ỦY BAN NHÂN DÂN TỈNH PHÚ THỌ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số:132 /2025/QĐ-UBND	*Phú Thọ, ngày 19 tháng 12 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ

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 Công nghệ thông tin số 67/2006/QH11;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14;

Căn cứ Nghị định số 78/2025/NĐ-CP ngày 01 tháng 4 năm 2025 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 năm 2025 được sửa đổi, bổ sung bởi Nghị định số 187/2025/NĐ-CP ngày 01 tháng 7 năm 2025 của Chính phủ;

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

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

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 26/2020/NĐ-CP ngày 28 tháng 02 năm 2020 quy định chi tiết một số điều của Luật bảo vệ bí mật nhà nước;

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

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 5907/TTr-CAT-ANM ngày 12 tháng 12 năm 2025;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế bảo đảm an

toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ.

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ.

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực thi hành từ ngày 01 tháng 01 năm 2026.

2. Các Quyết định sau hết hiệu lực kể từ ngày Quyết định này có hiệu lực thi hành: Quyết định số 998/QĐ-UBND ngày 29 tháng 4 năm 2016 của Ủy ban nhân dân tỉnh Phú Thọ ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ; Quyết định số 33/2023/QĐ-UBND, ngày 12 tháng 9 năm 2023 của Ủy ban nhân dân tỉnh Vĩnh Phúc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc; Quyết định số 20/2023/QĐ-UBND, ngày 27 tháng 7 năm 2023 của Ủy ban nhân dân tỉnh Hòa Bình ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hòa Bình.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các Sở, ban, ngành; Chủ tịch Ủy ban nhân dân các xã, phường 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;
- Văn phòng Chính phủ;
- Bộ Công an;
- Bộ Khoa học và Công nghệ;
- Cục KTVB&QLXL VPHC-Bộ Tư pháp;
- TT TU, TT HĐND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- CT, các PCT UBND tỉnh;
- Các Sở, ban, ngành;
- HĐND, UBND các xã, phường;
- CVP, các PCVP UBND tỉnh;
- Trung tâm TT-CB;
- Lưu: VT, NC2.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trần Duy Đông

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ

(Ban hành kèm theo Quyết định 132 /2025/QĐ-UBND)

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 bảo đảm an toàn thông tin các hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ.

2. Quy chế này được áp dụng đối với

a) Các cơ quan quản lý hành chính nhà nước và các đơn vị sự nghiệp công lập thuộc Ủy ban nhân dân tỉnh Phú Thọ;

b) Các tổ chức chính trị - xã hội được ngân sách nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai;

c) Tổ chức, cá nhân có liên quan đến an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước.

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, 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. "*An toàn thông tin mạng", "Mạng", "Hệ thống thông tin", "Chủ quản hệ thống thông tin", "Sự cố an toàn thông tin mạng", "Phần mềm độc hại", "Thông tin cá nhân"* theo Điều 3 Luật An toàn thông tin mạng; *"Tấn công mạng"* theo Điều 2 Luật An ninh mạng; "*Đơn vị chuyên trách về công nghệ thông tin"* theo Điều 3 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ.

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

6. *Mạng riêng ảo (Virtual Private Network - VPN)* là dịch vụ mạng dùng riêng để kết nối máy tính của các cơ quan, đơn vị hoặc máy tính cá nhân truy cập vào mạng nội bộ để bảo đảm an toàn an ninh thông tin trên đường truyền.

7. *Tường lửa (Firewall)* là hệ thống an ninh mạng, có thể là phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát lưu lượng truy cập (traffic) vào, ra hệ thống.

8. *Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS)* là phần mềm ứng dụng hoặc thiết bị được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống.

9. *Hệ thống ngăn ngừa xâm nhập (Intrusion Prevention System - IPS)* là hệ thống phát hiện xâm nhập ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động xâm nhập không mong muốn đối với hệ thống thông tin.

10. *Mật khẩu mạnh* là mật khẩu bao gồm chữ hoa, chữ thường, chữ số, ký tự đặc biệt (!, @, #, $, …) và có độ dài 9 ký tự trở lên.

11. *Cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin* là cán bộ, công chức, viên chức được tuyển dụng để phụ trách an toàn thông tin/ công nghệ thông tin tại các cơ quan, đơn vị.

