Ký bởi: Ủy ban nhân dân tỉnh Lạng Sơn
Cơ quan: Tỉnh Lạng Sơn
Thời gian ký: 14/10/2026 10:55:41

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

QUY CHẾ
Bảo đảm an ninh mạng đối với hệ thống thông tin trên địa bàn tỉnh Lạng Sơn

(Ban hành kèm theo Quyết định số 75/2026/QĐ-UBND ngày 14 tháng 10 năm 2026 của Ủy ban nhân dân tỉnh Lạng Sơn)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định công tác bảo đảm an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh Lạng Sơn và các hệ thống thông tin của cơ quan, đơn vị có kết nối, tích hợp, khai thác, sử dụng hoặc chia sẻ dữ liệu với hệ thống thông tin dùng chung của tỉnh.

2. Đối tượng áp dụng

a) Các sở, ban, ngành; các tổ chức, đơn vị trực thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân xã, phường (sau đây viết tắt là cơ quan, đơn vị). Quy chế này chỉ áp dụng đối với việc kết nối, tích hợp, khai thác, sử dụng, chia sẻ dữ liệu với các hệ thống thông tin dùng chung thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh hoặc hoạt động phối hợp theo quy định của pháp luật. Việc quản lý, vận hành và bảo đảm an ninh mạng đối với hệ thống thông tin nội bộ, hệ thống thông tin chuyên dùng của các cơ quan, tổ chức này thực hiện theo quy định của pháp luật và quy định của cơ quan có thẩm quyền.

b) Cán bộ, công chức, viên chức, người lao động đang làm việc trong các cơ quan, đơn vị quy định tại điểm a khoản này.

c) Các tổ chức, đơn vị, cá nhân tham gia cung cấp dịch vụ công nghệ thông tin, an ninh mạng; quản trị, vận hành, kết nối, tích hợp, khai thác, sử dụng hệ thống thông tin của tỉnh hoặc thực hiện nhiệm vụ có liên quan theo hợp đồng, quyết định giao nhiệm vụ hoặc căn cứ pháp lý khác (sau đây viết tắt là bên cung cấp dịch vụ).

d) Đối với Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân tỉnh, Hội đồng nhân dân cấp xã, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội; các cơ quan Đảng, cơ quan Trung ương và các cơ quan, tổ chức khác không thuộc phạm vi quản lý trực tiếp của Ủy ban nhân dân tỉnh.

Điều 2. Giải thích từ ngữ

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

1. *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.

2. *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.

3. *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.

4. *Trung tâm dữ liệu:* là công trình viễn thông, bao gồm nhà, trạm, hệ thống cáp, hệ thống máy tính và hệ thống điện cùng các thiết bị phụ trợ được lắp đặt vào đó để xử lý, lưu trữ và quản lý dữ liệu của một hoặc nhiều tổ chức, cá nhân. Trung tâm dữ liệu của tỉnh là trung tâm dữ liệu được đầu tư từ nguồn ngân sách nhà nước thực hiện nhiệm vụ quản lý, vận hành các hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

5. *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. Ủy ban nhân dân tỉnh là chủ quản các hệ thống thông tin do Ủy ban nhân dân tỉnh quyết định chủ trương đầu tư sử dụng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

6. *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. Trường hợp thuê dịch vụ công nghệ thông tin, việc xác định đơn vị vận hành thực hiện theo 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 và quyết định giao nhiệm vụ, hợp đồng thuê dịch vụ có liên quan

7. *Vùng mạng nội bộ (LAN - Local Area Network):* là vùng mạng do cơ quan, tổ chức thiết lập, quản lý và sử dụng trong phạm vi nội bộ, cung cấp kết nối mạng cho các máy tính và thiết bị công nghệ thông tin của người sử dụng vào hệ thống.

8. *Mạng LAN độc lập:* là mạng máy tính cục bộ được thiết lập, giới hạn trong một trụ sở cơ quan, tổ chức, không kết nối với mạng Internet, mạng viễn thông, mạng máy tính khác có kết nối ra ngoài trụ sở đó và có biện pháp bảo đảm an ninh, an toàn, phòng, chống kết nối, tấn công, thu thập thông tin trái phép.

9. *Điểm truy nhập Internet công cộng tại cơ quan nhà nước:* là địa điểm mà cơ quan nhà nước cung cấp dịch vụ truy cập Internet cho người dân sử dụng phục vụ giải quyết thủ tục hành chính.

10. *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.

11. *Phần mềm độc hại:* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc 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. *Mật khẩu mạnh:* là một chuỗi có tối thiểu 08 ký tự, bao gồm chữ thường, chữ in hoa, ký tự đặc biệt, chữ số.

13. *Nhật ký (log):* là một tập hợp các bản ghi được tạo ra liên tục bởi một hệ thống, ứng dụng hoặc thiết bị, ghi lại các sự kiện, trạng thái, cảnh báo hoặc lỗi xảy ra trong quá trình hoạt động.

14. *Người sử dụng:* là cán bộ, công chức, viên chức, người lao động của các cơ quan, đơn vị sử dụng máy tính hoặc thiết bị công nghệ thông tin thuộc hệ thống thông tin để xử lý công việc.

Điều 3. Nguyên tắc chung

1. Tuân thủ các nguyên tắc bảo vệ an ninh mạng tại Điều 4 Luật An ninh mạng.

2. Bảo đảm an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình thiết kế, xây dựng, vận hành, nâng cấp cho đến hủy bỏ hệ thống thông tin; là nhiệm vụ trọng yếu, thường xuyên, liên tục, được ưu tiên trong các kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số và phát triển kinh tế - xã hội của tỉnh.

3. Việc bảo đảm an ninh mạng phải được thực hiện trên cơ sở tuân thủ các quy định của pháp luật về an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các quy định khác có liên quan.

4. Thủ trưởng các cơ quan, đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an ninh mạng. Mỗi cán bộ, công chức, viên chức, người lao động tại các cơ quan, đơn vị phải có trách nhiệm chủ động, tự giác áp dụng các biện pháp bảo đảm an ninh mạng.

5. Hệ thống thông tin phải được phân loại, xác định cấp độ và áp dụng biện pháp bảo đảm an ninh mạng phù hợp theo từng cấp độ.

6. Hệ thống thông tin phải được giám sát, cảnh báo an ninh mạng phù hợp với cấp độ, tính chất, quy mô, phạm vi ảnh hưởng của hệ thống; có phương án ứng cứu, khắc phục sự cố, duy trì hoạt động giao dịch bình thường, sẵn sàng cho các tình huống khẩn cấp.

7. Việc ứng cứu sự cố an ninh mạng thực hiện phương châm "4 tại chỗ: chỉ huy tại chỗ, lực lượng tại chỗ, phương tiện tại chỗ và hậu cần tại chỗ". Ứng cứu sự cố trước hết phải được thực hiện bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

8. Công tác bảo đảm an ninh mạng luôn có sự phối hợp chặt chẽ, thống nhất, phân định rõ trách nhiệm các cơ quan, đơn vị dưới sự chỉ đạo, điều phối

của Ủy ban nhân dân tỉnh; Công an tỉnh là cơ quan chủ trì tham mưu, hướng dẫn thực hiện.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm thực hiện theo quy định của Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước, Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu, Luật Giao dịch điện tử, Luật Chuyển đổi số và các quy định khác của pháp luật có liên quan.

2. Tự ý kết nối thiết bị cá nhân, thiết bị mạng, thiết bị phát sóng không dây hoặc thiết bị khác vào mạng nội bộ của cơ quan, đơn vị khi chưa được người có thẩm quyền cho phép

3. Tự ý cài đặt, gỡ bỏ, thay đổi cấu hình phần mềm, thiết bị hoặc dịch vụ công nghệ thông tin thuộc phạm vi quản lý của cơ quan, đơn vị khi chưa được phân quyền hoặc chưa được người có thẩm quyền cho phép.

4. Tự ý sử dụng tài khoản, thiết bị, phần mềm, hệ thống thông tin hoặc tài nguyên công nghệ thông tin của cơ quan, đơn vị không đúng mục đích, phạm vi hoặc quyền sử dụng được giao.

5. Tự ý sao chép, di chuyển dữ liệu, hồ sơ, tài liệu công việc từ hệ thống, thiết bị hoặc môi trường lưu trữ của cơ quan, đơn vị sang thiết bị, tài khoản hoặc dịch vụ lưu trữ khác không thuộc phạm vi được phép sử dụng.

6. Tự ý đưa phần mềm, thiết bị lưu trữ, dữ liệu hoặc tài nguyên từ bên ngoài vào hệ thống, thiết bị công nghệ thông tin của cơ quan, đơn vị không thực hiện theo quy trình kiểm tra, phê duyệt hoặc kiểm soát được quy định.

7. Không thực hiện hoặc cố ý bỏ qua các yêu cầu, quy trình kiểm soát, sao lưu, cập nhật, kiểm tra và báo cáo về an toàn thông tin theo quy định nội bộ của cơ quan, đơn vị khi đã được giao trách nhiệm thực hiện.

Điều 5. Xây dựng quy định bảo đảm an ninh mạng

1. Các cơ quan, đơn vị phải xây dựng quy định bảo đảm an ninh mạng phù hợp với hệ thống thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của cơ quan, đơn vị mình. Quy định bảo đảm an ninh mạng được lãnh đạo có thẩm quyền ký ban hành và triển khai thực hiện trong toàn cơ quan, đơn vị.

