BỘ XÂY DỰNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1994 /QĐ-BXD	*Hà Nội, ngày 20 tháng 11 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an ninh mạng Bộ Xây dựng

BỘ TRƯỞNG BỘ XÂY DỰNG

Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10 tháng 12 năm 2025;

Căn cứ Nghị định số 33/2025/NĐ-CP ngày 25 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Xây dựng;

Căn cứ Nghị định số 354/2026/NĐ-CP ngày 11 tháng 9 năm 2026 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 33/2025/NĐ-CP ngày 25 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Xây dựng;

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;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Theo đề nghị của Giám đốc Trung tâm Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng Bộ Xây dựng.

Điều 2. Quyết định này có hiệu lực từ ngày ký ban hành và thay thế Quyết định số 1324/QĐ-BXD ngày 13 tháng 8 năm 2025 của Bộ trưởng Bộ Xây dựng ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng Bộ Xây dựng.

Điều 3. Chánh Văn phòng Bộ, các Vụ trưởng, Cục trưởng, Giám đốc Trung tâm Công nghệ thông tin và Thủ trưởng các cơ quan, đơn vị thuộc Bộ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để báo cáo);
- Các đồng chí Thứ trưởng;
- Bộ Công an;
- Cổng TTĐT Bộ Xây dựng;
- Lưu: VT, TTCNTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Phạm Minh Hà

BỘ XÂY DỰNG

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

QUY CHẾ
BẢO ĐẢM AN NINH MẠNG BỘ XÂY DỰNG

(Kèm theo Quyết định số 1994 /QĐ-BXD ngày 20 tháng 11 năm 2026 của Bộ trưởng Bộ Xây dựng)

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 về bảo đảm an ninh mạng trong các hoạt động chuyển đổi số của Bộ Xây dựng.

2. Đối tượng áp dụng:

a) Các cơ quan, đơn vị thuộc Bộ Xây dựng (sau đây gọi tắt là đơn vị).

b) Cán bộ, công chức, viên chức và người lao động trong các đơn vị thuộc Bộ Xây dựng (sau đây gọi tắt là cá nhân).

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 hệ thống thông tin thuộc thẩm quyền quản lý của Bộ Xây dựng hoặc đơn vị thuộc Bộ Xây dựng.

2. *Chủ quản hệ thống thông tin* là Bộ Xây dựng hoặc cơ quan, đơn vị được xác định theo Điều 4 Nghị định số 331/2026/NĐ-CP và quyết định của cấp có thẩm quyền.

3. *Đơn vị vận hành* là đơn vị được giao nhiệm vụ hoặc ký hợp đồng thực hiện việc quản trị, vận hành, duy trì hoạt động của hệ thống thông tin thuộc phạm vi quản lý.

4. *Người quản trị* là cá nhân được giao thực hiện việc quản trị, cấu hình và vận hành kỹ thuật hệ thống thông tin.

5. *Người sử dụng* là công chức, viên chức, người lao động hoặc cá nhân được cấp quyền sử dụng hệ thống thông tin, thiết bị, tài khoản, dữ liệu hoặc dịch vụ số thuộc phạm vi quản lý của Bộ Xây dựng.

6. Các từ ngữ khác được sử dụng trong Quy chế này được hiểu theo quy định của pháp luật về an ninh mạng và pháp luật có liên quan.

Điều 3. Nguyên tắc bảo đảm an ninh mạng

1. Bảo đảm an ninh mạng là yêu cầu bắt buộc, tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An ninh mạng và các quy định pháp luật khác có liên quan.

2. Từng đơn vị phải có trách nhiệm bảo đảm an ninh mạng của đơn vị mình, theo đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

3. Xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị (hoặc người đại diện hợp pháp), từng bộ phận và cá nhân trong đơn vị đối với công tác bảo đảm an ninh mạng.

4. An ninh mạng được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo các tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng được các cơ quan có thẩm quyền ban hành.

5. Việc bảo đảm an ninh mạng được thực hiện trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của đơn vị.

6. Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro an ninh mạng có thể xảy ra trong đơn vị.

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

8. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

9. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 7 Luật An ninh mạng.

2. Các hành vi nghiêm cấm khác về an ninh mạng theo quy định của pháp luật.

Chương II

BẢO ĐẢM AN NINH MẠNG HỆ THỐNG THÔNG TIN BỘ XÂY DỰNG

Mục 1

BẢO ĐẢM AN NINH MẠNG TRONG THIẾT KẾ, XÂY DỰNG, HỦY BỎ HỆ THỐNG THÔNG TIN

Điều 5. Thiết kế an toàn hệ thống thông tin

1. Trong quá trình xây dựng hoặc nâng cấp hệ thống, phải có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin; thiết kế và các thành phần của hệ thống thông tin; phương án bảo đảm an ninh mạng theo cấp độ; phương án lựa chọn giải pháp công nghệ bảo đảm an ninh mạng.

2. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết

kế đối với các yêu cầu an toàn đặt ra đối với hệ thống; có phương án quản lý và bảo vệ hồ sơ thiết kế.

3. Đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an ninh mạng trước khi triển khai thực hiện.

Điều 6. Yêu cầu về an ninh mạng cho hệ thống

1. Xây dựng các yêu cầu về an ninh mạng đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

2. Đánh giá, xác định cấp độ và tuân thủ đầy đủ các quy định về bảo đảm an ninh mạng của hệ thống theo cấp độ tương ứng.

