ỦY BAN NHÂN DÂN THÀNH PHỐ HÀ NỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2223 /QĐ-UBND	*Hà Nội, ngày 14 tháng 4 năm 2023*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước thành phố Hà Nội

CHỦ TỊCH ỦY BAN NHÂN DÂN THÀNH PHỐ HÀ NỘI

Căn cứ Luật Tổ chức chính quyền địa phương năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương năm 2019;

Căn cứ Luật An toàn thông tin mạng năm 2015;

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

Căn cứ Thông tư số 12/2019/TT-BTTTT ngày 05/11/2019 của Bộ Thông tin và Truyền thông quy định về việc sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, 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 ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

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 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố ATTTM Việt Nam;

Căn cứ Chỉ thị số 23/CT-TTg ngày 26 tháng 12 năm 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;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 807/TTr-STTTT ngày 31/3/2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước thành phố Hà Nội.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế Quyết định số 411/QĐ-UBND ngày 27/01/2015 của UBND thành phố Hà Nội về việc ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước thành phố Hà Nội.

Điều 3. Chánh Văn phòng UBND Thành phố; Thủ trưởng các sở, ban, ngành, đơn vị thuộc Thành phố; Chủ tịch UBND các quận, huyện, thị xã; Chủ tịch UBND các xã, phường, thị trấn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thường trực Thành ủy;
- Bộ Thông tin và Truyền thông;
- Chủ tịch UBND Thành phố;
- Thường trực HĐND Thành phố;
- Các Phó Chủ tịch UBND Thành phố;
- VPUB: CVP, các PCVP, phòng, đơn vị trực thuộc;
- Trung tâm báo chí Thủ đô;
- Lưu: VT, KGVX Dg.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hà Minh Hải

QUY CHẾ

Bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước thành phố Hà Nội

(Ban hành kèm theo Quyết định số 2223 /QĐ-UBND ngày 14 tháng 4 năm 2023 của Ủy ban nhân dân thành phố Hà Nội)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định bảo đảm an toàn thông tin mạng trong hoạt động chuyển đổi số, ứng dụng công nghệ thông tin, vận hành, khai thác hệ thống, hạ tầng, phần mềm, dữ liệu thuộc phạm vi của các cơ quan nhà nước, đơn vị sự nghiệp thành phố Hà Nội.

Điều 2. Đối tượng áp dụng

1. Các cơ quan nhà nước thành phố Hà Nội, bao gồm: các Sở, ban, ngành, các đơn vị sự nghiệp trực thuộc UBND Thành phố; UBND các quận, huyện, thị xã; UBND các phường, xã, thị trấn và các đơn vị trực thuộc (sau đây gọi tắt là đơn vị).

2. Các tổ chức, cá nhân liên quan đến an toàn thông tin mạng trong các cơ quan nhà nước, đơn vị sự nghiệp thành phố Hà Nội.

3. Khuyến khích các tổ chức, cá nhân liên quan khác áp dụng các quy định tại Quy chế này để bảo đảm an toàn thông tin mạng.

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* (sau đây gọi tắt là ATTTM) 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. *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.

3. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Đối với cơ quan, tổ chức nhà nước, chủ quản hệ thống thông tin là các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương hoặc là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó.

4. *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.

5. *Sự cố ATTTM* là việc thông tin, hệ thống thông tin bị tấn công hoặc gây

nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng (sau đây gọi tắt là sự cố).

6. *Ứng cứu sự cố ATTTM* là hoạt động nhằm xử lý, khắc phục sự cố gây mất ATTTM gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

7. *Đầu mối ứng cứu sự cố* là bộ phận hoặc cá nhân được thành viên mạng lưới ứng cứu sự cố ATTTM quốc gia cử để thay mặt cho thành viên liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia về ứng cứu sự cố hoặc các thành viên khác trong hoạt động điều phối, ứng cứu sự cố.

8. *Cán bộ được giao phụ trách bảo đảm an toàn thông tin* là cán bộ kỹ thuật hoặc cán bộ quản lý được giao phụ trách công tác bảo đảm ATTTM cho việc triển khai, vận hành, khai thác hệ thống công nghệ thông tin (sau đây gọi tắt là CNTT) tại đơn vị.

9. *Bên thứ ba* là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống CNTT.

10. Các trang thiết bị, thông tin thuộc hệ thống CNTT của đơn vị bao gồm:

a) Trang thiết bị vật lý: là các thiết bị CNTT, phương tiện truyền thông và các thiết bị phục vụ hoạt động cho hệ thống thông tin (bao gồm cả các trang thiết bị hỗ trợ như máy tính, camera giám sát và các trang thiết bị khác theo quy định);

b) Thông tin: là các dữ liệu, tài liệu liên quan đến hệ thống CNTT.

c) Phần mềm: là các phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, hệ quản trị cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển.

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

1. Bảo đảm ATTTM được thực hiện xuyên suốt trong các hoạt động mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

2. Trách nhiệm bảo đảm ATTTM gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

3. Trường hợp có quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

4. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 5. Quản lý trang thiết bị CNTT

1. Đơn vị phải thống kê, kiểm kê trang thiết bị CNTT (trang thiết bị vật lý, thông tin, phần mềm) tối thiểu mỗi năm 01 lần. Gắn quyền sử dụng trang thiết bị CNTT cho các cá nhân hoặc bộ phận cụ thể. Người sử dụng trang thiết bị CNTT phải tuân thủ các quy định về quản lý, sử dụng, bảo đảm trang thiết bị CNTT được sử dụng đúng mục đích và an toàn.

