ỦY BAN NHÂN DÂN **XÃ BA NAM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 123/QĐ-UBND	*Ba Nam , ngày 30 tháng 7 năm 2024*

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 Nam

ỦY BAN NHÂN DÂN XÃ BA NAM

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19 tháng 6 năm 2015;Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức Chính quyền địa phương số 47/2019/QH14 ngày 22/11/2019;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006; 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 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính Phủ Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về đảm bảo an toàn Hệ thống mạng nội bộ theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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 Quyết định số 03/2019/QĐ-UBND ngày 21 tháng 02 năm 2019 của UBND tỉnh Quảng Ngãi về việc ban hành Quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi;

Căn cứ Quyết định số 25/QĐ-UBND ngày 07/3/2024 của UBND huyện Ba Tơ về việc ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn huyện Ba Tơ;

Căn cứ Quyết định số 2148/QĐ-UBND, ngày 29/7/2024 của UBND huyện Ba Tơ Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ của UBND xã Ba Nam;

Theo đề nghị của công chức Văn phòng – Thống kê Xã Ba Nam.

QUYẾT ĐỊNH:

Điều 1. Ban hành Quyết định kèm theo Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của UBND Xã Ba Nam.

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

Điều 3. Công chức Văn phòng - Thống kê, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND huyện Ba Tơ;
- Phòng Văn hóa và Thông tin huyện;
- Ban chỉ đạo chuyển đổi số xã;
- Chủ tịch, các PCT UBND xã;
- Lưu: VT Thế.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ BA NAM H.BA TƠ T.QUẢNG NGÃI

Phạm Văn Đin

ỦY BAN NHÂN DÂN XÃ BA NAM	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 Nam

(Ban hành kèm theo Quyết định số 123 /QĐ-UBND ngày 30/7/2024 của Ủy ban nhân dân Xã Ba Nam)

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 nội dung về bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của UBND Xã Ba Nam quản trị, vận hành *(sau đây gọi tắt là Hệ thống mạng nội bộ)*.

2. Đối tượng áp dụng

a) Cán bộ, công chức và người lao động thuộc UBND Xã Ba Nam;

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ tại UBND Xã Ba Nam;

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 mạng lan 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. 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.

6. 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.

7. 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.

8. 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

Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an toàn thông tin mạng, an ninh mạng trong quá trình ứng dụng công nghệ thông tin, chuyển đổi số trong hoạt động của các cơ quan.

2. Nguyên tắc

Hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị phải tuân thủ theo nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 của Luật An toàn thông tin mạng và Điều 41 của Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước.

Điều 4. Những hành vi nghiêm cấm

1. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của các cơ quan, cá nhân khác trái pháp luật.

2. Tạo ra, cài đặt, phát tán phần mềm độc hại.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Nghiêm cấm tự ý lắp đặt các thiết bị phát sóng wifi vào mạng máy tính của cơ quan và lắp đặt các thiết bị tiếp sóng wifi trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của lãnh đạo cơ quan.

7. Các hành vi khác làm mất an toàn, an ninh thông tin, bí mật của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường 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; liên hệ, phối hợp trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

UBND xã giao công chức Văn phòng – Thống kê phụ trách Công nghệ thông tin 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 và liên hệ, phối hợp trong công tác hỗ trợ điều phối xử lý sự

cố an toàn thông tin với các tổ chức, cơ quan có thẩm quyền.

2. Tham dự các lớp diễn tập đảm bảo an toàn thông tin mạng; lớp đào tạo, tập huấn chuyên sâu về an toàn thông tin mạng khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng, phân công nhiệm vụ

Công chức phụ trách an toàn thông tin có trình độ, chuyên ngành về công nghệ thông tin hoặc thường xuyên được đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin.

2. Trong quá trình làm việc

- Với người sử dụng: Thường xuyên tổ chức quán triệt các quy định về ATTT nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT; tạo điều kiện cho cán bộ, công chức, người lao động tham gia các lớp bồi dưỡng, tập huấn về an toàn thông tin.