3. Xây dựng các yêu cầu về trách nhiệm cập nhật, vá lỗi, khắc phục lỗ hổng bảo mật của hệ thống thông tin được phát hiện trong quá trình vận hành.

4. Các biện pháp bảo đảm an ninh mạng phải đáp ứng đầy đủ yêu cầu bắt buộc theo quy định của pháp luật đối với cấp độ, loại hình hệ thống thông tin và thông tin, dữ liệu được xử lý. Ngoài các yêu cầu bắt buộc, chủ quản hệ thống thông tin quyết định áp dụng biện pháp tăng cường trên cơ sở đánh giá rủi ro và yêu cầu hoạt động của hệ thống. Phạm vi, đối tượng và mức độ áp dụng từng biện pháp phải được xác định trong phương án bảo đảm an ninh mạng được phê duyệt.

Điều 7. Quản lý an ninh mạng máy chủ

1. Quản lý, vận hành hoạt động của hệ thống máy chủ

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

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

c) Quản lý các thay đổi cấu hình kỹ thuật; thường xuyên cập nhật các bản vá lỗi và loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

2. Quản lý truy cập máy chủ

Bảo đảm 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.

3. Quản trị máy chủ

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Chỉ kết nối Internet cho máy chủ theo phương án bảo vệ của từng hệ thống đã được phê duyệt, có phân vùng và kiểm soát.

d) Áp dụng xác thực đa nhân tố đối với truy cập của người sử dụng vào

máy chủ theo yêu cầu bảo vệ tương ứng với cấp độ hệ thống thông tin; việc thay đổi thông tin xác thực thực hiện theo quy định quản lý truy cập của hệ thống.

đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

e) Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

Điều 8. Quản lý an toàn ứng dụng

1. An toàn ứng dụng

Các phần mềm ứng dụng nghiệp vụ phải đạt các yêu cầu tối thiểu về an toàn ứng dụng sau:

a) Kiểm tra tính hợp lệ của dữ liệu đầu vào khi nhập liệu từ người dùng hoặc các hệ thống bên ngoài.

b) Kiểm tra tính hợp lệ của dữ liệu trao đổi giữa các thành phần của hệ thống.

c) Có các biện pháp bảo đảm tính xác thực và tính toàn vẹn dữ liệu.

d) Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng.

đ) Khóa mật mã và các thông tin xác thực khác phải được bảo vệ theo tính chất, mục đích sử dụng và yêu cầu bảo đảm an ninh mạng của hệ thống.

2. Quản trị ứng dụng

a) Có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ đối với tài khoản quản trị của ứng dụng.

b) Việc truyền mật khẩu và thông tin xác thực bí mật qua mạng phải được thực hiện bằng kênh truyền mã hóa an toàn, có xác thực bên nhận. Không ghi mật khẩu, khóa mật mã bí mật và thông tin xác thực bí mật vào nhật ký hoặc thông báo lỗi ở dạng có thể đọc được.

c) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

Điều 9. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa:

a) Đơn vị 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.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Có cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

5. 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).

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

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

Điều 10. Quản lý mật mã

1. Quy định và đưa vào sử dụng các biện pháp mã hóa mật mã theo các chuẩn quốc gia hoặc quốc tế đã được công nhận, có biện pháp quản lý khóa để bảo vệ thông tin.

2. Khóa mật mã bí mật và các thông tin xác thực bí mật khác phải được quản lý, bảo vệ trong quá trình tạo lập, cấp phát, sử dụng, lưu trữ, truyền nhận, thay đổi, thu hồi và hủy bỏ; áp dụng mã hóa hoặc biện pháp bảo vệ phù hợp với tính chất, mục đích sử dụng. Thông tin, dữ liệu phải bảo mật theo quy định của pháp luật phải được áp dụng biện pháp mã hóa, bảo vệ khi truyền qua mạng và khi lưu trữ theo yêu cầu của pháp luật có liên quan.

Điều 11. Quản lý sự thay đổi hệ thống thông tin

1. Có quy định để bảo đảm hệ thống hoạt động ổn định, an toàn khi thay đổi các phần mềm hệ thống như hệ điều hành, hệ quản trị cơ sở dữ liệu.

2. Kiểm soát chặt chẽ việc sửa đổi mã nguồn phần mềm.

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

Điều 12. Quản lý rủi ro an ninh mạng

1. Chủ quản hệ thống thông tin có trách nhiệm tổ chức quản lý rủi ro an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý trong toàn bộ vòng đời của hệ thống thông tin.

2. Việc quản lý rủi ro bao gồm xác định tài sản, nguy cơ, mối đe dọa, điểm yếu, lỗ hổng, khả năng xảy ra và mức độ ảnh hưởng; phân tích, đánh giá, xử lý, theo dõi và trao đổi thông tin về rủi ro.

3. Căn cứ kết quả đánh giá rủi ro, chủ quản, đơn vị vận hành xác định biện pháp xử lý rủi ro, thứ tự ưu tiên, trách nhiệm, nguồn lực và thời hạn thực hiện; tổ chức theo dõi, kiểm tra việc thực hiện.

4. Việc đánh giá, rà soát rủi ro được thực hiện định kỳ theo quy định của pháp luật và khi có thay đổi về hệ thống thông tin, thông tin, dữ liệu, môi trường vận hành; khi phát hiện điểm yếu, lỗ hổng, nguy cơ, sự cố hoặc có yêu cầu của cơ quan có thẩm quyền.