2. Đơn vị có trách nhiệm kiểm tra, đánh giá mức độ an toàn đối với các trang thiết bị CNTT trước khi đưa vào sử dụng. Trước khi đưa vào sử dụng, đơn vị có trách nhiệm đề nghị Công an Thành phố phối hợp kiểm tra, đánh giá an toàn thông tin đối với các thiết bị CNTT sử dụng tại cơ quan trọng yếu, phục vụ các công việc yêu cầu bảo đảm bí mật,... (đặc biệt là các sở, ngành thuộc 11 lĩnh vực quan trọng cần ưu tiên bảo đảm ATTTM theo Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm ATTTM và hệ thống thông tin quan trọng quốc gia).

3. Việc quản lý, sử dụng các trang thiết bị CNTT khi thực hiện các hoạt động có liên quan đến nước ngoài (đi công tác nước ngoài, giao dịch, làm việc với các tổ chức nước ngoài,...) thực hiện theo quy định pháp luật và Thành phố. Các thiết bị CNTT sử dụng khi đi công tác nước ngoài phải được kiểm tra, đánh giá an toàn thông tin trước và sau mỗi chuyến công tác.

4. Việc quản lý, sử dụng trang thiết bị CNTT khi thực hiện các hoạt động bên ngoài trụ sở làm việc của đơn vị phải bảo đảm an toàn theo quy định của thành phố và nhà nước nhằm tránh xâm nhập trái phép, lộ lọt dữ liệu. Trường hợp làm mất hoặc lộ thông tin trên thiết bị hoặc phương tiện xử lý thông tin có chứa dữ liệu về hệ thống thông tin, phải báo cáo ngay cho lãnh đạo và đơn vị/bộ phận có thẩm quyền để có biện pháp xử lý, khắc phục kịp thời.

5. Thông tin liên quan đến trang thiết bị CNTT (loại trang thiết bị, số hiệu, vị trí, thông tin bản quyền, các mô tả khác cho việc thay thế, phục hồi, khắc phục sửa lỗi nhanh) cần được lưu trữ, quản lý và cập nhật kịp thời.

6. Phân loại trang thiết bị CNTT (vật lý, thông tin, phần mềm) theo mức độ giá trị, độ nhạy cảm, tầm ảnh hưởng đối với hệ thống, tần suất sử dụng, thời gian lưu trữ để xây dựng, điều chỉnh nội quy, biện pháp kỹ thuật nghiệp vụ phù hợp (định kỳ sao lưu dữ liệu, bảo trì hệ thống,...).

7. Định kỳ hằng năm, đơn vị phải xây dựng kế hoạch kiểm tra, bảo trì, bảo dưỡng trang thiết bị CNTT. Trang thiết bị lưu trữ thông tin khi không sử dụng nữa cần phải được hủy bỏ, việc hủy bỏ bảo đảm tránh mất mát dữ liệu và không thể phục hồi.

8. Khi bên thứ ba thực hiện việc cung cấp, bảo dưỡng, sửa chữa trang thiết bị CNTT cho đơn vị, phải thực hiện việc quản lý bảo đảm an toàn thông tin của đơn vị như sau:

a) Đánh giá về năng lực kỹ thuật, nhân sự, khả năng tài chính của bên thứ ba trước khi ký kết hợp đồng cung cấp hàng hóa, dịch vụ;

b) Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản về việc xử lý khi có vi phạm quy chế an toàn, bảo mật thông tin và trách nhiệm phải bồi thường thiệt hại của bên thứ ba trong trường hợp có thiệt hại do hành vi vi phạm của bên thứ ba gây ra;

c) Chú ý đến các vấn đề về tính bí mật, tính toàn vẹn, tính sẵn sàng, tin cậy, hiệu năng tối đa, khả năng phục hồi thảm họa, phương tiện lưu trữ của hệ thống thông tin khi có sự tham gia của bên thứ ba;

d) Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép truy cập vào hệ thống CNTT của đơn vị;

đ) Yêu cầu bên thứ ba chủ trì, phối hợp với đơn vị kiểm tra, đánh giá an toàn thông tin sau khi bảo dưỡng, sửa chữa trang thiết bị CNTT.

Điều 6. Quản lý nguồn nhân lực

1. Cán bộ, công chức, viên chức, người lao động phải tuân thủ thực hiện các quy chế bảo đảm an toàn thông tin của đơn vị mình.

2. Cán bộ, công chức, viên chức, người lao động và cơ quan, đơn vị quản lý trực tiếp chịu trách nhiệm trước UBND Thành phố, Chủ tịch UBND Thành phố khi để lộ, lọt thông tin, tài liệu mật, vi phạm các quy định về bảo vệ bí mật nhà nước.

3. Đơn vị bố trí nhân sự có năng lực, chất lượng và đạo đức đảm nhận vị trí lãnh đạo bộ phận chuyên trách an toàn thông tin và vị trí chuyên trách an toàn thông tin, quản trị hệ thống CNTT của đơn vị.

4. Hằng năm, đơn vị phải lập kế hoạch đào tạo cho cán bộ, công chức, viên chức và người lao động để nâng cao kiến thức cơ bản và kỹ năng ATTTM; đồng thời phổ biến, cập nhật các quy chế về an toàn thông tin để cán bộ hiểu rõ các quyền và trách nhiệm đối với công tác bảo đảm ATTTM.

5. Thường xuyên kiểm tra việc thực hiện quy chế về ATTTM của đơn vị đối với cán bộ, công chức, viên chức, người lao động theo định kỳ.

6. Khi chấm dứt hoặc thay đổi công việc, đơn vị phải: Xác định rõ trách nhiệm của cán bộ, công chức, viên chức và người lao động và các bên liên quan về hệ thống CNTT; thu hồi hoặc thay đổi quyền truy cập hệ thống CNTT phù hợp với công việc được thay đổi.