12. *Cán bộ, công chức, viên chức quản lý, vận hành hệ thống thông tin* là cán bộ, công chức, viên chức được tuyển dụng hoặc được phân công phụ trách quản lý, vận hành hoạt động thường xuyên của một hoặc nhiều hệ thống thông tin của cơ quan, đơn vị.

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

1. Bảo đảm an ninh mạng, an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin từ thiết kế, xây dựng, vận hành, nâng cấp cho đến hủy bỏ hệ thống thông tin. Bảo đảm an toàn, tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An ninh mạng, Điều 4 Luật An toàn thông tin mạng và Điều 4 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.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin (ATTT) mạng. Hoạt động ATTT mạng của cơ quan, tổ chức, cá nhân phải đúng các quy định của pháp luật liên quan.

3. Xử lý sự cố ATTT phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị và theo quy định của pháp luật.

4. Công tác bảo đảm ATTT mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

5. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị. Lãnh đạo cơ quan, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

Điều 4. Những hành vi bị cấm

1. Các hành vi bị nghiêm cấm về an ninh mạng, an toàn thông tin mạng quy định tại Điều 7 Luật An toàn thông tin mạng; Điều 8, Luật An ninh mạng; Điều 5, Luật Bảo vệ bí mật nhà nước.

2. Các hành vi bị cấm trong quản lý, cung cấp, sử dụng dịch vụ internet và thông tin mạng:

a. Lợi dụng việc cung cấp sử dụng dịch vụ internet và thông tin trên mạng nhằm mục đích:

Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo;

Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc;

Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định;

Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân;

Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm;

Giả mạo tổ chức, cá nhân và phát tán thông tin giả mạo, thông tin sai sự thật xâm hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

b. Cản trở trái pháp luật việc cung cấp và truy cập thông tin hợp pháp, việc cung cấp và sử dụng các dịch vụ hợp pháp trên Internet của tổ chức, cá nhân.

c. Cản trở trái pháp luật hoạt động của hệ thống máy chủ tên miền quốc gia Việt Nam ".vn", hoạt động hợp pháp của hệ thống thiết bị cung cấp dịch vụ internet và thông tin trên mạng.

d. Sử dụng trái phép mật khẩu, khóa mật mã của tổ chức, cá nhân; thông tin riêng, thông tin cá nhân và tài nguyên Internet.

đ. Tạo đường dẫn trái phép đối với tên miền hợp pháp của tổ chức, cá nhân; tạo, cài đặt, phát tán phần mềm độc hại, vi-rút máy tính; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, tạo lập công cụ tấn công trên Internet.

3. Tạo, cài đặt, phát tán phần mềm độc hại, xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, tạo lập công cụ tấn công trên internet.

CHƯƠNG II
QUY ĐỊNH ĐẢM BẢO 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. 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 Ủy ban nhân dân 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.

2. 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; thiết lập chế độ rà quét máy tính định kỳ hằng tuần.

3. 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.

4. 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.

5. Đặt mật khẩu với độ an toàn cao (tối thiểu 9 ký tự bao gồm: có chữ thường, chữ in hoa, chữ 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.

6. 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 cơ quan, đơn vị.

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 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 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 theo quy định tại Nghị định số 85/2016/NĐ-CP và Nghị định số 53/2022/NĐ-CP của Chính phủ. Việc đảm bảo an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức 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. Nội dung yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo quy định tại Điều 9 và Điều 10 Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông.

2. Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo, tổ chức thực hiện phương án đảm bảo an toàn hệ thống thông tin theo cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP của Chính phủ.

3. Đơn vị vận hành hệ thống thông tin thực hiện xác định cấp độ và lập hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP của Chính phủ, gửi cơ quan có thẩm quyền thẩm định, phê duyệt theo quy định tại khoản 1 Điều 14 Nghị định số 85/2016/NĐ-CP của Chính phủ.

4. Công an tỉnh là đơn vị chuyên trách về an toàn thông tin trên địa bàn tỉnh.

5. Thẩm quyền phê duyệt cấp độ an toàn hệ thống thông tin:

Hồ sơ đề xuất cấp độ 1, cấp độ 2 Công an tỉnh thẩm định và phê duyệt; hồ sơ đề xuất cấp độ 3 Công an tỉnh thẩm định, Ủy ban nhân dân tỉnh phê duyệt; hồ sơ đề xuất cấp độ 4, cấp độ 5 Công an tỉnh cho ý kiến chuyên môn, Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) thẩm định (trừ hệ thống thông tin do Bộ Công an, Bộ Quốc phòng quản lý).

