

QUYẾT ĐỊNH

Ban hành quy chế an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Đảng ủy xã Quảng Uyên

Căn cứ Điều lệ Đảng Cộng sản Việt Nam;

Căn cứ Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

Căn cứ Quyết định số 204-QĐ/TW, ngày 19/12/2024 của Ban Bí thư Trung ương Đảng về phê duyệt Đề án chuyển đổi số trong các cơ quan Đảng;

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

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

Căn cứ 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 Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư 12/2022/TT-BTTTT ngày 18/12/2022 của Bộ Thông tin Truyền thông về việc 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;

Xét đề nghị của Văn phòng Đảng ủy,

BAN THƯỜNG VỤ ĐẢNG ỦY QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy chế an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Đảng ủy xã Quảng Uyên.

Điều 2. Giao Văn phòng Đảng ủy chịu trách nhiệm hướng dẫn và tổ chức thực hiện theo đúng nội dung Quy chế này.

Điều 3. Chánh Văn phòng Đảng ủy, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Quyết định có hiệu lực thi hành kể từ ngày ký.

Nơi nhận:

- Như điều 3,
- Sở Khoa học và Công nghệ tỉnh,
- Thường trực Đảng ủy, HĐND, UBND, Ủy ban MTTQ VN xã;
- Cán bộ, công chức xã,
- Lưu Văn phòng Đảng ủy.

T/M BAN THƯỜNG VỤ

BÍ THƯ



Ma Kiên Ngọc

QUY CHẾ

Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Đảng ủy xã Quảng Uyên

(Ban hành kèm theo Quyết định số: 68-QĐ/ĐU ngày 24/7/2025 của Ban Thường vụ Đảng ủy xã Quảng Uyên)



Chương I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định biện pháp, chính sách quản lý nhằm bảo đảm an toàn thông tin hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin của Đảng ủy xã Quảng Uyên.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng với các Cơ quan hành chính thuộc Đảng ủy xã Quảng Uyên; cán bộ, công chức, viên chức, người lao động làm việc tại các cơ quan nêu trên.

2. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các cơ quan, đơn vị thuộc khoản 1 Điều này.

Điều 3. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. An toàn thông tin mạng: Là công tác 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. 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 của một cơ quan, tổ chức.

3. 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.

4. 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. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

5. 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.

6. 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.

7. Mạng ngang hàng: Là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

8. Đơn vị chuyên trách về công nghệ thông tin: Là đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin do chủ quản hệ thống thông tin chỉ định.

9. Đơn vị chuyên trách về an toàn thông tin: Là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

10. Cán bộ chuyên trách: Là cán bộ, công chức, viên chức, người lao động được tuyển dụng phụ trách an toàn thông tin, công nghệ thông tin tại các cơ quan, đơn vị.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Yêu cầu thiết kế, xây dựng hệ thống thông tin

1. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin phải xây dựng phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định (hoặc đơn vị chuyên trách về an toàn thông tin của tỉnh) trước khi trình cấp có thẩm quyền phê duyệt dự án.

2. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin.

a) Chủ quản hệ thống thông tin có trách nhiệm tổ chức đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) để áp dụng phương án bảo đảm an toàn thông tin phù hợp.

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin hoặc đơn vị chuyên trách về an toàn thông tin của tỉnh thẩm định, trình cấp có thẩm quyền phê duyệt.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, Chủ quản hệ thống thông tin phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo

quy định tại Điều 9 Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng.

Điều 6. Quản lý thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan, đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ công nghệ thông tin

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan.

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

3. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin.

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm;

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ;

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại...

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ.

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 7. 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 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 cơ quan hành chính nhà nước phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 8. Quy định về cấp phát thu hồi cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Cán bộ chuyên trách thực hiện quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các cơ quan, đơn vị. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính; hủy quyền truy cập hệ thống thông tin đối với cán bộ, công chức, viên chức (CBCC) nghỉ chế độ, chuyển công tác và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi CBCC đó. Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

3. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như!, @, #, \$, %, ...).

Điều 9. Bảo đảm nguồn nhân lực

1. Khi tuyển dụng cán bộ chuyên trách phụ trách an toàn thông tin, công nghệ thông tin phải xây dựng các quy định đối với công tác tuyển dụng. Cán bộ chuyên trách 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. Cán bộ chuyên trách được đảm bảo các điều kiện về trang thiết bị, học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Cán bộ được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

4. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho tổ chức, cá nhân sử dụng hệ thống thông tin do đơn vị quản.