7. Đối với bên thứ ba, trong quá trình triển khai đơn vị cần:

a) Yêu cầu bên thứ ba cung cấp danh sách nhân sự tham gia và yêu cầu bên thứ ba ký cam kết không tiết lộ thông tin của đơn vị đối với các thông tin quan trọng;

b) Cung cấp và yêu cầu bên thứ ba tuân thủ đầy đủ các quy chế về ATTTM của đơn vị và giám sát quá trình thực hiện;

c) Trong trường hợp phát hiện dấu hiệu vi phạm của bên thứ ba, đơn vị cần: Tạm dừng hoặc đình chỉ hoạt động của bên thứ ba tùy theo mức độ vi phạm; thông báo chính thức các vi phạm về an toàn thông tin cho bên thứ ba; kiểm tra xác định, lập báo cáo mức độ vi phạm và thông báo cho bên thứ ba thiệt hại xảy ra; thu hồi quyền truy cập hệ thống CNTT đã được cấp cho bên thứ ba;

d) Sau khi kết thúc công việc: Yêu cầu bên thứ ba bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc; thu hồi quyền truy cập hệ thống CNTT đã được cấp của bên thứ ba ngay sau khi kết thúc công việc; thay đổi các khóa, mật khẩu nhận bàn giao từ bên thứ ba.

Điều 7. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ ATTTM của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; 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.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 8. Bảo đảm an toàn thông tin hạ tầng vật lý

1. Bảo đảm an toàn thông tin hạ tầng vật lý là việc bảo vệ hệ thống kỹ thuật đối với các rủi ro mất an toàn về cháy, nổ, nhiệt độ, độ ẩm, thiên tai, mất điện, xâm nhập trái phép của con người và các hành vi liên quan khác có thể gây ảnh hưởng đến hoạt động hệ thống.

2. Các biện pháp bảo đảm an toàn thông tin hạ tầng vật lý bao gồm:

a) Quản lý trung tâm dữ liệu/phòng máy chủ:

- Trung tâm dữ liệu/phòng máy chủ phải được thiết lập cơ chế bảo vệ, theo dõi, phát hiện xâm nhập và biện pháp kiểm soát truy cập, kết nối vật lý phù hợp đối với từng khu vực.

- Quá trình vào, ra trung tâm dữ liệu/phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu/phòng máy chủ và phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học,...). Chỉ những cá nhân có quyền, nhiệm vụ được phép vào trung tâm dữ liệu/phòng máy chủ.

- Xây dựng phương án, kế hoạch phòng, chống và khắc phục sự cố ngập, rò rỉ nước, sét, tĩnh điện, cháy nổ; áp dụng các quy chuẩn kỹ thuật về an toàn kỹ thuật nhiệt, độ ẩm, ánh sáng cho các thiết bị tính toán, lưu trữ; bảo đảm điều kiện hoạt

động ổn định cho các hệ thống hỗ trợ như máy điều hòa nhiệt độ, nguồn cấp điện, dây dẫn.

- Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

- Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS,... phải được đặt trong trung tâm dữ liệu/phòng máy chủ, phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực như: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

- Đơn vị chủ quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

b) Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về tính khả dụng.

c) Các đường truyền dữ liệu, đường truyền Internet và hệ thống dây dẫn các hệ thống mạng diện rộng (WAN), hệ thống mạng nội bộ (LAN) phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt các cổng kết nối không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

d) Cá nhân sử dụng thiết bị lưu trữ dữ liệu di động để lưu trữ thông tin, dữ liệu cơ quan, đơn vị mình có trách nhiệm bảo vệ thiết bị này và thông tin lưu trên thiết bị, tránh làm mất hoặc lộ, lọt thông tin, dữ liệu.

đ) Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải được 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). Khi thanh lý thiết bị phải xóa nội dung lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

3. Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về ATTTM thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 9. Bảo đảm ATTTM khi sử dụng máy tính

1. Máy tính dùng để soạn thảo tài liệu mật thực hiện theo các quy định về bảo vệ bí mật nhà nước.

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 bộ phận chuyên trách về CNTT để được xử lý kịp thời.

3. Cá nhân chỉ cài đặt phần mềm hợp lệ; không được tự ý cài đặt hoặc gỡ bỏ

các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về CNTT; thường xuyên cập nhật phần mềm và hệ điều hành.

4. Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

5. Không được sử dụng máy tính của đơn vị để thâm nhập bất hợp pháp vào các mạng máy tính khác.

6. Thường xuyên thay đổi mật khẩu truy cập hệ thống thông tin, tối thiểu 03 tháng/lần. Khuyến khích đặt mật khẩu theo nguyên tắc: (1) mật khẩu có tối thiểu 08 ký tự, (2) mật khẩu bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

Điều 10. Bảo đảm an toàn trong quá trình vận hành, khai thác sử dụng các hệ thống thông tin

1. Trong quá trình khai thác, vận hành và sử dụng các ứng dụng, cơ sở hạ tầng, các đơn vị phải tuân thủ các quy chế về bảo đảm an toàn thông tin theo yêu cầu của từng hệ thống, ứng dụng.

2. Trong quá trình triển khai việc tích hợp ứng dụng, chia sẻ dữ liệu cần triển khai các giải pháp bảo đảm an toàn thông tin cho từng ứng dụng và trong quá trình chia sẻ dữ liệu cũng như làm rõ trách nhiệm của từng cơ quan, đơn vị và từng ứng dụng tham gia vào hệ thống.