2. Quy định bảo đảm an ninh mạng cần đáp ứng các yêu cầu an ninh mạng tương ứng với từng cấp độ của hệ thống thông tin và tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng.

3. Quy định bảo đảm an ninh mạng thường xuyên được rà soát, sửa đổi, bổ sung nhằm bảo đảm sự đầy đủ, phù hợp với các quy định của pháp luật hiện hành về bảo đảm an ninh mạng.

Chương II

BẢO ĐẢM AN NINH MẠNG

Mục 1

QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 6. Tài sản công nghệ thông tin

1. Tài sản công nghệ thông tin, bao gồm:

a) Tài sản phần cứng: Thiết bị công nghệ thông tin, vật mang tin và các thiết bị phục vụ cho hoạt động của hệ thống thông tin, như: máy chủ, máy tính, thiết bị lưu trữ (USB, Ổ cứng, CD/DVD, băng từ...); thiết bị mạng và bảo mật (bộ định tuyến (Router), bộ chuyển mạch (Switch), tường lửa vật lý (Firewall), thiết bị cân bằng tải,...); thiết bị ngoại vi (máy in, máy quét,...); hệ thống cáp mạng; thiết bị cung cấp nguồn điện;...

b) Tài sản phần mềm: Phần mềm hệ thống, phần mềm ứng dụng, phần mềm tiện ích, hệ quản trị cơ sở dữ liệu, mã nguồn và công cụ phát triển phần mềm.

c) Tài sản thông tin: Dữ liệu, thông tin ở dạng số được tạo lập, thu thập, xử lý, lưu trữ, truyền đưa thông qua hệ thống thông tin.

d) Các thành phần liên quan khác.

2. Tài sản công nghệ thông tin phải được lập danh sách, phân loại và quản lý gắn với từng hệ thống thông tin.

Điều 7. Quản lý tài sản phần cứng

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị phải lập danh sách tài sản phần cứng gồm các thông tin cơ bản sau: Tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, vị trí lắp đặt, chủ thể quản lý, mục đích sử dụng, hệ thống thông tin tương ứng, tình trạng sử dụng, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có). Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần cứng định kỳ tối thiểu 06 tháng 1 lần.

2. Tài sản phần cứng phải được giao, gắn trách nhiệm cho bộ phận hoặc cá nhân quản lý, sử dụng; được định kỳ bảo trì, bảo dưỡng; được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

3. Tài sản phần cứng thuộc hệ thống thông tin phải được kiểm tra, đánh giá an ninh mạng trước khi đưa vào sử dụng; bảo đảm về nguồn điện dự phòng, chống quá tải, sụt giảm điện áp, chống sét lan truyền và có hệ thống tiếp địa trong quá trình sử dụng.

4. Thông tin, dữ liệu lưu trữ trong tài sản phần cứng khi thanh lý, thay đổi mục đích sử dụng được tiêu hủy về mặt vật lý hoặc được xóa dữ liệu an toàn bảo đảm không có khả năng phục hồi. Trường hợp không thực hiện xóa, ghi đè dữ liệu, thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

5. Không tự ý sửa chữa tài sản phần cứng ở các cơ sở, dịch vụ ngoài cơ quan, đơn vị. Trường hợp cấp bách phải sửa chữa ở các cơ sở bên ngoài, thì phải được sự đồng ý, phê duyệt của Thủ trưởng cơ quan, đơn vị đồng thời có biện pháp xóa dữ liệu an toàn hoặc lưu giữ lại bộ phận lưu trữ dữ liệu trước khi thực hiện sửa chữa. Trong quá trình sửa chữa, bảo trì hệ thống, thiết bị công nghệ thông tin do bên thứ ba thực hiện, đơn vị chủ quản, vận hành hệ thống thông tin phải cử bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng giám sát và ghi nhật ký đầy đủ.

Điều 8. Quản lý tài sản phần mềm

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị lập danh sách tài sản phần mềm với các thông tin cơ bản gồm: tên tài sản, mục đích, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin tương ứng, tình trạng sử dụng. Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 06 tháng 1 lần.

2. Tài sản phần mềm phải được giao trách nhiệm cho bộ phận hoặc cá nhân quản lý, sử dụng; việc cài đặt, cấu hình, cập nhật, gia hạn bản quyền chỉ thực hiện bởi bộ phận hoặc người được giao nhiệm vụ theo quy định của cơ quan, đơn vị.

3. Cơ quan, đơn vị định kỳ rà soát, cập nhật, khắc phục các điểm yếu, lỗ hổng bảo mật có nguy cơ gây mất an ninh mạng.

Điều 9. Quản lý tài sản thông tin

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị phải lập danh sách tài sản thông tin với các thông tin cơ bản gồm: tên tài sản, mức độ tiếp cận, chủ thể quản lý, phạm vi truy cập thông tin, thời gian lưu trữ, hệ thống thông tin tương ứng. Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi trong cơ quan, đơn vị ảnh hưởng đến danh sách.

2. Thông tin được phân loại theo mức độ tiếp cận và có thể gắn thuộc tính đặc thù, cụ thể:

a) Thông tin phân loại theo mức độ công khai là thông tin được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó.

b) Thông tin phân loại theo mức độ nội bộ là thông tin được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể.

c) Thông tin phân loại theo mức độ cá nhân là thông tin gắn với việc xác định danh tính một người cụ thể.

d) Thông tin phân loại theo mức độ bí mật nhà nước được quy định tại Luật Bảo vệ bí mật nhà nước.

3. Tài sản thông tin thuộc danh mục bí mật nhà nước phải tuân thủ các quy định của Luật Bảo vệ bí mật nhà nước và các quy định khác có liên quan đến quá trình tạo lập, lưu trữ, trao đổi và tiêu hủy.

Mục 2

XÂY DỰNG, QUẢN LÝ, VẬN HÀNH, HỦY BỎ HỆ THỐNG THÔNG TIN

Điều 10. Yêu cầu khi xây dựng các hệ thống thông tin

1. Khi xây dựng mới hoặc nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin phải tổ chức xác định cấp độ, lập, thẩm định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Chương III 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.

2. Khi triển khai các sản phẩm bảo đảm an ninh mạng trong các hệ thống thông tin phải đáp ứng theo các tiêu chuẩn, quy chuẩn Việt Nam và các hướng dẫn về an ninh mạng của Bộ Công an, Công an tỉnh. Ưu tiên sử dụng sản phẩm, giải pháp và dịch vụ về an ninh mạng của các đơn vị, tổ chức trong nước.

Điều 11. Yêu cầu quản lý, vận hành, hủy bỏ hệ thống thông tin

1. Cơ quan, đơn vị quản lý, vận hành hệ thống thông tin thực hiện quản lý, vận hành, sử dụng hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật, yêu cầu kỹ thuật, quy định về bảo đảm an toàn thông tin, an ninh mạng và hướng dẫn của cơ quan có thẩm quyền; bảo đảm hệ thống thông tin hoạt động ổn định, an toàn, đáp ứng yêu cầu quản lý, khai thác và sử dụng theo chức năng, nhiệm vụ được giao.

2. Cơ quan, đơn vị quản lý, vận hành hệ thống thông tin tổ chức kiểm tra, theo dõi tình trạng hoạt động của hệ thống thông tin và kịp thời xử lý hoặc báo cáo cơ quan có thẩm quyền xử lý các vấn đề phát sinh theo quy định.

3. Cơ quan, đơn vị quản lý, vận hành hệ thống thông tin căn cứ chức năng, nhiệm vụ, phạm vi quản lý và yêu cầu thực tế để tổ chức theo dõi, đánh giá tình hình hoạt động, nhu cầu nâng cấp, mở rộng hệ thống; việc xây dựng, ban hành hoặc áp dụng tiêu chuẩn, quy chuẩn, yêu cầu kỹ thuật thực hiện theo thẩm quyền và theo quy định, hướng dẫn của cơ quan có thẩm quyền.

4. Khi phát hiện sự cố hoặc nguy cơ mất an toàn thông tin, cơ quan, đơn vị quản lý, vận hành hệ thống thông tin thực hiện các biện pháp xử lý theo quy trình, phương án và hướng dẫn đã được cơ quan có thẩm quyền phê duyệt hoặc ban hành; trường hợp vượt quá khả năng, phạm vi hoặc thẩm quyền xử lý thì kịp thời báo cáo, đề nghị cơ quan có thẩm quyền phối hợp, hướng dẫn hoặc xử lý theo quy định

5. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin.

a) Các cơ quan, đơn vị phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo

đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận, lưu giữ và bảo vệ nhằm phục vụ công tác phân tích, kiểm tra, điều tra, giám sát an ninh mạng.

b) Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

c) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó, đồng thời, kết nối, chia sẻ nhật ký về Trung tâm An ninh mạng tỉnh (nếu có) để giám sát.

6. Hủy bỏ hệ thống thông tin do chủ quản hệ thống thông tin quyết định bằng văn bản và thông báo đến các tổ chức, cá nhân liên quan và đơn vị chuyên trách an ninh mạng của tỉnh. Quá trình hủy bỏ thực hiện theo phương án bảo đảm an ninh mạng đã được phê duyệt; trước khi hủy bỏ, phải sao lưu toàn bộ dữ liệu, cấu hình và nhật ký để phục vụ công tác tra cứu, lưu trữ và quản lý tài sản công nghệ thông tin của hệ thống theo quy định của pháp luật.