Điều 10. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a) Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin của các cơ quan nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao.

b) Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. Trang bị thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan, đơn vị khi kết nối với hệ thống bên ngoài; Xây dựng hoặc thuê hệ thống giám sát an toàn thông tin để kiểm soát, phát hiện truy cập trái phép vào hệ thống.

c) Khi thực hiện truy nhập từ xa vào mạng nội bộ thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin (như: SSL/TLS, VPN...) và thiết lập mật khẩu có độ phức tạp cao.

d) Xây dựng quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

đ) Không tự ý đấu nối thiết bị mạng, thiết bị cáp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ cơ quan, đơn vị.

e) Không tự ý thay đổi, gỡ bỏ biện pháp, giải pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tháo dỡ thành phần của máy tính phục vụ công việc. Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý hệ thống mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc 8 ký tự đặc

biệt như: !, @, #, \$, %), cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

c) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài, cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 11. Bảo đảm an toàn máy tính cá nhân và ứng dụng

1. Trên máy tính cá nhân

a) Hệ điều hành được cài đặt là phần mềm có bản quyền (bao gồm bản quyền thương mại hoặc mã nguồn mở có nguồn gốc rõ ràng), các dịch vụ cài đặt trên máy tính là các dịch vụ được sử dụng dùng chung cho cơ quan, đơn vị, không cài đặt các dịch vụ không sử dụng.

b) Thiết lập chế độ tự động cập nhật phiên bản và hệ điều hành, phần mềm, ứng dụng và phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy tính.

2. Cơ quan, đơn vị có trách nhiệm trang bị phần mềm phòng chống mã độc (antivirus) có bản quyền cho hệ thống máy tính; thiết lập chế độ tự động cập nhật phiên bản mới, các bản vá lỗi; chế độ tự động quét mã độc khi sao chép, mở các tập tin; chế độ quét toàn bộ máy tính định kỳ hằng tuần.

3. Định kỳ hằng tuần cơ quan phải kiểm tra các tiến trình trên máy tính nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy tính.

Điều 12. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi cấp tài khoản, chữ ký số lần đầu cho người dùng truy nhập, cơ quan, đơn vị vận hành phải thông báo (qua email, điện thoại) và người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu.

b) Các hệ thống thông tin khi phân quyền phải thiết lập chế độ giới hạn số lần đăng nhập không hợp lệ vào hệ thống tối đa không quá 05 lần, khi người dùng đăng nhập sai vượt quá số lần quy định, tài khoản chuyển sang chế độ khóa quyền truy cập; các hệ thống thông tin xác lập chế độ thoát ra khỏi hệ thống nếu người sử dụng không tương tác trên hệ thống của phiên làm việc quá 10 phút.

c) Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác (ví dụ tài khoản thư điện tử, chữ ký số, chứng thư số) để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu.

d) Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@caobang.gov.vn và chữ ký số do Ban Cơ yếu Chính phủ cấp) để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác; định kỳ 01 năm kiểm tra việc lưu trữ của hệ thống thư điện

tử, tiến hành xóa các mail quá cũ, không cần thiết để đảm bảo hệ thống hoạt động ổn định thông suốt.

đ) Tài khoản quản trị hệ thống được giao cho cán bộ chuyên trách công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Công chức, viên chức quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau.

e) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm Quyết định có hiệu lực, cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho cơ quan, đơn vị vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số.

2. Cơ chế mã hóa và sao lưu dữ liệu phải đảm bảo tính toàn vẹn của dữ liệu.

3. Cán bộ chuyên trách phối hợp với các đơn vị có liên quan thực hiện xác định các thông tin, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có. Các nội dung thực hiện gồm: Lập danh sách các dữ liệu (thông tin cấu hình của mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; thực hiện quy trình sao lưu dự phòng và phục hồi.

4. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

5. Khi thực hiện chia sẻ tài nguyên trên máy tính, các đơn vị phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

6. Đơn vị sử dụng máy tính và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

7. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

Điều 13. Bảo đảm an toàn thiết bị đầu cuối

1. Trên máy tính cá nhân phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc; thiết lập chế độ tự động cập nhật phần mềm phòng chống mã

độc, chế độ tự động rà quét mã độc khi sao chép, mở các tập tin, chế độ rà quét máy tính định kỳ hằng tuần.