- Với cán bộ, công chức quản lý và vận hành hệ thống mạng nội bộ: Được tạo điều kiện tham gia các lớp đào tạo, bồi dưỡng, tập huấn về an toàn thông tin; thiết lập phương án 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; tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng Hệ thống mạng nội bộ.

3. Chấm dứt thay đổi công việc

a) Cán bộ, 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) 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
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 7. Những quy định bảo đảm an toàn thông tin mạng

1. Công chức phụ trách an toàn thông tin phổ biến những kiến thức cơ bản về an toàn thông tin mạng cho cá nhân trước khi tham gia sử dụng hệ thống thông tin.

2. Bố trí người phụ trách công nghệ thông tin phải thường xuyên được đào tạo, bồi dưỡng nghiệp vụ về an toàn, an ninh thông tin.

3. Xác định và ưu tiên bố trí kinh phí cần thiết cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, virus máy tính trên hệ thống máy chủ, máy trạm và các công tác khác liên quan đến việc bảo đảm an toàn, an ninh thông tin.

4. Cán bộ, công chức thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng phải được trang bị những kiến thức và được tập huấn về công tác bảo đảm an toàn thông tin mạng.

5. Nhiệm vụ quản lý, xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng theo định kỳ.

6. Hệ thống thông tin phải được triển khai chức năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký (logfile) ra vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây mất an toàn thông tin mạng; chức năng không cho người dùng truy cập một số website không phù hợp với quy định hiện hành.

7. Hệ thống mạng không dây (wireless) của trong cơ quan phải được thiết lập các tham số: tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu (password) có độ phức tạp cao (độ dài tối thiểu 8 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

8. Tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng phải được thiết lập mật khẩu; mật khẩu phải được đặt ở mức bảo mật, có độ phức tạp cao (độ dài tối thiểu 8 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số); mật khẩu phải thường xuyên thay đổi với tần suất tối thiểu 03 tháng/lần; danh sách tài khoản phải được quản lý, kiểm tra và cập nhật kịp thời; quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng đối tượng.

Điều 8. Quản lý và phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được cài đặt phần mềm phòng chống phần mềm độc hại hoặc phần mềm diệt virus có bản quyền. Các phần mềm này phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét khi sao chép, mở các tập tin.

2. Nâng cao nhận thức của cán bộ, công chức, người lao động về phòng chống phần mềm độc hại, các rủi ro do phần mềm độc hại gây ra; không tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy tính khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

3. Tất cả các máy tính của cơ quan phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

4. Các máy tính cá nhân, thiết bị điện tử trước khi kết nối vào mạng nội bộ của cơ quan phải đảm bảo đã được cài đặt chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

5. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

6. Người sử dụng không được thiết lập chia sẻ dữ liệu trên máy tính của mình cho tất cả mọi người; không được chia sẻ với phân quyền tối đa; nghiêm cấm lưu trữ dữ liệu cá nhân trên máy chủ hoặc các hệ thống lưu trữ dùng chung của cơ quan.

7. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu..., người sử dụng phải tắt máy, cách ly máy tính ra khỏi hệ thống và báo trực tiếp cho bộ phận có trách nhiệm của cơ quan để xử lý.

Điều 9. Quản lý an toàn dữ liệu

1. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

2. Các dữ liệu quan trọng của cơ quan phải được sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; bản ghi nhật ký hệ thống.

3. Định kỳ hàng năm, chỉ đạo thực hiện sao lưu dữ liệu, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra. Dữ liệu sao lưu ngoại tuyến phải được tách biệt hoàn toàn, không kết nối mạng, cô lập để phòng chống tấn công leo thang vào hệ thống lưu trữ.

Điều 10. Quản lý truy cập

1. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được giao cho một người quản lý, sử dụng và chịu trách nhiệm chính về bảo mật an toàn, an ninh thông tin truy cập tài khoản.

2. Mỗi cán bộ, công chức, người lao động chỉ được phép truy cập 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.

3. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp (không quá 05 lần) vào hệ thống. Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

4. Tất cả máy trạm, máy chủ và các hệ thống thông tin phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 12 phút không sử dụng.