5. Hồ sơ quản lý rủi ro phải được lập, cập nhật và quản lý theo quy định; là căn cứ để xác định, điều chỉnh biện pháp bảo đảm an ninh mạng và phương án ứng phó, khắc phục sự cố và rà soát, cập nhật hồ sơ đề xuất cấp độ.

Điều 13. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

4. Có đơn vị độc lập hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

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

Điều 14. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Xây dựng quy định về bảo đảm an ninh mạng khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

2. Xây dựng quy trình xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

3. Phương án kỹ thuật thực hiện xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

Mục 2

BẢO ĐẢM AN NINH MẠNG TRONG QUẢN LÝ, VẬN HÀNH, DUY TRÌ HỆ THỐNG THÔNG TIN

Điều 15. Trách nhiệm quản lý và quy trình vận hành của đơn vị

1. Ban hành các quy trình vận hành hệ thống thông tin, tối thiểu bao gồm: Quy trình khởi động, đóng hệ thống; quy trình sao lưu, phục hồi dữ liệu; quy trình vận hành ứng dụng; quy trình xử lý sự cố; quy trình giám sát và ghi nhật ký hoạt động của hệ thống.

2. Kiểm soát sự thay đổi của phiên bản phần mềm, cấu hình phần cứng, quy trình vận hành: ghi chép lại các thay đổi; lập kế hoạch, thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả và phải được phê duyệt trước khi áp dụng chính thức.

3. Hệ thống thông tin vận hành chính thức phải đáp ứng yêu cầu:

a) Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm.

b) Có biện pháp, giải pháp bảo đảm an ninh mạng.

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng trên hệ thống vận hành chính thức.

Điều 16. Quản lý tài sản công nghệ thông tin

1. Tài sản công nghệ thông tin thuộc hệ thống thông tin hoặc thuộc phạm vi quản lý của đơn vị bao gồm:

a) Tài sản phần cứng: hạ tầng kỹ thuật, thiết bị công nghệ thông tin, thiết bị mạng, thiết bị lưu trữ, thiết bị đầu cuối, đường truyền, vật mang tin và tài sản vật lý khác;

b) Tài sản phần mềm: hệ điều hành, phần mềm hệ thống, phần mềm ứng dụng, công cụ quản trị, phần mềm bảo đảm an ninh mạng và các phần mềm khác;

c) Tài sản thông tin: cơ sở dữ liệu, thông tin, dữ liệu số, tài khoản, thông tin cấu hình, dữ liệu nhật ký và các thông tin, dữ liệu khác.

2. Chủ quản, đơn vị vận hành hệ thống thông tin có trách nhiệm kiểm kê, lập, cập nhật và quản lý danh mục tài sản công nghệ thông tin thuộc phạm vi được giao quản lý, vận hành hoặc khai thác; xác định rõ đơn vị, cá nhân chịu trách nhiệm quản lý đối với từng tài sản.

3. Việc quản lý tài sản công nghệ thông tin phải được thực hiện trong toàn bộ vòng đời từ đầu tư, tiếp nhận, đưa vào sử dụng, vận hành, bảo trì, nâng cấp, chuyển giao, thu hồi, thanh lý hoặc hủy bỏ; gắn với yêu cầu bảo đảm an ninh mạng và bảo vệ thông tin, dữ liệu.

4. Chủ quản, đơn vị vận hành hệ thống thông tin áp dụng biện pháp quản lý, bảo vệ phù hợp đối với từng loại tài sản; kiểm soát việc cài đặt, kết nối, sử dụng, bảo trì, thay thế và đưa tài sản ra ngoài trụ sở. Không kết nối hoặc sử dụng thiết bị, phần mềm, tài khoản hoặc dịch vụ không được phép theo quy định.

5. Khi chuyển giao, thu hồi, tái sử dụng, thanh lý hoặc xử lý tài sản công nghệ thông tin có lưu trữ thông tin, dữ liệu, đơn vị có trách nhiệm thực hiện biện pháp sao lưu, bàn giao, xóa dữ liệu hoặc hủy thiết bị, vật mang tin theo quy định, bảo đảm thông tin, dữ liệu không bị lộ, mất và không thể bị khôi phục trái phép.

6. Việc kiểm kê, rà soát, cập nhật danh mục tài sản công nghệ thông tin được thực hiện định kỳ hoặc khi có thay đổi; là cơ sở để tổ chức bảo vệ, đánh giá rủi ro, giám sát và xử lý sự cố an ninh mạng.

Điều 17. Xây dựng quy trình bảo đảm hoạt động liên tục

1. Xây dựng quy trình xử lý các tình huống gián đoạn hoạt động của từng cấu phần trong hệ thống thông tin.

2. Quy trình xử lý phải được kiểm tra và cập nhật khi có sự thay đổi của hệ thống thông tin, cơ cấu tổ chức, nhân sự và phân công trách nhiệm của các bộ phận có liên quan trong đơn vị.

3. Hệ thống dự phòng cần được định kỳ kiểm tra để luôn bảo đảm tính sẵn sàng khi xảy ra các sự cố an ninh mạng.

Điều 18. Quản lý, vận hành hoạt động bình thường của hệ thống

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

2. Quản lý các thay đổi cấu hình kỹ thuật; thường xuyên cập nhật các bản vá lỗi và loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

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

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

5. Sử dụng các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng theo yêu cầu bảo vệ tương ứng với cấp độ hệ thống thông tin.

