ỦY BAN NHÂN DÂN TỈNH QUẢNG NINH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 42 /2026/QĐ-UBND	*Quảng Ninh, ngày 25 tháng 5 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, khai thác, sử dụng và bảo vệ an ninh mạng đối với hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh

Căn cứ Luật Tổ chức Chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 được sửa đổi, bổ sung bởi Luật số 87/2025/QH15;

Căn cứ Luật an ninh mạng số 116/2025/QH15;

Căn cứ Luật bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Luật dữ liệu số 60/2024/QH15;

Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;

Căn cứ Nghị định số 78/2025/NĐ-CP của Chính phủ quy định chi tiết một số điều và biện pháp để tổ chức, hướng dẫn thi hành Luật Ban hành văn bản quy phạm pháp luật được sửa đổi, bổ sung bởi Nghị định số 187/2025/NĐ-CP;

Căn cứ Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 147/2024/NĐ-CP của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

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

Theo đề nghị của Công an tỉnh tại Tờ trình số 119/TTr-CAT-ANM ngày 29 tháng 4 năm 2026; Báo cáo thẩm định số 120/BC-STP ngày 14 tháng 4 năm 2026 của Sở Tư pháp.

Ủy ban nhân dân tỉnh ban hành Quyết định ban hành Quy chế quản lý, khai thác, sử dụng và bảo vệ an ninh mạng đối với hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh.

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, khai thác, sử dụng và bảo vệ an ninh mạng đối với hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2026. Quyết định số 708/QĐ-UBND ngày 14 tháng 4 năm 2014 của Ủy ban nhân dân tỉnh về ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Quảng Ninh hết hiệu lực thi hành kể từ ngày Quyết định này có hiệu lực thi hành.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc, Thủ trưởng các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các xã, phường, đặc khu và các cơ quan, đơn vị, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Công an;
- Cục Kiểm tra văn bản và tổ chức thi hành pháp luật - Bộ Tư pháp;
- Chủ tịch, các PCT UBND tỉnh;
- V0, V1-4, VX1;
- TT Thông tin - VP UBND tỉnh;
- Lưu: VT, VX4

Ký bởi: Nguyễn Hoàng Anh

Ký bởi: Vũ Tất Bằng

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Nguyễn Văn Công

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

QUY CHẾ

Quản lý, khai thác, sử dụng và bảo vệ an ninh mạng đối với hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh

(Ban hành kèm theo Quyết định số 42 /2026/QĐ-UBND ngày 25tháng 5 năm 2026 của Ủy ban nhân dân tỉnh Quảng Ninh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy chế này quy định về các hoạt động quản lý, khai thác, sử dụng và các biện pháp bảo vệ an ninh mạng đối với các hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh.

2. Đối tượng áp dụng

a) Các cơ quan nhà nước thuộc tỉnh Quảng Ninh, bao gồm: Các sở, ban, ngành; Ủy ban nhân dân các xã, phường, đặc khu; các đơn vị sự nghiệp công lập và các cơ quan, đơn vị khác có quản lý, vận hành, khai thác hệ thống thông tin thuộc phạm vi điều chỉnh của Quy chế này;

b) Cán bộ, công chức, viên chức và người lao động trong các cơ quan nhà nước quy định tại điểm a khoản 2 Điều này;

c) Các tổ chức, cá nhân có liên quan đến việc quản lý, vận hành, khai thác và sử dụng hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh.

Điều 2. Giải thích từ ngữ

1. Các từ ngữ: "An ninh mạng", "An ninh dữ liệu", "Bảo vệ an ninh mạng", "Hệ thống thông tin", "Chủ quản hệ thống thông tin" được sử dụng trong Quy chế này có nội dung định nghĩa theo quy định tại Điều 2 Luật An ninh mạng số 116/2025/QH15.

2. Ngoài các từ ngữ quy định tại khoản 1 Điều này, các từ ngữ dưới đây được hiểu như sau:

a) 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;

b) Đơn vị chuyên trách về an ninh mạng là đơn vị có chức năng, nhiệm vụ bảo đảm an ninh mạng của chủ quản hệ thống thông tin;

c) Đơn vị thuê dịch vụ là cơ quan nhà nước sử dụng hạ tầng, phần mềm hoặc giải pháp đảm bảo an ninh mạng do một đơn vị thứ ba (doanh nghiệp) cung cấp thay vì tự xây dựng hệ thống riêng.

Điều 3. Nguyên tắc chung

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin. Mọi hoạt động bảo vệ an ninh mạng phải tuân thủ quy định của pháp luật về an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước, dữ liệu cá nhân và các quy định pháp luật liên quan khác.

2. Việc bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức là yêu cầu bắt buộc, được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật.

3. Việc quản lý, khai thác và sử dụng dữ liệu trong hệ thống thông tin phải thực hiện đúng mục đích, thẩm quyền và trình tự, thủ tục quy định. Dữ liệu được thu thập, cập nhật vào hệ thống phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật và có giá trị pháp lý theo quy định của pháp luật.

4. Quản lý, khai thác và sử dụng được thực hiện đồng bộ, chặt chẽ với bảo vệ an ninh mạng.

Điều 4. Các hành vi bị cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An ninh mạng số 116/2025/QH15, Điều 5 Luật Bảo vệ bí mật nhà nước số 117/2025/QH15, Điều 7 Luật bảo vệ Dữ liệu cá nhân số 91/2025/QH15, Điều 10 Luật Dữ liệu số 60/2024/QH15.

2. Hành vi nghiêm cấm khác về an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước, dữ liệu cá nhân theo quy định của pháp luật.

