ỦY BAN NHÂN DÂN TỈNH THÁI NGUYÊN	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 60 /2026/QĐ-UBND	*Thái Nguyên, ngày 09 tháng 6 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy định bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên

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

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

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

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

Căn cứ Luật Dữ liệu số 60/2024/QH15;

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

Căn cứ Nghị định số 63/2026/NĐ-CP ngày 28 tháng 02 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ bí mật nhà nước;

Căn cứ Nghị định số 365/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ về quy định chi tiết một số điều và biện pháp thi hành Luật bảo vệ dữ liệu cá nhân;

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;

Theo đề nghị của Giám đốc Công an tỉnh Thái Nguyên;

Uỷ ban nhân dân tỉnh ban hành Quyết định ban hành Quy định bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên.

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

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực từ ngày 01 tháng 7 năm 2026.

2. Các Quyết định sau hết hiệu lực kể từ ngày Quyết định này có hiệu lực thi hành:

a) Quyết định số 10/2020/QĐ-UBND ngày 08 tháng 5 năm 2020 của Ủy ban nhân dân tỉnh Thái Nguyên ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên.

b) Quyết định số 73/2024/QĐ-UBND ngày 31 tháng 12 năm 2024 của Ủy ban nhân dân tỉnh Thái Nguyên về sửa đổi, bổ sung một số điều của Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên ban hành kèm theo Quyết định số 10/2020/QĐ-UBND ngày 08 tháng 5 năm 2020 của Ủy ban nhân dân tỉnh Thái Nguyên.

c) Quyết định số 22/2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh Bắc Kạn ban hành quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Bắc Kạn.

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 tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Công an;
- Cục Kiểm tra văn bản và Tổ chức thi hành pháp luật - Bộ Tư pháp;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Các sở, ban, ngành;
- UBND các xã, phường;
- Trung tâm thông tin tỉnh;
- Các chuyên viên NCTH;
- Lưu: VT, NC.

Vandt

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Vương Quốc Tuấn

ỦY BAN NHÂN DÂN
TỈNH THÁI NGUYÊN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY ĐỊNH
Bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên

(Ban hành kèm theo Quyết định số 60 /2026/QĐ-UBND)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy định này quy định một số nội dung có liên quan đến bảo đảm an ninh mạng các hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên (sau đây gọi tắt là cơ quan, đơn vị).

2. Đối tượng áp dụng

a) Các cơ quan quản lý hành chính nhà nước và các đơn vị sự nghiệp công lập trên địa bàn tỉnh Thái Nguyên, bao gồm:

- Các sở, ban, ngành và các đơn vị trực thuộc.
- Các đơn vị sự nghiệp công lập thuộc UBND tỉnh.
- Ủy ban nhân dân các xã, phường.

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 UBND tỉnh triển khai;

c) Tổ chức, cá nhân có liên quan đến an ninh mạng trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị thuộc điểm a, điểm b khoản 2 Điều này.

Điều 2. Mục đích, nguyên tắc bảo đảm an ninh mạng

1. Việc áp dụng Quy định này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an ninh mạng, an ninh thông tin mạng trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan, đơn vị.

2. Hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị phải tuân thủ theo nguyên tắc bảo đảm an ninh mạng, an ninh thông tin mạng được quy định tại Điều 4 Luật An ninh mạng số 116/2025/QH15, Điều 3 Luật Bảo vệ bí mật nhà nước số 117/2025/QH15, Điều 5 Luật Giao dịch điện tử số 20/2023/QH15, Điều 8 Luật Dữ liệu số 60/2024/QH15.

Điều 3. Giải thích từ ngữ

Trong quy định này, từ ngữ dưới đây được hiểu như sau:

Giám sát hệ thống thông tin là biện pháp giám sát, theo dõi trạng thái hoạt động của hệ thống để phát hiện, cảnh báo sớm các sự cố có thể gây gián đoạn hoạt động của hệ thống và làm mất tính khả dụng của hệ thống thông tin.