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

7. Đối với hệ thống có kết nối Internet, bố trí kết nối dự phòng đáp ứng yêu cầu bảo vệ tương ứng với cấp độ hệ thống thông tin và yêu cầu duy trì hoạt động liên tục. Trường hợp phương án bảo đảm an ninh mạng được phê duyệt yêu cầu duy trì ít nhất 02 kết nối Internet, các kết nối phải sử dụng hạ tầng kết nối của các nhà cung cấp dịch vụ Internet khác nhau.

Điều 19. Sao lưu dự phòng

1. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo mức độ quan trọng, 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.

2. Dữ liệu của các hệ thống thông tin quan trọng phải được sao lưu ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực tiến hành sao lưu. Kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu 06 tháng một lần.

3. Cần tách biệt giữa sao lưu dữ liệu và sao lưu ứng dụng. Việc sao lưu ứng dụng được thực hiện theo yêu cầu khôi phục hệ thống bảo đảm khả năng khôi phục khi việc cài đặt, cập nhật hoặc gỡ bỏ ứng dụng gây sự cố.

Điều 20. Bảo đảm an ninh mạng về vật lý và môi trường

1. Chủ quản hệ thống thông tin, đơn vị vận hành có trách nhiệm áp dụng biện pháp bảo vệ phù hợp đối với khu vực đặt hạ tầng kỹ thuật, thiết bị công nghệ thông tin, thiết bị mạng, thiết bị lưu trữ, đường truyền và tài sản công nghệ thông tin khác thuộc phạm vi quản lý, vận hành hoặc khai thác.

2. Khu vực có yêu cầu bảo vệ cao, bao gồm khu vực đặt máy chủ, thiết bị lưu trữ, thiết bị bảo đảm an ninh mạng, thiết bị mạng, thiết bị truyền thông và tài sản công nghệ thông tin quan trọng khác, phải được bố trí phù hợp; có biện pháp kiểm soát người, phương tiện và hoạt động ra, vào khu vực.

3. Việc ra, vào, làm việc, lắp đặt, bảo trì, sửa chữa, thay thế hoặc di chuyển tài sản công nghệ thông tin tại khu vực có yêu cầu bảo vệ cao phải được thực hiện theo thẩm quyền, nhiệm vụ được giao và quy định của pháp luật.

4. Áp dụng biện pháp phòng ngừa, phát hiện và xử lý nguy cơ ảnh hưởng đến an ninh mạng, an toàn hoạt động của hệ thống thông tin do cháy, nổ, ngập nước, nhiệt độ, độ ẩm, mất điện, sét, thiên tai và các yếu tố môi trường khác.

5. Đơn vị vận hành có trách nhiệm thường xuyên kiểm tra tình trạng bảo vệ vật lý và môi trường; kịp thời xử lý hoặc báo cáo chủ quản hệ thống thông tin và đơn vị có thẩm quyền khi phát hiện nguy cơ, sự cố có thể ảnh hưởng đến hoạt động của hệ thống thông tin.

Điều 21. Giám sát và ghi nhật ký hoạt động của hệ thống

1. Ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin.

2. Thực hiện các biện pháp giám sát, phân tích nhật ký, cảnh báo rủi ro, xử lý và báo cáo kết quả.

3. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

4. Thực hiện việc đồng bộ thời gian giữa các hệ thống thông tin.

Điều 22. Quản lý nhân sự trong hoạt động an ninh mạng

1. Các đơn vị bố trí nhân sự thực hiện nhiệm vụ bảo đảm an ninh mạng phù hợp với chức năng, nhiệm vụ, vị trí việc làm, yêu cầu chuyên môn và mức độ bảo vệ hệ thống thông tin thuộc phạm vi quản lý.

2. Việc phân công nhiệm vụ cho đơn vị vận hành, người quản trị, đầu mối an ninh mạng và cá nhân có liên quan phải xác định rõ trách nhiệm, phạm vi quyền hạn và yêu cầu bảo đảm an ninh mạng.

3. Cá nhân được giao thực hiện nhiệm vụ có liên quan đến quản trị, vận hành, bảo đảm an ninh mạng, quản lý dữ liệu hoặc quyền truy cập phải tuân thủ quy định về bảo vệ bí mật nhà nước, bí mật công tác, bảo vệ dữ liệu cá nhân và các quy định của pháp luật có liên quan.

4. Khi cá nhân thay đổi vị trí công tác, nghỉ hưu, thôi việc hoặc không còn được giao nhiệm vụ liên quan, đơn vị có trách nhiệm tổ chức bàn giao công việc, tài sản, thông tin, dữ liệu; kịp thời điều chỉnh, khóa hoặc thu hồi tài khoản, quyền truy cập không còn phù hợp. Việc bàn giao phải bảo đảm duy trì hoạt động của hệ thống và bảo mật thông tin xác thực.

5. Các đơn vị tổ chức đào tạo, bồi dưỡng, cập nhật kiến thức, kỹ năng về an ninh mạng cho người quản trị, nhân sự vận hành và cá nhân có liên quan phù hợp với nhiệm vụ được giao.

Mục 3

BẢO ĐẢM AN NINH MẠNG ĐỐI VỚI THIẾT BỊ ĐẦU CUỐI

Điều 23. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối.

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa.

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống.

4. Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

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

Điều 24. Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Quản lý truy cập, sử dụng tài nguyên nội bộ.

2. Quản lý truy cập mạng và tài nguyên trên Internet.

3. Cài đặt và sử dụng máy tính an toàn.

Điều 25. 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 máy tính, máy chủ và thiết bị di động (máy tính xách tay, máy tính bảng, điện thoại di động…).

2. Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên các thiết bị đầu cuối; 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 thiết bị đầu cuối.

