ỦY BAN NHÂN DÂN TỈNH BẮC NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 40/2025/QĐ-UBND	*Bắc Ninh, ngày 09 tháng 10 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Bắc Ninh

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

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

Căn cứ Luật An 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 85/2016/NĐ của Chính phủ Về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP của Chính phủ Bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định 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;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 2377/TTr-CAT-ANM ngày 30 tháng 9 năm 2025;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Bắc Ninh.

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Bắc Ninh.

Điều 2. Quyết định này có hiệu lực kể từ ngày 20/10/2025.

Điều 3. Thủ trưởng các sở, ban, ngành cấp tỉnh liên quan, Chủ tịch UBND các xã, phường và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Vụ pháp luật, VPCP;
- Cục KTVB&QLXLVPHC, Bộ Tư pháp;
- TT Tỉnh ủy, TT HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Đoàn ĐBQH tỉnh;
- VP Tỉnh ủy, VP Đoàn ĐBQH&HĐND tỉnh;
- UBMTTQ Việt Nam tỉnh và các TCCTXH tỉnh;
- Các cơ quan TW đóng trên địa bàn tỉnh;
- Các Sở, cơ quan thuộc UBND tỉnh;
- UBND các xã, phường;
- VP UBND tỉnh: LĐVP, các phòng, TTTT *(01 bản giấy, 01 bản điện tử đăng Công báo)*;
- Lưu: VT, NC.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Vương Quốc Tuấn

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

QUY CHẾ

Bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Bắc Ninh

(Ban hành kèm theo Quyết định số 40/2025/QĐ-UBND ngày 09/10/2025 của UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về bảo đảm an ninh mạng, an toàn thông tin mạng trong các hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh.

2. Quy chế này áp dụng đối với các sở, ban, ngành, đơn vị thuộc UBND tỉnh; UBND các xã, phường; các đơn vị sự nghiệp sử dụng ngân sách nhà nước; các cơ quan Trung ương trên địa bàn tỉnh, 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 và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT), chuyển đổi số của các cơ quan nhà nước tỉnh Bắc Ninh (sau đây gọi tắt là cơ quan, đơn vị); cán bộ, công chức, viên chức, người lao động, đang làm việc tại các cơ quan, đơn vị nêu trên.

Điều 2. Giải thích từ ngữ

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

1. An ninh an toàn mạng là viết tắt của an ninh mạng và an toàn thông tin mạng.

2. 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.

3. Mật khẩu mạnh là mật khẩu đáp ứng các yêu cầu: Có tối thiểu 12 ký tự, gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 - 9), các ký tự khác (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /).

4. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, số, hình ảnh, âm thanh hoặc dạng tương tự trong môi trường điện tử gắn với một cá nhân hoặc

giúp nhận biết một cá nhân. Việc thu thập, xử lý, chia sẻ, lưu trữ dữ liệu cá nhân phải tuân thủ quy định về bảo vệ dữ liệu cá nhân.

Điều 3. Nguyên tắc bảo đảm an ninh an toàn mạng

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an ninh an toàn mạng. Hoạt động bảo đảm an ninh an toàn mạng phải tuân quy định của pháp luật về an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước, bí mật công tác, dữ liệu cá nhân, giao dịch điện tử và các quy định khác có liên quan.

2. Bảo đảm an ninh an toàn mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

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

4. Xử lý sự cố an ninh an toàn mạng phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 8 Luật An ninh mạng và Điều 7 Luật An toàn thông tin mạng.

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

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH AN TOÀN MẠNG

Điều 5. Phân công vai trò, trách nhiệm bảo đảm an ninh an toàn mạng

1. Chủ quản hệ thống thông tin

a) Ủy ban nhân dân tỉnh là chủ quản các hệ thống thông tin do các đơn vị (bao gồm đơn vị tham mưu, đơn vị hành chính, đơn vị sự nghiệp công lập và doanh nghiệp nhà nước) thuộc phạm vi quản lý làm chủ đầu tư.

b) Cơ quan, đơn vị trực thuộc được Ủy ban nhân dân tỉnh quyết định là chủ quản hệ thống thông tin đối với các hệ thống thông tin do đơn vị tự quyết định đầu tư, nếu đáp ứng hai điều kiện sau đây:

- Một là, có đủ năng lực thực thi quy định tại khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP, cụ thể:

Người đứng đầu đơn vị phải chỉ định được đơn vị trực thuộc làm đơn vị chuyên trách về an toàn thông tin theo quy định tại khoản 5 Điều 3 và điểm b khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP;