Chương II
QUY ĐỊNH QUẢN LÝ, KHAI THÁC VÀ SỬ DỤNG HỆ THỐNG THÔNG TIN

Điều 5. Quy trình quản lý, vận hành hệ thống thông tin

1. Cơ quan chủ quản hệ thống thông tin có trách nhiệm ban hành quy trình vận hành cụ thể đối với từng hệ thống thông tin, bao gồm các nội dung chính sau:

a) Quản lý cấu hình, thay đổi và cập nhật hệ thống

Quy trình này phải mô tả rõ ràng các bước để quản lý cấu hình ban đầu của hệ thống, quy trình phê duyệt và thực hiện các thay đổi cấu hình, cũng như quy trình cập nhật phần mềm, bản vá bảo mật và các thành phần khác của hệ thống. Mỗi thay đổi phải được ghi nhận, kiểm soát phiên bản và có khả năng khôi phục

về trạng thái trước đó;

b) Quản lý truy cập và nhật ký hệ thống

Quy trình cần xác định rõ cách thức cấp phát, thu hồi quyền truy cập cho người dùng và quản trị viên; các chính sách về mật khẩu, xác thực đa yếu tố. Đồng thời, phải quy định việc thu thập, lưu trữ, phân tích và kiểm tra định kỳ nhật ký hệ thống (log) để phát hiện các hoạt động bất thường hoặc truy cập trái phép;

c) Sao lưu, phục hồi dữ liệu

Quy trình này phải thể hiện chi tiết tần suất sao lưu (hằng ngày, hằng tuần, hằng tháng), phương pháp sao lưu (toàn bộ, gia tăng, khác biệt), nơi lưu trữ bản sao lưu (trung tâm dữ liệu dự phòng, kho lưu trữ an toàn) và quy trình kiểm thử khả năng phục hồi dữ liệu sau sự cố;

d) Giám sát hoạt động và khắc phục sự cố kỹ thuật

Quy trình phải bao gồm các hoạt động giám sát liên tục hiệu năng, trạng thái hoạt động và các chỉ số an toàn của hệ thống. Khi phát hiện sự cố kỹ thuật, quy trình phải hướng dẫn các bước để phân loại sự cố, thông báo, chẩn đoán nguyên nhân, khắc phục và ghi nhận lại toàn bộ quá trình xử lý.

2. Đơn vị vận hành có trách nhiệm:

a) Xác định cấp độ và phương án bảo vệ an ninh mạng đối với hệ thống thông tin đang vận hành theo quy định tại Điều 13 Quy chế này;

b) Đơn vị vận hành phải thiết lập và duy trì hệ thống ghi nhật ký (log) đối với thông tin đăng nhập, hoạt động truy cập dữ liệu, thay đổi cấu hình hệ thống, lỗi và cảnh báo bảo mật phục vụ cho việc giám sát, kiểm tra và điều tra khi có sự cố;

c) Thiết lập và thực hiện quy trình quản lý thay đổi đối với phần mềm, phần cứng và cấu hình hệ thống đảm bảo mọi thay đổi phải được phê duyệt, lưu trữ hồ sơ (bao gồm: lý do, người thực hiện, thời gian, kết quả) và đảm bảo khả năng khôi phục trạng thái ổn định của hệ thống trước khi thay đổi nếu có sự cố phát sinh;

d) Cập nhật bản vá bảo mật, phần mềm hệ thống, trình điều khiển và các dịch vụ định kỳ tối thiểu 01 lần/quý hoặc theo khuyến nghị của nhà sản xuất, cơ quan, tổ chức chuyên môn về an ninh mạng để phòng ngừa các lỗ hổng bảo mật;

đ) Kiểm thử toàn bộ hệ thống sau mỗi lần cập nhật hoặc nâng cấp

Sau mỗi lần thực hiện cập nhật hoặc nâng cấp hệ thống (bao gồm cả phần mềm và phần cứng), đơn vị vận hành phải tiến hành kiểm thử toàn diện để bảo đảm các thay đổi không gây ra lỗi mới, không ảnh hưởng đến chức năng hoạt động bình thường và không tạo ra các lỗ hổng bảo mật tiềm ẩn.

3. Bảo đảm tính sẵn sàng và liên tục:

a) Căn cứ cấp độ an toàn được phê duyệt, các cơ quan, đơn vị phải xây dựng phương án dự phòng bảo đảm tính liên tục của hệ thống thông tin để sẵn sàng chuyển đổi hoạt động khi xảy ra sự cố mất an toàn thông tin;

b) Xây dựng kế hoạch khôi phục khi xảy ra sự cố an ninh mạng để nhanh chóng đưa hệ thống trở lại hoạt động bình thường

Kế hoạch phải được xây dựng chi tiết, bao gồm các bước cụ thể để phục hồi hệ thống và dữ liệu trong trường hợp xảy ra sự cố nghiêm trọng như hỏa hoạn, lũ lụt, tấn công mạng quy mô lớn hoặc các thảm họa tự nhiên khác. Kế hoạch phải xác định rõ vai trò, trách nhiệm của từng cá nhân, đội ngũ, các công cụ và quy trình cần thiết để đưa hệ thống trở lại trạng thái hoạt động bình thường trong thời gian ngắn nhất có thể;

c) Tổ chức kiểm tra hoặc diễn tập phương án khôi phục hệ thống tối thiểu 01 lần/năm để bảo đảm tính khả thi và khả năng sẵn sàng ứng phó khi xảy ra sự cố; kịp thời phát hiện các hạn chế, bất cập để hoàn thiện quy trình ứng cứu sự cố và bảo đảm đội ngũ nhân sự sẵn sàng tham gia ứng cứu khi xảy ra sự cố.

Điều 6. Quản lý tài khoản và truy cập

1. Tài khoản người dùng phải được cấp riêng biệt, gắn định danh công vụ; không dùng chung tài khoản nhằm bảo đảm trách nhiệm cá nhân và khả năng truy vết các hoạt động trên hệ thống. Người dùng phải thực hiện đăng xuất tài khoản sau khi kết thúc phiên làm việc; thường xuyên xóa bộ nhớ đệm (cache) và cookie trên trình duyệt.

2. Quy trình cấp quyền, thay đổi quyền và thu hồi quyền truy cập phải được phê duyệt bằng văn bản của cấp có thẩm quyền hoặc qua hệ thống quản lý người dùng tập trung với các bước xác thực rõ ràng.

3. Mật khẩu phải đáp ứng tiêu chuẩn bảo mật (tối thiểu 08 ký tự, gồm chữ hoa, chữ thường, số, ký tự đặc biệt), được thay đổi tối thiểu 03 tháng/lần để giảm thiểu rủi ro bị lộ mật khẩu. Không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động trên trình duyệt hay các ứng dụng khác.

