ỦY BAN NHÂN DÂN **XÃ SƠN NHAM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 232/QĐ-UBND	*Sơn Nham, ngày 01 tháng 8 năm 2024*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ UBND Xã Sơn Nham

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ SƠN NHAM

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

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

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

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

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông về 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 Quyết định số 03/2019/QĐ-UBND ngày 21 tháng 02 năm 2019 của UBND tỉnh Quảng Ngãi ban hành Quy định về bảo đảm an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Quảng Ngãi;

Căn cứ Quyết định số 1359/QĐ-UBND ngày 30 tháng 7 năm 2024 của UBND huyện Sơn Hà về việc Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống thông tin mạng nội bộ UBND Xã Sơn Nham;

Theo đề nghị của Công chức văn phòng thống kê Xã Sơn Nham.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ UBND Xã Sơn Nham.

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

Điều 3. Công chức Văn phòng -Thống kê; Tài chính - Kế toán; các bộ phận liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Phòng Văn hóa thông tin huyện;
- Chủ tịch, các PCT xã;
- Lưu: VT.

CHỦ TỊCH

Lê Công Nhân

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

QUY CHẾ
Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ UBND Xã Sơn Nham

(Ban hành kèm theo Quyết định số 232/QĐ-UBND ngày 01 tháng 8 năm 2024 của Chủ tịch Ủy ban nhân dân Xã Sơn Nham)

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 mạng cho Hệ thống mạng nội bộ UBND Xã Sơn Nham (sau đây gọi tắt là Hệ thống), 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

a) Cán bộ, Công chức, người lao động thuộc Ủy ban nhân dân Xã Sơn Nham;

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống;

c) 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.

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 phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin (*Quy định tại khoản 1, Điều 3 của Luật An toàn thông tin mạng năm 2015*).

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 (*Quy định tại khoản 2, Điều 3 của Luật An toàn thông tin mạng năm 2015*).

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 (*Quy định tại khoản 3, Điều 3 của Luật An toàn thông tin mạng năm 2015*).

4. *Chủ quản hệ thống thông tin*: là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin (*Quy định tại khoản 5, Điều 3 của Luật An toàn thông tin mạng năm 2015)*.

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 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 Hệ thống.

2. Nguyên tắc

a) Cơ quan, tổ chức 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 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 (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

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

ii. 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 của UBND Xã Sơn Nham 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

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

2. Các hành vi bị nghiêm cấm quy định tại Điều 4, Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi và Điều 21, Quyết định số 821/QĐ-UBND ngày 09/6/2021 của Chủ tịch UBND tỉnh Quảng Ngãi.

3. Tự ý thay đổi, gỡ bỏ các biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

Điều 5. Phối hợp với các 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:

Chủ tịch Ủy ban nhân dân Xã Sơn Nham giao Văn phòng - Thống kê:

a) Làm 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.

b) Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống.

c) 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: Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

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) UBND Xã Sơn Nham:

- Người liên hệ: Bà Nguyễn Thị Hồng Tính – Công chức Văn phòng - Thống kê, phụ trách về ATTT.

- Số điện thoại: 0977305393.

b) UBND Huyện Sơn Hà

- Người liên hệ: Lê Như Hổ - Chuyên viên Văn phòng HĐND và UBND

huyện Sơn Hà

- Số điện thoại: 0946228521.

c) Sở Thông tin và Truyền thông tỉnh Quảng Ngãi

Số điện thoại thường trực: 02553 716968

d) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố
- Số điện thoại: 0869100317
- Email: ir@vncert.vn
- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn
- Báo cáo sự cố qua website của VNCERT/CC: https://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 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, công chức 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 thông tin.

+ 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 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 cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt hoặc thay đổi công việc

a) Công chức 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) Công chức chuyên trách công nghệ thông tin của Ủy ban nhân dân Xã SƠN NHAM thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động 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 thông tin

1. 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. 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. 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. 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. 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 Chủ tịch Ủy ban nhân dân Xã Sơn Nham quyết định trước khi thực hiện thay đổi.

Điều 8. Phát triển phần mềm thuê khoán

a) 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.

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

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 Chủ tịch Ủy ban nhân dân Xã Sơn Nham 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. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần.

3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

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

Hệ thống không sử dụng máy chủ và ứng dụng cài trên máy chủ.

Điều 12. 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 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: 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) Ủy ban nhân dân Xã Sơn Nham

- Người liên hệ : Đồng chí Nguyễn Thị Hồng Tính - công chức Văn phòng - Thống kê xã, phụ trách về ATTT
- Số điện thoại: 0977305393.

b) Ủy ban nhân dân huyện Sơn Hà

- Người liên hệ: Lê Như Hổ
- Số điện thoại: 0946228521.

c) Sở Thông tin và Truyền thông tỉnh Quảng Ngãi

Số điện thoại thường trực: 02553 716968

d) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố
- Số điện thoại: 0869100317
- Email: ir@vncert.vn
- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn
- Báo cáo sự cố qua website của VNCERT/CC: https://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

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. 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 đảm bảo không để lộ lọt 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 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 BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 17. Trách nhiệm của các phòng, đơn vị thuộc Ủy ban nhân dân Xã Sơn Nham

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 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 phòng, đơn vị quản lý.

Điều 18. Trách nhiệm của cá nhân thuộc Ủy ban nhân dân Xã Sơn Nham và các tổ chức, cá nhân sử dụng hệ thống

1. Thực hiện các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

2. Chịu trách nhiệm về các vi phạm làm mất an toàn thông tin mạng do không tuân thủ Quy chế này và các quy định của pháp luật.

Điều 19. Trách nhiệm của bộ phận chuyên trách/phụ trách về an toàn thông tin

1. Phân định vai trò, trách nhiệm, cơ chế phối hợp của bộ phận chuyên trách/ phụ trách về an toàn thông tin.

2. Bộ phận chuyên trách/ phụ trách về an toàn thông tin có trách nhiệm xây dựng và tham mưu cho Lãnh đạo Ủy ban nhân dân Xã Sơn Nham tổ chức thực hiện các chính sách an toàn thông tin.

CHƯƠNG V
TỔ CHỨC THỰC HIỆN

Điều 20. Xây dựng và công bố

1. Chính sách được thông qua và công bố công khai trước khi áp dụng.

2. Tổ chức tuyên truyền, phổ biến cho toàn thể công chức, người lao động trong cơ quan để triển khai thực hiện.

Điều 21. Rà soát, cập nhật, bổ sung Quy chế

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

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.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các phòng, đơn vị phản ánh kịp thời về Văn phòng - Thống kê để tổng hợp báo cáo Lãnh đạo UBND Xã Sơn Nham xem xét, điều chỉnh, bổ sung./.