3. Quản lý hệ thống mạng máy tính:

a) Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình mạng phân lớp, hạn chế sử dụng mô hình mạng ngang hàng. Các đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập hệ thống mạng riêng bảo mật để bảo đảm an toàn cho mạng nội bộ.

b) Khi thiết lập mạng không dây tại đơn vị, chỉ cho phép truy cập Internet, không cho phép kết nối vào mạng nội bộ của đơn vị. Thiết bị không dây cần được thiết lập các tham số như: tên, mật khẩu, mã hóa dữ liệu… và thông báo các thông tin liên quan đến điểm truy cập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

4. Quản lý nhật ký hệ thống: Hệ thống thông tin cần ghi nhận đầy đủ thông tin trong các bản ghi nhật ký khi thao tác trên hệ thống và lưu giữ nội dung nhật ký trong khoảng thời gian nhất định để phục vụ việc quản lý, kiểm soát hệ thống thông tin. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Các rủi ro có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, xóa mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

5. Quản lý tài khoản truy cập hệ thống:

a) Các hệ thống thông tin cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Tổ chức theo dõi và kiểm soát tất cả các phương pháp truy cập từ xa tới hệ thống thông tin; yêu cầu người dùng đặt mật khẩu với độ an toàn cao;

b) Cá nhân 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;

c) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ chế độ, trong vòng 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho cơ quan, đơn vị vận hành hệ thống thông tin bằng văn bản có xác nhận của thủ trưởng đơn vị để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin;

d) Tài khoản quản trị (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản quản trị phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị;

Trường hợp chia sẻ tài khoản quản trị thì phải được phê duyệt bởi cấp có thẩm quyền và xác định được trách nhiệm cá nhân tại mỗi thời điểm sử dụng;

Giới hạn và kiểm soát các truy cập sử dụng tài khoản quản trị: (1) Thiết lập cơ chế kiểm soát việc tạo tài khoản quản trị để bảo đảm không một tài khoản nào sử dụng được khi chưa được cấp có thẩm quyền phê duyệt; (2) Phải có biện pháp giám sát việc sử dụng tài khoản quản trị; (3) Việc sử dụng tài khoản quản trị phải được giới hạn bảo đảm chỉ có 01 truy cập quyền quản trị duy nhất, tự động thoát khỏi phiên đăng nhập khi không có hoạt động trong khoảng thời gian nhất định;

đ) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin hoặc đơn vị được giao vận hành hệ thống thông tin để xem xét, thực hiện. Đơn vị vận hành hệ thống thông tin có quyền 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;

e) Chủ quản hệ thống thông tin chủ động xây dựng quy định quản lý tài khoản truy cập hệ thống phù hợp thực tế triển khai tại đơn vị.

6. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy tính đang sử dụng, khi thực hiện việc chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ thông tin.

7. Khai thác, sử dụng các ứng dụng, hệ thống thông tin theo đúng chức năng, nhiệm vụ được giao, bảo đảm phục vụ tốt công tác chuyên môn, nghiệp vụ của đơn vị, phục vụ công dân, doanh nghiệp.

8. Trong quá trình vận hành hệ thống cần thực hiện quy định về phòng chống vi-rút, mã độc đáp ứng các yêu cầu cơ bản như:

a) Định kỳ kiểm tra, diệt vi-rút, mã độc và phương tiện mang thông tin, dữ liệu nhận từ bên ngoài trước khi sử dụng; Không mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi-rút, mã độc;

b) Không vào các trang/cổng thông tin điện tử không có nguồn gốc xuất xứ rõ ràng, đáng ngờ;

c) Báo ngay cho người quản trị hệ thống xử lý trong trường hợp phát hiện nhưng không diệt được vi-rút, mã độc;

d) Không tự ý cài đặt các phần mềm khi chưa được phép của người quản trị hệ thống.

9. Ứng dụng chữ ký số chuyên dùng để bảo đảm an toàn, an ninh thông tin trong việc triển khai ứng dụng CNTT trong hoạt động cơ quan nhà nước và phục vụ công dân, tổ chức.

10. Đối với bên thứ ba:

a) Thực hiện giám sát và kiểm tra các dịch vụ do bên thứ ba cung cấp bảo đảm mức độ cung cấp dịch vụ, khả năng hoạt động hệ thống đáp ứng đúng theo thỏa thuận đã ký kết;

b) Bảo đảm triển khai, duy trì các biện pháp an toàn, bảo mật của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận;

c) Quản lý các thay đổi đối với các dịch vụ của bên thứ ba cung cấp bao gồm: Nâng cấp phiên bản mới; sử dụng các kỹ thuật mới, các công cụ và môi trường phát triển mới;

d) Đánh giá đầy đủ tác động của việc thay đổi, bảo đảm an toàn khi được đưa vào sử dụng.

Điều 11. Xác định cấp độ và phương án bảo đảm an toàn cho các hệ thống thông tin

1. Chủ quản hệ thống thông tin thực hiện phân loại, xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin.

Việc phân loại, phê duyệt hồ sơ đề xuất cấp độ và bảo đảm an toàn thông tin theo cấp độ thực hiện theo quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT.

2. Chủ quản hệ thống thông tin phải có phương án bảo đảm an toàn hệ thống thông tin phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-BTTTT, tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách ATTTM của cơ quan ngành dọc Trung ương (nếu có).

Điều 12. Kiểm tra, đánh giá an toàn thông tin mạng

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

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

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT.

Điều 13. Giám sát an toàn thông tin mạng

1. Chủ quản hệ thống thông tin chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý.

2. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại và các văn bản quy phạm khác có liên quan.

3. Đơn vị chuyên trách an toàn thông tin của chủ quản hệ thống thông tin có trách nhiệm cử đầu mối giám sát ATTTM để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Đội ứng cứu sự cố ATTTM thành phố Hà Nội.

4. Sau khi Hệ thống giám sát, điều hành an toàn, an ninh mạng (Security Operations Center - SOC) đi vào hoạt động, chủ quản hệ thống thông tin có trách nhiệm chia sẻ, phối hợp trong công tác giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý.