Điều 12. Quản lý thuê dịch vụ công nghệ thông tin

1. Xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu, dữ liệu cá nhân và xử lý vi phạm, trách nhiệm bồi thường, khắc phục thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra trước khi ký kết hợp đồng thuê.

2. Trách nhiệm của cơ quan, đơn vị chủ trì trong quá trình thuê dịch vụ công nghệ thông tin.

a) Phải tuân thủ quy định pháp luật về đầu tư công, quản lý tài sản, tài chính công; lựa chọn nhà thầu, nhà cung cấp dịch vụ có năng lực, pháp nhân được cơ quan có thẩm quyền cấp phép hoạt động.

b) Quản lý chặt chẽ thông tin, dữ liệu phát sinh từ dịch vụ thuê, chỉ cho phép truy cập trong phạm vi cần thiết để thực hiện hợp đồng; theo quyền tối thiểu, đúng mục đích, thời hạn, tài khoản được phê duyệt; có xác thực, giám sát và ghi nhật ký.

c) 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 ninh mạng theo quy định tại Quy chế này và các quy định khác có liên quan.

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

đ) Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an ninh mạng phải tạm dừng quyền truy cập; tạm dừng phần dịch vụ có liên quan theo hợp đồng và thẩm quyền; bảo toàn hệ thống, dữ liệu, chứng cứ; thông báo cho cơ quan có thẩm quyền khi có dấu hiệu vi phạm để phối hợp xử lý vi phạm theo quy định pháp luật; thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ; 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, khắc phục thiệt hại.

e) Phối hợp với bên cung cấp dịch vụ trong việc lập, hoàn thiện hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định; yêu cầu bên cung cấp dịch vụ cung cấp đầy đủ tài liệu thiết kế, cấu hình, phương án kỹ thuật được quy định tại 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.

g) Yêu cầu bên cung cấp dịch vụ phải đảm bảo khả năng kết nối, mở rộng, chia sẻ dữ liệu với các hệ thống thông tin dùng chung của tỉnh; tuân thủ Khung kiến trúc Chính phủ số Việt Nam; Khung kiến trúc Chính quyền điện tử hướng đến Chính quyền số tỉnh Lạng Sơn, Khung kiến trúc số tỉnh Lạng Sơn.

3. Trách nhiệm của cơ quan, đơn vị chủ trì thuê khi kết thúc hợp đồng sử dụng dịch vụ công nghệ thông tin

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản công nghệ thông tin 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 bàn giao dữ liệu, cấu hình, tài liệu, tài khoản, khóa, công cụ thuộc phạm vi hợp đồng để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ; mã nguồn chỉ bàn giao khi hợp đồng/quyền sở hữu/ quyền sử dụng hoặc pháp luật có quy định

4. Có phương án hợp đồng chặt chẽ với bên cung cấp dịch vụ và có cơ chế quản lý đối với các tài khoản thuộc các hệ thống thuê dịch vụ hạ tầng của bên cung cấp dịch vụ, tránh tình trạng ủy quyền toàn bộ việc quản trị, vận hành hệ thống cho bên cung cấp dịch vụ liên quan đến khai thác, sử dụng cơ sở dữ liệu hệ thống.

5. Khi có thay đổi lớn về chức năng, phạm vi, kiến trúc, công nghệ, hệ thống, ứng dụng, mã nguồn hoặc cấu hình có khả năng ảnh hưởng đến an ninh mạng, bên cung cấp dịch vụ phải thông báo kịp thời cho chủ quản hệ thống thông tin, đơn vị chủ trì thuê dịch vụ và đơn vị vận hành để đánh giá, xử lý theo hợp đồng và quy định của pháp luật. Trường hợp thuộc diện phải kiểm tra, đánh giá an ninh mạng, việc kiểm tra, đánh giá thực hiện theo quyết định hoặc yêu cầu của cơ quan có thẩm quyền. Công an tỉnh thực hiện tham mưu, phối hợp theo chức năng, nhiệm vụ và thẩm quyền.

Điều 13. Quản lý Trung tâm dữ liệu/Phòng máy chủ

1. Các thiết bị tường lửa, máy chủ, hệ thống lưu trữ phải được đặt trong Trung tâm dữ liệu/Phòng máy chủ và thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập vật lý phù hợp.

2. Máy chủ phải được cài đặt phần mềm phòng chống mã độc và quản lý thống nhất, tập trung. Nhật ký hoạt động của thiết bị, phần mềm bảo đảm thời gian lưu giữ theo đúng cấp độ an toàn của hệ thống thông tin.

3. Mang thiết bị vào, ra Trung tâm dữ liệu/Phòng máy chủ để lắp đặt, sửa chữa hoặc tác động vật lý, kết nối, kiểm tra tín hiệu phải có sự chấp thuận của thủ trưởng cơ quan, đơn vị quản lý, vận hành và phải có cán bộ, nhân viên có trách nhiệm kiểm soát, ghi nhật ký, lập biên bản (nếu cần).

Điều 14. Quản lý Hệ thống mạng máy tính

1. Hệ thống mạng máy tính phải được thiết kế phân vùng theo chức năng và mức độ an ninh phù hợp với từng cấp độ an ninh mạng của hệ thống thông tin theo TCVN 14423:2026 - An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản. Dữ liệu trao đổi giữa các vùng mạng phải được kiểm soát chặt chẽ bởi thiết bị tường lửa và các thiết bị bảo mật khác.

2. Hệ thống mạng máy tính kết nối Internet phải có hệ thống tường lửa, hệ thống bảo vệ truy cập Internet, và có khả năng bảo vệ trước các loại tấn công từ chối dịch vụ (DDoS); thực hiện lọc bỏ, ngăn chặn truy cập các trang tin được xác định là chứa mã độc hoặc nội dung không phù hợp.

3. Truy cập từ xa vào vùng mạng nội bộ phải thông qua kết nối mạng riêng ảo (VPN) được mã hóa, có kiểm soát và áp dụng hình thức xác thực đa yếu tố (MFA).

4. Kết nối không dây (Wi-Fi) phải sử dụng chế độ xác thực mạnh (như WPA2- Enterprise) hoặc mật khẩu mạnh, thay đổi định kỳ. Đối với vùng mạng nội bộ phải thực hiện quản lý thiết bị kết nối Wi-Fi theo địa chỉ phần cứng MAC của thiết bị.

5. Điểm truy nhập Internet công cộng tại cơ quan nhà nước phải niêm yết công khai nội quy sử dụng dịch vụ Internet ở nơi dễ nhận biết; thiết lập thành vùng mạng riêng biệt, không kết nối vùng mạng nội bộ chứa dữ liệu chuyên môn; thiết lập mật khẩu mạnh, khuyến khích sử dụng cổng xác thực (Captive Portal) yêu cầu người dùng chấp nhận nội quy sử dụng trước khi truy cập Internet qua Wi-Fi.

6. Mạng truyền số liệu chuyên dùng trên địa bàn tỉnh được triển khai, quản lý, vận hành và sử dụng phải tuân thủ các quy định của Thủ tướng Chính phủ và hướng dẫn của Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ. Chỉ được sử dụng cho mục đích công vụ, không được kết nối trực tiếp ra Internet.

Điều 15. Quản lý, sử dụng máy tính, thiết bị ngoại vi và phần mềm

1. Máy tính và các thiết bị ngoại vi tại các cơ quan, đơn vị phải được cài đặt hệ điều hành, phần mềm ứng dụng có bản quyền hoặc sử dụng phần mềm mã nguồn mở hợp pháp được trang cấp theo quy định.

2. Chỉ cài đặt các phần mềm có bản quyền nằm trong danh mục được phép sử dụng do cơ quan có thẩm quyền ban hành. Nghiêm cấm việc tự ý cài đặt các phần mềm không rõ nguồn gốc, phần mềm bẻ khóa, các phần mềm không phục vụ công tác chuyên môn hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị.

3. Tất cả các máy tính phải được cài đặt phần mềm phòng, chống mã độc và được thiết lập chế độ cập nhật tự động cơ sở dữ liệu nhận dạng mã độc, bản vá cho hệ điều hành và phần mềm. Người sử dụng có trách nhiệm thường xuyên rà quét mã độc đối với máy tính và các thiết bị lưu trữ di động (USB, Ổ cứng ngoài) trước khi sử dụng. Đối với thiết bị xử lý bí mật nhà nước hoặc thiết bị hoạt động trong mạng độc lập, việc cập nhật được thực hiện theo quy định chuyên ngành.

4. Khi phát hiện máy tính có dấu hiệu bất thường (hoạt động chậm, tự động mở các cửa sổ lạ, mất dữ liệu, nhận được cảnh báo từ phần mềm phòng, chống mã độc), người sử dụng phải ngay lập tức ngắt kết nối mạng của máy tính đó và báo cáo cho bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị để được hỗ trợ, xử lý kịp thời.

5. Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; không truy nhập, mở các trang tin, tệp đính kèm hoặc liên kết trong thư điện tử không rõ nguồn gốc, có dấu hiệu đáng ngờ; thực hiện quét mã độc của tệp đính kèm tải về trước khi mở ra xem; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

6. Khi bàn giao, tiếp nhận quản lý, sử dụng máy tính, thiết bị ngoại vi, phần mềm phải được cán bộ, công chức lập biên bản hoặc ghi sổ theo dõi và được lãnh đạo có thẩm quyền ký xác nhận, lưu trữ theo quy định.

