QUY CHẾ

Bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng thông tin xã Đại Đồng

(Ban hành kèm theo Quyết định số 295/QĐ-UBND ngày 22/5/2026 của Uỷ ban nhân dân xã Đại Đồng)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống mạng nội bộ và các hệ thống thông tin của UBND xã Đại Đồng, bao gồm phạm vi quản lý vật lý, logic, các ứng dụng, dịch vụ và nguồn nhân lực.

2. Đối tượng áp dụng

Quy chế này áp dụng đối với tất cả các cán bộ, công chức, viên chức thuộc các phòng, ban, ngành của UBND xã Đại Đồng và các tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin của UBND xã Đại Đồng.

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: 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 bị phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Mạng: Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. 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.

4. Chủ quản hệ thống thông tin: Là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý về an toàn thông tin, cơ quan quản lý cấp trên là Ủy ban nhân dân tỉnh, Công an tỉnh Hưng Yên, Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng để tránh bị truy nhập, sử

dụng, tiết lộ, gián đoạn, sửa đổi hoặc bị phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của Hệ thống thông tin.

2. Nguyên tắc

a) Các tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc, nhiệm vụ của mình theo quy định của pháp luật, theo hướng dẫn của các cơ quan, đơn vị có thẩm quyền và thực hiện nghiêm các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (*Sau đây viết tắt là ATTT*) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống thông tin UBND xã Đại Đồng được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

Theo quy định tại Điều 7 Luật An toàn thông tin mạng, các hành vi sau đây bị nghiêm cấm, cụ thể gồm:

1. Hành vi 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.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Bộ phận chuyên trách về an toàn thông tin

- UBND xã chỉ định ít nhất 01 cán bộ là bộ phận chuyên trách chính về an toàn thông tin và 01 cán bộ dự phòng hoặc sẽ theo phân công nhiệm vụ trực tiếp của UBND xã trong trường hợp thay thế, thực hiện nhiệm vụ tiếp nhận, báo cáo, phối hợp, ứng cứu, xử lý sự cố về an toàn thông tin đối với Hệ thống thông tin UBND xã.

- Bộ phận chuyên trách về an toàn thông tin có trách nhiệm tham gia đầy đủ các hoạt động phối hợp, đào tạo, tập huấn, các chương trình công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

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

Chủ tịch Ủy ban nhân dân xã giao Văn phòng HĐND&UBND (Phòng Văn hóa - Xã hội xã) là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh thông tin cho Hệ thống thông tin UBND xã Đại Đồng; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống mạng nội bộ; phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

- Người liên hệ 1: Bà Nguyễn Thị Đào - Phó trưởng Phòng Văn hóa - Xã hội xã.

+ Số điện thoại: 0968.223.389

+ Email: ntdao.daidong@hungyen.gov.vn

- Người liên hệ 2: Ông Đỗ Mạnh Hà - Phó chánh Văn phòng HĐND &UBND xã.

+ Số điện thoại: 0966996813

+ Email: domanhha02091990@gmail.com

3. Đầu mối liên hệ, phối hợp với các cơ quan, đơn vị, tổ chức, cá nhân trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin

a) Công an tỉnh Hưng Yên

- Người liên hệ/bộ phận: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (PA05).

- Số điện thoại: 0939 184 986

b) Bộ Công an/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC).

- Người liên hệ/bộ phận: Ban Giám sát và ứng cứu sự cố

- Số điện thoại: 0593 505 999

- Email: report@vncert.vn

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: soar.soc.gov.vn

- Báo cáo sự cố qua website của Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam: vncert.vn

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Công chức được tuyển dụng vào vị trí làm về an toàn thông tin (hoặc kiêm nhiệm) có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với cán bộ quản lý và vận hành hệ thống:

+ Cán bộ quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

+ Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin, an ninh mạng cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

b) Cán bộ nghỉ việc phải có cam kết giữ bí mật thông tin liên quan đến tổ

chức sau khi nghỉ việc.

c) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

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 hệ thống thông tin

1. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

3. Bộ phận chuyên trách xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

4. Bộ phận chuyên trách xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

5. Bộ phận chuyên trách 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, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

Điều 8. Quản lý nhà cung cấp sản phẩm, dịch vụ

1. Lập và cập nhật danh sách các nhà cung cấp sản phẩm, dịch vụ định kỳ. Đơn vị vận hành xây dựng quy trình đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng sau đó đánh giá và cập nhật danh sách tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách**.**

2. Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.

