ỦY BAN NHÂN DÂN THÀNH PHỐ CẦN THƠ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 37 /2026/QĐ-UBND	*Cần Thơ, ngày 09 tháng 4 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;

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

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 16/2024/TT-BTTTT ngày 30 tháng 12 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng;

Theo đề nghị của Giám đốc Công an thành phố;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ.

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ.

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực thi hành từ ngày *09* tháng 4 năm 2026.

2. Quyết định này bãi bỏ các Quyết định sau:

a) Quyết định số 2945/QĐ-UBND ngày 09 tháng 10 năm 2015 của Ủy ban nhân dân thành phố Cần Thơ về việc ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ;

b) Quyết định số 48/2024/QĐ-UBND ngày 22 tháng 11 năm 2024 của Ủy ban nhân dân tỉnh Hậu Giang ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hậu Giang.

Điều 3. Giám đốc Công an thành phố, Giám đốc Sở, Thủ trưởng cơ quan, ban, ngành thành phố, Chủ tịch Ủy ban nhân dân xã, phường và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Công an;
- Cục KTVB và TCTHPL - Bộ Tư pháp;
- Thường trực Thành ủy;
- Thường trực HĐND TP;
- CT, các PCT UBND TP;
- UBMTTQVN TP;
- Sở, ban, ngành TP;
- UBND xã, phường;
- Báo và PTTH Cần Thơ;
- Cổng TTĐT TP;
- Công báo TP;
- VP UBND TP (2C, 3C);
- Lưu: VT, VHQ.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

ỦY BAN NHÂN DÂN THÀNH PHỐ CẦN THƠ

Trương Cảnh Tuyên

ỦY BAN NHÂN DÂN **THÀNH PHỐ CẦN THƠ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ

Bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ

(Ban hành kèm theo Quyết định số 37 /2026/QĐ-UBND)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung liên quan đến bảo đảm an toàn thông tin (ATTT) trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước thuộc Ủy ban nhân dân (UBND) thành phố Cần Thơ (sau đây gọi tắt là cơ quan, đơn vị).

Điều 2. Đối tượng áp dụng

1. Các cơ quan nhà nước thành phố Cần Thơ, bao gồm: Sở, ban, ngành, đơn vị sự nghiệp trực thuộc UBND thành phố; UBND xã, phường và các đơn vị trực thuộc.

2. Các tổ chức, cá nhân liên quan đến an toàn thông tin mạng (ATTTM) trong các cơ quan nhà nước nêu tại khoản 1 Điều này.

Điều 3. Giải thích từ ngữ

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

1. *Cán bộ được giao phụ trách bảo đảm ATTT* là cán bộ, công chức, viên chức, người lao động được giao phụ trách công tác bảo đảm ATTTM cho việc triển khai, vận hành, khai thác hệ thống CNTT tại cơ quan nhà nước.

2. *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 thông tin (HTTT).

3. *Phần mềm hệ thống (Firmware)* là một loại chương trình máy tính đặc biệt được lưu trữ trực tiếp trên bộ nhớ của thiết bị điện tử. Nó cung cấp kiểm soát mức thấp và quản lý hoạt động của phần cứng cụ thể trong thiết bị. Firmware chịu trách nhiệm điều khiển các chức năng cơ bản và nâng cao của thiết bị, đồng thời đảm bảo hoạt động ổn định và chính xác.

4. *Mức độ rủi ro ATTT (Critical, High, Medium, Low)* là mức độ đánh giá ảnh hưởng của lỗ hổng, sự cố hoặc nguy cơ ATTT đối với HTTT, được phân thành các mức sau đây:

a) Mức độ nghiêm trọng đặc biệt cao (Critical) là mức độ rủi ro cao nhất, có khả năng gây gián đoạn nghiêm trọng hoặc làm tê liệt hoạt động của HTTT, gây mất, lộ, thay đổi dữ liệu quan trọng hoặc ảnh hưởng lớn đến hoạt động của cơ quan, đơn vị;

b) Mức độ nghiêm trọng cao (High) là mức độ rủi ro có khả năng gây ảnh hưởng lớn đến HTTT, làm suy giảm đáng kể tính bảo mật, toàn vẹn hoặc khả dụng của dữ liệu nếu không được xử lý kịp thời;

c) Mức độ nghiêm trọng trung bình (Medium) là mức độ rủi ro có khả năng gây ảnh hưởng ở mức trung bình đến hoạt động của HTTT, chưa gây gián đoạn nghiêm trọng nhưng cần được theo dõi, khắc phục để phòng ngừa rủi ro phát sinh;

d) Mức độ nghiêm trọng thấp (Low) là mức độ rủi ro ít ảnh hưởng đến hoạt động của HTTT, chưa gây tác động đáng kể và có thể được xử lý trong quá trình vận hành thông thường.