Điều 26. Trách nhiệm của cá nhân

1. Gắn trách nhiệm cho cá nhân quản lý, sử dụng thiết bị đầu cuối.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ thiết bị đầu cuối:

a) Cá nhân chỉ cài đặt phần mềm hợp pháp trên máy tính và thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

d) Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý và thực hiện các biện pháp bảo đảm an ninh mạng cho thiết bị lưu trữ di động như mã hóa dữ liệu, quét mã độc định kỳ.

đ) Khóa màn hình khi rời vị trí làm việc; đăng xuất, tắt thiết bị theo quy trình vận hành, bảo đảm kiểm soát truy cập và yêu cầu hoạt động liên tục của hệ thống.

Điều 27. Trách nhiệm của đơn vị

1. Xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn người dùng cách sử dụng, quản lý, vận hành thiết bị đầu cuối.

2. Thực hiện định kỳ kiểm tra công tác bảo đảm an ninh mạng đối với thiết bị đầu cuối.

Mục 4

BIỆN PHÁP QUẢN LÝ TRUY CẬP MẠNG

Điều 28. Yêu cầu nghiệp vụ đối với kiểm soát truy cập

1. Quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng, các thiết bị, công cụ sử dụng để truy cập bảo đảm đáp ứng yêu cầu nghiệp vụ và yêu cầu an ninh mạng, bao gồm các nội dung cơ bản sau:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập.

b) Giới hạn và kiểm soát các truy cập sử dụng tài khoản quản trị hệ thống.

c) Quản lý việc tạo lập, cấp phát, sử dụng, thay đổi, thu hồi và bảo vệ mật khẩu, khóa mật mã và các thông tin xác thực khác phục vụ truy cập mạng, hệ điều hành, hệ thống thông tin và ứng dụng.

d) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng.

đ) Yêu cầu, điều kiện an toàn, an ninh đối với các thiết bị, công cụ sử dụng để truy cập.

2. Quy định về quản lý mật khẩu, khóa mật mã và các thông tin xác thực khác phải đáp ứng các yêu cầu sau:

a) Phân biệt mật khẩu dùng để xác thực người sử dụng, khóa mật mã dùng trong hoạt động mật mã và các thông tin xác thực khác; xác định yêu cầu quản lý, bảo vệ phù hợp với từng loại và mục đích sử dụng.

b) Quy định yêu cầu về độ dài, chất lượng mật khẩu và kiểm tra tự động khi thiết lập; thay đổi mật khẩu mặc định trước khi đưa thiết bị, phần mềm, cơ sở dữ liệu vào sử dụng. Khóa mật mã, thông tin xác thực mặc định phải được thay thế hoặc xử lý theo hướng dẫn kỹ thuật và yêu cầu bảo vệ của hệ thống.

c) Việc truyền mật khẩu, thông tin xác thực bí mật qua mạng thực hiện theo điểm b khoản 2 Điều 8 của Quy chế này; việc lưu trữ phải áp dụng biện pháp bảo vệ phù hợp, không lưu ở dạng bản rõ.

d) Việc quản lý, bảo vệ khóa mật mã và các thông tin xác thực bí mật khác thực hiện theo Điều 10 của Quy chế này; kiểm soát quyền tiếp cận, không sử dụng chung giữa các chủ thể không được phép và kịp thời thay đổi, thu hồi khi có nguy cơ bị lộ hoặc không còn nhu cầu sử dụng.

3. Người sử dụng, người quản trị và cá nhân được giao quản lý mật khẩu, khóa mật mã, thông tin xác thực có trách nhiệm bảo vệ thông tin được giao; không cung cấp cho người không có thẩm quyền; thông báo ngay khi phát hiện hoặc nghi ngờ bị lộ, mất, sử dụng trái phép.

Điều 29. Quy định về kiểm soát truy cập mạng

1. Đơn vị phải ban hành các quy định về quản lý kết nối, truy cập, trách nhiệm cá nhân của người sử dụng khi truy cập, sử dụng các hệ thống mạng, hệ thống thông tin sau:

a) Mạng Internet.

b) Mạng nội bộ.

c) Hệ thống thông tin và các ứng dụng.

2. Đơn vị phải có biện pháp kiểm soát, bảo đảm người sử dụng tuân thủ các quy định đề ra.

3. Quản lý truy cập và cấu hình hệ thống

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

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

c) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy cập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho các thiết bị mạng, bảo mật trong hệ thống cần được thực hiện trước khi đưa hệ thống vào vận hành, khai thác.

Mục 5

QUẢN LÝ, SỬ DỤNG HỆ THỐNG MẠNG MÁY TÍNH

Điều 30. Quản lý, sử dụng mạng nội bộ (LAN)

1. Mạng nội bộ được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an ninh mạng riêng), bao gồm: vùng mạng người dùng, vùng mạng kết nối Internet và các mạng khác (nếu có), vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ, vùng mạng quản trị.

2. Các đơn vị, cá nhân tham gia sử dụng mạng nội bộ có trách nhiệm:

a) Thực hiện các biện pháp, giải pháp để phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

b) Không tiết lộ thiết kế, thông số cấu hình hệ thống mạng nội bộ cho tổ chức, cá nhân khác khi chưa được phép của cấp có thẩm quyền; không được phép truy cập bất hợp pháp vào các khu vực không được cấp quyền.

c) Không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

Điều 31. Quản lý, sử dụng mạng diện rộng (WAN) Bộ Xây dựng

1. Trung tâm Công nghệ thông tin quy hoạch và quản lý tài nguyên địa chỉ IP của mạng WAN Bộ Xây dựng. Các cơ quan, đơn vị sử dụng địa chỉ IP được cấp bảo đảm đúng quy định.

