ỦY BAN NHÂN DÂN **PHƯỜNG AN HẢI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:1076 /QĐ-UBND	*An Hải, ngày 25 tháng 6 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh mạng trong hoạt động ứng dụng Công nghệ thông tin của UBND phường An Hải

UỶ BAN NHÂN DÂN PHƯỜNG AN HẢI

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

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Văn bản hợp nhất số 65/VBHN-VPQH ngày 15/08/2025 của Văn phòng Quốc hội về Luật Công nghệ thông tin;

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 24/6/2022 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 Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng;

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

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 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Văn bản hợp nhất số 12/VBHN-BTTTT ngày 26/9/2022 của Bộ Thông tin và Truyền thông về việc quy định chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp;

Theo đề nghị của Trưởng phòng Văn hoá - Xã hội phường.

QUYẾT ĐỊNH:

Điều 1. Ban hành theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại UBND phường An Hải.

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

Điều 3. Chánh Văn phòng Hội đồng nhân dân và Ủy ban nhân dân phường, Trưởng các phòng, cơ quan, đơn vị, công chức, viên chức, người lao động thuộc UBND phường An Hải và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Công an thành phố; (để báo cáo)
- Thường trực Đảng ủy;
- Thường trực HĐND phường;
- Lãnh đạo UBND phường;
- Các phòng chuyên môn;
- Như điều 3;
- Lưu: VT, HS.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D PHƯỜNG AN HẢI T.P HẢI PHÒNG

Lương Thế Quý

UỶ BAN NHÂN DÂN **PHƯỜNG AN HẢI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ
Bảo đảm an toàn, an ninh mạng trong ứng dụng công nghệ thông tin của các cơ quan tại UBND phường An Hải

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng 6 năm 2026 của UBND phường An Hải)

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 giải pháp 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 tại UBND phường An Hải.

2. Đối tượng áp dụng

a) Các phòng, ban đơn vị thuộc UBND phường An Hải.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống thông tin mạng nội bộ tại UBND phường An Hải.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng phục vụ hoạt động của Hệ thống thông tin mạng nội bộ tại UBND phường An Hải.

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. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

5. *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.

6. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

7. *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.

8. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. *Đánh giá rủi ro an toàn thông tin mạng* là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

10. *Quản lý rủi ro an toàn thông tin mạng* là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

11. *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.

12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

14. *Xung đột thông tin* là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

15. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó.

17. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

18. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

20. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, 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 thông tin mạng nội bộ UBND 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:

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

- 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 số 86/2015/QH13 và Điều 8 Luật An ninh mạng số 24/2018/QH14.

2. Đăng tải, phát tán thông tin có nội dung sau trên không gian mạng:

a) Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

b) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

c) Bịa đặt, vu khống, thông tin sai sự thật, xâm phạm nhân phẩm, danh dự, uy tín của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

3. Thực hiện hành vi sau trên không gian mạng:

a) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Kích động, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

c) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh; chiếm đoạt, mua bán, thu giữ, cố ý làm lộ bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người, các bộ phận cơ thể người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

đ) Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

e) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng, tài sản mã hóa, tài sản số của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức;

g) Sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; tạo lập, đăng tải, phát tán thông tin quy định tại khoản 2 Điều này;

h) Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác;

i) Hướng dẫn, xúi giục, lôi kéo, kích động người khác phạm tội hoặc thực hiện hành vi vi phạm pháp luật;

k) Thực hiện hành vi khác trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

4. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin.

5. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoặc phát tán thư rác, tin nhắn rác, cuộc gọi rác, chương trình tin học gây hại đến hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử.

6. Xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

7. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

8. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi

9. 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/5G, điện thoại di động, máy tính bảng, máy tính xách tay).

10. 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. Đầu mối phối hợp với các cơ quan, tổ chức có thẩm quyền

a) Giao Văn phòng HĐND và UBND phường là đầu mối liên hệ, phối hợp với 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 Hệ thống thông tin tại UBND phường An Hải.

b) Văn phòng HĐND và UBND phối hợp với Tổ chuyên trách an toàn thông tin phường làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống thông tin mạng nội bộ tại Uỷ ban nhân dân. Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

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

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

b) Là đầu mối liên hệ, phối hợp với 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 do UBND phường triển khai;

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

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

e) Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh

chóng và đạt hiệu quả;

f) Phối hợp chặt chẽ với Công an thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

