ỦY BAN NHÂN DÂN TỈNH LÀO CAI	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 460 /QĐ-UBND	*Lào Cai, ngày 13 tháng 02 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh Lào Cai

ỦY BAN NHÂN DÂN TỈNH LÀO CAI

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

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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

Căn cứ 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;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 01/10/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 01/7/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 01/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 01/10/2022 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức không gian mạng đến năm 2025, tầm nhìn 2030;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 1365/TTr-CAT-ANM ngày 06/02/2026.

QUYẾT ĐỊNH:

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

Điều 2. Hiệu lực thi hành.

1. Quyết định này có hiệu lực thi hành kể từ ngày ký.

2. Bãi bỏ toàn bộ các quyết định sau:

a) Quyết định số 24/2012/QĐ-UBND ngày 04/7/2012 của Ủy ban nhân dân tỉnh Yên Bái ban hành quy định đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin trong các cơ quan, đơn vị hành chính nhà nước trên địa bàn tỉnh Yên Bái;

b) Quyết định số 61/2021/QĐ-UBND ngày 21/12/2021 của Ủy ban nhân dân tỉnh Lào Cai ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Công an tỉnh, Thủ trưởng các sở, ban, ngành, đơn vị sự nghiệp thuộc Ủy ban nhân dân tỉnh, Chủ tịch Uỷ ban nhân dân các xã, phường và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- TT. Tỉnh ủy;
- Chủ tịch UBND tỉnh;
- Các PCT UBND tỉnh;
- Cục ANM và PCTPSDCNC, Bộ Công an;
- Văn phòng Tỉnh ủy;
- Chánh, các PCVP UBND tỉnh;
- Các chuyên viên tham mưu tổng hợp;
- Lưu: VT, HCC, CTTĐT, NC.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Ngô Hạnh Phúc

ỦY BAN NHÂN DÂN **TỈNH LÀO CAI**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ
Bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh Lào Cai

(Ban hành kèm theo Quyết định số: 460 /QĐ-UBND ngày 13 /02/2026 của Ủy ban nhân dân tỉnh Lào Cai)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế quy định cụ thể về nguyên tắc, nội dung, trách nhiệm, cơ chế phối hợp và các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong quá trình xây dựng, quản lý, vận hành, khai thác và sử dụng các hệ thống thông tin, cơ sở dữ liệu, hạ tầng kỹ thuật công nghệ thông tin phục vụ hoạt động của các cơ quan nhà nước, đơn vị sự nghiệp công lập và chính quyền hai cấp trên địa bàn tỉnh Lào Cai. Ngoài ra, Quy chế cũng quy định các yêu cầu về bảo vệ dữ liệu cá nhân, dữ liệu nội bộ, ứng cứu và khôi phục hệ thống khi xảy ra sự cố an ninh mạng, nhằm bảo đảm an toàn, thông suốt cho các hệ thống thông tin của tỉnh.

2. Quy chế này được áp dụng cho các sở, ban, ngành, đơn vị sự nghiệp thuộc Ủy ban nhân dân tỉnh, Ủy ban nhân dân cấp xã, cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân khác có liên quan đến việc quản lý, vận hành, khai thác các hệ thống thông tin trên địa bàn tỉnh Lào Cai.

Điều 2. Giải thích từ ngữ

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

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

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

4. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

5. *Đơn vị vận hành hệ thống thông tin* là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

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

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

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

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

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

11. *Phần mềm độc hại (virus)* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

12. *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.

13. *Thiết bị đầu cuối* là thiết bị công nghệ thông tin cố định hoặc di động được kết nối vào hệ thống thông tin trên môi trường mạng để gửi, truyền, nhận và xử lý thông tin, ví dụ như máy tính để bàn, laptop, máy tính bảng, điện thoại thông minh, máy in, máy scan...

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

1. Việc bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin, phải tuân thủ các quy định của pháp luật về an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước, bí mật công tác, thông tin, dữ liệu cá nhân và các quy định khác có liên quan. Đồng thời, phải gắn với cải cách hành chính, chuyển đổi số và sử dụng hiệu quả ngân sách nhà nước.

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

3. Việc tổ chức triển khai bảo đảm an toàn thông tin theo cấp độ cho hệ thống thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, trong quá trình vận hành, khai thác, nâng cấp, phát triển mở rộng, cho đến hủy bỏ hệ thống, tuân thủ các quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT, Tiêu chuẩn quốc gia Việt Nam TCVN 11930:2017 về công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

4. Các sở, ban, ngành, Ủy ban nhân dân cấp xã có trách nhiệm bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin của đơn vị mình; bố trí nhân sự chuyên trách/kiêm nhiệm chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của thủ trưởng đơn vị, của từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an ninh, an toàn thông tin mạng.

5. Cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan có trách nhiệm bảo đảm an ninh mạng, an toàn thông tin trong phạm vi xử lý công việc của mình theo quy định tại Quy chế này và các quy định liên quan.

6. Thông tin thuộc danh mục bí mật nhà nước phải được bảo vệ theo quy định của pháp luật về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

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

Điều 4. Các hành vi bị nghiêm cấm

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

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

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

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Bảo đảm an ninh mạng, an toàn thông tin thiết bị đầu cuối trong hệ thống thông tin

1. Giao, gắn trách nhiệm bằng văn bản cho cá nhân hoặc tập thể quản lý, sử dụng thiết bị đầu cuối.

a) Khi giao thiết bị đầu cuối cho cán bộ, công chức, viên chức, người lao động sử dụng phải lập biên bản bàn giao, trong đó thể hiện cụ thể tình trạng, nhãn hiệu (nếu có), mã số máy tính (số serial nếu có), nhãn hiệu, mã số ổ cứng (bắt buộc), nhãn hiệu, mã số thiết bị ngoại vi khác (máy in, máy scan nếu có).

b) Đối với trường hợp nhiều cán bộ, công chức, viên chức, người lao động cùng sử dụng một thiết bị đầu cuối phải giao cho một người trực tiếp quản lý.

c) Cơ quan, đơn vị lập danh sách quản lý thiết bị đầu cuối được trang cấp và thiết bị đầu cuối của cán bộ, công chức, viên chức, người lao động tự trang cấp (tên, chủng loại, nhãn hiệu, địa chỉ MAC, số serial) khi kết nối vào hệ thống thông tin và cập nhật khi có thay đổi (theo Phụ lục kèm theo Quy chế này).

2. Quy định việc sử dụng, cài đặt, bảo vệ trang thiết bị công nghệ thông tin

a) Trang thiết bị đầu cuối có lưu trữ dữ liệu nhạy cảm (dữ liệu cá nhân, dữ liệu nội bộ) khi thay đổi mục đích sử dụng hoặc thanh lý, cơ quan, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, cơ quan, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị đó.

b) Thiết bị đầu cuối có bộ phận lưu trữ hoặc thiết bị lưu trữ khi chuyển giao cho cá nhân, tổ chức khác để bảo hành, bảo dưỡng, sửa chữa 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).

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

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

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 khác.

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, lập biên bản về việc xóa dữ liệu và thực hiện điểm b khoản 2 của Điều này.

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

a) Các cơ quan, đơn vị phải bố trí ít nhất một máy tính độc lập, máy in không kết nối và không có lịch sử kết nối mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu trữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, lưu trữ các văn bản có nội dụng bí mật nhà nước.

b) 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;

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

d) 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. Kết quả sửa chữa, bảo hành phải được ghi nhận bằng biên bản.

e) 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 được cài đặt hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật và phần mềm phòng, chống mã độc, phải thường xuyên cập nhật bản vá cho hệ điều hành và các ứng dụng trên máy tính.

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, mạng máy tính của hệ thống thông tin 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.

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

Điều 6. Bảo đảm an ninh mạng, an toàn thông tin đối với cá nhân, tổ chức sử dụng, khai thác, vận hành hệ thống thông tin

1. Đối với cơ quan, đơn vị chủ quản, vận hành hệ thống thông tin

a) Xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng, an toàn thông tin đối với từng vị trí việc làm cụ thể. Sau khi tuyển dụng, tiếp nhận nhân sự mới, cơ quan, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an ninh mạng, an toàn thông tin; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, cơ quan, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm nếu để xảy ra sự cố nghiêm trọng do buông lỏng quản lý hoặc không thực hiện đầy đủ các biện pháp bảo đảm an toàn thông tin theo quy định.

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

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

d) Định kỳ hằng năm tổ chức đào tạo hoặc cử đi đào tạo về an ninh mạng, an toàn thông tin cho cán bộ kỹ thuật, cán bộ quản lý, người sử dụng trong hệ thống do cơ quan, đơn vị có thẩm quyền tổ chức.

e) Khi công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc, phải thực hiện:

- Lập biên bản thu hồi tài khoản truy cập, các trang thiết bị công nghệ thông tin và các tài sản khác đã trang cấp cho công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc; có cam kết bảo mật thông tin nội bộ, thông tin về hệ thống thông tin của cơ quan, đơn vị.

- Vô hiệu hóa các thông tin của công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công 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 nghỉ việc hoặc thay đổi công việc vào tài nguyên, hệ thống phần mềm của đơn vị quản lý;

2. Đối với cá nhân sử dụng, khai thác hệ thống thông tin

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

b) Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về an ninh mạng, an toàn thông tin.

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

d) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

đ) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác; đổi mật khẩu ngay sau khi được cấp tài khoản đăng nhập các dịch vụ, ứng dụng của Ủy ban nhân dân; đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: chữ in thường, chữ in hoa, chữ số và ký tự đặc biệt) và thay đổi mật khẩu tối thiểu 06 tháng/1 lần; các tài khoản đăng nhập hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt web trên máy tính.

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

g) 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.

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

3. Đối với cán bộ quản lý, vận hành hệ thống

a) 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;

b) Phân công 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;

c) 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;

d) 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.

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

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

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

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

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

c) Các cơ quan, đơn vị, địa phương hoàn thành việc xác định và phê duyệt cấp độ an toàn hệ thống thông tin trước ngày 30/6/2026.

Điều 8. Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin

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

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 trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 9. Bảo đảm an ninh mạng, an toàn thông tin đối với 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 mạng, an toàn thông tin 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 10. Bảo đảm 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 mạng, an toàn thông tin 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 11. Giám sát an ninh mạng, an toàn thông tin

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 số 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 an ninh mạng, an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý tin và kết nối, chia sẻ kết quả giám sát về cơ quan điều phối ứng cứu sự cố quốc gia theo quy định.

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

Điều 12. Quản lý rủi ro, lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin

1. Trách nhiệm đơn vị vận hành hệ thống thông tin

a) Quản lý thông tin điểm yếu an ninh mạng, an toàn thông tin 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 mạng, an toàn thông tin từ các cơ quan, tổ chức có chức năng cảnh báo về an ninh mạng, an toàn thông tin ; 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 mạng, an toàn thông tin đối với các điểm yếu khi cần thiết.

d) Tổ Ứng cứu sự cố an toàn thông tin/cán bộ, công chức được giao nhiệm vụ ứng cứu sự cố an toàn thông tin mạng phải báo cáo lãnh đạo, cán bộ quản lý ngay khi phát hiện hoặc được thông báo điểm yếu an ninh mạng, an toàn thông tin ở mức độ nghiêm trọng; thực hiện cảnh báo và xử lý điểm yếu an ninh mạng, an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an ninh mạng, an toàn thông tin 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 mạng, an toàn thông tin. Sử dụng và cập nhật liên tục các công cụ dò quét lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin 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 mạng, an toàn thông tin 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 mạng, an toàn thông tin 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 mạng, an toàn thông tin 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 mạng, an toàn thông tin 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 mạng, an toàn thông tin cho toàn bộ hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an ninh mạng, an toàn thông tin 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.

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

Điều 13. Thiết kế an toàn hệ thống thông tin đối với các hệ thống thông tin khi xây dựng mới hoặc nâng cấp nhằm đảm bảo an toàn thông tin theo cấp độ an toàn thông tin cần đảm bảo các yêu cầu

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

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

7. Có bộ phận chuyên môn, hoặc thuê đơn vị có đủ năng lực để đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện.

Điều 14. Quản lý thuê dịch vụ công nghệ thông tin, phát triển phần mềm thuê khoán

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, các đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và rõ trách nhiệm của bên cung cấp dịch.

2. Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

3. Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm.

4. Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

5. Trách nhiệm của các đơn vị trong quá trình sử dụng dịch vụ công nghệ thông tin.

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý;

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

c) 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 đơn vị.

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

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

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

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

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

7. 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 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 15. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng; giao bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống; thực hiện các nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống đảm bảo theo quy định của pháp luật (Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước).

2. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Điều 16. Ứng cứu sự cố an toàn hệ thống thông tin

1. Trách nhiệm của các cơ quan, đơn vị trong hoạt động ứng cứu sự cố an ninh mạng, an toàn thông tin

a) Công an tỉnh (Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao) đảm nhiệm vai trò đơn vị chuyên trách ứng cứu sự cố an ninh mạng, an toàn thông tin của Ủy ban nhân dân tỉnh (gọi tắt là đơn vị chuyên trách), chịu trách nhiệm triển khai công tác ứng cứu sự cố các hệ thống thông tin do Ủy ban nhân dân 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 cơ quan, đơn vị có trách nhiệm xây dựng kế hoạch, phương án ứng cứu sự cố hằng năm cho các hệ thống thông tin do cơ quan, đơn vị trực tiếp quản lý, vận hành; phối hợp Đội ứng cứu sự cố trong công tác ứng cứu sự cố an toàn thông tin mạng.

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 mạng, an toàn thông tin .

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

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

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) Mức 1: Phạm vi ảnh hưởng cục bộ, hệ thống vẫn có thể cung cấp dịch vụ, không có dữ liệu nhạy cảm bị truy cập

Đơn vị chủ quản, vận hành hệ thống thông tin có thể xử lý nội bộ, thực hiện khắc phục theo quy trình sẵn có, thu thập dữ liệu theo yêu cầu của Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh, và gửi báo cáo tổng kết kèm dữ liệu theo yêu cầu cho Công an tỉnh sau khi hoàn tất.

b) Mức 2: Ảnh hưởng trung bình, có gián đoạn cục bộ, nguy cơ rò rỉ dữ liệu người dùng hoặc chưa xác định rõ toàn bộ vùng bị tác động

Đơn vị chủ quản, vận hành hệ thống thông tin phải phối hợp chặt chẽ với đơn vị chuyên trách để đánh giá hiện trạng và xác lập phạm vi ảnh hưởng. Trong trường hợp cần thiết, đơn vị chuyên trách có thể xem xét huy động sự hỗ trợ kỹ thuật từ doanh nghiệp an toàn thông tin nhằm hỗ trợ khoanh vùng, loại bỏ nguyên nhân và phục hồi hệ thống trong thời gian sớm nhất.

c) Mức 3: Sự cố nghiêm trọng, có dấu hiệu phá hoại, lộ lọt tài liệu nội bộ, nhạy cảm, tấn công có chủ đích hoặc phạm vi ảnh hưởng vượt quá khả năng kiểm soát của đơn vị chủ quản, vận hành hệ thống thông tin.

Đơn vị chuyên trách về an ninh mạng giữ vai trò điều phối chính trong toàn bộ quá trình ứng phó, điều tra và khắc phục sự cố. Tùy theo tình hình cụ thể, đơn vị chuyên trách có thể triển khai các biện pháp kỹ thuật trực tiếp, đồng thời huy động lực lượng từ các doanh nghiệp cung cấp dịch vụ an toàn thông tin phù hợp để hỗ trợ khôi phục hệ thống trong thời gian ngắn nhất, đảm bảo duy trì hoạt động tối thiểu và giảm thiểu thiệt hại.

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 thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì 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 2.

c) Bước 2: Báo sự cố đến Công an tỉnh theo Mẫu số 03 của Thông tư số 20/2017/TT-BTTTT.

d) Bước 3: Phối hợp với Đội Ứng cứu sự cố an toàn thông tin mạng và các cơ quan, đơn vị, tổ chức, cá nhân có liên quan để tiến hành khắc phục sự cố.

đ) Bước 4: 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 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.

Điều 18. Kiểm tra, đánh giá an ninh mạng, an toàn thông tin

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do cơ quan, đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

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

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

Điều 19. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng, an toàn thông tin

1. Các cơ quan, đơn vị xác định nhu cầu về đào tạo cho nguồn nhân lực để bảo đảm an ninh mạng, an toàn thông tin tại đơn vị mình gửi Công an tỉnh để tổng hợp, tham mưu trình cấp có thẩm quyền triển khai thực hiện.

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

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

Chương III
TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Điều 20. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp Sở Khoa học và Công nghệ và các cơ quan, đơn vị, tổ chức, doanh nghiệp có liên quan xây dựng kế hoạch phòng ngừa, đấu tranh, ngăn chặn tội phạm lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia, gây mất an ninh trật tự và an ninh mạng, an toàn thông tin trong cơ quan nhà nước trên địa bàn tỉnh. Tham mưu giúp Ủy ban nhân dân tỉnh về công tác bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc tham mưu bảo đảm an ninh mạng, an toàn thông tin cho các hệ thống thông tin của tỉnh.

2. Chỉ đạo, tổ chức bảo đảm an ninh mạng, an toàn thông tin cho hạ tầng kỹ thuật của Trung tâm dữ liệu tỉnh.

3. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao; chịu trách nhiệm quản lý, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống mạng gây hại đến an ninh mạng, an toàn thông tin của các cơ quan, đơn vị, tổ chức, doanh nghiệp.

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

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

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

7. Định kỳ tổ chức diễn tập ứng cứu sự cố an ninh mạng, an toàn thông tin trên địa bàn tỉnh, tham gia diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

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

9. Chủ trì và phối hợp các cơ quan, đơn vị liên quan thực hiện công tác kiểm tra việc thực hiện Quy chế này tại các cơ quan, đơn vị và tổng hợp, báo cáo Ủy ban nhân dân tỉnh theo quy định.

10. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan điều tra và xử lý các trường hợp vi phạm an ninh mạng, an toàn thông tin theo thẩm quyền và theo quy định của pháp luật.

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

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

Điều 21. 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 mạng, an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh.

4. Thông báo cho cán bộ đầu mối về công nghệ thông tin/ an ninh mạng, an toàn thông tin 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 mạng, an toàn thông tin chung cho các cơ quan, đơn vị triển khai thực hiện.

Điều 22. Trách nhiệm của đơn vị vận hành hệ thống thông tin

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

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

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

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng, an toàn thông tin, báo cáo Ủy ban nhân dân tỉnh điều chính nếu cần thiết.

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

đ) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Bộ Công an trong công tác bảo đảm an ninh mạng, an toàn thông tin.

e) Kịp thời thống báo sự cố an ninh mạng, an toàn thông tin và phối hợp ứng cứu sự cố an ninh mạng, an toàn thong tin với các cơ quan, đơn vị liên quan.

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

3. Trường hợp hệ thống thông tin do các cơ quan, đơn vị thực hiện thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê), đơn vị vận hành được xác định như sau:

a) Trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin (đồng thời là đơn vị chủ trì, trực tiếp ký hợp đồng thuê dịch vụ công nghệ thông tin): Theo quy định tại khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP, đơn vị vận hành là đơn vị cung cấp dịch vụ.

b) Trường hợp chủ quản hệ thống thông tin giao một đơn vị trực thuộc chủ trì thuê dịch vụ công nghệ thông tin: Đơn vị chủ trì thuê dịch vụ tiếp tục là đơn vị vận hành nếu chủ quản hệ thống thông tin không giao đơn vị cung cấp dịch vụ hoặc đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin.

Đơn vị cung cấp dịch vụ có trách nhiệm phối hợp với chủ quản hệ thống thông tin/đơn vị chủ trì thuê dịch vụ cập nhật thông tin trong hồ sơ đề xuất cấp độ theo đúng hiện trạng hạ tầng đã cài đặt để tổ chức thẩm định, phê duyệt (nếu chưa phê duyệt) hoặc gửi đơn vị chuyên trách về an toàn thông tin để cập nhật.

Điều 23. Trách nhiệm của các cơ quan, đơn vị

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

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

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

4. Ban hành nội quy bảo đảm an ninh mạng, an toàn thông tin trong cơ quan, đơn vị phù hợp với Quy chế này và các quy định của pháp luật.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra, khắc phục sự cố an ninh mạng, an toàn thông tin kịp thời, nhanh chóng và hiệu quả.

