

Số:106/QĐ-UBND

Tiên Lữ, ngày 11 tháng 11 năm 2025

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng
đối với hệ thống thông tin trên địa bàn xã Tiên Lữ**

ỦY BAN NHÂN DÂN XÃ TIÊN LŨ

Căn cứ Luật tổ chức Chính quyền địa phương ngày 16 tháng 6 năm 2025;

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 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về
đảm bảo an toàn hệ thống thông tin theo cấp độ và Nghị định số 53/2022/NĐ -
CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng;*

*Căn cứ Quyết định số 1479/QĐ -UBND ngày 22/10/2025 của Chủ tịch
UBND tỉnh Hưng Yên về việc ban hành quy chế bảo đảm an ninh mạng, an toàn
thông tin đối với hệ thống thông tin tỉnh Hưng Yên;*

Theo đề nghị của Phòng Văn hóa - Xã hội xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quy chế đảm bảo an toàn thông tin, an ninh mạng đối với hệ thống thông tin trên địa bàn xã Tiên Lữ.

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

Điều 3. Chánh Văn phòng HĐND-UBND xã; Thủ trưởng các phòng, ban, ngành, đoàn thể xã và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này. /

Nơi nhận:

- Như điều 3;
- Sở Khoa học và Công nghệ tỉnh;
- Chủ tịch, các PCT UBND xã;
- Lưu: VT.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**



Bùi Trung Kiên



CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY CHẾ

**Quy chế bảo đảm an toàn thông tin, an ninh mạng
đối với hệ thống thông tin trên địa bàn xã Tiên Lữ**
(Ban hành kèm theo Quyết định số: 106/QĐ-UBND
ngày 11 tháng 11 năm 2025 của UBND xã Tiên Lữ)

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 thông tin trên địa bàn xã Tiên Lữ.

2. Đối tượng áp dụng

Các đơn vị thuộc, trực thuộc UBND xã Tiên Lữ

Cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin của UBND xã.

Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng phục vụ hoạt động của hệ thống thông tin.

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.

2. *An ninh mạng*: Là việc bảo đảm thông tin mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *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.

4. *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.

5. *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.

6. *Đơn vị vận hành hệ thống thông tin* là cơ quan, tổ chức, được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

7. *Bộ phận chuyên trách về an toàn thông tin* là bộ phận do chủ quản hệ

thông tin thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng.

8. *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và quyền lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

9. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

10. *Ứng cứu các sự cố an toàn thông tin mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất ATTT mạng, gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, kiểm tra, xác định sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

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

Bảo đảm an ninh mạng, an toàn thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An ninh mạng, Điều 4 Luật An toàn thông tin và Điều 4 Nghị định số 85/2016/NĐ-CP.

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. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ 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, trao đổi thành phần của máy tính phục vụ công việc.

CHƯƠNG II

QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Bảo đảm an ninh mạng, an toàn thông tin khi sử dụng máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi của đơn vị phải được cài đặt hệ điều hành, phần mềm soạn thảo văn bản, phần mềm chuyên dụng để xử lý công việc và tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở được đầu tư (hoặc thuê dịch vụ) có nguồn gốc rõ ràng); không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa

có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...), phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

d) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thu điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

đ) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, !,...) và thay đổi mật khẩu tối thiểu 6 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt trên máy tính.

e) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi đơn vị.

2. Trước khi mang máy tính, thiết bị công nghệ thông tin có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc phải báo cáo và phải được lãnh đạo đơn vị đồng ý, cho phép. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ, e khoản 1 Điều này và chịu sự giám sát của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

3. Đối với thiết bị soạn thảo, lưu trữ bí mật nhà nước

a) Các đơn vị phải bố trí ít nhất một máy tính độc lập, máy in (photocopy) không kết nối và không có lịch sử 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 để soạn thảo, lưu trữ các văn bản có nội dung bí mật nhà nước.

b) Công chức, viên chức, nhân viên được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung BMNN chỉ sử dụng máy tính, thiết bị theo quy định tại điểm a của khoản này; việc lưu trữ phải được thực hiện ở các thiết bị riêng biệt, bảo đảm các yêu cầu của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

Điều 6. Quản lý trang thiết bị công nghệ thông tin, an toàn, an ninh thông tin đối với cá nhân

1. Quản lý trang thiết bị công nghệ thông tin đối với cá nhân

a) Giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.

b) Quy định việc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: Mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

c) 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 bảo đảm 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.

d) Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ 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).

