ỦY BAN NHÂN DÂN TỈNH AN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1049/QĐ-UBND	*An Giang, ngày 30 tháng 3 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế vận hành, bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh An Giang

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH AN GIANG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16 tháng 6 năm 2025;

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

Căn cứ Luật Viễn thông số 24/2023/QH15 ngày 24 tháng 11 năm 2023;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

Căn cứ 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;

Căn cứ 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 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ về quy định về định danh và xác thực điện tử;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ uy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 19/2021/TT-BTTTT ngày 03 tháng 12 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục sản phẩm công nghệ thông tin trọng điểm;

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 dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 46/2022/TT-BCA ngày 04 tháng 11 năm 2022 của Bộ trưởng Bộ Công an quy định về việc kết nối, chia sẻ và khai thác thông tin giữa Cơ sở dữ liệu quốc gia về dân cư với cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 122/TTr-CAT ngày 11 tháng 3 năm 2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế vận hành, bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh An Giang.

Điều 2. Giao Công an tỉnh chủ trì, phối hợp với các sở, ban, ngành tỉnh, Ủy ban nhân dân các xã, phường, đặc khu và các tổ chức, cá nhân có liên quan hướng dẫn, triển khai thực hiện Quy chế này.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký.

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

Nơi nhận:
- Như Điều 3;
- CT và các PCT UBND tỉnh;
- Sở, ban, ngành tỉnh;
- Lãnh đạo VP UBND tỉnh;
- UBND xã, phường, đặc khu;
- Phòng KGVX;
- Trung tâm CBTH;
- Lưu: VT, ntgiang.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH AN GIANG

Nguyễn Thanh Phong

ỦY BAN NHÂN DÂN TỈNH AN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ VẬN HÀNH, BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN TỈNH AN GIANG

(Kèm theo Quyết định số 1049/QĐ-UBND ngày 30 tháng 3 năm 2026 của Chủ tịch Ủy ban nhân dân tỉnh An Giang)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh:

Quy chế này quy định về vận hành, bảo đảm an ninh mạng (ANM), an toàn thông tin (ATTT) đối với hệ thống thông tin trên địa bàn tỉnh.

2. Đối tượng áp dụng:

- Các sở, ban, ngành, Ủy ban nhân dân (UBND) cấp xã, phường, đặc khu, đơn vị sự nghiệp, cán bộ, công chức, viên chức, người lao động và các tổ chức cá nhân có liên quan đến việc quản lý, vận hành, khai thác hệ thống thông tin trên địa bàn tỉnh.

- Các cơ quan, tổ chức, doanh nghiệp, cá nhân cung cấp dịch vụ công nghệ thông tin (CNTT), Internet, ATTT mạng hoặc có tham gia vào các hoạt động chuyển đổi số của các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 2. Giải thích từ ngữ

1. An ninh mạng là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước (BMNN), quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. An toàn thông tin là sự bảo vệ thông tin số và các hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và thiết bị ngoại vi trao đổi thông tin trên mạng.

Điều 3. Nguyên tắc bảo đảm an ninh mạng, an toàn thông tin

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

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 8 Luật An ninh mạng.

2. Các hành vi bị nghiêm cấm về an toàn thông tin quy định tại Điều 7 Luật An toàn thông tin.

3. Các hành vi bị nghiêm cấm về an toàn thông tin quy định tại Điều 5 Luật Bảo vệ bí mật nhà nước.

4. Các hành vi bị nghiêm cấm về an toàn thông tin quy định tại Điều 7 Luật Bảo vệ dữ liệu cá nhân.

5. Hành vi nghiêm cấm khác về an ninh mạng, an toàn thông tin theo quy định của pháp luật.

Chương II
QUY ĐỊNH BẢO ĐẢM ANM, ATTT

Điều 5. Bảo đảm ANM, ATTT khi sử dụng máy tính, thiết bị ngoại vi và hệ thống mạng

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

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở được đầu tư (hoặc thuê dịch vụ) có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do đơn vị có thẩm quyền của UBND tỉnh ban hành (nếu có); không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

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

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

2. Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư

điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động, tự động điền.

3. Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...) và thay đổi mật khẩu tối thiểu 4 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt trên máy tính.

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

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

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

a) Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý (trong trường hợp thiết bị sử dụng chung), sử dụng trang thiết bị công nghệ thông tin phải tuân thủ các quy định sau:

- Các máy tính dành cho công chức, viên chức, người lao động tiếp nhận hồ sơ tại Bộ phận tiếp nhận và trả kết quả các cấp cần phải bảo đảm trang bị các phần mềm có bản quyền: hệ điều hành, phần mềm soạn văn bản và phần mềm phòng chống mã độc (kết nối về Trung tâm giám sát an toàn không gian mạng quốc gia).

- Tuyệt đối không tự ý lắp đặt thêm thiết bị; không sử dụng phần mềm bên thứ ba hoặc công cụ tự nghiên cứu, phát triển riêng nhưng chưa được cơ quan chuyên trách về ATTT mạng kiểm tra, đánh giá an ninh, ATTT để tra cứu, khai thác Cơ sở dữ liệu quốc gia về dân cư.

- Các thiết bị, máy tính phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ đệm và phiên đăng nhập được lưu trong trình duyệt trên máy tính.

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

- Báo cáo và phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép trước khi mang máy tính, thiết bị CNTT có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ khoản này và chịu sự giám sát của bộ phận phụ trách, chuyên trách về ATTT mạng của cơ quan, đơn vị.

- Thiết bị có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

b) Thực hiện đúng quy định việc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt, cấu hình thiết bị mã hóa.

c) Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

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

2. Quản lý, bảo vệ an ninh mạng các hệ thống thông tin của đơn vị:

a) Khi thực hiện mua sắm trang thiết bị, máy tính liên quan đến bí mật nhà nước, phải được kiểm định ATTT của cơ quan có thẩm quyền trước khi đưa vào sử dụng quy định tại Điều 11 và Điều 12, Luật An ninh mạng

b) Khuyến khích các cơ quan, đơn vị đầu tư, mua sắm thiết bị CNTT sản xuất trong nước. Không mua sắm thiết bị CNTT thuộc danh mục sản phẩm, hàng hóa có khả năng gây mất ATTT theo các thông báo của Công an tỉnh và Sở Khoa học và Công nghệ được quy định tại Điều 3, Luật An ninh mạng.

c) Quản lý thuê dịch vụ CNTT

- Xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm ATTT khi ký kết hợp đồng thuê. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm ATTT và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

- Cơ quan, đơn vị chủ trì thuê dịch vụ CNTT phải có trách nhiệm

+ Quản lý chặt chẽ thông tin, dữ liệu phát sinh từ dịch vụ thuê, không cho phép bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

+ 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 ATTT theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan.

+ 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.

+ Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm ATTT phải tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm; thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ cho cơ quan chức năng để phối hợp xử lý vi phạm theo quy định pháp luật; thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ; 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.

+ Yêu cầu bên cung cấp dịch vụ phải có trách nhiệm phối hợp xây dựng hồ sơ ATTT theo cấp độ được quy định tại Nghị định số 85/2016/NĐ-CP.

+ Yêu cầu bên cung cấp dịch vụ phải đảm bảo khả năng kết nối, mở rộng, chia sẻ dữ liệu với các hệ thống thông tin dùng chung của tỉnh; tuân thủ Kiến trúc chính quyền điện tử tỉnh An Giang; Khung kiến trúc chính phủ điện tử Việt Nam hiện hành.

+ Trách nhiệm của cơ quan, đơn vị chủ trì thuê khi kết thúc hợp đồng sử dụng dịch vụ phải 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. 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.

- Đơn vị sử dụng dịch vụ khi có thay đổi về mặt hệ thống, ứng dụng, mã nguồn và chức năng hệ thống phần mềm phục vụ kết nối cơ sở dữ liệu quốc gia về dân cư cần báo cáo về Sở Khoa học và Công nghệ và Công an tỉnh để tổng hợp báo cáo Tổ chức có liên quan về triển khai và đảm bảo an toàn cơ sở dữ liệu quốc gia về dân cư trên địa bàn tỉnh để phối hợp đơn vị nghiệp vụ Bộ Công an, Bộ Khoa học và Công nghệ thực hiện kiểm tra an ninh, ATTT đảm bảo đáp ứng các tiêu chí theo hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ và quy định pháp luật.

- Có phương án hợp đồng chặt chẽ với nhà cung cấp dịch vụ và có cơ chế quản lý đối với các tài khoản thuộc các hệ thống thuê dịch vụ hạ tầng của nhà cung cấp dịch vụ, tránh tình trạng ủy quyền toàn bộ việc quản trị, vận hành hệ thống cho nhà cung cấp dịch vụ liên quan đến khai thác, sử dụng cơ sở dữ liệu quốc gia về dân cư.

3. Các cơ quan, đơn vị khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định của Luật An toàn thông tin mạng và Luật An ninh mạng và các quy định sau:

a) Phải xây dựng các yêu cầu, trách nhiệm bảo đảm ANM, ATTT đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm ANM, ATTT tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

b) Thường xuyên tổ chức quán triệt các quy định về ANM, ATTT, nhằm nâng cao nhận thức về trách nhiệm bảo đảm ANM, ATTT của từng cá nhân trong đơn vị.

c) Các hệ thống thông tin phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

d) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu phải:

- Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao trong vòng không quá 05 ngày làm việc, cơ quan, đơn vị quản lý.

- Thay đổi hoặc thu hồi các máy móc, thiết bị CNTT liên quan theo quy định; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị nền tảng, phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

4. 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 mạnh, 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 3 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 sử dụng, cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng, phân lớp, phân vùng mạng riêng, tách biệt mạng LAN nội bộ cơ quan, giới hạn băng thông và có mật khẩu truy cập phù hợp đối với đối tượng này. Trường hợp người ngoài cơ quan, đơn vị muốn sử dụng mạng không dây nội bộ cơ quan thì phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép.

Điều 7. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản, chữ ký số và thiết bị có liên quan

a) Khi được cấp tài khoản, chữ ký số lần đầu cho người dùng truy nhập, người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu; chủ tài khoản, chữ ký số không chia sẻ, không giao quyền tài khoản, không giao chứng thư chữ ký số, mật khẩu truy nhập thiết bị có liên quan cho người khác.

b) Các Cổng/Trang thông tin điện tử phải được cấu hình truy cập sử dụng theo tiêu chuẩn kết nối giao thức truyền tải siêu văn bản (HTTPS - HyperText Transfer Protocol Secure). 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) Tài khoản thư điện tử công vụ (https://mail.angiang.gov.vn), chữ ký số chuyên dùng công vụ chỉ 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.

2. Đối với các dữ liệu quan trọng, các cơ quan, đơn vị cần lên phương án sao lưu dự phòng theo phương án sao lưu tối thiểu theo quy tắc 3-2-1, bao gồm: giữ ít nhất ba bản sao dữ liệu, lưu trữ hai bản sao trên các phương tiện lưu trữ khác nhau, lưu trữ một bản sao lưu ngoại vi. Các cơ quan, đơn vị khi thuê dịch vụ cần yêu cầu nhà cung cấp dịch vụ thiết lập các giải pháp sao lưu tự động đối với dữ liệu trên máy chủ cơ sở dữ liệu và máy chủ ứng dụng và xây dựng các kịch bản có sẵn để khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục khi xảy ra sự cố. 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).

3. Tên miền phục vụ cho tổ chức, cơ quan chính phủ trên địa bàn tỉnh (*.angiang.gov.vn) khi không còn sử dụng, các cơ quan, đơn vị có văn bản gửi đến Sở Khoa học và Công nghệ để đề nghị thu hồi tên miền; các hệ thống thông tin không sử dụng, chủ quản hệ thống thông tin thực hiện việc thu hồi máy chủ, thu hồi ứng dụng và thực hiện việc lưu trữ dữ liệu ra thiết bị lưu trữ ngoài và yêu cầu cơ quan, đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

4. Cơ quan, đơn vị quản lý máy chủ, máy trạm 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. Trường hợp thiết bị lưu trữ cần bảo hành, bảo dưỡng, sửa chữa phải sao lưu dữ liệu trên thiết bị sang thiết bị lưu trữ khác 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.

5. Thông tin, dữ liệu thuộc phạm vi BMNN phải được quản lý theo quy định Luật bảo vệ BMNN và các văn bản hướng dẫn có liên quan đến bảo vệ BMNN

a) Quy định về soạn thảo, in ấn, phát hành và sao, chụp tài liệu mật

Không được soạn thảo, lưu giữ, chuyển giao, đăng tải, phát hành thông tin, có chứa nội dung BMNN trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính (trừ mạng LAN độc lập), mạng viễn thông, trừ trường hợp lưu giữ BMNN theo quy định của pháp luật về cơ yếu và các quy định khác có liên quan.

b) Không được in, sao, chụp tài liệu BMNN trên các thiết bị kết nối mạng Internet, mạng máy tính, mạng viễn thông.

c) Phải bố trí ít nhất 01 máy tính độc lập riêng, không kết nối mạng nội bộ và mạng Internet, thực hiện kiểm tra an toàn thông tin máy tính trước khi đưa vào sử dụng và được bảo quản theo chế độ mật, dùng để quản lý, soạn thảo, lưu trữ các văn bản, tài liệu mật của nhà nước theo quy định.

d) Khi sửa chữa, khắc phục sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị 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.

e) Trước khi thanh lý, chuyển mục đích sử dụng các máy tính hoặc các thiết bị khác trong các cơ quan nhà nước có mang thông tin mật, phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu BMNN trên các thiết bị.

Điều 8. Bảo vệ dữ liệu cá nhân

1. Công chức, viên chức, người lao động có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại Luật Bảo vệ dữ liệu cá nhân và văn bản pháp luật có liên quan.

2. Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị trên địa bàn tỉnh, có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh. Thực hiện bảo mật tài khoản truy cập các hệ thống, không chia sẻ tài khoản, mật khẩu, thông tin cá nhân với người khác nếu trường hợp bận công tác thì phải có giấy ủy quyền việc quản lý, sử dụng tài khoản ghi rõ thời gian ủy quyền, nêu rõ trách nhiệm của các bên.

b) Phải thực hiện việc đổi mật khẩu mạnh ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị; Thực hiện cơ chế xác thực hai hay nhiều yếu tố xác thực khi đăng nhập (nếu hệ thống có hỗ trợ tính năng), định kỳ thay đổi mật khẩu ít nhất 04 tháng một lần.

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập internet công cộng, phải bảo đảm sử dụng tiêu chuẩn kết nối giao thức truyền tải siêu văn bản **(**HTTPS - HyperText Transfer Protocol Secure) khi đăng nhập các tài khoản, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

3. Các cơ quan, đơn vị khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung quy định tại Điều 36, 37 Luật bảo vệ dữ liệu cá nhân và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi Công chức, viên chức, người lao động đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các máy móc, thiết bị CNTT liên quan theo quy định; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị nền tảng, phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

c) Việc cấp phát, đóng, khóa tài khoản công chức, viên chức, người lao động có quyền tra cứu thông tin trên Cơ sở dữ liệu quốc gia về dân cư liên quan đến các hệ thống thông tin, nền tảng ứng dụng dùng chung của tỉnh An Giang:

- Các cơ quan, đơn vị có văn bản gửi về Phòng Cảnh sát quản lý hành chính về trật tự xã hội – Công an tỉnh An Giang khi có thông tin liên quan đến việc thêm mới, đóng, khóa tài khoản có quyền tra cứu thông tin công dân.

- Công chức, viên chức, người lao động thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu thì trong vòng không quá 05 ngày làm việc, cơ quan, đơn vị quản lý công chức, viên chức, người lao động đó phải thông báo cho cơ quan, đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng trên hệ thống thông tin, nền tảng ứng dụng dùng chung của tỉnh.

4. Công an tỉnh thực hiện công tác quản lý nhà nước về bảo vệ dữ liệu cá nhân theo các nội dung quy định tại Điều 36 của Luật Bảo vệ dữ liệu cá nhân.

5. Thực hiện các hoạt động bảo vệ dữ liệu cá nhân theo quy định tại Chương II của Luật Bảo vệ dữ liệu cá nhân.

Điều 9. Xác định cấp độ và phương án bảo đảm ANM, ATTT hệ thống thông tin

1. Người đứng đầu cơ quan, đơn vị trực tiếp chỉ đạo và phụ trách công tác bảo đảm ATTT mạng; chịu trách nhiệm trước pháp luật và Chủ tịch UBND tỉnh nếu để hệ thống thông tin thuộc phạm vi quản lý không bảo đảm ATTT mạng, để xảy ra sự cố nghiêm trọng.

2. Việc đảm bảo an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, đơn vị phải 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 của tiêu chuẩn TCVN, các quy định có liên quan khác và xác định cấp độ ATTT theo Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, bao gồm 05 cấp độ: Cấp độ 1, Cấp độ 2, Cấp độ 3, Cấp độ 4 và Cấp độ 5, tương ứng với mức độ ảnh hưởng khi xảy ra sự cố ATTT đối với hoạt động của cơ quan, đơn vị. Trong đó, Công an tỉnh là đơn vị chuyên trách an toàn thông tin của UBND tỉnh, thực hiện thẩm định hồ sơ từ cấp độ 1 đến cấp độ 3 và phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin cấp độ 1 và cấp độ 2 theo Điều 12, Nghị định số 85/2016/NĐ-CP.

3. Trên cơ sở cấp độ ATTT đã được phê duyệt, đơn vị quản lý, vận hành hệ thống thông tin có trách nhiệm xây dựng, triển khai và duy trì phương án bảo đảm ANM, an toàn hệ thống thông tin tương ứng, bao gồm các biện pháp quản lý, bảo vệ BMNN, biện pháp kỹ thuật, biện pháp bảo vệ vật lý, phương án sao lưu, khôi phục dữ liệu và phương án ứng cứu, xử lý sự cố ATTT, bảo đảm đáp ứng yêu cầu tối thiểu theo cấp độ ATTT của hệ thống thông tin theo quy định của pháp luật.

4. Việc rà soát, cập nhật cấp độ và phương án bảo đảm ANM, an toàn hệ thống thông tin được thực hiện khi có thay đổi về chức năng, phạm vi, quy mô, công nghệ của hệ thống thông tin hoặc theo yêu cầu của cơ quan, đơn vị có thẩm quyền.

5. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp phải được kiểm thử về tính an toàn, bảo mật trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng theo quy định tại Điều 10 Thông tư số 16/2024/TT-BTTTT ngày 30 tháng 12 năm 2024 của Bộ Khoa học và Công nghệ 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.

6. Lưu trữ nhật ký kết nối, chia sẻ, khai thác thông tin với Cơ sở dữ liệu quốc gia về dân cư tuân thủ theo quy định tại Điều 8 của Thông tư số 46/2022/TT-BCA ngày 04 tháng 11 năm 2022 của Bộ trưởng Bộ Công an quy định về việc kết nối, chia sẻ và khai thác thông tin giữa cơ sở dữ liệu quốc gia về

dân cư với Cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác.

7. Hệ thống thông tin có kết nối, chia sẻ và khai thác thông tin với Cơ sở dữ liệu quốc gia về dân cư tại các cơ quan, đơn vị, doanh nghiệp phải được thực hiện theo Chương II của Thông tư số 46/2022/TT-BCA ngày 04 tháng 11 năm 2022 của Bộ trưởng Bộ Công an quy định về việc kết nối, chia sẻ và khai thác thông tin giữa cơ sở dữ liệu quốc gia về dân cư với Cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác.

Điều 10. Giám sát ANM, ATTT

1. Các hệ thống thông tin phải được thực hiện giám sát ANM, ATTT và kết nối, chia sẻ kết quả giám sát về Trung tâm an ninh mạng tỉnh An Giang. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với Công an tỉnh tổ chức thực hiện việc giám sát hệ thống thông tin theo Luật An toàn thông tin mạng.

2. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, thực hiện giám sát ANM theo Điều 14 Luật An ninh mạng.

3. Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại cơ quan, đơn vị. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

4. Thủ trưởng các cơ quan, đơn vị thực hiện thành lập Tổ giám sát và xử lý sự cố ATTT mạng tại các cơ quan, đơn vị. Trường hợp không đủ điều kiện thành lập Tổ giám sát và xử lý sự cố ATTT mạng thì việc giám sát và xử lý sự cố ATTT mạng sẽ do bộ phận phụ trách về ATTT mạng, chuyển đổi số của cơ quan, đơn vị thực thiện.

Điều 11. Ứng cứu sự cố an toàn hệ thống thông tin

1. Đơn vị chuyên trách ứng cứu khẩn cấp sự cố ANM, ATTT là Công an tỉnh (Phòng ANM và phòng, chống tội phạm sử dụng công nghệ cao) theo Quyết định số 1903/QĐ-UBND ngày 13/11/2025 của UBND tỉnh về việc thành lập Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh An Giang có trách nhiệm:

a) Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng, ứng phó sự cố ATTT mạng.

b) Xây dựng quy trình ứng cứu sự cố ATTT mạng 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 ATTT; yêu cầu bên cung cấp dịch vụ 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) Tổ chức diễn tập phương án xử lý sự cố ATTT.

2. Kế hoạch, phương án ứng phó sự cố bảo đảm ANM, ATTT: Các cơ quan, đơn vị tổ chức xây dựng, phê duyệt kế hoạch và phương án ứng phó sự cố ANM cho các hệ thống, ưu tiên các hệ thống thông tin quan trọng và các loại sự cố ANM ảnh hưởng đến các yếu tố quan trọng của hệ thống (ví dụ ransomware; lộ lọt dữ liệu đối với các hệ thống văn bản quan trọng, lưu trữ dữ liệu cá nhân; deface đối với các cổng thông tin;...)

3. Phân nhóm sự cố ATTT

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.

4. 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.

5. Quy trình phối hợp ứng cứu sự cố

a) Bước 1: Khi phát hiện dấu hiệu bất thường trong hệ thống (thông qua giám sát, cảnh báo kỹ thuật hoặc phản ánh từ người dùng...), chủ quản hệ thống thông tin phải kịp thời kích hoạt quy trình ứng phó sự cố. Toàn bộ cán bộ, nhân viên có trách nhiệm thông báo sự cố tới đội quản trị hệ thống và đội phản ứng sự cố nội bộ (nếu đã được thành lập).

b) Bước 2: Ngay sau khi phát hiện sự cố, chủ quản hệ thống thông tin (Đội ứng cứu cố nội bộ) có trách nhiệm tiến hành ứng phó ban đầu nhằm hạn chế mức độ ảnh hưởng và cô lập khu vực bị tác động, đồng thời giữ nguyên hiện trạng hệ thống và thực hiện theo hướng dẫn của Phòng ANM và phòng, chống tội phạm sử dụng công nghệ cao để phục vụ công tác điều tra (Phòng ANM và phòng, chống tội phạm sử dụng công nghệ cao có trách nhiệm yêu cầu thực hiện

việc này đối với các sự cố nghi ngờ do tấn công mạng). Các hành động ưu tiên bao gồm:

- Cách ly hệ thống bị ảnh hưởng bằng cách ngắt kết nối mạng (nhưng không tắt nguồn hoặc khởi động lại thiết bị); ghi nhận các thông tin tại thời điểm xảy ra sự cố (tiến trình đang chạy, kết nối mạng, IP truy cập...); sao lưu nhật ký hệ thống (log), các file nghỉ ngờ, ảnh ổ đĩa, dữ liệu RAM theo đúng quy trình pháp y số.

- Đối với hệ thống không thể cách ly hoàn toàn, tìm các phương án chặn lọc kết nối của hệ thống với các IP nghi ngờ là độc hại.

- Trường hợp cần duy trì và khôi phục hoạt động của hệ thống bị ảnh hưởng, tiến hành việc chuyển sang hệ thống dự phòng hoặc khôi phục trên hạ tầng mới từ các bản sao lưu.

- Trong trường hợp có sự cố ở mức độ cao, nghiêm trọng, khẩn cấp vượt quá khả năng khắc phục của cơ quan, đơn vị hoặc có yếu tố tấn công có chủ đích không đủ năng lực tự xử lý, chủ quản hệ thống thông tin phải đề nghị lực lượng chuyên trách về ANM trực tiếp phối hợp điều tra, hoặc chủ trì điều phối các doanh nghiệp ATTT chuyên nghiệp hỗ trợ xử lý. Khi đó, Phòng ANM và phòng, chống tội phạm sử dụng công nghệ cao triệu tập Đội ứng cứu sự cố ATTT mạng tỉnh để hỗ trợ chủ quản xử lý sự cố và phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao – Bộ Công an (VNCERT) trong trường hợp không xử lý được các vấn đề phức tạp, nghiêm trọng để nhận sự hỗ trợ.

c) Bước 3: Sau khi sự cố đã được xử lý và hệ thống đi vào vận hành ổn định, chủ quản hệ thống thông tin có trách nhiệm hoàn thiện báo cáo kết quả xử lý sự cố gửi về lực lượng chuyên trách ANM. Báo cáo cần nêu rõ nguyên nhân, quy trình xử lý, các biện pháp đã triển khai, đánh giá thiệt hại và đề xuất khuyến nghị phòng ngừa. Đồng thời, chủ quản hệ thống thông tin phải tiến hành rút kinh nghiệm nội bộ, cập nhật quy trình ứng phó, điều chỉnh chính sách ATTT, bổ sung công cụ giám sát, khắc phục các lỗ hổng bảo mật và tổ chức tập huấn lại cho các bộ phận liên quan. Hồ sơ sự cố phải được lưu trữ đầy đủ, có chữ ký xác nhận, và bảo quản trong thời gian tối thiểu ba năm để phục vụ thanh tra, kiểm tra khi cần thiết.

Điều 12. Kiểm tra, đánh giá ATTT

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 ATTT 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. Nội dung, hình thức, đối tượng thẩm quyền kiểm tra, đánh giá hệ thống thông tin

a) Nội dung kiểm tra, đánh giá

- Kiểm tra việc thực hiện 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 theo cấp độ; kiểm tra hiệu quả của các biện pháp, phương án bảo đảm, ứng phó, khắc phục sự cố ATTT mạng.

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

- Kiểm tra công tác giám sát ATTT và ứng phó khi xảy ra sự cố ATTT.

- Kiểm tra, đánh giá các nội dung khác theo quy định của chủ quản hệ thống thông tin.

b) Hình thức kiểm tra, đánh giá

- Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin và đơn vị chuyên trách về ATTT của tỉnh.

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

c) Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin.

3. Công an tỉnh thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm ATTT theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm ATTT cho phù hợp.

Điều 13. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về ANM, ATTT

1. Các cơ quan, đơn vị xác định nhu cầu về đào tạo cho nguồn nhân lực để bảo đảm ATTT tại đơn vị mình gửi Công an tỉnh tổng hợp.

2. Công an tỉnh tổ chức đào tạo, bồi dưỡng nghiệp vụ về ATTT cho cán bộ công nghệ thông tin, cán bộ chuyên trách ANM, ATTT các đơn vị trực thuộc; đào tạo cơ bản về ATTT cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị.

3. Sở, ban, ngành tỉnh, UBND các xã/phường/đặc khu và các cơ quan, tổ chức, doanh nghiệp cung cấp dịch vụ CNTT, Internet, ATTT mạng hoặc có tham gia vào các hoạt động chuyển đổi số của các cơ quan, đơn vị trên địa bàn tỉnh phải bảo đảm nguồn nhân lực bảo vệ an ninh mạng và thực hiện tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng theo quy định tại Điều 31 và 32 Luật An ninh mạng.

4. Các cơ quan, đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể cán bộ, công chức, viên chức và người lao động tại đơn vị.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm của Công an tỉnh

1. 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, gây mất an ninh trật tự và ANM, ATTT trong cơ quan nhà nước trên địa bàn tỉnh. Tham mưu giúp UBND tỉnh về công tác bảo đảm ANM, ATTT trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm ANM, ATTT cho các hệ thống thông tin của tỉnh.

2. Chỉ đạo, tổ chức bảo đảm ANM, ATTT cho hạ tầng kỹ thuật của Trung tâm dữ liệu tỉnh.

3. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao; chịu trách nhiệm quản lý, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống mạng gây hại đến ANM, ATTT của cơ quan, cá nhân.

4. Phối hợp với Văn phòng UBND tỉnh, Sở Khoa học và Công nghệ trong công tác thanh tra, kiểm tra về ANM, ATTT.

5. Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác ANM, ATTT trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định.

6. Xây dựng và triển khai các chương trình đào tạo, tuyên truyền về ANM, ATTT trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

7. Định kỳ tổ chức diễn tập ứng cứu sự cố ANM, ATTT trên địa bàn tỉnh, tham gia diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

8. Chỉ đạo, hướng dẫn về nghiệp vụ về bảo đảm ANM, ATTT; hỗ trợ giải quyết sự cố khi có yêu cầu.

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

10. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy định nội bộ và thực hiện việc bảo đảm ANM, ATTT cho hệ thống thông tin theo quy định của Nhà nước.

11. Tổng hợp và báo cáo về tình hình ANM, ATTT theo định kỳ cho Bộ Công an, UBND tỉnh và các cơ quan, đơn vị có liên quan.

Điều 15. Trách nhiệm của các cơ quan

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 UBND tỉnh trong công tác bảo đảm ANM, ATTT của đơn vị mình.

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

3. Phân công bộ phận hoặc cán bộ chuyên trách bảo đảm ANM, ATTT của đơn vị; tạo điều kiện để các cán bộ phụ trách ANM, ATTT được học tập, nâng cao trình độ về ANM, ATTT; thường xuyên tổ chức quán triệt các quy định về ANM, ATTT trong cơ quan; xác định các yêu cầu, trách nhiệm đảm bảo ANM, ATTT đối với các vị trí cần tuyển dụng hoặc phân công.

4. Ban hành quy chế nội bộ về bảo đảm ANM, ATTT phù hợp với Quy chế này và các quy định của pháp luật.

5. 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 ANM, ATTT kịp thời, nhanh chóng và đạt hiệu quả.

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 hoạt động xâm phạm ANM, ATTT.

7. Định kỳ 06 tháng (trước ngày 15/6) và hằng năm (trước ngày 15/12) báo cáo tình hình ANM, ATTT của cơ quan theo quy định gửi về Công an tỉnh tổng hợp, báo cáo UBND tỉnh.

Điều 16. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Trách nhiệm của các cơ quan, đơn vị được cấp có thẩm quyền giao vận hành hệ thống thông tin:

a) Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP.

b) Thực hiện bảo vệ hệ thống thông tin theo Quy chế này, các quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn ATTT.

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm ANM, ATTT, báo cáo UBND tỉnh điều chỉnh nếu cần thiết.

d) Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của UBND tỉnh hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

đ) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan, của Công an tỉnh trong công tác bảo đảm ANM, ATTT.

e) Kịp thời thông báo sự cố ANM, ATTT và phối hợp ứng cứu xử lý sự cố ANM, ATTT với các cơ quan, đơn vị liên quan.

2. Trường hợp hệ thống thông tin do các cơ quan thực hiện đầu tư: Cơ quan chủ đầu tư đóng vai trò là Đơn vị vận hành hệ thống thông tin thực hiện các quy định tại Khoản 1 Điều này.

3. Trường hợp hệ thống thông tin do các cơ quan thực hiện thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Đơn vị cung cấp dịch vụ đóng vai trò là Đơn vị vận hành hệ thống thông tin, có trách nhiệm thực hiện các quy định tại Khoản 1 Điều này; phối hợp chặt chẽ với cơ quan chủ trì thuê dịch vụ trong quá trình thực hiện; tổng hợp báo cáo UBND tỉnh hoặc cơ quan nhà nước có thẩm quyền thông qua đơn vị chủ trì thuê dịch vụ.

Điều 17. Trách nhiệm của đơn vị vận hành Trung tâm dữ liệu tỉnh

1. Giám sát ANM, ATTT cho các hệ thống thông tin lưu ký tại Trung tâm dữ liệu tỉnh; trực tiếp bảo đảm ANM, ATTT cho hạ tầng kỹ thuật Trung tâm dữ liệu tỉnh.

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

3. Thường xuyên cập nhật các nguy cơ gây mất ANM, ATTT và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

4. Là đầu mối để tiếp nhận điều phối ứng cứu các sự cố mất ANM, ATTT của tỉnh.

Điều 18. 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 ANM, ATTT. Chịu trách nhiệm bảo đảm ANM, ATTT trong phạm vi trách nhiệm và quyền hạn được giao;

b) Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm ANM, ATTT cho tài khoản, các thiết bị mà mình được giao sử dụng;

c) Khi phát hiện sự cố mất ANM, ATTT phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách công nghệ thông tin hoặc phụ trách ATTT của cơ quan để kịp thời ngăn chặn, xử lý;

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn về ANM, ATTT do UBND tỉnh chỉ đạo hoặc cơ quan chuyên trách về ANM, ATTT tổ chức.

2. Trách nhiệm của cán bộ phụ trách công nghệ thông tin/ATTT: Ngoài các quy định tại Khoản 1 Điều này, cán bộ phụ trách công nghệ thông tin/ATTT có trách nhiệm:

a) Chủ trì tham mưu với lãnh đạo cơ quan thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến ANM, ATTT;

b) Tham mưu lãnh đạo cơ quan ban hành các quy định nội bộ và triển khai các giải pháp kỹ thuật bảo đảm ANM, ATTT;

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 và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm ANM, ATTT trong hoạt động ứng dụng công nghệ thông tin;

d) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay thủ trưởng cơ quan các sự cố mất ANM, ATTT và mức độ nghiêm trọng của các sự cố đó;

đ) Phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố ANM, ATTT.

Điều 19. Công tác kiểm tra

1. Các cơ quan, đơn vị phải thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình, coi đây là nhiệm vụ trọng tâm của đơn vị.

2. Giao Công an tỉnh kiểm tra và báo cáo UBND tỉnh việc thực hiện Quy chế này tại các cơ quan, đơn vị.

Điều 20. Chế độ, nội dung báo cáo

Các đơn vị báo cáo tình hình ANM, ATTT định kỳ 06 tháng, năm và đột xuất cho UBND tỉnh (qua Công an tỉnh) như sau:

1. Báo cáo 06 tháng

a) Nội dung báo cáo:

- Tổng hợp việc thực hiện bảo đảm ANM, ATTT của đơn vị theo quy định tại Quy chế này;

- Các nội dung chỉnh sửa, bổ sung quy chế bảo đảm ANM, ATTT của đơn vị (nếu có).

- Mốc thời gian báo cáo từ 15/12 của năm trước đến 14/6 năm nay.

b) Thời hạn gửi báo cáo: trước ngày 15 tháng 6.

2. Báo cáo năm

a) Nội dung báo cáo:

- Tổng hợp việc thực hiện bảo đảm ANM, ATTT trong năm của đơn vị theo quy định tại Quy chế này;

- Các nội dung chỉnh sửa, bổ sung quy chế bảo đảm ANM, ATTT của đơn vị (nếu có).

- Mốc thời gian báo cáo từ 15/12 của năm trước đến 14/12 năm nay.

b) Thời hạn gửi báo cáo: trước ngày 15 tháng 12.

2. Báo cáo đột xuất

a) Các sự cố mất ANM, ATTT:

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

- Nội dung vụ, việc;

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

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

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

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

- Kiến nghị, đề xuất (nếu có).

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

Điều 21. Kinh phí thực hiện

1. Kinh phí bảo đảm ANM, ATTT được bố trí từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Căn cứ vào kế hoạch hàng năm, Công an tỉnh có trách nhiệm phối hợp các đơn vị liên quan xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm ANM, ATTT cho UBND tỉnh; kịp thời tham mưu UBND tỉnh bổ sung kinh phí ngoài dự toán khi phát sinh sự cố khẩn cấp, bảo đảm hệ thống nhanh chóng được khắc phục.

Điều 22. Trách nhiệm thi hành

1. Thủ trưởng các sở, ban, ngành tỉnh, Chủ tịch UBND các xã/phường/đặc khu và các cơ quan, tổ chức, doanh nghiệp, cá nhân cung cấp dịch vụ CNTT, Internet, ATTT mạng hoặc có tham gia vào các hoạt động chuyển đổi số của các cơ quan, đơn vị trên địa bàn tỉnh 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 cơ quan, tổ chức; chịu trách nhiệm trước pháp luật và trước UBND 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 UBND tỉnh xem xét, quyết định./.