ỦY BAN NHÂN DÂN **XÃ VŨ DƯƠNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

QUY CHẾ
Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn xã Vũ Dương

(Ban hành kèm theo Quyết định số 767/QĐ-UBND ngày 31/3/2026 của UBND xã Vũ Dương)

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.

2. Đối tượng áp dụng

a) Các cơ quan, đơn vị thuộc UBND xã Vũ Dương.

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

c) 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 ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân..

2. *An toàn thông tin* 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.

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. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

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* được quy định tại Điều 5 Chương I của Thông tư 12/2022/TT-BTTTT.

7. *Hạ tầng kỹ thuật* là tập hợp thiết bị tính toán (máy chủ, máy trạm), thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng.

8. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

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. *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.

11. *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 thông tin.

12. *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.

13. *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.

14. *Giám sát an toàn hệ thống thông tin* là hoạt động lựa chọn đối tượng giám sát, thu thập, phân tích trạng thái thông tin của đối tượng giám sát nhằm xác định những nhân tố ảnh hưởng đến an toàn hệ thống thông tin; báo cáo, cảnh báo hành vi xâm phạm an toàn thông tin mạng hoặc hành vi có khả năng gây ra sự cố an toàn thông tin mạng đối với hệ thống thông tin; tiến hành phân tích yếu tố then chốt ảnh hưởng tới trạng thái an toàn thông tin mạng; đề xuất thay đổi biện pháp kỹ thuật.

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

16. *Đầu mối ứng cứu sự cố* là bộ phận hoặc cá nhân được thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia cử để thay mặt cho thành viên liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia về ứng cứu sự cố hoặc các thành viên khác trong hoạt động điều phối, ứng cứu sự cố.

17. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

18. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

Điều 3. Nguyên tắc tổ chức thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin

1. Công tác bảo đảm an ninh mạng, an toàn thông tin trong hoạt động của UBND xã được thực hiện thống nhất dưới sự chỉ đạo của UBND xã; gắn với trách nhiệm của người đứng đầu, trách nhiệm của từng bộ phận, cá nhân trong quản lý, vận hành, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu phục vụ công việc.

2. Phòng Văn hóa - Xã hội là đầu mối tham mưu UBND xã trong công tác bảo đảm an ninh mạng, an toàn thông tin; chủ trì hoặc phối hợp với Văn phòng HĐND và UBND, Phòng Kinh tế, Trung tâm Phục vụ hành chính công và các bộ phận, cá nhân có liên quan tổ chức thực hiện quy chế này theo chức năng, nhiệm vụ được giao.

3. Văn phòng HĐND và UBND, Phòng Kinh tế, Trung tâm Phục vụ hành chính công và các bộ phận, cá nhân có liên quan trong phạm vi chức năng, nhiệm vụ được giao có trách nhiệm phối hợp thực hiện các yêu cầu, biện pháp bảo đảm an ninh mạng, an toàn thông tin; quản lý, sử dụng an toàn hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu thuộc phạm vi quản lý, sử dụng.

4. Việc bảo đảm an ninh mạng, an toàn thông tin phải được thực hiện đồng bộ trong quá trình tiếp nhận, quản lý, vận hành, sử dụng, thay đổi, kết nối, chia sẻ, khai thác và xử lý thông tin, dữ liệu phục vụ hoạt động của cơ quan; bảo đảm phù hợp với chức năng, nhiệm vụ, điều kiện thực tế và quy định của pháp luật.

5. Trường hợp hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản hoặc dữ liệu có liên quan đến cơ quan, đơn vị quản lý, vận hành ở cấp trên hoặc đơn vị cung cấp dịch vụ, các bộ phận, cá nhân có liên quan của UBND xã có trách nhiệm phối hợp thực hiện theo hướng dẫn, yêu cầu và quy định của cơ quan, đơn vị có thẩm quyền.

Điều 4. Nguyên tắc bảo đảm an ninh mạng, 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 mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

Điều 5. Các hành vi bị nghiêm cấm

1. Thực hiện các hành vi bị nghiêm cấm trong lĩnh vực an ninh mạng, an toàn thông tin mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các hành vi khác bị nghiêm cấm theo quy định của pháp luật.

2. Trong phạm vi quản lý, vận hành, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, dữ liệu và môi trường mạng thuộc UBND xã, nghiêm cấm các hành vi sau đây:

a) Truy cập, xâm nhập, can thiệp, chiếm quyền, làm sai lệch, xóa, hủy hoại, sao chép, phát tán hoặc sử dụng trái phép thông tin, dữ liệu, tài khoản, phần mềm, hệ thống thông tin;

b) Cản trở, gây gián đoạn, làm ảnh hưởng trái phép đến hoạt động bình thường của hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng hoặc hoạt động mạng của cơ quan;

c) Tự ý cài đặt, gỡ bỏ, thay đổi cấu hình thiết bị, phần mềm, ứng dụng, tài khoản, kết nối mạng, thiết bị mạng, bộ phát wifi, camera, thiết bị lưu trữ hoặc thiết bị khác có khả năng kết nối mạng khi chưa được phép;

d) Tự ý kết nối thiết bị cá nhân, thiết bị không rõ nguồn gốc, thiết bị không phục vụ công việc vào hệ thống thông tin hoặc mạng nội bộ của cơ quan trái quy định;