7. Người sử dụng phải khóa màn hình máy tính (sử dụng tính năng có sẵn của hệ điều hành) khi rời khỏi vị trí làm việc và tắt hoàn toàn máy tính khi hết giờ làm việc.

Điều 16. Quản lý, sử dụng chữ ký số, chứng thư chữ ký số chuyên dùng công vụ

1. Việc cung cấp, quản lý và sử dụng chữ ký số, chứng thư chữ ký số chuyên dùng công vụ trong cơ quan nhà nước thực hiện theo Nghị định số 68/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về chữ ký số chuyên dùng công vụ và pháp luật có liên quan.

2. Cá nhân được cấp chữ ký số, chứng thư chữ ký số chuyên dùng công vụ chịu trách nhiệm quản lý, bảo vệ an ninh, bí mật khóa bí mật và thiết bị lưu khóa bí mật.

3. Nghiêm cấm việc cho người khác mượn thiết bị lưu khóa bí mật hoặc sử dụng chữ ký số được cấp vào các mục đích cá nhân, không phục vụ công vụ.

4. Tổ chức, cá nhân được cấp chứng thư chữ ký số chuyên dùng công vụ thực hiện nghiêm túc trách nhiệm của thuê bao quy định tại Điều 39 Nghị định số 68/2024/NĐ-CP ngày 25/6/2024 của Chính phủ quy định về chữ ký số chuyên dùng công vụ.

Điều 17. Quản lý tài khoản và quyền truy cập tài khoản của người dùng

1. Mỗi cá nhân, đơn vị được cấp một tài khoản định danh duy nhất từ Hệ thống định danh và xác thực tập trung của tỉnh để truy cập các hệ thống thông tin dùng chung của tỉnh.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được giao cho một người quản lý, sử dụng và chịu trách nhiệm chính về bảo mật tài khoản, thông tin xác thực và hoạt động truy cập tài khoản. Việc sử dụng chung tài khoản bị nghiêm cấm.

3. Mỗi người sử dụng chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Tài khoản người dùng phải đặt mật khẩu mạnh và thay đổi định kỳ tối thiểu 90 ngày/lần. Hệ thống có cơ chế xác thực người dùng; bắt buộc người dùng thay đổi mật khẩu ngay trong lần đăng nhập đầu tiên; tự động khóa tài khoản tạm thời sau 05 lần đăng nhập sai liên tiếp.

5. Tài khoản quản trị, vận hành hệ thống phải tách biệt với tài khoản truy cập của người sử dụng thông thường, được giao đích danh cá nhân làm công tác quản trị và phải đặt mật khẩu mạnh tối thiểu 14 ký tự. Hệ thống có cơ chế xác thực 02 yếu tố; thay đổi mật khẩu định kỳ tối thiểu 90 ngày/lần; tự động khóa tài khoản tạm thời sau 05 lần đăng nhập sai liên tiếp; hiển thị lịch sử đăng nhập thành công của mỗi tài khoản và thông báo về tài khoản quản trị.

6. Đơn vị quản lý, vận hành hệ thống thông tin có quyền khóa tài khoản truy cập trong trường hợp khi không tuân thủ các quy định về an ninh mạng hoặc phát hiện tài khoản đó có hành vi tấn công mạng hoặc gây mất an ninh mạng.

7. Căn cứ vị trí công việc, phạm vi tiếp cận và mức độ quan trọng của thông tin, dữ liệu hoặc hệ thống thông tin, cơ quan, đơn vị xác định biện pháp cam kết bảo mật phù hợp đối với cá nhân được giao nhiệm vụ. Cam kết có thể được thể hiện bằng văn bản riêng hoặc tích hợp trong hợp đồng làm việc, hợp đồng lao động, quyết định giao nhiệm vụ hoặc quy định nội bộ. Phụ lục 07 kèm theo Quy chế này là mẫu tham khảo, không phải thành phần hồ sơ bắt buộc.

Điều 18. Bảo đảm an ninh dữ liệu, sao lưu dự phòng và khôi phục

1. Cơ quan, đơn vị xây dựng và tổ chức thực hiện chính sách/quy trình quản lý dữ liệu (phân loại dữ liệu, phân quyền truy cập, lưu trữ, sao lưu, khôi phục, tiêu hủy), bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng, trong đó tối thiểu bao gồm: kiểm soát truy cập, ghi nhật ký, mã hóa phù hợp đối với dữ liệu quan trọng/nhạy cảm khi lưu trữ và khi truyền nhận, quản lý khóa mã hóa theo thẩm quyền. Các cơ quan, đơn vị khi thuê dịch vụ cần yêu cầu bên cung cấp dịch vụ thiết lập các giải pháp sao lưu tự động đối với dữ liệu trên máy chủ cơ sở dữ liệu và máy chủ ứng dụng và xây dựng các kịch bản có sẵn để khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục khi xảy ra sự cố.

2. Khuyến khích triển khai các giải pháp tăng tính sẵn sàng cho lưu trữ như RAID/nhân bản/cluster để giảm gián đoạn dịch vụ, lưu ý các cơ chế này không thay thế sao lưu.

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

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

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

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

5. Dữ liệu sao lưu phải được lưu giữ trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

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

7. Thông tin, dữ liệu thuộc phạm vi bí mật nhà nước thực hiện theo pháp luật về bảo vệ bí mật nhà nước; dữ liệu cá nhân thực hiện theo pháp luật về bảo vệ dữ liệu cá nhân và văn bản hướng dẫn thi hành.

Điều 19. Bảo đảm an ninh mạng đối với người sử dụng

1. Các cơ quan, đơn vị phải xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, cơ quan, đơn vị có trách nhiệm phổ biến các quy định về bảo đảm an ninh mạng đối với hệ thống thông tin được quản lý, sử dụng. Đối với vị trí tiếp xúc, quản lý thông tin, dữ liệu quan trọng hoặc quản trị hệ thống thông tin quan trọng, cơ quan, đơn vị xác định hình thức cam kết bảo mật phù hợp; cam kết có thể được lập thành văn bản riêng hoặc tích hợp trong hợp đồng làm việc, hợp

đồng lao động, quyết định giao nhiệm vụ hoặc quy định nội bộ. Mẫu tại Phụ lục 07 chỉ có tính chất tham khảo.

2. Các cơ quan, đơn vị phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản công nghệ thông tin liên quan đến hệ thống thông tin đối với các cá nhân do cơ quan, đơn vị quản lý. Người sử dụng phải kiểm tra thông tin, dữ liệu được lưu giữ trên các tài sản công nghệ thông tin trước khi tiếp nhận.

3. Khi cá nhân chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị có trách nhiệm

a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

4. Việc kết nối thiết bị thuộc sở hữu cá nhân (máy tính xách tay, điện thoại thông minh, máy tính bảng) vào vùng mạng nội bộ của cơ quan, đơn vị để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan, đơn vị và phải tuân thủ các quy định về bảo đảm an ninh mạng được quy định tại quy chế này; chịu sự giám sát của bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị.

Điều 20. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến kiến thức về an ninh mạng

1. Các cơ quan, đơn vị phải tổ chức tập huấn, hướng dẫn quản lý, sử dụng hệ thống thông tin bảo đảm an ninh mạng trước khi triển khai chính thức hoặc sau khi nâng cấp hệ thống.

2. Các cơ quan, đơn vị xác định nhu cầu đào tạo, bồi dưỡng nguồn nhân lực về bảo đảm an ninh mạng tại cơ quan, đơn vị mình gửi Công an tỉnh tổng hợp, xác định nội dung, yêu cầu đào tạo, bồi dưỡng. Công an tỉnh chủ trì, phối hợp với Sở Nội vụ và các cơ quan, đơn vị có liên quan tham mưu tổ chức đào tạo, bồi dưỡng theo quy định.

3. Các cơ quan, đơn vị tổ chức đào tạo, bồi dưỡng nghiệp vụ về an ninh mạng cho cán bộ chuyên trách/phụ trách về an ninh mạng các cơ quan, đơn vị trực thuộc; đào tạo cơ bản về an ninh mạng cho người sử dụng thuộc cơ quan, đơn vị.

4. 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 đến toàn thể cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị.

Mục 3

BẢO ĐẢM HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 21. Phân loại và xác định cấp độ hệ thống thông tin

1. Tất cả các hệ thống thông tin do các cơ quan, đơn vị trong tỉnh quản lý, vận hành phải được phân loại và xác định cấp độ hệ thống thông tin để áp dụng các biện pháp quản lý và kỹ thuật tương ứng nhằm bảo vệ hệ thống thông tin.

2. Việc phân loại cấp độ hệ thống thông tin được thực hiện theo 5 cấp độ, từ cấp độ 1 đến cấp độ 5, dựa trên các tiêu chí quy định từ Điều 11 đến Điều 15 của 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.

3. Chủ quản hệ thống thông tin có trách nhiệm chủ trì, chỉ đạo đơn vị vận hành hệ thống thông tin thực hiện việc xác định và đề xuất cấp độ cho các hệ thống thông tin thuộc phạm vi quản lý của mình.

Điều 22. Lập, thẩm định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin

1. Đơn vị vận hành hệ thống thông tin có trách nhiệm lập hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 21 của Nghị định số 331/2026/NĐ-CP ngày 19/8/2026, bao gồm: Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin; tài liệu thiết kế; tài liệu thuyết minh về việc đề xuất cấp độ hệ thống thông tin; thuyết minh phương án bảo đảm an ninh mạng theo cấp độ; ý kiến của đơn vị chuyên trách về an ninh mạng đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5.