Đơn vị được chỉ định là đơn vị chuyên trách về an toàn thông tin phải đáp ứng các điều kiện: Là một đơn vị trực thuộc của chủ quản hệ thống thông tin, có

chức năng, nhiệm vụ bảo đảm an toàn thông tin hoặc được giao nhiệm vụ là đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin; Có năng lực để bảo đảm thực thi các quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP, trong đó: có nhân sự đáp ứng yêu cầu chuyên môn, đảm bảo tổ chức thẩm định hồ sơ đề xuất cấp độ; có tư cách pháp nhân để ban hành quyết định phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được đề xuất cấp độ 1, 2 theo thẩm quyền được giao tại khoản 1 Điều 12 Nghị định số 85/2016/NĐ-CP, phù hợp các quy định của pháp luật về dân sự và các quy định của pháp luật có liên quan;

- Hai là, có đủ năng lực để thực thi đầy đủ các quy định tại khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP.

c) Trách nhiệm của chủ quản hệ thống thông tin quy định tại khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP.

2. Đơn vị chuyên trách về an toàn thông tin

a) Công an tỉnh đảm nhiệm vai trò đơn vị chuyên trách về an toàn thông tin đối với các hệ thống thông tin do UBND tỉnh làm chủ quản.

b) Chủ quản hệ thống thông tin thành lập hoặc chỉ định bộ phận chuyên trách an toàn thông tin thuộc đơn vị của chủ quản hệ thống thông tin.

c) Công an tỉnh là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an ninh an toàn mạng phục vụ việc bảo đảm an ninh an toàn mạng cho các hệ thống thông tin do UBND tỉnh làm chủ quản.

d) Công an tỉnh là đầu mối, tổ chức thực hiện việc tiếp nhận và điều phối, xử lý các sự cố về an ninh an toàn mạng. Phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an và các đơn vị có liên quan, hướng dẫn xử lý, ứng cứu các sự cố an ninh an toàn mạng.

đ) Đơn vị chuyên trách về an toàn thông tin mạng thực hiện nhiệm vụ theo quy định của pháp luật và các nhiệm vụ khác do chủ quản hệ thống thông tin giao.

3. Đơn vị vận hành hệ thống thông tin

a) Là cơ quan, đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

b) Là chủ đầu tư dự án đối với các dự án đầu tư, chủ trì thuê dịch vụ công nghệ thông tin.

c) Trường hợp hệ thống thông tin đang trong thời gian thuê dịch vụ công nghệ thông tin, đơn vị cung cấp dịch vụ thực hiện vai trò đơn vị vận hành hệ thống thông tin.

d) Trách nhiệm của đơn vị vận hành hệ thống thông tin quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP.

đ) Ban hành, tham mưu ban hành Quy chế quản lý, vận hành, khai thác, đảm bảo an ninh an toàn hệ thống thông tin.

e) Đối với hệ thống thông tin đáp ứng tiêu chí hệ thống thông tin quan trọng về an ninh quốc gia, đơn vị vận hành hệ thống thông tin lập hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trình UBND tỉnh (thông qua Công an tỉnh) gửi Bộ Công an thẩm định.

Điều 6. Bảo đảm, quản lý nguồn nhân lực

1. Việc tuyển dụng công chức, viên chức làm về an ninh an toàn mạng thực hiện theo quy định của pháp luật.

2. Trong quá trình làm việc

a) Đối với người dùng

- Có trách nhiệm tuân thủ các quy định, hướng dẫn bảo đảm an ninh an toàn mạng, bảo vệ dữ liệu cá nhân và các quy định khác của pháp luật đối với từng vị trí công việc;

- Thông báo ngay cho đơn vị chủ quản hệ thống thông tin khi nghi ngờ hoặc phát hiện sự cố, hiện tượng bất thường của hệ thống thông tin;

- Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về an ninh an toàn mạng;

- Đổi mật khẩu ngay sau khi được cấp tài khoản đăng nhập các dịch vụ, ứng dụng của UBND. Giữ bí mật tài khoản cá nhân khi tham gia khai thác, sử dụng, không ghi mật khẩu ra những nơi người khác có thể biết; không lưu trữ, truyền, gửi mật khẩu khi chưa được mã hóa an toàn và chia sẻ mật khẩu của cá nhân cho người khác; định kỳ 3 tháng phải thay đổi mật khẩu hoặc ngay sau khi nghi ngờ tài khoản có dấu hiệu bị lộ, lọt;

- Chịu trách nhiệm quản lý, sử dụng trang thiết bị CNTT được giao bảo đảm an ninh an toàn mạng; không được giao cho các tổ chức, cá nhân khác sử dụng trang thiết bị CNTT đã được giao sử dụng; không được sử dụng trang thiết bị CNTT cá nhân để kết nối, truy cập vào các hệ thống thông tin nội bộ nếu chưa được phép của đơn vị chủ quản; không tự thay thế, lắp mới, thay đổi thành phần của máy tính công vụ; không mang tài sản CNTT của đơn vị ra ngoài nếu chưa được phép của thủ trưởng đơn vị; có trách nhiệm bàn giao cho đơn vị quản lý các trang thiết bị CNTT khi chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ việc;