đ) Tự ý sử dụng phần mềm không rõ nguồn gốc, phần mềm trái phép, phần mềm điều khiển từ xa hoặc các công cụ có khả năng gây mất an ninh mạng, an toàn thông tin;

e) Cho mượn, chia sẻ, tiết lộ, sử dụng chung hoặc sử dụng trái phép tài khoản, mật khẩu, thông tin xác thực;

g) Tự ý lưu trữ, sao chép, truyền nhận, chia sẻ, cung cấp, phát tán dữ liệu công vụ, dữ liệu cá nhân, tài liệu nội bộ hoặc thông tin thuộc phạm vi quản lý của cơ quan trái quy định;

h) Sử dụng tài khoản thư điện tử cá nhân, nền tảng lưu trữ cá nhân, ứng dụng nhắn tin, ứng dụng chia sẻ dữ liệu hoặc phương tiện khác không bảo đảm an toàn để xử lý, lưu trữ, truyền nhận thông tin, tài liệu phục vụ công việc trái quy định;

i) Sử dụng thiết bị, phần mềm, ứng dụng, tài khoản, dữ liệu hoặc hệ thống thông tin của cơ quan vào mục đích cá nhân trái quy định hoặc làm ảnh hưởng đến an ninh mạng, an toàn thông tin của cơ quan;

k) Cố ý che giấu, không báo cáo, báo cáo không trung thực, báo cáo chậm về dấu hiệu, nguy cơ hoặc sự cố mất an ninh mạng, an toàn thông tin;

l) Tự ý xóa dữ liệu, thay đổi hiện trạng thiết bị, tài khoản, phần mềm hoặc hệ thống khi đang có dấu hiệu bất thường, đang được kiểm tra, rà soát hoặc xử lý sự cố mà không được phép.

Điều 6. Đầu mối tham mưu, liên hệ và phối hợp thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin

1. Phòng Văn hóa - Xã hội là đầu mối tham mưu UBND xã trong công tác bảo đảm an ninh mạng, an toàn thông tin; có trách nhiệm tiếp nhận, tổng hợp, tham mưu xử lý hoặc phối hợp xử lý các nội dung liên quan đến an ninh mạng, an toàn thông tin trong phạm vi quản lý, sử dụng của UBND xã theo quy định và theo phân công.

2. Văn phòng HĐND và UBND, phòng Kinh tế, Trung tâm Phục vụ hành chính công và các bộ phận, cá nhân có liên quan có trách nhiệm phối hợp với phòng Văn hóa - Xã hội trong việc cung cấp thông tin, triển khai biện pháp bảo đảm an ninh mạng, an toàn thông tin; thực hiện kiểm tra, rà soát, khắc phục, báo cáo và các nội dung liên quan khác khi có yêu cầu.

3. Khi có yêu cầu từ cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên, đơn vị quản lý, vận hành hệ thống hoặc khi phát sinh vụ việc liên quan đến an ninh mạng, an toàn thông tin, các bộ phận, cá nhân có liên quan có trách nhiệm kịp thời phối hợp, cung cấp thông tin, hiện trạng và các điều kiện cần thiết phục vụ việc kiểm tra, xác minh, xử lý theo quy định.

4. Trường hợp cần thiết hoặc vượt quá khả năng xử lý của UBND xã, phòng Văn hóa - Xã hội chủ trì tham mưu UBND xã báo cáo, đề nghị cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên hoặc đơn vị có liên quan hướng dẫn, hỗ trợ xử lý theo quy định.

5. Việc tham mưu, liên hệ, phối hợp thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin được thực hiện theo quy định của pháp luật, quy chế này và hướng dẫn của cơ quan có thẩm quyền.

Điều 7. Bảo đảm nguồn nhân lực và nâng cao nhận thức về an ninh mạng, an toàn thông tin

1. Công chức Phòng Văn hóa – Xã hội được giao phụ trách công nghệ thông tin, an toàn thông tin là đầu mối tham mưu UBND xã trong công tác bảo đảm an ninh mạng, an toàn thông tin; có trách nhiệm chủ động nghiên cứu, cập nhật quy định, tham gia tập huấn, bồi dưỡng, hướng dẫn chuyên môn nghiệp vụ và phối hợp với cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên trong phạm vi nhiệm vụ được giao.

2. Cán bộ, công chức, viên chức, người lao động thuộc UBND xã phải được tuyên truyền, phổ biến, quán triệt hoặc hướng dẫn về an ninh mạng, an toàn thông tin phù hợp với vị trí công tác, nhiệm vụ được giao và yêu cầu sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản, dữ liệu trong quá trình thực hiện công vụ.

3. Cán bộ, công chức, viên chức, người lao động có trách nhiệm:

a) Chấp hành các quy định của pháp luật, quy chế này và các hướng dẫn có liên quan về bảo đảm an ninh mạng, an toàn thông tin;

b) Quản lý, bảo quản thiết bị, tài khoản, dữ liệu và các phương tiện phục vụ công việc được giao sử dụng; không tự ý thay đổi, tháo lắp, chuyển giao, cho mượn hoặc sử dụng trái quy định;

c) Kịp thời báo cáo người có thẩm quyền hoặc công chức Phòng Văn hóa – Xã hội được giao phụ trách công nghệ thông tin, an toàn thông tin khi phát hiện dấu hiệu mất an ninh mạng, mất an toàn thông tin hoặc nguy cơ ảnh hưởng đến hệ thống thông tin, thiết bị, phần mềm, tài khoản, dữ liệu phục vụ công việc.

4. Khi cán bộ, công chức, viên chức, người lao động nghỉ việc, chuyển công tác, thay đổi vị trí công tác hoặc chấm dứt nhiệm vụ có liên quan đến hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản hoặc dữ liệu, bộ phận và cá nhân có liên quan có trách nhiệm thực hiện việc bàn giao, thu hồi, cập nhật hoặc hủy quyền truy cập theo quy định; bảo đảm không để lộ, mất, thất thoát hoặc sử dụng trái phép thông tin, dữ liệu của cơ quan.

