ỦY BAN NHÂN DÂN **PHƯỜNG NGÔ QUYỀN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 515/QĐ-UBND	*Phường Ngô Quyền, ngày 08 tháng 8 năm 2025*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng hệ thống thông tin nội bộ Ủy ban nhân dân Phường Ngô Quyền

CHỦ TỊCH ỦY BAN NHÂN DÂN PHƯỜNG

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

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

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

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

Căn cứ các Nghị định của Chính phủ: Số 64/2007/NĐ-CP ngày 10/4/2007 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; số 72/2013/NĐ-CP ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng; số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ 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;

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 Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát;

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 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Trưởng phòng Phòng Văn hóa - Xã hội.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng hệ thống thông tin nội bộ của Ủy ban nhân dân Phường Ngô Quyền.

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

Điều 3. Chánh Văn phòng HĐND và UBND phường, Trưởng các phòng, ban, đơn vị thuộc Ủy ban nhân dân Phường Ngô Quyền và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

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

CHỦ TỊCH

U.B.N.D PHƯỜNG NGÔ QUYỀN T.P HẢI PHÒNG

Nguyễn Quốc Thái

QUY CHẾ
Bảo đảm an toàn, an ninh mạng hệ thống thông tin nội bộ Ủy ban nhân dân Phường Ngô Quyền

(Ban hành kèm theo Quyết định số 515/QĐ-UBND ngày 08/8/2025 của Ủy ban nhân dân Phường Ngô Quyền)

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 về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của Ủy ban nhân dân Phường Ngô Quyền.

2. Đối tượng áp dụng:

- Các phòng, ban, đơn vị (sau đây gọi tắt là đơn vị) và cán bộ, công chức, viên chức, người lao động thuộc Ủy ban nhân dân Phường Ngô Quyền.

- Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho Ủy ban nhân dân phường và các đơn vị thuộc Ủy ban nhân dân phường.

- Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động cho các hệ thống thông tin của Ủy ban nhân dân phường.

Điều 2. Mục đích bảo đảm an ninh, an toàn trên môi trường mạng

1. Thực hiện bảo vệ bí mật nhà nước, phòng, chống các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tham gia hoạt động trên môi trường mạng.

2. Công tác đảm bảo an ninh thông tin, bảo mật trên môi trường mạng là một trong những nhiệm vụ trọng tâm để đảm bảo thành công trong việc ứng dụng công nghệ thông tin tại các đơn vị.

Điều 3. 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 số và các 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. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không

gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. *Bảo vệ an ninh mạng* là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

4. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

5. *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.

6. *Môi trường mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

7. *Hệ thống thông tin* là tập hợp thiết bị 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 như: Hệ thống mạng nội bộ, hệ thống văn phòng điện tử, hệ thống thư điện tử, trang thông tin điện tử, hệ thống camera giám sát…

8. *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.

9. *Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

10. *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.

11. *Đơn vị vận hành hệ thống thông tin* là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

12. *Tài khoản số* là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.

13. *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.

14. *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.

15. *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.

16. *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.

17. *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.

18. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng...

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Các đơn vị thuộc Ủy ban nhân dân phường có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; bố trí nhân sự chuyên trách/bán chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của Trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

3. Cán bộ, Công chức, viên chức và người lao động trong các đơn vị trực thuộc Ủy ban nhân dân phường có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và các quy định liên quan.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước, quy định của Ủy ban nhân dân phường về công tác bảo vệ bí mật Nhà nước và các nội dung tương ứng trong Quy chế này.

5. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 5. Các hành vi bị nghiêm cấm

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

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào hệ thống mạng LAN, hệ thống máy chủ, hệ thống camera giám sát...

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.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy cập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

8. Để lộ hoặc cung cấp cấu hình cài đặt, đường dẫn, tài khoản của các hệ thống; Xóa, thay đổi, sao chép hoặc tiết lộ trái phép các dữ liệu hình ảnh được lưu trữ trên hệ thống camera giám sát.

9. Lạm dụng nhiệm vụ, quyền hạn được giao lấy cắp, sử dụng dữ liệu nhằm trục lợi, sách nhiễu, xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân.