Điều 14. Nguyên tắc chung trong ứng cứu sự cố

1. Nguyên tắc ứng cứu sự cố:

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả;

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin;

c) 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) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của đơn vị; cá nhân bảo mật thông tin cá nhân, thông tin riêng của đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Các sự cố an toàn thông tin dưới đây cần được xem xét phân loại và xử lý theo quy chế này, bao gồm:

a) Những truy cập trái phép, hành vi vi phạm tính bảo mật và tính toàn vẹn dữ liệu, ứng dụng;

b) Phát hiện mã độc, tấn công từ chối dịch vụ;

c) Phát hiện ra điểm yếu, lỗ hổng bảo mật của hạ tầng, hệ điều hành, ứng dụng;

d) Hệ thống trục trặc nhiều lần hoặc quá tải;

đ) Mất thiết bị, phương tiện CNTT;

e) Không tuân thủ chính sách an toàn thông tin hoặc các chỉ dẫn bắt buộc của đơn vị hoặc hành vi vi phạm an ninh vật lý;

g) Các trục trặc của phần mềm hay phần cứng không khắc phục được gây ảnh hưởng đến hoạt động của hệ thống CNTT;

h) Các sự cố khác gây gián đoạn, ảnh hưởng đến hoạt động bình thường của các ứng dụng CNTT tại đơn vị.

3. Đơn vị cần phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của đơn vị;

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến hoạt động chung của đơn vị;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của đơn vị.

4. Khi có sự cố hoặc nguy cơ mất an toàn thông tin thì lãnh đạo đơn vị phải chỉ đạo kịp thời:

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo cơ quan cấp trên quản lý trực tiếp;

b) Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ (mẫu báo cáo về sự cố mất an toàn thông tin quy định tại Phụ lục 1 kèm theo Quyết định này);

c) Tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố và thực hiện theo đúng hướng dẫn;

d) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết cho cơ quan cấp trên quản lý trực tiếp;

đ) Báo cáo bằng văn bản về sự cố cho cơ quan cấp trên quản lý trực tiếp và cơ quan quản lý nhà nước.

5. Tất cả công chức, viên chức, người lao động và bên thứ ba khi phát hiện các sự cố của đơn vị cần thực hiện việc báo cáo với đơn vị đó nhằm ngăn chặn các sự cố an toàn thông tin.

6. Thiết lập cơ chế sao lưu và phục hồi hệ thống:

a) Ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết;

b) 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;

c) Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên bảo đảm sẵn sàng cho việc sử dụng khi cần;

d) Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 06 tháng/lần.

7. Kế hoạch ứng phó sự cố ATTTM:

a) Các đơn vị tổ chức xây dựng, phê duyệt Kế hoạch ứng phó sự cố cho các

hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II, Quyết định số 05/2017/QĐ-TTg;

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi Sở Thông tin và Truyền thông tổng hợp thành kế hoạch chung của Thành phố. Sở Thông tin và Truyền thông có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Thành phố và trình Lãnh đạo UBND Thành phố phê duyệt;

c) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh trước ngày 31/10 hằng năm (nếu cần thiết), làm cơ sở để xây dựng kế hoạch bảo đảm ATTTM năm tiếp theo.

8. Quy trình ứng cứu sự cố ATTTM:

a) Các đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố ATTTM cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin liên quan, đơn vị chuyên trách về ứng cứu sự cố ATTTM thông qua đầu mối tiếp nhận thông báo sự cố được đăng công khai trên cổng thông tin điện tử. Sở Thông tin và Truyền thông có trách nhiệm cập nhật thông tin đầu mối tiếp nhận thông báo sự cố ATTTM của Thành phố và các đơn vị trên Cổng giao tiếp điện tử thành phố Hà Nội.

b) Khi xảy ra sự cố ATTTM thuộc loại hình và có mức độ được quy định tại Điều 14 Quy chế này, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại điểm a Khoản 1 Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9, Biểu mẫu số 03 Phụ lục I Thông tư số 20/2017/TT-BTTTT, đồng thời báo cáo Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND Thành phố. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố ATTTM theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

c) Quy trình ứng cứu sự cố ATTTM được thực hiện theo Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

9. Diễn tập ứng cứu sự cố ATTTM:

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt;

b) Sở Thông tin và Truyền thông chủ trì, phối hợp với các đơn vị tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức; hằng năm tổ chức diễn tập ứng cứu sự cố ATTTM trong phạm vi của Thành phố được quy định tại điểm b, nhiệm vụ 4 Mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ về phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố ATTTM trên toàn quốc đến 2020, định hướng đến 2025.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 15. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức được giao phụ trách an toàn thông tin:

a) Chịu trách nhiệm bảo đảm ATTTM của đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm ATTTM;

c) Thực hiện việc giám sát, đánh giá, báo cáo lãnh đạo cơ quan các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố ATTTM;

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm ATTTM của đơn vị.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động của đơn vị:

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. Chịu trách nhiệm bảo đảm ATTTM trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cán bộ, công chức, viên chức và người lao động phải 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 ATTTM phải báo cáo ngay với cấp trên và bộ phận chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về ATTTM được thành phố hoặc đơn vị tổ chức.

Điều 16. Trách nhiệm của các đơn vị

1. Giám đốc, Thủ trưởng các đơn vị chịu trách nhiệm trước Chủ tịch UBND Thành phố nếu lơ là trong công tác bảo đảm ATTTM, để xảy ra hậu quả, thiệt hại nghiêm trọng tại đơn vị thuộc phạm vi quản lý.

2. Giám đốc, Thủ trưởng các đơn vị có trách nhiệm tổ chức thực hiện các quy định tại quy chế này và chịu trách nhiệm trong công tác bảo đảm ATTTM của đơn vị mình.

3. Bảo đảm tỷ lệ kinh phí cho các sản phẩm, dịch vụ ATTTM đạt tối thiểu 10% trong tổng kinh phí triển khai ứng dụng CNTT hằng năm, giai đoạn 05 năm và các dự án CNTT của đơn vị.