4. Tài khoản quản trị hệ thống phải được thiết lập riêng biệt với tài khoản người dùng thông thường và được phân quyền truy cập ở mức cao nhất. Tài khoản này phải sử dụng phương thức xác thực đa yếu tố (MFA) khi đăng nhập hệ thống.

5. Khi cán bộ, công chức, viên chức, người lao động nghỉ việc, luân chuyển hoặc thay đổi nhiệm vụ, cơ quan chủ quản phải thu hồi tài khoản trong thời gian 24 giờ. Bộ phận làm công tác tổ chức cán bộ có trách nhiệm thông báo cho bộ phận Quản trị hệ thống ngay khi có quyết định nhân sự để thực hiện thu hồi tài khoản.

Điều 7. Quản lý dữ liệu và sao lưu

1. Dữ liệu trong hệ thống thông tin phải được phân loại theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng để áp dụng các biện pháp bảo vệ tương ứng với cấp độ an toàn hệ thống.

2. Phải thực hiện sao lưu dữ liệu định kỳ để phòng ngừa mất dữ liệu do sự cố kỹ thuật, tấn công mạng hoặc lỗi của con người.

a) Đối với các hệ thống thông tin có tính chất trọng yếu, hoạt động liên tục và chứa dữ liệu thường xuyên thay đổi, việc cấu hình, sao lưu dữ liệu phải được thực hiện theo thiết kế của hệ thống để đảm bảo dữ liệu mới nhất luôn được bảo vệ;

b) Đối với dữ liệu nghiệp vụ phát sinh thường xuyên khác, thực hiện sao lưu tối thiểu 01 lần/tuần;

c) Đối với dữ liệu dùng chung, dữ liệu ít thay đổi và dữ liệu trên máy tính cá nhân của cán bộ, công chức, viên chức, người lao động, thực hiện sao lưu dữ liệu tối thiểu 01 lần/tháng.

3. Ưu tiên phối hợp với Sở Khoa học và Công nghệ để thực hiện lưu trữ tập trung đối với các cơ sở dữ liệu chuyên ngành có dung lượng lớn, cấu trúc phức tạp tại Trung tâm tích hợp dữ liệu của tỉnh. Việc lưu trữ tập trung không thay thế trách nhiệm của đơn vị trong việc duy trì các bản sao lưu dự phòng theo quy định tại Khoản 6 Điều này.

4. Dữ liệu sao lưu phải được mã hóa và lưu trữ tại vị trí an toàn, tách biệt với hệ thống chính. Căn cứ điều kiện thực tế, cơ quan, đơn vị thực hiện lưu trữ tại Trung tâm dữ liệu dự phòng của tỉnh hoặc các kho lưu trữ dữ liệu số chuyên dụng đảm bảo an toàn về vật lý và an ninh mạng.

5. Việc phục hồi dữ liệu sau sự cố phải được kiểm thử định kỳ tối thiểu 02 lần/năm. Mọi hoạt động sao lưu và phục hồi phải được ghi nhật ký chi tiết (bao gồm: người thực hiện, thời gian, trạng thái và các tình huống phát sinh) để phục vụ công tác kiểm tra, giám sát.

6. Quy định cụ thể cho việc bảo vệ bản sao dữ liệu.

Việc bảo vệ bản sao dữ liệu phải bảo đảm tính sẵn sàng và toàn vẹn, cụ thể:

a) Cách thức lưu trữ: Dữ liệu phải được lưu trữ tối thiểu thành 03 bản sao trên ít nhất 02 loại hình phương tiện lưu trữ khác nhau; trong đó có tối thiểu 01 bản lưu trữ độc lập (offline), cách ly hoàn toàn với môi trường mạng;

b) Kiểm soát quyền sử dụng: Quyền quản trị hệ thống sao lưu phải tách biệt hoàn toàn với quyền quản trị hệ thống chính; áp dụng phương thức xác thực đa yếu tố khi truy cập dữ liệu sao lưu. Thiết lập tính năng chỉ đọc đối với dữ liệu sao lưu để ngăn chặn việc chỉnh sửa hoặc xóa dữ liệu trái phép;

c) Bảo vệ an toàn vật lý: Các phương tiện lưu trữ vật lý phải được dán nhãn, quản lý theo danh mục và bảo quản trong tủ an toàn chuyên dụng có khóa, kiểm soát quyền ra vào;

d) Mã hóa và kiểm tra: Dữ liệu sao lưu phải được đặt mật khẩu bảo vệ ở mức cao nhất. Định kỳ hằng tháng, bộ phận kỹ thuật phải kiểm tra các bản sao lưu để bảo đảm dữ liệu không bị lỗi và có thể sử dụng được ngay khi cần thiết.

Điều 8. Bảo trì, cập nhật và nâng cấp hệ thống

1. Thực hiện bảo trì định kỳ để bảo đảm hiệu năng, tính ổn định và an toàn.

Các hoạt động bảo trì định kỳ phải được thực hiện theo lịch trình cụ thể, bao

gồm kiểm tra phần cứng, tối ưu hóa phần mềm, dọn dẹp hệ thống, kiểm tra các bản ghi lỗi và các công việc khác nhằm duy trì hiệu năng hoạt động tối ưu, bảo đảm tính ổn định và an toàn của hệ thống.

2. Việc nâng cấp, thay đổi cấu hình, cập nhật phần mềm phải có:

a) Kế hoạch cụ thể được cấp có thẩm quyền phê duyệt, trong đó xác định rõ mục tiêu, phạm vi, quy trình và biện pháp dự phòng rủi ro;

b) Biên bản thực hiện ghi rõ nội dung, thời gian, người thực hiện và các thông số kỹ thuật đã thay đổi;

c) Báo cáo đánh giá rủi ro đối với các thay đổi lớn, kèm theo các biện pháp giảm thiểu rủi ro đã được đề xuất và áp dụng.

3. Chỉ được phép sử dụng phần mềm có bản quyền hợp pháp, có nguồn gốc rõ ràng và được kiểm duyệt về an ninh mạng trước khi triển khai.