đ) Các đơn vị có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

2. Quản lý an ninh mạng, an toàn thông tin đối với cá nhân

a) Mọi thông tin, tài liệu liên quan đến công vụ chỉ được truyền tải qua kênh liên lạc chính thức (Email công vụ, hệ thống phần mềm hành chính).

b) Các đơn vị phải thường xuyên tuyên truyền tổ chức quán triệt các quy định về an ninh mạng, an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an ninh mạng, an toàn thông tin của từng cá nhân trong đơn vị.

c) Cán bộ, công chức, người lao động có trách nhiệm bảo vệ mật khẩu, tài khoản truy cập, không tiết lộ hoặc chia sẻ cho người khác.

Điều 7. Xác định cấp độ và phương án bảo đảm an ninh mạng, an toàn thông tin hệ thống thông tin

1. UBND xã thực hiện xác định cấp độ an toàn thông tin đối với hệ thống mạng nội bộ, phần mềm quản lý hành chính, cơ sở dữ liệu theo hướng dẫn của Công an tỉnh.

2. Căn cứ cấp độ đã xác định, UBND xã xây dựng phương án bảo đảm an ninh mạng tương ứng, bao gồm các biện pháp kỹ thuật, tổ chức, nhân sự và tài chính.

3. Định kỳ hoặc khi có thay đổi hệ thống, phương án bảo đảm an ninh mạng phải được rà soát, cập nhật phù hợp thực tế.

Điều 8. Giám sát an ninh mạng, an toàn thông tin

1. UBND xã tổ chức giám sát thường xuyên tình trạng hệ thống mạng, thiết bị, dữ liệu; phát hiện sớm nguy cơ tấn công, xâm nhập, hoặc rò rỉ dữ liệu.

2. Hệ thống giám sát an ninh mạng được kết nối, phối hợp chia sẻ cảnh báo với phòng Văn hóa - Xã hội và Công an tỉnh, các Sở, ngành chuyên môn cấp.

3. Kết quả giám sát phải được ghi chép, báo cáo định kỳ hoặc đột xuất khi có yêu cầu của cấp trên.

Điều 9. Ứng cứu sự cố an toàn hệ thống thông tin

1. Khi phát hiện sự cố an toàn thông tin, cán bộ, công chức phải ngay lập

tức ngắt kết nối thiết bị, báo lưu hiện trạng và báo cáo lãnh đạo UBND xã.

2. UBND xã kịp thời thông báo cho cơ quan chuyên môn cấp trên để phối hợp ứng cứu, khôi phục hệ thống và điều tra nguyên nhân.

3. Sau khi khắc phục sự cố, phải tổ chức đánh giá, rút kinh nghiệm và cập nhật lại quy trình ứng cứu, phòng ngừa tái diễn.

Điều 10. Kiểm tra, đánh giá an toàn thông tin

1. Định kỳ hằng năm, UBND xã tổ chức kiểm tra, đánh giá mức độ an toàn thông tin, rà soát các lỗ hổng, nguy cơ rủi ro,

2. Kết quả kiểm tra được lập biên bản, lưu trữ và làm căn cứ để nâng cấp, hoàn thiện hệ thống.

3. Khi có yêu cầu của cơ quan chuyên môn hoặc dấu hiệu mất an toàn, UBND xã thực hiện kiểm tra đột xuất.

Điều 11. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng, an toàn thông tin

1. Cán bộ, công chức, người lao động được phổ biến, tập huấn, bồi dưỡng định kỳ kiến thức, kỹ năng bảo đảm an toàn thông tin.

2. UBND xã phối hợp với Công an tỉnh và các Sở, ngành chuyên môn cấp tỉnh tổ chức đào tạo, hướng dẫn thực hành ứng cứu sự cố, bảo mật dữ liệu.