4. Phân công một bộ phận hoặc cán bộ chuyên trách bảo đảm an toàn thông tin của đơn vị, tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

5. Xây dựng quy định, quy trình khai thác dữ liệu cho các phần mềm ứng dụng, cơ sở dữ liệu; quy chế, quy trình nội bộ về bảo đảm an toàn thông tin, ứng cứu sự cố phù hợp với quy chế này, các quy định của pháp luật và tình hình từng đơn vị.

6. Công bố thông tin đầu mối (số điện thoại, thư điện tử hoặc các kênh liên lạc khác) tiếp nhận thông báo sự cố trên cổng thông tin điện tử của đơn vị. Thông báo thông tin đầu mối cho Sở Thông tin và Truyền thông tổng hợp, cập nhật trên Cổng giao tiếp điện tử thành phố Hà Nội.

7. 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.

8. Phối hợp chặt chẽ với Công an thành phố trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm ATTTM.

9. Chủ động phối hợp Sở Thông tin và Truyền thông trong việc duy trì kết nối, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực để được hỗ trợ giám sát, phân tích, cảnh báo sớm về các nguy cơ về ATTTM và tấn công mạng.

10. Chủ động tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin trong công tác quản lý nhà nước tại đơn vị.

11. Định kỳ hằng năm, các cơ quan lập báo cáo về tình hình an toàn thông tin theo Biểu mẫu tại Phụ lục kèm theo Quy chế này và gửi về UBND thành phố Hà Nội (thông qua Sở Thông tin và Truyền thông) trước ngày 15/01 của năm tiếp theo.

12. Định kỳ trước ngày 22 hằng tháng, cung cấp thông tin về tình hình, kết quả triển khai xây dựng, thẩm định và phê duyệt Hồ sơ đề xuất cấp độ về Bộ Thông tin và Truyền thông, UBND thành phố Hà Nội (thông qua Sở Thông tin và Truyền thông).

Điều 17. Trách nhiệm của Sở Thông tin và Truyền thông

1. Là cơ quan chuyên trách về an toàn thông tin của thành phố, có trách nhiệm tham mưu UBND Thành phố về công tác bảo đảm ATTTM trên địa bàn thành phố.

2. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

3. Là cơ quan chuyên trách về ứng cứu sự cố ATTTM của thành phố, đầu mối thực hiện các nhiệm vụ về ứng cứu sự cố ATTTM trên địa bàn thành phố và có trách nhiệm thực hiện quy định tại Khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

4. Chủ trì kiện toàn Đội ứng cứu sự cố ATTTM thành phố Hà Nội.

5. Thực hiện nhiệm vụ là Thành viên Mạng lưới ứng cứu sự cố an toàn không gian mạng quốc gia. Phối hợp với Cơ quan điều phối quốc gia về ứng cứu sự cố, các thành viên Mạng lưới ứng cứu sự cố ATTTM quốc gia, bộ phận tác nghiệp ứng cứu khẩn cấp quốc gia để triển khai hoạt động ứng cứu sự cố ATTTM khi có yêu cầu.

6. Chủ trì, phối hợp với các đơn vị liên quan tham mưu UBND Thành phố xây dựng, sửa đổi, ban hành Quy chế hoạt động của Đội ứng cứu sự cố ATTTM thành phố Hà Nội và Phương án, kịch bản ứng cứu sự cố cho các hệ thống thông tin của thành phố Hà Nội.

7. Tùy theo mức độ sự cố, phối hợp Trung tâm Công nghệ thông tin và Giám sát an ninh mạng - Ban Cơ yếu Chính phủ, Bộ Tư lệnh 86 - Bộ Quốc phòng, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố ATTTM.

8. Phối hợp Trung tâm Công nghệ thông tin và Giám sát an ninh mạng - Ban Cơ yếu Chính phủ, Bộ Tư lệnh 86 - Bộ Quốc phòng, Cục An toàn thông tin - Bộ Thông tin và Truyền thông và các đơn vị có liên quan trong việc duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực về Hệ thống giám sát quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về ATTTM và tấn công mạng.

9. Chủ trì, phối hợp với Văn phòng UBND Thành phố, Công an Thành phố và các đơn vị liên quan tiến hành kiểm tra công tác bảo đảm ATTTM định kỳ hằng năm đối với các đơn vị.

10. Tổng hợp và báo cáo về tình hình ATTTM định kỳ gửi Bộ Thông tin và Truyền thông, UBND Thành phố và các đơn vị có liên quan theo quy định.

11. Hằng năm xây dựng và triển khai các chương trình đào tạo về ATTTM cho lực lượng bảo đảm an toàn thông tin của các đơn vị. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin trong công tác quản lý nhà nước trên địa bàn Thành phố.

Điều 18. Trách nhiệm của Công an thành phố Hà Nội

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội, ảnh hưởng đến an toàn thông tin trong cơ quan nhà nước.

2. Xử lý các trường hợp vi phạm pháp luật về an toàn thông tin theo thẩm quyền.

3. Hỗ trợ các đơn vị thực hiện việc kiểm tra, đánh giá các trang thiết bị CNTT trước khi đưa vào sử dụng khi có yêu cầu.

Điều 19. Tổ chức thực hiện

Trong quá trình thực hiện nếu có các vấn đề nảy sinh, không phù hợp hoặc chưa được quy định rõ, các đơn vị gửi kiến nghị, đề xuất về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND Thành phố kịp thời xem xét điều chỉnh, bổ sung phù hợp với tình hình thực tiễn./.

Phụ lục

MẪU BÁO CÁO CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN

(Ban hành kèm theo Quyết định số 2223/QĐ-UBND ngày 14 tháng 4 năm 2023 của Ủy ban nhân dân thành phố Hà Nội)

UBND THÀNH PHỐ HÀ NỘI **Tên đơn vị.....**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

Hà Nội, ngày tháng năm 20...

BÁO CÁO CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN NĂM.....