5. *Mạng riêng ảo (VPN - Virtual Private Network)* là một mạng máy tính dành riêng để kết nối các máy tính của các cơ quan nhà nước với nhau thông qua mạng Internet.

Điều 4. Nguyên tắc bảo đảm an toàn an ninh mạng

1. Việc bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp, sử dụng và hủy bỏ trong ứng dụng CNTT của cơ quan nhà nước; bảo đảm ATTTM được thực hiện một cách tổng thể, đồng bộ, tập trung, xuyên suốt trong các hoạt động đầu tư, mua sắm, nâng cấp các giải pháp, vận hành, bảo trì, ngừng sử dụng hạ tầng, HTTT, phần mềm, dữ liệu. Có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

2. Việc thực hiện các phương pháp bảo đảm an toàn, an ninh thông tin phải tuân theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13, Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

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.

5. Bố trí nguồn lực phù hợp với quy mô, điều kiện của cơ quan, đơn vị nhằm thực hiện tốt nhất công tác bảo đảm an toàn, an ninh thông tin.

Điều 5. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng thực hiện theo quy định tại Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13, Điều 8 Luật An ninh mạng số 24/2018/QH14, Điều 5 Luật Bảo vệ bí mật nhà nước số 117/2025/QH15.

Điều 6. Đầu mối liên hệ, ứng cứu sự cố ATTTM

1. Đầu mối ứng cứu sự cố ATTTM trong cơ quan nhà nước thành phố Cần Thơ:

Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Công an thành phố Cần Thơ, điện thoại: 0693672605, thư điện tử: anninhmang.catpcantho@cantho.gov.vn.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức ngoài thành phố trong công tác hỗ trợ điều phối xử lý sự cố ATTTM:

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT), điện thoại 0692205199, thư điện tử: report@vncert.vn.

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

Điều 7. Thiết kế an toàn HTTT

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

2. Có tài liệu mô tả thiết kế và các thành phần của HTTT.

3. Có tài liệu mô tả phương án bảo đảm ATTT theo cấp độ.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT.

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.

Điều 8. Phát triển phần mềm thuê khoán

1. Có biên bản, hợp đồng và các cam kết đối với bên thứ ba các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá ATTT trước khi đưa vào sử dụng.

Điều 9. Thử nghiệm và nghiệm thu HTTT

1. Thực hiện thử nghiệm và nghiệm thu HTTT trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu HTTT.

3. Có bộ phận chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu HTTT.

4. Có bên thứ ba là đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu HTTT.

5. Có báo cáo nghiệm thu được xác nhận của bộ phận phụ trách ATTT và phê duyệt của chủ quản HTTT trước khi đưa vào sử dụng.

Điều 10. Xác định cấp độ và phương án bảo đảm an toàn cho các HTTT

1. Chủ quản HTTT thực hiện phân loại, xác định cấp độ HTTT, giao đơn vị vận hành HTTT xây dựng hồ sơ đề xuất bảo đảm an toàn HTTT theo cấp độ trong đó phải có phương án bảo đảm an toàn HTTT phù hợp với cấp độ của HTTT và đáp ứng yêu cầu quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách ATTTM của cơ quan Trung ương được tổ chức theo ngành dọc đóng trên địa bàn thành phố (nếu có).

2. HTTT đang vận hành trong các cơ quan nhà nước hoặc HTTT khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp phải được thẩm định, phê duyệt hồ sơ cấp độ và triển khai đầy đủ các phương án bảo đảm ATTT theo cấp độ tương ứng.

3. Các HTTT đang vận hành trong các cơ quan nhà nước phải được kiểm tra đánh giá định kỳ theo hồ sơ đề xuất cấp độ đã phê duyệt và bố trí kinh phí để nâng cấp, vá lỗi.

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

Điều 11. Quản lý trang thiết bị ứng dụng CNTT trong hoạt động của cơ quan, đơn vị

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị ứng dụng CNTT trong hoạt động của cơ quan, đơn vị.