- Thực hiện soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ tài liệu mật tại máy tính được trang bị cho việc soạn thảo, lưu trữ văn bản mật theo quy định. Không sử dụng thiết bị lưu trữ ngoài để lưu thông tin, tài liệu mật, trừ trường hợp có áp dụng các biện pháp mã hóa do Ban Cơ yếu Chính phủ cung cấp;

- Không tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên máy tính phục vụ công việc.

b) Đối với cán bộ quản lý, vận hành hệ thống

- Tuân thủ nghiêm ngặt theo các quy trình, quy định, nội quy đơn vị đã

được ban hành và phải chịu trách nhiệm nếu sự cố xảy ra nghiêm trọng;

- Phân rõ trách nhiệm quản lý, vận hành hệ thống thông tin đến từng cá nhân; không giao cho một người quản trị tất cả chức năng về an ninh an toàn mạng của hệ thống thông tin;

- Việc khai thác thông tin, dữ liệu phải bảo đảm nguyên tắc bảo mật, an toàn thông tin, không được tự ý cung cấp thông tin, dữ liệu ra bên ngoài;

- Khi thực hiện các nghiệp vụ chuyên môn có sự tác động đến các thiết bị, hệ thống phải được ghi chép cụ thể vào sổ Nhật ký hệ thống.

c) Đối với cơ quan, tổ chức

- Định kỳ hằng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an ninh an toàn mạng cho người dùng;

- Định kỳ hằng năm tổ chức đào tạo hoặc cử đi đào tạo về an ninh an toàn mạng cho cán bộ kỹ thuật, cán bộ quản lý, người sử dụng trong hệ thống;

- Phối hợp với Công an tỉnh tham mưu xây dựng, triển khai kế hoạch đào tạo, bồi dưỡng, tập huấn về công tác bảo đảm an ninh an toàn mạng cho đội ngũ công chức, viên chức của cơ quan, đơn vị.

3. Đối với công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc

a) Công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải tuân thủ:

- Phải bàn giao lại công việc, tài khoản truy cập hệ thống thông tin, tài sản CNTT của cơ quan, đơn vị;

- Phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc: Không tiết lộ thông tin được tiếp xúc trong quá trình công tác tại đơn vị cho các cá nhân, tổ chức gây ảnh hưởng bất lợi đến lợi ích của đơn vị; Không sử dụng các thông tin được tiếp xúc trong quá trình công tác tại đơn vị vào mục đích trục lợi cá nhân.

b) Quy trình thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động thôi việc:

- Thu hồi tài khoản truy cập, các trang thiết bị máy móc, phần cứng và các tài sản khác thuộc sở hữu của đơn vị quản lý;

- Vô hiệu hóa các thông tin của công chức, viên chức, người lao động thôi việc được lưu trên các phương tiện lưu trữ, phần mềm;

- Vô hiệu hóa tất cả các quyền truy cập của công chức, viên chức, người lao động thôi việc vào tài nguyên, hệ thống phần mềm của đơn vị quản lý;

- Kiểm tra lại các quyền ra vào, truy cập tài nguyên, quản trị hệ thống đã

cấp cho công chức, viên chức, người lao động thôi việc để bảo đảm đã hoàn toàn được gỡ bỏ khỏi hệ thống.

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin:

a) Tài liệu phân tích lựa chọn kiến trúc, công nghệ.

b) Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống.

c) Các vùng mạng trong hệ thống: Vùng mạng nội bộ; vùng mạng biên; vùng mạng DMZ; vùng máy chủ nội bộ; vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; vùng mạng máy chủ cơ sở dữ liệu; vùng quản trị; vùng quản trị thiết bị hệ thống.

d) Các giải pháp, thiết bị của hệ thống thông tin đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư số 12/2022/TT-BTTTT).

2. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả "Kiến trúc hệ thống" trong đó có mô tả thiết kế và các thành phần của hệ thống thông tin thông qua một số mô hình kiến trúc khác nhau nhằm mô tả hệ thống dưới nhiều góc nhìn khác nhau, bao gồm:

a) Thiết kế kiến trúc ứng dụng;

b) Thiết kế kiến trúc dữ liệu;

c) Thiết kế kiến trúc vật lý.

3. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả phương án bảo đảm an toàn thông tin theo từng cấp độ tương ứng với hồ sơ đề xuất cấp độ được quy định tại Thông tư số 12/2022/TT-BTTTT.

4. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin, trong đó cần bảo đảm các tiêu chí:

a) Bảo đảm có từ 2 - 3 công nghệ được phân tích và đưa ra phương án lựa chọn.

b) Phân tích các ưu, nhược điểm của từng công nghệ để từ đó chọn ra công nghệ áp dụng phù hợp nhất.

5. Khi có thay đổi thiết kế, đơn vị được giao chủ trì cần phối hợp với các đơn vị liên quan đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an ninh an toàn mạng đặt ra đối với hệ thống, xây dựng lại hồ sơ đề xuất cấp độ cho hệ thống và trình cấp có thẩm quyền thẩm định, phê duyệt theo quy định.

6. Phương án quản lý và bảo vệ hồ sơ thiết kế

a) Hồ sơ thiết kế không được tùy tiện cung cấp cho cá nhân, đơn vị khác không có đủ thẩm quyền;

b) Hồ sơ thiết kế được bảo quản, lưu trữ theo quy định.

Điều 8. Phát triển và nghiệm thu phần mềm, hệ thống

1. Đối với các nội dung liên quan đến việc phát triển phần mềm thuê khoán, nhà phát triển phải bảo đảm có các cam kết bảo đảm an ninh an toàn mạng. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Nhà phát triển phải cung cấp mã nguồn sản phẩm cho đơn vị thuê theo hình thức ghi đĩa DVD hoặc USB; yêu cầu DVD, USB cần phải đặt mật khẩu để bảo đảm an ninh an toàn mạng; Mã nguồn đã được nhà phát kiểm thử nội bộ trước khi bàn giao.

3. Phần mềm phải được kiểm thử tại ít nhất một đơn vị thụ hưởng trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng.

4. Phần mềm phải được kiểm tra, đánh giá an ninh an toàn mạng trước khi đưa vào sử dụng.

5. Hoạt động thử nghiệm và nghiệm thu hệ thống thực hiện theo hướng dẫn tại Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của 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.

Điều 9. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn.

g) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

h) Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

i) Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

k) Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

a) 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.

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c) Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d) Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) 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.

4. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 10. Quản lý an toàn máy chủ và ứng dụng

1. Quy định với máy chủ

a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để bảo đảm hoạt động liên tục.

b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ.

c) Máy chủ phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; thực hiện biện pháp phòng chống xâm nhập; phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao.

d) Máy chủ phải được nâng cấp, xử lý điểm yếu an ninh an toàn mạng trên máy chủ trước khi đưa vào sử dụng.

đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.

e) Phần mềm hệ điều hành cài lên máy chủ phải có bản quyền hoặc phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.

g) Người quản trị chỉ được cấp quyền truy cập vào các máy chủ có thẩm quyền. Để được cấp tài khoản quản trị phải gửi công văn xin cấp bao gồm các thông tin tối thiểu: Tên, căn cước công dân, số điện thoại, phòng ban đơn vị công tác, mục đích, phạm vi máy chủ cần truy cập và được phê duyệt bởi đơn vị quản lý hệ thống thông tin.

h) Ghi nhật ký, quy định thời gian về hoạt động tác động vào các máy chủ, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra giám sát về sau.

2. Quy định với ứng dụng

a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần bảo đảm nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật.

b) Ứng dụng phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải bảo đảm trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

đ) Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

3. Quy định với ứng dụng thư điện tử

a) Không sử dụng các hộp thư điện tử công cộng trong công việc; không sử dụng thư điện tử công vụ vào mục đích cá nhân.

b) Mỗi cá nhân cần đặt mật khẩu mạnh cho hộp thư điện tử của mình.

c) Khi công chức, viên chức, người lao động nghỉ việc thì hộp thư điện tử sẽ bị khóa và xóa bỏ khỏi hệ thống thư điện tử.

d) Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án bảo đảm an toàn và tính khả dụng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử.

đ) Bảo đảm an toàn cho hệ thống thư điện tử theo quy định.

4. Quy định đối với Cổng, trang thông tin điện tử

a) Quản lý toàn bộ các phiên bản của mã nguồn, tổ chức mô hình Cổng, trang thông tin điện tử hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu hệ thống thông tin của Cổng, trang thông tin điện tử phải có các hệ thống phòng vệ như tường lửa, thiết bị phát hiện, phòng chống xâm nhập (IDS/IPS), tường lửa web (WAF- Web Application Firewall).

b) Cổng, trang thông tin điện tử khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (XSS).

c) Xây dựng phương án sao lưu, phục hồi Cổng, trang thông tin điện tử, trong đó chú ý mỗi tháng thực hiện việc sao lưu dữ liệu toàn bộ nội dung Cổng, trang thông tin điện tử một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

d) Bảo đảm an toàn cho Cổng, trang thông tin điện tử theo quy định.

Điều 11. Quản lý an toàn dữ liệu

1.Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để bảo đảm sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an ninh an toàn mạng xảy ra.

3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống.

4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

7. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

8. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ, phương tiện lưu trữ.

9. Dữ liệu sao lưu được khôi phục trong các trường hợp: có yêu cầu khôi phục dữ liệu từ người dùng; ứng dụng, cơ sở dữ liệu đang hoạt động bị sự cố, cần khôi phục từ bản sao lưu; hoặc theo yêu cầu của cơ quan có thẩm quyền.

Điều 12. Quản lý an toàn thiết bị đầu cuối

Các thiết bị đầu cuối khi kết nối vào hệ thống phải được quản lý như sau:

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

5. Kiểm tra, đánh giá, xử lý điểm yếu an ninh an toàn mạng cho thiết bị đầu cuối trước khi đưa vào sử dụng.

6. Quy định đối với máy tính kết nối mạng truyền số liệu chuyên dùng

a) Sử dụng hệ điều hành có bản quyền được hỗ trợ bản vá lỗ hổng bảo mật; trường hợp đã hết hỗ trợ phải có kế hoạch nâng cấp, thay thế. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn. Cài đặt phần mềm phòng chống mã độc và cập nhật phần mềm thường xuyên.

b) Không kết nối với mạng không dây (wifi), mạng dữ liệu di động.

c) Máy tính trước khi kết nối vào truyền số liệu chuyên dùng phải đáp ứng được quy định tại điểm a của khoản này; ngắt kết nối mạng của máy tính không đáp ứng quy định.

d) Máy tính khi được chuyển sử dụng từ cá nhân này sang cá nhân khác hoặc không tiếp tục sử dụng cho công việc của cơ quan phải thực hiện xóa toàn bộ dữ liệu trên ổ cứng và có biên bản về việc xóa dữ liệu. Máy tính khi mang đi bảo hành, bảo dưỡng, sửa chữa, phải tháo ổ cứng hoặc xóa dữ liệu lưu trên ổ cứng.

7. Máy tính soạn thảo, lưu trữ bí mật nhà nước

a) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền. Không kết nối vào mạng Internet, mạng nội bộ, mạng không dây, mạng viễn thông, trừ trường hợp đã áp dụng các biện pháp bảo vệ theo quy định. Không sử

dụng thiết bị lưu trữ ngoại vi, trừ trường hợp cần cài đặt hệ điều hành, sửa chữa, nâng cấp phần mềm cho máy tính hoặc phục vụ công tác kiểm tra, thanh tra về an ninh an toàn mạng;

b) Phân quyền truy cập máy tính theo tên người hoặc đơn vị cấp phòng được giao soạn thảo bí mật nhà nước.

c) Trường hợp ổ cứng lỗi cần mang đi bảo hành, phải thực hiện biện pháp xóa dữ liệu vĩnh viễn trước khi mang ổ cứng ra khỏi cơ quan. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng), nếu yêu cầu phải tiếp cận các tệp tin trên ổ cứng, phải thực hiện dưới sự giám sát của đơn vị sử dụng máy tính, đảm bảo không lộ lọt dữ liệu trên ổ cứng máy tính ra bên ngoài trong quá trình này.

d) Đơn vị được cấp sử dụng máy tính soạn thảo, lưu trữ bí mật nhà nước chịu trách nhiệm giám sát, đảm bảo việc sử dụng máy tính tuân thủ đúng quy định tại khoản này.

8. Trường hợp máy tính xách tay được cơ quan trang bị để sử dụng bên ngoài trụ sở cơ quan, nếu kết nối Internet, phải cài đặt hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật và phần mềm phòng chống mã độc, phải cập nhật thường xuyên bản vá cho hệ điều hành và mẫu nhận diện mã độc do nhà sản xuất cung cấp.

9. Đối với máy tính bảng được cơ quan trang bị để phục vụ công việc phải sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt phần mềm phục vụ công việc và các phần mềm theo hướng dẫn cơ quan chức năng.

10. Máy tính do người dùng tự trang bị khi kết nối vào mạng truyền số liệu chuyên dùng phải đáp ứng đầy đủ các điều kiện dưới đây:

a) Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành; cài đặt phần mềm phòng chống mã độc và cập nhật mẫu nhận diện mã độc mới nhất.

b) Không cài đặt, sử dụng phần mềm, công cụ có tính năng hoặc tạo rủi ro mất an ninh an toàn mạng (như cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công).

Điều 13. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe).

3. Các cán bộ, công chức, viên chức, người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được

tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

5. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

6. Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

7. Máy chủ, máy trạm chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

Điều 14. Giám sát an ninh an toàn mạng

1. Trình tự, thủ tục giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia quy định tại Điều 15 Nghị định 53/2022/NĐ-CP.

2. Nguyên tắc, yêu cầu, phương thức về hoạt động giám sát an toàn hệ thống thông tin thực hiện theo quy định tại Thông tư số 31/2017/TT- BTTTT.

3. Chủ quản hệ thống thông tin chỉ đạo thực hiện giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý.

4. Công an tỉnh làm đầu mối giám sát, cảnh báo an ninh an toàn mạng của tỉnh; chịu trách nhiệm tổ chức, triển khai, thực hiện giám sát an ninh, an toàn hệ thống thông tin tập trung trên địa bàn tỉnh và bảo đảm kết nối, chia sẻ thông tin với hệ thống giám sát của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Bộ Công an.

5. Các cơ quan, đơn vị cử cá nhân hoặc bộ phận làm đầu mối giám sát, cung cấp, tiếp nhận thông tin cảnh báo, kịp thời với đơn vị chuyên trách về an toàn thông tin của tỉnh nhằm tăng cường công tác đảm bảo an ninh an toàn mạng và phòng, chống tội phạm sử dụng công nghệ cao. Đầu mối giám sát thực hiện bảo đảm các điều kiện cho hoạt động kết nối tại điểm giám sát và triển khai giám sát trong phạm vi hệ thống thông tin của cơ quan, đơn vị mình.

6. Công tác triển khai: Hệ thống giám sát trung tâm; thông tin giám sát và danh mục các đối tượng giám sát; thực thi nhiệm vụ giám sát; nâng cao năng lực hoạt động giám sát; trách nhiệm giám sát an toàn thông tin của các Hệ thống thông tin của tỉnh được thực hiện theo Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

Điều 15. Quản lý rủi ro, lỗ hổng, điểm yếu an ninh an toàn mạng

1. Đơn vị vận hành hệ thống thông tin có trách nhiệm:

a) Quản lý thông tin điểm yếu an ninh an toàn mạng đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Lập danh sách toàn bộ thiết bị, phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý của chủ quản hệ thống thông tin: nhãn hiệu phần cứng, tên phần mềm và phiên bản (hệ điều hành, cơ sở dữ liệu, ứng dụng, các tiện ích khác).

c) Thiết lập, duy trì kênh tiếp nhận thông tin về lỗ hổng, điểm yếu an ninh an toàn mạng từ các cơ quan, tổ chức có chức năng cảnh báo về an ninh an toàn mạng; các đơn vị cung cấp thiết bị, phần mềm công nghệ thông tin thuộc phạm vi quy định tại điểm b khoản này. Phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an ninh an toàn mạng đối với các điểm yếu khi cần thiết.

d) Quản trị viên hệ thống báo cáo lãnh đạo, cán bộ quản lý ngay khi phát hiện điểm yếu an ninh an toàn mạng ở mức độ nghiêm trọng; thực hiện cảnh báo và xử lý điểm yếu an ninh an toàn mạng theo chỉ đạo. Việc xử lý điểm yếu an ninh an toàn mạng phải bảo đảm không làm ảnh hưởng, gián đoạn hoạt động của hệ thống.

đ) Quản lý, giám sát việc cài đặt bản vá lỗ hổng, điểm yếu an ninh an toàn mạng. Sử dụng và cập nhật liên tục các công cụ dò quét lỗ hổng, điểm yếu an ninh an toàn mạng để các công cụ này có thể phát hiện được các lỗ hổng bảo mật mới nhất; hoặc sử dụng kết quả kiểm tra, đánh giá an ninh an toàn mạng để xác định các lỗ hổng, điểm yếu của hệ thống thông tin.

e) Triển khai cài đặt bản vá lỗ hổng, điểm yếu an ninh an toàn mạng sau khi bản vá được phát hành; Áp dụng các biện pháp bảo vệ tạm thời trong trường hợp bản vá bảo mật chưa được phát hành hoặc chưa đủ điều kiện để triển khai.

g) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an ninh an toàn mạng chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

2. Đối với hệ thống, hệ thống thành phần được đề xuất cấp độ phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an ninh an toàn mạng cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

3. Định kỳ hằng năm kiểm tra, đánh giá điểm yếu an ninh an toàn mạng cho toàn bộ hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an ninh an toàn mạng khi có thông tin hoặc nhận được cảnh báo.

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định

số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

5. Đơn vị vận hành hệ thống thông tin triển khai quản lý rủi ro an ninh an toàn mạng trên cơ sở quản lý lỗ hổng, điểm yếu an ninh an toàn mạng theo quy định tại khoản 1 Điều này và theo hướng dẫn của cơ quan chức năng.

Điều 16. Ứng cứu sự cố an ninh an toàn mạng

1. Đơn vị chuyên trách về ứng cứu sự cố an ninh an toàn mạng (gọi tắt là Đơn vị chuyên trách ứng cứu sự cố)

a) Công an tỉnh đảm nhiệm vai trò đơn vị chuyên trách ứng cứu sự cố an ninh an toàn mạng của UBND tỉnh, chịu trách nhiệm triển khai công tác ứng cứu sự cố các hệ thống thông tin do UBND tỉnh làm chủ quản.

b) Đơn vị chuyên trách ứng cứu sự cố trình chủ quản hệ thống thông tin thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý.

c) Các đơn vị thuộc UBND tỉnh có trách nhiệm phối hợp đơn vị chuyên trách ứng cứu sự cố và các thành viên trong Đội ứng cứu sự cố trong công tác ứng cứu sự cố.

2. 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 an toàn 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 an toàn mạng 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.

3. Phân loại 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; tấn công truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; tấn công phá hoại thông tin, dữ liệu, phần mềm; tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu.

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

c) Sự cố do lỗi của công chức, viên chức quản trị, vận hành hệ thống.

d) Sự cố do các thảm họa tự nhiên.

4. Phân loại mức độ nghiêm trọng sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp.

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

5. 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 thuộc Sở Khoa học và Công nghệ quản lý (các hệ thống dùng chung của 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 03 của Thông tư số 20/2017/TT-BTTTT và thực hiện tiếp Bước 4.

d) Bước 4: Phối hợp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Công an tỉnh; Sở Khoa học và Công nghệ 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 04 của Thông tư số 20/2017/TT-BTTTT, 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.

6. 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, Cục an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an để được hướng dẫn, hỗ trợ.

7. Trình tự, thủ tục, phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia quy định tại Điều 17, Điều 25 Nghị định số 53/2022/NĐ-CP.

Điều 17. Kết thúc sử dụng hệ thống thông tin

1. Hệ thống thông tin phải kết thúc sử dụng khi: đã được thay thế hoàn toàn bằng hệ thống thông tin khác; hoặc không còn giá trị sử dụng; hoặc sử dụng phiên bản phần mềm có lỗ hổng bảo mật nghiêm trọng và không có biện pháp ngăn chặn việc khai thác các lỗ hổng bảo mật này; hoặc các thành phần tài sản của hệ thống thông tin đã hết thời gian khấu hao sử dụng theo quy định pháp luật về quản lý, sử dụng tài sản công và được cấp có thẩm quyền cho phép dừng sử dụng.

2. Thủ tục kết thúc vận hành, khai thác, hủy bỏ hệ thống thông tin:

a) Đơn vị vận hành hệ thống thông tin báo cáo chủ quản hệ thống thông tin cho phép kết thúc vận hành, khai thác hệ thống thông tin.

b) Đơn vị vận hành thực hiện dừng hoạt động của hệ thống; thu hồi tài nguyên máy chủ ảo hóa (nếu hệ thống thông tin sử dụng nền tảng ảo hóa) hoặc xóa bỏ hoàn toàn (không có khả năng phục hồi) nội dung thông tin, dữ liệu trên thiết bị vật lý với sự xác nhận của chủ quản hệ thống thông tin trước khi chuyển sang bộ phận quản lý tài sản chờ thanh lý; thu hồi địa chỉ mạng, cấu hình trên hệ thống mạng, hệ thống an ninh, an toàn thông tin áp dụng cho hệ thống thông tin.

3. Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

4. Việc thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin được thực hiện theo quy định của pháp luật hiện hành.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN NINH AN TOÀN MẠNG

Điều 18. Trách nhiệm của Công an tỉnh

1. Tham mưu UBND tỉnh về công tác bảo đảm an ninh an toàn mạng trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm an toàn cho các hệ thống thông tin cấp tỉnh.

2. Xây dựng và triển khai các Kế hoạch, chương trình, đào tạo về an ninh an toàn mạng trên địa bàn tỉnh.

3. Tùy theo mức độ sự cố, phối hợp Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Bộ Công an và các đơn vị có liên quan hướng dẫn điều phối, xử lý, ứng cứu các sự cố an ninh an toàn mạng trên địa bàn tỉnh;

cảnh báo các vấn đề về an ninh an toàn mạng trong các cơ quan nhà nước trên địa bàn tỉnh.

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

5. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền đến các phương tiện truyền thông đại chúng trên địa bàn tỉnh về công tác bảo đảm an ninh an toàn mạng.

6. Hằng năm, tổ chức đào tạo hoặc cử nhân sự tham gia các khoá đào tạo chuyên sâu về an ninh an toàn mạng cho cán bộ làm công tác bảo đảm an ninh an toàn mạng của các cơ quan, đơn vị.

7. Tham mưu xây dựng kế hoạch và tổ chức kiểm tra định kỳ, kiểm tra đột xuất công tác bảo đảm an ninh an toàn mạng; đánh giá việc thực hiện bảo đảm an toàn hệ thống thông tin theo cấp độ tại các cơ quan, đơn vị.

8. Tổ chức đánh giá an ninh an toàn mạng cho các hệ thống thông tin dùng chung, hạ tầng Trung tâm tích hợp dữ liệu của tỉnh hằng năm theo quy định.