4. Đơn vị vận hành có trách nhiệm báo cáo kết quả bảo trì, cập nhật, nâng cấp hệ thống thông tin theo kế hoạch bảo trì hằng năm đã được phê duyệt hoặc đột xuất theo yêu cầu của chủ quản hệ thống thông tin.

Điều 9. Khai thác và sử dụng hệ thống thông tin

1. Phân quyền và khai thác

a) Người sử dụng chỉ được phép truy cập và khai thác trong phạm vi chức năng được phân quyền;

b) Mọi hành vi cố ý truy cập, sử dụng chức năng hoặc dữ liệu ngoài phạm vi quyền hạn được xem là hành vi vi phạm quy chế.

2. Mọi hoạt động khai thác dữ liệu phục vụ công tác chuyên môn phải tuân thủ quy định về bảo vệ dữ liệu cá nhân, bảo vệ dữ liệu, bảo vệ bí mật nhà nước và các quy định khác có liên quan.

Điều 10. Quản lý thiết bị, hạ tầng và tài nguyên hệ thống

1. Tất cả các thiết bị công nghệ thông tin quan trọng như máy chủ, thiết bị lưu trữ dữ liệu, thiết bị mạng (switch, router) và thiết bị bảo mật (firewall, IDS/IPS) phải được dán nhãn rõ ràng, có số hiệu tài sản và được quản lý chặt chẽ trong hệ thống quản lý tài sản của cơ quan. Việc kiểm kê tài sản phải được thực hiện định kỳ hằng năm để đối chiếu, cập nhật và phát hiện các sai lệch.

2. Các thành phần vật lý quan trọng của hạ tầng mạng như cáp mạng, thiết bị chuyển mạch (switch), tường lửa (firewall) và máy chủ phải được đặt trong các khu vực an toàn, có kiểm soát ra vào chặt chẽ. Khu vực này cần được trang bị hệ thống camera giám sát hoạt động 24/7 và có cơ chế khóa cửa an toàn để ngăn chặn truy cập trái phép.

3. Mọi hoạt động liên quan đến vòng đời của thiết bị công nghệ thông tin, từ việc cấp phát cho người dùng, thu hồi khi không còn sử dụng, cho đến việc thanh lý thiết bị cũ, đều phải được ghi nhận trong hồ sơ quản lý vận hành. Hồ sơ này

bao gồm thông tin về thiết bị, người nhận/trả, thời gian và các biên bản liên quan.

4. Trong trường hợp chuyển giao quyền quản lý, nâng cấp hoặc thay thế hệ thống thông tin, đơn vị bàn giao có trách nhiệm chuyển giao toàn bộ các thông tin cần thiết cho đơn vị tiếp nhận, bao gồm dữ liệu, các tập tin cấu hình hệ thống, mật khẩu quản trị (được bàn giao an toàn và thay đổi ngay sau đó) và toàn bộ nhật ký hoạt động của hệ thống để bảo đảm tính liên tục và minh bạch trong quản lý.

Chương III
QUY ĐỊNH BẢO VỆ AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN

Điều 11. Bảo vệ an ninh mạng khi sử dụng máy tính và thiết bị ngoại vi

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

a) Chỉ được phép cài đặt các phần mềm hợp lệ (có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở đã được kiểm định, có nguồn gốc rõ ràng) và phải thuộc danh mục phần mềm được phép sử dụng do đơn vị có thẩm quyền của Ủy ban nhân dân tỉnh ban hành (nếu có). Không tự ý cài đặt hoặc gỡ bỏ bất kỳ phần mềm nào khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; đồng thời phải thường xuyên cập nhật phần mềm và hệ điều hành để vá các lỗ hổng bảo mật;

b) Máy tính công vụ phải được cài đặt phần mềm phòng, chống mã độc và cấu hình chế độ tự động cập nhật cơ sở dữ liệu nhận diện mã độc. Người sử dụng phải thực hiện rà quét mã độc trước khi kết nối thiết bị lưu trữ di động với máy tính và trước khi mở các tệp tin được tải xuống từ Internet hoặc sao chép từ thiết bị lưu trữ di động;

c) Khi phát hiện dấu hiệu nhiễm mã độc, người dùng phải dừng việc khai thác, sử dụng thiết bị và báo cáo ngay bộ phận hoặc nhân sự phụ trách an ninh mạng tại đơn vị để xử lý;

d) Chỉ truy cập các trang, cổng thông tin điện tử và ứng dụng trực tuyến phục vụ thực hiện nhiệm vụ, công vụ. Phải sử dụng trình duyệt web được cơ quan có thẩm quyền phê duyệt hoặc khuyến nghị kỹ thuật; không truy cập các liên kết, ứng dụng hoặc tệp tin không xác định rõ danh tính nguồn gửi trên môi trường mạng;

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

2. Trước khi mang máy tính, thiết bị công nghệ thông tin thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để xử lý công việc, cá nhân phải báo cáo và phải được lãnh đạo đơn vị đồng ý, cho phép (ưu tiên bằng văn bản). Trong trường hợp được phép, cá nhân đó phải tuân thủ nghiêm ngặt tất cả các quy định về an ninh mạng đã nêu tại các điểm a, b, c, d, đ khoản 1 Điều này và phải chịu

sự giám sát của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

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

a) Các cơ quan, đơn vị có trách nhiệm bố trí tối thiểu 01 máy tính, 01 máy in và 01 máy sao chụp độc lập, không kết nối và không có lịch sử kết nối với mạng Internet để phục vụ soạn thảo, lưu trữ bí mật nhà nước. Các thiết bị này phải được Công an tỉnh kiểm tra an ninh, dán tem quản lý trước khi đưa vào sử dụng. Không kết nối các thiết bị lưu trữ ngoài, điện thoại thông minh hoặc các thiết bị có tính năng thu phát sóng vào máy tính soạn thảo bí mật nhà nước, trừ thiết bị kỹ thuật chuyên dụng đã được kiểm định và cấp phép;

b) Cán bộ, công chức, viên chức, người lao động được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung bí mật nhà nước chỉ sử dụng các máy tính và thiết bị độc lập đã được bố trí theo quy định tại điểm a, b khoản này. Việc lưu trữ các tài liệu này phải được thực hiện trên các thiết bị lưu trữ riêng biệt (USB an toàn, ổ cứng ngoài,…), được bảo vệ nghiêm ngặt và tuân thủ pháp luật về bảo vệ bí mật nhà nước và cơ yếu;

c) Đối với máy tính soạn thảo văn bản mật, mật khẩu đăng nhập máy tính phải được thiết lập theo quy định tại Điều 6 Quy chế này.