6. Thành phần hồ sơ đề xuất cấp độ an toàn hệ thống thông tin gồm:

a) Văn bản đề nghị thẩm định, phê duyệt Hồ sơ đề xuất cấp độ theo Mẫu số 01 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP của Chính phủ (đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2) hoặc Văn bản đề nghị thẩm định Hồ sơ đề xuất cấp độ theo Mẫu số 02 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP của Chính phủ (đối với hệ thống thông tin đề xuất cấp độ 3 trở lên).

b) Tài liệu Hồ sơ đề xuất cấp độ bao gồm: Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin, có đầy đủ các nội dung theo quy định tại khoản 3 Điều 8 Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông; tài liệu thuyết minh về việc đề xuất cấp độ, có đầy đủ các nội dung theo quy định tại khoản 4 Điều 8 Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông. Trường hợp hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, cần làm rõ thêm các nội dung theo quy định tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông; tài liệu thuyết minh phương án đảm bảo an toàn thông tin theo cấp độ tương ứng, có đầy đủ các nội dung thuyết minh đáp ứng các yêu cầu về quản lý và kỹ thuật tương ứng với cấp độ đề xuất, theo quy định tại khoản 6 Điều 8, Điều 9 và Điều 10 Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông.

c) Tài liệu thiết kế hệ thống thông tin.

d) Dự thảo quy chế hoặc quy chế bảo đảm an toàn thông tin đã được cấp có thẩm quyền ban hành và các văn bản, quy chế được tham chiếu, áp dụng.

đ) Văn bản ý kiến chuyên môn của đơn vị chuyên trách về an toàn thông tin đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5.

7. Trình tự thẩm định, phê duyệt cấp độ

a) Gửi thẩm định hồ sơ đề xuất cấp độ;

b) Tổ chức thẩm định, phê duyệt cấp độ an toàn thông tin:

Đối với hệ thống thông tin được đề xuất cấp độ 1, cấp độ 2 thời gian xử lý phê duyệt tối đa là 7 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

Đối với hệ thống thông tin được đề xuất cấp độ 3 thời gian thẩm định tối đa là 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

Đối với hệ thống thông tin được đề xuất cấp độ 4, cấp độ 5 thời gian thẩm định tối đa là 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ.

8. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp cần được kiểm thử về tính an toàn, bảo mật trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng.

Điều 8. Quản lý, giám sát an ninh mạng, an toàn hệ thống 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 của Chính phủ và Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng 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.

4. Chủ quản hệ thống thông tin phải triển khai hệ thống giám sát an toàn thông tin đáp ứng các yêu cầu tại 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.

5. Công an tỉnh có trách nhiệm tổ chức giám sát an toàn thông tin đối với các hệ thống thông tin của tỉnh.

6. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm tích hợp dữ liệu của tỉnh thì chủ quản hệ thống thông tin có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ bảo đảm các yêu cầu giám sát an toàn hệ thống thông tin theo quy định của pháp luật và có kết nối, chia sẻ hoạt động giám sát về Công an tỉnh để quản lý.

7. 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.

Điều 9. An toàn thông tin dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan, đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ

của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

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

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

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

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

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

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

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

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

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ công nghệ thông tin:

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

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

Điều 10. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. 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 trữ bí mật nhà nước (BMNN) theo quy định của pháp luật về cơ yếu để soạn thảo, lưu trữ các văn bản có nội dung BMNN.

2. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) 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 Khoản 1 Điều 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 BMNN và cơ yếu.

b) Không được soạn thảo, lưu trữ, chuyển giao, đăng tải, phát tán thông tin, tài liệu có chứa nội dung bí mật nhà nước trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu trữ BMNN theo quy định của pháp luật về cơ yếu.

c) Không được in, sao chụp tài liệu BMNN trên các thiết bị kết nối internet.

3. Khi sửa chữa, khắc phục các sự cố của máy tính dùng để soạn thảo văn bản có chứa nội dung BMNN, 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.

4. Khi sử dụng các thiết bị lưu trữ ngoài (USB, ổ cứng di động, …) để lưu trữ BMNN phải đảm bảo chất lượng, an toàn; định kỳ được rà quét bằng phần mềm diệt virus; sao lưu, bảo quản đúng quy định.

5. Trước khi thanh lý các máy tính, thiết bị có bộ nhớ trong dùng để soạn thảo, lưu trữ BMNN tại các cơ quan nhà nước phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong các thiết bị lưu trữ dữ liệu điện tử.