2. Thẩm quyền, trình tự, thủ tục thẩm định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin thực hiện theo quy định tại các điều từ Điều 18 đến Điều 25 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.

Điều 23. Phương án bảo đảm an ninh mạng theo cấp độ

1. Chủ quản hệ thống thông tin có trách nhiệm yêu cầu đơn vị vận hành xây dựng và triển khai đầy đủ phương án bảo đảm an ninh mạng đã được phê duyệt trong hồ sơ đề xuất cấp độ.

2. Phương án bảo đảm an ninh mạng phải đáp ứng các yêu cầu về quản lý, kỹ thuật tương ứng với cấp độ đã được phê duyệt, bao gồm các nội dung chính theo quy định tại Điều 29 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 và các điều kiện an ninh mạng theo Tiêu chuẩn quốc gia TCVN 14423:2026 – An ninh mạng – Hệ thống thông tin – Yêu cầu cơ bản

3. Công an tỉnh hướng dẫn, đôn đốc, kiểm tra việc triển khai phương án bảo đảm an ninh mạng tại các cơ quan, đơn vị theo chức năng, nhiệm vụ, thẩm quyền và quy định của pháp luật.

Điều 24. Bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia trên địa bàn tỉnh

1. Các cơ quan, đơn vị có trách nhiệm rà soát, xác định các hệ thống thông tin thuộc phạm vi quản lý có đủ tiêu chuẩn, khả năng thuộc danh mục quan trọng cần ưu tiên bảo đảm an ninh mạng và lập hồ sơ đề nghị đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo quy định.

2. Việc bảo đảm an ninh mạng cho Hệ thống thông tin quan trọng về an ninh quốc gia phải được ưu tiên hàng đầu, được đầu tư nguồn lực tương xứng và áp dụng các biện pháp quản lý, kỹ thuật tăng cường.

3. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia tổ chức triển khai đầy đủ các biện pháp bảo đảm an ninh mạng theo quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật áp dụng. Việc kết nối, chia sẻ thông tin giám sát thực hiện theo quy định của pháp luật, yêu cầu của cơ quan có thẩm quyền và phương án được phê duyệt; phải xác định rõ loại thông tin, dữ liệu, mục đích, phạm vi, phương thức và đầu mối thực hiện; bảo đảm bí mật nhà nước, an ninh dữ liệu và bảo vệ dữ liệu cá nhân khi kết nối, chia sẻ với Trung tâm An ninh mạng quốc gia và Trung tâm An ninh mạng tỉnh (nếu có).

Mục 4

KIỂM TRA, GIÁM SÁT, CẢNH BÁO VÀ ỨNG CỨU SỰ CỐ

Điều 25. Kiểm tra, đánh giá an ninh mạng

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

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Hoạt động kiểm tra, đánh giá an ninh mạng được thực hiện định kỳ hoặc đột xuất nhằm xác định thực trạng hệ thống thông tin; phát hiện, cảnh báo, khắc phục các lỗ hổng, điểm yếu bảo mật và đánh giá sự tuân thủ các quy định.

4. Việc kiểm tra an ninh mạng của cơ quan, lực lượng có thẩm quyền thực hiện theo Điều 26 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 và quy định của pháp luật có liên quan.

5. Hoạt động kiểm tra, đánh giá an ninh mạng do chủ quản tổ chức thực hiện theo Điều 27 và điểm c khoản 2 Điều 31 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.

6. Cơ quan, đơn vị được kiểm tra có trách nhiệm phối hợp, cung cấp thông tin, tài liệu, nhật ký cần thiết, tạo điều kiện cho đoàn kiểm tra; tổ chức khắc phục các tồn tại theo yêu cầu và báo cáo kết quả khắc phục theo thời hạn được thông báo.

7. Việc cung cấp thông tin, tài liệu, nhật ký; kết nối, chia sẻ thông tin, dữ liệu phục vụ kiểm tra, giám sát và ứng cứu sự cố phải đúng thẩm quyền, đúng mục đích, bảo đảm giới hạn trong phạm vi cần thiết và tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các thông tin thuộc phạm vi bảo vệ.

Điều 26. Giám sát, cảnh báo an ninh mạng

1. Các hệ thống thông tin phải được giám sát, cảnh báo an ninh mạng phù hợp với cấp độ, phạm vi, quy mô, tính chất xử lý thông tin; hệ thống từ cấp độ 3 trở lên và hệ thống quan trọng cần ưu tiên giám sát thường xuyên, liên tục theo quy định. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với Công an tỉnh tổ chức thực hiện việc giám sát hệ thống thông tin theo Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Các cơ quan, đơn vị là chủ quản hệ thống thông tin có trách nhiệm triển khai giải pháp giám sát an ninh mạng cho các hệ thống thuộc phạm vi quản lý (có thể tự triển khai hoặc thuê dịch vụ chuyên nghiệp).

3. Các hệ thống thông tin thuộc đối tượng/phạm vi giám sát tập trung phải bảo đảm khả năng tích hợp; đấu nối thực tế theo phương án được phê duyệt. Quy định rõ trường log/thông tin cần chia sẻ, phương thức, quyền truy cập, thời hạn lưu giữ và yêu cầu bảo vệ dữ liệu.

Điều 27. Ứng cứu sự cố an ninh mạng

1. Đội ứng cứu sự cố an ninh mạng tỉnh do đơn vị chuyên trách an ninh mạng tỉnh (Công an tỉnh) tham mưu Ủy ban nhân dân tỉnh thành lập, kiện toàn có vai trò đầu mối điều phối các hoạt động ứng cứu sự cố trên toàn tỉnh.

2. Chủ quản hệ thống thông tin căn cứ quy mô, tính chất, cấp độ của hệ thống để thành lập Tổ ứng cứu sự cố an ninh mạng nội bộ hoặc chỉ định bộ phận, cá nhân làm đầu mối thực hiện nhiệm vụ giám sát, tiếp nhận thông tin, xử lý và phối hợp khắc phục sự cố an ninh mạng trong phạm vi quản lý.

3. Khi ứng cứu sự cố an ninh mạng phải ưu tiên xử lý tại chỗ bằng lực lượng của chủ quản hệ thống thông tin và đơn vị vận hành hệ thống thông tin. Khi sự cố an ninh mạng vượt quá khả năng, Tổ ứng cứu sự cố an ninh mạng nội bộ tham mưu chủ quản hệ thống thông tin báo cáo ngay cho Công an tỉnh để kích hoạt cơ chế điều phối.

4. Phương án, kế hoạch ứng cứu sự cố an ninh mạng

a) Công an tỉnh tham mưu Ủy ban nhân dân tỉnh ban hành, triển khai phương án ứng cứu sự cố an ninh mạng trên địa bàn tỉnh.

b) Tổ ứng cứu sự cố an ninh mạng nội bộ tham mưu chủ quản hệ thống thông tin ban hành, triển khai kế hoạch ứng cứu sự cố an ninh mạng cho các hệ thống thông tin theo cấp độ được phê duyệt.

Điều 28. Quy trình ứng cứu sự cố an ninh mạng

1. Quy trình ứng cứu sự cố an ninh mạng tuân thủ quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

2. Hoạt động của Tổ ứng cứu sự cố an ninh mạng nội bộ:

a) Chủ động rà soát các lỗ hổng, điểm yếu bảo mật của hệ thống thông tin trong phạm vi quản lý và triển khai các giải pháp để khắc phục các nguy cơ này.

b) Tiếp nhận thông tin về sự cố từ hệ thống giám sát, người dùng hoặc thông báo từ cơ quan, đơn vị khác.

c) Kích hoạt quy trình ứng cứu, phân công nhiệm vụ và triển khai các biện pháp đánh giá, xử lý sự cố ban đầu; yêu cầu hỗ trợ, điều phối ứng cứu sự cố khi vượt khả năng.

d) Tổ chức thực hiện theo hướng dẫn của lực lượng chuyên trách, cơ quan điều phối ứng cứu sự cố an ninh mạng cấp trên.

đ) Tổng hợp, báo cáo và cập nhật diễn biến sự cố theo quy định.

3. Hoạt động của Đội ứng cứu sự cố an ninh mạng tỉnh khi tiếp nhận yêu cầu hỗ trợ điều phối hoặc thông báo sự cố:

a) Ghi nhận, tiếp nhận đúng quy định và phản hồi ngay cho tổ chức, cá nhân gửi thông báo hoặc yêu cầu hỗ trợ, điều phối.

b) Chủ trì, điều hành, phân công nhiệm vụ cho các thành viên Đội ứng cứu sự cố an ninh mạng tỉnh và các cơ quan, đơn vị liên quan triển khai xác minh và xử lý sự cố an ninh mạng.

c) Phối hợp, đề nghị doanh nghiệp cung cấp dịch vụ viễn thông, internet và tổ chức, cá nhân có liên quan triển khai các biện pháp kỹ thuật cần thiết để ngăn chặn nguồn tấn công, hạn chế, lọc lưu lượng độc hại trong phạm vi pháp luật và thỏa thuận cung cấp dịch vụ cho phép; trường hợp cần áp dụng biện pháp thuộc thẩm quyền cơ quan nhà nước thì báo cáo, đề xuất cơ quan có thẩm quyền quyết định hoặc thực hiện theo quy định.

d) Là đầu mối liên lạc, phối hợp với Trung tâm An ninh mạng quốc gia và các cơ quan Trung ương trong các trường hợp cần thiết.

