ỦY BAN NHÂN DÂN XÃ QUANG SƠN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 253 /QĐ-UBND	*Quang Sơn, ngày 30 tháng 8 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Quang Sơn

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ QUANG SƠN

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

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ các Nghị định của Chính phủ: số 64/2007/NĐ-CP ngày 10/4/2007 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ; số 147/2024/NĐ-CP ngày 09/11/2024 về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ các Quyết định của Thủ tướng Chính phủ: số 05/2017/QĐ-TTg ngày 16/3/2017 ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; số 8/2023/QĐ-TTg ngày 05/4/2023 về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Căn cứ các Thông tư của Bộ Thông tin và Truyền thông: số 20/2017/TT-BTTTT ngày 12/9/2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; số 12/2019/TT-BTTTT ngày 05/11/2019 quy định về sửa đổi, bổ sung một số điều của Thông tư số 27/2017/ TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; số 19/2023/TT-BTTTT ngày 25/12/2023 quy định chi tiết và hướng dẫn một số điều của Quyết định số 8/2023/QĐ-TTg ngày 05 tháng 4 năm 2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Căn cứ các Quyết định của UBND tỉnh Thái Nguyên: số 10/2020/QĐ-UBND ngày 08/5/2020 về việc ban hành Nội quy bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên; số 73/2024/QĐ-UBND ngày 31/12/2024 về sửa đổi, bổ sung một số điều của Quy chế bảo đảm an toàn thông tin mạng trong hoạt động

ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên, ban hành kèm theo Quyết định số 10/2020/QĐ-UBND ngày 08/5/2020 của UBND tỉnh Thái Nguyên;

Theo đề nghị của phòng Văn hóa - Xã hội tại Tờ trình số 22/TTr-VHXH ngày 29/8/2025 Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Quang Sơn.

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Quang Sơn.

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

Điều 3. Chánh Văn phòng HĐND và UBND xã; Trưởng phòng Văn hoá - Xã hội và Thủ trưởng các đơn vị liên quan căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 3;
- Công an tỉnh;
- Thường trực Đảng uỷ xã;
- Thường trực HĐND xã;
- Chủ tịch và các PCT UBND xã;
- Các phòng, ban, ngành, đoàn thể của xã;
- Các cơ quan, đơn vị thuộc xã;
- Lưu: VT, VHXH.

CHỦ TỊCH

Trần Mạnh Tuấn

ỦY BAN NHÂN DÂN **XÃ QUANG SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ

Bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Quang Sơn

(Ban hành kèm Quyết định số 253 /QĐ-UBND ngày 30 /8/2025 của UBND xã Quang Sơn)

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 Quang Sơn, bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức;
- Các ứng dụng, dịch vụ hệ thống cung cấp;
- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

- Cán bộ, công chức, viên chức và người lao động thuộc UBND xã Quang Sơn;
- Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ tại UBND xã Quang Sơn;
- Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống mạng nội bộ.

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 mạng nội bộ 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. 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 mạng nội bộ: 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 mạng nội bộ: là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với Hệ thống mạng nội bộ.

5. Bộ phận chuyên trách: bao gồm công chức phòng Văn hóa – Xã hội được giao phụ trách mảng chuyển đổi số, công nghệ thông tin, an toàn thông tin;

công chức Văn phòng HĐND&UBND được giao quản lý hạ tầng công nghệ thông tin, văn thư - lưu trữ điện tử và các công chức khác có liên quan.

6. Sự cố an toàn thông tin mạng: là việc thông tin, Hệ thống mạng nội bộ bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

7. Rủi ro an toàn thông tin mạng: là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

8. Đánh giá rủi ro an toàn thông tin mạng: là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, Hệ thống mạng nội bộ.

9. Quản lý rủi ro an toàn thông tin mạng: là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

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 mạng nội bộ 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 Hệ thống mạng nội bộ.

2. Nguyên tắc bảo đảm an toàn thông tin

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

b) Bảo đảm an toàn thông tin 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 mạng nội bộ 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

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

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

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

- UBND xã Quang Sơn giao công chức chuyên trách chuyển đổi số, an toàn thông tin mạng, an ninh mạng 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 mạng cho Hệ thống mạng nội bộ.

- Công chức được giao nhiệm vụ 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 trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) Công an xã Quang Sơn

- Người liên hệ/bộ phận: Tổ An ninh

- Số điện thoại: 0976. 506.328

b) Công an tỉnh Thái Nguyên

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

- Số điện thoại: 0692.669.656

c) Bộ Công an/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam

- 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. 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 công chức quản lý và vận hành hệ thống:

+ Công chức 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 mạng nội bộ.

+ Công chức 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 mạng nội bộ.

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

2. Chấm dứt thay đổi công việc

a) Cán bộ, công chức, viên chức chấm dứt hoặc thay đổi công việc phải thu

hồi tài khoản 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, công chức, viên chức 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, công chức, viên chức thôi việc.

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

Điều 7. Thiết kế an toàn Hệ thống mạng nội bộ

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 mạng nội bộ 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 mạng nội bộ 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 được 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. 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:

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

- Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

Điều 9. 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

Điều 10. Quản lý an toàn mạng

1. Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

5. 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, 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.

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

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

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

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

1. Quy định với máy chủ

- Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

- Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần.

- Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

- Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.

- Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

2. Quy định với ứng dụng

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

- 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.

- 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

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

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

- 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

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

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

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

- 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

- 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.

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

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

Điều 12. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu

- 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.

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

- 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: tập tin cấu hình hệ thống, bản dự phòng hệ điều

hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

Điều 13. Quản lý sự cố an toàn thông tin

1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.

2. Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

3. Liên hệ với đầu mối ứng cứu sự cố theo thông tin đưa ra dưới đây:

a) Công an xã Quang Sơn

- Người liên hệ/bộ phận: Tổ An ninh

- Số điện thoại: 0976.506.328

b) Công an tỉnh Thái Nguyên

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

- Số điện thoại: 0692669656

c) Bộ Công an/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam

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

- Số điện thoại: 0593505999

- 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 14. Quản lý an toàn người sử dụng đầu cuối

1. 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.

2. 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.

3. 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.

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

Điều 15. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 16. 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. Quy định hủy bỏ các thông tin/dữ liệu bảo mật 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.

2. Quy định về xử lý và hủy bỏ phương tiện lưu trữ điện tử

- Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin 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.

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

3. Quy định về xử lý thông tin trên các phương tiện và thiết bị CNTT

- Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo 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 công nghệ thông tin đó.

- Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu 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).

Điều 17. 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

- 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.

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

- 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 xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 18. Xây dựng và công bố

Quy chế này được phòng Văn hóa - Xã hội xã xây dựng, trình Chủ tịch UBND xã trước khi ban hành.

Điều 19. 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 mạng nội bộ của đơn vị.

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 20. Rà soát, cập nhật, bổ sung Quy chế

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

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin./.