Điều 11. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập hệ thống thông tin

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

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

3. Quản lý tài khoản và chữ ký số:

a) Khi cấp tài khoản, chữ ký số lần đầu cho người dùng truy nhập, cơ quan, đơn vị vận hành phải thông báo (qua email, điện thoại) và người dùng

phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu, mật khẩu được đổi phải đảm bảo yếu tố đủ mạnh;

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

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

d) Tài khoản thư điện tử, chữ ký số chuyên dùng do Ban Cơ yếu Chính phủ cấp để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác; định kỳ 01 năm kiểm tra việc lưu trữ của hệ thống thư điện tử, tiến hành xóa các mail quá cũ, không cần thiết để đảm bảo hệ thống hoạt động ổn định thông suốt;

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

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

Điều 12. 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 an toàn thông tin là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá an toàn thông tin. 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 13. Bảo đảm an toàn hạ tầng mạng

1. Hệ thống mạng nội bộ phải được cài đặt, thiết lập, cấu hình tuân thủ

các quy định, tiêu chuẩn kỹ thuật và bảo đảm an toàn thông tin.

2. Căn cứ điều kiện, yêu cầu thực tế về bảo mật dữ liệu, khuyến khích các cơ quan, đơn vị là chủ quản hệ thống mạng nội bộ chủ động triển khai xây dựng mô hình, giải pháp an toàn bảo mật, bao gồm các biện pháp kỹ thuật sau đây:

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

b) Đối với các phòng, ban, đơn vị trực thuộc không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết;

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

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

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

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

6. Quản lý hệ thống mạng không dây:

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu có độ phức tạp cao, 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 vận hành phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 14. Bảo đảm an toàn máy chủ và ứng dụng

1. Trên hệ thống máy chủ:

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

b) Thiết lập chế độ tự động cập nhật phiên bản và hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ;

c) Các máy chủ cần được cài đặt mật khẩu ở phần cấu hình (setup) của BIOS (Basic Input/Output System), trong đó lưu ý việc vô hiệu hóa các cổng USB trên máy chủ.

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

3. Định kỳ hằng tuần, cơ quan, đơn vị vận hành phải kiểm tra các tiến trình trên máy chủ nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy chủ.

4. Quản lý tệp tin lưu trữ sự kiện (logfile): Cơ quan, đơn vị vận hành phải thường xuyên kiểm tra, quản lý, sao lưu các logfile theo từng tháng, thời gian lưu trữ logfile trên máy chủ và thiết bị từ 06 - 12 tháng, các tập tin logfile cũ trong 03 năm trước đó cần được lưu trữ trên các ổ cứng ngoài; định kỳ 06 tháng kiểm tra, bảo đảm tính toàn vẹn của các logfile, hạn chế tình trạng tràn logfile gây ảnh hưởng đến hoạt động của hệ thống thông tin.

5. Quản lý lưu ký hệ thống: Việc thực hiện lưu ký hệ thống thông tin yêu cầu cơ quan, đơn vị cung cấp dịch vụ lưu ký phải tổ chức máy chủ cơ sở dữ liệu và máy chủ ứng dụng nằm trên hai máy chủ khác nhau và được bảo vệ bởi lớp bảo vệ bao gồm: Tường lửa, thiết bị phòng chống tấn công từ chối dịch vụ DDoS (Distributed Denial of Service), thiết bị phát hiện và phòng chống xâm nhập trái phép (IPS/IDS);

6. Quản lý phiên bản: Cơ quan, đơn vị vận hành xây dựng nhật ký quản lý phiên bản hệ thống thông tin bao gồm các thông tin: Chủ đầu tư, tên hệ thống thông tin, đơn vị phát triển, tên phiên bản; các chức năng của phiên bản; các chức năng thay đổi so với phiên bản trước, thời gian thay đổi; lưu trữ các phiên bản hệ thống thông tin tại hệ thống lưu trữ độc lập;

7. Khi thiết lập cung cấp các dịch vụ ra môi trường mạng (tuân thủ theo TCP/UDP Port), cơ quan, đơn vị vận hành yêu cầu nhà cung cấp dịch vụ cấu hình trên máy chủ ứng dụng những dịch vụ thiết yếu nhất để bảo đảm hoạt động

của hệ thống, không kích hoạt những chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không sử dụng (không thiết lập cấu hình các dịch vụ ra môi trường mạng đối với máy chủ cơ sở dữ liệu).