2. Khuyến khích các đơn vị đầu tư, mua sắm thiết bị công nghệ thông tin sản xuất trong nước.

3. Kết nối máy tính, thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của tổ chức;

b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin;

4. Trong quá trình sử dụng thiết bị đầu cuối

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

Điều 14. Ứng cứu sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả;

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin;

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin;

d) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị; cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố

2. Phân nhóm sự cố an toàn thông tin

a) Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác;

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật;

c) Sự cố do lỗi của người quản trị, vận hành hệ thống;

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài

phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

3. Phân loại mức độ nghiêm trọng sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị;

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị;

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp;

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp;

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Quy trình phối hợp ứng cứu xử lý sự cố

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Ứng dụng Khoa học và Công nghệ trực thuộc Sở Khoa học và Công nghệ quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố về Sở Khoa học và Công nghệ (qua Trung tâm Ứng dụng Khoa học và Công nghệ)

d) Bước 4: Phối hợp với Trung tâm Ứng dụng Khoa học và Công nghệ và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

e) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho Đảng ủy xã (qua Văn phòng Đảng ủy).

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của Văn phòng Đảng ủy thì tham mưu cho Thường trực Đảng ủy xã báo cáo ngay Sở Khoa học và Công nghệ để được hướng dẫn, hỗ trợ.

6. Chuyên viên Văn phòng Đảng ủy xã phụ trách tham mưu về an toàn thông tin có trách nhiệm:

a) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Thực hiện quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định.

c) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

d) Tham gia diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của ngành cấp trên.

Chương III

KIỂM TRA ĐÁNH GIÁ CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 15. Kế hoạch kiểm tra hàng năm

1. Văn phòng Đảng ủy xã phối hợp với các Cơ quan chuyên môn thuộc Đảng ủy xã và các đơn vị liên quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn theo Kế hoạch công tác hàng năm.

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin trên địa bàn.

Điều 16. Nội dung hình thức kiểm tra đánh giá hệ thống thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực theo các nội dung theo Quy chế này; việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin; kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin;

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn thông tin tại đơn vị; phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

c) Kiểm tra, đánh giá các nội dung khác theo quy định hệ thống an toàn thông tin.

2. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của Đảng ủy xã và đơn vị chuyên trách về an toàn thông tin của tỉnh;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

Chương IV

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 17. Trách nhiệm của Văn phòng Đảng ủy xã

1. Tham mưu cho Đảng ủy xã vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công cán bộ phận kỹ thuật (quản lý ứng dụng; quản lý dữ liệu; 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.

2. Tham mưu cho Đảng ủy xã xây dựng hồ sơ đề xuất cấp độ an toàn thông tin và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng, đặc biệt là các văn bản liên quan đến công tác mật.

3. Chủ trì, phối hợp với các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Đảng ủy xã đối với các cơ quan nhà nước đóng trên địa bàn.

4. Hàng năm, cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ phụ trách an toàn thông tin mạng. Tổ chức tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn.

5. Phối hợp với Công an xã có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các trang thông tin điện tử, mạng xã hội.

6. Phối hợp với Ủy ban nhân dân xã và Công an xã Quảng Uyên Là cơ quan đầu mối thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn xã.

Điều 18. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình; quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

2. Chỉ đạo cán bộ, công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong đơn vị.

3. Thực hiện bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an xã, các cán bộ, công chức chuyên môn và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

Điều 19. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong đơn vị

1. Trách nhiệm của cán bộ phụ trách về an toàn thông tin, công nghệ thông tin tại đơn vị

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị.

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

c) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

2. Trách nhiệm của người sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được đơn vị chuyên môn tổ chức.

Điều 20. Trách nhiệm của các tổ chức, đơn vị cá nhân có liên quan

Các tổ chức, đơn vị, cá nhân sử dụng các hệ thống thông tin do Đảng ủy xã triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước xã phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Điều 21. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị thuộc Đảng ủy xã Quảng Uyên 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.

2. Văn phòng Đảng ủy xã có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Lãnh đạo Thường trực Đảng ủy xã theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của Lãnh đạo Thường trực Đảng ủy xã và cơ quan có thẩm quyền của tỉnh.

3. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Văn phòng Đảng ủy xã để tổng hợp báo cáo Lãnh đạo Thường trực Đảng ủy xã xem xét điều chỉnh, bổ sung.