5. Khi thiết lập mạng không dây trong nội bộ cơ quan, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

6. Đối với cá nhân sử dụng, khai thác các phần mềm dùng chung của tỉnh phải thay đổi mật khẩu mặc định, thiết lập mật khẩu có độ phức tạp cao; không đặt chế độ ghi nhớ mật khẩu khi sử dụng; khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong các trình duyệt.

Điều 11. Bảo vệ bí mật Nhà nước trong công tác ứng dụng công nghệ thông tin, chuyển đổi số

1. Không được sử dụng thiết bị (máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh...) có kết nối mạng để soạn thảo văn bản, lưu trữ thông tin có nội dung thuộc bí mật Nhà nước; không cung cấp tin, tài liệu và đưa thông tin bí mật Nhà nước trên mạng.

2. Không bật các thiết bị kết nối mạng trong các cuộc họp có nội dung bí mật Nhà nước.

3. Không được in, sao chụp tài liệu bí mật Nhà nước trên các thiết bị kết nối mạng.

4. Khi sửa chữa, khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật phải có sự giám sát, quản lý chặt chẽ của cán bộ, công chức có thẩm quyền.

5. Đối với các thiết bị công nghệ thông tin, viễn thông,... được sử dụng để lưu trữ và truyền thông tin bí mật Nhà nước phải được kiểm định của cơ quan chức năng trước khi đưa vào sử dụng.

6. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Các thiết bị lưu trữ không sử dụng tiếp cho công việc của cơ quan, đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng, đảm bảo không phục hồi được dữ liệu.

Điều 12. Công chức phụ trách về công nghệ thông tin

1. Được đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ đối với lĩnh vực an toàn thông tin mạng, an ninh mạng.

2. Quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật Nhà nước.

3. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của cơ quan; hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

4. Triển khai áp dụng các giải pháp tổng thể bảo đảm an toàn thông tin mạng trong toàn hệ thống; triển khai các giải pháp kỹ thuật chống virus, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin.

5. Thường xuyên cập nhật các bản vá lỗi đối với hệ thống, cập nhật các phiên bản mới đối với chương trình chống virus.

6. Cấu hình hệ thống với những chính sách bảo mật phù hợp hoạt động của hệ thống thông tin của cơ quan, đơn vị; đồng thời xác định các chức năng, cổng giao tiếp (port), giao thức (protocol) và dịch vụ (service) mạng không cần thiết để ngăn cấm hoặc hạn chế.

7. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải bảo đảm tính sẵn sàng và toàn vẹn.

8. Sử dụng công cụ hỗ trợ để kiểm tra, giám sát dữ liệu, thông tin từ bên

trong hệ thống, thông tin gửi ra bên ngoài khi cần thiết.

9. Thực hiện thu hồi và vô hiệu hóa sử dụng tất cả các tài khoản, thiết bị thẻ, eToken, sim PKI… dùng để truy cập vào hệ thống thông tin của cá nhân ngay sau khi không còn làm việc tại cơ quan.

10. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ mất an toàn thông tin mạng đối với hệ thống thông tin của cơ quan; nguyên nhân gây ra các rủi ro và nguy cơ mất an toàn thông tin bao gồm: hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét…), truy cập trái phép, virus, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ xảy ra.

Điều 13. Giải quyết và khắc phục sự cố về an toàn thông tin mạng

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho công chức phụ trách công nghệ thông tin của cơ quan khi phát hiện các sự cố gây mất an toàn thông tin, an ninh mạng trong quá trình tham gia vào hệ thống thông tin của cơ quan.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với công chức phụ trách công nghệ thông tin

a) Lập biên bản ghi nhận sự cố gây mất an toàn thông tin đối với hệ thống thông tin của cơ quan; đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có).

b) Khẩn trương triển khai các biện pháp kỹ thuật để giải quyết và khắc phục sự cố; đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho thủ trưởng cơ quan.

c) Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải báo cáo khẩn cấp bằng điện thoại cho Phòng Văn hóa – Thông tin, Trung tâm Công nghệ thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông, Công an tỉnh, Trung tâm Công nghệ thông tin và Truyền thông.