Chương II
NỘI DUNG NHIỆM VỤ BẢO ĐẢM AN NINH MẠNG

Điều 4. Quản lý trang thiết bị ứng dụng công nghệ thông tin trong hoạt động của cơ quan, đơn vị

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị. Người đứng đầu hoặc cấp phó được giao nhiệm vụ có trách nhiệm phân công cán bộ trực tiếp sử dụng, quản lý và theo dõi tình trạng của từng trang thiết bị CNTT thuộc phạm vi sử dụng của đơn vị mình.

2. Cơ quan, đơn vị quy định các quy tắc nội bộ khai thác, sử dụng, bảo vệ trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

3. Trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị khi thay đổi mục đích sử dụng hoặc thanh lý thì cơ quan, 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 ứng dụng CNTT trong hoạt động cơ quan, đơn vị đó.

4. 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).

5. Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của đơn vị; thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị dự phòng).

6. Khi làm mất, thất lạc, hư hỏng hoặc khi phát hiện trang thiết bị, ứng dụng CNTT của cơ quan, đơn vị bị mất, thất lạc, hư hỏng hoặc có dấu hiệu bị truy cập, chiếm đoạt trái phép, người quản lý hoặc người sử dụng trực tiếp phải báo cáo ngay cho lãnh đạo đơn vị và bộ phận phụ trách công nghệ thông tin để kịp thời thực hiện các biện pháp khóa truy cập, bảo vệ dữ liệu và thông báo cho cơ quan chuyên trách về an ninh mạng để phối hợp xử lý.

Điều 5. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

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

a) Không được soạn thảo, lưu trữ bí mật nhà nước trên máy tính hoặc thiết bị khác đang kết nối với mạng máy tính (trừ mạng LAN độc lập), mạng Internet, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu và quy định khác của pháp luật có liên quan.

b) Không được in, sao, chụp tài liệu bí mật nhà nước trên các phương tiện, thiết bị kết nối mạng máy tính (trừ mạng LAN độc lập), mạng Internet, mạng viễn thông, trừ trường hợp thực hiện theo quy định pháp luật về cơ yếu và quy định khác của pháp luật có liên quan.

c) Máy tính, thiết bị khác dùng để soạn thảo, lưu giữ tài liệu bí mật nhà nước, gửi nhận văn bản điện tử bí mật nhà nước phải được kiểm tra đảm bảo an ninh, an toàn, phòng, chống xâm phạm bí mật nhà nước trước khi đưa vào sử dụng.

2. Khi sửa chữa, khắc phục các 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.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 6. Quản lý cán bộ, công chức, viên chức và người lao động trong hoạt động ứng dụng công nghệ thông tin

1. Cơ quan, đơn vị tổ chức quán triệt các quy định về an ninh mạng, an ninh thông tin mạng nhằm nâng cao nhận thức về trách nhiệm bảo đảm an ninh mạng của từng cá nhân trong cơ quan, đơn vị.

2. Cán bộ, công chức, viên chức, người lao động phải tuân thủ thực hiện các quy định bảo đảm an ninh mạng, an ninh thông tin mạng theo quy định của pháp luật và của cơ quan, đơn vị mình.

3. Bố trí nhân sự có năng lực và đạo đức đảm nhận vị trí phụ trách công tác bảo đảm an ninh mạng, an ninh thông tin mạng, quản trị hệ thống CNTT của cơ quan, đơn vị.

4. Cơ quan, đơn vị lập kế hoạch đào tạo cho cán bộ, công chức, viên chức và người lao động để nâng cao kiến thức cơ bản và kỹ năng an ninh mạng, an ninh thông tin mạng; đồng thời, phổ biến, cập nhật các quy chế về an ninh mạng, an ninh thông tin mạng hằng năm để mọi người hiểu rõ các quyền và trách nhiệm. Kiểm tra việc thực hiện các nội quy, quy định về an ninh mạng, an ninh thông tin mạng của cơ quan, đơn vị đối với cán bộ, công chức, viên chức, người lao động theo định kỳ.