Mục 5

BẢO VỆ BÍ MẬT NHÀ NƯỚC, DỮ LIỆU CÁ NHÂN

Điều 29. Bảo vệ bí mật nhà nước trên không gian mạng

1. Các cơ quan, đơn vị có xử lý thông tin bí mật nhà nước phải bố trí máy tính, máy in và các thiết bị ngoại vi được tách biệt hoàn toàn về mặt vật lý với mạng Internet và các mạng máy tính khác (trừ mạng LAN độc lập) để phục vụ riêng cho việc soạn thảo, lưu trữ, in ấn tài liệu bí mật nhà nước.

2. Không sử dụng máy tính, thiết bị đã dùng để soạn thảo, lưu giữ bí mật nhà nước để kết nối với mạng máy tính (trừ mạng LAN độc lập), mạng Internet, mạng viễn thông khi chưa hoàn thành việc chuyển mục đích sử dụng tài sản phần cứng; sử dụng máy tính, thiết bị có lịch sử kết nối với mạng máy tính (trừ mạng LAN độc lập), mạng Internet, mạng viễn thông để soạn thảo, lưu giữ bí mật nhà nước.

3. Thiết bị kỹ thuật liên quan đến việc bảo vệ bí mật nhà nước thuộc trường hợp phải kiểm định, kiểm tra an ninh thì thực hiện kiểm định, kiểm tra an ninh theo quy định của pháp luật về bảo vệ bí mật nhà nước và pháp luật có liên quan. Việc quản lý, sử dụng thiết bị sau kiểm định, kiểm tra an ninh thực hiện theo quy định pháp luật có hiệu lực tại thời điểm thực hiện

4. Tài sản phần cứng khi mang khỏi trụ sở của cơ quan, đơn vị phải được sự phê duyệt của cấp có thẩm quyền và thực hiện biện pháp bảo vệ đối với thông tin, tài liệu bí mật nhà nước lưu trữ trên tài sản phần cứng.

5. Các thiết bị lưu trữ di động (USB, Ổ cứng ngoài) dùng để sao chép, lưu trữ thông tin, tài liệu bí mật nhà nước phải được quản lý chặt chẽ, sử dụng riêng và áp dụng các biện pháp mã hóa để bảo vệ dữ liệu.

6. Việc truyền đưa thông tin thuộc bí mật nhà nước qua không gian mạng phải được mã hóa bằng sản phẩm mật mã của Ban Cơ yếu Chính phủ và tuân thủ tuyệt đối các quy định của pháp luật về cơ yếu, an ninh mạng, bảo vệ bí mật nhà nước.

Điều 30. Yêu cầu chung trong xử lý dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân tại các cơ quan, đơn vị phải tuân thủ đầy đủ các nguyên tắc bảo vệ dữ liệu cá nhân quy định tại Điều 3 Luật Bảo vệ dữ liệu cá nhân.

2. Mọi hoạt động thu thập, xử lý dữ liệu cá nhân phải được sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác. Dữ liệu chỉ được xử lý đúng mục đích đã đăng ký hoặc thông báo.

3. Các cơ quan, đơn vị áp dụng các biện pháp quản lý và kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân trong suốt quá trình xử lý, lưu trữ và hủy bỏ.

Điều 31. Quyền và nghĩa vụ của các bên liên quan trong bảo vệ dữ liệu cá nhân

1. Chủ thể dữ liệu là cán bộ, công chức, viên chức, người lao động và công dân có các quyền và nghĩa vụ theo quy định tại Điều 4 Luật Bảo vệ dữ liệu cá nhân.

2. Thủ trưởng cơ quan, đơn vị chịu trách nhiệm trực tiếp, toàn diện về việc bảo đảm an ninh dữ liệu cá nhân thuộc phạm vi quản lý của cơ quan, đơn vị mình.

3. Cán bộ, công chức, viên chức và người lao động được giao nhiệm vụ xử lý dữ liệu cá nhân có trách nhiệm bảo mật thông tin, không được tiết lộ, chia sẻ dữ liệu trái phép và phải chịu trách nhiệm nếu để xảy ra lộ, mất dữ liệu.

Điều 32. Trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, đơn vị

1. Các cơ quan, đơn vị là Bên Kiểm soát dữ liệu hoặc Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm

a) Phân công bộ phận hoặc nhân sự phụ trách bảo vệ dữ liệu cá nhân.

b) Xây dựng và ban hành nội dung quy định nội bộ về bảo vệ dữ liệu cá nhân.

c) Thực hiện đánh giá tác động xử lý dữ liệu cá nhân và lập hồ sơ gửi Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an theo quy định.

2. Khi phát hiện vi phạm quy định về bảo vệ dữ liệu cá nhân, cơ quan, đơn vị phải thực hiện biện pháp khắc phục, lập hồ sơ/biên bản và thực hiện nghĩa vụ thông báo theo Điều 23 Luật Bảo vệ dữ liệu cá nhân và Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ. Trường hợp vi phạm có thể gây tổn hại đến quốc phòng, an ninh quốc gia, trật tự an toàn xã hội hoặc xâm phạm tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản của chủ thể dữ liệu cá nhân thì thông báo cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất 72 giờ kể từ khi phát hiện.

3. Áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong hoạt động ứng dụng công nghệ thông tin, bao gồm: quản lý quyền truy cập, ghi nhật ký hệ thống, mã hóa dữ liệu quan trọng và các biện pháp kỹ thuật khác theo hướng dẫn của cơ quan chức năng.

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG

Điều 33. Trách nhiệm của Công an tỉnh

1. Tham mưu, quản lý nhà nước

a) Chủ trì tham mưu, giúp Ủy ban nhân dân tỉnh thực hiện công tác quản lý nhà nước về an ninh mạng trên địa bàn tỉnh.

b) Xây dựng, trình Ủy ban nhân dân tỉnh ban hành và tổ chức thực hiện các chiến lược, chương trình, đề án, kế hoạch của tỉnh về bảo đảm an ninh mạng.

2. Thẩm định, thanh tra, kiểm tra, đánh giá

a) Đối với hệ thống thông tin do Ủy ban nhân dân tỉnh là chủ quản, Công an tỉnh thực hiện nhiệm vụ của đơn vị chuyên trách về an ninh mạng của chủ quản khi được cấp có thẩm quyền giao hoặc xác định theo quy định pháp luật; thực hiện thẩm định, phê duyệt hoặc cho ý kiến chuyên môn đối với hồ sơ đề xuất cấp độ theo đúng phạm vi, thẩm quyền quy định tại Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ. Việc thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thực hiện theo Luật An ninh mạng và quy định có liên quan.

b) Tham mưu Ủy ban nhân dân tỉnh hướng dẫn, đôn đốc, theo dõi việc thực hiện quy định về bảo đảm an ninh mạng; thực hiện hoặc phối hợp kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin theo chức năng, nhiệm vụ, thẩm quyền và quy định của pháp luật; kiến nghị chủ quản hệ thống thông tin khắc phục lỗ hổng, điểm yếu, nguy cơ mất an ninh mạng được phát hiện.

3. Giám sát và cảnh báo

a) Thực hiện nhiệm vụ quản lý, vận hành Trung tâm An ninh mạng tỉnh khi được cấp có thẩm quyền giao; tổ chức giám sát tập trung, phân tích, cảnh báo sớm các nguy cơ, mối đe dọa an ninh mạng theo phạm vi nhiệm vụ được giao.

b) Tham mưu Ủy ban nhân dân tỉnh hướng dẫn bảo đảm an ninh mạng cho hạ tầng kỹ thuật của các Trung tâm dữ liệu của tỉnh.

c) Chủ trì, phối hợp với các cơ quan chức năng xử lý thông tin vi phạm pháp luật trên không gian mạng.

d) Tổ chức triển khai kết nối, chia sẻ thông tin giám sát, cảnh báo với Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an.

4. Ứng cứu sự cố an ninh mạng

a) Thực hiện nhiệm vụ Cơ quan Thường trực Đội ứng cứu sự cố an ninh mạng tỉnh theo quyết định của cấp có thẩm quyền; làm đầu mối tiếp nhận, tham mưu điều phối hoạt động ứng cứu sự cố an ninh mạng theo chức năng, nhiệm vụ, thẩm quyền.

b) Tham mưu Ủy ban nhân dân tỉnh ban hành và tổ chức triển khai phương án ứng cứu sự cố an ninh mạng trên địa bàn tỉnh, kết nối với hệ thống phương án ứng cứu quốc gia.

5. Phòng, chống tội phạm và vi phạm pháp luật

a) Chủ trì, phối hợp với các cơ quan chức năng trong công tác phòng, chống tấn công mạng, gián điệp mạng, khủng bố mạng, phòng, chống mã độc và các loại tội phạm sử dụng công nghệ cao. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao.

b) Điều tra, xử lý các hành vi vi phạm pháp luật về an ninh mạng theo thẩm quyền.

c) Tham mưu Ủy ban nhân dân tỉnh triển khai các biện pháp bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

6. Hướng dẫn, đào tạo và diễn tập

a) Hướng dẫn nghiệp vụ về bảo đảm an ninh mạng; hỗ trợ giải quyết sự cố khi có yêu cầu. Hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ và triển khai thực hiện việc bảo đảm an ninh mạng cho hệ thống thông tin theo quy định của pháp luật.