Điều 9. Phát triển phần mềm thuê khoán

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán 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:

a) Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách.

b) Bộ phận chuyên trách có trách nhiệm quản lý, lưu trữ mã nguồn an toàn.

Điều 10. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

3. Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình Lãnh đạo đơn vị phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

4. Bộ phận chuyên trách phối hợp với bên triển khai hệ thống thực hiện thử nghiệm và nghiệm thu hệ thống, trước khi đưa vào vận hành, khai thác.

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

Điều 11. Quản lý tài sản Công nghệ thông tin

1. Quản lý tài sản phần cứng và phần mềm: Lập danh sách, kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ tối thiểu 02 lần/năm.

2. Xây dựng quy trình xử lý tài sản chưa được quản lý: Rà soát, xử lý tài sản phần cứng không có trong danh sách định kỳ tối thiểu 01 lần/tháng và phần mềm trái phép định kỳ tối thiểu 01 lần/quý.

3. Quản lý tài sản thông tin: Mức độ nhạy cảm của tài sản thông tin phải được phân loại thành: Công khai, Nội bộ, Hạn chế truy cập và Bí mật nhà nước. Định kỳ kiểm tra cấp độ phân quyền dữ liệu tối thiểu 01 lần/tháng.

Điều 12. Quản lý tài khoản

1. Quản lý tách biệt giữa các loại tài khoản dùng trong hệ thống thông tin (quản trị, nghiệp vụ, kỹ thuật, dịch vụ).

2. Xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý tài khoản. Định kỳ rà soát và cập nhật quy định quản lý tài khoản tối thiểu 01 lần/năm.

Điều 13. Quản lý an toàn mạng

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

a) Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn

và bảo mật. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

b) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; kiểm soát truy cập từ bên trong mạng; kết nối về hệ thống giám sát tập trung; phòng, chống xâm nhập giữa các vùng mạng; phòng, chống phần mềm độc hại trên môi trường mạng. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

c) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

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

a) Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như: USB, DVD hoặc SAN, …

b) Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; kiểm soát truy cập từ bên trong mạng; kết nối về hệ thống giám sát tập trung; phòng, chống xâm nhập giữa các vùng mạng; phòng, chống phần mềm độc hại trên môi trường mạng.

c) Xây dựng và triển khai quy trình kết nối thiết bị đầu cuối vào hệ thống quản trị. Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

d) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

4. Các thiết bị trong hệ thống cần được cấu hình tối ưu, tăng cường bảo mật, ưu tiên sử dụng thiết bị chuyên dụng trước khi đưa vào vận hành, khai thác.

Điều 14. Quản lý an toàn máy chủ, ứng dụng (khi được trang bị) và máy trạm người dùng

Quy định về quản lý an toàn máy chủ và ứng dụng như sau:

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

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

d) Có phương án cập nhật bản vá lỗi, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ tối thiểu 01 lần/tháng;

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. Người dùng không được can thiệp vào các phần mềm đã cài đặt (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận chuyên trách về công nghệ thông tin.

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

f) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ.

2. Quy định với ứng dụng

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.

3. Truy cập mạng của máy chủ

a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.

b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).

c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN.

4. Truy cập và quản trị máy chủ và ứng dụng

a) Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng nhiệm vụ được giao.

c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.

d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.

5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

a) Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

6. Các máy chủ (khi được trang bị) trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

e) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

7. Bảo đảm an toàn máy trạm

a) Chính sách xác thực: Thiết lập cơ chế xác thực riêng biệt cho từng người dùng trên máy trạm, xóa hoặc vô hiệu hóa các tài khoản không còn sử dụng hoặc tài khoản không hoạt động sau 45 ngày.

b) Quản lý mật khẩu: Thiết lập độ dài mật khẩu tối thiểu 08 ký tự (nếu có MFA) hoặc 14 ký tự (nếu không có MFA). Mật khẩu quản trị phải được thay đổi định kỳ ít nhất 01 lần/02 tháng.

c) Phân quyền tài khoản: Thực hiện tách biệt giữa tài khoản sử dụng nghiệp vụ thông thường và tài khoản có quyền cài đặt, cấu hình hệ thống (quản trị)

d) Tự động khóa phiên làm việc: Cấu hình máy tính tự động khóa màn hình hoặc đóng phiên làm việc khi không có thao tác sử dụng sau không quá 15 phút.