Điều 6. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

a) Ủy ban nhân dân Phường Ngô Quyền giao Phòng Văn hóa - Xã hội là đầu mối liên hệ, phối hợp với 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 các đơn vị trực thuộc Ủy ban nhân dân phường vận hành; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của các hệ thống thông tin thuộc cơ quan Ủy ban nhân dân phường; phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin. 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.

b) Các đơn vị cử đầu mối tiếp nhận và xử lý các sự cố về an toàn thông tin của các hệ thống thông tin do các đơn vị trực tiếp vận hành, khai thác.

2. Các đơn vị, cá nhân trực thuộc Ủy ban nhân dân phường tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 7. Bảo vệ bí mật nhà nước trong ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) Không được sử dụng máy tính nối mạng (Internet và nội bộ) để soạn

thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung bí mật nhà nước; không được cung cấp tin, bài, tài liệu và đưa thông tin bí mật nhà nước lên trang thông tin điện tử. Nghiêm cấm cài cắm các thiết bị lưu trữ tài liệu có nội dung bí mật nhà nước vào máy tính nối mạng internet.

b) Không được in, sao chụp tài liệu, vật mang bí mật nhà nước trên các thiết bị kết nối mạng internet.

2. Khi máy tính dùng để soạn thảo văn bản mật có sự cố, các phòng, ban, đơn vị phải báo cho Phòng Văn hóa - Xã hội để xử lý theo quy định. Không được tự ý sửa chữa hoặc cho phép cá nhân tổ chức không có trách nhiệm trực tiếp sửa chữa, xử lý và khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật.

Đối với các máy tính để soạn thảo văn bản mật tại các đơn vị: đơn vị phải xây dựng nội quy, quy định quản lý sử dụng đảm bảo theo quy định của Luật Bảo vệ bí mật nhà nước hiện hành.

3. Trước khi thanh lý các máy tính trong đơn vị, cán bộ chuyên trách/bán chuyên trách công nghệ thông tin phải tiêu huỷ dữ liệu trong ổ cứng máy tính. Không được thanh lý ổ cứng máy tính dùng soạn thảo và chứa các nội dung mật.

Điều 8. Bảo đảm nguồn nhân lực

1. Vị trí việc làm:

Khi xây dựng đề án vị trí việc làm, đơn vị phải bố trí 01 vị trí việc làm công nghệ thông tin.

2. Tuyển dụng:

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, theo đề án vị trí việc làm được duyệt.

3. Trong quá trình làm việc:

a) Có 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.

b) Có kế hoạch và định kỳ hằng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.

c) Có kế hoạch và định kỳ hằng năm tổ chức đào tạo về an toàn thông tin hằng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

d) Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin

cho tổ chức, cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

4. Chấm dứt thay đổi công việc:

Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, đơn vị phải:

a) Xác định rõ trách nhiệm của cá nhân và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

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

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

d) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Chương II

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

Điều 9. Thiết kế an toàn hệ thống thông tin

Đối với các hệ thống thông tin khi xây dựng mới hoặc nâng cấp nhằm đảm bảo an toàn thông tin theo cấp độ an toàn thông tin cần đảm bảo các yêu cầu sau:

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

6. Có phương án quản lý và bảo vệ hồ sơ thiết kế.

7. Có bộ phận chuyên môn hoặc thuê đơn vị có đủ năng lực để đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện.

Điều 10. Quản lý thuê dịch vụ công nghệ thông tin, phát triển phần mềm thuê khoán

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, các đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều

khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và rõ trách nhiệm của bên cung cấp dịch vụ.

2. Kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.

3. Khi thay đổi mã nguồn, kiến trúc phần mềm, thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm.

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

5. Trách nhiệm của các đơn vị trong quá trình sử dụng dịch vụ công nghệ thông tin:

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy cập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan.

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của đơn vị.

6. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin:

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm.

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại…

7. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ:

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 11. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng; Giao bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống; thực hiện các nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống đảm bảo theo quy định của pháp luật (Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước).

2. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

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

Điều 12. Quản lý an toàn mạng

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

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 tập tin nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

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

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

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

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

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

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

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

k) Duy trì ít nhất 02 kết nối mạng internet từ các nhà cung cấp dịch vụ internet (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.

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 theo thời gian quy định của từng hệ thống.

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 hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, 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 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 trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 13. 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) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), máy chủ, hệ thống lưu trữ... phải được đặt trong phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp.

b) Hệ điều hành được cài đặt là phần mềm có bản quyền, các dịch vụ cài

đặt trên máy chủ là các dịch vụ được sử dụng dùng chung cho các đơn vị, không cài đặt các dịch vụ không sử dụng; Thiết lập chế độ tự động cập nhật phiên bản và hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật khẩu truy cập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ.

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

d) Định kỳ hằng tuần các đơn vị có hệ thống máy chủ phải kiểm tra các tiến trình trên máy chủ tại đơn vị nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy chủ.

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 như 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) 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.

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

đ) 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.

e) 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.

4. 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.

b) 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.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.

7. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

Điều 14. Quản lý an toàn dữ liệu

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

Mục đích của việc mã hóa dữ liệu là bảo vệ dữ liệu số khi nó được lưu trữ trên các hệ thống máy tính và truyền qua internet hay các mạng máy tính khác. Các thuật toán mã hóa thường cung cấp những yếu tố bảo mật then chốt như xác thực, tính toàn vẹn và không thu hồi. Xác thực cho phép xác minh nguồn gốc của dữ liệu, tính toàn vẹn chứng minh rằng nội dung của dữ liệu không bị thay đổi kể từ khi nó được gửi đi. Không thu hồi đảm bảo rằng người gửi không thể hủy việc gửi dữ liệu.

Quá trình mã hóa sẽ biến nội dung sang một dạng mới, vì thế sẽ tăng thêm một lớp bảo mật cho dữ liệu. Như vậy cho dù dữ liệu của bạn bị đánh cắp thì việc giải mã dữ liệu cũng vô cùng khó khăn, tốn nhiều nguồn lực tính toán và cần rất nhiều thời gian.

a) Các đơn vị phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp 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; Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

4. 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).

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

6. 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).

7. Bảo đảm an toàn thông tin mức dữ liệu:

a) Các đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu...

b) Các đơn vị trực thuộc Ủy ban nhân dân phường phải bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

c) Các đơn vị trực thuộc Ủy ban nhân dân phường phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

d) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 15. Quản lý an toàn thiết bị đầu cuối

1. Cán bộ chuyên trách công nghệ thông tin có trách nhiệm quản lý các thiết bị công nghệ thông tin phục vụ công việc, hoạt động chung của Ủy ban nhân dân phường. Cán bộ chuyên trách/bán chuyên trách công nghệ thông tin của các đơn vị có trách nhiệm quản lý các thiết bị công nghệ thông tin phục vụ công việc, hoạt động chung của các đơn vị trực thuộc Ủy ban nhân dân phường.

2. Công chức, viên chức, người lao động có trách nhiệm sử dụng và bảo quản các thiết bị công nghệ thông tin được cấp để phục vụ công việc hằng ngày.

3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu, tài liệu khi thay đổi mục đích sử dụng hoặc thanh lý, phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi.

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

Điều 16. Bảo đảm an toàn thông tin khi sử dụng máy tính

1. Cán bộ, công chức, viên chức và người lao động chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm

quyền ban hành trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của lãnh đạo đơn vị; thường xuyên cập nhật phần mềm và hệ điều hành; Khóa màn hình máy tính khi rời khỏi bàn làm việc. Đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng. Tắt máy sau mỗi buổi làm việc.

2. Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính, phải tắt máy và báo trực tiếp cho cán bộ chuyên trách/bán chuyên trách về công nghệ thông tin để được xử lý kịp thời.

