

Phú Thái, ngày 09 tháng 9 năm 2025

QUY CHẾ

**Đảm bảo an toàn thông tin trên Hệ thống mạng và thiết bị đầu cuối
của UBND xã Phú Thái**

CHƯƠNG I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định về bảo đảm an toàn thông tin trên hệ thống mạng và thiết bị đầu cuối trong các hoạt động ứng dụng công nghệ thông tin của UBND xã Phú Thái.

2. Quy chế này áp dụng đối với:

a) Các phòng, cơ quan, đơn vị trực thuộc UBND xã; Công An xã; công chức, viên chức, người lao động của UBND xã.

b) Cơ quan, tổ chức, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng và sử dụng các thiết bị đầu cuối của UBND xã.

c) Các tổ chức, cá nhân, doanh nghiệp có tham gia quản lý, cung cấp, vận hành, khai thác, ứng dụng công nghệ thông tin trong hoạt động của các cơ quan, đơn vị trực thuộc UBND xã.

Điều 2. Giải thích từ ngữ

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

1. *Hệ thống mạng*: bao gồm dịch vụ kết nối Internet; mạng nội bộ; mạng truyền số liệu chuyên dùng.

2. *Mạng nội bộ (LAN)*: là tập hợp các trang thiết bị công nghệ thông tin được kết nối với nhau thông qua các bộ chuyển mạch, bộ định tuyến, bộ điểm truy cập và các máy chủ, thiết bị quản lý mạng, phần mềm quản lý mạng, thiết bị an toàn hệ thống mạng trong phạm vi quản lý của . Mạng nội bộ bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

3. *Phòng mạng*, bao gồm: Thiết bị chuyển mạch, thiết bị định tuyến, thiết bị lưu trữ, thiết bị bảo đảm an toàn thông tin mạng, thiết bị ngoại vi, thiết bị phụ trợ, đường truyền kết nối Internet và thiết bị phòng cháy, chữa cháy, chống sét và các thiết bị khác theo quy định đặt tại phòng mạng.

4. *Mạng truyền số liệu chuyên dùng*: là mạng của các cơ quan Đảng, Nhà nước, là hệ thống thông tin quan trọng tại các cơ quan, đơn vị, được sử dụng riêng trong hoạt động truyền số liệu và ứng dụng công nghệ thông tin của các cơ quan Đảng, Nhà nước.

5. *Trang thiết bị công nghệ thông tin cá nhân*: bao gồm máy tính để bàn, máy tính xách tay, thiết bị số (máy tính bảng, điện thoại thông minh) của cá nhân.

6. *Máy tính bảo vệ bí mật nhà nước (MTBVBMNN)*: là máy tính dùng trong hoạt động ứng dụng công nghệ thông tin chỉ được dùng để xử lý các tài liệu mật được quy định theo pháp luật về bảo vệ bí mật nhà nước.

7. *Đơn vị vận hành hệ thống thông tin*: là đơn vị chủ trì việc quản lý và vận hành kỹ thuật hệ thống thông tin.

8. *Thiết bị đầu cuối*: là một thiết bị truyền thông được cài đặt ở 2 đầu dây giúp kết nối hệ thống mạng, các thiết bị này sẽ thu và phát các tín hiệu truyền đi hay nhận lại.

Điều 3. Phạm vi bảo đảm an toàn thông tin

1. Hệ thống mạng LAN, Internet, mạng WAN và Hội nghị trực tuyến.
2. Hệ thống thông tin quản lý gồm: các phần mềm nghiệp vụ và cơ sở dữ liệu phục vụ công tác quản lý, điều hành hoạt động của UBND xã.
3. Trang thiết bị công nghệ thông tin đầu cuối của các phòng và cá nhân.
4. Máy tính bảo vệ bí mật nhà nước.

Điều 4. Nguyên tắc đảm bảo an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối

1. Đảm bảo an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Bảo đảm an toàn thông tin trên hệ thống mạng và các thiết bị phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ.