Điều 6. Bảo đảm nguồn nhân lực

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

a) 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;

b) Hội đồng tuyển dụng cán bộ an toàn thông tin phải có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

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 phụ 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 phụ 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, đơn vị và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của Hệ thống mạng máy tính tại Uỷ ban nhân dân 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. Văn phòng HĐND và UBND phường 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:

- 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

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. Quản lý phát triển phần mềm và dịch vụ thuê khoán

1. Quản lý phát triển phần mềm thuê khoán.

Việc quản lý phát triển phần mềm theo hình thức thuê khoán phải tuân thủ các yêu cầu sau:

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

b) Đơn vị phát triển phần mềm phải cung cấp đầy đủ mã nguồn phần mềm và các tài liệu kỹ thuật liên quan cho đơn vị khi bàn giao sản phẩm.

c) Phần mềm thuê khoán phải được kiểm thử trên môi trường thử nghiệm trước khi đưa vào sử dụng chính thức.

d) Phần mềm phải được kiểm tra, đánh giá về an toàn thông tin trước khi đưa vào vận hành trong hệ thống thông tin của cơ quan.

e) Văn phòng HĐND và UBND tùy theo từng hợp đồng thuê khoán phần mềm, chỉ định bộ phận có trách nhiệm thực hiện thử nghiệm, kiểm tra và nghiệm

thu hệ thống trước khi đưa vào sử dụng.

2. Quản lý dịch vụ thuê khoán.

Trường hợp thuê khoán các dịch vụ công nghệ thông tin từ đơn vị bên ngoài (như vận hành, quản trị hệ thống, bảo trì thiết bị mạng, hỗ trợ kỹ thuật hoặc các dịch vụ CNTT khác), việc triển khai phải bảo đảm các yêu cầu sau:

a) Có hợp đồng hoặc thỏa thuận dịch vụ quy định rõ phạm vi công việc, trách nhiệm của đơn vị cung cấp dịch vụ và các yêu cầu bảo đảm an toàn thông tin.

b) Đơn vị cung cấp dịch vụ chỉ được truy cập vào hệ thống thông tin trong phạm vi công việc được giao và phải tuân thủ các quy định về bảo mật thông tin của đơn vị.

c) Việc truy cập, vận hành hoặc bảo trì hệ thống phải được giám sát, kiểm soát bởi bộ phận phụ trách an toàn thông tin của đơn vị.

d) Đơn vị cung cấp dịch vụ có trách nhiệm bảo mật thông tin, dữ liệu của cơ quan; không được sao chép, sử dụng hoặc cung cấp thông tin cho bên thứ ba khi chưa được phép của lãnh đạo đơn vị.

e) Sau khi kết thúc hợp đồng dịch vụ, đơn vị cung cấp dịch vụ phải bàn giao đầy đủ tài khoản quản trị, thông tin cấu hình hệ thống, tài liệu kỹ thuật liên quan và phối hợp thực hiện thu hồi hoặc hủy bỏ các quyền truy cập đã được cấp, bảo đảm không còn quyền truy cập vào hệ thống thông tin của đơn vị.

Chương III

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

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 03 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

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

e) 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.

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

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

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

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

j) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

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

l) Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

m) Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet)

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

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy 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, firmware các thiết bị mạng (firewall, router, switch, access point...).

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

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

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

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 tại mạng nội bộ Uỷ ban nhân dân theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

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

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

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác

4. Quản lý an toàn thiết bị mạng chính

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

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

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

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

5. Các yêu cầu quản lý an toàn mạng khác.

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

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

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

d) Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học, thư rác cho những hệ thống xung yếu (máy chủ thư điện tử, máy chủ website, máy chủ tên miền, vv...) và tại các máy chủ, máy trạm khác trong hệ thống;

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

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

1. Hạ tầng mạng triển khai hệ thống phải được thiết kế theo các phân vùng chức năng, tách biệt và có biện pháp kỹ thuật để hạn chế và giám sát được truy cập giữa các phân vùng mạng, tuân theo thiết kế đã được phê duyệt, bao gồm tối thiểu 03 phân vùng mạng:

a) Vùng mạng nội bộ (LAN - local area network): được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống.

b) Vùng mạng biên (outside zone): được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

c) Vùng DMZ (demilitarized zone): được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet

2. 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.

3. 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 như bên ngoài vào hệ thống.

4. 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.

d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

e) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

f) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

g) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

5. 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.

6. 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 chuyên trách an toàn 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.

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

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

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

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

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

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

Điều 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 an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 13. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.docx), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) ….

3. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

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

7. Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu

hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 14. Quản lý giám sát an toàn hệ thống thông tin

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

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

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

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

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

Điều 15. Quản lý điểm yếu an toàn thông tin

1. Văn phòng HĐND và UBND phường có nhiệm vụ:

a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Báo cáo Lãnh đạo Uỷ ban nhân dân ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

2. Định kỳ hằng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

3. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 11 Thông tư số 12/2022/TT-BTTTT.

Điều 16. 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 phường 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 phường 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 phường 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 cho đơn vị hoặc làm ảnh hưởng lớn tới trật tự phường hội, lợi ích công cộng, đe dọa nghiêm trọng tới an ninh, quốc phòng của đất nước.

2. Tổ chức, cá nhân được giao 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 theo kế hoạch ứng phó sự cố an toàn thông tin mạng đã được cấp thẩm quyền phê duyệt; trường hợp xác định sự cố có khả năng là sự cố nghiêm trọng, cần báo cáo ngay với chủ quản hệ thống thông tin, đơn vị chuyên trách về ứng cứu sự cố liên quan để đề xuất nâng cấp sự cố nghiêm trọng, đồng thời gửi Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an thành phố.

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. Bộ phận chuyên trách về an toàn thông tin có trách nhiệm.

a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định số 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng;

b) Xây dựng kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

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

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

e) Xây dựng 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. 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. Trách nhiệm của người dùng

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

Điều 17. 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) Đảm bảo thiết bị camera được mã hóa bảo mật đường truyền; đ) Hỗ trợ cơ chế cập nhật phần mềm;

e) 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;

f) 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;

g) Hỗ trợ đáp ứng các tiêu chuẩn an toàn tầng giao vận TLS (v1.2) và an toàn truyền tệp tin HTTPS;

h) 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;

i) Hệ thống máy chủ lưu trữ dữ liệu camera phải được đặt tại Việt Nam nhằm đảm bảo tính bảo mật, an ninh an toàn thông tin theo quy định hiện hành của Việt Nam, không sử dụng thiết bị camera có chuyển dữ liệu tới máy chủ được đặt ở nước ngoài.

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 18. Quản lý an toàn người sử dụng đầu cuối

1. Quản lý 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 cứng hóa bảo mật trước khi kết nối vào hệ thống.

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

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

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

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

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

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

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

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

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

Điều 19. Quản lý rủi ro an toàn thông tin

1. Xác định tài sản.

a) Lập danh mục thiết bị, máy chủ, phần mềm, dịch vụ, ứng dụng thuộc hệ thống;

b) Kịp thời cập nhật danh mục, nội dung hồ sơ đề xuất cấp độ an toàn thông tin của hệ thống khi có thay đổi.

2. Đánh giá rủi ro.

a) Xác định rủi ro: Định kỳ hàng tháng, Văn phòng HĐND & UBND chủ trì, phối hợp với Công an phường và các phòng ban liên quan tiến hành rà soát, xác định các mối đe dọa, điểm yếu, lỗ hổng bảo mật có thể ảnh hưởng, gây mất an toàn thông tin (ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn sàng) đối với các thành phần của hệ thống theo danh mục tài sản đã được xác định hoặc các yêu cầu về chính sách về quản lý, kỹ thuật được khuyến nghị thực hiện để bảo đảm an toàn thông tin

nhưng chưa thể thực hiện được;

b) Phân tích tác động của rủi ro: Làm rõ mức độ tác động, ảnh hưởng của từng rủi ro được xác định và đề xuất phương án xử lý;

c) Phân loại rủi ro theo mức độ ảnh hưởng:

- Mức thấp: Rủi ro mất an toàn thông tin có thể xử lý thông qua cập nhật miễn phí bản vá của hệ điều hành, phần mềm, ứng dụng, dịch vụ;
- Mức cao: Rủi ro mất an toàn thông tin không thể xử lý thông qua cập nhật hoặc phải trả phí để được cập nhật bản vá của hệ điều hành, phần mềm, ứng dụng, dịch vụ

3. Xử lý rủi ro.

a) Văn phòng HĐND & UBND chủ trì, phối hợp với Công an phường chủ động, kịp thời xử lý các rủi ro ở mức thấp;

b) Báo cáo Lãnh đạo đơn vị quyết định phương án xử lý đối với các rủi ro ở mức cao.