2. Thông tin được sử dụng, chia sẻ và lưu trữ trên mạng WAN Bộ Xây dựng

phải là thông tin phục vụ công tác chỉ đạo, điều hành của Lãnh đạo Bộ Xây dựng và chuyên môn, nghiệp vụ của các cơ quan, đơn vị thuộc Bộ. Thông tin, dữ liệu phải bảo mật theo quy định của pháp luật phải được áp dụng các biện pháp bảo vệ phù hợp. Việc truyền nhận, lưu trữ thông tin, dữ liệu chứa bí mật nhà nước chỉ được thực hiện trên hệ thống đáp ứng yêu cầu bảo vệ bí mật nhà nước và được bảo mật bằng giải pháp mật mã cơ yếu theo quy định.

Điều 32. Quản lý, sử dụng mạng không dây (Wifi)

1. Mạng Wifi kết nối ra Internet phải thiết lập phân vùng riêng, không được phép truy cập bất hợp pháp vào các phân vùng khác.

2. Mạng Wifi chỉ được sử dụng cho mục đích công việc tại cơ quan, đơn vị, không dùng cho các hoạt động cá nhân không liên quan.

3. Cá nhân không tự ý lắp đặt các thiết bị phát sóng Wifi tại cơ quan, đơn vị, bộ phận vận hành định kỳ kiểm tra các thiết bị phát sóng kết nối vào mạng để phát hiện và ngăn chặn các thiết bị không được ủy quyền.

4. Đối với mạng sử dụng mật khẩu dùng chung, sử dụng mật khẩu Wifi phải có tối thiểu 08 ký tự, trong đó có các loại ký tự sau: chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 - 9) và các ký tự đặc biệt khác trên bàn phím máy tính. Định kỳ thay đổi mật khẩu 03 tháng/01 lần và ngay khi có nguy cơ bị lộ.

Điều 33. Quản lý, sử dụng mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước

Bảo đảm an ninh mạng đối với Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước thực hiện theo quy định tại Điều 7, Điều 8 của Quyết định số 33/2025/QĐ-TTg ngày 15 tháng 9 năm 2025 của Thủ tướng Chính phủ về mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước.

Điều 34. Quản lý, sử dụng hệ thống mạng kết nối Internet

1. Áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an ninh mạng trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau:

a) Có hệ thống tường lửa và hệ thống bảo vệ các vùng truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng, có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ.

b) Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

2. Cá nhân sử dụng mạng máy tính có kết nối Internet, sử dụng tài khoản truy cập hệ thống qua mạng riêng ảo phải tuân thủ quy định tại Quy chế này. Khi phát hiện các nguy cơ mất an toàn, an ninh mạng, kịp thời thông báo cho bộ phận chuyên trách về an ninh mạng của đơn vị để xử lý.

Điều 35. Quản lý, sử dụng hệ thống mạng gửi, nhận văn bản mật

Hệ thống mạng gửi, nhận văn bản mật Bộ Xây dựng bao gồm: Phần mềm quản lý văn bản mật của Chính phủ phân quyền quản trị, sử dụng cho Bộ Xây dựng; thiết bị đầu cuối và hạ tầng mạng truyền dẫn văn bản mật.

1. Bảo đảm hạ tầng kỹ thuật

a) Văn phòng Bộ tổng hợp nhu cầu thiết bị đầu cuối; tổ chức trang bị theo nhiệm vụ, thẩm quyền được giao để phục vụ gửi, nhận văn bản mật tại cơ quan Bộ. Văn phòng Bộ hướng dẫn nghiệp vụ tiếp nhận, phát hành, sao, chụp văn bản, tài liệu chứa bí mật nhà nước trong quá trình sử dụng phần mềm quản lý văn bản mật theo quy định.

b) Các đơn vị (trừ các cơ quan tham mưu, giúp việc Bộ trưởng) có trách nhiệm triển khai, quản lý, sử dụng và bảo đảm an ninh mạng thiết bị đầu cuối thuộc phạm vi đơn vị; hạ tầng truyền dẫn từ đơn vị đến Bộ phục vụ công tác gửi, nhận văn bản mật của đơn vị.

c) Thiết bị đầu cuối phục vụ công tác gửi, nhận văn bản mật phải đáp ứng yêu cầu kỹ thuật theo quy định; được cài đặt hệ điều hành, phần mềm bảo mật ngành cơ yếu, phần mềm ứng dụng và được kiểm tra an ninh mạng trước khi đưa vào sử dụng, trừ các trường hợp được cơ quan có thẩm quyền xác định không phải thực hiện kiểm tra.

d) Trung tâm Công nghệ thông tin chủ trì kết nối, vận hành kỹ thuật và bảo đảm an ninh mạng Hệ thống mạng gửi, nhận văn bản mật tại Bộ Xây dựng thông qua mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước và được bảo mật bằng giải pháp mật mã cơ yếu theo quy định.