đ) Quản trị từ xa an toàn: Trường hợp cần truy cập máy trạm từ xa, bắt buộc phải sử dụng kênh truyền bảo mật VPN kết hợp với xác thực đa nhân tố.

e) Cứng hóa máy trạm: Loại bỏ các thành phần hệ điều hành, dịch vụ và giao thức mạng không cần thiết hoặc không an toàn để giảm thiểu bề mặt tấn công.

f) Trang bị phần mềm chuyên dụng: Cài đặt phần mềm phòng chống mã độc (Antivirus) cho toàn bộ máy trạm trong hệ thống.

g) Cập nhật và Quét tự động: Thiết lập chế độ tự động cập nhật mẫu mã độc mới nhất và thực hiện quét mã độc định kỳ cho máy tính.

h) Kiểm soát thiết bị lưu trữ ngoài: Bắt buộc thực hiện rà quét mã độc và vô hiệu hóa tính năng tự động thực thi (autorun) đối với các phương tiện lưu trữ di động như USB, thẻ nhớ, ổ cứng ngoài trước khi kết nối vào máy trạm.

i) Cập nhật bản vá: Thiết lập quy trình kiểm tra và thực hiện cập nhật bản vá cho hệ điều hành và các phần mềm ứng dụng trên máy trạm tối thiểu 01 lần/tháng.

k) Rà soát lỗ hổng: Định kỳ thực hiện rà soát, đánh giá lỗ hổng bảo mật trên máy trạm để kịp thời khắc phục các điểm yếu kỹ thuật.

l) Thiết lập ghi nhật ký: Kích hoạt chức năng ghi nhật ký các sự kiện an ninh quan trọng trên máy trạm (đăng nhập, thay đổi cấu hình, lỗi hệ thống).

m) Quản lý kết nối: có danh sách quản lý tất cả máy trạm kết nối vào mạng (bao gồm tên máy, địa chỉ MAC, IP…) và rà soát các thiết bị kết nối trái phép định kỳ 01 lần/tháng.

n) Kiến trúc mạng: Máy trạm phải được quy hoạch vào vùng mạng nội bộ riêng biệt, tách rời với vùng mạng không dây dành cho khách để đảm bảo an toàn.

Điều 15. Quản lý lỗ hổng bảo mật và Nhật ký an ninh mạng

1. Lỗ hổng bảo mật: Tiến hành rà soát và cập nhật quy trình đánh giá, xử lý lỗ hổng bảo mật tối thiểu 01 lần/ năm hoặc xử lý ngya khi có xảy ra sự thay đổi lớn.

2. Nhật ký (Log): Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 12 tháng để tránh thất thoát dữ liệu. Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/tuần.

Điều 16. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu

a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

2. Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng

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 theo định kỳ hàng tháng hoặc khi có sự thay đổi cấu hình trên hệ thống.

3. Sao lưu dự phòng và khôi phục dữ liệu

a) 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.

b) Đơn vị vận hành xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ…

Điều 17. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng: Văn phòng HĐND&UBND phối hợp với phòng Văn hóa - Xã hội xã Đại Đồng cùng các đơn vị vận hành xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

3. Kế hoạch ứng phó sự cố an toàn thông tin mạng: Văn phòng HĐND&UBND phối hợp với phòng Văn hóa - Xã hội xã Đại Đồng cùng các đơn vị vận hành xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, cụ thể:

a) Văn phòng HĐND&UBND phối hợp với phòng Văn hóa - Xã hội xã Đại Đồng cùng các đơn vị vận hành điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống.

b) Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của đơn vị khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

5. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng: Văn phòng HĐND&UBND phối hợp với phòng Văn hóa - Xã hội xã Đại Đồng cùng các đơn vị vận hành xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

6. Công chức phụ trách về Thông tin quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của lãnh đạo.

7. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

8. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của lãnh đạo.

Điều 18. Quản lý an toàn người sử dụng đầu cuối

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

a) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng

c) Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

d) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mạng quản trị hoặc nghiệp vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

đ) Thiết lập mạng công cộng cho các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống.

e) Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc.

f) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan,

đơn vị để kịp thời ngăn chặn và xử lý.