4. Chấp nhận rủi ro.

Việc xử lý sớm toàn bộ các rủi ro là khó khả thi. Đối với các rủi ro ở mức thấp hoặc rủi ro ở mức cao được phát hiện nhưng được đánh giá không làm tổn hại đến hoạt động bình thường của hệ thống hoặc đã có các biện pháp hạn chế rủi ro thì có thể chấp nhận sự tồn tại của rủi ro trên hệ thống. Tuy nhiên, cần từng bước có biện pháp xử lý triệt để các rủi ro.

5. Trường hợp sự cố mất an toàn thông tin xảy ra.

a) Văn phòng HĐND & UBND chủ trì, phối hợp Công an phường chủ động thực hiện các biện pháp nghiệp vụ cần thiết để tự xử lý.

b) Trong trường hợp sự cố mất an toàn thông tin vượt quá khả năng tự xử lý, Văn phòng HĐND & UBND kịp thời báo cáo Lãnh đạo đơn vị, phối với Công an phường, đồng thời nhanh chóng báo cáo và phối hợp với Công an thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để kịp thời xử lý.

Điều 20. 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.

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.

c) 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.

2. Trường hợp hệ thống phải kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

Văn phòng HĐND & UBND chủ trì, phối hợp với Công an phường tham mưu Lãnh đạo đơn vị báo cáo Lãnh đạo UBND thành phố Hải Phòng phương án thực hiện, trong đó làm rõ:

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

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

c) Phương án gỡ bỏ các phần mềm, ứng dụng hoặc dịch vụ có liên quan: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối có cài đặt phần mềm, ứng dụng hoặc dịch vụ có liên quan đến hệ thống cần thực hiện gỡ bỏ. Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung đề xuất xử lý, phương thức xử lý bảo đảm phần mềm, ứng dụng, dịch vụ được xóa hoàn toàn, không thể phục hồi trên các máy chủ, thiết bị mạng, thiết bị đầu cuối có liên quan;

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

3. Trình tự, thủ tục thực hiện

Sau khi được sự đồng ý bằng văn bản của UBND Thành phố Hải Phòng, Văn phòng HĐND & UBND chủ trì, phối hợp với Công an phường tham mưu Lãnh đạo UBND phường thực hiện thanh lý, hủy bỏ hệ thống theo đúng các quy định tại Điều 29, Điều 30 Nghị định số 186/2025/NĐ-CP của Chính phủ quy định chi tiết một số điều của Luật quản lý, sử dụng tài sản công.

Chương IV

KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 21. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

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

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

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

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

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của Thành uỷ, Ủy ban nhân dân thành phố, Công an thành phố.

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 chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

Điều 22. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin; Kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

c) Kiểm tra các nội dung khác tại quy chế.

2. Thẩm quyền kiểm tra

a) Văn phòng HĐND và UBND phường chịu trách nhiệm kiểm tra.

b) Các đơn vị khác tự kiểm tra trong nội bộ đơn vị.

3. Hoạt động kiểm tra về an toàn thông tin do Văn phòng HĐND và UBND phường thực hiện tại các đơn vị thuộc công tác ứng dụng công nghệ thông tin hằng năm, theo kế hoạch được phê duyệt. Hoạt động kiểm tra về an toàn thông tin do các cơ quan, đơn vị thực hiện có thể lồng ghép trong chương trình kiểm tra công tác ứng dụng công nghệ thông tin hàng năm, theo kế hoạch được Lãnh đạo đơn vị phê duyệt.

Chương V

BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 23. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hằng năm gồm các nội dung quy định tại Điều 14 Thông tư số 12/2022/TT-BTTTT, cụ thể như sau:

- Tình hình an toàn thông tin của hệ thống thông tin trong kỳ báo cáo;
- Tiến độ triển khai, áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;
- Hiệu quả áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;
- Đề xuất thay đổi cấp độ, phương án bảo đảm an toàn hệ thống thông tin (nếu có);
- Nội dung khác phục vụ công tác bảo đảm an toàn hệ thống thông tin theo cấp độ

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư số 31/2017/TT-BTTTT.

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

3. Trách nhiệm lập, phê duyệt báo cáo

a) Văn phòng HĐND và UBND phường chịu trách nhiệm:

- Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi cơ quan quản lý nhà nước về an toàn thông tin, an ninh mạng trước ngày 15 tháng 11 hằng năm.

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi Ủy ban nhân dân thành phố trước ngày 15 tháng 6 và 15 tháng 12 hằng năm.