Điều 12. Quản lý trang thiết bị công nghệ thông tin đối với cá nhân

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

a) Mỗi trang thiết bị công nghệ thông tin được cấp phát cho cá nhân hoặc tập thể phải được giao trách nhiệm quản lý và sử dụng rõ ràng. Cá nhân hoặc tập thể được giao phải chịu trách nhiệm về việc bảo quản, sử dụng đúng mục đích và bảo đảm an toàn cho thiết bị đó;

b) Mỗi cơ quan đơn vị phải ban hành các quy định chi tiết về việc sử dụng, bảo quản và bảo vệ trang thiết bị trong các tình huống cụ thể. Điều này bao gồm quy định về việc mang thiết bị ra khỏi cơ quan, các biện pháp bảo mật khi thiết bị chứa dữ liệu nhạy cảm và quy trình cài đặt, cấu hình thiết bị để bảo đảm an toàn;

c) Đối với thiết bị công nghệ thông tin có lưu trữ bí mật nhà nước, dữ liệu cá nhân hoặc thông tin quan trọng: Khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa vĩnh viễn hoặc tiêu hủy dữ liệu để không có khả năng phục hồi. Trường hợp việc xóa dữ liệu không đảm bảo an toàn, phải tiêu hủy vật lý thành phần lưu trữ dữ liệu của thiết bị;

d) Trước khi bàn giao thiết bị hoặc phương tiện lưu trữ dữ liệu để bảo trì, sửa chữa tại các đơn vị bên ngoài hoặc khi thay đổi mục đích sử dụng, phải thực hiện thu hồi, tháo rời thành phần lưu trữ hoặc xóa toàn bộ dữ liệu trên thiết bị. Quy định này không áp dụng đối với trường hợp sửa chữa nhằm mục đích phục hồi dữ liệu;

đ) Các cơ quan, đơn vị có trách nhiệm bảo trì, bảo dưỡng định kỳ hệ thống hạ tầng kỹ thuật; ban hành hướng dẫn quản lý, vận hành và sử dụng an toàn cho người dùng. Thiết lập bộ phận hoặc chỉ định cán bộ chuyên trách thực hiện quản lý, vận hành và định kỳ kiểm tra, bảo trì hệ thống thiết bị đang hoạt động và thiết

bị dự phòng.

2. Trách nhiệm bảo vệ an ninh mạng đối với cá nhân:

a) Cơ quan, đơn vị có trách nhiệm ban hành quy định về bảo vệ an ninh mạng gắn với trách nhiệm của từng vị trí công việc và thực hiện phổ biến cho nhân sự mới khi tuyển dụng hoặc tiếp nhận. Đối với nhân sự được giao quản lý, vận hành hệ thống thông tin trọng yếu hoặc tiếp cận dữ liệu thuộc danh mục bí mật nhà nước, phải thực hiện ký cam kết bảo mật thông tin bằng văn bản hoặc cụ thể hóa trong hợp đồng làm việc, hợp đồng lao động;

b) Các đơn vị phải thường xuyên tổ chức các buổi quán triệt, tập huấn về các quy định liên quan an ninh mạng, nhằm nâng cao nhận thức, trang bị kỹ năng cần thiết trong việc bảo vệ an ninh mạng;

c) Các cơ quan, đơn vị có trách nhiệm ban hành quy trình cấp mới, quản lý và thu hồi tài khoản truy cập hệ thống thông tin. Quy trình phải xác định rõ thẩm quyền, trách nhiệm của từng cá nhân và bảo đảm chỉ cấp quyền truy cập đủ để hoàn thành nhiệm vụ được giao;

d) Khi cán bộ, công chức, viên chức, người lao động chấm dứt hoặc thay đổi vị trí công tác, cơ quan, đơn vị có trách nhiệm rà soát, xác định rõ trách nhiệm của cá nhân đối với các tài sản công nghệ thông tin được giao và thực hiện lập biên bản bàn giao theo quy định; đồng thời phải thực hiện thay đổi hoặc thu hồi toàn bộ quyền truy cập vào các hệ thống thông tin, ứng dụng và dữ liệu để ngăn chặn các hành vi truy cập trái phép.

Điều 13. Xác định cấp độ và phương án bảo vệ an ninh mạng đối với hệ thống thông tin

1. Hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh phải được thực hiện xác định cấp độ và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ tương ứng, tuân thủ quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT, Tiêu chuẩn quốc gia TCVN 11930:2017 về công nghệ thông tin, các kỹ thuật an toàn và yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ và các quy định của pháp luật về bảo vệ an ninh mạng đối với hệ thống thông tin.

2. Trách nhiệm của chủ quản hệ thống thông tin:

a) Chỉ đạo việc phân loại, xác định cấp độ an toàn hệ thống thông tin thuộc phạm vi quản lý;

b) Tổ chức thẩm định và phê duyệt hồ sơ đề xuất cấp độ đối với các hệ thống thông tin theo thẩm quyền;

c) Chỉ đạo, đôn đốc đơn vị vận hành thực hiện các phương án bảo vệ sau khi được phê duyệt.

3. Trách nhiệm của đơn vị vận hành hệ thống thông tin:

a) Chủ trì xây dựng hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông;

b) Trực tiếp triển khai các biện pháp kỹ thuật, quy trình quản lý và vận hành hệ thống theo đúng hồ sơ cấp độ đã được phê duyệt.

4. Trách nhiệm của đơn vị chuyên trách về an ninh mạng:

a) Hướng dẫn, tư vấn kỹ thuật cho chủ quản hệ thống thông tin và đơn vị vận hành trong việc xác định cấp độ; thực hiện đánh giá, kiểm tra việc tuân thủ các phương án bảo vệ theo quy định của pháp luật và Quy chế này;

b) Tổ chức thẩm định và phê duyệt hồ sơ đề xuất cấp độ đối với các hệ thống thông tin theo thẩm quyền.