Điều 15. Bảo đảm an toàn dữ liệu

1. Các cơ quan, đơn vị khi triển khai dịch vụ sao lưu dự phòng ở mức vật lý cần thiết lập chức năng RAID (Redundant Arrays of Inexpensive Disks hoặc Redundant Arrays of Independent Disks) để tăng tốc độ đọc ghi hoặc bảo đảm khả năng lưu trữ dự phòng. 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.

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

3. Đối với công tác sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ):

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu;

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.

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

5. 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).

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

7. Thông tin, dữ liệu thuộc phạm vi bí mật nhà nước phải được quản lý

theo quy định hiện hành về bảo vệ bí mật nhà nước.

Điều 16. Bảo đảm an toàn thiết bị đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống:

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

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

c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

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 cho phép.

3. Trong quá trình sử dụng thiết bị đầu cuối:

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

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

Điều 17. 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 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.

3. Nguyên tắc ứng cứu xử lý sự cố

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

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

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

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

4. Phân nhóm sự cố an toàn thông tin:

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

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

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

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, cháy nổ.

5. 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.

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

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng đến các hệ thống được triển khai tập trung tại Trung tâm tích hợp dữ liệu tỉnh thì thực hiện tiếp Bước 3;

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

c) Bước 3: Báo sự cố đến Công an tỉnh theo Mẫu số 01 kèm theo Quy chế;

d) Bước 4: Phối hợp với Đội ứng cứu sự cố An toàn thông tin mạng và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo Mẫu số 02 kèm theo Quy chế này. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Công an tỉnh.

7. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị; Lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Công an tỉnh để được hướng

dẫn, hỗ trợ.

8. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm:

a) Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng;

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định;

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

d) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.

Điều 18. 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 cho nguồn nhân lực để bảo đảm an toàn thông tin tại đơn vị mình gửi Sở Nội vụ, 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
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 19. Trách nhiệm của Công an tỉnh

1. Tham mưu giúp Ủy ban nhân dân tỉnh về công tác bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc tham mưu bảo đảm an ninh mạng, an toàn thông tin cho các hệ thống thông tin của tỉnh.

2. Chỉ đạo, 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. Xây dựng và triển khai các Kế hoạch, chương trình đào tạo, tập huấn, hội thảo, tuyên truyền về an ninh mạng, an toàn thông tin mạng cho cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin của các cơ quan, đơn vị trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

6. 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.

7. Chỉ đạo, hướng dẫn về nghiệp vụ về bảo đảm an ninh mạng, an toàn thông tin; hỗ trợ giải quyết sự cố khi có yêu cầu.

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, an toàn thông tin theo thẩm quyền và theo quy định của pháp luật.

9. 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.

10. Tổng hợp, 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.

11. Thực hiện thủ tục xác định cấp độ an toàn thông tin và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

12. Là cơ quan đầu mối, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh.

Điều 20. Trách nhiệm của các cơ quan đơn vị chủ quản hệ thống thông tin

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 chủ quản 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 cơ quan; 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. Thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

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

9. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin 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... cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện.

10. Trách nhiệm phối hợp liên ngành:

a) Cơ quan, tổ chức, cá nhân tham gia hoạt động an toàn thông tin mạng có trách nhiệm phối hợp với cơ quan nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin mạng;

b) Chủ quản hệ thống thông tin chủ động chỉ đạo đơn vị vận hành hệ thống thông tin phối hợp với đơn vị chức năng liên quan của Công an tỉnh trong việc triển khai thiết bị, kết nối tới hệ thống kỹ thuật xử lý, giảm thiểu tấn công mạng, hỗ trợ giám sát an toàn thông tin cho hệ thống thông tin cung cấp dịch vụ công trực tuyến, phát triển chính phủ điện tử.

Điều 21. 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 của Chính phủ;

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 22. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức, người sử dụng:

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 Công an tỉnh và 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 23. Trách nhiệm của các tổ chức, cá nhân liên quan

Các tổ chức, cá nhân liên quan đến sử dụng, khai thác các hệ thống thông tin hoặc liên quan đến việc triển khai hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về an ninh mạng, an toàn thông tin.