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm bảo đảm an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối đối của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin do đơn vị mình quản lý. Sử dụng phần mềm có bản quyền, thường xuyên cập nhật bản sửa lỗi phần mềm và cài phần mềm diệt Virus.

3. Cá nhân sử dụng thiết bị đầu cuối có trách nhiệm bảo đảm an toàn thông tin trên hệ thống mạng và các thiết bị trong phạm vi xử lý công việc của mình theo quy định của Nhà nước.

4. Xử lý sự cố an toàn thông tin trên hệ thống mạng và các thiết bị phải phù hợp với trách nhiệm, quyền hạn và đảm bảo lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 5. 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 an toàn thông tin mạng 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.

7. Các hành vi bị nghiêm cấm quy định tại Điều 8 Luật An ninh mạng.

CHƯƠNG II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN TRÊN HỆ THỐNG MẠNG VÀ CÁC THIẾT BỊ ĐẦU CUỐI

Điều 6. Bảo đảm an toàn thông tin trên hệ thống mạng nội bộ

1. Sử dụng thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài. Khi kết nối từ xa vào mạng nội bộ, phải sử dụng giao thức mạng có mã hóa thông tin và thiết lập mật khẩu mạnh.

2. Mạng không dây để kết nối với mạng nội bộ phải thiết lập mật khẩu mạnh, mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3. Mật khẩu truy cập phải được thay đổi định kỳ 06 tháng/lần.

3. Hệ điều hành, phần mềm tích hợp trên các thiết bị mạng phải thường xuyên được cập nhật các bản vá lỗi theo khuyến nghị của các nhà sản xuất. Phải lưu trữ nhật ký khi thay đổi cấu hình kỹ thuật của các thiết bị mạng.

4. Đảm bảo an toàn thông tin mạng nội bộ (LAN) và mạng truyền số liệu chuyên dùng. Các cơ quan, đơn vị có trách nhiệm quản lý, vận hành và sử dụng hệ thống mạng đã được lắp đặt và tổ chức triển khai thực hiện các biện pháp bảo đảm an toàn thông tin, giám sát kết nối mạng Internet của thiết bị đầu cuối; phát hiện và ngăn chặn các thiết bị lạ lắp đặt vào hệ thống thông tin, các hành vi làm hư hỏng mạng nội bộ (LAN), WAN và mạng hội nghị trực tuyến. Khi phát hiện sự cố làm hư hỏng, mất kết nối phải báo Văn phòng HĐND và UBND xã để triển khai ngay các biện pháp khắc phục, sửa chữa đảm bảo hệ thống hoạt động liên tục, thông suốt.

Điều 7. Bảo đảm an toàn thiết bị đầu cuối

1. Máy tính cá nhân phải đặt mật khẩu truy cập; thường xuyên cập nhật bản vá lỗi hỏng bảo mật hệ điều hành và phần mềm ứng dụng; cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật mẫu mã độc mới, tự động rà quét khi sao

chép, mở các tập tin. Phần mềm phòng chống mã độc phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Thông tin và Truyền thông.

2. Khi sử dụng máy tính, thiết bị đầu cuối trong mạng nội bộ cơ quan để xử lý công việc mang tính chất công vụ phải tuân thủ các quy định sau:

a) Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.

b) Cán bộ, công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin; thường xuyên thay đổi để tăng cường công tác bảo mật.

c) Không tự ý gỡ bỏ phần mềm phòng chống mã độc trên máy tính. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.

d) Chỉ sử dụng thư điện tử công vụ để trao đổi, gửi, nhận tài liệu công vụ.

e) Khi phát hiện dấu hiệu máy tính nhiễm mã độc phải kịp thời thông báo cho bộ phận có trách nhiệm của cơ quan để xử lý.

3. Cá nhân khi mang máy tính, thiết bị di động thuộc sở hữu riêng kết nối với mạng nội bộ để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan và tuân thủ các quy định tại khoản 1 và khoản 2 Điều này.