5. Thẩm quyền và trình tự, thủ tục lập, thẩm định, phê duyệt hồ sơ đề xuất cấp độ

Thực hiện theo quy định Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT, Tiêu chuẩn quốc gia TCVN 11930:2017 và các quy định của pháp luật quy định về bảo vệ an ninh mạng đối với hệ thống thông tin.

6. Phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phải bao gồm các nội dung về phương án kỹ thuật và phương án quản lý tương ứng với từng cấp độ của hệ thống, đảm bảo tính khả thi và khả năng ứng phó với các nguy cơ tấn công mạng.

Điều 14. Giám sát an ninh mạng

1. Hệ thống thông tin phải được giám sát liên tục về trạng thái hoạt động, an toàn và hiệu năng.

a) Hệ thống giám sát phải có cơ chế cảnh báo tự động đến cán bộ quản trị khi phát hiện các dấu hiệu bất thường, bao gồm: Lỗi hệ thống, các cuộc tấn công mạng hoặc khi tải hệ thống vượt ngưỡng định mức cho phép;

b) Khi phát hiện sự cố an ninh mạng, đơn vị vận hành cần thực hiện báo cáo đột xuất theo quy định tại khoản 2 Điều 27 Quy chế này;

c) Đối với trường hợp hệ thống thông tin ngừng hoạt động vì lý do bảo trì, nâng cấp, đơn vị vận hành phải thông báo bằng văn bản cho cơ quan chủ quản và các đơn vị liên quan trước khi thực hiện để phối hợp và chủ động thông tin cho người dân, doanh nghiệp.

2. Đối với các hệ thống thông tin được xác định là quan trọng về an ninh quốc gia, việc giám sát an ninh mạng phải được thực hiện theo các quy định đặc biệt tại Điều 11 của Luật An ninh mạng số 116/2025/QH15.

Điều 15. Ứng cứu sự cố an ninh mạng đối với hệ thống thông tin

1. Đơn vị chuyên trách ứng cứu sự cố an ninh mạng của Ủy ban nhân dân tỉnh là Công an tỉnh (Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao).

2. Các cơ quan, đơn vị có trách nhiệm tự tổ chức xây dựng, phê duyệt kế

hoạch ứng cứu sự cố chi tiết cho các hệ thống thông tin trực tiếp quản lý và tổ chức triển khai kế hoạch sau khi phê duyệt. Thực hiện diễn tập phương án ứng cứu sự cố tối thiểu 01 lần/năm tại hệ thống thông tin của đơn vị.

Điều 16. Kiểm tra, đánh giá an ninh mạng

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Công an tỉnh chủ trì đánh giá việc thực hiện các biện pháp bảo đảm an ninh mạng theo thẩm quyền. Kết quả đánh giá là căn cứ để các cơ quan, đơn vị điều chỉnh, hoàn thiện phương án bảo đảm an ninh mạng của cơ quan, đơn vị.

Điều 17. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng.

1. Công an tỉnh có trách nhiệm tham mưu cho Ủy ban nhân dân tỉnh xây dựng và triển khai các chương trình đào tạo, tuyên truyền về an ninh mạng trên địa bàn tỉnh. Hằng năm, tổ chức đào tạo hoặc cử nhân sự tham gia các khóa đào tạo chuyên sâu về an ninh mạng cho cán bộ làm công tác bảo vệ an ninh mạng của các cơ quan, tổ chức.

2. Các cơ quan, đơn vị có trách nhiệm tự đánh giá, xác định nhu cầu đào tạo về an ninh mạng cho nguồn nhân lực của mình và gửi về Công an tỉnh tổng hợp báo cáo Ủy ban nhân dân tỉnh; đồng thời thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến để nâng cao nhận thức về bảo vệ an ninh mạng đến toàn thể cán bộ, công chức, viên chức, người lao động.

Chương IV
TRÁCH NHIỆM BẢO VỆ AN NINH MẠNG

Điều 18. Trách nhiệm của chủ quản hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị chủ quản hệ thống thông tin theo quy định tại Quy chế này.

2. Chỉ đạo, phân công các đơn vị vận hành các hệ thống thông tin triển khai công tác bảo vệ an ninh mạng trong tất cả các hoạt động liên quan đến hệ thống thông tin.

3. Ban hành và tổ chức thực hiện các quy định, quy trình nội bộ về vận hành, bảo vệ an ninh mạng; đảm bảo tính thống nhất với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện thuận lợi để cơ quan chuyên trách thực hiện công tác kiểm tra, ứng cứu và khắc phục sự cố an ninh mạng theo quy định.

5. Phối hợp chặt chẽ với Công an tỉnh và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các nguy cơ đe dọa an ninh mạng trên địa bàn tỉnh Quảng Ninh.

Điều 19. Trách nhiệm của Công an tỉnh

1. Tham mưu Ủy ban nhân dân tỉnh thực hiện quản lý nhà nước về bảo vệ an ninh mạng đối với hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh theo quy định của pháp luật.

2. Chủ trì, phối hợp với Sở Khoa học và Công nghệ và các cơ quan, đơn vị có liên quan xây dựng kế hoạch phòng ngừa, đấu tranh, ngăn chặn tội phạm lợi dụng hệ thống thông tin 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 trên địa bàn tỉnh Quảng Ninh.

3. Chủ trì, phối hợp Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an và các đơn vị có liên quan hướng dẫn điều phối, xử lý, ứng cứu các sự cố an ninh mạng trên địa bàn tỉnh; cảnh báo các vấn đề về an ninh mạng trong các cơ quan nhà nước trên địa bàn tỉnh.

4. Tham mưu, hướng dẫn và phối hợp tổ chức triển khai các biện pháp bảo vệ an ninh mạng toàn diện, chuyên sâu cho hạ tầng kỹ thuật của Trung tâm dữ liệu tỉnh và các hệ thống thông tin dùng chung của tỉnh.