5. Khi có sự chấm dứt hay thay đổi công việc, cơ quan, đơn vị và cán bộ, công chức, viên chức, người lao động cần xác định rõ trách nhiệm trong việc khai thác, sử dụng hệ thống CNTT; cơ quan, đơn vị có trách nhiệm thu hồi tài khoản, thay đổi quyền truy cập hệ thống đối với cán bộ, công chức, viên chức, người lao động có sự thay đổi công việc.

Điều 7. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an ninh mạng, an ninh thông tin mạng đối với trung tâm dữ liệu/phòng máy chủ

a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống. Đơn vị vận hành trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

b) Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ được giao theo quy định mới được phép vào trung tâm dữ liệu/phòng máy chủ. Việc vào, ra phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (như: thẻ từ, sinh trắc học, …).

c) Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

d) Trung tâm dữ liệu/phòng máy chủ phải có hệ thống làm mát điều hòa không khí, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp. Đơn vị phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

2. Bảo đảm an ninh thông tin mạng khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành (nếu có) trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về CNTT; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cá nhân cài đặt phần mềm phòng, chống mã độc có bản quyền và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về CNTT để được xử lý kịp thời.

c) Cá nhân 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; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

3. Bảo đảm an ninh thông tin mạng đối với hệ thống mạng máy tính của cơ quan, đơn vị

a) Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản phù hợp chính sách an ninh mạng riêng của cơ quan, đơn vị, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

b) Định kỳ sao lưu thông tin, dữ liệu dùng chung lưu trữ trên mạng diện rộng; không được tiết lộ phương thức đăng nhập (các thông tin như; tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) cho các tổ chức, cá nhân khác để truy nhập vào hệ thống mạng diện rộng; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

c) Áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy nhập Internet, đáp ứng nhu cầu kết nối, đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

d) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

e) Các tên miền (bao gồm cả tên miền *.thainguyen.gov.vn) khi không còn sử dụng, các cơ quan, đơn vị có văn bản gửi đến Sở Khoa học và Công nghệ, Trung Tâm Internet Việt Nam (VNNIC) 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. Quản lý tài khoản truy cập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho cơ quan, đơn vị vận hành hệ thống thông tin bằng văn bản có xác nhận của thủ trưởng đơn vị để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

c) Tài khoản quản trị hệ thống (như: tài khoản quản trị mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

d) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin hoặc đơn vị được giao vận hành trực tiếp hệ thống thông tin để xem xét, thực hiện. Đơn vị vận hành hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin; xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay sau khi có thay đổi về nhân sự quản lý tài khoản.

e) Việc quản lý tài khoản thư điện tử quy định theo quy chế của tỉnh về thiết lập, quản lý và sử dụng Hệ thống thư điện tử công vụ trong các cơ quan nhà nước.

f) Việc quản lý tài khoản phải đảm bảo đáp ứng các yêu cầu sau: sử dụng mật khẩu duy nhất cho mỗi tài khoản; thay đổi mật khẩu định kỳ 01 lần/ 02 tháng; đối với các hệ thống sử dụng xác thực đa yếu tố, quy định mật khẩu có tối thiểu 08 ký tự; đối với các hệ thống không sử dụng xác thực đa yếu tố, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số; mật khẩu mới không được trùng với 10 mật khẩu trước đó.

5. Bảo đảm an ninh thông tin mạng mức ứng dụng

a) Yêu cầu về bảo đảm an ninh mạng, an ninh thông tin mạng phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách CNTT quản lý.

e) Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 90 ngày với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

f) Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an ninh mạng trước khi đưa vào sử dụng và trong quá trình sử dụng.

g) Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

6. Bảo đảm an ninh dữ liệu

a) Cơ quan, đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

b) Cơ quan, đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

c) Cơ quan, đơn vị phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

d) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, cơ quan, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 8. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc

quy định tại các Nghị định của Chính phủ, Thông tư của Bộ trưởng Bộ Công an và các văn bản hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ.