5. Việc tuyên truyền, phổ biến, hướng dẫn, tập huấn về an ninh mạng, an toàn thông tin được thực hiện phù hợp với điều kiện thực tế của UBND xã và theo hướng dẫn của cơ quan có thẩm quyền.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 8. Tiếp nhận, đưa vào sử dụng và thay đổi hệ thống thông tin, thiết bị công nghệ thông tin

1. Việc tiếp nhận, đưa vào sử dụng, thay đổi, nâng cấp, kết nối mới, điều chuyển hoặc ngừng sử dụng đối với hệ thống thông tin, phần mềm, thiết bị công nghệ thông tin, thiết bị mạng và các thiết bị có khả năng kết nối mạng tại UBND xã phải bảo đảm yêu cầu an ninh mạng, an toàn thông tin theo quy định của pháp luật và hướng dẫn của cơ quan có thẩm quyền.

2. Trước khi đưa vào sử dụng đối với hệ thống thông tin, phần mềm hoặc thiết bị công nghệ thông tin mới, bộ phận hoặc cá nhân được giao phụ trách có trách nhiệm kiểm tra, rà soát, bảo đảm không làm phát sinh nguy cơ mất an ninh mạng, an toàn thông tin đối với mạng nội bộ, dữ liệu và các hệ thống đang vận hành của cơ quan.

3. Đối với các hệ thống thông tin, phần mềm, cơ sở dữ liệu và nền tảng dùng chung do cơ quan cấp trên triển khai hoặc quản lý, UBND xã có trách nhiệm tiếp nhận, quản lý, khai thác, sử dụng đúng mục đích; tổ chức phổ biến, hướng dẫn người sử dụng tuân thủ yêu cầu bảo đảm an toàn thông tin và phối hợp với cơ

quan có thẩm quyền trong quá trình cài đặt, cấu hình, kiểm tra, khắc phục sự cố, thay đổi tài khoản hoặc nâng cấp hệ thống khi có yêu cầu.

4. Khi thực hiện thay đổi, nâng cấp, thay thế, điều chuyển, thanh lý hoặc ngừng sử dụng hệ thống thông tin, phần mềm, thiết bị công nghệ thông tin, bộ phận hoặc cá nhân được giao quản lý có trách nhiệm thực hiện các biện pháp cần thiết để bảo đảm an toàn thông tin, bao gồm kiểm tra dữ liệu, sao lưu cần thiết, thu hồi tài khoản, quyền truy cập, xử lý dữ liệu theo quy định và bàn giao rõ trách nhiệm quản lý, sử dụng.

5. Đối với các hệ thống thông tin do UBND xã trực tiếp đầu tư, quản lý (nếu có), việc xác định yêu cầu bảo đảm an toàn thông tin và tổ chức thực hiện các biện pháp bảo vệ được thực hiện theo quy định của pháp luật và hướng dẫn của cơ quan chuyên môn cấp trên.

Điều 9. 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 sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng thông tin điện tử, Trang thông tin điện tử.

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

c) Phải bố trí máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo 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 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, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Chương III

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

Điều 10. Quản lý an toàn mạng, thiết bị, phần mềm và tài khoản sử dụng

1. Mạng nội bộ, mạng không dây, thiết bị công nghệ thông tin, thiết bị kết nối mạng, phần mềm, ứng dụng và tài khoản sử dụng phục vụ hoạt động của

UBND xã phải được quản lý, sử dụng đúng mục đích, đúng thẩm quyền, đúng chức năng, nhiệm vụ được giao; bảo đảm yêu cầu an ninh mạng, an toàn thông tin trong quá trình khai thác, sử dụng.

2. Thiết bị công nghệ thông tin, thiết bị mạng và các thiết bị có khả năng kết nối, truyền, nhận, lưu trữ dữ liệu trong phạm vi quản lý, sử dụng của UBND xã phải được giao quản lý, sử dụng cụ thể; việc lắp đặt, kết nối, cài đặt, thay thế, sửa chữa, nâng cấp, điều chuyển, thu hồi hoặc thanh lý phải được thực hiện theo phân công hoặc theo ý kiến của người có thẩm quyền.

3. Việc quản lý, sử dụng mạng nội bộ, mạng không dây và kết nối Internet tại UBND xã phải bảo đảm các yêu cầu sau đây:

a) Sử dụng đúng mục đích công vụ, bảo đảm an toàn thông tin và hạn chế truy cập trái phép;

b) Không công khai, chia sẻ tùy tiện thông tin truy cập mạng nội bộ của cơ quan;

c) Không tự ý lắp đặt, đấu nối, mở rộng, thay đổi thiết bị mạng, thiết bị phát sóng, thiết bị truyền dẫn hoặc các thiết bị có khả năng kết nối mạng khi chưa được phép.

4. Phần mềm, ứng dụng sử dụng trong hoạt động của UBND xã phải là phần mềm hợp pháp, có nguồn gốc rõ ràng, phục vụ công việc chuyên môn hoặc được cơ quan có thẩm quyền cho phép sử dụng.

5. Tài khoản sử dụng trên các hệ thống thông tin, phần mềm, ứng dụng phục vụ công việc phải được quản lý đúng người, đúng nhiệm vụ, đúng phạm vi được phân quyền; việc cấp, thay đổi, thu hồi, khóa hoặc chấm dứt sử dụng tài khoản phải được thực hiện kịp thời khi có thay đổi về vị trí công tác, nhiệm vụ hoặc theo yêu cầu của người có thẩm quyền.