2. Cơ quan, đơn vị quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị ứng dụng CNTT trong hoạt động của cơ quan, đơn vị trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị ứng dụng CNTT trong hoạt động của cơ quan, đơn vị liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

3. Trang thiết bị ứng dụng CNTT trong hoạt động của cơ quan, đơn vị khi thay đổi mục đích sử dụng hoặc thanh lý thì cơ quan, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị đó.

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

5. 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 đơn vị; thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị dự phòng).

Điều 12. Bảo đảm ATTT hạ tầng vật lý

1. Bảo đảm ATTT 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 hạ tầng vật lý.

2. Quản lý an toàn trung tâm dữ liệu/phòng máy chủ:

a) 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;

b) 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;

c) 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;

d) 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 (mười lăm) phút khi có sự cố mất điện;

đ) 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..., 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;

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

3. Quản lý an toàn hệ thống mạng máy tính, kết nối Internet:

a) Quản lý hệ thống mạng nội bộ: mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát (tường lửa phải được cập nhật dữ liệu hàng năm), có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu;

b) Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây, 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, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu có độ phức tạp cao (có độ dài tối thiểu 08 (tám) ký tự, có ký tự thường, ký tự hoa, ký tự số, ký tự đặc biệt), cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật (WPA2 hoặc WPA3). Trường hợp cần thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ ít nhất 03 (ba) tháng một lần;

c) Quản lý truy cập từ xa vào mạng nội bộ: đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, nhắc nhở khuyến cáo thường xuyên thay đổi mật mã, tăng cường sử dụng mạng riêng ảo, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng;

d) 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;

đ) Đối với các cơ quan nhà nước có sử dụng đường truyền Internet ngoài đường truyền số liệu chuyên dùng trong hệ thống các cơ quan Đảng, Nhà nước thì phải thông báo về Công an thành phố để được hướng dẫn đấu nối, thiết lập các thông số của các thiết bị định tuyến, cấu hình địa chỉ IP cho hệ thống mạng nội bộ, các máy chủ, máy trạm trong cơ quan thống nhất với toàn hệ thống.

4. 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.

5. Thường xuyên cập nhật bản vá lỗ hổng bảo mật, nâng cấp Firmware đối với các thiết bị mạng.

6. Cá nhân sử dụng thiết bị lưu trữ dữ liệu di động để lưu trữ thông tin, dữ liệu cơ quan nhà nước 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.

7. 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 hoặc phá hủy vật lý.

8. Cơ quan nhà nước 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 phụ 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 13. 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 phòng chống mã độc 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 mã độc trên máy tính phải tắt máy và báo trực tiếp cho bộ phận phụ trách về ATTTM 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 phụ trách về ATTTM; 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 cơ quan nhà nước để thâm nhập bất hợp pháp vào các mạng máy tính khác.

6. Thường xuyên thay đổi mật khẩu truy cập HTTT, tối thiểu 03 (ba) tháng/lần; thay đổi mật khẩu mặc định trong lần đăng nhập đầu tiên; giới hạn một số hữu hạn lần đăng nhập sai liên tiếp, sau từ 03 (ba) đến 05 (năm) lần đăng nhập không thành công hệ thống sẽ tự động khóa tài khoản người dùng và có cơ chế chống vét cạn, mã captcha. Yêu cầu đặt mật khẩu theo nguyên tắc: mật khẩu có tối thiểu 08 (tám) ký tự bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

Điều 14. Quản lý nhật ký hệ thống

HTTT 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 HTTT. 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 HTTT.

Điều 15. Quản lý tài khoản truy cập hệ thống

1. Cơ quan nhà nước xây dựng quy định quản lý tài khoản truy cập HTTT phù hợp thực tế triển khai tại đơn vị.

2. Tổ chức theo dõi và kiểm soát tất cả các phương pháp truy cập từ xa đến HTTT; cần có chức năng ghi nhận các dấu hiệu bất thường liên quan đến việc sử dụng tài khoản người dùng.

3. Cá nhân sử dụng HTTT được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó.

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

5. 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; phải được giao đích danh cá nhân làm công tác quản trị; hạn chế sử dụng 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.

6. Giới hạn và kiểm soát các truy cập sử dụng tài khoản quản trị:

a) 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;

b) Phải có biện pháp giám sát việc sử dụng tài khoản quản trị;

c) Việc sử dụng tài khoản quản trị phải được giới hạn bảo đảm chỉ có 01 (một) 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.

