh, đánh giá sự cố; thực hiện ngay các hoạt động ứng cứu sự cố ban đầu, triển khai quy trình ứng cứu sự cố.

3. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

a) Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng.

b) Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

c) Triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

d) Đơn vị, cá nhân vận hành hệ thống chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

đ) Đơn vị, cá nhân vận hành hệ thống và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

4. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin:

Đơn vị vận hành hệ thống phối hợp với các 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 liên quan đến hệ thống

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

Bước 1: Thông báo sự cố

Cán bộ công chức, viên chức, người lao động tại các phòng, ban, đơn vị thuộc Phường, khi gặp sự cố trong quá trình sử dụng hệ thống thông tin thực hiện thông báo ngay cho Trung tâm Phục vụ hành chính công phường.

Bước 2: Tiếp nhận sự cố

Trung tâm Phục vụ hành chính công tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp, ...

Bước 3: Xác minh/xác nhận sự cố

Trung tâm Phục vụ hành chính công triển khai tiến hành xác minh, xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xãy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);
- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);
- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);
- Và địa điểm xảy ra sự cố.

Bước 4: Phân loại sự cố

Trung tâm Phục vụ hành chính công thực hiện phân loại sự cố (các loại sự cố ở Điều 5)

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

Ngay sau khi phân loại được sự cố Trung tâm Phục vụ hành chính công có trách nhiệm báo cáo lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành xử lý.

Trường hợp sự cố được phân loại thông thường Trung tâm Phục vụ hành chính công chủ trì khắc phục sự cố, tổng hợp báo cáo UBND Phường

Trường hợp sự cố được phân loại nghiêm trọng thì gửi báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hải Phòng (qua Sở Khoa học và Công nghệ, Công an thành phố) về sự cố nghiêm trọng để có phương án ứng cứu và tổ chức ứng cứu, xử lý sự cố.

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

Điều 13. Quản lý an toàn thông tin hệ thống camera

1. Yêu cầu an toàn thông tin về mặt kỹ thuật

a) Bảo đảm không truyền, lưu trữ các dữ liệu phát sinh trong quá trình hoạt động cho các đối tượng không được cấp quyền truy cập;

b) Không sử dụng thiết bị camera từ các nhà sản xuất đã bị cảnh báo không đảm bảo an toàn thông tin bởi các tổ chức uy tín trên thế giới;

c) Phải có cơ chế xác thực bằng mật khẩu (có 8 ký tự trở lên, bao gồm số, chữ in hoa, in thường và ký tự đặc biệt hoặc các biện pháp tăng tính bảo mật khác như xác nhận qua mail, OTP);

d) Hỗ trợ cơ chế cập nhật phần mềm;

đ) Nhà cung cấp camera phải cung cấp chứng nhận xuất xứ (CO) của sản phẩm hoặc các bán thành phẩm cấu tạo nên sản phẩm hoặc các nguyên vật liệu là vi mạch tích hợp cấu tạo nên bo mạch chủ. Và đảm bảo sản phẩm hoặc các bán thành phẩm cấu tạo nên sản phẩm hoặc các nguyên vật liệu là vi mạch tích hợp cấu tạo nên bo mạch chủ được sản xuất hoặc gia công bởi các nhà sản xuất có uy tín.

e) Có phương án chống lại các cuộc tấn công như DDos, tấn công cơ sở dữ liệu, tấn công bằng phần mềm độc hại, tấn công Brute-force;

f) Hỗ trợ đáp ứng các tiêu chuẩn an toàn tầng giao vận và an toàn truyền tệp tin;

g) Bảo đảm thiết bị camera được bảo mật mật khẩu, lọc địa chỉ IP, mã hóa HTTPS, kiểm soát truy cập mạng IEEE 802.1X, xác thực thông tin nhật ký truy cập người dùng;

2. Yêu cầu an toàn thông tin về mặt quản lý

a) Đơn vị quản lý hệ thống camera có trách nhiệm phân công nhân sự phụ trách quản trị hệ thống của đơn vị mình; quản lý, lưu trữ bảo mật và thường xuyên thay đổi mật khẩu tài khoản quản trị. Việc cấp, quản lý tài khoản truy cập vào các hệ thống camera thuộc quản lý của đơn vị phải phù hợp với chức năng, nhiệm vụ và phân quyền của từng đối tượng sử dụng.