2. 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 các Nghị định của Chính phủ, Thông tư của Bộ trưởng Bộ Công an và các văn bản hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ.

3. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) 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 các Nghị định của Chính phủ, Thông tư của Bộ trưởng Bộ Công an và các văn bản hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ.

b) 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 các Nghị định của Chính phủ, Thông tư của Bộ trưởng Bộ Công an và các văn bản hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ, gửi cơ quan có thẩm quyền thẩm định, phê duyệt theo quy định tại các Nghị định của Chính phủ, Thông tư của Bộ trưởng Bộ Công an và các văn bản hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ, đồng thời có trách nhiệm rà soát, cập nhật và đánh giá lại cấp độ an toàn thông tin định kỳ hằng năm hoặc khi có thay đổi về hạ tầng kỹ thuật, phạm vi dữ liệu, kết nối hệ thống để bảo đảm phù hợp với thực tế vận hành.

4. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp cần được vận hành thử, kiểm thử về tính an toàn, bảo mật trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng theo quy định tại khoản 1 Điều 9 Thông tư số 16/2024/TT-BTTTT ngày 30 tháng 12 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông 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.

5. Phương án bảo đảm an toàn hệ thống thông tin

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu theo các Nghị định của Chính phủ, Thông tư của Bộ trưởng Bộ Công an và các văn bản hướng dẫn của Bộ Công an; phù hợp với Tiêu chuẩn Quốc gia TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ và Tiêu chuẩn Quốc gia TCVN 14423:2025 An ninh mạng – Yêu cầu đối với hệ thống thông tin quan trọng; các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin (nếu có).

b) Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Đơn vị/bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

Điều 9. Bảo đảm an ninh mạng khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, đơn vị phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Cơ quan, đơn vị liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác đảm bảo an toàn thông tin, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống ra bên ngoài.

Điều 10. Quản lý giám sát an ninh mạng

1. Chủ quản hệ thống thông tin chỉ đạo việc giám sát hệ thống thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với đơn vị chuyên trách về an ninh mạng của tỉnh và lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an giám sát theo quy định.

2. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại các Nghị định của Chính phủ, Thông tư của Bộ Công an và các văn bản hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ quy định hoạt động giám sát an toàn hệ thống thông tin.

3. Đơn vị chuyên trách về an toàn thông tin của cơ quan, đơn vị cử 01 lãnh đạo đơn vị và 01 cán bộ (hoặc 01 đơn vị trực thuộc) làm đầu mối giám sát an ninh mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với đơn vị chuyên trách về an ninh mạng của tỉnh trong các hoạt động giám sát an ninh mạng tại cơ quan, đơn vị.

4. Sở Khoa học và Công nghệ có trách nhiệm tổ chức giám sát an ninh mạng đối với các hệ thống thông tin được đặt tại Trung tâm dữ liệu tỉnh. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm dữ liệu 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.

5. Định kỳ hằng 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 11. Quản lý thuê 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 ninh mạng, an ninh thông tin mạng. 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, an ninh mạng theo quy định tại Quy định này, Luật An toàn An ninh mạng năm 2025, Luật Dữ liệu năm 2024 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 ninh mạng, an ninh thông tin mạng.

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

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 12. Kiểm tra, đánh giá an ninh mạng

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị/bộ phận chuyên trách về an ninh mạng của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do mình 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. Nội dung, hình thức kiểm tra, đánh giá theo quy định các Nghị định của Chính phủ, Thông tư của Bộ Công an và các văn bản hướng dẫn của Bộ Công an.

4. Đơn vị chuyên trách về an ninh mạng của tỉnh thực hiện việc kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Tỉnh theo các Nghị định của Chính phủ, Thông tư của Bộ Công an và các văn bản hướng dẫn của Bộ Công an.