3. Cán bộ, công chức, viên chức và người lao động chỉ được sử dụng máy tính vào các hoạt động nghiệp vụ. Không sử dụng máy tính để truy cập, tải về, lưu trữ, phát tán những nội dung vi phạm pháp luật; Không tự tiện thay đổi cấu hình, phần cứng của máy tính được trang bị; Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của lãnh đạo đơn vị; Thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị lưu trữ di động như quét mã độc định kỳ, mã hóa dữ liệu.

4. Quản lý tài khoản truy cập:

a) Cán bộ, công chức, viên chức và người lao động sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó.

b) Trường hợp cán bộ, công chức, viên chức và người lao động thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc: Phòng Văn hóa và Xã hội thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin thuộc Ủy ban nhân dân phường; Các đơn vị chủ động thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin do đơn vị vận hành quản lý.

c) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo phòng, ban, đơn vị phải yêu cầu bằng văn bản gửi Phòng Văn hóa và Xã hội. Phòng Văn hóa và Xã hội phối hợp với đơn vị liên quan để khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

Đối với các tài khoản thuộc hệ thống thông tin do đơn vị quản lý vận hành, trưởng đơn vị quy định, giao quyền cho bộ phận chuyên môn thực hiện việc quản lý tài khoản, cấp và khoá tài khoản khi có yêu cầu.

Điều 17. Đảm bảo an toàn thông tin cho hệ thống camera giám sát

1. Các đơn vị phải đảm bảo an toàn, an ninh thông tin và tuân thủ theo các quy định pháp luật cho hệ thống camera giám sát.

2. Đơn vị quản lý, vận hành hệ thống camera có trách nhiệm phân công cán bộ 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.

3. Việc chia sẻ, sử dụng dữ liệu hệ thống camera giám sát phải đảm bảo tính kịp thời, chính xác, khách quan, minh bạch, đúng mục đích, đúng chức năng, nhiệm vụ, quyền hạn của cơ quan, đơn vị. Đồng thời phải đảm bảo các yếu tố bảo mật thông tin, dữ liệu.

4. Khi triển khai đầu tư, lắp đặt, nâng cấp các hệ thống camera phải thực hiện theo đúng các tiêu chuẩn, hướng dẫn kỹ thuật hiện hành; Sử dụng camera giám sát đáp ứng các yêu cầu về bảo đảm an toàn thông tin mạng theo quy định; không sử dụng camera giám sát không có chứng nhận xuất xứ, chất lượng sản phẩm hoặc đã được cơ quan có thẩm quyền cảnh báo không bảo đảm an toàn thông tin mạng.

5. Về xác định cấp độ cho các hệ thống thông tin có sử dụng camera giám sát phụ thuộc vào việc xác định loại hình hệ thống thông tin, các đơn vị thực hiện theo hướng dẫn của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông tại văn bản số 294/CATTT-ATHTTT ngày 13/3/2023.

6. Triển khai đầy đủ phương án bảo đảm an toàn theo quy định cho các hệ thống thông tin có sử dụng camera giám sát đang vận hành.

7. Bộ tiêu chí và Quy chuẩn kỹ thuật quốc gia về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát, các đơn vị áp dụng theo quy định của Bộ Thông tin và Truyền thông.

Chương IV
QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 18. Phân nhóm sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

a) Hệ thống thông tin bị sự cố là hệ thống thông tin của Ủy ban nhân dân phường, các đơn vị trực thuộc Ủy ban nhân dân phường và bị một trong số các

sự cố sau: Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin...

b) Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý sự cố.

2. Sự cố an toàn thông tin thường gặp:

a) Sự cố do bị tấn công mạng.

b) Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, không gian lưu trữ dữ liệu (hosting)…

c) Sự cố do lỗi của người quản trị, vận hành hệ thống...

Điều 19. 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 Ủy ban nhân dân phường khi gặp sự cố trong quá trình sử dụng máy tính có kết nối mạng thực hiện thông báo ngay cho bộ phận đầu mối/cán bộ chuyên trách/bán chuyên trách công nghệ thông tin tại đơn vị (Bộ phận ứng cứu sự cố).