5. Chủ trì, phối hợp chặt chẽ với các cơ quan liên quan trong việc tham mưu xây dựng kế hoạch và tổ chức kiểm tra định kỳ, kiểm tra đột xuất công tác bảo vệ an ninh mạng; đánh giá việc thực hiện bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ tại các cơ quan, tổ chức.

6. Hướng dẫn, giám sát các đơn vị xây dựng quy chế và thực hiện việc bảo vệ an ninh mạng cho hệ thống thông tin theo quy định; hướng dẫn các cơ quan về khung báo cáo; định kỳ tổng hợp báo cáo Ủy ban nhân dân tỉnh, Bộ Công an và các cơ quan có thẩm quyền về công tác bảo vệ an ninh mạng trên địa bàn tỉnh.

7. Định kỳ tổ chức diễn tập ứng cứu sự cố an ninh mạng trên địa bàn tỉnh, tham gia các hoạt động diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

8. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan điều tra và xử lý các trường hợp vi phạm an ninh mạng theo thẩm quyền và theo quy định của pháp luật.

9. Chủ trì rà soát, yêu cầu gỡ bỏ thông tin vi phạm liên quan đến dữ liệu cá nhân và xâm hại trẻ em trên các hệ thống thông tin thuộc phạm vi quản lý của tỉnh.

10. Chủ trì thẩm định, đánh giá về an ninh mạng đối với các dự án công nghệ thông tin, mô hình chuyển đổi số trên địa bàn tỉnh từ khâu thiết kế đến vận hành, khai thác sử dụng.

Điều 20. Trách nhiệm của Sở Khoa học và Công nghệ

1. Giám sát an ninh mạng cho các hệ thống thông tin lưu ký tại Trung tâm Tích hợp dữ liệu tỉnh; trực tiếp bảo đảm an ninh mạng cho hạ tầng kỹ thuật Trung tâm Tích hợp dữ liệu tỉnh bao gồm máy chủ, thiết bị mạng, hệ thống lưu trữ và các thiết bị liên quan. Đối với các hệ thống thông tin dùng chung của tỉnh lưu trữ tại Trung tâm Tích hợp dữ liệu tỉnh: Sở Khoa học và Công nghệ có trách nhiệm thiết lập đầu mối kỹ thuật thông qua Trung tâm Chuyển đổi số và Công nghệ thông tin để phối hợp với Công an tỉnh và các đơn vị liên quan trong việc thực hiện kiểm tra, giám sát, thu thập nhật ký hệ thống và xử lý sự cố theo đúng chức năng, nhiệm vụ được giao.

2. 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.

3. Thường xuyên cập nhật các nguy cơ gây mất an ninh mạng. Khi phát hiện các nguy cơ tiềm ẩn, phải thông báo cho các cơ quan, đơn vị liên quan biết để chủ động triển khai các biện pháp phòng ngừa, ngăn chặn, xử lý.

4. Chủ trì công tác ứng cứu sự cố an ninh mạng tại Trung tâm tích hợp dữ liệu tỉnh; đồng thời phối hợp chặt chẽ với Công an tỉnh ứng cứu các sự cố mất an ninh mạng trên địa bàn tỉnh.

5. Trực tiếp tham mưu cho Ủy ban nhân dân tỉnh trong việc xây dựng, triển khai và tổ chức thực hiện các giải pháp kỹ thuật, quản lý nhằm bảo vệ an ninh mạng tại Trung tâm Tích hợp dữ liệu tỉnh, bao gồm:

a) Đề xuất đầu tư, nâng cấp hạ tầng kỹ thuật, trang thiết bị an ninh mạng;

b) Triển khai các giải pháp giám sát, cảnh báo, phòng chống tấn công mạng;

c) Xây dựng, cập nhật các quy trình vận hành, phương án bảo vệ an ninh mạng, kế hoạch ứng cứu sự cố và khôi phục hệ thống.

Điều 21. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo vệ an ninh mạng của đơn vị mình.

2. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định.

3. Các cơ quan, đơn vị phải bố trí bộ phận chuyên trách hoặc nhân sự phụ trách an ninh mạng; tổ chức hoặc phối hợp tổ chức tập huấn, bồi dưỡng nghiệp vụ định kỳ cho đội ngũ này. Đồng thời, phải phổ biến quy định về an ninh mạng đến toàn thể cán bộ, công chức, viên chức, người lao động và xác định trách nhiệm bảo đảm an ninh mạng cụ thể đối với từng vị trí công việc.

4. Ban hành quy chế nội bộ về bảo vệ an ninh mạng để xác định rõ trách nhiệm các chủ thể chính liên quan hệ thống thông tin đơn vị đang quản lý; đảm bảo tính thống nhất với Quy chế này và các quy định của pháp luật.

5. Xây dựng và tổ chức thực hiện phương án ứng phó, xử lý sự cố an ninh mạng; bảo đảm sẵn sàng khi xảy ra sự cố. 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 an ninh mạng.

6. Phối hợp chặt chẽ với Công an tỉnh và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các tình huống nguy hiểm về an ninh mạng.

7. Thực hiện chế độ báo cáo quy định tại Điều 27 Quy chế này.

Điều 22. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện xác định cấp độ và phương án bảo vệ an ninh mạng đối với hệ thống thông tin đang vận hành theo quy định tại Điều 13 Quy chế này.

2. Triển khai các biện pháp bảo vệ hệ thống thông tin một cách toàn diện, tuân thủ các quy định của quy chế này, các văn bản pháp luật hiện hành, cũng như các hướng dẫn, tiêu chuẩn và quy chuẩn kỹ thuật về an ninh mạng.

3. Định kỳ hằng năm tổ chức đánh giá việc thực hiện các biện pháp bảo vệ an ninh mạng và báo cáo Ủy ban nhân dân tỉnh kết quả thực hiện; tham mưu phương án điều chỉnh, bổ sung biện pháp bảo vệ đáp ứng yêu cầu bảo đảm an ninh mạng theo quy định.

4. Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo vệ an ninh mạng đối với hệ thống thông tin theo yêu cầu của Ủy ban nhân dân tỉnh hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

5. Phối hợp và thực hiện các yêu cầu của cơ quan liên quan trong hoạt động kiểm tra, đánh giá, điều tra và ứng phó sự cố an ninh mạng theo quy định của pháp luật.