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

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 mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Người sử dụng chỉ được truy cập các tài nguyên mạng, hệ thống thông tin và dịch vụ Internet phù hợp với chức năng, nhiệm vụ được giao; không được tự ý truy cập trái phép vào các hệ thống, dịch vụ không được cấp quyền.

c) Áp dụng các biện pháp kỹ thuật để kiểm soát, giám sát và ngăn chặn truy cập tới các trang thông tin điện tử, dịch vụ Internet có nguy cơ mất an toàn thông tin, chứa mã độc hoặc nội dung không phù hợp.

d) Nghiêm cấm việc sử dụng mạng của cơ quan, đơn vị để: Truy cập, phát tán nội dung vi phạm pháp luật; phát tán thư rác, mã độc, phần mềm không rõ nguồn gốc; thực hiện các hành vi gây mất an toàn thông tin mạng hoặc ảnh hưởng đến hoạt động của cơ quan, đơn vị.

đ) Việc tải xuống, cài đặt và sử dụng phần mềm từ Internet phải được kiểm soát; chỉ được phép cài đặt các phần mềm phục vụ công việc, có nguồn gốc rõ ràng và được phê duyệt theo quy định.

e) Kết nối từ xa vào hệ thống thông tin của đơn vị phải thông qua các giải pháp bảo mật theo quy định (như VPN, xác thực đa yếu tố hoặc các biện pháp tương đương).

f) Thực hiện phân tách và kiểm soát truy cập giữa các vùng mạng (mạng nội bộ, mạng quản trị, mạng Internet, mạng khách) nhằm hạn chế nguy cơ tấn công và lây lan mã độc.

g) Hoạt động truy cập mạng và sử dụng tài nguyên Internet phải được ghi nhận, lưu trữ nhật ký để phục vụ công tác kiểm tra, giám sát và xử lý sự cố khi cần thiết.

h) Định kỳ hoặc khi cần thiết, thực hiện rà soát, đánh giá việc sử dụng mạng và tài nguyên Internet nhằm phát hiện nguy cơ, hành vi vi phạm và có biện pháp xử lý kịp thời.

i) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

Điều 19. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy chủ, máy trạm phải được trang bị phần mềm phòng chống mã độc đáp ứng yêu cầu tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

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 20. Quản lý điểm yếu an toàn thông tin

Đơn vị vận hành có trách nhiệm:

1. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Báo cáo lãnh đạo/cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

5. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

6. Định kỳ 01 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

Điều 21. Quản lý rủi ro an toàn thông tin mạng

1. Nguyên tắc chung: Việc quản lý rủi ro an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục trong suốt vòng đời của hệ thống thông tin nhằm phát hiện, kiểm soát và giảm thiểu các nguy cơ gây mất an toàn thông tin; bảo đảm rủi ro được duy trì trong ngưỡng chấp nhận được của đơn vị.

2. Nội dung quản lý rủi ro an toàn thông tin mạng

a) Xác định rủi ro:

- Xác định tài sản thông tin (dữ liệu, hệ thống, ứng dụng, hạ tầng kỹ thuật).

- Xác định các mối đe dọa, lỗ hổng, điểm yếu có thể ảnh hưởng đến tài sản thông tin.

- Xác định các kịch bản rủi ro có thể xảy ra.

b) Phân tích rủi ro:

- Phân tích khả năng xảy ra của từng kịch bản rủi ro.

- Phân tích mức độ ảnh hưởng đối với hoạt động của đơn vị khi rủi ro xảy ra.

- Xác định mức độ rủi ro dựa trên tiêu chí kết hợp giữa khả năng xảy ra và mức độ ảnh hưởng.

c) Đánh giá rủi ro

- Phân loại rủi ro theo các mức: cao, trung bình, thấp hoặc theo tiêu chí do đơn vị quy định.

- So sánh mức độ rủi ro với ngưỡng chấp nhận rủi ro của đơn vị để làm cơ sở xử lý.

d) Xử lý rủi ro

Định kỳ 06 tháng phải tiến hành đánh giá và cải thiện hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro trong đó lựa chọn và áp dụng một hoặc nhiều biện pháp xử lý rủi ro, bao gồm:

- Giảm thiểu rủi ro thông qua việc triển khai các biện pháp kỹ thuật và quản lý.

- Tránh rủi ro bằng cách thay đổi, dừng hoặc không triển khai hoạt động có rủi ro.

- Chuyển giao rủi ro thông qua thuê dịch vụ hoặc các hình thức phù hợp.

- Chấp nhận rủi ro khi rủi ro nằm trong ngưỡng chấp nhận.