Điều 24. 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.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 25. Công tác kiểm tra

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc thực hiện 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 bảo đảm an toàn thông tin;

b) 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;

c) Kiểm tra công tác giám sát an toàn thông tin và ứng phó khi xảy ra sự cố an toàn thông tin;

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

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin và đơn vị chuyên trách về an toàn thông tin của tỉnh;

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

3. Thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Đơn vị chuyên trách ATTT tại Trung ương;

b) Ủy ban nhân dân tỉnh hoặc Công an tỉnh (đơn vị chuyên trách về an toàn thông tin trên địa bàn tỉnh);

c) 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.

4. Đối tượng kiểm tra, đánh giá là cơ quan chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

Điều 26. 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 với Sở Tài chính và các đơn vị liên quan cân đối, tham mưu Ủy ban nhân dân tỉnh đảm bảo nguồn kinh phí triển khai các hoạt động bảo đảm an ninh mạng, an toàn thông tin.

Điều 27. Trách nhiệm thi hành

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn tỉnh và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện trong phạm vi quản lý; định kỳ 6 tháng (trước ngày 15/6), hằng năm (trước ngày 15/12) hoặc khi có yêu cầu đột xuất, các đơn vị báo cáo Ủy ban nhân dân tỉnh kết quả triển khai, thực hiện Quy chế (qua Công an tỉnh).

2. Công an tỉnh có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân tỉnh theo định kỳ hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

3. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Công an tỉnh để tổng hợp báo cáo Ủy ban nhân dân tỉnh xem xét điều chỉnh, bổ sung./.

PHỤ LỤC
Danh mục mẫu biểu quy định
ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Phú Thọ

(Ban hành kèm theo Quyết định số 132 */2025/QĐ-UBND)*

STT	Mẫu số	Tên Mẫu biểu
1	Mẫu số 01	Báo cáo ban đầu sự cố an toàn thông tin mạng
2	Mẫu số 02	Báo cáo kết thúc ứng phó sự cố

MẪU SỐ 01

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

• Tên tổ chức/cá nhân báo cáo sự cố (*) .....

• Địa chỉ: (*) .....

• Điện thoại (*) ..... Email (*) .....

NGƯỜI LIÊN HỆ

• Họ và tên (*) ..... Chức vụ: .....

• Điện thoại (*) ..... Email (*) .....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ IP liên quan*
Phân loại cấp độ của hệ thống thông tin, (nếu có)	Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5 □
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*
Mô tả sơ bộ về sự cố (*)	
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố: ..... ……. …….	

Ngày phát hiện sự cố (*) / / (dd/mm/yy)	Thời gian phát hiện (*):	… giờ … phút

HIỆN TRẠNG SỰ CỐ (*)

□ Đã được xử lý

□ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

□ Qua hệ thống phát hiện xâm nhập □ Kiểm tra dữ liệu lưu lại (Log File)

□ Nhận được thông báo từ: .....

□ Khác, đó là ……

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

□ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

□ ISP đang trực tiếp cung cấp dịch vụ

□ Cơ quan điều phối

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

• Hệ điều hành .....Version .....

• Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

□ Web server □ Mail server □ Database server

□ Dịch vụ khác, đó là .....

□ Các biện pháp an toàn thông tin đã triển khai (*Đánh dấu những biện pháp đã triển khai)*

□ Antivirus □ Firewall □ Hệ thống phát hiện xâm nhập

□ Khác: .....

• Các địa chỉ IP của hệ thống

(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)

……..

• Các tên miền của hệ thống .....

• Mục đích chính sử dụng hệ thống.....

• Thông tin gửi kèm

□ Nhật ký hệ thống □ Mẫu virus / mã độc

□ Khác:.....

• Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:

□ Có □ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có) …….. …….. ……..

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ

(ngày/tháng/năm/giờ/phút):

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT

(Ký tên, đóng dấu)

MẪU SỐ 02

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

• Tên tổ chức/cá nhân báo cáo sự cố (*) .....

• Địa chỉ: (*) .....

• Điện thoại (*) ..... Email (*) .....

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ

Số ký hiệu .....Ngày báo cáo: …/../201…

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin:	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	□ Cấp độ 1	□ Cấp độ 2	□ Cấp độ 3	□ Cấp độ 4	□ Cấp độ 5
Tên/Mô tả về sự cố					
Ngày phát hiện sự cố …/.../…. (dd/mm/yy)		Thời gian phát hiện (*):		giờ.... phút	
Kết quả xử lý sự cố					
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...					
Các tài liệu đính kèm					
Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file…)					

CÁ NHÂN/ NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT

(Ký tên, đóng dấu)