5. Đơn vị chuyên trách về an ninh mạng của tỉnh, đơn vị chuyên trách về an ninh mạng của cơ quan, đơn vị thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an ninh mạng cho phù hợp.

Điều 13. Sao lưu dữ liệu dự phòng

1. Đối với các cơ quan, đơn vị và người sử dụng

a) Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng. Khi lưu trữ, trao đổi thông tin, dữ liệu quan trọng phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

b) Phải lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ ít nhất một lần trong tháng các dữ liệu quan trọng, bao gồm: cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh, các tập tin

dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (như: đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

2. Đối với cơ quan, đơn vị chủ quản các hệ thống thông tin

a) Có trách nhiệm ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu.

b) Xây dựng 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.

c) Phải lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và được kiểm tra thường xuyên, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

Điều 14. Ứng cứu sự cố an ninh mạng

1. 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 ninh mạng.

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 ninh mạng phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị, cá nhân và 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.

2. Phân nhóm sự cố an ninh mạng

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; huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để ứng phó với các sự cố quy định tại khoản 1 điều này theo phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu hoạt động ứng cứu sự cố an toàn thông tin.

3. 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.

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

Khi có sự cố hoặc nguy cơ mất an ninh mạng xảy ra như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a) Bước 1: Nếu hệ thống có nguy cơ mất an ninh mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2.

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, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố đến Công an tỉnh và thực hiện tiếp Bước 4.

d) Bước 4: Phối hợp với Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) và các cơ quan, 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, 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.

5. 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.

6. Đơn vị/bộ phận chuyên trách về an ninh mạng có trách nhiệm.

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

b) Xây dựng quy trình ứng cứu sự cố an ninh 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 ninh mạng theo chỉ đạo của lãnh đạo.

Điều 15. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng

1. Cơ quan, đơn vị xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an ninh mạng tại đơn vị gửi Công an tỉnh. Công an tỉnh tổng hợp, xây dựng trình UBND tỉnh phê duyệt kế hoạch dài hạn, kế hoạch hằng năm về đào tạo, bồi dưỡng nghiệp vụ an ninh mạng cho cán bộ, công chức, viên chức và người lao động trên địa bàn tỉnh và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

2. Cơ quan, đơn vị tổ chức đào tạo, bồi dưỡng nghiệp vụ về an ninh mạng cho cán bộ CNTT, cán bộ chuyên trách an ninh mạng của cơ quan, đơn vị; đào tạo cơ bản về an ninh mạng cho cán bộ quản lý, người sử dụng máy tính thuộc cơ quan, đơn vị.

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

4. Công an tỉnh tổ chức tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng trên địa bàn tỉnh và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Điều 16. Bảo vệ dữ liệu cá nhân trong hệ thống thông tin

1. Đơn vị tham gia sử dụng hệ thống thông tin xử lý dữ liệu cá nhân có trách nhiệm xác định chính xác các cá nhân được phép truy cập hệ thống thông tin để xử lý dữ liệu cá nhân; gửi đề nghị thay đổi, thu hồi tài khoản truy cập hệ thống thông tin tới đơn vị vận hành hệ thống thông tin ngay sau khi có sự thay đổi phân công về xử lý dữ liệu cá nhân tại đơn vị.

2. Cá nhân được cấp tài khoản truy cập hệ thống thông tin để xử lý dữ liệu cá nhân trên hệ thống có trách nhiệm:

a) Giữ bí mật mật khẩu và bảo vệ các phương tiện xác thực khác (nếu có) để truy cập hệ thống thông tin.

b) Không thực hiện các hoạt động xử lý hoặc khai thác dữ liệu cá nhân trên hệ thống thông tin ngoài phạm vi trách nhiệm, nhiệm vụ được phân công.

c) Khi không còn được phân công xử lý dữ liệu cá nhân trên hệ thống thông tin, yêu cầu đơn vị quản lý thực hiện thay đổi, thu hồi tài khoản; có trách nhiệm bàn giao tài khoản cho người tiếp nhận công việc này theo phân công của đơn vị quản lý.

Chương III
HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Điều 17. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan, đơn vị

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) Xây dựng phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng.

b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý.

c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng.

d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ trực tuyến, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác.

đ) Triển khai kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

2. Người đứng đầu cơ quan, đơn vị có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

Điều 18. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Cơ quan, đơn vị có hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm:

1. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng theo quy định tại Luật An ninh mạng năm 2025.

2. Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất.

3. Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý.

4. Xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng, phần mềm độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp.

5. Xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền.

6. Tuân thủ các quy định liên quan khác tại Luật An ninh mạng năm 2025.

Điều 19. Lực lượng bảo vệ an ninh mạng

1. Lực lượng bảo vệ an ninh mạng của tỉnh là Tiểu ban an ninh mạng và Công an tỉnh Thái Nguyên.

2. Cơ quan, đơn vị có hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm bố trí lực lượng an ninh mạng để bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

3. Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

Chương IV
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC LIÊN QUAN

Điều 20. Trách nhiệm của Công an tỉnh

1. Là cơ quan chuyên trách về an ninh mạng của UBND tỉnh, có trách nhiệm tham mưu UBND tỉnh về công tác bảo đảm an ninh mạng trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm an ninh mạng, an ninh thông tin mạng cho các hệ thống thông tin của tỉnh.

2. Thực hiện thủ tục xác định cấp độ an ninh mạng và bảo đảm an ninh mạng cho các hệ thống thông tin theo quy định của Luật An ninh mạng năm 2025, các Nghị định của Chính phủ, Thông tư của Bộ Công an và theo các hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ, đặc biệt đối với các hệ thống thông tin đã kết nối hoặc có nhu cầu kết nối với Cơ sở dữ liệu quốc gia về dân cư, Hệ thống định danh và xác thực điện tử (Hệ thống thông tin phục vụ triển khai Đề án 06).

3. Tham mưu cho UBND tỉnh ban hành kế hoạch, hướng dẫn về công tác bảo vệ bí mật nhà nước, bảo vệ an ninh mạng, bảo vệ dữ liệu, bảo vệ dữ liệu cá nhân, phòng chống tội phạm mạng, tội phạm sử dụng công nghệ cao, lợi dụng mạng để xâm phạm an ninh trật tự, xâm phạm an ninh quốc gia trong cơ quan nhà nước trên địa bàn tỉnh.

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

5. Chủ trì, phối hợp với các cơ quan, đơn vị liên quan thanh tra, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an ninh mạng trên địa bàn tỉnh.

6. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về bảo vệ an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

7. Chỉ đạo, hướng dẫn về nghiệp vụ quản lý vận hành, kỹ thuật bảo đảm an ninh mạng; hỗ trợ giải quyết sự cố khi có yêu cầu.

8. Là cơ quan đầu mối, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an ninh mạng; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an ninh mạng trên địa bàn tỉnh. Tham gia mạng lưới ứng cứu sự cố an ninh mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu an ninh mạng quốc gia.

9. Điều tra và xử lý các tổ chức, cá nhân vi phạm pháp luật về an ninh mạng, sử dụng công nghệ cao theo thẩm quyền.

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

Điều 21. Trách nhiệm của Sở Tài chính

Trên cơ sở đề xuất của các sở, ban, ngành và các đơn vị có liên quan, căn cứ các quy định, chế độ, tiêu chuẩn, định mức, chế độ chi ngân sách hiện hành, tổng hợp, tham mưu UBND tỉnh nguồn kinh phí ngân sách địa phương theo phân cấp để thực hiện các đề án, dự án, nhiệm vụ về đảm bảo an ninh mạng.