6. Cán bộ, công chức, viên chức, người lao động trong quá trình sử dụng mạng, thiết bị, phần mềm, ứng dụng và tài khoản có trách nhiệm:

a) Sử dụng đúng mục đích công vụ, đúng chức năng, nhiệm vụ được giao;

b) Bảo quản thiết bị được giao; không tự ý thay đổi cấu hình, hiện trạng kỹ thuật, mục đích sử dụng hoặc cho người khác sử dụng trái quy định;

c) Không tự ý cài đặt, gỡ bỏ, thay đổi phần mềm, ứng dụng; không sử dụng phần mềm không rõ nguồn gốc, phần mềm không phục vụ công việc hoặc có nguy cơ gây mất an toàn thông tin;

d) Không tự ý kết nối thiết bị cá nhân, thiết bị không rõ nguồn gốc hoặc thiết bị không phục vụ công việc vào mạng nội bộ, thiết bị công nghệ thông tin của cơ quan; không tự ý thiết lập chia sẻ dữ liệu, chia sẻ thiết bị, truy cập từ xa hoặc các hình thức kết nối trái phép khác;

đ) Bảo vệ thông tin đăng nhập; không tiết lộ, chia sẻ tài khoản, mật khẩu hoặc thông tin xác thực; không sử dụng tài khoản của người khác hoặc để người khác sử dụng trái phép tài khoản của mình;

e) Kịp thời báo cáo người có thẩm quyền hoặc bộ phận, cá nhân được giao phụ trách công nghệ thông tin khi phát hiện dấu hiệu bất thường liên quan đến mạng, thiết bị, phần mềm, ứng dụng hoặc tài khoản sử dụng.

7. Khi phát hiện hoặc nghi ngờ có dấu hiệu mất an ninh mạng, mất an toàn thông tin liên quan đến mạng, thiết bị, phần mềm, ứng dụng hoặc tài khoản sử dụng, cá nhân sử dụng có trách nhiệm báo cáo ngay cho người có thẩm quyền hoặc bộ phận, cá nhân được giao phụ trách công nghệ thông tin để kiểm tra, xử lý theo quy định; không được tự ý thay đổi cấu hình, khôi phục cài đặt, xóa dữ liệu hoặc thực hiện các biện pháp xử lý khác khi chưa được phép hoặc chưa có hướng dẫn của người có trách nhiệm.

8. Công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin là đầu mối tham mưu UBND xã trong việc quản lý, theo dõi, hướng dẫn sử dụng mạng, thiết bị công nghệ thông tin, phần mềm, ứng dụng và tài khoản sử dụng; phối hợp với các bộ phận, cá nhân có liên quan trong việc kiểm tra, rà soát, tiếp nhận, thay đổi, thu hồi hoặc xử lý các vấn đề phát sinh theo phân công hoặc theo yêu cầu của người có thẩm quyền.

9. Đối với các hệ thống thông tin, phần mềm, ứng dụng, tài khoản và hạ tầng kỹ thuật dùng chung do cơ quan cấp trên quản lý, UBND xã và các cá nhân sử dụng có trách nhiệm thực hiện đúng quy chế quản lý, vận hành, hướng dẫn sử dụng và yêu cầu bảo đảm an toàn thông tin của cơ quan có thẩm quyền; phối hợp thực hiện trong phạm vi trách nhiệm được giao.

Điều 11. Quản lý an toàn dữ liệu

1. Dữ liệu, thông tin phục vụ hoạt động của UBND xã phải được quản lý, lưu trữ, khai thác, sử dụng, chia sẻ và bảo vệ an toàn theo quy định của pháp luật; bảo đảm tính đầy đủ, chính xác, toàn vẹn, bí mật và khả năng khai thác, sử dụng phục vụ công việc.

2. Dữ liệu, thông tin thuộc phạm vi quản lý của UBND xã phải được quản lý theo đúng chức năng, nhiệm vụ; chỉ cơ quan, bộ phận, cá nhân được giao nhiệm vụ mới được tiếp cận, khai thác, sử dụng, xử lý trong phạm vi được phân công, phân quyền.

3. Việc khai thác, sử dụng, trao đổi, cung cấp, chia sẻ dữ liệu, thông tin trong nội bộ cơ quan và với cơ quan, tổ chức, cá nhân khác phải đúng mục đích, đúng thẩm quyền, đúng quy định; bảo đảm an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước và bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

4. Dữ liệu, thông tin công vụ, dữ liệu cá nhân, hồ sơ điện tử, tài liệu nội bộ và các dữ liệu khác thuộc phạm vi quản lý của UBND xã phải được lưu trữ, quản lý, sử dụng đúng quy định; bảo đảm không để lộ, mất, thất thoát, bị khai thác, sử dụng trái phép hoặc sử dụng sai mục đích.

5. Dữ liệu, thông tin quan trọng phục vụ công việc, dữ liệu nghiệp vụ, hồ sơ điện tử và các dữ liệu cần thiết khác phải được sao lưu, lưu trữ, bảo quản phù hợp để phục vụ khai thác, sử dụng và khôi phục khi cần thiết. Việc sao lưu, lưu trữ, phục hồi dữ liệu được thực hiện theo phân công hoặc theo hướng dẫn của bộ phận, cá nhân được giao phụ trách công nghệ thông tin.