3. Việc đào tạo, bồi dưỡng được coi là một tiêu chí đánh giá mức độ hoàn thành nhiệm vụ hàng năm của cán bộ, công chức.

Chương III TỔ CHỨC THỰC HIỆN

Điều 12. Trách nhiệm của Chủ tịch Ủy ban nhân dân xã

1. Chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh Hưng Yên về công tác bảo đảm an ninh mạng, an toàn thông tin mạng trong hoạt động của UBND xã.

2. Chỉ đạo việc xây dựng, triển khai, cập nhật và tổ chức thực hiện Quy chế này; ban hành các văn bản hướng dẫn chi tiết (nếu cần thiết) để phù hợp với thực tế hoạt động của xã; kịp thời xử lý hoặc báo cáo cấp có thẩm quyền khi xảy ra sự cố, vi phạm.

3. Quyết định các biện pháp ứng cứu, khắc phục sự cố an ninh mạng huy động nguồn lực, nhân lực và thiết bị phục vụ công tác bảo đảm an toàn thông tin mạng.

4. Phân công cụ thể cán bộ phụ trách công tác an ninh mạng, quản trị hệ thống thông tin, đồng thời chịu trách nhiệm giám sát, kiểm tra định kỳ hoặc đột xuất việc thực hiện Quy chế.

Điều 13. Trách nhiệm của Công an xã

1. Tham mưu, giúp Chủ tịch UBND, UBND xã trong công tác bảo đảm an ninh mạng, an toàn thông tin mạng; thực hiện chức năng nắm tình hình, phát hiện, phòng ngừa, đấu tranh với các hành vi vi phạm pháp luật về an ninh mạng trên địa bàn.

2. Phối hợp với Văn phòng HĐND - UBND xã trong việc tuyên truyền, hướng dẫn cán bộ, công chức, người dân nâng cao nhận thức về bảo mật thông

tin và phòng ngừa tội phạm công nghệ cao.

3. Khi xảy ra sự cố hoặc nghi vấn về hành vi tấn công, xâm nhập, phá hoại, thu thập trái phép thông tin của cơ quan, Công an xã chủ trì điều tra ban đầu, bảo vệ hiện trường dữ liệu và báo cáo cấp trên theo quy định.

3. Định kỳ hoặc đột xuất, phối hợp với các cơ quan chuyên môn kiểm tra, đánh giá mức độ an toàn hệ thống mạng của UBND xã.

Điều 14. Trách nhiệm của phòng Văn hóa - Xã hội

1. Là đầu mối giúp Chủ tịch UBND, UBND xã triển khai công tác vào đêm an ninh mạng, an toàn thông tin; tổ chức phổ biến, hướng dẫn và theo dõi việc thực hiện Quy chế này.

2. Là đầu mối để tiếp nhận điều phối ứng cứu các sự cố mất an ninh mạng, an toàn thông tin của xã.

3. Tham mưu cho UBND xã trong việc tuyên truyền, phổ biến quy định của pháp luật về an toàn thông tin, an ninh mạng đến Nhân dân và các tổ chức trên địa bàn.

4. Phối hợp với Văn phòng HĐND và UBND xã trong công tác hướng dẫn, giám sát việc đăng tải thông tin, hình ảnh, dữ liệu lên các trang thông tin điện tử, mạng xã hội chính thức của xã, bảo đảm đúng quy định, không để lộ, lọt thông tin nội bộ.

5. Theo dõi, tổng hợp tình hình vi phạm trong lĩnh vực thông tin - truyền thông; báo cáo Chủ tịch UBND xã và cơ quan chuyên môn cấp trên theo định kỳ hoặc khi có yêu cầu.

6. Tổng hợp, báo cáo định kỳ (6 tháng, 1 năm) hoặc đột xuất về tình hình an ninh mạng, an toàn thông tin mạng của UBND xã.

Điều 15. Trách nhiệm của Văn phòng HĐND và UBND xã

1. Quản lý, vận hành hệ thống mạng nội bộ, thiết bị công nghệ thông tin, phần mềm quản lý cảnh chính của xã; bảo đảm hoạt động ổn định, an toàn, tuân thủ quy trình sao lưu, bảo mật dữ liệu.