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

Điều 16. Quản lý an toàn máy chủ và ứng dụng

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

a) Có bộ phận thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng hệ thống;

b) Giải pháp giám sát HTTT tập trung phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thiết bị hệ thống bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của thiết bị hệ thống, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực.

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

a) Định kỳ hàng tháng hoặc khi có thay đổi cấu hình thiết bị hệ thống, toàn bộ tập tin cấu hình thiết bị hệ thống được sao lưu dự phòng trên thiết bị và hệ thống lưu trữ độc lập;

b) Tệp tin cấu hình của toàn bộ thiết bị hệ thống phải được sao lưu dự phòng theo từng phiên bản khác nhau, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn;

c) Sơ đồ thiết kế hệ thống về logic và vật lý phải được cập nhật khi có sự thay đổi về thiết kế và được sao lưu dự phòng theo từng phiên bản khác nhau, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn;

d) Có thiết bị hoặc thiết lập hệ thống, phân vùng lưu trữ độc lập để lưu trữ tệp tin cấu hình, sơ đồ hệ thống và các dữ liệu khác phục vụ quản lý an toàn mạng; dữ liệu được lưu trữ phải được phân loại và gán nhãn dữ liệu, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn.

3. Truy cập và quản lý cấu hình hệ thống:

a) Chỉ cho phép truy cập, cấu hình thiết bị hệ thống từ vùng mạng quản trị;

b) Truy cập, cấu hình thiết bị hệ thống từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng;

d) Toàn bộ thao tác thay đổi, thiết lập cấu hình thiết bị hệ thống phải được ghi nhật ký hệ thống.

4. Thường xuyên nâng cấp, cập nhật bản vá lỗ hổng bảo mật đối với các nền tảng ảo hóa, nền tảng ứng dụng, hệ điều hành để đáp ứng được yêu cầu bảo đảm ATTT.

Điều 17. Quản lý an toàn dữ liệu

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

a) Toàn bộ cơ sở dữ liệu, dữ liệu nghiệp vụ của hệ thống khi lưu trữ trên thiết bị và hệ thống lưu trữ độc lập phải được mã hóa và kèm theo mã kiểm tra tính toàn vẹn;

b) Dữ liệu được sao lưu dự phòng theo từng phiên bản và có nhật ký ghi lại thông tin dữ liệu sau mỗi lần thực hiện sao lưu, dự phòng;

c) Độ dài của khóa bí mật dùng để mã hóa dữ liệu tối thiểu 128 bit.

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

a) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu hệ thống (tệp tin cấu hình, ảnh hệ điều hành,…) được quản lý bởi bộ phận phụ trách ATTTM;

b) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu nghiệp vụ (tệp tin dữ liệu, cơ sở dữ liệu,…) được quản lý bởi bộ phận nghiệp vụ tương ứng;

c) Thông tin khóa bí mật phải được lưu trữ mã hóa, kèm theo mã kiểm tra tính toàn vẹn trên thiết bị và hệ thống lưu trữ độc lập;

d) Chỉ có bộ phận/cán bộ có chức năng có quyền quản lý và truy cập khóa bí mật;

đ) Thông tin mỗi khóa bí mật phải có thông tin nhật ký quản lý, cán bộ quản lý tại mỗi thời điểm.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu không được sử dụng các thuật toán, giải pháp tồn tại điểm yếu ATTT ở mức cao theo khuyến cáo, công bố của cơ quan nhà nước có thẩm quyền hoặc các tổ chức quốc tế có uy tín.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ phải được mã hóa đáp ứng yêu cầu ở trên.

5. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ phải được đồng bộ theo thời gian thực.

6. Định kỳ hàng tháng 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 HTTT.

Điều 18. Quản lý phòng chống mã độc

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động:

a) Máy tính, máy chủ và thiết bị di động phải được cập nhật phần mềm phòng chống mã độc trước khi kết nối vào hệ thống;

b) Phần mềm phòng, chống mã độc trên máy tính, máy chủ và thiết bị di động phải được thiết lập chế độ tự động cập nhật dấu hiệu mã độc từ nhà cung cấp và chế độ bảo vệ theo thời gian thực;

c) Triển khai giải pháp phòng, chống mã độc có chức năng quản lý tập trung.

2. Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng:

a) Phần mềm trước khi cài đặt trên máy tính, thiết bị di động phải kiểm tra mã độc;

b) Phần mềm trước khi cài đặt trên máy tính, thiết bị di động phải xác thực nguồn gốc từ nhà sản xuất theo mã kiểm tra tính toàn vẹn;

c) Phần mềm sau khi cài đặt phải được xử lý điểm yếu ATTT và cập nhật lên phiên bản mới nhất;

d) Hệ thống phải được trang bị giải pháp kỹ thuật để quản lý và ngăn chặn truy cập đến các trang thông tin độc hại trên mạng.

3. Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động phải thực hiện qua kênh kết nối an toàn sử dụng giao thức mã hóa, xác thực không được tồn tại điểm yếu ATTT ở mức cao theo khuyến cáo, công bố của cơ quan nhà nước có thẩm quyền hoặc các tổ chức quốc tế có uy tín.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 19. Quản lý giám sát an toàn HTTT

1. Quản lý, vận hành hoạt động của hệ thống giám sát thực hiện theo quy định tại khoản 1 Điều 16 Quy chế này.

2. Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ.

3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

4. Truy cập và quản trị hệ thống giám sát chỉ được thực hiện từ vùng mạng quản trị; trường hợp truy cập và quản trị từ mạng bên ngoài thì phải thông qua kênh kết nối VPN.

5. Loại thông tin cần được giám sát bao gồm tối thiểu các loại sau: thông tin giám sát lớp mạng, lớp máy chủ, lớp ứng dụng, cơ sở dữ liệu và thiết bị đầu cuối.

6. Lưu trữ và bảo vệ thông tin giám sát phải được lưu trữ tập trung đầy đủ các loại thông tin tại khoản 5 Điều này theo thời gian thực.

7. Toàn bộ thành phần trong hệ thống giám sát, máy chủ, thiết bị hệ thống và ứng dụng phải được đồng bộ thời gian.

8. Bộ phận giám sát thực hiện giám sát an toàn HTTT 24/7 để thực hiện theo dõi, giám sát và cảnh báo sự cố phát hiện được trên HTTT.

Điều 20. Quản lý điểm yếu ATTT

1. Quản lý thông tin các thành phần có trong HTTT có khả năng tồn tại điểm yếu ATTT: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống nếu có.

2. Quản lý, cập nhật nguồn cung cấp điểm yếu ATTT; phân nhóm và mức độ của điểm yếu cho các thành phần trong HTTT đã xác định:

a) Điểm yếu ATTT được phân nhóm theo mức độ nghiêm trọng (Critical, High, Medium, Low);

b) Khi phát hiện điểm yếu ATTT ở mức độ Critical phải xử lý trong vòng 01 (một) ngày kể từ khi phát hiện;

c) Khi phát hiện điểm yếu ATTT ở mức độ Critical phải xử lý trong vòng 02 (hai) ngày kể từ khi phát hiện;

d) Khi phát hiện điểm yếu ATTT ở mức độ Medium phải xử lý trong vòng 03 (ba) ngày kể từ khi phát hiện.

3. Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT:

a) Bên thứ ba phải có trách nhiệm hỗ trợ xử lý điểm yếu ATTT theo yêu cầu của cơ quan nhà nước;

b) Khi cần thiết cần tổ chức phối hợp xử lý điểm yếu ATTT từ các nhóm chuyên gia, tổ chức ATTTM.

4. Kiểm tra, đánh giá và xử lý điểm yếu ATTTM cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

5. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu ATTT cho toàn bộ HTTT; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu ATTT khi có thông tin hoặc nhận được cảnh báo về điểm yếu ATTT đối với thành phần cụ thể trong HTTT.

Điều 21. Quản lý sự cố ATTTM

1. Nguyên tắc ứng cứu sự cố theo quy định tại Điều 4 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

2. Cơ quan nhà nước xây dựng phương án quản lý sự cố ATTTM bao gồm các nội dung sau:

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

b) Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTTM;

c) Kế hoạch ứng phó sự cố ATTTM;

d) Giám sát, phát hiện và cảnh báo sự cố ATTT;

đ) Quy trình ứng cứu sự cố ATTTM thông thường;

e) Quy trình ứng cứu sự cố ATTTM nghiêm trọng;

g) Cơ chế phối hợp với Đội Ứng cứu sự cố ATTTM thành phố, cơ quan chức năng trong và ngoài thành phố, các nhóm chuyên gia, bên thứ ba trong việc xử lý, khắc phục sự cố ATTT.

3. Phương án Quản lý sự cố ATTT phải được ban hành cùng Quy chế bảo đảm ATTT trước khi đưa hệ thống vào vận hành, khai thác.

4. Định kỳ hàng năm tổ chức diễn tập phương án xử lý sự cố ATTT.

Điều 22. Quản lý an toàn người sử dụng đầu cuối

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

a) Người sử dụng đầu cuối phải tuân thủ các quy định của pháp luật và quy định tại Quy chế này khi truy cập, sử dụng tài nguyên nội bộ;

b) Không truy cập từ xa vào trực tiếp các máy tính trong mạng nội bộ của đơn vị. Trường hợp, người sử dụng cần truy cập từ xa thì phải truy cập gián tiếp qua giao thức mạng an toàn, có hỗ trợ mã hóa bảo mật thông tin như VPN;

c) Không được kết nối các thiết bị lưu trữ di động của tổ chức, cá nhân bên ngoài vào máy tính để bàn của đơn vị, trừ trường hợp thật sự cần thiết và đã được bộ phận chuyên trách về ATTT kiểm tra, xác nhận trước khi thực hiện.

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

a) Không truy cập trang thông tin theo đường link, mở tệp tin đính kèm từ những thư điện tử lần đầu tiên nhận được, không rõ nguồn gửi hoặc nghi ngờ có thể gây hại. Trường hợp, người sử dụng cần thiết phải truy cập hoặc mở tệp tin đính kèm thì đề nghị bộ phận chuyên trách kiểm tra ATTT trước khi truy cập hoặc mở tệp tin;

b) Không truy cập các trang thông tin không rõ nguồn gốc hoặc có nội dung độc hại;

c) Thiết bị di động của người sử dụng được kết nối vào mạng không dây công cộng của cơ quan nhà nước nhưng không kết nối thiết bị di động vào mạng ngang hàng với mạng máy tính để bàn của cán bộ, công chức. Trường hợp người sử dụng cần thiết phải kết nối vào mạng ngang hàng thì phải đề nghị bộ phận phụ trách ATTTM kiểm tra ATTT cho thiết bị di động trước khi thực hiện;

d) Thiết bị di động khi kết nối vào mạng nội bộ của cơ quan nhà nước phải được quản lý truy cập ra các vùng mạng khác của hệ thống và mạng Internet;

đ) Thiết bị di động phải được quản lý, kiểm soát truy cập thông qua việc cấp phát địa chỉ mạng theo địa chỉ vật lý (MAC).

3. Cài đặt và sử dụng máy tính an toàn:

a) Đặt mật khẩu cho các tài khoản của hệ điều hành theo quy tắc: tối thiểu 08 (tám) ký tự; bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt. Định kỳ 03 (ba) tháng thay đổi mật khẩu;

b) Khóa máy tính và các thiết bị có tính năng tương tự máy tính khi tạm thời rời khỏi vị trí làm việc. Đóng các phiên làm việc của ứng dụng khi đã hoàn tất, trừ khi đã có cơ chế bảo vệ thích hợp;

c) Không tự ý thay đổi cấu hình thiết bị đã được thiết lập, việc thay đổi phải thông báo đến bộ phận chuyên trách.

Điều 23. Quản lý thuê dịch vụ CNTT

1. Các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ CNTT theo yêu cầu riêng theo quy định tại Mục 2 Chương III Thông tư số 16/2024/TT-BTTTT ngày 30 tháng 12 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng CNTT; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ CNTT theo yêu cầu riêng.

2. Khi ký kết hợp đồng thuê dịch vụ CNTT, cơ quan, 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 ATTT. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm ATTT và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

3. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ CNTT:

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, 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 ATTT theo quy định tại Quy chế này, Luật An toàn thông tin mạng số 86/2015/QH13 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 HTTT của cơ quan, đơn vị.

4. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm ATTT:

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 HTTT 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 theo quy định.

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

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

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 cơ quan, 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 24. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ,...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát bảo đảm không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị CNTT cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, bảo đảm không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 25. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan nhà nước

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động được giao phụ trách công tác ATTT:

a) Chịu trách nhiệm bảo đảm ATTTM của cơ quan nhà nước;

b) Tham mưu lãnh đạo cơ quan nhà nước 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 nhà nước các rủi ro mất ATTTM 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 cơ quan nhà nước.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động của cơ quan nhà nước:

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

b) 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 phụ trách ATTTM của cơ quan nhà nước để kịp thời ngăn chặn và xử lý theo Mẫu số 03 Phụ lục I ban hành kèm theo Thông tư số 20/2017/TT-BTTTT; báo cáo kết thúc ứng phó sự cố theo Mẫu số 04 Phụ lục I ban hành kèm theo Thông tư số 20/2017/TT BTTTT sau khi xử lý xong;

d) Tích cực tham gia các chương trình đào tạo, hội nghị về ATTTM được thành phố tổ chức.

