ỦY BAN NHÂN DÂN **XÃ NGHĨA SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do – Hạnh phúc**
Số: 206 /QĐ-UBND	*Nghĩa Sơn, ngày 20 tháng 11 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số trên địa bàn xã Nghĩa Sơn

ỦY BAN NHÂN DÂN XÃ NGHĨA SƠN

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

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

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

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

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng11 năm 2015;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước;

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 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên môi trường mạng; Nghị định 27/2018/NĐ-CP ngày 01/3/2018 của Chính phủ về sửa đổi, bổ sung một số điều của Nghị định số 72/2013/NĐ-CP;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dân một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về ban hành quy định đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi;

Xét đề nghị của bộ phận chuyên môn và ý kiến của các thành viên UBND xã Nghĩa Sơn.

QUYẾT ĐỊNH:

Điều 1. Ban hành Quyết định kèm theo Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số trên địa bàn xã Nghĩa Sơn.

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

Điều 3. Văn phòng UBND xã, các cơ quan, đơn vị và các tổ chức, cá nhân, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Phòng VH-TT huyện;
- Thường trực Đảng ủy;
- Thường trực HĐND;
- CT, các PCT UBND;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ NGHĨA SƠN H.TƯ NGHĨA T.QUẢNG NGÃI

Phạm Văn Phùng

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

QUY CHẾ
An toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn xã Nghĩa Sơn

(Ban hành kèm theo Quyết định số 206/QĐ-UBND ngày 20/11/2024 của Uỷ ban nhân dân xã Nghĩa Sơn)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung về bảo đảm an toàn thông tin mạng, an ninh mạng đối với việc xây dựng, vận hành, khai thác hệ thống thông tin, hạ tầng mạng, thiết bị, dữ liệu, giám sát an toàn thông tin mạng và ứng cứu xử lý sự cố về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn xã Nghĩa Sơn.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với Ủy ban nhân dân xã Nghĩa Sơn *(sau đây gọi là cơ quan, đơn vị).*

Cán bộ, công chức, người lao động *(sau đây gọi là cá nhân)* trong các cơ quan, đơn vị nêu tại khoản 1 Điều này và những cá nhân, tổ chức có liên quan áp dụng quy chế này trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại các cơ quan, đơn vị.

Điều 3. Giải thích từ ngữ

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

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.

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.

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.

Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin qua mạng viễn thông và mạng máy tính.

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.

Tính toàn vẹn là bảo vệ tính chính xác, tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

Tính sẵn sàng là bảo đảm những người được cấp quyền có thể truy cập thông tin và các tài liệu có liên quan ngay khi có nhu cầu.

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.

Phần mềm gián điệp là loại phần mềm chuyên thu thập các thông tin từ các máy tính qua mạng mà không có sự nhận biết và cho phép của chủ máy.

Thư rác là thư điện tử, tin nhắn được gửi đến người nhận mà người nhận đó không mong muốn hoặc không có trách nhiệm phải tiếp nhận theo quy định của pháp luật.

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.

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.

Điều 4. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

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

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

Điều 5. Các hành vi bị nghiêm cấm

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

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Những quy định bảo đảm an toàn thông tin mạng

Cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn thông tin mạng cho cá nhân trước khi tham gia sử dụng hệ thống thông tin.

Bố trí người làm công tác chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp hoặc được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an

toàn thông tin mạng.

Bố trí kinh phí tối thiểu 10% của tổng kinh phí chi cho chuyển đổi số, ứng dụng công nghệ thông tin của các cơ quan, đơn vị cho hạng mục về an toàn thông tin mạng.

Cán bộ, công chức, viên chức tham gia đoàn kiểm tra công tác bảo đảm an toàn thông tin mạng phải được trang bị đầy đủ những kiến thức và được tập huấn về công tác bảo đảm an toàn thông tin mạng.

Điều 7. Bảo đảm an toàn thông tin mạng trong xây dựng, quản lý, vận hành, sử dụng hệ thống thông tin

Các hoạt động liên quan đến xây dựng, thiết lập, nâng cấp, mở rộng, quản lý, vận hành hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Nghị định số 85/2016/NĐ-CP); Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Thông tư số 12/2022/TT-BTTTT).