2. Tạo lập, phân quyền, quản lý tài khoản

a) Trung tâm Công nghệ thông tin thực hiện tạo lập tài khoản sử dụng hệ thống cho người dùng trong phạm vi quản lý theo đề nghị của Văn phòng Bộ bằng tài khoản quản trị của Bộ được phân cấp.

b) Mỗi đơn vị, cá nhân chỉ được cấp duy nhất một tài khoản sử dụng (cho mỗi vai trò được giao) gắn liền với thông tin đơn vị, cá nhân. Tài khoản khi cấp mới chỉ được cấp đúng và đủ quyền hạn theo vai trò công việc được giao, không cấp thừa quyền nhằm hạn chế rủi ro lộ lọt dữ liệu.

c) Tài khoản chỉ được cấp cho người sử dụng đã được cơ quan có thẩm quyền xét duyệt theo quy định của pháp luật về bảo vệ bí mật nhà nước, đã cam kết bảo vệ bí mật nhà nước và đã được tập huấn sử dụng hệ thống.

d) Tài khoản phải được khóa hoặc thu hồi ngay khi người sử dụng nghỉ hưu, thôi việc, chuyển công tác hoặc không còn được giao nhiệm vụ liên quan; khóa tạm thời khi đăng nhập sai quá số lần quy định; tự động kết thúc phiên làm việc khi không có thao tác quá thời gian quy định.

đ) Định kỳ tối thiểu 06 tháng một lần hoặc khi phát hiện quyền truy cập của người dùng không còn phù hợp, Văn phòng Bộ và các đơn vị gửi danh sách tài khoản của người dùng và đề nghị điều chỉnh cho Trung tâm Công nghệ thông tin thực hiện theo phân cấp.

3. Quản lý, vận hành hệ thống

Việc quản lý, vận hành Hệ thống phải bảo đảm:

a) Phân định rõ trách nhiệm, quyền hạn của từng cá nhân; thực hiện phân

quyền, kiểm soát truy cập, không giao một cá nhân quản trị toàn bộ các chức năng an ninh mạng.

b) Kiểm soát chặt chẽ việc thay đổi cấu hình, phần mềm, phần cứng và quy trình vận hành; giám sát hoạt động quản trị, truy cập, khai thác và sử dụng hệ thống.

c) Thực hiện các biện pháp bảo đảm an ninh truy cập, đăng nhập và tính sẵn sàng của hệ thống.

d) Có phương án xử lý khi xảy ra sự cố an ninh mạng hoặc gián đoạn hoạt động của hệ thống.

đ) Không tự ý thay đổi cấu hình, cài đặt phần mềm, kết nối thiết bị, mạng hoặc thực hiện thao tác có khả năng làm thay đổi mức độ an ninh mạng của Hệ thống khi chưa được phép.

e) Các đơn vị, cá nhân sử dụng hệ thống phải sử dụng đúng tài khoản, quyền hạn và mục đích; bảo vệ thông tin xác thực, thiết bị và thông tin mật; không chia sẻ tài khoản, thông tin xác thực hoặc cho phép người không có thẩm quyền truy cập hệ thống.

g) Khi phát hiện dấu hiệu mất an ninh mạng, truy cập trái phép, lộ, mất thông tin mật hoặc sự cố, phải kịp thời dừng, ngắt kết nối hoặc cô lập hoạt động có nguy cơ gây mất an toàn; thông báo ngay cho Trung tâm Công nghệ thông tin và cơ quan chức năng theo Điều 46 của Quy chế này để thực hiện ứng cứu, khắc phục theo quy định.

Mục 6

QUẢN LÝ SỰ CỐ AN NINH MẠNG

Điều 36. Nguyên tắc kiểm soát và khắc phục sự cố

1. Các sự cố mất an ninh mạng phải được thông báo ngay đến đầu mối theo điểm a khoản 2 Điều 46.

2. Xác định nguyên nhân và thực hiện các biện pháp phòng ngừa.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ. Thực hiện biện pháp bảo vệ, chống chỉnh sửa, hủy hoại đối với tài liệu lưu trữ về sự cố.

4. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố.

Điều 37. Quản lý sự cố

Quản lý sự cố an ninh mạng bao gồm các nội dung:

1. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an ninh mạng.

2. Kế hoạch ứng phó sự cố an ninh mạng.

3. Giám sát, phát hiện và cảnh báo sự cố an ninh mạng.

4. Quy trình ứng cứu sự cố an ninh mạng.

5. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an ninh mạng.

6. Định kỳ tổ chức diễn tập phương án xử lý sự cố an ninh mạng.

Điều 38. Quy trình xử lý sự cố

Khi xảy ra sự cố an ninh mạng, thực hiện theo quy trình sau:

Bước 1. Phát hiện, tiếp nhận thông tin nguy cơ, sự cố.

Bước 2. Xác minh sự cố.

Bước 3. Phân tích, phân loại sự cố.

Bước 4. Xử lý ban đầu, cô lập và bảo toàn.

Bước 5. Xác định phương án điều phối, ứng cứu sự cố.

Bước 6. Khắc phục, khôi phục và kiểm tra kết quả.

Bước 7. Tổng kết, báo cáo và lưu hồ sơ sự cố.

(Quy trình chi tiết thực hiện theo Phụ lục I kèm theo Quy chế này.)

Điều 39. Ứng phó sự cố an ninh mạng

1. Kế hoạch ứng phó sự cố bảo đảm an ninh mạng

a) Hằng năm, các đơn vị tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố an ninh mạng cho các hệ thống thông tin do đơn vị mình trực tiếp quản lý. Tổ chức triển khai kế hoạch sau khi được phê duyệt.

b) Kế hoạch ứng phó sự cố của đơn vị phải gửi cho Trung tâm Công nghệ thông tin trước ngày 31 tháng 10 hằng năm để tổng hợp thành kế hoạch chung của Bộ. Trung tâm Công nghệ thông tin có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Bộ Xây dựng, trình Lãnh đạo Bộ phê duyệt.