b) Người đứng đầu cơ quan, đơn vị và các cá nhân được cấp tài khoản truy cập vào hệ thống quản lý camera có trách nhiệm quản lý tài khoản được cấp, thường xuyên thay đổi mật khẩu truy cập và áp dụng các biện pháp phù hợp để phòng, chống các hành vi truy cập, xâm nhập và khai thác trái phép vào hệ thống camera.

c) Các hoạt động thay đổi về dữ liệu, quá trình đăng nhập hệ thống phải được ghi nhận vào nhật ký của hệ thống quản lý tập trung camera giám sát.

Điều 14. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận vận hành hệ thống.

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

2. Trong quá trình sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

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

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

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

Điều 15. Phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

1. Quản lý thiết bị công nghệ thông tin khi sửa chữa, thanh lý

a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, …) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không lộ lọt thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành. Có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu

b). Trước khi tiến hành thanh lý, loại bỏ thiết bị công nghệ thông tin cũ phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi. Với trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

2. Việc thu hồi hoặc chuyển giao phần cứng, phần mềm giữa các phòng, đơn vị, bộ phận trực thuộc phải được lập thành biên bản trong đó có chứng kiến và ký xác nhận của lãnh đạo các phòng, đơn vị, bộ phận thực hiện việc giao nhận và bộ phận chuyên trách công nghệ thông tin của đơn vị. Việc sao lưu dữ liệu phải được các bên thực hiện trước khi thu hồi hoặc bàn giao và phải được ghi rõ trong nội dung biên bản.

Chương IV
KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 16. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ;

b) Đánh giá hiệu quả của các biện pháp bảo đảm an toàn hệ thống thông tin;

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

d) Kiểm tra, đánh giá khác do Ủy ban nhân dân thành phố quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ hoặc theo kế hoạch của Ủy ban nhân dân thành phố, Uỷ ban nhân dân phường;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

4. Đối tượng kiểm tra, đánh giá là các hệ thống thông tin có liên quan.

Điều 17. Quản lý rủi ro

1. Xác định mức rủi ro.

Khi thực hiện đánh giá và quản lý rủi ro an toàn thông tin cần xác định đầy đủ về các rủi ro an toàn thông tin có khả năng gặp phải, đánh giá sắp xếp mức độ ưu tiên và xây dựng hệ thống các biện pháp kiểm soát tổng thể, thống nhất và đầy đủ để giảm thiểu rủi ro.

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

Hoạt động đánh giá và quản lý rủi ro của đơn vị vận hành, quản lý hệ thống bao gồm các 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý rủi ro; (4) Chấp nhận rủi ro

3. Biện pháp kiểm soát rủi ro.

a. Theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, hệ thống thông tin phải đáp ứng các yêu cầu an toàn cơ bản, tối thiểu. Tuy nhiên, mỗi hệ thống thông tin khác nhau sẽ có sẽ có đặc thù riêng và yêu cầu mức độ an toàn khác nhau phù hợp với yêu cầu thực tế. Do đó, trên cơ sở đánh giá và quản lý rủi ro cần rà soát, bổ sung các yêu cầu an toàn (biện pháp kiểm soát rủi ro) cho phù hợp với yêu cầu thực tế.

b. Các biện pháp kiểm soát cơ bản đối với hệ thống thông tin được quy định tại Điều 19 Nghị định 85/2016/NĐ-CP ngày 10/7/2016, Điều 9, 10 Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017.

Điều 18. Xây dựng, rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 02 năm hoặc khi có thay đổi lớn về hệ thống, Quy chế bảo đảm an toàn thông tin sẽ được kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. Quy chế sau khi điều chỉnh sẽ được trình lên UBND phường xem xét thông qua trước khi công bố áp dụng.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Trung tâm Phục vụ hành chính công phường để tổng hợp, trình lãnh đạo UBND xem xét, sửa đổi, bổ sung quy chế cho phù hợp./.