- Xây dựng kế hoạch xử lý rủi ro, trong đó xác định rõ biện pháp, lộ trình, nguồn lực và trách nhiệm thực hiện.

đ) Chấp nhận rủi ro

- Việc chấp nhận rủi ro phải được xem xét, phê duyệt bởi người có thẩm quyền theo quy định của đơn vị.

- Các rủi ro được chấp nhận phải được lập thành hồ sơ, nêu rõ lý do chấp nhận và thời hạn xem xét lại.

e) Theo dõi và rà soát rủi ro

- Thực hiện theo dõi, giám sát tình trạng rủi ro định kỳ hoặc khi có thay đổi đối với hệ thống thông tin.

- Rà soát, cập nhật đánh giá rủi ro khi xuất hiện mối đe dọa mới, lỗ hổng mới hoặc thay đổi về công nghệ, quy trình.

- Đánh giá lại hiệu quả các biện pháp xử lý rủi ro đã triển khai.

f) Hồ sơ và báo cáo rủi ro

- Thiết lập và duy trì danh mục rủi ro an toàn thông tin.

- Lưu trữ đầy đủ kết quả đánh giá, xử lý, chấp nhận rủi ro.

- Thực hiện chế độ báo cáo định kỳ hoặc đột xuất về tình hình rủi ro an toàn thông tin theo quy định.

3. Hình thức thực hiện quản lý rủi ro

- Thực hiện định kỳ theo kế hoạch hằng năm hoặc theo quy định của pháp luật.

- Thực hiện đột xuất khi có yêu cầu của cấp có thẩm quyền hoặc khi phát sinh sự cố, nguy cơ mất an toàn thông tin.

4. Trách nhiệm thực hiện

- Đơn vị chuyên trách an toàn thông tin: chủ trì tổ chức đánh giá và quản lý rủi ro.

- Đơn vị vận hành, quản trị hệ thống thông tin: phối hợp cung cấp thông tin, triển khai biện pháp xử lý rủi ro.

- Lãnh đạo đơn vị: xem xét, phê duyệt việc xử lý và chấp nhận rủi ro.

- Các cá nhân, bộ phận liên quan: có trách nhiệm tuân thủ các biện pháp kiểm soát rủi ro đã được ban hành.

Điều 22. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị công nghệ thông tin 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 đảm bảo 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 công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị công nghệ thông tin: 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.

Điều 23. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

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

a) Không được soạn thảo, lưu giữ, chuyển giao, đăng tải, phát tán thông tin, tài liệu có chứa nội dung bí mật nhà nước trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu.

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

c) Phải bố trí ít nhất 01 máy vi tính độc lập riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo, lưu trữ các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 24. Bộ phận chuyên trách về an toàn thông tin

1. Giao công chức phụ trách (kiêm nhiệm) về công nghệ thông tin xã là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin. Văn phòng HĐND&UBND xã là bộ phận vận hành Hệ thống thông tin.

2. Phòng Văn hóa - Xã hội xã là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; có trách nhiệm phổ biến hướng dẫn triển khai Quy chế này và các quy định về an toàn thông tin có liên quan.

3. Văn phòng HĐND&UBND phối hợp với phòng Văn hóa - Xã hội xã tham mưu thực hiện chế độ báo cáo định kỳ theo quy định của pháp luật, báo cáo đột xuất theo yêu cầu của cấp trên.

Điều 25. Xây dựng và công bố Quy chế

Quy chế này được Văn phòng HĐND&UBND (Phòng Văn hóa - Xã hội) xã trình người đứng đầu đơn vị vận hành trước khi công bố, áp dụng.

Điều 26. Trách nhiệm của các bộ phận, tổ chức, cá nhân

1. Tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của Nhà nước đối với các cá nhân thuộc bộ phận, đơn vị mình về an toàn thông tin mạng.

2. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin mạng trong công việc của cá nhân do đơn vị quản lý.

3. Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ- CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 27. Khen thưởng và xử lý vi phạm

1. Xem xét, khen thưởng cho các cá nhân, phòng ban có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng trong quản lý, vận hành, khai thác Hệ thống thông tin.

2. Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 28. Tổ chức triển khai Quy chế

1. Quy định trong Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

2. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp của Quy chế và thực hiện rà soát, cập nhật, bổ sung.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, cán bộ, công chức phản ánh kịp thời về Phòng Văn hóa - Xã hội xã để tổng hợp báo cáo Ủy ban nhân dân xã xem xét điều chỉnh, bổ sung./.