Nhiệm vụ quản lý, xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng; tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 12/2022/TT-BTTTT.

Các cơ quan, đơn vị chủ quản hệ thống thông tin phải tổ chức kiểm tra, đánh giá định kỳ về an toàn thông tin mạng của các hệ thống thông tin đang quản lý. Bảo đảm an toàn mạng trang bị các thiết bị phần cứng, phần mềm về bảo mật như tường lửa (firewall), thiết bị phát hiện, phòng, chống xâm nhập trái phép (IDS/IPS); tổ chức mô hình mạng hợp lý, phù hợp với quy mô hệ thống thông tin của cơ quan, đơn vị.

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

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

Mạng riêng ảo (VPN) của các cơ quan, đơn vị kết nối để truy cập vào hệ thống thông tin phải được bảo mật, quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng.

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

Khuyến khích cài đặt, cấu hình, tổ chức hệ thống mạng nội bộ (LAN) theo mô hình Server/Client, hạn chế sử dụng mô hình mạng ngang hàng. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập mạng riêng ảo (VPN) để đảm bảo an toàn thông tin mạng cho mạng nội bộ.

Các cơ quan, đơn vị tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về bảo đảm an toàn thông tin mạng theo quy định tại các Điều 11, 12, 13 của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm '20n của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; Quyết định số 08/2019/QĐUBND ngày 5 tháng 4 năm 2019 của Ủy ban nhân dân tỉnh Quảng Ngãi ban hành Quy chế quản lý, vận hành và sử dụng mạng Truyền số liệu chuyên dùng cấp II trên địa bàn tỉnh.

Bảo đảm an toàn máy chủ và máy tính cá nhân (gọi tắt là máy tính) Tài khoản đăng nhập máy tính phải được thiết lập mật khẩu phức tạp; khi sử dụng máy tính hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing) qua môi trường mạng, nếu có sử dụng chức năng này cần thiết lập thuộc tính bảo mật bằng mật khẩu, phân quyền và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

Thay đổi các tài khoản mặc định trên máy tính hoặc vô hiệu hóa (nếu không sử dụng). Thiết lập giới hạn thời gian chờ (time out) để đóng các phiên truy cập, kết nối khi máy tính không nhận được yêu cầu từ người dùng.

Thiết lập ghi lại nhật ký thông tin đăng nhập vào máy chủ, thông tin thay đổi cấu hình, thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có).

Vô hiệu hóa, đóng tất cả các cổng (port) dịch vụ khi không sử dụng; thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành, phần mềm cơ sở dữ liệu... được cài đặt trên các máy chủ.

Khi kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, cài đặt phải sử dụng phương thức kết nối có mã hóa như SSH, VPN...

Cài đặt phần mềm phòng, chống virus, mã độc có bản quyền cho tất cả các máy tính, đồng thời bảo đảm các phần mềm phòng, chống virus, mã độc này luôn được cập nhật, nhận dạng virus, mã độc mới.

Sử dụng các thiết bị lưu trữ (USB, ổ cứng gắn ngoài,...) an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính: khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước khi sử dụng; thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

Chỉ được mở các tập tin đính kèm trong thư điện tử khi biết rõ nguồn gốc người gửi thư; không được mở các thư điện tử có tập tin đính kèm không rõ nguồn gốc người gửi để tránh trường hợp có thể virus, phần mềm gián điệp... được đính kèm theo thư và lây nhiễm vào máy tính.

Bảo đảm an toàn ứng dụng

Bảo đảm an toàn thông tin mạng đối với các ứng dụng dùng chung của tỉnh

Phải tổ chức mô hình hợp lý; trang bị các hệ thống phòng thủ quan trọng như tường lửa (Firewall), thiết bị phát hiện/phòng, chống xâm nhập trái phép (IDS/IPS), tường lửa mức ứng dụng web (Web Application Firewall); khi xây dựng mới hoặc nâng cấp, mở rộng phải tuân thủ khung phát triển phần mềm an toàn và đáp ứng yêu cầu an toàn cơ bản đối với phần mềm nội bộ.

Các website khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ mới... cần phải đánh giá, kiểm định nhằm tránh các lỗi bảo mật thường xuyên xảy ra trên ứng dụng web như: SQL Injection, Cross Site Scripting (XSS)...