Bước 2: Tiếp nhận sự cố

Bộ phận ứng cứu sự cố tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp…

Bước 3: Xác minh/xác nhận sự cố

Bộ phận ứng cứu sự cố triển khai tiến hành xác minh/xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xảy 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

Bộ phận ứng cứu sự cố có trách nhiệm phân loại sự cố:

- Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, không gian lưu trữ dữ liệu (hosting)…
- Sự cố do lỗi của người quản trị, vận hành hệ thống.
- Sự cố do bị tấn công mạng nhưng trên phạm vi 01 máy tính, có thể khắc phục.
- Sự cố về tấn công thay đổi giao diện (deface).
- Sự cố về tấn công lừa đảo (phishing).

- Sự cố về tấn công phát tán mã độc (malware).

- Sự cố về tấn công từ chối dịch vụ (DoS/DDoS).

- Sự cố có yếu tố nước ngoài (hợp tác quốc tế).

- Sự cố tấn công khác.

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

Ngay sau khi phân loại được sự cố, Bộ phận ứng cứu sự cố 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 thì Bộ phận ứng cứu sự cố báo cho các bên liên quan để tiếp tục triển khai theo phương án ứng cứu sự cố an toàn thông tin mạng thông thường theo quy trình ứng cứu sự cố thông thường của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017; báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng thành phố (qua Công an thành phố) để phối hợp xử lý.

- 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 (qua Công an thành phố) về sự cố nghiêm trọng để có phương án ứng cứu; và tổ chức ứng cứu, xử lý sự cố: các đơn vị tham gia lực lượng ứng cứu; nguồn lực cần thiết để ứng cứu sự cố; dự kiến triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp và thực hiện tiếp các bước tiếp theo được quy định tại Điều 14 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.

Bước 6: Phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng thành phố: 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 20. Kế hoạch ứng phó sự cố an toàn thông tin mạng

1. Điều kiện, nguyên tắc, phương châm ứng phó sự cố:

a) Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng.

b) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

c) Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan, đơn vị, ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

d) Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của hệ thống thông tin đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.

đ) Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

e) Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố.

2. Các đơn vị vận hành, quản lý hệ thống thông tin cần thực hiện thường xuyên việc đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm cả đơn vị đã ký hợp đồng cung cấp dịch vụ nếu có).

3. Triển khai các nội dung phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin theo quy định về phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin Phường Ngô Quyền.

4. Các đơn vị quản lý, vận hành hệ thống thông tin tổ chức triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố theo quy định.

5. Đầu tư trang thiết bị bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố: Căn cứ điều kiện, tình hình thực tế tại đơn vị từ đó chủ động trang bị thiết bị, công cụ, phương tiện cần thiết để phục vụ ứng phó sự cố an toàn thông tin mạng; chuẩn bị các điều kiện bảo đảm, sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

Điều 21. Quản lý giám sát an toàn hệ thống thông tin

1. Cán bộ, công chức, viên chức và người lao động khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho cán bộ chuyên trách/bán chuyên trách của các đơn vị để kịp thời xử lý.

2. Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về an toàn thông tin đưa ra cảnh bảo sớm về nguy cơ mất an toàn thông tin trong hệ thống.

3. Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

Điều 22. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro

Khi thực hiện đánh giá và quản lý rủi ro an toàn thông tin các đơn vị 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. Cụ thể như sau:

a) Bước thiết lập bối cảnh: Đưa ra thông tin tổng quan, phạm vi và các thành phần của hệ thống cần bảo vệ (sơ đồ tổng thể và các thành phần trong hệ thống: thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối, thông tin, tài liệu…).

b) Bước đánh giá rủi ro: Thực hiện nhận biết rủi ro, phân tích rủi ro và ước lượng rủi ro (điểm yếu, mối đe dọa, hậu quả và mức ảnh hưởng đối với đơn vị khi rủi ro xảy ra).

c) Bước xử lý rủi ro: xác định các phương án xử lý rủi ro, bao gồm các biện pháp quản lý và kỹ thuật để có thể xử lý, giảm thiểu các mối đe dọa có thể xảy ra đối với hệ thống thông tin.

d) Bước xác định mức chấp nhận rủi ro: xác định mức chấp nhận rủi ro và các rủi ro còn lại sau khi xử lý.