6. Khi thay đổi, điều chuyển, sửa chữa, thu hồi, thanh lý hoặc ngừng sử dụng thiết bị công nghệ thông tin có chứa dữ liệu, bộ phận hoặc cá nhân được giao quản lý, sử dụng có trách nhiệm kiểm tra, sao lưu cần thiết, bàn giao, thu hồi và xử lý dữ liệu theo quy định, bảo đảm không để lộ, mất, thất thoát hoặc bị khai thác trái phép.

7. Cán bộ, công chức, viên chức, người lao động trong quá trình xử lý dữ liệu, thông tin có trách nhiệm bảo đảm an toàn thông tin; kịp thời báo cáo người có thẩm quyền hoặc bộ phận, cá nhân được giao phụ trách công nghệ thông tin khi phát hiện dữ liệu có dấu hiệu bị mất, bị lộ, bị sửa đổi, bị xóa trái phép hoặc có nguy cơ mất an toàn thông tin.

8. Việc kết nối, chia sẻ dữ liệu số với cơ quan nhà nước khác được thực hiện theo quy định của pháp luật về quản lý, kết nối, chia sẻ dữ liệu số của cơ quan nhà nước và các quy định pháp luật có liên quan.

Điều 12. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 13. Quản lý phòng, chống phần mềm độc hại

1. Thiết bị công nghệ thông tin phục vụ hoạt động của UBND xã phải được áp dụng biện pháp phòng, chống phần mềm độc hại phù hợp theo quy định và điều kiện thực tế sử dụng; ưu tiên sử dụng phần mềm phòng, chống mã độc hợp

pháp, được cập nhật và quản lý theo phân công hoặc theo hướng dẫn của cơ quan có thẩm quyền.

2. Cán bộ, công chức, viên chức, người lao động trong quá trình sử dụng thiết bị công nghệ thông tin có trách nhiệm thực hiện các biện pháp phòng, chống phần mềm độc hại; không mở, cài đặt, sao chép, tải xuống hoặc sử dụng các tập tin, phần mềm, ứng dụng, đường dẫn, thư điện tử, thiết bị lưu trữ hoặc nội dung điện tử có nguồn gốc không rõ ràng hoặc có nguy cơ gây mất an toàn thông tin.

3. Tập tin, tài liệu, phần mềm, ứng dụng và dữ liệu trước khi đưa vào sử dụng trên thiết bị công nghệ thông tin phục vụ công việc phải được kiểm tra, rà soát phù hợp để hạn chế nguy cơ lây nhiễm phần mềm độc hại.

4. Cán bộ, công chức, viên chức, người lao động phải được tuyên truyền, hướng dẫn về nguy cơ, dấu hiệu nhận biết và biện pháp phòng, chống phần mềm độc hại trong quá trình sử dụng thiết bị, phần mềm, ứng dụng và thư điện tử phục vụ công việc.

5. Khi phát hiện hoặc nghi ngờ thiết bị, tài khoản, tập tin, phần mềm, ứng dụng hoặc dữ liệu có dấu hiệu bị nhiễm phần mềm độc hại, cá nhân sử dụng có trách nhiệm báo cáo ngay cho người có thẩm quyền hoặc bộ phận, cá nhân được giao phụ trách công nghệ thông tin để kiểm tra, xử lý theo quy định; không được tự ý tiếp tục sử dụng, phát tán, sao chép hoặc thực hiện các thao tác có thể làm lây lan, che giấu hoặc làm phức tạp tình trạng mất an toàn thông tin.

6. Việc kiểm tra, rà soát, xử lý nguy cơ hoặc dấu hiệu phần mềm độc hại được thực hiện theo quy định của pháp luật, quy chế này và hướng dẫn của cơ quan có thẩm quyền.

Điều 14. Theo dõi, tiếp nhận cảnh báo và rà soát nguy cơ mất an toàn thông tin

1. UBND xã tổ chức theo dõi, tiếp nhận thông tin, cảnh báo và yêu cầu kiểm tra, rà soát liên quan đến an ninh mạng, an toàn thông tin trong quá trình quản lý, vận hành, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, dữ liệu và môi trường mạng thuộc phạm vi quản lý, sử dụng của cơ quan.

2. Công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin là đầu mối tiếp nhận, tổng hợp thông tin, cảnh báo, yêu cầu kiểm tra, rà soát về an ninh mạng, an toàn thông tin; tham mưu lãnh đạo UBND xã tổ chức thực hiện hoặc phối hợp thực hiện theo quy định.

3. Khi nhận được cảnh báo, thông báo hoặc yêu cầu kiểm tra, rà soát từ cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên, đơn vị quản lý, vận hành hệ thống hoặc khi phát hiện dấu hiệu bất thường trong quá trình sử dụng, các bộ

phận, cá nhân có liên quan có trách nhiệm phối hợp kiểm tra, rà soát, khắc phục theo yêu cầu và hướng dẫn của người có thẩm quyền.

4. Các bộ phận, cá nhân được giao quản lý, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, dữ liệu và tài khoản có trách nhiệm cung cấp thông tin, hiện trạng và các nội dung cần thiết khác phục vụ việc kiểm tra, rà soát, xác minh khi có yêu cầu.

5. Trong quá trình kiểm tra, rà soát, các bộ phận, cá nhân có liên quan có trách nhiệm chấp hành yêu cầu của người có thẩm quyền; không được tự ý thay đổi hiện trạng thiết bị, tài khoản, phần mềm, dữ liệu hoặc hệ thống khi chưa được phép, trừ trường hợp cần thiết để bảo đảm an toàn thông tin theo chỉ đạo hoặc hướng dẫn của cơ quan có thẩm quyền.