Thiết lập thời gian chờ (time out) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng; phân quyền truy cập, quản trị, sử dụng tài nguyên phù hợp với từng người dùng.

Sử dụng kết nối an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.

Đối với cá nhân sử dụng, khai thác các phần mềm dùng chung của tỉnh

Thay đổi mật khẩu mặc định, thiết lập mật khẩu các tài khoản được cấp có độ phức tạp cao (độ dài tối thiểu 8 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số).

Nghiêm cấm đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh; không đặt chế độ ghi nhớ mật khẩu khi sử dụng; khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong các trình duyệt.

Bảo đảm an toàn dữ liệu

Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế sao lưu (backup) dữ liệu ở mức hệ thống, dữ liệu của các ứng dụng, dữ liệu của người sử

dụng; cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên; thiết bị lưu trữ dữ liệu được sao lưu phải bảo đảm yêu cầu kỹ thuật; dữ liệu được sao lưu phải bảo đảm tính sẵn sàng và toàn vẹn đáp ứng yêu cầu phục hồi dữ liệu cho hệ thống thông tin hoạt động bình thường khi có sự cố xảy ra.

Trang bị hệ thống/thiết bị lưu trữ dữ liệu (tủ/băng, đĩa/DAS/NAS/ SAN...) và tổ chức mô hình sao lưu độc lập (tách biệt về mặt vật lý) phù hợp với quy mô hệ thống thông tin của cơ quan, đơn vị.

Phải thiết lập cơ chế sao lưu định kỳ một cách tự động nhằm đảm bảo việc sao lưu đầy đủ các dữ liệu theo yêu cầu; áp dụng chính sách ghi, lưu tập trung biên bản hoạt động (logfile) cần thiết để phục vụ công tác điều tra, khắc phục khi xảy ra sự cố.

Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

Điều 8. Giám sát an toàn thông tin mạng cho các hệ thống thông tin

Bảo đảm triển khai đầy đủ giám sát kỹ thuật an toàn thông tin mạng gồm: giám sát lớp mạng; giám sát lớp máy chủ và cơ sở dữ liệu; giám sát lớp ứng dụng và giám sát lớp thiết bị đầu cuối.

Tổ chức giám sát cho tất cả các hệ thống thông tin quan trọng trên địa bàn xã.

Bảo đảm duy trì việc kết nối, chia sẻ dữ liệu giám sát theo thời gian thực của các hệ thống thông tin về Trung tâm Giám sát an toàn không gian mạng quốc gia. Thiết lập chế độ chia sẻ dữ liệu giám sát phù hợp để bảo đảm chất lượng chia sẻ.

Điều 9. Bảo vệ bí mật Nhà nước trong công tác ứng dụng công nghệ thông tin, chuyển đổi số

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

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

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

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

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

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

Điều 10. Công chức, viên chức phụ trách về công nghệ thông tin

Phải bảo đảm điều kiện được đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ đối với lĩnh vực an toàn thông tin mạng, an ninh mạng.

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

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

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

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

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

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

Sử dụng công cụ hỗ trợ để kiểm tra, giám sát dữ liệu, thông tin từ bên trong hệ thống, thông tin gửi ra bên ngoài khi cần thiết.

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

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

Điều 11. Giải quyết và khắc phục sự cố về an toàn thông tin mạng

Đối với người sử dụng

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

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

Đối với công chức, viên chức chuyên trách về công nghệ thông tin

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

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

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

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 12. Trách nhiệm của các cơ quan, đơn vị

Trưởng các ban, ngành, cơ quan, chịu trách nhiệm trước Ủy ban nhân dân xã trong công tác bảo đảm an toàn thông tin, an ninh mạng đối với toàn bộ hệ thống thông tin của cơ quan, đơn vị mình.

Tuyên truyền, phổ biến Quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin mạng, an ninh mạng trong phạm vi trách nhiệm và quyền hạn của từng cơ quan, đơn vị; thực hiện và chỉ đạo các cá nhân thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy chế này.

Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định khác.

Thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn thông tin mạng cho hệ thống thông tin của cơ quan, đơn vị theo quy định tại Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT.

Phối hợp với Sở Thông tin và Truyền thông trong công tác giám sát an toàn thông tin mạng đối với các hệ thống thông tin của cơ quan, đơn vị mình.