6. Báo cáo sự cố an ninh mạng quy định tại Điều 27 Quy chế này và phối hợp ứng cứu, xử lý sự cố an ninh mạng với các cơ quan, tổ chức liên quan.

Điều 23. Trách nhiệm của Đội ứng cứu sự cố an ninh mạng

1. Đội ứng cứu sự cố an ninh mạng tỉnh Quảng Ninh (gọi tắt là Đội ứng cứu) được Chủ tịch Ủy ban nhân dân tỉnh thành lập và ban hành Quy định về phương án ứng phó khẩn cấp sự cố an ninh mạng trên địa bàn tỉnh.

2. Triển khai các giải pháp nhằm hỗ trợ các cơ quan, tổ chức trên địa bàn tỉnh về công tác bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số.

3. Phối hợp chặt chẽ với các cơ quan chức năng khác thực hiện kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin của các cơ quan, tổ chức trên địa bàn tỉnh.

4. Thường xuyên tổ chức diễn tập ứng cứu sự cố an ninh mạng với các kịch bản khác nhau, giúp các thành viên làm quen với quy trình và cải thiện khả năng phối hợp.

5. Điều phối các hoạt động ứng cứu sự cố về an ninh mạng và tổ chức ứng cứu sự cố an ninh mạng tại các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 24. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Chấp hành Quy chế này, quy chế nội bộ của cơ quan và các quy định của pháp luật về an ninh mạng. Chịu trách nhiệm bảo vệ an ninh mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cá nhân có trách nhiệm tự quản lý, bảo quản, bảo vệ an ninh mạng cho tài khoản người dùng, các thiết bị công nghệ thông tin (máy tính, điện thoại, USB,…) mà mình được giao sử dụng;

c) Khi phát hiện sự cố an ninh mạng, phải thông báo ngay cho người đứng đầu cơ quan, đơn vị và bộ phận hoặc nhân sự phụ trách an ninh mạng tại đơn vị;

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn về an ninh mạng do Ủy ban nhân dân tỉnh chỉ đạo hoặc các cơ quan chuyên trách về an ninh mạng tổ chức nhằm nâng cao kiến thức và kỹ năng bảo mật.

2. Trách nhiệm của cán bộ phụ trách công nghệ thông tin/an ninh mạng:

Ngoài các quy định tại Khoản 1 Điều này, cán bộ phụ trách công nghệ thông tin/an ninh mạng có trách nhiệm:

a) Chủ trì tham mưu cho lãnh đạo cơ quan, đơn vị trong việc triển khai và thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến an ninh mạng;

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy chế nội bộ về quản lý, sử dụng, khai thác và bảo đảm an ninh mạng đối với hệ thống thông tin của đơn vị;

c) Trực tiếp thiết lập hoặc tham mưu các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức,

người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo vệ an ninh mạng trong hoạt động ứng dụng công nghệ thông tin;

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

Chương V
TỔ CHỨC THỰC HIỆN

Điều 25. Kinh phí thực hiện

1. Kinh phí bảo đảm an ninh mạng được bố trí từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Các cơ quan, đơn vị hằng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an ninh mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm đối với các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an ninh an toàn mạng và đưa vào dự toán chi năm sau để triển khai thực hiện.

Điều 26. Công tác kiểm tra

1. Cơ quan, đơn vị có trách nhiệm định kỳ kiểm tra, tự đánh giá công tác bảo vệ an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý. Kết quả tự kiểm tra, đánh giá phải được lưu trữ hồ sơ và là căn cứ để phục vụ công tác thanh tra, kiểm tra của cơ quan chuyên trách.

2. Công an tỉnh chủ trì, tham mưu Ủy ban nhân dân tỉnh tổ chức kiểm tra việc thực hiện Quy chế này đối với các cơ quan, đơn vị trên địa bàn tỉnh; tổng hợp, báo cáo kết quả và đề xuất biện pháp xử lý vi phạm (nếu có) theo quy định.

Điều 27. Chế độ, nội dung báo cáo

1. Báo cáo định kỳ

a) Nội dung báo cáo: Bao gồm kết quả thực hiện các biện pháp bảo vệ an ninh mạng theo quy định tại Quy chế này và các nội dung chỉnh sửa, bổ sung quy chế bảo vệ an ninh mạng nội bộ của cơ quan, đơn vị (nếu có);

b) Thời hạn gửi báo cáo: Báo cáo 06 tháng (trước ngày 15 tháng 7); Báo cáo năm (trước ngày 15 tháng 12).

2. Báo cáo đột xuất

a) Khi phát hiện dấu hiệu tấn công mạng hoặc sự cố an ninh mạng, đơn vị vận hành phải thông báo cho Công an tỉnh trong vòng 01 giờ (đối với sự cố nghiêm trọng) hoặc 04 giờ (đối với sự cố thông thường) kể từ khi phát hiện;

b) Hình thức thông báo: Ưu tiên các hình thức thông báo nhanh qua đường dây nóng (Hotline), tin nhắn hoặc các ứng dụng trao đổi thông tin an toàn do Công an tỉnh thiết lập để kịp thời xử lý. Sau khi ổn định tình hình, đơn vị phải gửi văn bản báo cáo chính thức trong vòng 24 giờ;

c) Nội dung thông báo sơ bộ: Bao gồm loại hình tấn công (DDoS, mã độc, chiếm quyền,...), hệ thống bị ảnh hưởng, thời điểm phát hiện và các biện pháp xử lý ban đầu đã thực hiện;

d) Các trường hợp đột xuất khác theo yêu cầu của Ủy ban nhân dân tỉnh.

Điều 28. Trách nhiệm thi hành

1. Thủ trưởng sở, ban, ngành; Chủ tịch Ủy ban nhân dân các xã, phường, đặc khu có trách nhiệm triển khai thực hiện, phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức, người lao động trong đơn vị Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế tại đơn vị; chịu trách nhiệm trước pháp luật và trước Ủy ban nhân dân tỉnh về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị.

2. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, các đơn vị gửi về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định./.