Điều 14. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Cá nhân hoặc tập thể có trách nhiệm bảo đảm an toàn thông tin mạng trong quản lý, sử dụng thiết bị công nghệ thông tin được giao.

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 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

a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng cần phải sửa chữa thì phải có biện pháp kiểm tra, giám sát quá trình sửa chữa, 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.

b) 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. 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 mật 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).

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 15. Trách nhiệm của UBND Xã Ba Nam

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 bảo đảm an toàn Hệ thống mạng nội bộ theo cấp độ.

Điều 16. Trách nhiệm của cán bộ, công chức, người lao động cơ quan

1. Trách nhiệm của Công chức Văn phòng - Thống kê phụ trách an toàn, an ninh thông tin

a) Công chức Văn phòng – Thống kê phụ trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin; tham mưu xây dựng và tổ chức triển khai thực hiện các giải pháp kỹ thuật bảo đảm an toàn thông tin cho hệ thống mạng nội bộ của cơ quan; làm nhiệm vụ vận hành, quản lý hệ thống mạng nội bộ của cơ quan.

b) Thực hiện giám sát, đánh giá, báo cáo Chủ tịch UBND các rủi ro mất an toàn, an ninh thông tin và mức độ nghiêm trọng của các rủi ro.

c) Phối hợp với cán bộ, công chức, người lao động cơ quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

d) Tuân thủ các quy định về trách nhiệm của bộ phận phụ trách an toàn thông tin và vận hành an toàn hệ thống được giao tại Quy chế này.

2. Trách nhiệm của cán bộ, công chức, người lao động cơ quan

a) Nghiên túc chấp hành các quy định, quy trình nội bộ, quy định này và các quy định của pháp luật về an toàn, an ninh thông tin. Chịu trách nhiệm đảm bảo an toàn, an ninh thông tin trong phạm vi trách nhiệm và nhiệm vụ được giao.

b) Khi tham gia vận hành mạng máy tính của cơ quan phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức, người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; khóa máy tính tạm thời khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; không sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin có nội dung "mật", "tối mật" và "tuyệt mật" lên hệ thống máy tính có kết nối mạng Internet.

c) Cán bộ, công chức, người lao động không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng (không phải hệ thống thư điện tử của tỉnh) để trao đổi thông tin liên quan đến công việc chuyên môn của cơ quan.

d) Có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẽ mật khẩu với người khác. Đặt mật khẩu với độ an toàn cao và thay đổi mật khẩu tối thiểu 03 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng. Thực hiện các biện pháp mã hóa đối với các tài khoản, mật khẩu được lưu trữ trên thiết bị. Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan để kịp thời ngăn chặn và xử lý.

đ) Tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do cơ quan hoặc các cấp tổ chức.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 17. Tổ chức thực hiện

1. Cán bộ, công chức, người lao động tại UBND xã Ba Nam có trách nhiệm thực hiện Quy chế này và các văn bản pháp luật liên quan đến công tác đảm bảo an toàn thông tin mạng; có trách nhiệm tổ chức, quản lý các thiết bị, cơ sở dữ liệu quan trọng của cơ quan.

2. Công chức Văn phòng – Thống kê phụ trách an toàn thông tin phối hợp, cung cấp thông tin và tạo điều kiện cho Đội ứng cứu sự cố an toàn thông tin mạng của huyện và các đơn vị liên quan kiểm tra, hỗ trợ ngăn chặn, xử lý, khắc phục nguy cơ, sự cố an toàn thông tin mạng kịp thời, nhanh chóng, hiệu quả; theo dõi, tổng hợp và báo cáo định kỳ theo quy định.

Trong quá trình triển khai thực hiện Quy chế, nếu có vấn đề phát sinh, vướng mắc cá nhân phản hồi về UBND thị trấn (qua Công chức Văn phòng – Thống kê) để tổng hợp, báo cáo Chủ tịch UBND xã xem xét, sửa đổi, bổ sung./.