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 đặc thù riêng và yêu cầu mức độ an toàn khác nhau phù hợp với yêu cầu thực tế của mỗi đơn vị. Do đó, trên cơ sở đánh giá và quản lý rủi ro, đơn vị 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 số 85/2016/NĐ-CP ngày 10/7/2016, Điều 9, 10 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017.

Điều 23. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản hệ thống thông tin thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng 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. Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; 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; Thực hiện theo quy định tại Điều 15 của Quy chế này.

Chương V
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 24. Trách nhiệm của các phòng, ban, đơn vị trực thuộc Ủy ban nhân dân phường

1. Phổ biến và triển khai các hệ thống thông tin tại đơn vị tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của pháp luật về an toàn thông tin mạng.

2. Đối với các đơn vị có hệ thống thông tin: mạng LAN, hệ thống cơ sở dữ liệu, máy chủ, hệ thống camera giám sát..., triển khai áp dụng Quy chế này tại đơn vị và ban hành văn bản hướng dẫn để tổ chức thực hiện, trong đó bao gồm việc giao nhiệm vụ cụ thể cho bộ phận, cá nhân thực hiện công tác bảo đảm an toàn, an ninh thông tin mạng. Tuỳ theo mô hình quản lý, tính chất của hệ thông thông tin, các đơn vị xây dựng, ban hành quy chế đảm bảo an toàn thông tin mạng tại đơn vị (nếu cần).

3. Xây dựng sơ đồ tổng thể, đánh giá hiện trạng và bổ sung các thành phần trong hệ thống: thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối, thông tin, tài liệu… đảm bảo an toàn cho các hệ thống thông tin và xây dựng hồ sơ đề xuất cấp độ cho hệ thống thông tin tại đơn vị gửi Ủy ban nhân dân Phường Ngô Quyền (qua Phòng Văn hóa - Xã hội) để tổng hợp.

4. Thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị, coi đây là nhiệm vụ trọng tâm của đơn vị; chịu trách nhiệm trước pháp luật và lãnh đạo Ủy ban nhân dân phường về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

5. Chủ trì, phối hợp với Phòng Văn hóa - Xã hội trong việc bảo đảm an toàn thông tin trong quá trình triển khai hệ thống thông tin.

6. Cán bộ, công chức, viên chức, người lao động có trách nhiệm: tuân thủ Quy chế; thông báo kịp thời các vấn đề bất thường liên quan tới an toàn thông tin cho bộ phận chuyên trách/bán chuyên trách về an toàn thông tin mạng của Ủy ban nhân dân phường/đơn vị.

7. Tuỳ theo tình hình thực tế, các đơn vị có thể áp dụng Quy chế cho các hệ thống thông tin đã triển khai theo các dự án đầu tư công nghệ thông tin hoặc hệ thống thông tin đã có quy định riêng theo Quyết định của Ủy ban nhân dân thành phố.

Điều 25. Trách nhiệm của Phòng Văn hóa - Xã hội

1. Hướng dẫn triển khai Quy chế này và các quy định pháp luật có liên quan.

2. Tổ chức triển khai Quy chế cho các hệ thống thông tin Ủy ban nhân dân phường.

3. Xây dựng hồ sơ đề xuất cấp độ cho hệ thống thông tin Ủy ban nhân dân phường theo quy định và tổng hợp hồ sơ đề xuất của các đơn vị gửi Công an thành phố để phê duyệt cấp độ.

Điều 26. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí đánh giá kết quả thực hiện hằng năm của cá nhân, đơn vị đồng thời là tiêu chí bắt buộc để xem xét tình hình khen thưởng và danh hiệu thi đua đối với các tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Điều 27. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hằng năm hoặc khi có thay đổi chính sách an toàn thông tin, các đơn vị rà soát, kiểm tra lại tính phù hợp, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Phòng Văn hóa - Xã hội để tổng hợp, trình lãnh đạo Ủy ban nhân dân phường xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.