2. Thực hiện lưu trữ, bảo vệ, sao lưu định kỳ dữ liệu hành chính điện tử, hồ sơ công việc, thông tin công dân; bảo đảm không để xảy ra rò rỉ hoặc thất thoát thông tin.

3. Đầu mối phối hợp với phòng Văn hóa - Xã hội và các đơn vị chuyên môn trong việc kiểm tra, giám sát, ứng cứu sự cố an toàn thông tin.

Điều 16. Trách nhiệm của cán bộ, công chức, người lao động thuộc UBND xã

1. Thực hiện nghiêm túc các quy định về bảo đảm an ninh mạng, an toàn thông tin mạng; không thực hiện các hành vi bị cấm quy định tại Chương I của Quy chế này.

2. Có trách nhiệm quản lý, bảo vệ thiết bị được giao; giữ bí mật thông tin, mật khẩu, tài khoản; báo cáo kịp thời khi phát hiện sự cố hoặc nguy cơ mất an toàn thông tin.

3. Tham gia đầy đủ các lớp tập huấn, bồi dưỡng nghiệp vụ về an toàn, an ninh mạng; nâng cao ý thức, kỹ năng tự bảo vệ dữ liệu và thiết bị.

4. Cá nhân vi phạm Quy chế này tùy theo mức độ sẽ bị xử lý theo quy định của pháp luật về quy chế nội bộ của cơ quan.

Điều 17. Công tác phối hợp với cơ quan chuyên môn cấp trên

1. UBND xã phối hợp với Công an tỉnh và các Sở, ngành chuyên môn trong việc

- a) Hướng dẫn kỹ thuật, kiểm tra, đánh giá mức độ an toàn thông tin;
- b) Triển khai kết nối, chia sẻ dữ liệu, cảnh báo nguy cơ tấn công mạng;
- c) Ứng cứu, khắc phục sự cố mất an toàn thông tin;
- d) Đào tạo, bồi dưỡng, nâng cao năng lực cho cán bộ, công chức phụ trách CNTT.

CNTT.

2. Khi có yêu cầu từ cơ quan cấp trên, UBND xã có trách nhiệm cung cấp thông tin, báo cáo kịp thời về hiện trạng, sự cố và kết quả thực hiện công tác bảo đảm an ninh mạng.

Điều 18. Công tác kiểm tra, giám sát và báo cáo

1. UBND xã thực hiện kiểm tra, giám sát định kỳ tối thiểu 02 lần/năm đối với công tác bảo đảm an ninh mạng, an toàn thông tin.

2. Nội dung kiểm tra bao gồm: việc chấp hành các quy định trong Quy chế này; tình trạng thiết bị CNTT; quản lý tài khoản, mật khẩu; sao lưu, bảo mật dữ liệu; và việc khắc phục sau sự cố (nếu có).

3. Kết quả kiểm tra phải được lập biên bản, lưu trữ và báo cáo Chủ tịch UBND xã; đồng thời gửi cấp trên khi có yêu cầu.

4. Trường hợp phát hiện vi phạm, Chủ tịch UBND xã chỉ đạo xử lý kịp thời, khắc phục hậu quả, đồng thời rút kinh nghiệm trong toàn cơ quan.

Điều 19. Khen thưởng và xử lý vi phạm

1. Tập thể, cá nhân có thành tích trong công tác bảo đảm an ninh mạng, an toàn thông tin được biểu dương, khen thưởng theo quy định hiện hành.

2. Cán bộ, công chức, người lao động vi phạm các quy định của Quy chế này hoặc làm lộ, mất, hư hỏng dữ liệu, gây thiệt hại cho cơ quan sẽ bị xử lý theo quy định của pháp luật và quy định nội bộ của UBND xã.

3. Trường hợp vi phạm có dấu hiệu tội phạm, UBND xã chuyển hồ sơ sang cơ quan chức năng để xem xét, xử lý theo quy định của pháp luật.

Điều 20. Hiệu lực thi hành

1. Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành kèm theo Quyết định của UBND xã.

2. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, cá nhân phản ánh bằng văn bản về UBND xã (qua Công an xã) để xem xét, sửa đổi, bổ sung cho phù hợp./.