Xây dựng, triển khai kế hoạch bảo đảm an toàn thông tin mạng và báo cáo về Phòng Văn hoá và Thông tin huyện theo định kỳ hàng năm; hàng năm bố trí kinh phí bảo đảm an toàn thông tin mạng trong nội bộ cơ quan, đơn vị mình; đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác bảo đảm an toàn thông tin mạng.

Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của cơ quan, đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan liên quan.

Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố; lực lượng kỹ thuật tham gia khắc phục sự cố thực hiện đúng theo hướng dẫn chuyên môn của Sở Thông tin và Truyền thông.

Phối hợp với Phòng Văn hóa và Thông tin, Văn phòng HĐND và UBND huyện và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin, an ninh mạng.

Tạo điều kiện thuận lợi cho công chức chuyên trách về công nghệ thông tin được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn thông tin mạng, an ninh mạng.

Điều 13. Trách nhiệm của cá nhân

Trách nhiệm của công chức, viên chức chuyên trách công nghệ thông tin tại các cơ quan, đơn vị

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về bảo đảm an toàn thông tin mạng cho toàn bộ hệ thống thông tin của cơ quan, đơn vị mình đúng theo nội dung Quy chế này.

b) Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn thông tin mạng.

c) Tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn thông tin mạng.

d) Trách nhiệm của cá nhân tham gia sử dụng và khai thác hệ thống thông tin tại các cơ quan, đơn vị

đ) Nghiêm chỉnh thực hiện các nội quy, quy chế, quy trình nội bộ về bảo đảm an toàn thông tin, an ninh mạng của cơ quan, đơn vị cũng như các quy định khác của pháp luật về nội dung này.

e)Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho công chức, viên chức chuyên trách công nghệ thông tin của cơ quan, đơn vị mình để kịp thời ngăn chặn và xử lý.

g)Nâng cao ý thức cảnh giác và trách nhiệm về an toàn thông tin, an ninh mạng.

h) Không sử dụng mạng xã hội như: Google Plus+, MySpace, LinkedIn, Twitter, Facebook, Zalo, blog cá nhân.. .để đăng tải, phát tán, truyền tải lại những nội dung phản động, tuyên truyền, xuyên tạc; không được truy cập vào các liên kết (link) không rõ ràng; không sử dụng địa chỉ thư điện tử công vụ vào mục đích cá nhân như: đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua

mạng.;

i) Không sử dụng các hộp thư điện tử miễn phí Gmail, Yahoo,... trong hoạt động công vụ và tại máy tính có nối mạng ở cơ quan, đơn vị nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

k) Cá nhân sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng di động, băng từ...) để lưu thông tin thuộc danh mục bí mật Nhà nước có trách nhiệm bảo vệ các thiết bị này và thông tin trên thiết bị, tránh làm mất, lộ thông tin. Nghiêm cấm việc bán, cho mượn, giao người không có trách nhiệm sử dụng thiết bị do cá nhân tự trang bị có lưu giữ bí mật Nhà nước.

Điều 14. Trách nhiệm của tổ chức, doanh nghiệp, cá nhân có liên quan đối với việc bảo đảm an toàn thông tin mạng

Các tổ chức, doanh nghiệp cung cấp dịch vụ hạ tầng mạng, Internet, công nghệ thông tin phải thiết lập đầu mối liên lạc để phối hợp, tuân thủ việc điều phối của cơ quan chức năng và tham gia vào công tác ứng cứu, khắc phục sự cố đối với các hệ thống thông tin quan trọng của huyện.

Tổ chức, cá nhân tham gia cung cấp thông tin và sử dụng dịch vụ trên mạng có trách nhiệm bảo đảm an toàn thông tin mạng, an ninh mạng trong phạm vi hệ thống thông tin của mình; phối hợp với cơ quan quản lý Nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin trên mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 15. Tổ chức thực hiện

Giao Văn phòng - Thống kê chủ trì, tham mưu, phối hợp với các cơ quan, đơn vị triển khai thực hiện Quy chế này.

Thủ trưởng các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm túc Quy chế này.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các đơn vị kịp thời báo cáo về Phòng Văn hóa và Thông tin huyện để xem xét hướng dẫn./.