ỦY BAN NHÂN DÂN XÃ BA VÌ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1002/QĐ-UBND	*Ba Vì, ngày 17 tháng 11 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của UBND xã Ba Vì

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ BA VÌ

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

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

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

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

Căn cứ Quyết định số 2223/QĐ-UBND ngày 14/4/2023 của Ủy ban nhân dân thành phố Hà Nội về việc ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động của cơ quan nhà nước thành phố Hà Nội;

Theo đề nghị của Văn phòng HĐND&UBND xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Uỷ ban nhân dân xã Ba Vì.

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

Điều 3. Văn phòng HĐND&UBND xã, thủ trưởng các phòng, ban chuyên môn xã, cán bộ, công chức, viên chức và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thường trực Đảng uỷ xã;
- Thường trực HĐND xã;
- Chủ tịch, các Phó Chủ tịch UBND xã;
- Lưu: VT.

CHỦ TỊCH

Nguyễn Giáp Đông

ỦY BAN NHÂN DÂN XÃ BA VÌ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của UBND xã Ba Vì

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng năm 2025 của Chủ tịch Ủy ban nhân dân xã Ba Vì)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định bảo đảm an toàn thông tin mạng trong hoạt động quản lý, vận hành hệ thống thông tin tại UBND xã Ba Vì.

2. Áp dụng cho toàn bộ cán bộ, công chức, viên chức và người lao động sử dụng hệ thống Công nghệ thông tin tại UBND xã.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* (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. *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.

4. *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.

5. *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.

6. 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.

Chương II

NGUYÊN TẮC BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 3. 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 4. 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 III

BIỆN PHÁP KỸ THUẬT VÀ TỔ CHỨC

Điều 5. Biện pháp kỹ thuật

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 6. Biện pháp tổ chức

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.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 7. 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 8. 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 Văn phòng HĐND&UBND xã để tổng hợp báo cáo Chủ tịch UBND xã kịp thời xem xét điều chỉnh, bổ sung phù hợp với tình hình thực tiễn./.