6. Việc theo dõi, tiếp nhận cảnh báo và rà soát nguy cơ mất an toàn thông tin được thực hiện theo quy định của pháp luật, quy chế này và hướng dẫn của cơ quan có thẩm quyền.

Điều 15. Rà soát, khắc phục nguy cơ mất an toàn thông tin

1. UBND xã tổ chức thực hiện việc kiểm tra, rà soát, khắc phục các nguy cơ mất an ninh mạng, an toàn thông tin trong phạm vi quản lý, sử dụng của cơ quan theo quy định của pháp luật, quy chế này và hướng dẫn của cơ quan có thẩm quyền.

2. Công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin là đầu mối tham mưu lãnh đạo UBND xã trong việc theo dõi, tổng hợp, đôn đốc việc kiểm tra, rà soát, cập nhật, khắc phục các nguy cơ mất an toàn thông tin đối với hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu thuộc phạm vi quản lý, sử dụng của cơ quan.

3. Khi nhận được cảnh báo, thông báo hoặc yêu cầu kiểm tra, khắc phục từ cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên, đơn vị quản lý, vận hành hệ thống hoặc khi phát hiện dấu hiệu bất thường trong quá trình sử dụng, các bộ phận, cá nhân có liên quan có trách nhiệm phối hợp kiểm tra, rà soát, cập nhật, khắc phục theo hướng dẫn và yêu cầu của người có thẩm quyền.

4. Các bộ phận, cá nhân được giao quản lý, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu có trách nhiệm thực hiện các biện pháp khắc phục cần thiết trong phạm vi được giao; cập nhật phần mềm, ứng dụng, bản vá bảo mật, thay đổi thông tin xác thực hoặc thực hiện các yêu cầu kỹ thuật khác theo hướng dẫn của cơ quan có thẩm quyền hoặc người có trách nhiệm.

5. Trường hợp phát hiện nguy cơ mất an toàn thông tin có khả năng ảnh hưởng nghiêm trọng đến hoạt động của cơ quan, dữ liệu, tài khoản hoặc hệ thống

thông tin đang sử dụng, cá nhân phát hiện hoặc bộ phận liên quan phải kịp thời báo cáo lãnh đạo UBND xã và đầu mối phụ trách công nghệ thông tin, an toàn thông tin để tổ chức xử lý hoặc phối hợp xử lý theo quy định.

6. Đối với các hệ thống thông tin, phần mềm, ứng dụng, tài khoản và hạ tầng kỹ thuật dùng chung do cơ quan cấp trên quản lý, việc rà soát, khắc phục nguy cơ mất an toàn thông tin được thực hiện theo hướng dẫn, yêu cầu của cơ quan có thẩm quyền; UBND xã có trách nhiệm phối hợp thực hiện trong phạm vi được giao.

Điều 16. Quản lý sự cố an toàn thông tin

1. Sự cố an toàn thông tin là sự việc phát sinh trong quá trình quản lý, vận hành, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản, dữ liệu hoặc hoạt động mạng của UBND xã có dấu hiệu gây mất an ninh mạng, mất an toàn thông tin hoặc có nguy cơ ảnh hưởng đến hoạt động bình thường của cơ quan.

2. Cán bộ, công chức, viên chức, người lao động khi phát hiện hoặc nghi ngờ xảy ra sự cố an toàn thông tin có trách nhiệm báo cáo ngay cho người đứng đầu bộ phận, người quản lý trực tiếp và công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin để kịp thời kiểm tra, tham mưu, xử lý theo quy định.

3. Khi phát hiện sự cố an toàn thông tin, cá nhân sử dụng thiết bị, tài khoản, phần mềm, dữ liệu hoặc hệ thống có liên quan không được tự ý xử lý vượt quá thẩm quyền; không được tự ý xóa dữ liệu, khôi phục cài đặt, cài đặt lại thiết bị, thay đổi cấu hình hệ thống, tài khoản hoặc thực hiện các hành vi khác có thể làm mất dấu vết, ảnh hưởng đến việc kiểm tra, xác minh và xử lý sự cố.

4. Công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin có trách nhiệm tiếp nhận thông tin ban đầu về sự cố; kiểm tra, xác định sơ bộ tình trạng, phạm vi ảnh hưởng; tham mưu lãnh đạo UBND xã xem xét, chỉ đạo thực hiện các biện pháp xử lý ban đầu trong phạm vi được giao, bao gồm:

a) Cô lập thiết bị, tài khoản, hệ thống hoặc kết nối có liên quan khi cần thiết để hạn chế lây lan, phát sinh thiệt hại;

b) Bảo vệ dữ liệu, thiết bị, tài khoản, nhật ký sử dụng và các thông tin liên quan phục vụ việc kiểm tra, xác minh, xử lý sự cố;

c) Phối hợp với bộ phận, cá nhân có liên quan để khắc phục bước đầu, bảo đảm duy trì hoạt động cần thiết của cơ quan.

5. Đối với các sự cố có nguy cơ ảnh hưởng nghiêm trọng đến hoạt động của cơ quan, có dấu hiệu bị tấn công mạng, lộ lọt dữ liệu, mất quyền kiểm soát tài khoản, hệ thống hoặc vượt quá khả năng xử lý của UBND xã, UBND xã có trách

nhiệm kịp thời báo cáo, phối hợp với cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên hoặc đơn vị quản lý, vận hành hệ thống để được hướng dẫn, hỗ trợ xử lý theo quy định.