Điều 8: Máy tính bảo vệ bí mật nhà nước (MTBVBMMN) trong hoạt động ứng dụng công nghệ thông tin:

Ngoài việc phải thực hiện các Điều quy định tại Quy chế này, người sử dụng MTBVBMMN phải thực hiện các việc sau:

- Không được kết nối MTBVBMMN với các bên ngoài bằng bất kỳ hình thức nào, chỉ được kết nối trực tiếp với máy in riêng;

- MTBVBMMN phải được đặt mật khẩu và giao người quản lý theo quy định;

- MTBVBMMN chỉ cài các phần mềm theo quy định và chỉ được sử dụng để soạn thảo các tài liệu mật được giao;

- Khi MTBVBMMN bị hỏng thì báo cáo với bộ phận chuyên trách để xử lý theo quy định bảo mật;

- Cơ quan, đơn vị và cá nhân sử dụng MTBVBMMN làm mất dữ liệu, lộ lọt thông tin phải chịu trách nhiệm theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 9. Ứng cứu sự cố an toàn thông tin

1. Đơn vị chuyên trách ứng cứu sự cố an toàn thông tin

Công an xã là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của UBND xã; các cơ quan, đơn vị trực thuộc phân công bộ phận chuyên trách về ứng cứu sự cố an toàn thông tin mạng của đơn vị mình. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ và các quy định khác có liên quan.

2. Quy trình ứng cứu sự cố An toàn thông tin mạng được thực hiện theo Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông và các quy định hiện hành.

3. Diễn tập ứng cứu sự cố an toàn thông tin mạng

Công an xã chủ trì tham mưu cử cán bộ tham gia các cuộc diễn tập ứng cứu sự cố an toàn thông tin do cấp trên tổ chức hàng năm. Tổ chức tham gia diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố đã được lãnh đạo UBND xã phê duyệt.

CHƯƠNG III TỔ CHỨC THỰC HIỆN

Điều 10. Trách nhiệm của các cơ quan, đơn vị trực thuộc UBND xã

1. Văn phòng HĐND và UBND chủ trì, phối hợp với các cơ quan thực hiện tổng hợp các báo cáo theo yêu cầu của UBND xã. Chủ trì tổ chức theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Quy chế này.

1. Các cơ quan, đơn vị tổ chức triển khai các quy định bảo đảm an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối của UBND xã theo phân công tại Quy chế này. Hỗ trợ các đơn vị, cá nhân về công tác bảo đảm an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối.

2. Các cơ quan, đơn vị trực thuộc tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định tại Quy chế này và các quy định có liên quan khác; thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối do đơn vị quản lý.

Điều 11. Trách nhiệm của Cán bộ, công chức, người lao động thuộc quản lý của UBND xã

1. Thực hiện các quy định liên quan tại Quy chế này về bảo đảm an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối.

2. Tham gia đầy đủ các lớp đào tạo, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố.

3. Chịu trách nhiệm trước lãnh đạo cơ quan, đơn vị và trước pháp luật về các vi phạm làm mất an toàn thông tin trên hệ thống mạng và các thiết bị đầu cuối do không tuân thủ Quy chế này.

Điều 12. Trách nhiệm thi hành

1. Thủ trưởng các cơ quan, đơn vị trực thuộc UBND xã có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức và người lao động thực hiện các quy định của Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế; chịu trách nhiệm trước pháp luật và Lãnh đạo UBND xã về triển khai thực hiện Quy chế.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các cơ quan, đơn vị có văn bản phản ánh về UBND xã (qua Văn phòng HĐND và UBND xã,

trình Lãnh đạo UBND xã xem xét, phê duyệt sửa đổi, bổ sung Quy chế này.

Điều 13. Hiệu lực thi hành

Quy chế này có hiệu lực theo Quyết định ban hành./.

Nơi nhận:

- UBND thành phố;
- TT: Đảng ủy, HĐND xã;
- Lãnh đạo UBND xã;
- Công An xã;
- Các cơ quan, đơn vị trực thuộc UBND xã;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Phạm Tiên Nhuận