I. Đánh giá hiện trạng

1. Về chính sách, quản lý

Đơn vị:

+ Đã xây dựng kế hoạch để bảo đảm an toàn thông tin cho đơn vị?

❍ Rồi (đề nghị gửi kèm văn bản) ❍ Chưa

+ Có các biện pháp vận hành liên tục và khôi phục sự cố không?

❍ Có ❍ Không

+ Có thường xuyên cập nhật công nghệ bảo đảm an toàn thông tin hay không?

❍ Có ❍ Không

2. Về đầu tư

Đơn vị:

+ Phần trăm ngân sách trong tổng số ngân sách cho công nghệ thông tin để đầu tư vào việc bảo đảm an toàn thông tin: ..... %

+ Đã đầu tư, triển khai các nội dung bảo đảm an toàn thông tin nào dưới đây:

Lĩnh vực	Mô tả nội dung
1. Xây dựng chính sách/ hướng dẫn	
2. Sử dụng dịch vụ hỗ trợ bảo đảm an toàn thông tin	
3. Yêu cầu tư vấn	
4. Mua thiết bị an toàn thông tin	
5. Đào tạo nguồn nhân lực	
6. Các vấn đề khác:	

+ Đã sử dụng những công cụ nào để bảo đảm an toàn thông tin?

Công cụ	Mô tả nội dung
1. Công cụ diệt Virus(Anti Virus)	
2. Mật khẩu	
3. Tường lửa	
4. Công cụ lọc thư rác	
5. Công cụ mã hóa tập tin	
6. Công cụ chống DDos	
7. Chữ ký điện tử	
8. Mạng riêng ảo (VPN)	
9. Hệ thống phát hiện xâm nhập	
10. Những công cụ khác:	

3. Về tình hình an toàn thông tin mạng và xử lý sự cố

Loại sự cố/tấn công mạng	Số lượng	Số sự cố tự xử lý	Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác	Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài	Số sự cố đề nghị Đội UCSC ATTTM thành phố	Thiệt hại ước tính *(Đơn vị tính: đồng)*
Từ chối dịch vụ						
Tấn công giả mạo						
Tấn công sử dụng mã độc						
Truy cập trái phép, chiếm quyền điều khiển						
Thay đổi giao diện						
Mã hóa phần mềm, dữ liệu, thiết bị						
Phá hoại thông tin, dữ liệu, phần mềm						
Nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu						
Tấn công tổng hợp sử dụng kết hợp nhiều hình thức						
Các hình thức tấn công khác						
Tổng số						

+ Cho biết công việc mà cơ quan đã thực hiện sau khi khắc phục được sự cố trong năm qua:

☐ Sửa đổi chính sách/ hướng dẫn/ thủ tục

☐ Nâng cao ý thức

☐ Tăng cường thiết bị

☐ Rà soát lại hệ thống

☐ Mở rộng lại liên kết với các đơn vị hoạt động trong lĩnh vực an toàn thông tin

☐ Việc khác:

.....

.....

.....

.....

4. Tổ chức nhân lực và bồi dưỡng nghiệp vụ:

+ Đơn vị có cán bộ phụ trách về bảo đảm an toàn thông tin không?

O Có O Không

+ Nếu có, người phụ trách là?

O Lãnh đạo cơ quan O Giám đốc trung tâm CNTT

O Cán bộ chuyên trách CNTT O Khác: .....

+ Nếu chưa có, thì đơn vị có dự kiến tổ chức bộ phận đó không?

O Có O Không

Dự kiến sẽ triển khai thành lập vào tháng ..... năm ....., với số lượng cán bộ là ..... người.

+ Đơn vị có nhu cầu bồi dưỡng nghiệp vụ an toàn thông tin

☐ Dành cho lãnh đạo và cán bộ quản lý, số lượng dự kiến: ..... người

☐ Cơ bản/Nâng cao về an toàn thông tin cho cán bộ kỹ thuật, số lượng: ..... người

☐ Kỹ năng an toàn thông tin cho người dùng , Số lượng dự kiến: ..... người

+ Đơn vị đã có dự trù kinh phí cho đào tạo nguồn nhân lực bảo đảm an ninh thông tin của đơn vị hay chưa?

O Có O Chưa

+ Nếu tự đánh giá, mức độ ATTTM của đơn vị trong năm 20..... là:

Kém		Trung bình	Tốt		Rất tốt
O 0	O 1	O 2	O 3	O 4	O 5

II. Ý kiến phản hồi và góp ý thêm

.....

.....

.....

.....

.....

.....

Chú ý:

- Điền thông tin đầy đủ vào các câu hỏi:

- Để lựa chọn đánh dấu X

- Câu hỏi với ký hiệu ❍ trước mỗi lựa chọn thì chỉ được phép đánh dấu một kết quả (chọn một)

- Câu hỏi với ký hiệu ☐ trước mỗi lựa chọn thì có thể đánh dấu từ không tới nhiều kết quả (chọn nhiều)

- Ký, ghi tên và đóng dấu đầy đủ vào cuối báo cáo và gửi về theo đường công văn cho Sở Thông tin và Truyền thông.

Lãnh đạo đơn vị

(Ký tên đóng dấu)

Quy chế gồm 03 Chương 19 Điều với bố cục được vận dụng từ Quyết định số 411/QĐ-UBND ngày 27/01/2015 của UBND thành phố Hà Nội về việc ban hành quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước thành phố Hà Nội.