6. Người đứng đầu bộ phận, cá nhân được giao quản lý, sử dụng hệ thống thông tin, thiết bị, dữ liệu hoặc tài khoản có liên quan đến sự cố có trách nhiệm phối hợp cung cấp đầy đủ, kịp thời thông tin, hiện trạng, dữ liệu và các điều kiện cần thiết phục vụ việc kiểm tra, xác minh, xử lý sự cố theo yêu cầu của người có thẩm quyền.

7. Sau khi sự cố được xử lý, công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin có trách nhiệm phối hợp với các bộ phận, cá nhân có liên quan kiểm tra, đánh giá nguyên nhân, mức độ ảnh hưởng và khả năng khôi phục; tham mưu lãnh đạo UBND xã biện pháp phòng ngừa, chấn chỉnh trách nhiệm và thực hiện báo cáo theo quy định.

8. Việc báo cáo, phối hợp xử lý và khắc phục sự cố an toàn thông tin được thực hiện theo quy định của pháp luật, quy chế này và hướng dẫn của cơ quan có thẩm quyền.

Chương IV
KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 17. Nội dung, hình thức kiểm tra, rà soát

1. Việc kiểm tra, rà soát về an ninh mạng, an toàn thông tin được thực hiện nhằm đánh giá tình hình chấp hành quy chế này, phát hiện nguy cơ mất an toàn thông tin và kịp thời chấn chỉnh, khắc phục trong phạm vi quản lý, sử dụng của UBND xã.

2. Nội dung kiểm tra, rà soát bao gồm:

a) Việc chấp hành các quy định của pháp luật và quy chế này về bảo đảm an ninh mạng, an toàn thông tin trong quản lý, vận hành, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu;

b) Tình trạng quản lý, sử dụng mạng, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu phục vụ công việc;

c) Việc thực hiện các yêu cầu, hướng dẫn, cảnh báo, biện pháp khắc phục nguy cơ mất an toàn thông tin hoặc yêu cầu phối hợp xử lý của cơ quan có thẩm quyền;

d) Các nội dung khác theo yêu cầu của người có thẩm quyền hoặc theo quy định của pháp luật.

3. Việc kiểm tra, rà soát được thực hiện theo hình thức định kỳ hoặc đột xuất theo kế hoạch, yêu cầu, chỉ đạo của UBND xã hoặc cơ quan có thẩm quyền.

4. Công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin là đầu mối tham mưu, phối hợp tổ chức thực hiện việc kiểm tra, rà soát trong phạm vi quản lý, sử dụng của UBND xã theo phân công hoặc theo yêu cầu của người có thẩm quyền.

5. Các bộ phận, cá nhân được giao quản lý, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, phần mềm, ứng dụng, tài khoản và dữ liệu có trách nhiệm phối hợp, cung cấp thông tin, hiện trạng và thực hiện các yêu cầu phục vụ việc kiểm tra, rà soát theo quy định.

6. Việc kiểm tra, rà soát được thực hiện bảo đảm không làm ảnh hưởng trái quy định đến hoạt động bình thường của cơ quan; trường hợp phát hiện nguy cơ, dấu hiệu mất an toàn thông tin hoặc vi phạm quy định thì phải kịp thời báo cáo, xử lý hoặc kiến nghị xử lý theo thẩm quyền.

Điều 18. Xử lý kết quả kiểm tra, rà soát về an ninh mạng, an toàn thông tin

1. Kết quả kiểm tra, rà soát về an ninh mạng, an toàn thông tin là căn cứ để UBND xã xem xét, chỉ đạo chấn chỉnh, khắc phục thiếu sót, nguy cơ mất an toàn thông tin và xử lý trách nhiệm đối với các bộ phận, cá nhân có liên quan theo quy định.

2. Trường hợp qua kiểm tra, rà soát phát hiện tồn tại, thiếu sót, vi phạm hoặc nguy cơ mất an toàn thông tin, các bộ phận, cá nhân có liên quan có trách nhiệm thực hiện biện pháp khắc phục, chấn chỉnh theo yêu cầu của người có thẩm quyền trong thời hạn được giao.

3. Công chức hoặc cá nhân được giao phụ trách công nghệ thông tin, an toàn thông tin có trách nhiệm theo dõi, đôn đốc, tổng hợp tình hình thực hiện các nội dung khắc phục, chấn chỉnh sau kiểm tra, rà soát; tham mưu lãnh đạo UBND xã xem xét, chỉ đạo đối với các trường hợp chậm thực hiện, không thực hiện hoặc thực hiện không đầy đủ.

4. Trường hợp qua kiểm tra, rà soát phát hiện dấu hiệu sự cố an toàn thông tin, nguy cơ ảnh hưởng nghiêm trọng đến hoạt động của cơ quan hoặc nội dung vượt quá khả năng xử lý của UBND xã thì phải kịp thời báo cáo lãnh đạo UBND xã để xem xét, chỉ đạo báo cáo, phối hợp với cơ quan có thẩm quyền, cơ quan chuyên môn cấp trên hoặc đơn vị có liên quan theo quy định.

5. Kết quả kiểm tra, rà soát và việc thực hiện khắc phục, chấn chỉnh là một trong các căn cứ phục vụ công tác quản lý, đánh giá việc chấp hành quy định về an ninh mạng, an toàn thông tin trong phạm vi UBND xã.