Điều 26. Trách nhiệm của các cơ quan nhà nước

1. Giám đốc Sở, Thủ trưởng cơ quan, ban, ngành thành phố, Chủ tịch UBND xã, phường và Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm trước Chủ tịch Ủy ban nhân dân thành phố nếu thiếu trách nhiệm trong công tác bảo đảm ATTTM, để xảy ra hậu quả, thiệt hại nghiêm trọng tại cơ quan nhà nước thuộc phạm vi quản lý.

2. Giám đốc Sở, Thủ trưởng cơ quan, ban, ngành thành phố, Chủ tịch UBND xã, phường và Thủ trưởng các cơ quan, 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 cơ quan, đơn vị mình.

3. Phân công một bộ phận hoặc cán bộ phụ trách bảo đảm ATTTM của cơ quan, đơn vị, tạo điều kiện để các cán bộ phụ trách ATTTM được học tập, nâng cao trình độ về ATTTM.

4. Xây dựng quy định, quy chế, quy trình nội bộ về bảo đảm ATTTM, ứng cứu sự cố, quy trình khai thác dữ liệu cho các phần mềm ứng dụng, cơ sở dữ liệu phù hợp với Quy chế này, các quy định của pháp luật và tình hình từng cơ quan nhà nước.

5. 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 Công an thành phố tổng hợp, cập nhật.

6. 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.

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

8. Chủ động phối hợp Công an thành phố 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 các nguy cơ về ATTTM và tấn công mạng.

9. Chủ động tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về ATTT trong công tác quản lý nhà nước tại đơn vị.

10. Báo cáo về tình hình bảo đảm ATTTM của cơ quan nhà nước khi có yêu cầu của Công an thành phố.

Điều 27. Trách nhiệm của Công an thành phố

1. Hướng dẫn triển khai, giám sát, đôn đốc, kiểm tra việc triển khai các nội dung tại Quy chế này.

2. Là cơ quan chuyên trách về ATTTM của thành phố, có trách nhiệm tham mưu UBND thành phố về công tác bảo đảm ATTTM.

3. Là cơ quan chuyên trách về ứng cứu sự cố ATTTM của thành phố, đầu mối thực hiện các nhiệm vụ về tiếp nhận và xử lý các sự cố về ATTTM, ứng cứu sự cố ATTTM trong cơ quan nhà nước thành phố Cần Thơ và có trách nhiệm thực hiện quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

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

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 các đơn vị, tổ chức 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.

7. Chủ trì, phối hợp 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 HTTT vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội, ảnh hưởng đến ATTT trong cơ quan nhà nước; xử lý các trường hợp vi phạm pháp luật về ATTT theo thẩm quyền.

8. Tham mưu UBND thành phố trong công tác kiểm tra, đánh giá việc tuân thủ các quy định trong công tác bảo đảm an toàn HTTT theo cấp độ.

9. Tổng hợp và báo cáo định kỳ về tình hình bảo đảm ATTTM trong cơ quan nhà nước gửi Bộ Công an, UBND thành phố theo quy định.

10. Hàng năm xây dựng và triển khai các chương trình đào tạo về ATTTM cho lực lượng bảo đảm ATTT của các cơ quan nhà nước. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về ATTTM trong công tác quản lý nhà nước trên địa bàn thành phố.

Điều 28. Điều khoản thi hành

1. Trong quá trình thực hiện nếu có các vấn đề phát sinh, không phù hợp hoặc chưa được quy định rõ, các đơn vị gửi kiến nghị, đề xuất về Công an thành phố để tổng hợp, báo cáo UBND thành phố kịp thời xem xét điều chỉnh, bổ sung phù hợp với tình hình thực tiễn.

2. Trường hợp các văn bản pháp luật được dẫn chiếu để áp dụng tại Quy chế này được sửa đổi, bổ sung, thay thế thì áp dụng theo các văn bản sửa đổi, bổ sung, thay thế đó.