- Báo cáo đột xuất theo hướng dẫn của Công an thành phố.

Chương VI

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 24. Trách nhiệm của Văn phòng HĐND và UBND phường

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Tham mưu Lãnh đạo UBND phường về công tác bảo đảm an toàn thông tin mạng tại UBND phường và chịu trách nhiệm trước Lãnh đạo UBND phường trong việc bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của UBND phường.

3. Thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, 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 và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

4. 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.

5. Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của UBND phường theo quy định. Tổng hợp các Đề án, Dự án về bảo đảm an toàn thông tin mạng của các phòng, đơn vị; Chủ trì, phối hợp các đơn vị liên quan tham mưu Lãnh đạo UBND phường xây dựng dự trù kinh phí thực hiện các Đề án, Dự án về bảo đảm an toàn thông tin mạng

6. Chủ trì, phối hợp với các cơ quan, đơn vị liên quan thanh tra, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trong phạm vi của UBND phường.

7. Cử cán bộ tham gia các khóa đào tạo, hội nghị tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước do Công an thành phố tổ chức.

8. Tham mưu Lãnh đạo UBND phường thực hiện phổ biến, tuyên truyền, quán triệt các văn bản, quy định về ATTT nhằm nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức, người lao động bằng các hình thức: gửi tài liệu tuyên truyền qua Hệ thống quản lý văn bản và điều hành, đăng tải thông tin, tài liệu trên Cổng TTĐT của phường , ban hành văn bản, quán triệt tại các cuộc họp giao ban của Lãnh đạo phường, cuộc họp của các phòng ban, đơn vị ...

9. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

10. Hàng năm cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an toàn thông tin mạng của các đơn vị đề xuất Lãnh đạo UBND phường xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành.

11. Phối hợp với Công an phường, Công an thành phố (qua phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các Cổng/trang thông tin điện tử, mạng xã hội

Điều 25. Trách nhiệm của Công an phường

1. Tham mưu UBND phường vận hành hệ thống thông tin theo quy định tại

Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công cán bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) phối hợp với Văn phòng HĐND & UBND phường triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

3. Thực hiện biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các Cổng/trang thông tin điện tử, mạng xã hội của phường

4. Cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng do Công an thành phố tổ chức.

Điều 26. Trách nhiệm của đơn vị cung cấp dịch vụ

1. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; thiết kế, thiết lập hệ thống đáp ứng các yêu cầu kỹ thuật cấp độ 2 theo tiêu chuẩn TCVN 11930:2017.

2. Quản lý, vận hành, bảo đảm an toàn thông tin cho các thành phần hệ thống thuộc phạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

Điều 27. Trách nhiệm của các cơ quan, đơn vị; cán bộ, công chức, viên chức, người lao động thuộc quản lý của các cơ quan đơn vị

1. Trách nhiệm của các cơ quan, đơn vị.

a) Phân công cán bộ thực hiện việc bảo đảm an toàn thông tin của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị.

b) Thực hiện bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

c) 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 xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

d) Phối hợp chặt chẽ với Văn phòng HĐND & UBND, Công an phường và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

e) Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch mua phần mềm chống virus có bản quyền phần mềm... nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi để triển khai thực hiện.

f) Phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin. Thực hiện các báo cáo về an toàn thông tin mạng khi UBND phường có yêu cầu

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan đơn vị

a) Trách nhiệm của cán bộ phụ trách về an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị

- Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị;

- Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

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

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

- Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

b) Trách nhiệm của người sử dụng

- 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;

- Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

- 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;

- Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được đơn vị chuyên môn tổ chức

Điều 28. Bảo đảm an toàn thông tin mạng và an ninh mạng

Thực hiện theo Điều 6, Điều 7, Điều 8, Điều 9, Điều 10, Điều 11, Điều 14 của Quyết định số 439/QĐ-BKHCN ngày 04/04/2025 của Bộ trưởng Bộ Khoa học và công nghệ về việc ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng.

Chương VII

TỔ CHỨC THỰC HIỆN

Điều 29. Tổ chức triển khai Quy chế

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

2. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị tại phường và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Văn phòng HĐND và UBND phường để xem xét, bổ sung, sửa đổi.

Điều 30. 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 đúng với quy định của pháp luật. Quy chế sau khi điều chỉnh sẽ được trình lên Lãnh đạo Uỷ ban nhân dân 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 Văn phòng HĐND và UBND để tổng hợp, điều chỉnh, bổ sung./.