2. Cập nhật, sao lưu dự phòng và khôi phục hệ thống

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

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính theo yêu cầu bảo vệ tương ứng với cấp độ hệ thống thông tin, bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c) Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 12 tháng.

d) Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống phù hợp với tính chất, yêu cầu bảo vệ của thông tin, dữ liệu và cấp độ hệ thống thông tin.

3. Diễn tập bảo đảm an ninh mạng

a) Chủ quản hệ thống thông tin tổ chức diễn tập bảo đảm an ninh mạng theo kế hoạch ứng phó sự cố an ninh mạng của đơn vị được phê duyệt. Tham gia các cuộc diễn tập bảo đảm an ninh mạng do Bộ Công an và Bộ Xây dựng tổ chức.

b) Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị thuộc Bộ tổ chức diễn tập bảo đảm an ninh mạng chung của Bộ.

Mục 7

KIỂM TRA, GIÁM SÁT AN NINH MẠNG

Điều 40. Quản lý điểm yếu an ninh mạng

Chính sách, quy trình quản lý điểm yếu an ninh mạng bao gồm các nội dung:

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. Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an ninh mạng.

4. Kiểm tra, đánh giá và xử lý điểm yếu an ninh mạng cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

Điều 41. Kiểm tra, đánh giá an ninh mạng

1. Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo, tổ chức thực hiện kiểm tra, đánh giá an ninh mạng trong phạm vi cơ quan, tổ chức mình. Việc kiểm tra, đánh giá có thể do bộ phận hoặc đơn vị nội bộ độc lập với đơn vị vận hành thực hiện, tuân thủ biểu mẫu, tiêu chí và phương pháp đánh giá theo quy định. Đối với hệ thống thông tin cấp độ 5, hệ thống thông tin quan trọng về an ninh quốc gia và các trường hợp khác quy định tại điểm c khoản 2 Điều 31 Nghị định số 331/2026/NĐ-CP, việc kiểm tra, đánh giá phải do tổ chức chuyên môn đáp ứng điều kiện quy định tại điểm này thực hiện.

2. Nội dung kiểm tra, đánh giá an ninh mạng bao gồm: kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an ninh mạng hệ thống thông tin theo cấp độ; kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng theo phương án bảo đảm an ninh mạng được phê duyệt; kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

3. Định kỳ kiểm tra, đánh giá an ninh mạng, như sau:

- Định kỳ 02 năm thực hiện kiểm tra, đánh giá an ninh mạng tổng thể trong hoạt động của cơ quan, tổ chức mình.

- Định kỳ hằng năm thực hiện kiểm tra, đánh giá an ninh mạng đối với các hệ thống cấp độ 3 và cấp độ 4.

- Định kỳ 06 tháng (hoặc đột xuất khi thấy cần thiết hoặc theo yêu cầu, cảnh báo của cơ quan chức năng) thực hiện kiểm tra, đánh giá an ninh mạng đối với hệ thống cấp độ 5.

Điều 42. Giám sát an ninh mạng

1. Nguyên tắc giám sát

a) Bảo đảm được thực hiện thường xuyên, liên tục.

b) Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố an ninh mạng.

c) Bảo đảm hoạt động ổn định, bí mật cho thông tin được cung cấp, trao đổi trong quá trình giám sát.

2. Yêu cầu giám sát

a) Chủ quản hệ thống thông tin có trách nhiệm chủ động thực hiện giám sát an ninh mạng đối với các hệ thống thông tin do mình quản lý theo quy định hiện hành.

b) Đối với hệ thống thông tin cấp độ 3 trở lên, kết nối chia sẻ thông tin giám sát an ninh mạng với Hệ thống giám sát an ninh mạng tập trung của Bộ Xây dựng.

c) Chủ quản hệ thống thông tin có trách nhiệm cử cá nhân hoặc bộ phận làm đầu mối giám sát, cảnh báo an ninh mạng để phối hợp với các cơ quan chức năng liên quan.

3. Quản lý giám sát

Chính sách, quy trình quản lý giám sát an ninh mạng bao gồm các nội dung sau:

a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát.

b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có).

c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

d) Truy cập và quản trị hệ thống giám sát.

đ) Loại thông tin cần được giám sát.

e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống).

g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát.

h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.

i) Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin phù hợp với yêu cầu bảo vệ an ninh mạng theo cấp độ, tính chất và thời gian hoạt động của hệ thống thông tin.

Mục 8

XÁC ĐỊNH CẤP ĐỘ AN NINH MẠNG

Điều 43. Trách nhiệm của chủ quản hệ thống thông tin, đơn vị vận hành hệ thống và đơn vị chuyên trách về an ninh mạng

1. Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo đơn vị vận hành hệ thống thông tin xác định, lập hồ sơ đề xuất cấp độ hệ thống thông tin, hệ thống thông tin quan trọng về an ninh quốc gia; tổ chức thẩm định và phê duyệt hồ sơ đề xuất cấp độ theo quy định tại Nghị định số 331/2026/NĐ-CP.

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm xác định, lập hồ sơ đề xuất cấp độ hệ thống thông tin thuộc phạm vi quản lý, trình cấp có thẩm quyền thẩm định, phê duyệt.

3. Đơn vị chuyên trách về an ninh mạng

Trung tâm Công nghệ thông tin là đơn vị chuyên trách về an ninh mạng của Bộ, có trách nhiệm thẩm định hồ sơ đề xuất cấp độ 3; cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ 4, cấp độ 5; thