ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1479/QĐ-UBND	*Hưng Yên, ngày 22 tháng 10 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin tỉnh Hưng Yên

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN

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

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

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

Căn cứ Luật Công nghệ thông tin ngày 12 tháng 6 năm 2006;

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 64/2007/NĐ-CP ngày 10/4/2007 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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

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

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của 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 Quyết định số 332/QĐ-UBND ngày 18 tháng 7 năm 2025 của Ủy ban nhân dân tỉnh Hưng Yên về việc phân công đơn vị chuyên trách an toàn thông tin mạng của Uỷ ban nhân dân tỉnh Hưng Yên.

Căn cứ Quyết định số 565/QĐ-UBND ngày 14 tháng 8 năm 2025 của UBND tỉnh về việc kiện toàn Đội ứng cứu sự cố an ninh mạng tỉnh Hưng Yên;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 3174/TTr-CAT-PA05 ngày 15 tháng 10 năm 2025.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước trên không gian mạng đối với hệ thống thông tin tỉnh Hưng Yên.

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

Điều 3. Thủ trưởng các sở, ban, ngành, đoàn thể, tổ chức chính trị - xã hội tỉnh; Chủ tịch UBND các xã, phường; Thành viên Đội ứng cứu sự cố an ninh mạng tỉnh Hưng Yên và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bí thư Tỉnh ủy;
- Chủ tịch, các PCT UBND tỉnh;
- Công an tỉnh;
- Lãnh đạo VP UBND tỉnh;
- Lưu: VT, CVNC.

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

ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN
ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN
22/10/2025 10:57:55

Nguyễn Lê Huy

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

QUY CHẾ
Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin tỉnh Hưng Yên

(Ban hành kèm theo Quyết định số 1479/QĐ-UBND ngày 22/10/2025 của Chủ tịch UBND tỉnh Hưng Yên)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin tỉnh Hưng Yên.

2. Đối tượng áp dụng:

Các sở, ban, ngành, UBND cấp xã, phường, đơn vị sự nghiệp, cán bộ, công chức, viên chức và tổ chức, cá nhân có liên quan đến việc quản lý, vận hành, khai thác hệ thống thông tin tỉnh Hưng Yên.

Điều 2. Giải thích từ ngữ

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

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, 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 trao đổi thông tin trên mạng.

4. *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.

5. *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.

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

7. *Bộ phận chuyên trách về an toàn thông tin* là bộ phận do chủ quản hệ thống thông tin thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng.

8. *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

9. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

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

11. *Phần mềm độc hại (virus)* 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.

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. 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 AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Bảo đảm an ninh mạng, an toàn thông tin 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 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.

d) 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.

đ) 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 6 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.

e) 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.

2. Trước khi mang máy tính, thiết bị công nghệ thông tin 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 phải báo cáo và phải được lãnh đạo đơn vị đồng ý, cho phép. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ, e khoản 1 Điều này và 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 đơn vị phải bố trí ít nhất một máy tính độc lập, máy in (photocopy) không kết nối và không có lịch sử kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, lưu trữ các văn bản có nội dung bí mật nhà nước.

b) Công chức, viên chức, nhân viên được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung BMNN chỉ sử dụng máy tính, thiết bị theo quy định tại điểm a của khoản này; việc lưu trữ phải được thực hiện ở các thiết bị riêng biệt, bảo đảm các yêu cầu của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

Điều 6. Quản lý trang thiết bị công nghệ thông tin, an toàn, an ninh thông tin đối với 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, sử dụng trang thiết bị công nghệ thông tin.

b) 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 và cấu hình.

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 bảo đảm 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) Thiết bị tính toán 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).

đ) 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 an ninh mạng, an toàn thông tin đối với cá nhân:

a) Các đơn vị phải xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin 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) Các đơn vị phải thường xuyên tổ chức quán triệt các quy định về an ninh mạng, an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an ninh mạng, an toàn thông tin của từng cá nhân trong đơn vị.

c) Các đơn vị 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 chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị 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.

- Lập biên bản bàn giao tài sản công nghệ thông tin.

- Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 7. Xác định cấp độ và phương án bảo đảm an ninh mạng, an toàn thông tin hệ thống thông tin

1. Các hệ thống thông tin phải thực hiện bảo đảm an ninh mạng, an toàn thông tin theo cấp độ được quy định tại Nghị định số 85/2016/NĐ-CP; Nghị định số 53/2022/NĐ-CP và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ; nghiên cứu áp dụng tiêu chuẩn TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng.

2. Việc xây dựng phương án bảo đảm an ninh mạng, an toàn thông tin phải đáp ứng yêu cầu cơ bản theo từng cấp độ thực hiện theo nguyên tắc được quy định tại khoản 2 Điều 4 Nghị định 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT, cụ thể như sau:

- Đối với hệ thống thông tin cấp độ 1, 2, 3: Phương án bảo đảm an toàn thông tin phải xem xét khả năng dùng chung giữa các hệ thống thông tin đối với các giải pháp bảo vệ, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp, lãng phí;

- Đối với hệ thống thông tin cấp độ 4, 5: Phương án bảo đảm an toàn thông tin cần được thiết kế bảo đảm tính sẵn sàng, phân tách và hạn chế ảnh hưởng đến toàn bộ hệ thống khi một thành phần trong hệ thống hoặc có liên quan tới hệ thống bị mất an toàn thông tin.

Điều 8. Giám sát an ninh mạng, an toàn thông tin

1. Các hệ thống thông tin phải được thực hiện giám sát an ninh mạng, an toàn thông tin và kết nối, chia sẻ kết quả giám sát về Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT).

2. 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 Điều 15 của Nghị định số 53/2022/NĐ-CP và Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về quy định hoạt động giám sát an toàn hệ thống thông tin.

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

Điều 9. Ứng cứu sự cố an toàn hệ thống thông tin

1. Đơn vị chuyên trách ứng cứu khẩn cấp sự cố an ninh mạng, an toàn thông tin tại địa phương là Công an tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao).

2. Các cơ quan, đơn vị tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý và tổ chức triển khai kế hoạch sau khi phê duyệt.

Điều 10. Kiểm tra, đánh giá an toàn thông tin

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

Điều 11. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng, an toàn thông tin

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

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

3. 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 12. 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 an ninh mạng, an toàn thông tin trong cơ quan nhà nước trên địa bàn tỉnh. Tham mưu giúp UBND tỉnh về công tác bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc tham mưu bảo đảm an ninh mạng, an toàn thông tin cho các hệ thống thông tin của tỉnh.

2. Phối hợp với Sở Khoa học và Công nghệ tổ chức bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin của cơ quan, cá nhân.

4. Phối hợp với Sở Khoa học và Công nghệ trong công tác thanh tra, kiểm tra về an ninh mạng, an toàn thông tin.

5. Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin trên địa bàn tỉnh, tham gia diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

8. Chỉ đạo, hướng dẫn nghiệp vụ về bảo đảm an ninh mạng, an toàn thông tin; 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 an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin cho hệ thống thông tin theo quy định của Nhà nước.

11. Tổng hợp và báo cáo về tình hình an ninh mạng, an toàn thông tin theo định kỳ cho Bộ Công an, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan.

12. Là đầu mối để tiếp nhận điều phối ứng cứu các sự cố mất an ninh mạng, an toàn thông tin của tỉnh.

Điều 14. 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 Ủy ban nhân dân tỉnh trong công tác bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an ninh mạng, an toàn thông tin được học tập, nâng cao trình độ về an ninh mạng, an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an ninh mạng, an toàn thông tin trong đơn vị; xác định các yêu cầu, trách nhiệm đảm bảo an ninh mạng, an toàn thông tin đối với các vị trí cần tuyển dụng hoặc phân công.

4. Ban hành quy chế nội bộ về bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin.

7. Định kỳ 06 tháng (trước ngày 30/6) và hàng năm (trước ngày 31/12) báo cáo tình hình an ninh mạng, an toàn thông tin của cơ quan gửi Công an tỉnh tổng hợp, báo cáo Ủy ban nhân dân tỉnh.

Điều 15. 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 an toàn thông tin.

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng, an toàn thông tin, báo cáo Ủy ban nhân dân 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 Ủy ban nhân dân 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 Bộ Công an trong công tác bảo đảm an ninh mạng, an toàn thông tin.

e) Kịp thời thông báo sự cố an ninh mạng, an toàn thông tin và phối hợp ứng cứu xử lý sự cố an ninh mạng, an toàn thông tin 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 Ủy ban nhân dân tỉnh hoặc cơ quan nhà nước có thẩm quyền thông qua đơn vị chủ trì thuê dịch vụ.

Điều 16. Trách nhiệm của đơn vị vận hành Trung tâm dữ liệu tỉnh

1. Giám sát an ninh mạng, an toàn thông tin cho các hệ thống thông tin lưu ký tại Trung tâm dữ liệu tỉnh; trực tiếp bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

Điều 17. 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, an toàn thông tin. Chịu trách nhiệm bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin cho tài khoản, các thiết bị mà mình được giao sử dụng;

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

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn về an ninh mạng, an toàn thông tin do Ủy ban nhân dân tỉnh chỉ đạo hoặc cơ quan chuyên trách về an ninh mạng, an toàn thông tin tổ chức.

2. Trách nhiệm của cán bộ phụ trách công nghệ thông tin/an toàn thông tin: Ngoài các quy định tại khoản 1 Điều này, cán bộ phụ trách công nghệ thông tin/an toàn thông tin 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 an ninh mạng, an toàn thông tin;

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

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 an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin.

Điều 18. Kinh phí thực hiện

1. Kinh phí bảo đảm an ninh mạng, an toàn thông tin 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 an ninh mạng, an toàn thông tin cho UBND tỉnh; kịp thời tham mưu Ủy ban nhân dân 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 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

Hằng năm, các đơn vị gửi báo cáo tình hình an ninh mạng, an toàn thông tin (trước ngày 31/12) về Công an tỉnh (để tổng hợp, báo cáo Chủ tịch UBND tỉnh), như sau:

1. Báo cáo năm

a) Nội dung báo cáo:

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

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

b) Thời hạn gửi báo cáo: Trước ngày 31 tháng 12.

2. Báo cáo đột xuất

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

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

- Nội dung vụ, việc;

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

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

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

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

- Kiến nghị, đề xuất (nếu có).

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

Điều 21. Trách nhiệm thi hành

1. Quy chế này có hiệu lực từ ngày ký, ban hành.

2. Thủ trưởng sở, ban, ngành, Chủ tịch Ủy ban nhân dân các xã, phường 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 UBND tỉnh về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị.

3. 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./.