9. Kiểm tra, đánh giá an ninh, an toàn các thiết bị xử lý thông tin trước khi đưa vào sử dụng.

10. Điều tra và xử lý các tổ chức, cá nhân vi phạm pháp luật về an ninh an toàn mạng theo thẩm quyền.

Điều 19. Trách nhiệm của Sở Khoa học và Công nghệ

1. Quản lý, vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng trên địa bàn tỉnh; xử lý các vấn đề liên quan sự cố mạng truyền số liệu chuyên dùng.

2. Hướng dẫn, hỗ trợ sao lưu dự phòng các thông tin, cơ sở dữ liệu của các cơ quan nhà nước một cách an toàn.

3. Chịu trách nhiệm quản trị, vận hành và bảo đảm an ninh an toàn mạng cho các hệ thống thông tin dùng chung của tỉnh.

4. Thông báo cho cán bộ đầu mối về CNTT/an ninh an toàn mạng tại các cơ quan, đơn vị thời gian cụ thể khi có cập nhật thay đổi hệ thống hoặc báo ngay cho các đầu mối khi có sự cố của các hệ thống thông tin dùng chung để các đơn vị chủ động thông báo cho đơn vị.

5. Hướng dẫn xây dựng, triển khai mô hình kết nối mạng nội bộ (LAN) bảo đảm an ninh an toàn mạng chung cho các cơ quan, đơn vị triển khai thực hiện.

Điều 20. Trách nhiệm của các cơ quan, đơn vị

1. Tổ chức triển khai thực hiện Quy chế này và các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an ninh an toàn mạng trong phạm vi đơn vị.

2. Ban hành quy chế/quy định/nội quy về an ninh an toàn mạng của đơn vị phù hợp với trách nhiệm của đơn vị theo Quy chế này và các quy định của pháp luật về an ninh an toàn mạng.

3. Báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Công an.

4. Bố trí nhân lực chuyên trách hoặc kiêm nhiệm tại các cơ quan, đơn vị để thực hiện công tác bảo đảm an ninh an toàn mạng.

5. Khi được kiểm tra công tác bảo đảm an ninh an toàn mạng tại cơ quan, đơn vị cử cán bộ có chuyên môn tham gia đoàn kiểm tra; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác bảo đảm an ninh an toàn mạng.

Điều 21. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong cơ quan nhà nước

1. Tuân thủ quy chế này và các quy định khác của pháp luật về bảo đảm an ninh an toàn mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an ninh an toàn hệ thống thông tin, phải thông báo ngay đến cán bộ chuyên trách hoặc kiêm nhiệm an ninh an toàn mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật do không tuân thủ Quy chế.

3. Cán bộ chuyên trách hoặc kiêm nhiệm an ninh an toàn mạng:

a) Theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành bảo đảm an toàn hệ thống thông tin tại cơ quan, đơn vị;

b) Hướng dẫn, hỗ trợ người dùng tại cơ quan, đơn vị giải pháp phòng, chống mã độc. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro.

c) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an ninh an toàn mạng; tham gia khắc phục các sự cố mất an ninh an toàn mạng.

Điều 22. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và Internet

1. Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Công an, Bộ Khoa học và Công nghệ về an ninh an toàn mạng và các nội dung quy định tại Quy chế này.

2. Phối hợp với Công an tỉnh tham gia các hoạt động điều phối, ứng cứu, khắc phục sự cố thông tin bảo đảm an ninh an toàn mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác sử dụng dịch vụ.

3. Bảo đảm mạng truyền số liệu chuyên dùng cung cấp cho các cơ quan, đơn vị được thông suốt, ổn định.

Điều 23. Trách nhiệm của tổ chức, cá nhân khác khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an ninh an toàn mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an ninh an toàn hệ thống thông tin, phải thông báo ngay với cơ quan nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng CNTT trên địa bàn tỉnh chịu sự thanh tra, kiểm tra của các cơ quan nhà nước có thẩm quyền về lĩnh vực an ninh an toàn mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 24. Kinh phí thực hiện

1. Sở Tài chính chủ trì, phối hợp với Công an tỉnh và các cơ quan, tổ chức rà soát, cân đối, tham mưu Ủy ban nhân dân tỉnh bảo đảm nguồn kinh phí triển khai, thực hiện các mặt công tác bảo đảm an ninh an toàn mạng trên địa bàn tỉnh.

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

Điều 25. Trách nhiệm thi hành

1. Công an tỉnh chủ trì, phối hợp với các sở, ban, ngành, UBND các xã, phường và các tổ chức, cá nhân có liên quan triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, tổ chức, cá nhân kịp thời báo cáo về Công an tỉnh tổng hợp, trình UBND tỉnh xem xét, quyết định./.