Chương V
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 19. Chế độ báo cáo

Các phòng chuyên môn, Trung tâm phục vụ hành chính công báo cáo tình hình an ninh mạng, an toàn thông tin định kỳ 06 tháng (trước ngày 02/6) và báo cáo năm (trước ngày 02/11) hằng năm cho UBND xã (qua phòng Văn hóa – Xã hội) như sau:

1. Báo cáo năm

a) Nội dung báo cáo:

- Việc thực hiện bảo đảm an ninh mạng, an toàn thông tin theo quy định tại Quy chế này;

- Các nội dung chỉnh sửa, bổ sung quy chế bảo đảm an ninh mạng, an toàn thông tin của đơn vị (nếu có).

b) Thời hạn gửi báo cáo: trước ngày 02 tháng 11.

2. Báo cáo đột xuất

a) Các sự cố mất an ninh mạng, an toàn thông tin:

- Thời hạn gửi báo cáo: trong thời gian 24 giờ kể từ thời điểm vụ, việc được phát hiện;

- Nội dung vụ, việc;

- Thời gian, địa điểm phát sinh vụ, việc;

- Nguyên nhân xảy ra vụ, việc (nếu có);

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống thông tin và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan;

- Các biện pháp đơn vị đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro;

- Kiến nghị, đề xuất (nếu có).

b) Các trường hợp đột xuất khác theo yêu cầu của UBND xã.

3. Định kỳ 06 tháng và hàng năm Phòng Văn hóa – Xã hội có trách nhiệm tổng hợp báo cáo tình hình an ninh mạng, an toàn thông tin (trước ngày 05/6 và trước ngày 05/11 hàng năm) về UBND tỉnh (qua Công an tỉnh).

- Phòng Văn hóa – Xã hội căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an ninh mạng, an toàn thông tin của các phòng chuyên môn, Trung tâm Phục vụ hành chính công đề xuất UBND xã xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an ninh mạng, an toàn thông tin theo quy định hiện hành.

4. 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. Chia sẻ thông tin

Việc chia sẻ dữ liệu số của các hệ thống thông tin với các cơ quan nhà nước được thực hiện theo quy định tại Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về việc quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước.

Chương VI

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 21. Đơn vị chủ quản hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ định đơn vị vận hành, đơn vị/Bộ phận chuyên trách về an toàn thông tin của đơn vị mình.

Điều 22. Đơn vị vận hành

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo các đơn vị thuộc, trực thuộc thực hiện quản lý ứng dụng; quản lý dữ liệu và các đơn vị có liên quan vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật, triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

3. Lập hồ sơ đề xuất cấp độ, gửi về Đơn vị hoặc Bộ phận chuyên trách về ATTT của chủ quản hệ thống thông tin thẩm định (theo quy định tại Nghị định 15/2016/NĐ- CP).

Điều 23. Trách nhiệm của Đơn vị/Bộ phận chuyên trách về ATTT

Thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng theo các quy định tại Quy chế này tại UBND xã và hướng dẫn các đơn vị thuộc, trực thuộc UBND xã triển khai đảm bảo an toàn, an ninh mạng trong hoạt động ứng dụng CNTT tại đơn vị mình.

Điều 24. Trách nhiệm của đơn vị cung cấp dịch vụ

1. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; thiết kế, thiết lập hệ thống đáp ứng các yêu cầu kỹ thuật các cấp độ theo tiêu chuẩn quy định.

2. Quản lý, vận hành, bảo đảm an toàn thông tin cho các thành phần hệ thống thuộcphạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

3. Lập hồ sơ cấp độ của hệ thống thông tin, gửi về đơn vị vận hành hệ thống để chuyển đến đơn vị, các cấp có thẩm quyền để thẩm định, phê duyệt hệ thống.

Điều 25. Trách nhiệm của đơn vị, tổ chức, cá nhân sử dụng hệ thống

Sử dụng hệ thống thông tin đảm bảo an toàn thông tin theo Quy chế này.

Điều 26. Bảo đảm an ninh mạng

Thực hiện theo Điều 12, Điều 13, Điều 14 của Quyết định số 1512/QĐ-BTTTT ngày 05/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Quy chế bảo đảm an toàn thông tin mạng và các quy định khác có liên quan.

Chương VII
TỔ CHỨC THỰC HIỆN

1. Tổ chức triển khai Quy chế

- Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

- Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Bộ phận chuyên trách để xem xét, bổ sung, sửa đổi.

2. Xây dựng, rà soát, cập nhật, bổ sung Quy chế

- Định kỳ 02 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. Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng.

- Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Bộ phận chuyên trách về ATTT để tổng hợp báo cáo điều chỉnh, bổ sung.

3. Đơn vị hoặc Bộ phận chuyên trách về an toàn thông tin

- Giao một công chức phòng Văn hóa – Xã hội phối hợp với các phòng có liên quan đảm bảo về ATTT cho hệ thống thông tin của UBND xã.

- Giao một công chức Trung tâm Phục vụ hành chính công phối hợp với phòng Văn hoá – Xã hội tiến hành công tác đảm bảo an toàn thông tin mạng tại Trung tâm.

- Công chức phòng Văn hoá - Xã hội phối hợp Văn phòng HĐND và UBND, các phòng có liên quan nghiên cứu và tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo chỉ đạo của UBND xã .

- Triển khai các phương án đảm bảo an toàn thông tin tại cơ quan UBND xã.

4. Các cơ quan, đơn vị trên địa bàn xã

- Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn xã và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

- Phòng Văn hoá - Xã hội có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân xã theo định kỳ hàng năm hoặc đột xuất theo yêu cầu của UBND xã và cơ quan có thẩm quyền của tỉnh.

- Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời Phòng Văn hoá - Xã hội xã để tổng hợp báo cáo Ủy ban nhân dân xã xem xét điều chỉnh cho phù hợp./.