STT	Nội dung Quy chế	Căn cứ đề xuất
Chương I. Quy định chung (gồm 07 Điều: từ Điều 1 đến Điều 7)		
1	Điều 1. Phạm vi điều chỉnh Điều 2. Đối tượng áp dụng	Vận dụng theo Điều 1, Điều 2 Quyết định số 411/QĐ-UBND. Bổ sung thêm Khoản 3 Điều 2 với mục tiêu Quy chế này được phổ biến, áp dụng rộng rãi tới các tổ chức, đoàn thể chính trị trên địa bàn thành phố
2	Điều 3. Giải thích từ ngữ	Trên cơ sở Điều 4 Quyết định số 411/QĐ-UBND, đơn vị soạn thảo bổ sung (toàn văn) các nội dung theo các quy định mới tại Luật An toàn thông tin mạng, Chỉ thị số 23/CT-TTG năm 2022, Nghị định số 85/2016/NĐ-CP, Thông tư số 20/2017/TT-BTTTT.
3	Điều 4. Nguyên tắc bảo đảm ATTTM	Đơn vị soạn thảo đã điều chỉnh lại nhằm vẫn duy trì được nội dung cơ bản theo Điều 3 Quyết định số 411/QĐ-UBND và các quy định mới tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT cho phù hợp với tình hình hiện tại.
4	Điều 5. Quản lý trang thiết bị CNTT	Vận dụng lại Điều 5 Quyết định số 411/QĐ-UBND và một số quy định, nghị quyết liên quan đến bảo vệ bí mật nhà nước.
5	Điều 6. Quản lý nguồn nhân lực	Vận dụng lại Điều 6 Quyết định số 411/QĐ-UBND và điều chỉnh câu chữ phù hợp quy định hiện tại và tình hình thực tế
6	Điều 7. Các hành vi bị nghiêm cấm	Quyết định số 411/QĐ-UBND chưa quy định đối với nội dung này, đơn vị soạn thảo bổ sung toàn văn theo Điều 7 Luật An toàn thông tin mạng để các đơn vị thuận tiện trong nghiên cứu, triển khai.

STT	Nội dung Quy chế	Căn cứ đề xuất
Chương II. Bảo đảm an toàn thông tin mạng và ứng cứu sự cố an toàn thông tin mạng (gồm 07 Điều: từ Điều 8 đến Điều 14)		
7	Điều 8. Bảo đảm an toàn thông tin hạ tầng vật lý Điều 9. Bảo đảm ATTTM khi sử dụng máy tính Điều 10. Bảo đảm an toàn trong quá trình vận hành, khai thác sử dụng các hệ thống thông tin	Vận dụng từ một số nội dung vẫn còn phù hợp với tình hình thực tế tại Điều 7, Điều 8, Điều 9 Quyết định số 411/QĐ-UBND. Bên cạnh đó, đơn vị soạn thảo nghiên cứu, bổ sung thêm theo các hướng dẫn mới nhất như Công văn số 2290/BTTTT-CATTT ngày 17/7/2018 của Bộ Thông tin và Truyền thông về việc hướng dẫn kết nối, chia se thông tin về mã độc giữa các hệ thống kỹ thuật; Công văn số 1694/BTTTT-CATTT ngày 31/5/2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn yêu cầu an toàn thông tin cơ bản đối với hệ thống thông tin kết nối vào mạng Truyền số liệu chuyên dùng; Công văn số 3001/BTTTT-CATTT ngày 06/9/2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn bảo đảm an toàn thông tin cho hệ thống quản lý văn bản và điều hành; Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 của Cục An toàn thông tin về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ.
8	Điều 11. Xác định cấp độ và phương án bảo đảm an toàn cho các hệ thống thông tin Điều 12. Kiểm tra, đánh giá an toàn thông tin mạng Điều 13. Kiểm tra, đánh giá an toàn thông tin mạng Giám sát an toàn thông tin mạng	Nội dung này chưa được quy định tại Quyết định số 411/QĐ-UBND. Đây là nội dung mới, đơn vị soạn thảo trích dẫn và vận dụng từ các quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 31/2017/TT-BTTTT, Thông tư số 12/2022/TT-BTTTT về xác định cấp độ cho hệ thống thông tin, kiểm tra, đánh giá và giám sát an toàn thông tin mạng.
9	Điều 14. Nguyên tắc chung trong ứng cứu sự cố	Quy định về ứng cứu sự cố chưa được quy định tại Quyết định số 411/QĐ-UBND. Đơn vị soạn thảo trích dẫn và vận dụng theo Quyết định số 632/QĐ-TTg năm 2017, Quyết định số 05/QĐ-TTg năm 2017, Quyết định số 1622/QĐ-TTg năm 2017, Thông tư số 20/2017/TT-BTTTT, Thông tư số 31/2017/TT-BTTTT, Chỉ thị số 18/CT-TTg năm 2022, Công văn số 4258/BTTTT-

STT	Nội dung Quy chế	Căn cứ đề xuất
		CATTT ngày 26/10/2021 của Bộ Thông tin và Truyền thông về việc hướng dẫn tổ chức, hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng, Công văn số 793/CATTT-VNCERTCC ngày 25/6/2021 của Cục An toàn thông tin về việc hướng dẫn quy trình ứng cứu, xử lý sự cố tấn công mạng
Chương III. Tổ chức thực hiện (gồm 05 Điều: từ Điều 15 đến Điều 19)		
10	Điều 15. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các đơn vị Điều 16. Trách nhiệm của các đơn vị Điều 17. Trách nhiệm của Sở Thông tin và Truyền thông Điều 18. Trách nhiệm của Công an thành phố Hà Nội Điều 19. Tổ chức thực hiện	Quy định về tổ chức thực hiện, trách nhiệm của các cơ quan, đơn vị, tổ chức và cá nhân trong công tác bảo đảm an toàn hệ thống thông tin của cơ quan, đơn vị được vận dụng từ Điều 12, 13, 14, 15, 16 Quyết định số 411/QĐ-UBND và một số quy định như Chỉ thị số 14/CT-TTg năm 2018, Chỉ thị số 14/CT-TTg năm 2019, Chỉ thị số 18/CT-TTg năm 2022, Chỉ thị số 02/CT-TTg năm 2022, Chỉ thị số 23/CT-TTg năm 2022, Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT.