ỦY BAN NHÂN DÂN TỈNH ĐỒNG THÁP	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 2933 /QĐ-UBND	*Đồng Tháp, ngày 17 tháng 09 năm 2026*

QUYẾT ĐỊNH
Ban hành quy chế bảo đảm an ninh mạng Trung tâm Tích hợp dữ liệu tỉnh Đồng Tháp

ỦY BAN NHÂN DÂN TỈNH ĐỒNG THÁP

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

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Chuyển đổi số ngày 11 tháng 12 năm 2025;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Theo đề nghị của Giám đốc Sở Khoa học và Công nghệ.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng Trung tâm Tích hợp dữ liệu tỉnh Đồng Tháp.

Điều 2. Sở Khoa học và Công nghệ, Trung tâm Khởi nghiệp đổi mới sáng tạo và Chuyển đổi số và Công an tỉnh chịu trách nhiệm tổ chức thực hiện các nội dung tại Quy chế này; giám sát, kiểm tra, hỗ trợ các cơ quan, đơn vị và địa phương thực hiện quy trình bảo đảm an ninh mạng Trung tâm Tích hợp dữ liệu tỉnh Đồng Tháp.

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 4. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Khoa học và Công nghệ; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân các xã, phường và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 4;
- Thường trực Tỉnh uỷ;
- Thường trực HĐND tỉnh;
- CT và các PCT UBND tỉnh;
- Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội tỉnh;
- VPUB: CVP, các PCVP, Trung tâm Tin học và Công báo;
- Lưu: VT, KGVX(vttoan).

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

Huỳnh Minh Tuấn

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

QUY CHẾ
Bảo đảm an ninh mạng Trung tâm Tích hợp dữ liệu tỉnh Đồng Tháp

(kèm theo Quyết định số 2933 /QĐ-UBND ngày 17 tháng 09 năm 2026 của Ủy ban nhân dân tỉnh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định việc bảo đảm an ninh mạng trong quá trình quản lý, vận hành, khai thác và sử dụng các hệ thống thông tin đặt tại Trung tâm Tích hợp dữ liệu tỉnh Đồng Tháp (*sau đây gọi tắt là TTTHDL*).

2. Đối tượng áp dụng

Quy chế này áp dụng đối với cơ quan hành chính nhà nước, đơn vị sự nghiệp công lập trên địa bàn tỉnh Đồng Tháp; các tổ chức chính trị - xã hội, tổ chức, cá nhân có liên quan tham gia quản lý, vận hành, khai thác tài nguyên hạ tầng của TTTHDL.

3. Các hệ thống thông tin áp dụng

Quy chế này áp dụng cho tất cả các phần mềm dùng chung, các hệ thống thông tin chuyên ngành được Ủy ban nhân dân tỉnh thống nhất cho phép cài đặt, triển khai, vận hành tại TTTHDL.

Điều 2. Giải thích từ ngữ

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

1. Hệ thống thông tin: là tập hợp phần cứng, phần mềm và 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.

2. Phần mềm ứng dụng dùng chung: là các hệ thống nền tảng, phần mềm ứng dụng, cơ sở dữ liệu dùng chung, đồng bộ cho các cơ quan, đơn vị và người sử dụng được Ủy ban nhân dân tỉnh thống nhất triển khai, đưa vào hoạt động tại TTTHDL.

3. Phần mềm ứng dụng chuyên ngành: là hệ thống thông tin, cơ sở dữ liệu chuyên ngành của các cơ quan, đơn vị trên địa bàn tỉnh được Ủy ban nhân dân tỉnh cho phép triển khai, cài đặt, vận hành tại TTTHDL.

4. Mạng truyền số liệu chuyên dùng (gọi tắt là mạng TSLCD): là hệ thống thông tin quan trọng quốc gia, được sử dụng trong hoạt động truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

5. Hạ tầng kỹ thuật: là tập hợp thiết bị công nghệ thông tin (thiết bị định tuyến, thiết bị chuyển mạch, thiết bị lưu trữ dữ liệu, các thiết bị giám sát, bảo mật, máy chủ, máy trạm), thiết bị điện (điều hòa chính xác, tủ điện, chống sét, máng cáp điện), thiết bị phòng cháy, chữa cháy, thiết bị viễn thông, thiết bị ngoại vi, mạng nội bộ, mạng WAN, mạng TSLCD và các thiết bị kỹ thuật chuyên dùng khác.

6. Tính bí mật của thông tin: là thông tin chỉ được truy cập bởi những người được cấp quyền truy cập tương ứng.

7. Tính toàn vẹn của thông tin: là tính chính xác, đầy đủ của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền.

8. Tính sẵn sàng của thông tin: là việc thông tin được cung cấp đầy đủ và kịp thời cho người có quyền sử dụng khi có yêu cầu.

9. An ninh mạng: là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

10. An ninh thông tin mạng: là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin trên không gian mạng, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

11. An ninh dữ liệu: là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

12. Cơ quan chủ quản TTTHDL: Ủy ban nhân dân tỉnh Đồng Tháp.

13. Cơ quan được giao trách nhiệm quản lý TTTHDL (*gọi tắt là Đơn vị quản lý*): Sở Khoa học và Công nghệ.

14. Bộ phận trực tiếp vận hành TTTHDL (*gọi tắt là Bộ phận vận hành*): Trung tâm Khởi nghiệp đổi mới sáng tạo và Chuyển đổi số.

15. Đơn vị chuyên trách, bảo đảm an ninh mạng cho TTTHDL (*gọi tắt là Đơn vị chuyên trách ANM*): Công an tỉnh.

16. Đơn vị khai thác: là các cơ quan, đơn vị, địa phương và tổ chức, cá nhân được Ủy ban nhân dân tỉnh cho phép triển khai, cài đặt và vận hành phần mềm, ứng dụng trên hạ tầng TTTHDL (*gọi tắt là Đơn vị khai thác*).

Điều 3. Chức năng của TTTHDL

TTTHDL có chức năng lưu trữ dữ liệu lớn, bảo mật an toàn dữ liệu, hệ thống phụ trợ, mạng WAN, mạng TSLCD, các hệ thống thông tin, phần mềm ứng dụng dùng chung, phần mềm ứng dụng chuyên ngành và hệ thống thông tin khác trên địa bàn tỉnh.

Điều 4. Hạ tầng kỹ thuật của TTTHDL

Hạ tầng kỹ thuật của TTTHDL được chia thành các thành phần sau:

1. Đường truyền: TTTHDL sử dụng mạng TSLCD để kết nối hệ thống mạng diện rộng của tỉnh, được lựa chọn chính để truyền dẫn, trao đổi dữ liệu, các giao dịch hành chính, khai thác sử dụng các hệ thống thông tin dùng chung trên môi trường mạng của các cơ quan nhà nước và sử dụng đường truyền dự phòng *(qua Internet)* khi đường truyền chính bị sự cố.

2. Hệ thống mạng và bảo mật: hệ thống mạng được chia thành nhiều vùng khác nhau, mỗi vùng được thiết lập các chính sách an toàn và truy cập riêng phục vụ cho các mục đích khác nhau. Hệ thống bảo mật bao gồm các thiết bị tường lửa cho lớp mạng ngoài, lớp mạng trong và các thiết bị chuyên dụng khác, được thiết kế bảo đảm an toàn cho các kết nối từ TTTHDL kết nối vào và đến hệ thống khác. Các máy chủ được cài đặt phần mềm phòng chống mã độc *(antivirus)* có bản quyền, các thiết bị khi kết nối với hệ thống máy chủ tại TTTHDL được rà soát và kiểm tra bảo đảm an toàn trước khi kết nối với hệ thống.

Hệ thống mạng được thiết kế và vận hành theo nguyên tắc phân vùng mạng, đặc quyền tối thiểu và bảo đảm tính sẵn sàng; kiểm soát chặt chẽ kết nối giữa các vùng mạng. Tùy theo yêu cầu thực tế, hệ thống mạng được tổ chức tối thiểu gồm vùng mạng nội bộ, vùng mạng biên, vùng mạng máy chủ nội bộ, vùng mạng trung gian (DMZ) cung cấp dịch vụ, vùng mạng máy chủ cơ sở dữ liệu và vùng quản trị; trường hợp có mạng không dây thì bố trí vùng mạng riêng cho mạng không dây.

Đối với các thiết bị mạng trọng yếu, Bộ phận vận hành phải có phương án dự phòng, dự phòng nóng hoặc cân bằng tải phù hợp với yêu cầu hoạt động của hệ thống; có phương án dự phòng kết nối mạng cho các máy chủ cung cấp dịch vụ.

Các giải pháp bảo vệ mạng phải được cập nhật cơ sở dữ liệu, dấu hiệu nhận diện tấn công và bản cập nhật cần thiết theo quy định của nhà cung cấp; thường

xuyên kiểm tra tình trạng hoạt động, hiệu năng của thiết bị và hệ thống mạng.

3. Hệ thống giám sát an ninh mạng: được thiết kế nhằm thu thập và phân tích nhật ký, các sự kiện từ các máy chủ, thiết bị mạng và được lưu trữ tập trung, cho phép phân tích và báo cáo về các sự kiện an ninh mạng, giúp phát hiện sớm các cuộc tấn công mạng, lây nhiễm mã độc.

4. Hệ thống máy chủ: bao gồm các hệ thống máy chủ đã được đầu tư phục vụ cho Chính quyền điện tử với khả năng sẵn sàng cho việc mở rộng trong tương lai. Hệ thống máy chủ có khả năng cung cấp năng lực tính toán cho nhiều nền tảng với nhiều mục đích khác nhau như: Ứng dụng dùng chung, ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác.

5. Hệ thống lưu trữ: bao gồm thiết bị lưu trữ tập trung có năng lực xử lý lưu trữ ở mức cao, khả năng lưu trữ lớn và thiết bị sao lưu, phục hồi dữ liệu. Hệ thống được thiết kế bảo đảm khả năng mở rộng dung lượng lưu trữ trong tương lai.

6. Hệ thống phụ trợ: bao gồm hệ thống điện, điều hòa nhiệt độ, thiết bị lưu điện, máy phát điện, sàn nâng, hệ thống phòng cháy, chữa cháy, camera an ninh,... được thiết kế tương tự theo tiêu chuẩn TIA 942 - TIER 3 (*tiêu chuẩn quốc tế về TTTHDL*), bảo đảm các thiết bị luôn được hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

Điều 5. Cơ sở dữ liệu và phần mềm ứng dụng của TTTHDL

1. Hệ thống cơ sở dữ liệu: bao gồm các hệ cơ sở dữ liệu dùng chung hoặc chuyên ngành được xây dựng nhằm liên kết, tích hợp các ứng dụng dùng chung và chuyên ngành phục vụ ứng dụng công nghệ thông tin trong các cơ quan, đơn vị và phục vụ người dân, doanh nghiệp.

2. Các phần mềm ứng dụng dùng chung phục vụ cho việc triển khai ứng dụng công nghệ thông tin cho các cơ quan nhà nước, tổ chức chính trị - xã hội, bao gồm: Nền tảng kết nối, chia sẻ dữ liệu tỉnh (*LGSP*); Hệ thống Thư điện tử công vụ; Hệ thống Quản lý văn bản và điều hành; Hệ thống thông tin Giải quyết thủ tục hành chính của tỉnh và các phần mềm, ứng dụng, cơ sở dữ liệu chuyên ngành của các cơ quan nhà nước trong tỉnh.

3. Căn cứ vào nhu cầu thực tế, các đơn vị đăng ký bổ sung thêm các phần mềm, ứng dụng khác đưa vào cài đặt, triển khai, vận hành tại TTTHDL.

Điều 6. Nguyên tắc quản lý, vận hành và khai thác TTTHDL

1. Bảo đảm các yêu cầu về an ninh mạng theo Luật An ninh mạng và các văn bản pháp lý hiện hành.

2. Duy trì, vận hành, nâng cấp TTTHDL (*cơ sở hạ tầng, hệ thống thông tin, cơ sở dữ liệu chuyên ngành*) phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật do Nhà nước quy định và phù hợp với Kiến trúc Chính quyền điện tử tỉnh. Đồng thời, tuân thủ các quy định hiện hành về bảo đảm an ninh mạng.

3. Quản lý, kết nối và chia sẻ dữ liệu số không chứa thông tin bí mật nhà nước của TTTHDL phải tuân thủ theo Nghị định số 278/2025/NĐ-CP ngày 22/10/2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị.

4. Việc chia sẻ dữ liệu số chứa thông tin thuộc phạm vi bí mật nhà nước được thực hiện theo Luật Bảo vệ bí mật nhà nước và các văn bản pháp luật hiện hành. Các tài liệu, văn bản có nội dung mật được quản lý theo quy định riêng của từng ngành, lĩnh vực và các văn bản quy phạm pháp luật hiện hành.

5. Các tổ chức, cá nhân sử dụng các hệ thống thông tin của TTTHDL phải tuân thủ các quy định chung về bảo đảm an ninh mạng, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình.

6. Đơn vị quản lý TTTHDL chịu trách nhiệm quản lý tài sản hoặc phân cấp quản lý tài sản theo quy định hiện hành về quản lý, sử dụng tài sản công.

7. Bộ phận vận hành TTTHDL chịu trách nhiệm quản lý tài sản theo phân cấp, quản trị, vận hành bảo đảm khai thác an toàn hiệu quả hạ tầng kỹ thuật TTTHDL hiện có.

8. Ngân sách nhà nước hằng năm bảo đảm cho công tác duy trì, quản lý, vận hành và bảo trì, bảo dưỡng, thay thế các thiết bị hỏng hóc, bổ sung bản quyền (*license*) các thiết bị, phần mềm tại TTTHDL đầy đủ, kịp thời để phục vụ nhiệm vụ chung.

Chương II
BẢO ĐẢM AN NINH MẠNG TTTHDL

Điều 7. Đào tạo và chứng nhận năng lực an ninh mạng

1. Viên chức, nhân viên quản trị, vận hành hệ thống công nghệ thông tin tại TTTHDL phải được đào tạo và huấn luyện định kỳ ít nhất một (01) lần mỗi năm về an ninh mạng, kỹ năng ứng phó sự cố và các quy định pháp lý có liên quan.

2. Các quản trị viên hệ thống, nhân sự kỹ thuật chủ chốt phải đạt chứng chỉ chuyên môn cơ bản về an ninh mạng. Bộ phận vận hành có trách nhiệm tổ chức kiểm tra định kỳ năng lực vận hành và bảo đảm an ninh mạng của đội ngũ cán bộ kỹ thuật.

3. Bộ phận vận hành phối hợp với Đơn vị quản lý, Đơn vị chuyên trách ANM cùng các cơ quan liên quan xây dựng và triển khai chương trình nâng cao nhận thức an ninh mạng cho toàn thể cán bộ, công chức, viên chức thuộc các cơ quan, đơn vị sử dụng hệ thống.

4. Bộ phận vận hành có trách nhiệm thành lập hoặc bố trí riêng biệt các bộ phận, nhóm nhân sự thực hiện chức năng vận hành hệ thống, quản trị hệ thống và bảo vệ an ninh mạng. Chức năng, nhiệm vụ, quyền hạn, phạm vi tài khoản và trách nhiệm của từng bộ phận phải được quy định bằng văn bản; bảo đảm cơ chế hoạt động độc lập về chuyên môn và không để một cá nhân đồng thời tự thực hiện, tự kiểm tra hoặc phê duyệt cùng một công việc.

5. Nhân sự phụ trách vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn phù hợp về công nghệ thông tin, an toàn thông tin hoặc an ninh mạng; phải ký cam kết bảo mật thông tin trong quá trình làm việc và tiếp tục chịu trách nhiệm bảo mật sau khi nghỉ việc hoặc chuyển công tác.

6. Khi cán bộ, nhân viên nghỉ việc hoặc thay đổi vị trí công tác, Bộ phận vận hành phải thu hồi thẻ ra vào, chìa khóa, thiết bị xác thực, tài liệu, dữ liệu lưu trên các phương tiện lưu trữ, máy tính, thiết bị phần cứng, phần mềm, bản quyền và các tài sản khác đã được giao; đồng thời thực hiện bàn giao công việc, dữ liệu và lập biên bản xác nhận.

7. Phải xây dựng và thực hiện quy trình vô hiệu hóa, thu hồi toàn bộ quyền ra vào, quyền truy cập hệ thống, tài nguyên, dữ liệu, thư điện tử, VPN, tài khoản quản trị và các quyền truy cập từ xa của cán bộ nghỉ việc hoặc chuyển công tác. Việc thu hồi phải hoàn thành chậm nhất tại thời điểm quyết định nghỉ việc hoặc thay đổi công việc có hiệu lực; các mật khẩu dùng chung, khóa bảo mật và thông tin xác thực có liên quan phải được thay đổi kịp thời.

Điều 8. Phân loại và xác định cấp độ an ninh mạng cho Hệ thống thông tin

1. Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ, hệ thống thông tin được phân loại theo năm (05) cấp độ, từ cấp độ 1 đến cấp độ 5. Hệ thống cơ sở hạ tầng thông tin tại TTTHDL được xác định cấp độ là cấp độ 3, do có xử lý, lưu trữ và chia sẻ dữ liệu của các cơ quan nhà nước trên phạm vi toàn tỉnh; đồng thời có một số hệ thống thông tin dùng chung đang kết nối, chia sẻ dữ liệu chứa thông tin cá nhân hoặc dữ liệu phục vụ công tác chỉ đạo, điều hành với các hệ thống, cơ sở dữ liệu chuyên ngành ở Trung ương.

2. Đối với các hệ thống thông tin còn lại, việc xác định cấp độ an toàn phải được thực hiện độc lập, căn cứ trực tiếp trên tính chất của loại hình thông tin xử lý và đặc điểm vận hành của hệ thống; trong đó, yêu cầu bảo đảm an ninh mạng tối thiểu phải đạt từ cấp độ 2 trở lên. Tùy thuộc vào phạm vi tác động, chức năng

nghiệp vụ và mức độ quan trọng đối với hoạt động của đơn vị, từng phần mềm, dịch vụ cụ thể sẽ được rà soát, đánh giá để áp dụng các tiêu chuẩn kỹ thuật và quy trình quản lý tương ứng, bảo đảm tính đồng bộ và an toàn tối đa cho toàn bộ hạ tầng kỹ thuật.

Điều 9. Quản lý an ninh mạng đối với bên thứ ba

1. Bộ phận vận hành phải xây dựng, ban hành và duy trì quy trình đánh giá, lựa chọn, theo dõi và quản lý nhà cung cấp sản phẩm, dịch vụ an ninh mạng; nhà cung cấp dịch vụ lưu trữ, xử lý dữ liệu nhạy cảm; nhà cung cấp chịu trách nhiệm đối với quy trình, ứng dụng, nền tảng hoặc thành phần quan trọng của hệ thống; nhà cung cấp được phép truy cập vật lý hoặc truy cập từ xa vào TTTHDL.

2. Bộ phận vận hành phối hợp với Đơn vị chuyên trách ANM thiết lập và duy trì bản kiểm kê nhà cung cấp. Bản kiểm kê tối thiểu gồm tên nhà cung cấp; sản phẩm, dịch vụ cung cấp; đầu mối liên hệ; hệ thống, dữ liệu và phạm vi truy cập; thời hạn hợp đồng; trạng thái hoạt động; mức phân loại; ngày đánh giá gần nhất và kết quả đánh giá.

3. Nhà cung cấp trong danh sách quản lý phải được phân loại căn cứ vào mức độ quan trọng của sản phẩm, dịch vụ; loại dữ liệu được lưu trữ hoặc xử lý; phạm vi quyền truy cập; mức độ phụ thuộc của hệ thống và hậu quả khi dịch vụ bị gián đoạn. Phạm vi trách nhiệm của nhà cung cấp và cơ quan, đơn vị sử dụng dịch vụ phải được xác định rõ bằng hợp đồng, thỏa thuận hoặc văn bản có giá trị tương đương.

4. Danh sách và trạng thái nhà cung cấp phải được xem xét, cập nhật tối thiểu 01 lần/năm hoặc ngay khi có thay đổi về nhà cung cấp, hợp đồng, sản phẩm, dịch vụ, phạm vi truy cập, dữ liệu xử lý hoặc các thay đổi khác ảnh hưởng đến danh sách.

5. Trước khi ký kết hợp đồng cung cấp dịch vụ công nghệ thông tin, các đơn vị thuê ngoài phải chứng minh năng lực bảo đảm an ninh mạng, thông qua hồ sơ năng lực hoặc chứng chỉ liên quan. Hợp đồng thuê ngoài phải bao gồm điều khoản bảo mật thông tin và cam kết chịu trách nhiệm nếu để xảy ra rò rỉ dữ liệu hoặc sự cố an ninh mạng. Bộ phận vận hành và Đơn vị chuyên trách ANM có trách nhiệm tổ chức đánh giá tuân thủ an ninh mạng của các nhà cung cấp tối thiểu một (01) lần/năm.

6. Nhà cung cấp chỉ được truy cập hệ thống TTTHDL thông qua kênh kết nối VPN có xác thực đa nhân tố, với thời gian và phạm vi truy cập được cấp phép cụ thể. Trường hợp nhà cung cấp vi phạm quy định về an ninh mạng, Bộ phận vận hành có quyền đình chỉ truy cập và chấm dứt hợp đồng dịch vụ theo quy định hiện hành.

Điều 10. Kiểm tra, đánh giá an ninh mạng định kỳ

1. Bộ phận vận hành, Đơn vị khai thác và Đơn vị chuyên trách ANM phối hợp tổ chức kiểm tra, đánh giá an ninh mạng định kỳ theo quy định, ít nhất một (01) lần/năm đối với TTTHDL và các hệ thống thông tin có cấp độ 3 trở lên triển khai tại TTTHDL. Kết quả kiểm tra, đánh giá là cơ sở để xây dựng, cập nhật và triển khai kế hoạch bảo đảm an ninh mạng cho năm tiếp theo.

2. Bộ phận vận hành chủ trì, phối hợp với Đơn vị khai thác và Đơn vị chuyên trách ANM thiết lập, duy trì chương trình kiểm thử xâm nhập phù hợp với quy mô, mức độ phức tạp, cấp độ và trạng thái vận hành của TTTHDL và các hệ thống thông tin triển khai tại TTTHDL.

3. Trước mỗi đợt kiểm thử xâm nhập, kế hoạch kiểm thử phải được Bộ phận vận hành hoặc cấp có thẩm quyền phê duyệt và tối thiểu phải xác định:

a) Phạm vi tiến hành kiểm thử đối với một phần hoặc toàn bộ hạ tầng công nghệ thông tin; đối tượng, hệ thống, địa chỉ mạng và tài sản được phép kiểm thử.

b) Thời gian, phương pháp, công cụ, nhân sự thực hiện; đầu mối chỉ huy, đầu mối kỹ thuật và cơ chế phối hợp trong suốt quá trình kiểm thử.

c) Phương án bảo đảm an ninh mạng; phương án quản lý, bảo mật, lưu giữ, bàn giao hoặc tiêu hủy dữ liệu, bằng chứng và thông tin thu được từ hoạt động kiểm thử.

d) Đối với hệ thống đang vận hành, thời điểm và cách thức kiểm thử phải bảo đảm không làm gián đoạn dịch vụ; ưu tiên thực hiện trên môi trường phát triển, thử nghiệm hoặc trong khung thời gian bảo trì đã được phê duyệt.

đ) Tần suất kiểm thử theo mức độ rủi ro: hằng quý, nửa tháng, một năm hoặc đột xuất; trong đó TTTHDL và hệ thống thông tin có cấp độ 3 trở lên phải được kiểm thử ít nhất một (01) lần/năm.

e) Các giới hạn và hành vi bị cấm, bao gồm tấn công vật lý, tấn công lừa đảo, tấn công phi kỹ thuật hoặc hành vi khác ngoài phạm vi, trừ trường hợp được phê duyệt riêng bằng văn bản.

g) Cách thức phản ứng của tổ chức trong quá trình kiểm thử, bao gồm việc có hoặc không thực hiện ngăn chặn, điều kiện dừng khẩn cấp và cơ chế kiểm soát, bảo mật thông tin về cuộc kiểm thử trong nội bộ.

4. Khi có thay đổi lớn về kiến trúc, phần mềm hoặc hạ tầng kỹ thuật; sau sự cố nghiêm trọng; khi xuất hiện nguy cơ, lỗ hổng mới có ảnh hưởng lớn; hoặc theo yêu cầu của cơ quan có thẩm quyền, các đơn vị phải tổ chức đánh giá và kiểm thử đột xuất phù hợp.

5. Các tồn tại, điểm yếu và lỗ hổng phát hiện qua kiểm thử xâm nhập phải được đánh giá rủi ro, xác định mức độ ưu tiên, đơn vị chịu trách nhiệm và thời hạn khắc phục. Sau khi khắc phục phải kiểm tra lại để xác nhận hiệu lực của biện pháp xử lý.

6. Sau mỗi đợt kiểm thử xâm nhập, Bộ phận vận hành phối hợp với Đơn vị khai thác và Đơn vị chuyên trách ANM rà soát hiệu quả các biện pháp bảo mật, cập nhật cấu hình, quy trình, kế hoạch bảo đảm an ninh mạng và chương trình kiểm thử khi cần thiết.

7. Kế hoạch, văn bản phê duyệt, nhật ký thực hiện, báo cáo kết quả, hồ sơ khắc phục và kết quả kiểm tra lại phải được quản lý, bảo mật và lưu trữ theo quy định.

Điều 11. Cơ chế phối hợp và báo cáo công tác bảo đảm an ninh mạng

1. Bộ phận vận hành TTTHDL có trách nhiệm phối hợp chặt chẽ với Đơn vị quản lý, Đơn vị chuyên trách ANM và các cơ quan có thẩm quyền trong công tác phòng ngừa, phát hiện, ứng cứu và khắc phục sự cố an ninh mạng.

2. Khi phát hiện dấu hiệu tấn công mạng, lây lan mã độc diện rộng hoặc rò rỉ dữ liệu, Bộ phận vận hành phải báo cáo nhanh trong thời gian không quá hai (02) giờ kể từ thời điểm phát hiện.

3. Đơn vị chuyên trách ANM là cơ quan đầu mối tiếp nhận, điều phối và tổng hợp báo cáo gửi Ủy ban nhân dân tỉnh cùng các cơ quan, đơn vị có liên quan theo quy định.

Điều 12. Ứng phó và khắc phục sự cố an ninh mạng

1. TTTHDL phải xây dựng, duy trì kế hoạch, chương trình và năng lực ứng phó sự cố an ninh mạng, bao gồm chính sách, kế hoạch, quy trình, thủ tục, vai trò, đào tạo và các kênh liên lạc phục vụ ứng phó sự cố.

2. Kế hoạch, quy trình ứng phó sự cố an ninh mạng tối thiểu phải bao gồm:

a) Phân nhóm, phân loại sự cố an ninh mạng.

b) Phương án tiếp nhận, phát hiện, xác minh, phân loại, cảnh báo và xử lý ban đầu sự cố an ninh mạng.

c) Kế hoạch ứng phó, cô lập, ngăn chặn, khắc phục, phục hồi và báo cáo sự cố an ninh mạng.

d) Cơ chế giám sát, phát hiện và cảnh báo sự cố an ninh mạng.

đ) Quy trình ứng cứu sự cố an ninh mạng thông thường.

e) Quy trình ứng cứu sự cố an ninh mạng nghiêm trọng và đặc biệt nghiêm trọng.

g) Cơ chế phối hợp với cơ quan có thẩm quyền, các nhóm chuyên gia và nhà cung cấp dịch vụ hỗ trợ xử lý, khắc phục sự cố an ninh mạng.

h) Tổ chức diễn tập phương án ứng phó sự cố an ninh mạng định kỳ hằng năm.

3. Lực lượng ứng phó sự cố an ninh mạng được tổ chức và duy trì như sau:

a) Đơn vị quản lý, trên cơ sở đề xuất của Bộ phận vận hành và Đơn vị chuyên trách ANM, chỉ định bằng văn bản một người chủ chốt và ít nhất một người dự phòng để quản lý, điều phối quy trình ứng phó sự cố an ninh mạng.

b) Lập và cập nhật danh sách lực lượng tham gia ứng phó sự cố; phân công cụ thể vị trí, vai trò, trách nhiệm của từng thành viên và trách nhiệm phối hợp của các phòng, ban, cơ quan, đơn vị có liên quan.

c) Thiết lập, duy trì đầu mối liên hệ với cơ quan có thẩm quyền quản lý nhà nước về an ninh mạng, cơ quan điều hành Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia, các nhóm chuyên gia và nhà cung cấp dịch vụ hỗ trợ.

d) Thiết lập, duy trì các đầu mối và kênh liên lạc để tiếp nhận, báo cáo sự cố; tối thiểu mỗi năm một (01) lần phải xác minh, cập nhật thông tin liên hệ của các cơ quan, tổ chức hỗ trợ điều phối ứng phó sự cố.

4. Quy trình nội bộ báo cáo sự cố và quy trình ứng phó sự cố phải được đánh giá, cập nhật tối thiểu một (01) lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình.

5. Căn cứ mức độ ảnh hưởng, sự cố được phân loại theo ba (03) mức:

a) Mức 1 - sự cố thông thường: phạm vi ảnh hưởng hạn chế, có thể xử lý nội bộ trong phạm vi hệ thống.

b) Mức 2 - sự cố nghiêm trọng: ảnh hưởng đến một hoặc nhiều hệ thống thông tin của TTTHDL, dữ liệu quan trọng hoặc hoạt động cung cấp dịch vụ.

c) Mức 3 - sự cố đặc biệt nghiêm trọng: gây hoặc có nguy cơ gây ngưng trệ trên diện rộng, ảnh hưởng phạm vi toàn tỉnh hoặc vượt quá khả năng xử lý của TTTHDL, cần phối hợp với Đơn vị chuyên trách ANM, Đơn vị quản lý và cơ quan có thẩm quyền.

6. Bộ phận vận hành TTTHDL là đầu mối tiếp nhận, xử lý ban đầu; có trách nhiệm báo cáo sự cố trong thời gian không quá hai (02) giờ kể từ khi phát hiện tới Đơn vị chuyên trách ANM và các đơn vị có liên quan theo quy định. Toàn bộ hoạt động ứng phó phải được ghi nhận, lưu trữ nhật ký và tổng hợp báo cáo.

Điều 13. Quy định làm việc, chế độ vào, ra TTTHDL

1. Quy định đối với quản trị viên hệ thống

a) Trong quá trình làm việc tại TTTHDL phải tuân thủ nghiêm ngặt theo các quy trình, quy định làm việc, chế độ vào, ra đã được Bộ phận vận hành phê duyệt.

b) Quản trị, vận hành và sử dụng thông tin tại TTTHDL theo trách nhiệm và phân quyền được quy định; chỉ can thiệp vào các phần mềm ứng dụng, dữ liệu do các đơn vị khai thác triển khai tại TTTHDL khi có yêu cầu hỗ trợ từ đơn vị; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

2. Quy định đối với tổ chức, cá nhân đến làm việc tại TTTHDL

a) Yêu cầu:

- Tuân thủ nghiêm theo các quy trình, quy định làm việc, chế độ vào, ra tại TTTHDL.

- Không được mang, sử dụng các thiết bị điện thoại, máy tính xách tay, máy tính bảng hoặc các thiết bị điện tử cá nhân khác (*máy chụp hình, máy quay phim, thiết bị lưu trữ*...) khi vào bên trong TTTHDL, trừ các yêu cầu tác nghiệp đặc biệt của các cơ quan chức năng có thẩm quyền theo luật định.

b) Các tổ chức, cá nhân đến đăng ký làm việc, tham quan phải cung cấp giấy giới thiệu của cơ quan, đơn vị hoặc văn bản đề nghị làm việc tại TTTHDL; danh sách những người tham quan (*có thông tin về số Căn cước/CCCD hoặc Hộ chiếu kèm theo*) và tuân thủ theo các quy định của đơn vị quản lý TTTHDL.

Điều 14. Quy định về an toàn hoạt động

1. TTTHDL phải có nội quy vận hành và được giám sát thường xuyên thông qua việc kiểm soát vào, ra. Không đặt các thiết bị hư hỏng, các vật dụng dễ gây cháy nổ… vào TTTHDL.

2. TTTHDL phải được trang bị hệ thống quản lý môi trường (*nhiệt độ, độ ẩm*), hệ thống điều hòa chính xác bảo đảm độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị, hạ tầng kỹ thuật hoạt động ổn định, được bảo trì, bảo dưỡng ít nhất 02 lần/năm hoặc theo khuyến cáo của nhà sản xuất.

3. TTTHDL phải được trang bị hệ thống lưu điện dự phòng (*UPS*) cung cấp điện cho các thiết bị, hạ tầng kỹ thuật, được bảo trì, bảo dưỡng ít nhất 01 lần/năm và máy phát điện dự phòng để bảo đảm cho hệ thống hoạt động liên tục, ổn định kể cả khi có sự cố về nguồn điện lưới, được bảo trì, bảo dưỡng ít nhất 01 lần/năm, thay thế thiết bị hư hỏng, được bổ sung nhiên liệu thường xuyên.

4. Hệ thống phòng cháy, chữa cháy phải đáp ứng theo tiêu chuẩn quy định, vừa bảo đảm an toàn tuyệt đối cho toàn hệ thống thiết bị, vừa bảo đảm an toàn cho người quản trị tại TTTHDL. Hệ thống được bảo trì, bảo dưỡng ít nhất 01 lần/năm.

5. Hệ thống camera giám sát phải bảo đảm quan sát được khu vực phòng máy chủ của TTTHDL liên tục 24/24 giờ.

Điều 15. Quy định về an ninh mạng, an ninh thông tin mạng cho hệ thống

1. Các hệ thống thông tin tại TTTHDL phải đáp ứng các yêu cầu sau:

a) Các tiêu chuẩn, quy chuẩn kỹ thuật về bảo vệ an ninh mạng theo Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính Phủ và Quyết định phê duyệt cấp độ an ninh mạng đối với các hệ thống thông tin được triển khai, cài đặt, vận hành tại TTTHDL tỉnh Đồng Tháp của cơ quan nhà nước có thẩm quyền.

b) Các hệ thống thông tin từ cấp độ 3 trở lên đặt tại TTTHDL phải được kiểm tra, đánh giá an ninh mạng theo định kỳ ít nhất 01 lần/năm bởi doanh nghiệp, tổ chức độc lập thực hiện việc kiểm tra, đánh giá và tổng hợp, báo cáo theo định kỳ.

c) Tất cả các máy chủ đang cài đặt, vận hành các phần mềm ứng dụng dùng chung, ứng dụng chuyên ngành tại TTTHDL cần được cập nhật bản vá tự động hoặc thủ công và bảo đảm trạng thái hoạt động tốt nhất.

2. Bộ phận vận hành TTTHDL có trách nhiệm phối hợp với Đơn vị chuyên trách ANM bảo đảm an ninh mạng, an ninh thông tin mạng cho các hệ thống thông tin được vận hành, cài đặt, triển khai tại TTTHDL, phối hợp với các đơn vị khai thác, thực hiện:

a) Theo dõi, kiểm tra, xử lý các cảnh báo của hệ thống giám sát an ninh mạng của TTTHDL, ghi nhận đầy đủ các sự kiện, biện pháp xử lý. Thực hiện rà soát, đánh giá theo hướng dẫn nghiệp vụ của Đơn vị chuyên trách ANM và các cơ quan có thẩm quyền.

b) Thiết lập cấu hình, cập nhật tự động các dấu hiệu, phương thức tấn công mới để hệ thống bảo mật ở trạng thái hoạt động tốt nhất nhằm ngăn chặn, xử lý hiệu quả dấu hiệu tấn công mạng, bảo đảm mật, an ninh mạng cho TTTHDL.

c) Phối hợp với các đơn vị có thẩm quyền tham gia các hoạt động, công tác bảo đảm an ninh mạng theo quy định.

3. Lãnh đạo Bộ phận vận hành TTTHDL đảm nhận vai trò đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an ninh mạng, phối hợp Đơn vị chuyên trách ANM và các cơ quan, tổ chức liên quan trong công tác hỗ trợ điều phối xử lý sự cố an ninh mạng.

4. Quản lý trình duyệt web và dịch vụ thư điện tử

a) Bộ phận vận hành phối hợp với các đơn vị có liên quan xây dựng và duy trì danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng để truy cập, khai thác các hệ thống thông tin thuộc phạm vi Quy chế.

b) Trình duyệt web và dịch vụ thư điện tử được phép sử dụng phải còn trong thời gian được nhà cung cấp hỗ trợ; phiên bản sử dụng phải được rà soát và cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc áp dụng biện pháp kiểm soát rủi ro tương đương.

c) Hệ thống thư điện tử phải được triển khai các giải pháp bảo đảm an ninh mạng phù hợp nhằm phát hiện, ngăn chặn thư điện tử độc hại, giả mạo, lừa đảo và các nguy cơ an ninh mạng khác.

d) Thực hiện sử dụng dịch vụ lọc tên miền để ngăn chặn các tên miền giả mạo, độc hại khi điều kiện kỹ thuật cho phép.

đ) Việc cài đặt và sử dụng trình duyệt web, dịch vụ thư điện tử và các thành phần mở rộng phải tuân thủ danh mục, cấu hình và hướng dẫn bảo đảm an ninh mạng của Bộ phận vận hành; các thành phần không được phép hoặc không còn nhu cầu sử dụng phải được gỡ bỏ hoặc vô hiệu hóa.

Điều 16. Quy định về an toàn hệ thống mạng

1. Hệ thống mạng phải bảo đảm:

a) Hệ thống mạng hoạt động liên tục, ổn định, an toàn, đáp ứng được yêu cầu về băng thông cho các hệ thống phần mềm, ứng dụng. Các thiết bị mạng chính phải được triển khai phương án dự phòng nóng 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.

b) Thường xuyên theo dõi, phát hiện, xử lý kịp thời những cảnh báo của hệ thống kiểm soát truy cập mạng, bảo đảm các quy định về an ninh mạng, an ninh thông tin và các chính sách bảo mật.

c) Tuân thủ các tiêu chuẩn của TTTHDL về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức đi dây, đấu nối, phân bổ nút mạng, nguồn điện.

d) Đường truyền Internet cho TTTHDL phải kết nối ít nhất từ 02 nhà cung cấp dịch vụ khác nhau, trong đó phải có dải địa chỉ IP Public hoặc có số hiệu mạng ASN riêng khi kết nối định tuyến để bảo đảm dự phòng và tính sẵn sàng cho toàn hệ thống.

đ) Các kết nối Internet, kết nối mạng TSLCD, các phân vùng mạng nội bộ quan trọng phải có các giải pháp, chính sách bảo mật bảo đảm hệ thống tránh bị xâm nhập, tấn công mạng, lây nhiễm virus, phần mềm độc hại từ bên ngoài; ngăn chặn, không để phát tán mã độc, phần mềm độc hại từ các thiết bị ngoại vi khác, giữa các phân vùng mạng với nhau. Các đơn vị sử dụng mạng TSLCD kết nối vào TTTHDL phải tuân thủ các quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an ninh mạng trên mạng TSLCD theo Quyết định số 33/2025/QĐ-TTg

ngày 15/9/2025 của Thủ tướng Chính phủ và Thông tư số 06/2026/TT-BKHCN ngày 30/3/2026 của Bộ Khoa học và Công nghệ.

2. TTTHDL phải có phương án cảnh báo thời gian thực trực tiếp đến Bộ phận vận hành khi phát hiện sự cố trên hệ thống mạng. Bộ phận vận hành chịu trách nhiệm giám sát, kiểm tra hệ thống mạng và băng thông truy cập mạng, ngăn chặn, đề xuất các biện pháp xử lý các hành vi vi phạm.

3. Bộ phận vận hành TTTHDL quản lý việc truy cập, cấu hình các thiết bị mạng trọng yếu, bảo đảm tuân thủ các quy định về an toàn, bảo mật thông tin. Các thiết bị mạng phải được cấu hình tối ưu, có giải pháp cập nhật; sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

4. Bộ phận vận hành TTTHDL và các đơn vị khai thác (*khi có nhu cầu*) phải truy cập từ xa vào hệ thống thông qua mạng riêng ảo (*VPN*), đồng thời bắt buộc áp dụng cơ chế xác thực đa nhân tố (*MFA*). Các thiết bị đầu cuối phục vụ kết nối từ xa phải đáp ứng đầy đủ các tiêu chuẩn bảo mật nghiêm ngặt bao gồm: chỉ sử dụng các kết nối mạng an toàn; cấu hình giới hạn số lần đăng nhập sai nhằm chống tấn công vét cạn. Đồng thời, các thiết bị này phải được phân quyền truy cập, cài đặt phần mềm phòng chống mã độc tập trung và hoàn tất việc rà soát, xử lý các điểm yếu an ninh mạng trước khi chính thức kết nối vào hệ thống.

5. Bộ phận vận hành thực hiện quản lý thay đổi đối với cấu hình, kết nối và các thiết bị mạng thuộc phạm vi quản lý; các thay đổi có ảnh hưởng đến an ninh mạng, tính sẵn sàng hoặc hoạt động của hệ thống phải được đánh giá, ghi nhận và kiểm tra trước hoặc sau khi thực hiện phù hợp với tính chất thay đổi.

6. Các thiết bị mạng, thiết bị bảo mật và các thành phần hạ tầng mạng phải được theo dõi tình trạng hoạt động, hiệu năng và tài nguyên sử dụng; kịp thời phát hiện nguy cơ quá tải, suy giảm hiệu năng hoặc sự cố để xử lý.

7. Việc kết nối từ bên ngoài vào hệ thống và từ hệ thống ra bên ngoài phải được kiểm soát theo dịch vụ, ứng dụng và chính sách truy cập; chỉ cho phép các kết nối cần thiết, hợp lệ và được cấp có thẩm quyền cho phép. Việc quản trị từ xa phải thực hiện thông qua kết nối mạng an toàn, sử dụng VPN hoặc phương án tương đương và cơ chế xác thực phù hợp.

8. Đối với các hệ thống, ứng dụng cung cấp dịch vụ trên môi trường Internet, căn cứ điều kiện thực tế và mức độ rủi ro, phải triển khai giải pháp WAF hoặc phương án tương đương để bảo vệ ứng dụng web và giải pháp phòng, chống tấn công từ chối dịch vụ (DDoS) hoặc phương án tương đương.

Điều 17. Quy định quản lý an toàn máy chủ và ứng dụng

Bộ phận vận hành phối hợp đơn vị khai thác và các đơn vị liên quan thực

hiện quản lý, vận hành hoạt động bình thường của máy chủ và dịch vụ, bảo đảm:

1. Hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

2. Cấu hình, các tệp nhật ký hoạt động của hệ điều hành, phần mềm được định kỳ kiểm tra nhằm kịp thời phát hiện và xử lý những sự cố (nếu có).

3. Các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng được loại bỏ để tối ưu tài nguyên hệ thống.

4. Các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng như bên ngoài vào hệ thống.

5. Các tài khoản, mật khẩu mặc định được thay đổi ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

6. Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

7. Các máy chủ và dịch vụ phải được loại bỏ khỏi hệ thống khi không còn sử dụng, bảo đảm không ảnh hưởng đến các hệ thống thông tin khác.

8. Bộ phận vận hành thực hiện quản lý bản vá đối với hệ điều hành, phần mềm, ứng dụng, thiết bị và các thành phần thuộc hệ thống thông tin. Việc quản lý bản vá phải được thực hiện tập trung trong phạm vi điều kiện kỹ thuật cho phép; các bản vá phải được kiểm tra nguồn gốc, đánh giá tác động và kiểm thử trước khi triển khai trên các hệ thống xử lý hoặc lưu trữ dữ liệu quan trọng.

Đối với các hệ thống quan trọng, trước khi triển khai bản vá phải có phương án dự phòng, phục hồi hoặc khôi phục trong trường hợp việc cập nhật bản vá không thành công. Bộ phận vận hành thường xuyên theo dõi thông tin về bản vá và lỗ hổng mới để tổ chức cập nhật kịp thời.

9. Bộ phận vận hành xây dựng, ban hành và duy trì quy trình cấu hình an toàn đối với máy chủ, máy trạm, thiết bị mạng, thiết bị bảo mật, hệ điều hành, cơ sở dữ liệu, phần mềm ứng dụng và các tài sản phần cứng, phần mềm thuộc phạm vi quản lý, vận hành.

Xây dựng và duy trì tài liệu cấu hình tiêu chuẩn và tài liệu cấu hình tăng cường bảo mật (hardening baseline) cho từng nhóm tài sản phần cứng, phần mềm phù hợp với chức năng, yêu cầu bảo vệ và điều kiện vận hành thực tế.

Sử dụng giao thức kết nối an toàn; vô hiệu hóa các giao thức mạng không an toàn, dịch vụ, chức năng không cần thiết hoặc không sử dụng; thiết lập các biện

pháp kiểm soát truy cập và tường lửa phù hợp đối với máy chủ, máy trạm và các tài sản xử lý, lưu trữ dữ liệu quan trọng.

Tài sản phần cứng, phần mềm phải được cấu hình tối ưu và tăng cường bảo mật trước khi đưa vào vận hành, khai thác.

Mọi thay đổi cấu hình phải được phê duyệt theo thẩm quyền, ghi nhận, lưu vết và bảo đảm khả năng khôi phục về cấu hình trước khi thay đổi trong trường hợp cần thiết.

Thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng, phần mềm dựa trên yêu cầu sử dụng và kết quả đánh giá rủi ro; đối với phiên quản trị phần mềm, máy chủ, thiết bị mạng và các tài sản quan trọng, thời gian tự động khóa phiên khi không sử dụng không quá 05 phút, trừ trường hợp có biện pháp kiểm soát rủi ro tương đương được phê duyệt.

Quy trình cấu hình an toàn và các tài liệu cấu hình liên quan phải được đánh giá, cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến cấu hình, kiến trúc hoặc yêu cầu bảo đảm an ninh mạng của hệ thống.

Điều 18. Quản lý an toàn dữ liệu

1. Yêu cầu an ninh mạng đối với các hệ thống thông tin có triển khai phương pháp mã hóa:

a) Phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

c) Có phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

d) Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

2. Triển khai giải pháp phòng, chống thất thoát dữ liệu (*DLP*) đối với các máy chủ cơ sở dữ liệu, máy chủ trung gian, và máy tính phục vụ nghiệp vụ xử lý dữ liệu.

3. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống, các máy chủ phải 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.

4. Bộ phận vận hành phối hợp với các Đơn vị khai thác lập, quản lý và cập nhật danh mục tài sản thông tin thuộc phạm vi quản lý, vận hành và khai thác tại TTTHDL. Danh mục tài sản thông tin phải xác định tối thiểu: tên tài sản; mô tả; hệ thống thông tin chứa hoặc xử lý; chủ sở hữu; đơn vị quản lý; mức độ nhạy cảm;

phạm vi sử dụng; thời hạn lưu trữ; phương thức xử lý; yêu cầu bảo vệ và các tài khoản, đối tượng được phép truy cập.

5. Tài sản thông tin được phân loại theo 04 mức: Công khai, Nội bộ, Hạn chế truy cập và Bí mật nhà nước theo quy định tại TCVN 14423:2026 và quy định của pháp luật có liên quan.

6. Việc yêu cầu truy cập, thêm mới, sửa đổi, xóa dữ liệu phải được phê duyệt, kiểm soát và ghi nhận theo thẩm quyền. Danh sách quyền truy cập đối với từng tài sản thông tin phải được lập, quản lý và cập nhật.

7. Bộ phận vận hành phối hợp với các Đơn vị khai thác thực hiện rà soát quyền truy cập dữ liệu tối thiểu 01 lần trong 06 tháng và cập nhật danh mục tài sản thông tin tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến việc quản lý, khai thác và bảo vệ tài sản thông tin.

8. Dữ liệu không phải là thông tin, dữ liệu công khai và dữ liệu quan trọng phải được mã hóa hoặc áp dụng biện pháp kiểm soát rủi ro tương đương phù hợp với yêu cầu bảo vệ dữ liệu; việc quản lý khóa mã hóa phải được kiểm soát chặt chẽ trong suốt vòng đời sử dụng.

9. Đối với các tài sản thông tin quan trọng, phải xác định và tài liệu hóa các luồng dữ liệu chính; thực hiện phân tách môi trường xử lý, lưu trữ dữ liệu quan trọng với dữ liệu có mức độ nhạy cảm thấp bằng biện pháp logic hoặc vật lý phù hợp với kiến trúc và điều kiện vận hành của TTTHDL.

Điều 19. Quản lý phòng chống phần mềm độc hại

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc: dò quét, kiểm tra phần mềm độc hại trên các máy chủ vận hành, triển khai, cài đặt các hệ thống thông tin và trên máy tính của bộ phận vận hành.

2. 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.

3. Các dữ liệu, tập tin cần phải được dò quét mã độc trước khi gửi nhận qua môi trường mạng và phương tiện lưu trữ di động.

4. Đối với các phương tiện lưu trữ di động như USB, ổ cứng ngoài, thẻ nhớ và các thiết bị lưu trữ tương tự, phải thực hiện rà quét mã độc trước khi sử dụng, đồng thời vô hiệu hóa chức năng tự động thực thi (autorun, autoplay...) trên các thiết bị thuộc phạm vi quản lý khi có hỗ trợ.

5. Bộ phận vận hành thực hiện kích hoạt và duy trì các tính năng phòng chống khai thác lỗ hổng trên máy chủ, máy tính người dùng, thiết bị và phần mềm

nếu thành phần đó có hỗ trợ.

6. Đối với máy chủ và máy tính người dùng thuộc phạm vi quản lý, triển khai giải pháp phát hiện và phòng chống mã độc theo hành vi (EDR) hoặc giải pháp tương đương, có khả năng phát hiện các hành vi bất thường, mã độc và mối nguy an ninh mạng; kết nối, chia sẻ thông tin cảnh báo với hệ thống giám sát, quản lý và phân tích sự kiện an ninh mạng tập trung (SIEM) để phục vụ giám sát và cảnh báo theo thời gian thực.

7. Không được tự ý gỡ bỏ hoặc vô hiệu hóa hoạt động các phần mềm phòng chống mã độc.

8. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của TTTHDL; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích sử dụng cá nhân và mục đích khác, không phục vụ công việc.

9. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc máy tính bị nhiễm mã độc (máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…) Bộ phận vận hành TTTHDL ngắt kết nối từ máy tính đến mạng nội bộ, mạng WAN, mạng Internet,… và báo trực tiếp cho bộ phận có trách nhiệm của cơ quan, tổ chức để xử lý.

Điều 20. Quản lý tài sản phần cứng, thiết bị

1. Thiết bị công nghệ thông tin thuộc phạm vi quản lý của TTTHDL phải được nhận diện, lập danh sách, theo dõi và cập nhật trạng thái trong quá trình quản lý, vận hành.

Danh mục tài sản phần cứng phải bao gồm tối thiểu các thông tin: tên tài sản; địa chỉ mạng IP đối với thiết bị sử dụng địa chỉ IP tĩnh; địa chỉ phần cứng MAC hoặc mã nhận diện serial; thời gian ngừng hỗ trợ kỹ thuật của hãng nếu có; vị trí lắp đặt địa lý; vị trí lắp đặt trong hệ thống mạng; mục đích sử dụng; tình trạng sử dụng.

Tài sản phần cứng phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

2. Đối với các thiết bị không thuộc quyền kiểm soát của TTTHDL nhưng được phép kết nối vào hệ thống thông tin, phải được đăng ký, xác định trách nhiệm quản lý và áp dụng các biện pháp kiểm soát phù hợp trước khi kết nối.

Tổ chức, cá nhân sử dụng thiết bị di động phục vụ công việc có trách nhiệm tuân thủ các quy định về quản lý, sử dụng tài sản và bảo đảm an ninh mạng.

3. Đơn vị quản lý, Đơn vị khai thác và các tổ chức, đơn vị có liên quan khi thực hiện đầu tư, mua sắm thiết bị công nghệ thông tin để lắp đặt tại TTTHDL có

trách nhiệm thực hiện bàn giao theo quy định cho Bộ phận vận hành quản lý, quản trị và vận hành kỹ thuật. Việc khai thác, sử dụng thiết bị được thực hiện theo chức năng, nhiệm vụ, nhu cầu nghiệp vụ và phân cấp quản lý của từng đơn vị, phục vụ hoạt động chung của tỉnh.

Bộ phận vận hành có trách nhiệm theo dõi tình trạng, biến động và việc sử dụng tài sản phần cứng; thực hiện kiểm kê, rà soát và cập nhật danh mục tài sản định kỳ tối thiểu 01 lần/năm hoặc theo yêu cầu quản lý tài sản có liên quan; tổng hợp, báo cáo Đơn vị quản lý theo quy định.

4. Việc sửa chữa, nâng cấp, thay thế, bổ sung hoặc đưa tài sản phần cứng ra khỏi khai thác, sử dụng phải được thực hiện theo quy định về quản lý tài sản, quản lý vận hành và các quy trình có liên quan.

Tài sản phần cứng được bổ sung, thay thế hoặc nâng cấp phải đáp ứng yêu cầu kỹ thuật, an ninh mạng và các tiêu chuẩn, quy chuẩn có liên quan theo quy định.

5. Căn cứ điều kiện thực tế và mức độ quan trọng của hệ thống thông tin, Bộ phận vận hành tổ chức thực hiện kiểm tra an ninh đối với tài sản vật lý trước khi đưa vào sử dụng và áp dụng các biện pháp bảo đảm an ninh mạng phù hợp.

6. Việc phát hiện, xác minh và xử lý các tài sản phần cứng không có trong danh mục quản lý, tài sản chưa xác định được cá nhân hoặc bộ phận chịu trách nhiệm quản lý hoặc tài sản kết nối trái phép vào hệ thống thông tin được thực hiện theo các quy trình quản lý, vận hành và bảo đảm an ninh mạng có liên quan ban hành kèm theo Quy chế này.

Các tài sản không được phép kết nối phải được áp dụng biện pháp xử lý phù hợp như từ chối kết nối, cô lập, loại bỏ hoặc đưa ra phương án quản lý theo quy định.

7. Căn cứ điều kiện vận hành thực tế, áp dụng các công cụ, giải pháp kỹ thuật phù hợp để hỗ trợ phát hiện, rà soát, theo dõi và cập nhật danh mục tài sản phần cứng. Việc sử dụng nhật ký DHCP hoặc các nguồn thông tin kỹ thuật khác để hỗ trợ cập nhật danh sách tài sản được thực hiện phù hợp với kiến trúc hệ thống và điều kiện vận hành.

Điều 21. Quy định quản lý kiểm soát truy cập và xác thực

1. Bộ phận vận hành phải lập và duy trì danh sách tất cả tài khoản trên các tài sản phần cứng và phần mềm của TTTHDL, bao gồm tối thiểu tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật và tài khoản dịch vụ.

2. Danh sách tài khoản phải có tối thiểu: loại tài khoản; tên tài khoản; trạng thái; tài sản/hệ thống thông tin tương ứng; người quản lý; phòng ban; ngày kích hoạt; ngày vô hiệu hóa (nếu có).

3. Danh sách tài khoản phải được rà soát tối thiểu 01 lần/06 tháng và ngay khi có thay đổi về nhân sự, chức năng hoặc quyền truy cập.

4. Tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật và tài khoản dịch vụ phải được quản lý tách biệt. Không sử dụng tài khoản quản trị cho hoạt động tác nghiệp thông thường.

5. Việc cấp quyền phải tuân thủ nguyên tắc quyền tối thiểu và phân tách nhiệm vụ. Quyền chỉ được cấp trong phạm vi cần thiết để thực hiện nhiệm vụ.

6. Tài khoản đặc quyền phải được quản lý bằng giải pháp quản lý tài khoản đặc quyền hoặc biện pháp tương đương; mọi hoạt động sử dụng tài khoản đặc quyền phải được ghi nhật ký và giám sát.

7. Tài khoản không còn nhu cầu sử dụng phải được vô hiệu hóa; tài khoản của người thay đổi vị trí công tác, nghỉ việc hoặc không còn trách nhiệm quản lý hệ thống phải được thu hồi quyền kịp thời.

8. Tài khoản quản trị phải áp dụng xác thực đa yếu tố (MFA), trừ trường hợp có đánh giá rủi ro và biện pháp kiểm soát tương đương được phê duyệt.

Điều 22. Quy định quản lý chính sách thiết lập và quản lý mật khẩu

1. Lãnh đạo Bộ phận vận hành có trách nhiệm tiếp nhận mật khẩu quản trị hệ thống sau khi hệ thống được bàn giao và đưa vào sử dụng; sau đó tiến hành bàn giao cho nhân sự quản trị viên hệ thống có biên bản kèm theo, lưu vào nơi an toàn.

2. Sau khi tiếp nhận, quản trị viên hệ thống phải thực hiện đổi mật khẩu. Việc đổi mật khẩu cán bộ quản trị viên hệ thống phải tuân thủ theo quy định, hướng dẫn về mật khẩu an toàn.

3. Mật khẩu phải bảo đảm độ phức tạp về độ dài, nội dung và thời gian sử dụng

a) Độ dài của mật khẩu:

- Đối với mật khẩu của người sử dụng (*dùng để đăng nhập sử dụng các hệ thống thông tin dùng chung, các ứng dụng chuyên ngành*): Tối thiểu là 12 ký tự.

- Đối với mật khẩu quản trị hệ thống (*sử dụng cho quản trị các hệ thống mạng, bảo mật, máy chủ, ứng dụng dùng chung*): Tối thiểu là 12 ký tự. Yêu cầu xác thực đa nhân tố đối với truy cập của người dùng từ bên ngoài cơ quan, tổ chức, từ đối tác/bên thứ ba, từ Internet và truy cập vào tài khoản có quyền quản trị hệ thống.

b) Nội dung mật khẩu:

- Không bao gồm các từ dễ nhớ như tên, ngày sinh, số điện thoại.

- Không được đặt theo ký tự chữ cái, ký tự chữ số tuần tự hoặc một dãy các

ký tự giống nhau, ví dụ: ABCDEFGH, 98765432 hoặc @@@@@@@@.

- Đối với mật khẩu quản trị hệ thống phải kết hợp các loại ký tự sau: Chữ cái in thường (a, b, c), chữ cái in hoa (A, B, C), ký tự số (1, 2, 3) và các ký tự đặc biệt (!, @, #).

c) Thời gian sử dụng mật khẩu:

- Đối với mật khẩu của người sử dụng: Được thiết lập trên hệ thống định kỳ 03 tháng thay đổi một lần.

- Đối với mật khẩu của người quản trị hệ thống: Được thiết lập trên hệ thống định kỳ phải thay đổi 02 tháng một lần, đồng thời bổ sung yêu cầu MFA.

Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an ninh mạng, an ninh thông tin thì lãnh đạo Bộ phận vận hành TTTHDL quyết định việc thay đổi toàn bộ mật khẩu quản trị của TTTHDL.

d) Quy định sử dụng và lưu trữ mật khẩu:

- Người sử dụng phải thay đổi mật khẩu ngay từ lần đăng nhập đầu tiên.

- Không được lưu trữ mật khẩu trên máy tính cá nhân, các thiết bị điện tử.

- Không được tiết lộ mật khẩu của cá nhân, tổ chức; trường hợp bàn giao tài khoản truy cập ứng dụng phải có biên bản bàn giao.

- Phải tiến hành thay đổi mật khẩu ngay khi nghi ngờ bị lộ, lọt thông tin mật khẩu.

- Mật khẩu mới thay đổi phải bảo đảm không trùng với những mật khẩu đã từng sử dụng trước đó.

Điều 23. Quy định quản lý giám sát an ninh mạng

1. Bộ phận vận hành thực hiện lập danh sách các nút mạng (*Node*), các thiết bị, các máy chủ đang quản lý trên hệ thống. Danh sách bao gồm tối thiểu các thông tin như địa chỉ IP, chức năng, hệ điều hành, phiên bản.

2. TTTHDL phải triển khai giải pháp giám sát an ninh mạng, an ninh thông tin mạng (*SOC*) bao gồm giám sát các thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (*nếu có*), có phương án lưu trữ và bảo vệ thông tin giám sát. Các thiết bị được giám sát có sự đồng bộ thời gian với hệ thống SOC. Giải pháp bảo đảm kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát, thực hiện việc chia sẻ dữ liệu giám sát an ninh mạng về Bộ Công an theo quy định. Bộ phận vận hành có trách nhiệm phối hợp với Đơn vị chuyên trách ANM theo dõi, kiểm tra và quản trị hệ thống giám sát.

Giải pháp giám sát phải triển khai hoặc tích hợp hệ thống quản lý thông tin

và sự kiện an ninh mạng (SIEM) để tiếp nhận, chuẩn hóa, liên kết và phân tích các sự kiện liên quan; phát hiện dấu hiệu bất thường và phát sinh cảnh báo theo hướng dẫn, yêu cầu và quy định của cơ quan, tổ chức có thẩm quyền.

3. Khi phát hiện có lỗ hổng an ninh mạng hoặc nhận được các cảnh báo về lỗ hổng an ninh mạng từ nhà cung cấp hoặc các tổ chức, đối tác chuyên nghiệp, Bộ phận vận hành cần thông báo tới Đơn vị quản lý và triển khai phương án xử lý, khắc phục.

4. Việc xử lý các lỗ hổng an ninh mạng đối với các máy chủ, thiết bị mạng quan trọng cần phải có phân tích ảnh hưởng hoặc thử nghiệm trước khi áp dụng vào hệ thống đang hoạt động và có phương án dự phòng hoặc khôi phục lại hệ thống trong trường hợp xử lý không thành công. Quá trình xử lý được ghi nhận đầy đủ các bước, các thao tác trong hệ thống quản lý sự kiện an ninh mạng, được tái sử dụng nếu có lỗ hổng tương tự.

5. Đối với các lỗ hổng an ninh mạng cần cài đặt các bản vá lỗi để xử lý, bản vá lỗi phải được tải về từ nguồn tin cậy hoặc có biện pháp kiểm tra nguồn gốc của bản vá lỗi.

6. Bộ phận vận hành có trách nhiệm thiết lập và sử dụng các tính năng tường lửa, cảnh báo phát hiện và ngăn chặn xâm nhập trên hệ điều hành, thiết bị mạng, thiết bị bảo mật, máy chủ, ứng dụng và hệ thống nếu các thành phần này có hỗ trợ. Chính sách và dấu hiệu nhận diện tấn công phải được cập nhật, kiểm tra định kỳ, bảo đảm phù hợp với mô hình mạng và các nguy cơ an ninh mạng phát sinh.

7. Các thiết bị mạng có hỗ trợ phải được cấu hình để kiểm soát truy cập đối với các cổng kết nối mạng; các cổng không sử dụng phải được khóa hoặc vô hiệu hóa, các cổng cần sử dụng chỉ được mở theo yêu cầu nghiệp vụ và được cấp có thẩm quyền phê duyệt. Cổng quản trị ứng dụng, thiết bị và hệ thống phải được thay đổi khỏi giá trị mặc định, tách biệt với cổng cung cấp dịch vụ và chỉ cho phép truy cập từ vùng mạng, địa chỉ mạng hoặc thiết bị quản trị được cấp phép.

8. TTTHDL phải thực hiện thu thập nhật ký hoạt động hoặc dữ liệu lưu lượng từ các thiết bị mạng phù hợp để phục vụ việc rà soát, phân tích, phát hiện các hoạt động bất thường và phát sinh cảnh báo. Dữ liệu thu thập phải được đồng bộ thời gian, chuyển về hệ thống giám sát tập trung, lưu trữ và bảo vệ theo quy định.

9. Bộ phận vận hành phối hợp với Đơn vị chuyên trách ANM xây dựng danh mục ngưỡng cảnh báo an ninh mạng phù hợp với từng nhóm thiết bị, hệ thống, ứng dụng và dịch vụ. Các ngưỡng cảnh báo phải được rà soát, đánh giá và điều chỉnh tối thiểu 01 lần trong 06 tháng hoặc ngay khi có thay đổi lớn về kiến trúc, cấu hình, phạm vi hoạt động hoặc xuất hiện nguy cơ an ninh mạng mới. Kết

quả rà soát, điều chỉnh phải được ghi nhận và lưu trữ.

10. Quản lý nhật ký an ninh mạng

a) Bộ phận vận hành thực hiện thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng nhằm phục vụ phát hiện sớm, phân tích và ứng phó sự cố tấn công mạng.

b) Các hệ thống, thiết bị thuộc phạm vi giám sát phải thực hiện ghi nhật ký phù hợp với chức năng; tối thiểu thu thập nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng và nhật ký cảnh báo của các thiết bị bảo mật.

c) Nhật ký truy cập hệ thống tối thiểu phải thể hiện địa chỉ nguồn, địa chỉ đích, tài khoản thực hiện truy cập, thời điểm xảy ra và thông tin về hành vi thực hiện.

d) Nhật ký tiến trình hoạt động, khi có hỗ trợ, tối thiểu phải thể hiện thông tin thiết bị, thông tin tiến trình, tài khoản thực hiện và thời điểm xảy ra.

đ) Nhật ký cảnh báo an ninh mạng tối thiểu phải thể hiện tên cảnh báo, thiết bị phát sinh, mức độ cảnh báo, địa chỉ nguồn, loại cảnh báo và thời điểm xảy ra.

e) Nhật ký phải được đồng bộ thời gian thông qua máy chủ thời gian dùng chung của hệ thống; thực hiện lưu trữ và quản lý tập trung trên hệ thống giám sát hoặc hệ thống lưu trữ nhật ký phù hợp.

g) Hệ thống phải sử dụng giải pháp SIEM hoặc sản phẩm, phương án tương đương để tiếp nhận, chuẩn hóa, liên kết và phân tích tập trung các sự kiện an ninh mạng.

h) Duy trì không gian lưu trữ nhật ký tối thiểu 03 tháng và có biện pháp theo dõi dung lượng, cảnh báo khi không gian lưu trữ có nguy cơ đầy để tránh thất thoát nhật ký.

i) Thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần trong 06 tháng và khi phát hiện dấu hiệu bất thường, sự cố hoặc theo yêu cầu của cơ quan có thẩm quyền. Kết quả rà soát phải được ghi nhận và lưu trữ.

11. Việc truy cập, khai thác, sao chép, sửa đổi hoặc quản lý dữ liệu nhật ký phải được kiểm soát theo phân quyền; bảo đảm nhật ký không bị sửa đổi, xóa bỏ trái phép. Trường hợp nhật ký chứa thông tin quan trọng, thực hiện các biện pháp bảo vệ, lưu trữ phù hợp.

Điều 24. Quy định quản lý điểm yếu an ninh mạng

Bộ phận vận hành TTTHDL chủ trì, phối hợp với Đơn vị chuyên trách ANM và các đơn vị khai thác, thực hiện xây dựng chính sách, quy trình quản lý điểm yếu an ninh mạng bao gồm:

1. Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại

điểm yếu an ninh mạng: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (*nếu có*);

2. Quản lý, cập nhật nguồn cung cấp điểm yếu an ninh mạng; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;

3. Định kỳ kiểm tra, đánh giá điểm yếu an ninh mạng cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an ninh mạng khi có thông tin hoặc nhận được cảnh báo về điểm yếu an ninh mạng đối với thành phần cụ thể trong hệ thống; Phối hợp với các bên liên quan hỗ trợ trong việc xử lý, khắc phục điểm yếu an ninh mạng.

4. Việc rà quét, đánh giá điểm yếu an ninh mạng đối với toàn bộ hệ thống thông tin phải được thực hiện tối thiểu 01 lần trong 06 tháng và thực hiện bổ sung khi có thay đổi về hệ thống, cấu hình, thành phần công nghệ hoặc khi có thông tin, cảnh báo về điểm yếu an ninh mạng có khả năng ảnh hưởng đến hệ thống.

Kết quả rà quét, đánh giá phải được phân loại theo mức độ nghiêm trọng, xác định thứ tự ưu tiên xử lý; các điểm yếu đã xử lý phải được kiểm tra, đánh giá lại để xác nhận việc khắc phục.

5. Bộ phận vận hành thực hiện quản lý bản vá đối với các tài sản phần cứng và phần mềm thuộc phạm vi hệ thống thông tin. Trong phạm vi điều kiện kỹ thuật cho phép, triển khai giải pháp quản lý bản vá tập trung; bản vá đối với hệ thống xử lý hoặc lưu trữ dữ liệu quan trọng phải được đánh giá tác động, kiểm thử và có phương án phục hồi trước khi triển khai. Các bản vá phải được lấy từ nguồn tin cậy hoặc được kiểm tra, xác minh nguồn gốc trước khi sử dụng.

Điều 25. Quy định quản lý sao lưu dữ liệu

1. Tạo lập chế độ lưu trữ thông tin theo quy định với những yêu cầu sau:

a) Với dữ liệu trên máy chủ, lưu trữ chuyên dụng, thực hiện sao lưu lên thiết bị sao lưu chuyên dụng.

b) Chu kỳ sao lưu: đối với máy chủ thực hiện sao lưu đầy đủ ít nhất 02 lần/tháng, sao lưu dữ liệu đầy đủ ít nhất 04 lần/tháng; chu kỳ sao lưu dữ liệu thay đổi ít nhất 01 lần/ngày.

c) Đối chiếu, xóa bản sao lưu: bảo đảm nguyên tắc có ít nhất 01 bản sao lưu đầy đủ gần nhất, thực hiện đối chiếu, thử nghiệm khôi phục bảo đảm bản sao lưu hoạt động bình thường khi tiến hành khôi phục.

d) Thông tin về tất cả các lần sao lưu đều được ghi rõ trong nhật ký sao lưu dữ liệu.

2. Đối với dữ liệu quan trọng, Bộ phận vận hành đề xuất Đơn vị quản lý

thuê TTTHDL dự phòng để ngăn ngừa, bảo đảm an toàn dữ liệu của hệ thống. Bản sao lưu dữ liệu bảo đảm tính toàn vẹn, tính sẵn sàng và khả năng phục hồi của dữ liệu. Các bản sao lưu dữ liệu cần phải được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng tách biệt với môi trường vận hành. Thực hiện mã hóa đối với những bản sao lưu dữ liệu quan trọng.

Điều 26. Quy định quản lý, xử lý sự cố

1. Bộ phận vận hành chủ động phối hợp với Đơn vị chuyên trách ANM thực hiện công tác giám sát, phát hiện và cảnh báo sự cố an ninh mạng cho các hệ thống thông tin tại TTTHDL. Khi phát hiện có sự cố, Bộ phận vận hành thực hiện các biện pháp phân nhóm, cô lập và xác định nguyên nhân theo nguyên tắc hạn chế tối đa ảnh hưởng đến hoạt động của hệ thống; đồng thời thông báo cho Đơn vị khai thác và các cơ quan, đơn vị có liên quan.

2. Bộ phận vận hành chủ trì xây dựng và duy trì quy trình nội bộ tiếp nhận, báo cáo sự cố an ninh mạng. Quy trình phải quy định tối thiểu đối tượng báo cáo; đầu mối tiếp nhận; kênh liên lạc chính và dự phòng; nội dung, biểu mẫu, thời hạn báo cáo; phương thức xác minh, chuyển xử lý, lưu vết và bảo mật thông tin sự cố. Tổ chức, cá nhân khi phát hiện dấu hiệu hoặc sự cố phải báo cáo ngay qua kênh được công bố; trường hợp báo cáo khẩn cấp bằng điện thoại hoặc phương tiện tức thời khác phải bổ sung báo cáo bằng văn bản hoặc trên hệ thống quản lý sự cố.

3. Các sự cố an ninh mạng được phân nhóm theo quy định hiện hành và phân loại theo ba (03) mức là sự cố thông thường, sự cố nghiêm trọng và sự cố đặc biệt nghiêm trọng:

a) Đối với sự cố thông thường, Bộ phận vận hành nhanh chóng tổ chức xử lý. Trường hợp không xử lý được, phải thông báo Đơn vị quản lý và Đơn vị chuyên trách ANM để phối hợp giải quyết.

b) Đối với sự cố nghiêm trọng liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền, cơ sở dữ liệu, mất mát hoặc lộ lọt dữ liệu và các sự cố ảnh hưởng trực tiếp đến hoạt động của TTTHDL, Bộ phận vận hành phải thực hiện ngay biện pháp khắc phục tạm thời, cô lập, hạn chế thiệt hại; phối hợp với Đơn vị chuyên trách ANM đánh giá ảnh hưởng, đề xuất phương án xử lý và huy động nhóm chuyên gia, nhà cung cấp dịch vụ hỗ trợ khi cần thiết.

c) Đối với sự cố đặc biệt nghiêm trọng gây ngưng trệ hoặc có nguy cơ gây ngưng trệ trên diện rộng, Bộ phận vận hành phải tiến hành biện pháp cô lập, ngăn chặn lây lan hoặc tạm ngừng hệ thống khi cần thiết; phối hợp với Đơn vị chuyên trách ANM đánh giá ảnh hưởng và báo cáo ngay Ủy ban nhân dân tỉnh, cơ quan có thẩm quyền để xin ý kiến chỉ đạo xử lý.

4. Việc xử lý sự cố phải tuân thủ các nguyên tắc sau:

a) Tuân thủ quy trình ứng phó sự cố đã được phê duyệt và hướng dẫn của cơ quan có thẩm quyền.

b) Bảo đảm an toàn cho người, thiết bị, hệ thống và hạn chế thấp nhất việc gián đoạn dịch vụ.

c) Dữ liệu quan trọng phải được sao lưu hoặc áp dụng biện pháp bảo toàn phù hợp trước khi xử lý, trừ trường hợp cần hành động khẩn cấp để ngăn chặn thiệt hại lớn hơn.

d) Ghi nhật ký sự cố, bảo toàn dấu vết và bằng chứng điện tử phục vụ phân tích, điều tra, xử lý theo quy định.

đ) Trường hợp sự cố vượt quá khả năng tự xử lý, phải thông báo và phối hợp với Đơn vị chuyên trách ANM, cơ quan có thẩm quyền, nhóm chuyên gia và nhà cung cấp dịch vụ hỗ trợ để ngăn chặn, khắc phục.

e) Thông báo cho các đơn vị liên quan về tình trạng xử lý, thời gian dự kiến và thời điểm hoàn tất khắc phục sự cố.

g) Đối với sự cố nghiêm trọng và đặc biệt nghiêm trọng, Bộ phận vận hành phải báo cáo nhanh qua kênh khẩn cấp đến Đơn vị quản lý, Đơn vị chủ quản và Đơn vị chuyên trách ANM trong thời hạn tối đa hai (02) giờ kể từ khi phát hiện. Trong vòng 24 giờ, Bộ phận vận hành chủ trì, phối hợp với Đơn vị chuyên trách ANM hoàn thiện báo cáo chi tiết về diễn biến, ảnh hưởng và phương án xử lý để gửi cấp có thẩm quyền theo quy định.

h) Ghi nhận đầy đủ quá trình xử lý vào hệ thống quản lý sự kiện, sự cố an ninh mạng; cập nhật bài học kinh nghiệm và ưu tiên tái sử dụng phương án xử lý đã được xác nhận hiệu quả đối với sự cố có tính chất tương tự.

5. Định kỳ hằng năm, Đơn vị chuyên trách ANM tham mưu Đơn vị chủ quản TTTHDL tổ chức diễn tập ứng phó sự cố an ninh mạng đối với các hệ thống thông tin đang được cài đặt, triển khai, vận hành tại TTTHDL. Kết quả diễn tập phải được đánh giá, lưu hồ sơ và sử dụng để cập nhật phương án, quy trình ứng phó.

6. Quy trình nội bộ báo cáo sự cố, quy trình ứng phó sự cố và danh sách đầu mối liên lạc phải được rà soát tối thiểu một (01) lần/năm hoặc ngay khi có thay đổi về tổ chức, nhân sự, hệ thống, yêu cầu pháp lý hoặc điều kiện khác ảnh hưởng đến quy trình.

Điều 27. Quy định quản lý bản quyền phần mềm, ứng dụng

1. Các tài sản phần mềm, ứng dụng được cài đặt, triển khai và sử dụng thuộc phạm vi quản lý của TTTHDL phải được lập danh sách, theo dõi và cập nhật trạng

thái trong quá trình sử dụng.

Chỉ các phần mềm, ứng dụng đã được phê duyệt hoặc thuộc danh mục được phép sử dụng mới được cài đặt và sử dụng trên các hệ thống thuộc phạm vi quản lý.

2. Danh mục tài sản phần mềm, ứng dụng phải bao gồm tối thiểu các thông tin: tên tài sản; mục đích sử dụng; thời gian ngừng hỗ trợ kỹ thuật nếu có; phạm vi sử dụng; thông tin về cá nhân hoặc bộ phận quản lý; thông tin về bản quyền hoặc hình thức cấp phép; phiên bản; hệ thống thông tin thành phần hoặc tài sản phần cứng có liên quan nếu có.

Tài sản phần mềm phải được giao trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

3. Các phần mềm, ứng dụng có yêu cầu về bản quyền hoặc điều kiện cấp phép phải bảo đảm quyền sử dụng hợp pháp theo quy định của pháp luật và điều kiện của nhà sản xuất, nhà cung cấp.

Bộ phận vận hành có trách nhiệm theo dõi tình trạng sử dụng, thời hạn sử dụng, thời gian hỗ trợ kỹ thuật và các điều kiện liên quan để báo cáo, đề xuất biện pháp phù hợp, bao gồm gia hạn, nâng cấp, thay thế hoặc áp dụng biện pháp kiểm soát cần thiết, bảo đảm hoạt động liên tục, ổn định của hệ thống.

4. Việc kiểm kê, rà soát và cập nhật danh mục tài sản phần mềm được thực hiện định kỳ tối thiểu 01 lần/06 tháng hoặc khi có thay đổi đáng kể liên quan đến hệ thống thông tin.

Việc cài đặt, nâng cấp, thay đổi hoặc gỡ bỏ phần mềm, ứng dụng được thực hiện theo phân quyền và các quy trình quản lý, vận hành có liên quan ban hành kèm theo Quy chế này. Tần suất rà soát tối thiểu 06 tháng/lần.

5. Việc phát hiện, xác minh và xử lý phần mềm, ứng dụng không thuộc danh mục được phép sử dụng hoặc chưa được phê duyệt theo thẩm quyền được thực hiện theo các quy trình quản lý, vận hành và bảo đảm an ninh mạng có liên quan ban hành kèm theo Quy chế này.

Phần mềm, ứng dụng không được phép sử dụng phải được gỡ bỏ, vô hiệu hóa hoặc áp dụng biện pháp xử lý phù hợp.

Trường hợp cần thiết tiếp tục sử dụng để phục vụ hoạt động nghiệp vụ nhưng chưa đáp ứng đầy đủ điều kiện quản lý, phải được đánh giá rủi ro an ninh mạng, xem xét chấp thuận theo thẩm quyền và áp dụng các biện pháp kiểm soát phù hợp trong thời gian sử dụng.

6. Không được sao chép, phát tán, chia sẻ hoặc sử dụng trái phép phần mềm, ứng dụng thuộc phạm vi quản lý của TTTHDL, trừ trường hợp được phép theo

quy định của pháp luật hoặc điều kiện cấp phép của chủ sở hữu, nhà sản xuất hoặc nhà cung cấp.

Điều 28. Quy định an toàn trong phát triển phần mềm

1. Thiết lập và duy trì quy trình phát triển phần mềm, ứng dụng an toàn trong toàn bộ vòng đời:

a) Hệ thống thông tin khi xây dựng phải có đầy đủ tài liệu mô tả thiết kế các thành phần hệ thống; quy mô, phạm vi, đối tượng sử dụng, khai thác, quản lý vận hành; phương án lựa chọn giải pháp công nghệ và phương án bảo đảm an ninh mạng theo cấp độ phù hợp.

b) Phần mềm nội bộ được xây dựng mới, mở rộng hoặc nâng cấp phải tuân thủ khung, quy trình phát triển phần mềm an toàn. Đơn vị phát triển phải áp dụng tiêu chuẩn, quy trình về chất lượng, an ninh mạng và an ninh thông tin tương ứng hoặc cao hơn yêu cầu áp dụng tại TTTHDL.

c) Khi thay đổi thiết kế, mã nguồn, kiến trúc hoặc thành phần phụ thuộc, Đơn vị vận hành, Đơn vị khai thác và các đơn vị liên quan phải đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an ninh mạng.

d) Quy trình phát triển phần mềm, ứng dụng an toàn phải được đánh giá, cập nhật tối thiểu một (01) lần/năm hoặc khi có thay đổi có thể ảnh hưởng đến quy trình.

2. Việc xây dựng kiến trúc và phát triển ứng dụng phải kết hợp các nguyên tắc bảo mật, tối thiểu gồm:

a) Kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.

b) Kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về hệ thống hoặc thiết bị yêu cầu.

c) Có biện pháp bảo vệ ứng dụng trước các dạng tấn công phổ biến và áp dụng nguyên tắc phân quyền tối thiểu cần thiết.

d) Có chức năng kiểm soát lỗi, thông báo lỗi phù hợp; không để thông báo lỗi làm lộ mã nguồn, cấu hình, thông tin xác thực, dữ liệu nhạy cảm hoặc thông tin nội bộ của hệ thống.

đ) Không lưu trữ trực tiếp thông tin xác thực, khóa bí mật, mật khẩu hoặc thông tin bí mật khác trong mã nguồn ứng dụng; phải sử dụng cơ chế quản lý bí mật và cấu hình an toàn.

3. Đối với phần mềm phát triển thuê khoán:

a) Phải có biên bản, hợp đồng và cam kết bảo mật quy định rõ phạm vi công

việc, quyền sở hữu hoặc quyền sử dụng, trách nhiệm bảo vệ dữ liệu, trách nhiệm khắc phục lỗ hổng và trách nhiệm pháp lý của bên phát triển.

b) Yêu cầu bên phát triển bàn giao mã nguồn phần mềm, tài liệu kỹ thuật, hướng dẫn triển khai và các thành phần cần thiết để quản lý, kiểm tra an ninh mạng. Trường hợp không thể cung cấp mã nguồn, phải cung cấp chứng chỉ hoặc báo cáo đánh giá an toàn độc lập; hoặc thực hiện kiểm thử xâm nhập, áp dụng biện pháp giám sát rủi ro thay thế và cam kết chịu trách nhiệm pháp lý về tính an toàn của phần mềm.

c) Bên phát triển phải tuân thủ quy trình phát triển phần mềm an toàn, phối hợp tiếp nhận và khắc phục lỗ hổng trong suốt thời gian bảo hành, bảo trì hoặc cung cấp dịch vụ.

4. Kiểm tra an ninh, an toàn và nghiệm thu phần mềm, ứng dụng:

a) Thực hiện kiểm tra, đánh giá bảo mật bằng hình thức hộp đen (Black box), hộp xám (Gray box), hộp trắng (White box) hoặc hình thức phù hợp khác tùy theo nền tảng, mức độ rủi ro và khả năng tiếp cận.

b) Trước khi đưa vào vận hành chính thức, phải kiểm tra và khắc phục lỗ hổng của ứng dụng, lỗ hổng trong mã nguồn, thư viện, thành phần mở rộng và các thành phần của bên thứ ba mà ứng dụng sử dụng. Khi thay đổi mã nguồn, kiến trúc, thư viện hoặc thành phần phụ thuộc có ảnh hưởng đến an ninh mạng, phải kiểm tra, đánh giá lại.

c) Phải có nội dung, kế hoạch, quy trình kiểm thử và nghiệm thu; có đơn vị hoặc bộ phận giám sát; có báo cáo kết quả và xác nhận hoàn thành việc khắc phục các lỗ hổng thuộc mức phải xử lý trước khi bàn giao, đưa vào sử dụng.

5. Tiếp nhận và xử lý báo cáo lỗ hổng bảo mật phần mềm:

a) Bộ phận vận hành chủ trì, phối hợp với Đơn vị khai thác và Đơn vị chuyên trách ANM xây dựng, duy trì quy trình tiếp nhận và xử lý báo cáo lỗ hổng bảo mật phần mềm; công bố ít nhất một kênh để cá nhân, tổ chức bên ngoài có thể gửi báo cáo, như địa chỉ thư điện tử chuyên dụng, số điện thoại hoặc cổng tiếp nhận trực tuyến.

b) Báo cáo lỗ hổng phải được xác minh, phân loại, đánh giá mức độ rủi ro, giao đơn vị xử lý, theo dõi thời hạn, phản hồi cho bên báo cáo khi phù hợp, kiểm tra kết quả khắc phục và đóng hồ sơ.

c) Quy trình tiếp nhận và xử lý báo cáo lỗ hổng bảo mật phần mềm phải được đánh giá, cập nhật tối thiểu một (01) lần/năm hoặc khi có thay đổi có thể ảnh hưởng đến quy trình.

Điều 29. Quy định về vận hành, bảo trì, bảo dưỡng

1. Bộ phận vận hành thực hiện

a) Xây dựng và ban hành kế hoạch vận hành, bảo trì, bảo dưỡng hệ thống sử dụng nguồn ngân sách được cấp hằng năm.

b) Thực hiện đặt hàng cung cấp sản phẩm, dịch vụ công về vận hành, bảo trì, bảo dưỡng cho TTTHDL theo quy định của pháp luật.

2. Yêu cầu về vận hành, bảo trì, bảo dưỡng

a) Việc thực hiện vận hành, bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến tình hình vận hành của TTTHDL.

b) Quá trình vận hành, bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, kế hoạch và ghi nhật ký về tình trạng hoạt động trước và sau khi thực hiện.

Điều 30. Quy định về cung cấp, tiếp nhận thiết bị và phần mềm của các đơn vị tại TTTHDL

1. Việc triển khai các dự án, nhiệm vụ ứng dụng công nghệ thông tin trên hạ tầng TTTHDL phải được quy định cụ thể trong thiết kế kỹ thuật được cơ quan có thẩm quyền phê duyệt.

2. Đối với các cơ quan, đơn vị có nhu cầu đặt máy chủ để triển khai các ứng dụng dùng riêng cho cơ quan, đơn vị mình trên hạ tầng TTTHDL: Các cơ quan, đơn vị phối hợp Đơn vị quản lý xin chủ trương Ủy ban nhân dân tỉnh; sau khi có chủ trương đồng ý của Ủy ban nhân dân tỉnh, Đơn vị quản lý sẽ phối hợp các cơ quan, đơn vị và Bộ phận vận hành thực hiện quy trình/thủ tục cung cấp, tiếp nhận đặt máy chủ, cài đặt phần mềm và quản lý tài sản theo quy định hiện hành.

3. Các đơn vị có thiết bị hoặc ứng dụng đặt tại TTTHDL chịu trách nhiệm quản trị nội dung, phần mềm của đơn vị mình đồng thời tuân thủ các nguyên tắc và bảo đảm an ninh mạng, an ninh thông tin của hệ thống theo các quy định hiện hành.

Điều 31. Quy định về quản lý tài liệu liên quan hoạt động của TTTHDL

1. Danh sách các loại hồ sơ lưu trữ

a) Các quy trình vận hành kỹ thuật, bảo trì, bảo dưỡng các hệ thống.

b) Hồ sơ thiết kế, thuyết minh kỹ thuật, hoàn công.

c) Bảng thống kê danh sách thiết bị; danh sách các thiết bị hỏng, hết khấu hao sử dụng chờ thanh lý, thanh hủy; biên bản bàn giao thiết bị.

d) Tài liệu, biên bản kiểm tra, đánh giá của TTTHDL.

e) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ phải được lưu bằng văn bản, tập tin bản mềm trên máy tính và phải được cập nhật khi có sự thay đổi theo quy định.

Điều 32. Quy định kiểm tra, báo cáo định kỳ

1. Hằng tuần, quản trị viên hệ thống vận hành TTTHDL thực hiện báo cáo tình hình hoạt động của TTTHDL đến lãnh đạo Bộ phận vận hành.

2. Đơn vị quản lý tổ chức kiểm tra việc tuân thủ các quy định về quản lý, triển khai, vận hành và khai thác sử dụng TTTHDL theo các quy định tại Quy chế này tối thiểu 01 năm một lần.

3. Các nội dung kiểm tra

a) Việc bảo đảm các điều kiện về môi trường cho hoạt động của TTTHDL.

b) Tình hình sử dụng thiết bị, sử dụng ứng dụng của hệ thống.

c) Hoạt động của hệ thống máy chủ các dịch vụ (*cập nhật các bản vá, bản sửa lỗi, dung lượng ổ cứng, hiệu năng sử dụng*).

d) Tình hình an toàn, bảo mật hệ thống, đánh giá hiệu quả (*khả năng phát hiện và ngăn chặn*) của hệ thống bảo mật.

đ) Kiểm tra công tác sao lưu, lưu trữ, phục hồi dữ liệu.

e) Việc tuân thủ các quy định khác nêu tại quy chế này.

Điều 33. Quản lý rủi ro an ninh mạng

1. Nguyên tắc quản lý

Công tác bảo đảm an ninh mạng đối với các hệ thống thông tin, nền tảng, ứng dụng, hạ tầng kỹ thuật và dịch vụ thuộc phạm vi quản lý, vận hành của TTTHDL được thực hiện trên cơ sở quản lý rủi ro an ninh mạng.

Việc lựa chọn và triển khai các biện pháp bảo đảm an ninh mạng phải phù hợp với mức độ quan trọng của hệ thống thông tin, giá trị tài sản, tính chất của dữ liệu, mức độ rủi ro và các yêu cầu có liên quan theo quy định của pháp luật.

Việc quản lý rủi ro được thực hiện theo phạm vi trách nhiệm của Đơn vị quản lý, Đơn vị khai thác, Bộ phận vận hành và các tổ chức, cá nhân có liên quan đối với từng hệ thống thông tin.

2. Xác định phạm vi và rủi ro

Việc quản lý rủi ro an ninh mạng được thực hiện trên cơ sở xác định phạm vi, ranh giới vật lý, kết nối logic và các tài sản thuộc hệ thống thông tin.

Việc xác định rủi ro phải xem xét các yếu tố có liên quan, bao gồm tối thiểu tài sản phần cứng, phần mềm, ứng dụng, dữ liệu, hạ tầng kỹ thuật, tài khoản và

quyền truy cập, lỗ hổng bảo mật, các mối đe dọa, kết nối với hệ thống bên ngoài và rủi ro từ bên thứ ba, nhà cung cấp.

Việc xác định, nhận diện rủi ro có thể dựa trên quản lý tài sản, lỗ hổng, hạ tầng mạng, nhận thức, tài khoản và quyền truy cập; đồng thời phải xem xét rủi ro từ bên thứ ba, nhà cung cấp.

3. Đánh giá và xử lý rủi ro

Việc xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng được thực hiện theo Quy trình Quản lý rủi ro ban hành kèm theo Quy chế này.

Việc đánh giá, rà soát rủi ro được thực hiện định kỳ và thực hiện bổ sung khi có thay đổi liên quan đến hệ thống thông tin, xuất hiện lỗ hổng bảo mật mới, xảy ra sự kiện hoặc sự cố an ninh mạng, hoặc các thay đổi khác có khả năng ảnh hưởng đến mức độ rủi ro.

4. Biện pháp xử lý rủi ro

Căn cứ kết quả đánh giá rủi ro, các đơn vị, bộ phận có liên quan thực hiện các biện pháp xử lý rủi ro phù hợp theo Quy trình Quản lý rủi ro và các quy định có liên quan.

Việc xử lý rủi ro có thể bao gồm áp dụng biện pháp giảm thiểu rủi ro, chấp nhận rủi ro, chuyển giao hoặc chia sẻ rủi ro, hoặc loại bỏ nguyên nhân làm phát sinh rủi ro, phù hợp với kết quả đánh giá và thẩm quyền quyết định. Việc chấp nhận rủi ro phải được xem xét, chấp thuận theo thẩm quyền và phân cấp quản lý.

Đối với các rủi ro còn tồn tại sau khi áp dụng biện pháp xử lý, phải tiếp tục theo dõi và áp dụng phương án ứng phó phù hợp khi rủi ro xảy ra.

5. Giám sát rủi ro

Thực hiện theo dõi, giám sát và cập nhật các thay đổi liên quan đến rủi ro đã được xác định và hiệu quả của các biện pháp kiểm soát đã áp dụng.

Việc giám sát được thực hiện thông qua các hoạt động quản lý, vận hành, giám sát an ninh mạng và các công cụ kỹ thuật phù hợp với phạm vi, yêu cầu bảo đảm an ninh mạng của hệ thống. Kết quả giám sát là cơ sở để cập nhật thông tin rủi ro và thực hiện đánh giá, xử lý khi cần thiết.

6. Truyền thông và báo cáo rủi ro an ninh mạng

Kết quả đánh giá rủi ro và các thay đổi quan trọng liên quan đến rủi ro an ninh mạng được chia sẻ, thông báo cho các đơn vị, cá nhân có liên quan theo phạm vi trách nhiệm để phối hợp thực hiện các biện pháp xử lý phù hợp.

Các rủi ro có khả năng ảnh hưởng nghiêm trọng đến hoạt động của hệ thống

thông tin hoặc TTTHDL phải được báo cáo kịp thời cho cấp có thẩm quyền để xem xét, chỉ đạo xử lý.

Điều 34. Quản lý vòng đời kết thúc hệ thống thông tin

1. Nguyên tắc chung:

Việc kết thúc vận hành, thanh lý hoặc hủy bỏ hệ thống thông tin phải thực hiện theo quy trình kiểm soát chặt chẽ, bảo đảm tuyệt đối không làm lộ lọt, thất thoát hoặc sai lệch dữ liệu. Quá trình này phải tuân thủ đồng thời các quy định về an ninh mạng và pháp luật về quản lý, sử dụng tài sản công.

2. Lập kế hoạch chấm dứt hoạt động:

a) Xây dựng kế hoạch chi tiết bao gồm: Phạm vi hệ thống, lộ trình thực hiện, phương án xử lý dữ liệu và danh mục tài sản cần thu hồi.

b) Thực hiện đánh giá tác động, xác định các hệ thống liên quan và mức độ ảnh hưởng đến các quy trình nghiệp vụ khi hệ thống dừng hoạt động.

3. Sao lưu và bảo toàn dữ liệu:

a) Thực hiện sao lưu toàn bộ cơ sở dữ liệu và cấu hình hệ thống trọng yếu trước khi chính thức dừng vận hành.

b) Kiểm tra, xác nhận khả năng khôi phục và tính toàn vẹn của dữ liệu đã sao lưu; thực hiện lưu trữ hồ sơ dữ liệu theo thời hạn quy định của pháp luật hiện hành.

4. Xóa và tiêu hủy dữ liệu an toàn:

a) Áp dụng các biện pháp kỹ thuật chuyên dụng để xóa hoặc tiêu hủy dữ liệu không còn nhu cầu sử dụng, bảo đảm không thể khôi phục sau khi xử lý.

b) Đối với dữ liệu thuộc danh mục bí mật nhà nước hoặc dữ liệu nhạy cảm, quá trình tiêu hủy phải được giám sát chặt chẽ và lập biên bản xác nhận theo quy định.

5. Thu hồi tài khoản và vô hiệu hóa kết nối:

a) Thu hồi toàn bộ tài khoản quản trị, quyền truy cập của người dùng và các khóa bảo mật liên quan đến hệ thống.

b) Vô hiệu hóa các kết nối liên thông, các cổng giao tiếp API và quy trình trao đổi dữ liệu tự động với các hệ thống ngoại vi để bảo đảm an ninh mạng.

6. Xử lý hạ tầng thiết bị và tài sản:

a) Thu hồi các thiết bị phần cứng, hạ tầng mạng và tài sản công liên quan.

b) Thực hiện rà soát, xóa sạch dữ liệu trên các thiết bị lưu trữ trước khi chuyển đổi mục đích sử dụng hoặc thực hiện quy trình thanh lý tài sản theo quy định.

7. Đánh giá và hoàn tất hồ sơ:

a) Tổ chức kiểm tra, đánh giá toàn diện việc thực hiện các bước trong quy trình kết thúc hệ thống.

b) Lập biên bản xác nhận hoàn thành việc chấm dứt vận hành, thanh lý hoặc hủy bỏ hệ thống; thực hiện lưu trữ hồ sơ quyết định và các văn bản liên quan để phục vụ công tác hậu kiểm.

Chương III
TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC, CÁ NHÂN TRONG VIỆC BẢO ĐẢM AN NINH MẠNG TTTHDL

Điều 35. Trách nhiệm của Đơn vị khai thác

1. Sử dụng hạ tầng, phần mềm ứng dụng theo Quy chế này và các hướng dẫn kỹ thuật của Đơn vị quản lý, Bộ phận vận hành; chấp hành nghiêm các quy định pháp luật về an ninh mạng trong cơ quan nhà nước.

2. Chịu trách nhiệm trực tiếp về tính chính xác, hợp pháp của thông tin dữ liệu lưu trữ và nội dung phần mềm ứng dụng do đơn vị cung cấp tại TTTHDL.

3. Trường hợp có nhu cầu đặt máy chủ dùng riêng tại TTTHDL, đơn vị phải lập văn bản xin chủ trương và chỉ thực hiện các thủ tục tiếp nhận, cài đặt sau khi có sự đồng ý của Ủy ban nhân dân tỉnh.

4. Phân công ít nhất một công chức, viên chức có trình độ CNTT/ANM làm đầu mối kỹ thuật; chịu trách nhiệm quản trị ứng dụng tại đơn vị, bảo đảm tính thống nhất về cấu trúc hạ tầng vật lý và là đầu mối phối hợp ứng cứu sự cố.

5. Người dùng chịu trách nhiệm bảo mật tài khoản cá nhân, tuyệt đối không truy cập trái phép vào hệ thống của tổ chức khác. Khi truy cập từ xa, bắt buộc sử dụng VPN và xác thực đa nhân tố (*MFA*) theo hướng dẫn của Bộ phận vận hành.

6. Các thiết bị kết nối vào hệ thống phải bảo đảm đã được phân quyền, cài đặt phần mềm phòng chống mã độc và rà soát, xử lý các điểm yếu an ninh mạng trước khi thực hiện kết nối.

7. Khi phát sinh sự cố, phải thông báo ngay cho Bộ phận vận hành để phối hợp xử lý; đồng thời có trách nhiệm tiếp nhận và thực hiện các yêu cầu điều phối từ Bộ phận vận hành khi sự cố chung ảnh hưởng đến ứng dụng của đơn vị.

8. Khi thực hiện nâng cấp hoặc thay đổi thiết kế phần mềm, đơn vị phải chủ động phối hợp với các cơ quan chuyên trách để đánh giá lại tính phù hợp của các phương án bảo mật trước khi vận hành chính thức.

9. Chủ trì, phối hợp Bộ phận vận hành thực hiện trách nhiệm Đơn vị khai thác đối với các hệ thống thông tin do đơn vị triển khai tại TTTHDL; rà soát, lập hồ sơ đề xuất cấp độ đối với hệ thống thông tin do đơn vị triển khai tại TTTHDL.

10. Chủ trì, phối hợp với Đơn vị chuyên trách ANM, Bộ phận vận hành thực hiện công tác kiểm tra, đánh giá an ninh mạng định kỳ đối với hệ thống thông tin do đơn vị triển khai tại TTTHDL theo quy định hiện hành.

11. Đơn vị khai thác phải có trách nhiệm kịp thời thông báo bằng văn bản cho Đơn vị quản lý, Bộ phận vận hành biết trong trường hợp kết thúc vận hành phần mềm, ứng dụng đã triển khai trên hạ tầng TTTHDL để thực hiện quy trình kết thúc vận hành theo quy chế này.

Điều 36. Trách nhiệm của Bộ phận vận hành

1. Bộ phận vận hành chịu trách nhiệm về vận hành và khai thác có hiệu quả hoạt động của TTTHDL. Tuân thủ và tổ chức thực hiện các quy định liên quan theo Quy chế này.

2. Xây dựng kế hoạch, bố trí nhân sự trực vận hành hệ thống TTTHDL bảo đảm hệ thống vận hành thông suốt, liên tục trong vòng 24 giờ/ngày, 07 ngày/tuần kể cả các ngày lễ, Tết trong năm.

3. Xây dựng và tham mưu cho Đơn vị quản lý ban hành các quy trình vận hành Hệ thống quản lý an toàn thông tin và an ninh mạng theo tiêu chuẩn ISO/IEC 27001:2022, TCVN 14423:2026 và các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ và các tiêu chuẩn, quy chuẩn kỹ thuật chuyên ngành có liên quan.

4. Phối hợp Đơn vị khai thác rà soát, lập hồ sơ đề xuất cấp độ đối với hệ thống thông tin do Đơn vị khai thác triển khai tại TTTHDL theo quy định tại Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ, gửi về Đơn vị quản lý, cơ quan có thẩm quyền thẩm định xem xét, phê duyệt.

5. Bảo đảm các yêu cầu về hạ tầng kỹ thuật, chất lượng dịch vụ, an ninh mạng và hoạt động thông suốt của TTTHDL.

6. Đào tạo quản trị viên hệ thống có chuyên môn đáp ứng yêu cầu, được trang bị các kiến thức liên quan tới hoạt động của TTTHDL.

7. Xây dựng kế hoạch hợp tác, khai thác TTTHDL với các tổ chức có liên quan và triển khai các nhiệm vụ được cấp trên giao.

8. Thực hiện báo cáo định kỳ hằng năm cho Đơn vị quản lý về tình hình hoạt động của TTTHDL và báo cáo đột xuất khi có yêu cầu.

9. Chủ trì, phối hợp với Đơn vị chuyên trách ANM thực hiện công tác kiểm tra, đánh giá an ninh mạng định kỳ tối thiểu 01 lần/năm đối với TTTHDL; phối

hợp Đơn vị khai thác, Đơn vị chuyên trách ANM thực hiện công tác kiểm tra, đánh giá an ninh mạng định kỳ đối với các hệ thống thông tin do Đơn vị khai thác triển khai tại TTTHDL.

Điều 37. Trách nhiệm của Đơn vị quản lý

1. Quản lý nhà nước đối với tài sản tại TTTHDL theo quy định pháp luật; điều chuyển tài sản thuộc thẩm quyền quản lý cho Bộ phận vận hành để quản lý, sử dụng theo quy định pháp luật.

2. Chủ trì tổng hợp dự toán trên cơ sở đề xuất của Bộ phận vận hành TTTHDL trình cơ quan có thẩm quyền thẩm định, phê duyệt và giao dự toán để bảo đảm hệ thống hoạt động ổn định, liên tục.

3. Tiếp nhận báo cáo về tình trạng thiết bị từ Bộ phận vận hành để xin chủ trương của cơ quan có thẩm quyền bố trí ngân sách nhà nước theo pháp luật về ngân sách nhà nước hằng năm nhằm kịp thời sửa chữa, nâng cấp hoặc thay thế các thiết bị hư hỏng, lạc hậu.

4. Căn cứ đề xuất của Bộ phận vận hành, xem xét trình cơ quan có thẩm quyền quyết định việc thuê hạ tầng dự phòng (*DR*) cho các hệ thống dữ liệu quan trọng nhằm ngăn ngừa rủi ro và bảo đảm an ninh mạng của tỉnh.

5. Tổ chức kiểm tra việc tuân thủ quy định vận hành, điều kiện môi trường phòng máy và hiệu quả bảo mật an ninh mạng tại TTTHDL, tối thiểu 01 năm/lần.

6. Tiếp nhận báo cáo khẩn cấp (*trong vòng 02 giờ*) đối với các sự cố nghiêm trọng để kịp thời cho ý kiến chỉ đạo; phối hợp với Bộ phận vận hành và các đơn vị chuyên trách để khắc phục sự cố và lỗ hổng bảo mật.

7. Trực tiếp thực hiện các quy trình, thủ tục tiếp nhận máy chủ, cài đặt phần mềm cho các cơ quan, đơn vị có nhu cầu đặt thiết bị tại hạ tầng TTTHDL khi có chủ trương của Ủy ban nhân dân tỉnh.

8. Tiếp nhận và xử lý các phản ánh, vướng mắc phát sinh trong quá trình thực hiện Quy chế; tổng hợp báo cáo và tham mưu cho Ủy ban nhân dân tỉnh xem xét, quyết định đối với các vấn đề vượt thẩm quyền.

Điều 38. Trách nhiệm của Đơn vị chuyên trách ANM

1. Chủ trì tiếp nhận, điều phối và tổng hợp báo cáo các sự cố an ninh mạng trong toàn hệ thống để kịp thời báo cáo Ủy ban nhân dân tỉnh và thông báo cho các cơ quan, đơn vị liên quan.

2. Phối hợp chặt chẽ với Bộ phận vận hành trong công tác giám sát, phát hiện sớm và phát tin cảnh báo sự cố đối với các hệ thống thông tin tại TTTHDL.

3. Trực tiếp tham gia xử lý các sự cố mức độ 3 hoặc đặc biệt nghiêm trọng;

chủ trì đánh giá mức độ thiệt hại, đề xuất phương án khắc phục khẩn cấp và báo cáo Ủy ban nhân dân tỉnh để xin ý kiến chỉ đạo.

4. Định kỳ hằng năm, có trách nhiệm tham mưu cho Cơ quan chủ quản tổ chức các đợt diễn tập ứng cứu sự cố an ninh mạng nhằm nâng cao năng lực phản ứng nhanh cho đội ngũ kỹ thuật.

5. Phối hợp với Bộ phận vận hành, Đơn vị khai thác thực hiện công tác kiểm tra, đánh giá an ninh mạng định kỳ, tối thiểu 01 lần/năm đối với TTTHDL, các hệ thống thông tin từ cấp độ 3 trở lên theo quy định hiện hành.

6. Chủ trì, phối hợp với Bộ phận vận hành theo dõi, kiểm tra và quản trị nghiệp vụ đối với giải pháp giám sát an ninh mạng, an ninh thông tin (SOC), bảo đảm hệ thống giám sát hoạt động chính xác và hiệu quả.

7. Chủ trì, phối hợp với các đơn vị liên quan tham mưu ban hành các quy trình vận hành, quản lý lỗ hổng, điểm yếu an toàn thông tin và quản lý an ninh mạng theo tiêu chuẩn ISO/IEC 27001:2022, TCVN 14423:2026 và các tiêu chuẩn, quy chuẩn kỹ thuật chuyên ngành có liên quan.

8. Chủ trì, phối hợp với các cơ quan liên quan xây dựng nội dung và triển khai các chương trình đào tạo, tập huấn nâng cao nhận thức về an ninh mạng cho cán bộ, công chức, viên chức trên địa bàn tỉnh.

Chương IV
TỔ CHỨC THỰC HIỆN VÀ ĐIỀU KHOẢN THI HÀNH

Điều 39. Tổ chức triển khai Quy chế

Các cơ quan, đơn vị và địa phương có kết nối hoặc đang đặt hệ thống thông tin tại TTTHDL tỉnh có trách nhiệm thực hiện, phổ biến Quy chế này đến toàn thể công chức, viên chức, người lao động trong cơ quan, đơn vị và địa phương nắm để triển khai thực hiện; chịu trách nhiệm trước pháp luật và Ủy ban nhân dân tỉnh về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị.

Điều 40. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hằng năm hoặc khi có thay đổi chính sách an ninh mạng kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an ninh mạng.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an ninh mạng.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh,

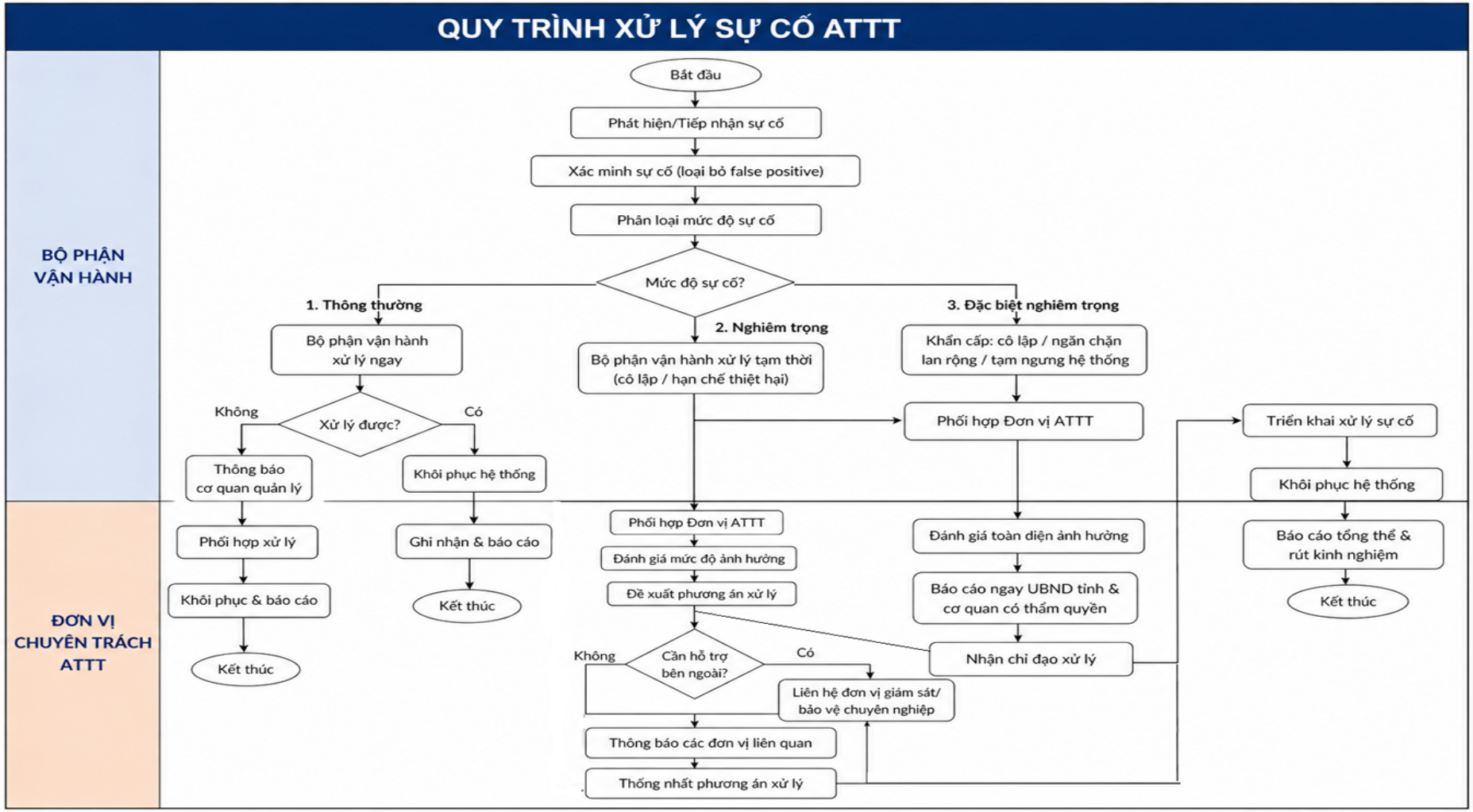
các đơn vị phản ánh kịp thời về Sở Khoa học và Công nghệ để phối hợp xử lý; trường hợp vượt quá thẩm quyền, Sở Khoa học và Công nghệ tổng hợp báo cáo, trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

Phụ lục

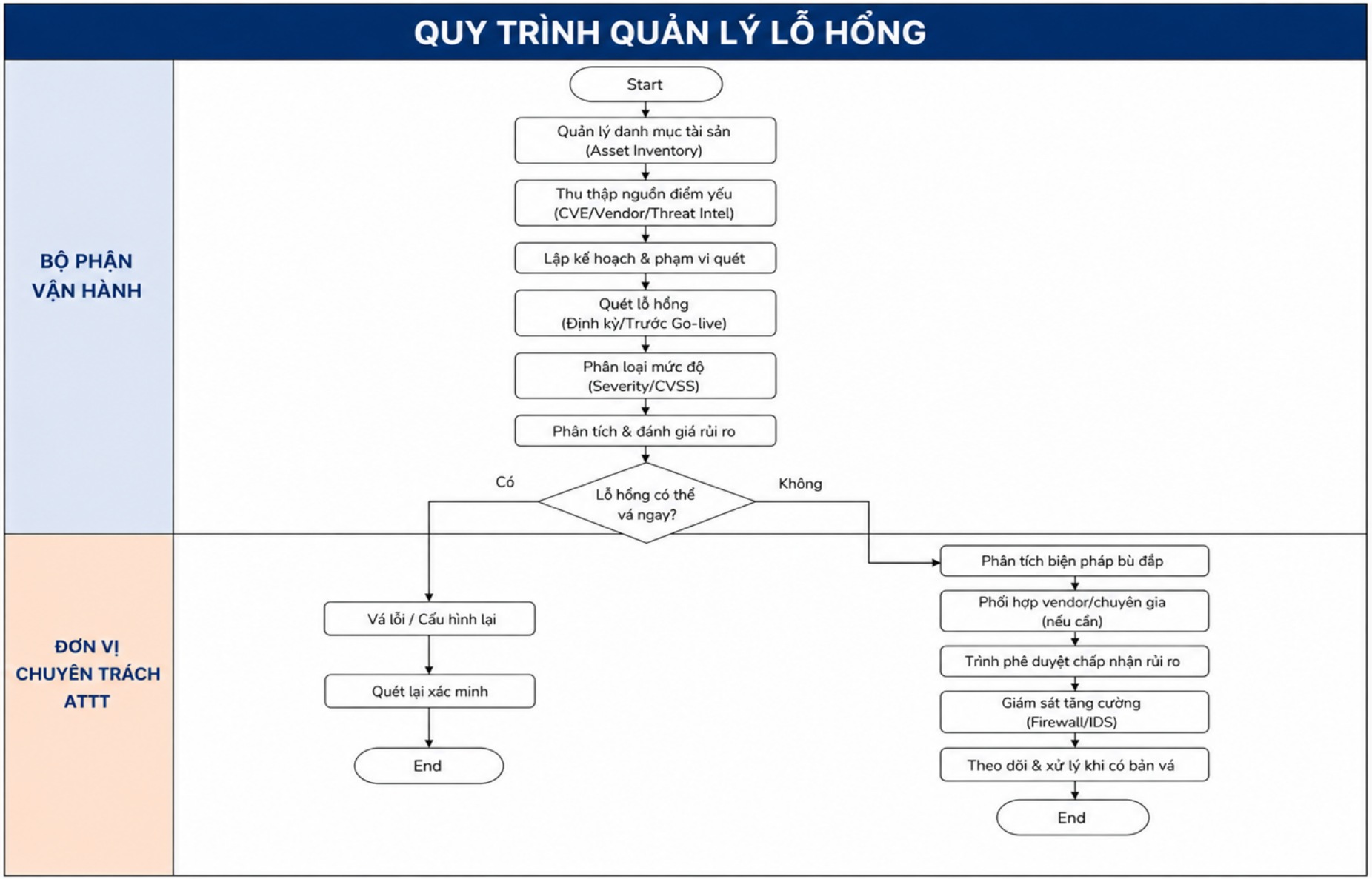
SƠ ĐỒ QUY TRÌNH QUẢN LÝ BẢO ĐẢM AN NINH MẠNG, AN NINH THÔNG TIN MẠNG

(Kèm theo Quyết định số 2933 /QĐ-UBND ngày 17 tháng 09 năm 2026 của Uỷ ban nhân dân tỉnh)

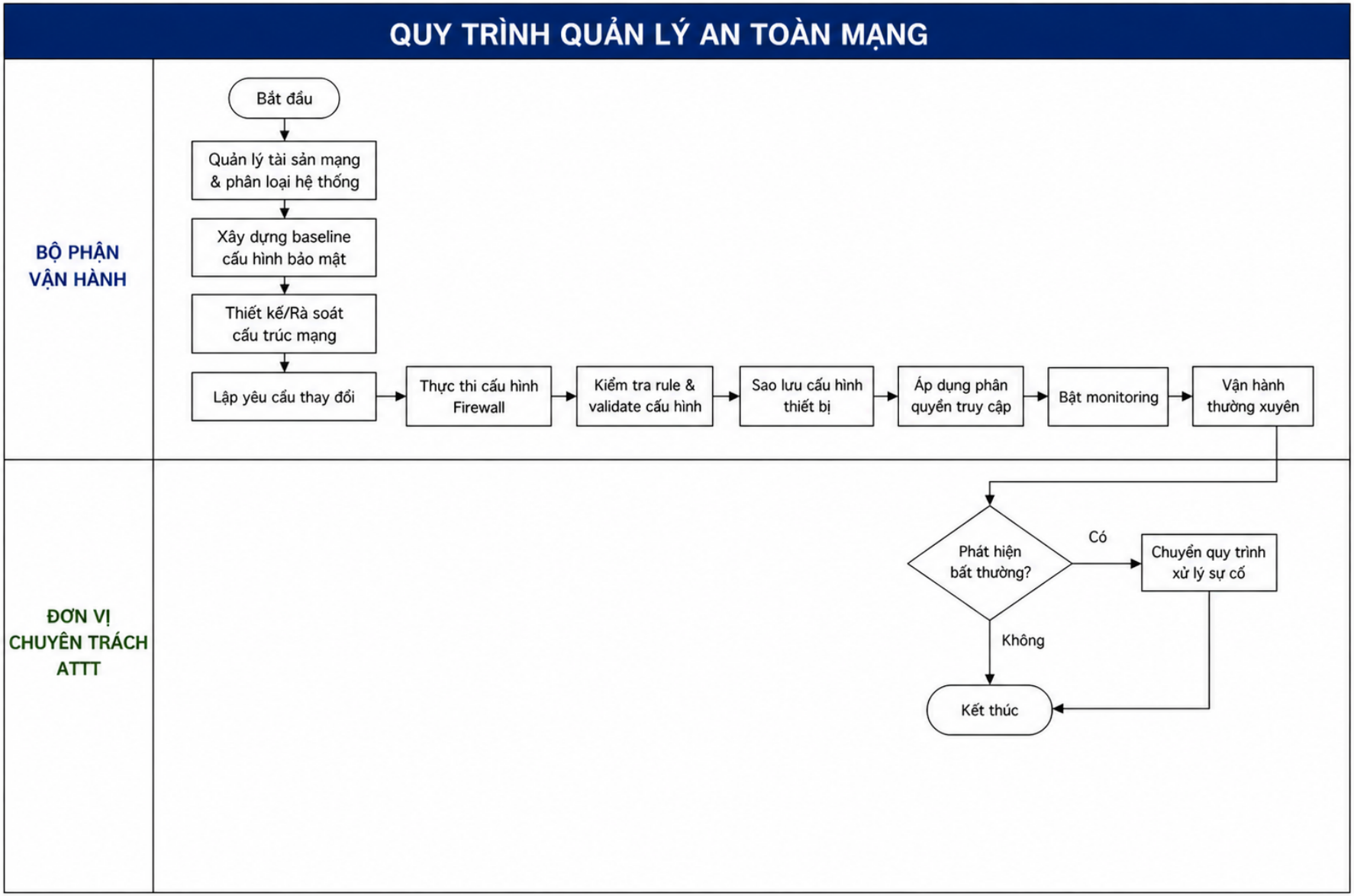
1. Sơ đồ quy trình Xử lý sự cố An ninh mạng



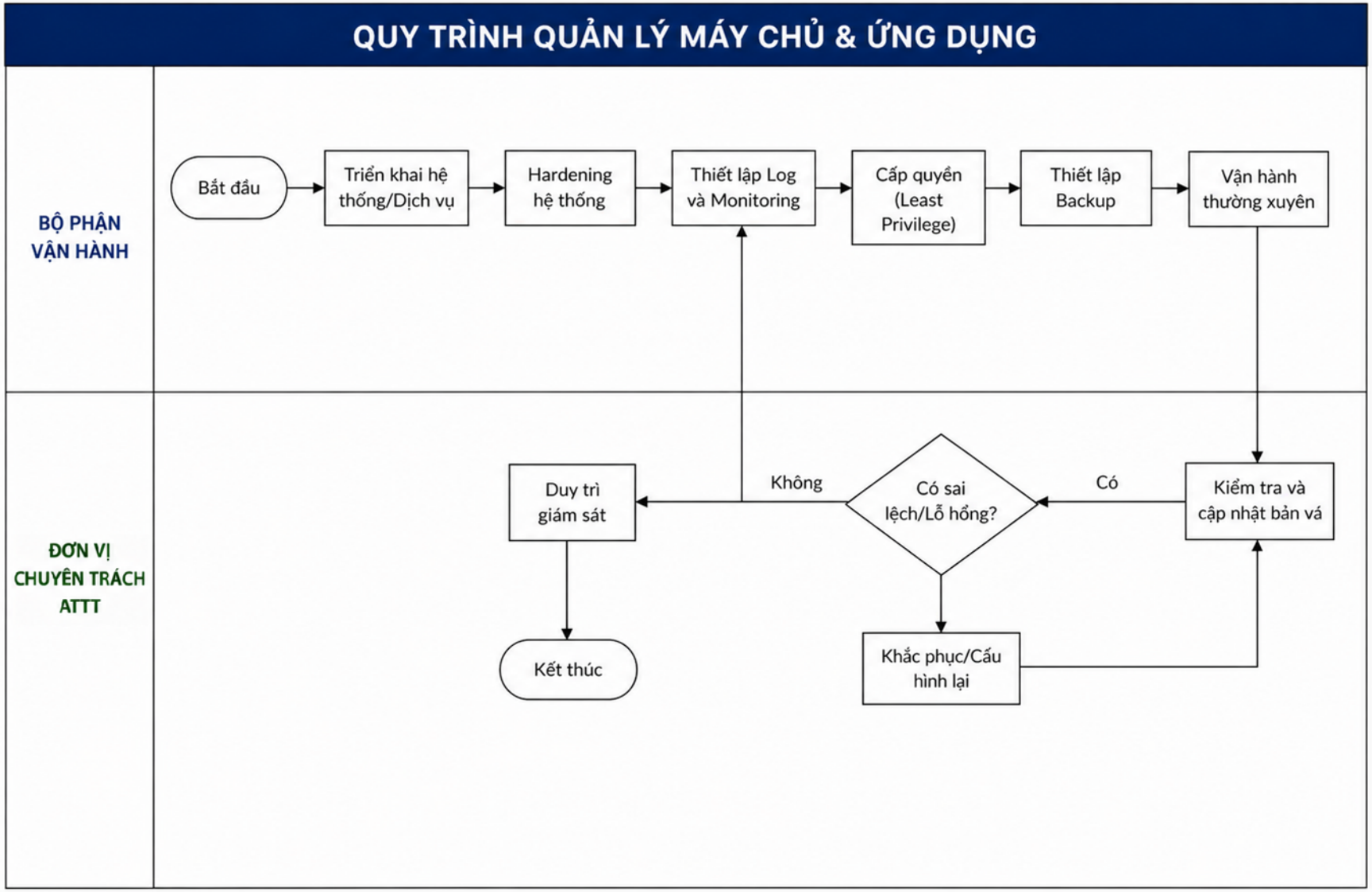
2. Sơ đồ quy trình Quản lý lỗ hổng



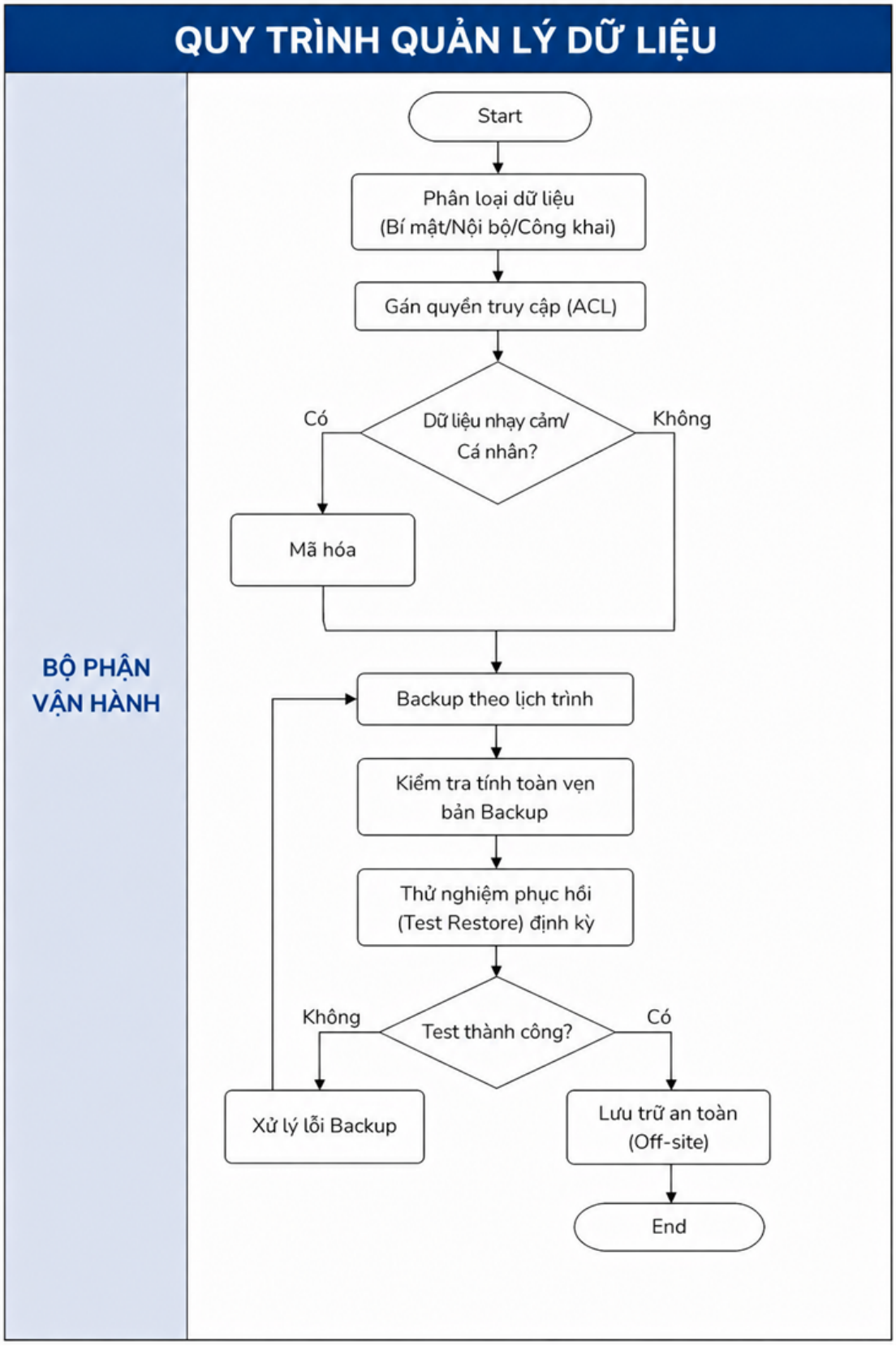
3. Sơ đồ quy trình Quản lý an toàn mạng



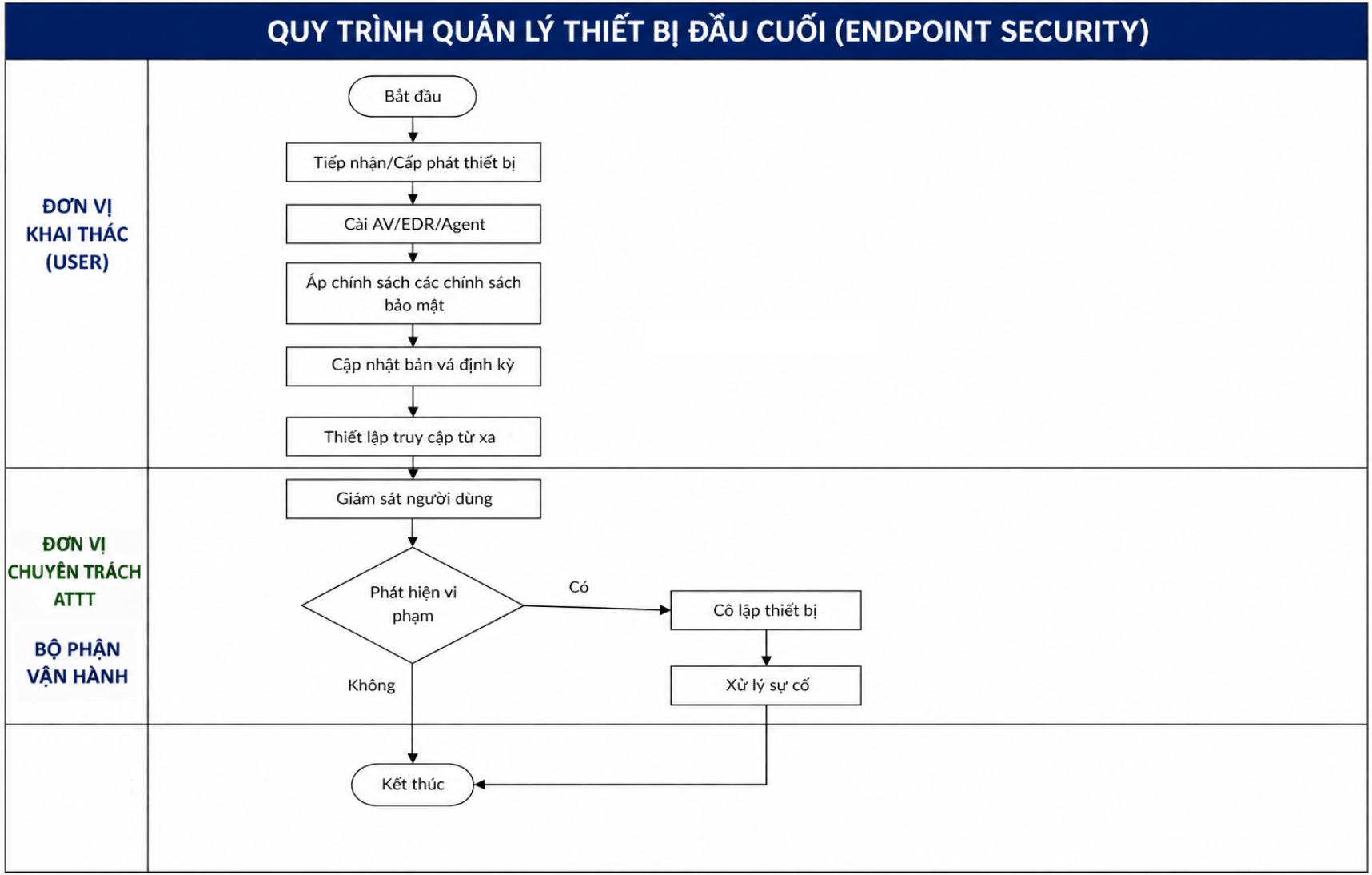
4. Sơ đồ quy trình Quản lý máy chủ và ứng dụng



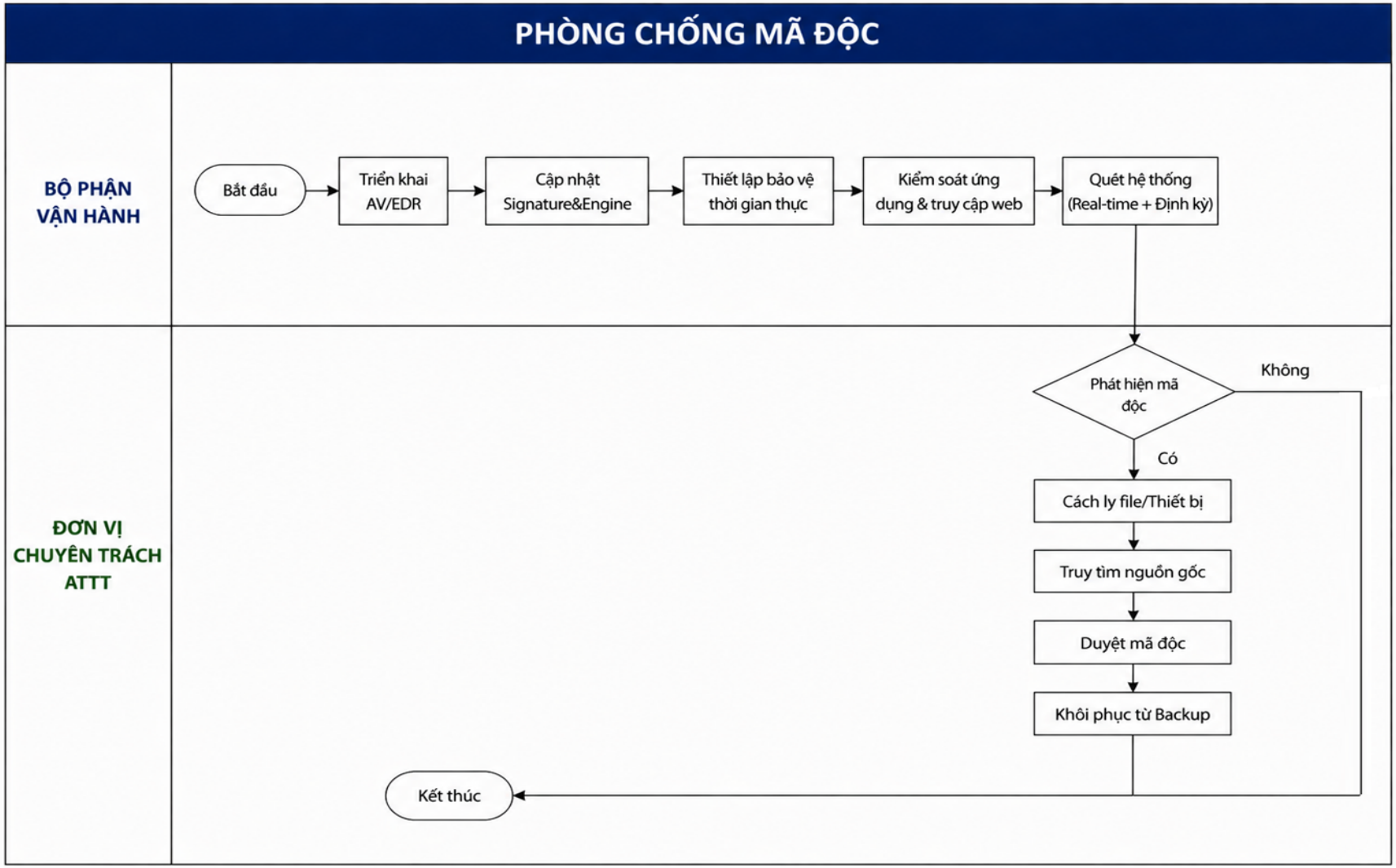
5. Sơ đồ quy trình Quản lý dữ liệu



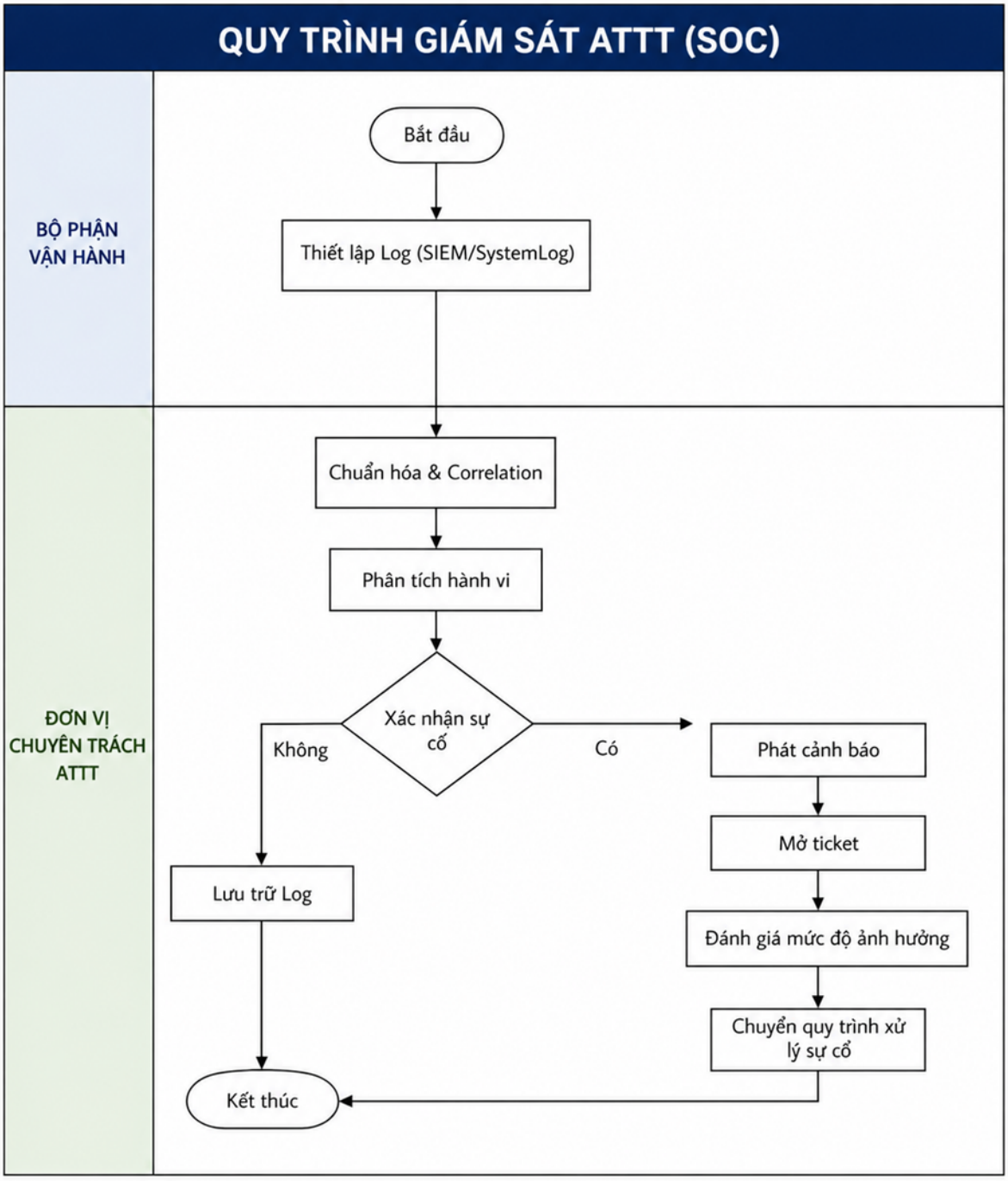
6. Sơ đồ quy trình Quản lý thiết bị đầu cuối (ENDPOINT SECURITY)



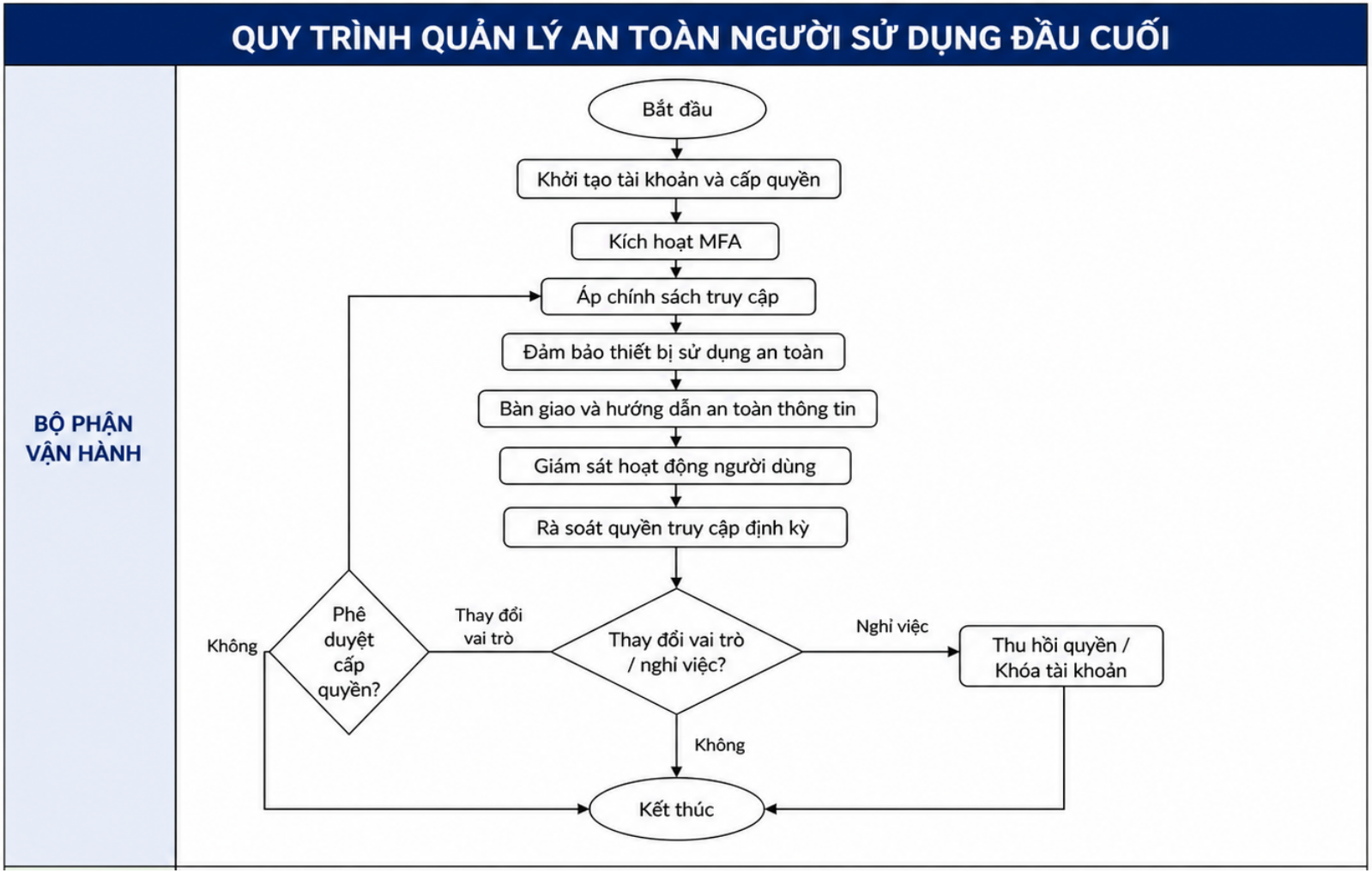
7. Sơ đồ quy trình Phòng chống mã độc



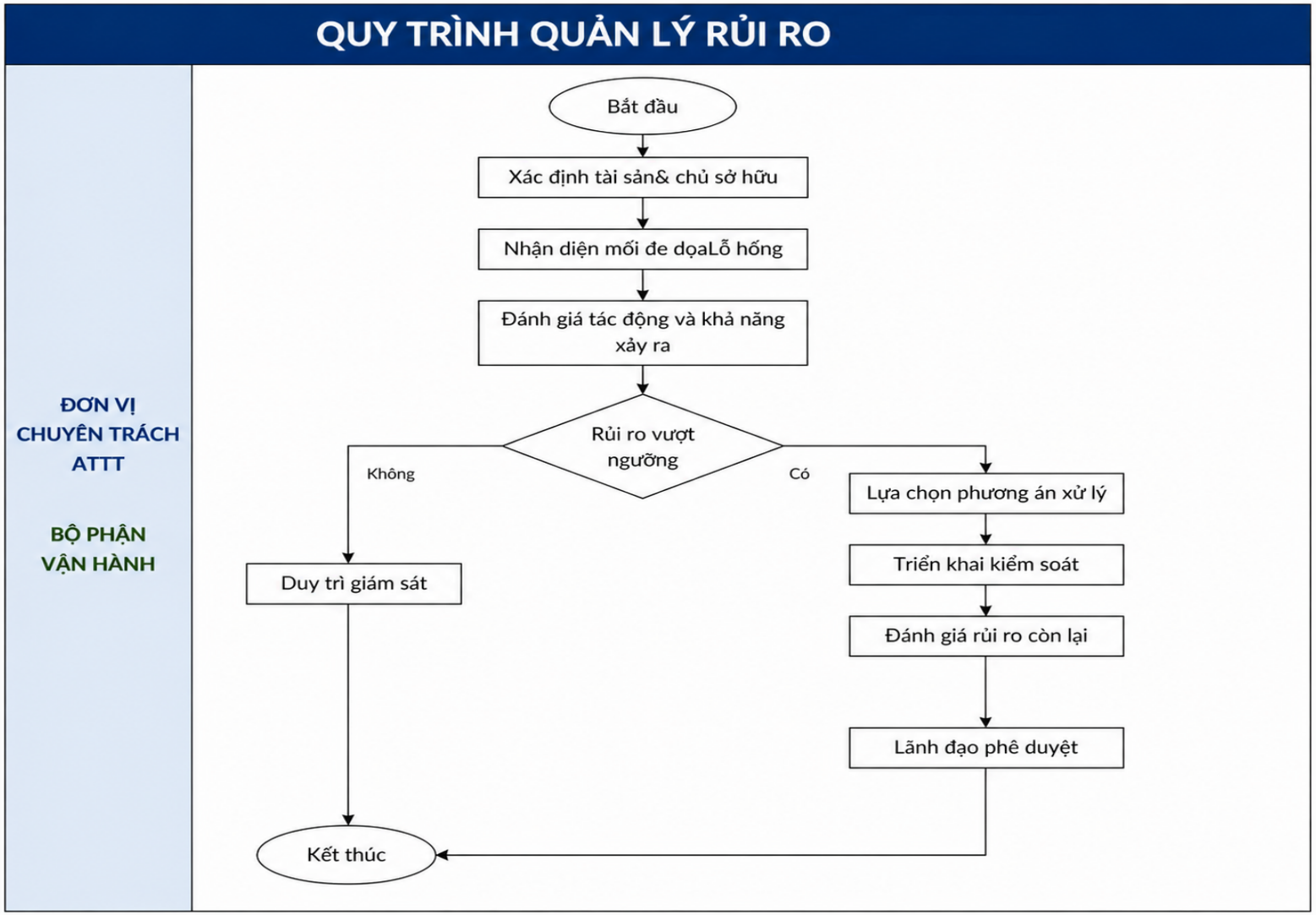
8. Sơ đồ quy trình Giám sát An ninh mạng (SOC)



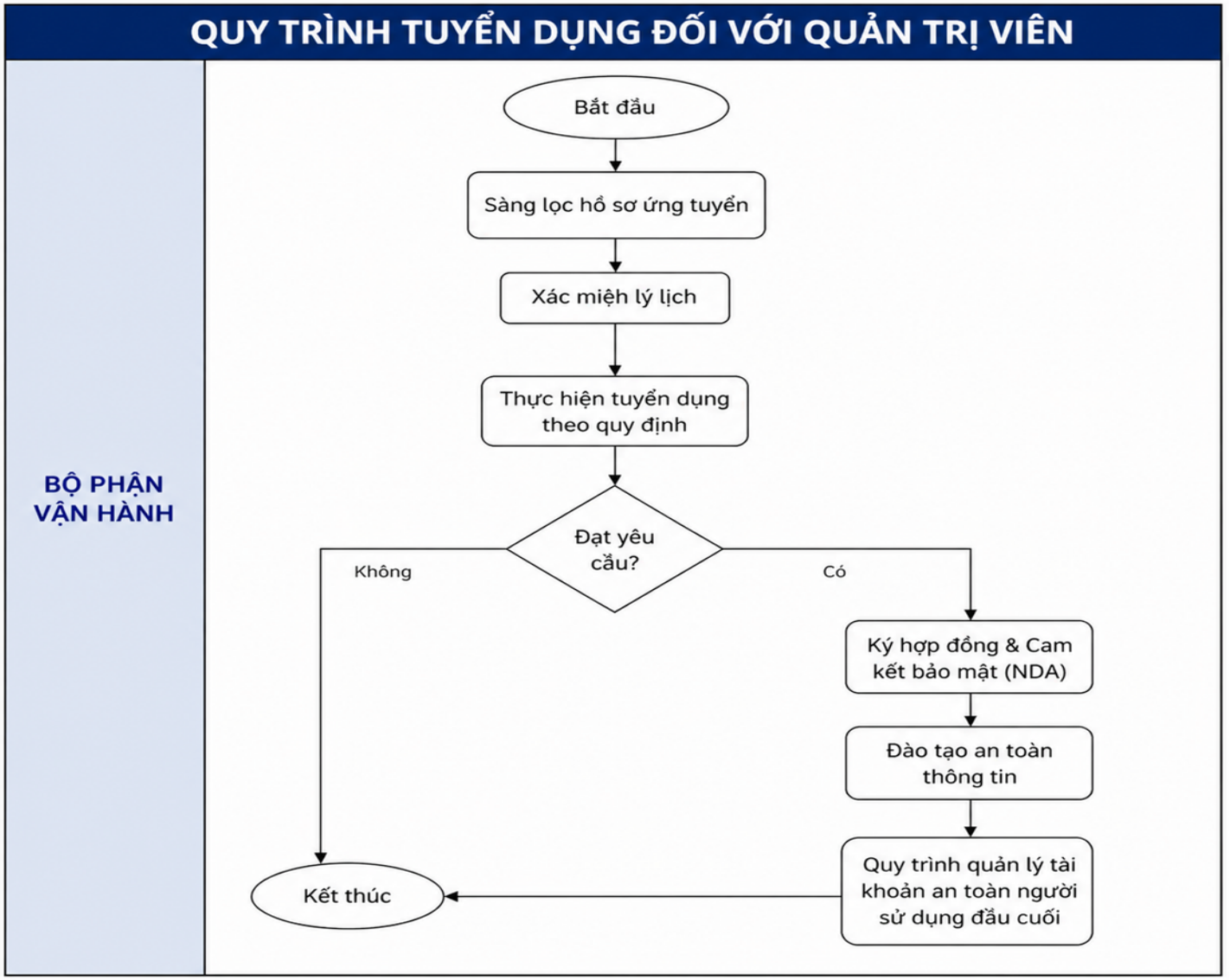
9. Sơ đồ quy trình Quản lý an toàn người sử dụng đầu cuối



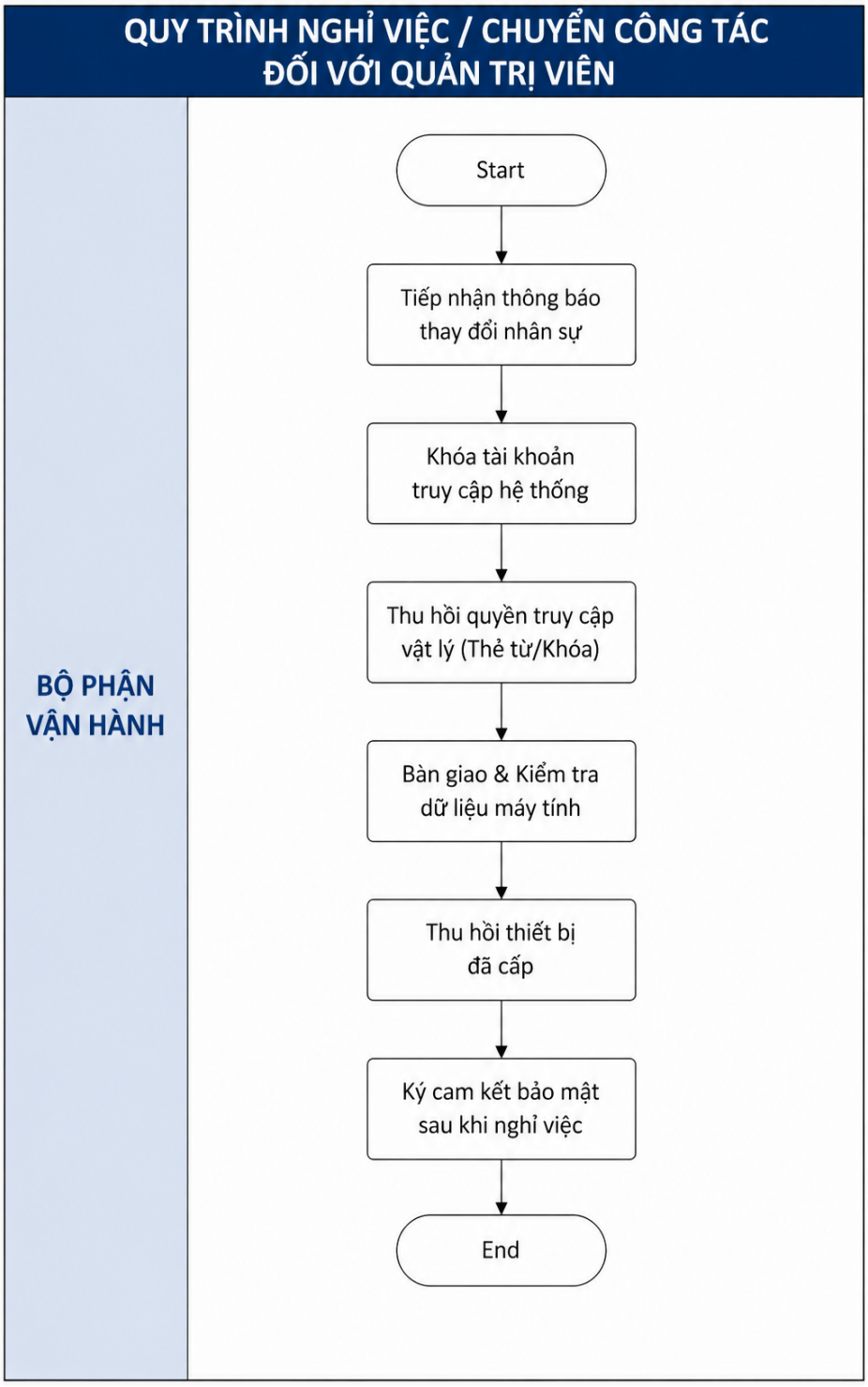
10. Sơ đồ quy trình Quản lý rủi ro



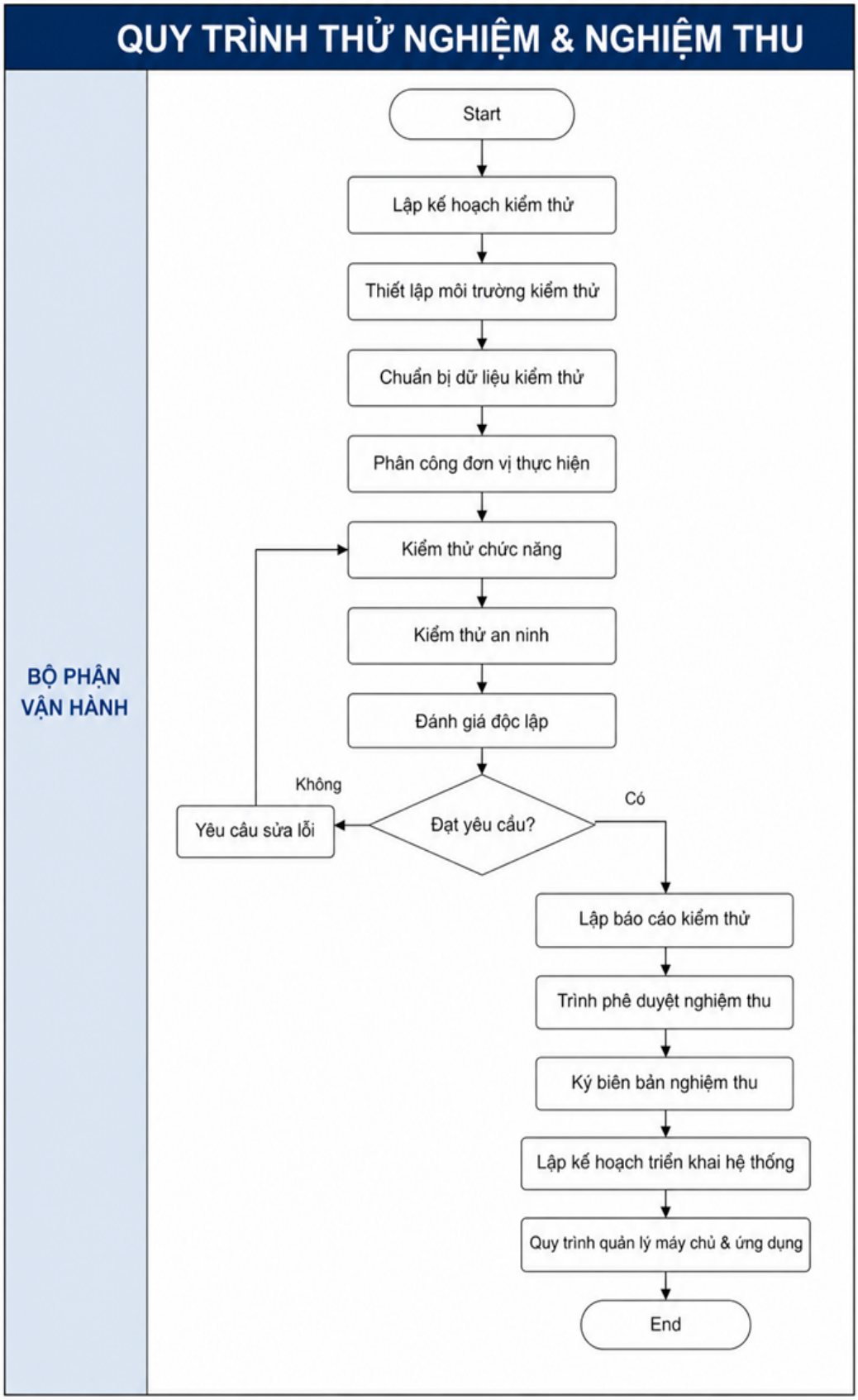
11. Sơ đồ quy trình Tuyển dụng đối với quản trị viên



12. Sơ đồ quy trình Nghỉ việc / Chuyển công tác đối với quản trị viên.



13. Sơ đồ quy trình Thử nghiệm và Nghiệm thu



14. Sơ đồ quy trình Kết thúc/Thanh lý