6. Phối hợp chặt chẽ với Công an tỉnh và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh mạng, an toàn thông tin.

7. Định kỳ 06 tháng **(trước ngày 10/6)** và hằng năm **(trước ngày 20/12)** báo cáo tình hình an ninh mạng, an toàn thông tin của cơ quan, đơn vị gửi Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh.

Điều 24. Trách nhiệm của đơn vị vận hành Trung tâm dữ liệu tỉnh

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

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

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

Điều 25. Trách nhiệm của cán bộ, công chức, viên chức, người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức, người lao động

a) Chấp hành Quy chế này, nội quy của cơ quan, đơn vị và các quy định của pháp luật về an ninh mạng, an toàn thông tin. Chịu trách nhiệm bảo đảm an ninh mạng, an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

b) Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm an ninh mạng, an toàn thông tin cho tài khoản, các thiết bị mà mình được giao sử dụng.

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

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

2. Trách nhiệm của cán bộ chuyên trách hoặc kiêm nhiệm công nghệ thông tin/an toàn thông tin

a) Chấp hành các quy định tại khoản 1 Điều này.

b) Chủ trì tham mưu lãnh đạo cơ quan, đơn vị thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến an ninh mạng, an toàn thông tin.

c) Tham mưu lãnh đạo cơ quan, đơn vị ban hành nội quy bảo đảm an ninh mạng, an toàn thông tin và triển khai các giải pháp kỹ thuật bảo đảm an ninh mạng, an toàn thông tin tại cơ quan, đơn vị.

d) Tham mưu các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong quá trình thực hiện nhiệm vụ, công tác.

đ) Phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an ninh mạng, an toàn thông tin.

Điều 26. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin và Internet

1. Doanh nghiệp có trách nhiệm phối hợp và bảo đảm chất lượng dịch vụ theo hợp đồng và quy định pháp luật hiện hành của Bộ Công an, Bộ Khoa học và Công nghệ về an ninh mạng, an toàn thông tin 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 mạng, an toàn thông tin 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 27. 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 mạng, an toàn thông tin.

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 công nghệ thông tin trên địa bàn tỉnh chịu sự thanh tra, kiểm tra của các cơ quan nhà nước có thẩm quyền về lĩnh vực an ninh mạng, an toàn thông tin.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 28. Kinh phí thực hiện

1. Kinh phí bảo đảm an ninh mạng, an toàn thông tin được bố trí từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Căn cứ chương trình công tác hằng năm, Công an tỉnh có trách nhiệm phối hợp với các cơ quan, đơn vị liên quan xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an ninh mạng, an toàn thông tin cho Ủy ban nhân dân tỉnh; kịp thời tham mưu Ủy ban nhân dân tỉnh bổ sung kinh phí ngoài dự toán khi phát sinh sự cố khẩn cấp, bảo đảm hệ thống nhanh chóng được khắc phục.

3. 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 mạng, an toàn thông tin trên địa bàn tỉnh.

4. Các cơ quan, đơn vị hằng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an ninh mạng, an toàn thông tin 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 mạng, an toàn thông tin và đưa vào dự toán chi năm sau để triển khai thực hiện.

Điều 29. Trách nhiệm thi hành

1. Thủ trưởng sở, ban, ngành, đơn vị sự nghiệp thuộc Ủy ban nhân dân tỉnh, Chủ tịch Ủy ban nhân dân các xã, phường có trách nhiệm triển khai thực hiện, phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức, người lao động trong đơn vị Quy chế này; thường xuyên kiểm tra việc thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin tại đơn vị; chịu trách nhiệm trước pháp luật và trước Ủy ban nhân dân tỉnh về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị.

2. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, các đơn vị gửi về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định./.

PHỤ LỤC I

DANH SÁCH THIẾT BỊ ĐẦU CUỐI TẠI CƠ QUAN/ĐƠN VỊ

STT	**Họ tên người sử dụng**	**Chủng loại thiết bị/ổ cứng** *(Chủng loại: PC, Laptop, Server, Switch, Router, Firewall, máy in, máy scan, Camera,…* *Lưu ý: lấy thông tin ổ cứng đối với các thiết bị có chức năng lưu trữ dữ diệu như máy tính, USB, ổ cứng di động,...)*	**Mã số thiết bị/ổ cứng (serial)**	**Địa chỉ MAC** *(nếu có)*	**Ghi chú**
1					
2					
3					
…					