Điều 22. Trách nhiệm của các cơ quan, đơn vị

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

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

3. Các cơ quan, đơn vị có trách nhiệm thực hiện xác định cấp độ an ninh mạng và bảo đảm an ninh mạng cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An ninh mạng năm 2025, các Nghị định của Chính phủ, Thông tư của Bộ Công an và các văn bản hướng dẫn của Bộ Công an.

4. 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 kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an tỉnh và các đơn vị liên quan trong công tác điều tra, làm rõ các hoạt động tấn công mạng.

6. Thường xuyên thông báo, báo cáo sự cố an ninh mạng (nếu có) về Công an tỉnh để phối hợp xử lý theo quy định.

Điều 23. 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 phụ trách an toàn thông tin và an ninh mạng:

a) Chịu trách nhiệm bảo đảm an ninh mạng, an ninh thông tin mạng của đơn vị.

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an ninh mạng.

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất an ninh mạng và mức độ nghiêm trọng của các rủi ro đó.

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

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

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

b) Khi tham gia vận hành mạng máy tính của cơ quan, đơn vị phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh mạng đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp.

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ, công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai như: hệ thống thư điện tử tỉnh (@thainguyen.gov.vn) hoặc hệ thống thư điện tử của bộ, ngành, lĩnh vực; hệ thống quản lý văn bản và điều hành. Mỗi cán bộ, công chức, viên chức và người lao động không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,... để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, đơn vị.

d) Khi phát hiện nguy cơ hoặc sự cố an ninh mạng phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

đ) Tham gia các chương trình đào tạo, hội nghị về an ninh mạng do các cơ quan, đơn vị chuyên trách hoặc Công an tỉnh tổ chức.

Điều 24. Trách nhiệm của các tổ chức, cá nhân khác

Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do UBND tỉnh triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Thái Nguyên phải tuân thủ Quy định này và các quy định hiện hành của pháp luật có liên quan.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 25. Kinh phí thực hiện

Kinh phí ứng dụng Công nghệ thông tin, công tác đảm bảo an ninh mạng của cơ quan, đơn vị thực hiện từ nguồn ngân sách nhà nước và các nguồn hợp pháp khác theo quy định của pháp luật.

Điều 26. 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 ninh 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 định này tại các cơ quan, đơn vị.

Điều 27. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an ninh mạng định kỳ hằng năm (trước ngày 01/12).

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng (trước ngày 01/6).

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an ninh mạng và các báo cáo đột xuất khác theo yêu cầu của Công an tỉnh hoặc yêu cầu của lãnh đạo tỉnh.

3. Trách nhiệm lập, phê duyệt báo cáo:

a) Các cơ quan, đơn vị liên quan có trách nhiệm lập báo cáo định kỳ, đột xuất theo yêu cầu và hướng dẫn của Công an tỉnh;

b) Công an tỉnh chịu trách nhiệm tập hợp, tổng hợp báo cáo của các cơ quan, đơn vị, trình UBND tỉnh phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Điều 28. Khen thưởng, kỷ luật

1. Hằng năm, Công an tỉnh căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an ninh mạng của các cơ quan, đơn vị đề xuất UBND tỉnh xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm quy định này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 29. Trách nhiệm thi hành

1. Công an tỉnh chủ trì, phối hợp với các sở, ban, ngành, UBND các xã, phường; cơ quan, đơn vị và các cá nhân, tổ chức có liên quan triển khai thực hiện tốt nội dung Quy định này.

2. Các cơ quan, đơn vị chủ động xây dựng, ban hành Quy chế nội bộ về đảm bảo an ninh mạng trong hoạt động ứng dụng CNTT tại đơn vị mình phù hợp với Quy định này.

3. Trường hợp các văn bản viện dẫn tại Quyết định này được sửa đổi, bổ sung, thay thế bằng văn bản mới thì áp dụng theo các văn bản sửa đổi, bổ sung hoặc thay thế.

Trong quá trình thực hiện Quy định này, nếu có những vấn đề khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh về UBND tỉnh (qua Công an tỉnh) để xem xét, quyết định./.