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

c) Tham mưu cho Ủy ban nhân dân tỉnh tổ chức các cuộc diễn tập ứng cứu sự cố an ninh mạng cấp tỉnh; tham gia các chương trình diễn tập quốc gia, quốc tế do Bộ Công an tổ chức.

Điều 34. Trách nhiệm của Sở Khoa học và Công nghệ

1. Chủ trì, tham mưu cho Ủy ban nhân dân tỉnh về chiến lược, chương trình, đề án, kế hoạch về chuyển đổi số, phát triển chính quyền số, kinh tế số và xã hội số trên địa bàn tỉnh, bảo đảm các yêu cầu về an ninh mạng được lồng ghép trong quá trình xây dựng.

2. Trong phạm vi chức năng, nhiệm vụ và thẩm quyền, thực hiện thẩm định hoặc tham gia ý kiến đối với nội dung kỹ thuật, công nghệ của thiết kế cơ sở, thiết kế chi tiết trong các dự án chuyển đổi số; phối hợp với Công an tỉnh xem xét các yêu cầu về an ninh mạng thuộc chức năng, nhiệm vụ, thẩm quyền của Công an tỉnh.

3. Phối hợp với Công an tỉnh trong việc tuyên truyền, hướng dẫn các doanh nghiệp công nghệ số thực hiện các quy định của pháp luật về an ninh mạng.

4. Phối hợp cung cấp thông tin, ý kiến chuyên môn về kỹ thuật, công nghệ thuộc phạm vi chức năng, nhiệm vụ, quyền hạn của Sở đối với các hệ thống thông tin, nền tảng số khi có yêu cầu của Công an tỉnh trong quá trình kiểm tra, đánh giá, ứng cứu sự cố an ninh mạng.

Điều 35. Trách nhiệm của chủ quản hệ thống thông tin

1. Đối với cơ quan, tổ chức được xác định là chủ quản hệ thống thông tin, người đứng đầu có trách nhiệm trực tiếp chỉ đạo và chịu trách nhiệm trước pháp luật về công tác bảo vệ an ninh mạng đối với hệ thống thuộc phạm vi quản lý.

2. Phân công bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng; bố trí đủ nguồn lực (nhân sự, kinh phí, trang thiết bị) để triển khai các nhiệm vụ bảo đảm an ninh mạng.

3. Trình cấp có thẩm quyền phê duyệt hồ sơ đề xuất cấp độ an ninh mạng của hệ thống thông tin; chỉ đạo xây dựng và ban hành phương án bảo đảm an ninh mạng tương ứng với cấp độ được duyệt và tổ chức triển khai thực hiện.

4. Ban hành và tổ chức thực hiện quy chế nội bộ về bảo đảm an ninh mạng tại cơ quan, đơn vị mình.

5. Tổ chức thực hiện việc kiểm tra, đánh giá, quản lý rủi ro an ninh mạng định kỳ theo quy định.

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

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

Điều 36. 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 hệ thống thông tin theo quy định tại Điều 20 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.

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

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết.

d) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng trong công tác bảo đảm an ninh mạng.

đ) Kịp thời kích hoạt phương án ứng cứu sự cố và thông báo, phối hợp xử lý sự cố an ninh mạng với các cơ quan, đơn vị liên quan *(Phụ lục 2)*.

e) Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an ninh mạng hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin.

g) Chịu trách nhiệm quản trị, vận hành kỹ thuật, giám sát, sao lưu, khôi phục hệ thống.

h) Hướng dẫn, hỗ trợ các xã, phường trong quá trình khai thác, sử dụng hệ thống.

i) Chủ động xử lý ban đầu và phối hợp ứng cứu khi xảy ra sự cố.

2. Trường hợp hệ thống thông tin có chủ quản 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 thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Bên cung cấp dịch vụ chỉ thực hiện trách nhiệm đơn vị vận hành trong phạm vi được xác định theo hợp đồng hoặc quyết định của chủ quản.

Điều 37. Trách nhiệm của cơ quan, đơn vị được giao quản lý, vận hành Trung tâm dữ liệu của tỉnh

1. Cơ quan, đơn vị được giao quản lý, vận hành Trung tâm dữ liệu của tỉnh thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 33 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 và Quy chế này đối với hệ thống thông tin thuộc phạm vi được giao quản lý, vận hành.

2. Bảo đảm tiêu chuẩn, quy chuẩn kỹ thuật về trung tâm dữ liệu; phù hợp với quy hoạch hạ tầng thông tin và truyền thông; có giải pháp bảo đảm an ninh mạng để kiểm soát, phát hiện, ngăn chặn tấn công, đột nhập, phá hoại; bảo đảm mức độ sẵn sàng của hệ thống, thiết kế hệ thống với mức dự phòng nhằm sẵn sàng trong trường hợp mở rộng khi cần thiết.

3. Thường xuyên cập nhật các nguy cơ gây mất an ninh mạng cho các hệ thống thông tin đang cài đặt và vận hành tại các Trung tâm dữ liệu của tỉnh và thông báo cho các cơ quan, đơn vị liên quan biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

Điều 38. Trách nhiệm của người đứng đầu, cấp phó của người đứng đầu; cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của người đứng đầu

a) Lãnh đạo, chỉ đạo toàn diện công tác đảm bảo an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; có văn bản phân công bộ phận hoặc cán bộ thực hiện nhiệm vụ quản trị, vận hành, bảo đảm an ninh mạng.

Đối với Ủy ban nhân dân các xã, phường nếu không bố trí cán bộ chuyên trách, thì phải giao cán bộ kiêm nhiệm nhưng vẫn bảo đảm thực hiện đầy đủ các yêu cầu của Quy chế, gồm: Ban hành Quy chế, quy định nội bộ về quản lý, sử dụng hệ thống thông tin, dữ liệu và thiết bị công nghệ thông tin; xây dựng kế hoạch bảo đảm an ninh mạng và phương án ứng cứu sự cố an ninh mạng; xây dựng hồ sơ đề xuất cấp độ an toàn thông tin trình cơ quan có thẩm quyền phê duyệt hoặc giao bộ phận chuyên trách về an toàn thông tin phê duyệt theo quy định pháp luật; xác định bảo đảm an ninh mạng là nhiệm vụ thường xuyên, gắn với công tác lãnh đạo, điều hành và chuyển đổi số của cơ quan, đơn vị; chỉ đạo triển khai các biện pháp phòng ngừa, phát hiện, xử lý nguy cơ mất an ninh mạng.

b) Chịu trách nhiệm theo quy định của pháp luật và theo chức trách, nhiệm vụ, quyền hạn được giao đối với công tác bảo đảm an ninh mạng thuộc phạm vi quản lý. Khi xảy ra lộ, mất bí mật nhà nước, dữ liệu cá nhân bị chiếm quyền điều khiển hệ thống thông tin, phát tán thông tin vi phạm pháp luật hoặc sự cố an ninh mạng phải có trách nhiệm chỉ đạo kiểm tra, đánh giá và phối hợp cơ quan chuyên trách về an ninh mạng để tổ chức khắc phục kịp thời sự cố an ninh mạng.

c) Bảo đảm nguồn lực: bố trí cán bộ có trình độ chuyên môn phù hợp làm đầu mối chuyên trách hoặc kiêm nhiệm phù hợp về an ninh mạng. Quan tâm đầu

tư trang thiết bị, phần mềm bảo mật, giải pháp sao lưu dữ liệu, giám sát và cảnh báo sớm. Tổ chức đào tạo, tập huấn nâng cao nhận thức cho cán bộ, công chức, viên chức.

d) Thực hiện chế độ kiểm tra, báo cáo: chỉ đạo thực hiện nghiêm chế độ trực, giám sát, báo cáo sự cố an ninh mạng theo quy định. Phối hợp với cơ quan chức năng trong công tác kiểm tra, đánh giá, ứng cứu và xử lý sự cố.

2. Trách nhiệm cấp phó của người đứng đầu: Cấp phó được phân công phụ trách lĩnh vực công nghệ thông tin, chuyển đổi số hoặc an ninh mạng có trách nhiệm:

a) Tham mưu cho người đứng đầu xây dựng kế hoạch, phương án bảo đảm an ninh mạng.

b) Trực tiếp chỉ đạo, kiểm tra việc triển khai các giải pháp kỹ thuật và biện pháp quản lý bảo mật.

c) Theo dõi, đôn đốc cán bộ, bộ phận chuyên môn thực hiện đúng quy trình bảo đảm an ninh mạng.

d) Kịp thời báo cáo người đứng đầu khi phát hiện nguy cơ mất an ninh mạng hoặc xảy ra sự cố an ninh mạng.

đ) Phối hợp với lực lượng chuyên trách an ninh mạng trong công tác phòng ngừa, xử lý và khắc phục sự cố.

e) Trường hợp được giao phụ trách trực tiếp mà có hành vi vi phạm hoặc thiếu trách nhiệm trong thực hiện nhiệm vụ thì chịu trách nhiệm theo quy định của pháp luật tương ứng với hành vi, lỗi, nhiệm vụ, thẩm quyền và hậu quả; không mặc nhiên xác định trách nhiệm liên đới nếu chưa có căn cứ pháp luật.

3. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

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

b) Cán bộ, công chức, viên chức và người lao động có trách nhiệm quản lý, bảo quản, bảo đảm an ninh mạng cho tài sản công nghệ thông tin được giao quản lý, sử dụng.

c) Khi phát hiện sự cố mất an ninh mạng phải thông báo ngay với cấp trên và bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

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

4. Trách nhiệm của cán bộ chuyên trách/phụ trách về an ninh mạng: ngoài các quy định tại khoản 3 Điều này, cán bộ chuyên trách/phụ trách về an ninh mạng có trách nhiệm:

a) Chủ trì tham mưu với thủ trưởng 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.

b) Trực tiếp thiết lập hoặc tham mưu Thủ trưởng cơ quan, đơn vị ban hành Quy chế nội bộ và các biện pháp kỹ thuật bảo đảm an ninh mạng cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin.

c) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay Thủ trưởng cơ quan, đơn vị các sự cố mất an ninh mạng và mức độ nghiêm trọng của các sự cố đó.

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

Điều 39. Trách nhiệm của tổ chức, đơn vị, cá nhân liên quan

Các tổ chức, đơn vị, cá nhân quy định tại điểm c khoản 2 Điều 1 có trách nhiệm tuân thủ Quy chế này trong phạm vi nhiệm vụ, quyền hạn, quyền truy cập, dịch vụ hoặc công việc được giao; đồng thời thực hiện các quy định của pháp luật về an ninh mạng và pháp luật có liên quan.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 40. Chế độ, nội dung báo cáo và biểu mẫu

1. Chế độ báo cáo

a) Báo cáo định kỳ hằng năm về công tác bảo đảm an ninh mạng đối với hệ thống thông tin được thực hiện theo quy định tại Điều 35 và Điều 36 Nghị định số 331/2026/NĐ-CP của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin.

b) Báo cáo đột xuất, thông báo sự cố an ninh mạng và các báo cáo khác được thực hiện theo yêu cầu của cơ quan có thẩm quyền và quy định của pháp luật có liên quan.

c) Việc lập, tổng hợp và gửi báo cáo thực hiện theo nguyên tắc đúng nội dung, đúng đối tượng, đúng thời hạn; không yêu cầu báo cáo lại những thông tin đã được cung cấp trong cùng kỳ báo cáo, trừ trường hợp thông tin có thay đổi hoặc cơ quan có thẩm quyền có yêu cầu khác.

2. Nội dung báo cáo

a) Báo cáo định kỳ hằng năm thực hiện theo Mẫu số 08 ban hành kèm theo Nghị định số 331/2026/NĐ-CP của Chính phủ.

b) Các thông tin bổ sung phục vụ công tác quản lý, tổng hợp tình hình bảo đảm an ninh mạng tại cơ quan, đơn vị, địa phương được thực hiện theo các phụ lục ban hành kèm theo quy chế này, trong phạm vi nội dung chưa được quy định hoặc chưa được thể hiện trong Mẫu số 08.

c) Nội dung tại các phụ lục được sử dụng để bổ sung, chi tiết hóa hoặc phục vụ tổng hợp, quản lý nội bộ, không thay thế Mẫu số 08 và không yêu cầu cơ quan, đơn vị cung cấp lại thông tin đã có trong Mẫu số 08 hoặc phụ lục khác trong cùng kỳ báo cáo.

d) Trường hợp thông tin tại các phụ lục có nội dung trùng với thông tin đã được báo cáo theo Mẫu số 08, cơ quan, đơn vị chỉ thực hiện cập nhật hoặc dẫn chiếu thông tin đã báo cáo, không lập lại báo cáo.

3. Thời gian chốt số liệu và thời hạn báo cáo

a) Thời gian chốt số liệu báo cáo định kỳ hằng năm được thực hiện từ ngày 15 tháng 12 của năm trước kỳ báo cáo đến ngày 14 tháng 12 của kỳ báo cáo.

b) Đơn vị chuyên trách về an ninh mạng, đơn vị vận hành hệ thống thông tin gửi báo cáo cho Chủ quản hệ thống thông tin trước ngày 20 tháng 12 hằng năm.

c) Chủ quản hệ thống thông tin gửi báo cáo theo thẩm quyền, trong đó có báo cáo gửi Bộ Công an theo quy định, trước ngày 25 tháng 12 hằng năm.

d) Thời điểm, đối tượng và thời hạn thực hiện báo cáo đột xuất được thực hiện theo yêu cầu của cơ quan có thẩm quyền và quy định của pháp luật.

4. Đơn vị thực hiện

a) Đơn vị chuyên trách về an ninh mạng, đơn vị vận hành hệ thống thông tin có trách nhiệm cung cấp, tổng hợp thông tin thuộc phạm vi chức năng, nhiệm vụ và gửi chủ quản hệ thống thông tin theo quy định.

b) Chủ quản hệ thống thông tin chịu trách nhiệm tổ chức tổng hợp, kiểm tra và gửi báo cáo theo đúng thẩm quyền, thời hạn và biểu mẫu quy định.

c) Công an tỉnh có trách nhiệm hướng dẫn, đôn đốc, tổng hợp báo cáo của các cơ quan, đơn vị thuộc phạm vi quản lý để phục vụ công tác quản lý nhà nước về an ninh mạng tại địa phương theo quy định.

d) Cơ quan, đơn vị thực hiện báo cáo chịu trách nhiệm về tính chính xác, đầy đủ và kịp thời của thông tin, số liệu thuộc phạm vi quản lý.

5. Biểu mẫu và phụ lục báo cáo

a) Mẫu số 08 – Báo cáo kết quả công tác bảo đảm an ninh mạng hệ thống thông tin ban hành kèm theo Nghị định số 331/2026/NĐ-CP là biểu mẫu báo cáo định kỳ chính thức.

b) Các phụ lục kèm theo Quy chế này được sắp xếp như sau:

Phụ lục 01: Mẫu thông tin bổ sung phục vụ quản lý, tổng hợp công tác bảo đảm an ninh mạng tại địa phương; phụ lục 02: Mẫu thông tin/báo cáo sự cố an ninh mạng; phụ lục 03: Mẫu danh mục hệ thống thông tin, cơ sở dữ liệu, phần mềm, nền tảng số; phụ lục 04: Danh mục nhóm hệ thống ưu tiên xem xét kết nối giám sát tập trung về trung tâm an ninh mạng tỉnh; phụ lục 05: Mẫu phân công đầu mối phụ trách an ninh mạng; phụ lục 06: Checklist yêu cầu tối thiểu

trước khi hệ thống thông tin kết nối, chia sẻ dữ liệu chính thức; phụ lục 7: Cam kết bảo đảm an ninh mạng.

c) Phạm vi và mục đích sử dụng của từng phụ lục được quy định ngay tại từng phụ lục, trong đó xác định rõ: đối tượng áp dụng, thời điểm thực hiện, nội dung cần cung cấp, cơ quan tiếp nhận và việc phụ lục có phải là thành phần của báo cáo định kỳ hay không.

d) Các phụ lục không mặc nhiên là thành phần của báo cáo định kỳ hằng năm, chỉ yêu cầu cơ quan, đơn vị thực hiện khi thuộc phạm vi áp dụng hoặc có yêu cầu cụ thể của cơ quan có thẩm quyền.

đ) Trường hợp một thông tin đã được cung cấp tại Mẫu số 08 hoặc tại một phụ lục khác thì không yêu cầu cung cấp lại, trừ trường hợp thông tin có thay đổi hoặc cần cập nhật để phục vụ một nhiệm vụ cụ thể.

Điều 41. Kinh phí thực hiện

1. Kinh phí thực hiện công tác bảo đảm an ninh mạng được bố trí từ ngân sách nhà nước theo phân cấp quản lý, sử dụng ngân sách hiện hành và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật. Các cơ quan, đơn vị căn cứ chức năng, nhiệm vụ và yêu cầu bảo đảm an ninh mạng có trách nhiệm lập dự toán kinh phí và thực hiện theo quy định của pháp luật về ngân sách nhà nước.

2. Cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và đơn vị sự nghiệp công lập do ngân sách nhà nước bảo đảm phải bố trí kinh phí bảo vệ an ninh mạng trong dự toán chi thực hiện nhiệm vụ chuyển đổi số, ứng dụng công nghệ thông tin hằng năm; đồng thời bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng.

Điều 42. Khen thưởng và xử lý vi phạm

1. Hằng năm, căn cứ kết quả công tác bảo đảm an ninh mạng của các cơ quan, đơn vị, Công an tỉnh tham mưu cấp có thẩm quyền xem xét khen thưởng tổ chức, cá nhân có thành tích xuất sắc theo quy định của pháp luật về thi đua, khen thưởng.

2. Tổ chức, cá nhân có hành vi vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm và hậu quả xảy ra, bị xử lý theo quy định của pháp luật.

Điều 43. Trách nhiệm thi hành

1. Thủ trưởng các cơ quan, đơn vị và các tổ chức, đơn vị, cá nhân liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình. Quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc phát sinh, các cơ quan, đơn vị phản ánh kịp thời về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung.

2. Trường hợp văn bản quy phạm pháp luật được viện dẫn tại Quy chế này được sửa đổi, bổ sung hoặc thay thế bằng văn bản quy phạm pháp luật khác thì

thực hiện theo nội dung của văn bản quy phạm pháp luật sửa đổi, bổ sung hoặc thay thế đó.

3. Công an tỉnh chủ trì, phối hợp với các cơ quan, đơn vị liên quan theo dõi, hướng dẫn, đôn đốc, kiểm tra việc thực hiện Quy chế này theo chức năng, nhiệm vụ và thẩm quyền; định kỳ tổng hợp, báo cáo Ủy ban nhân dân tỉnh./.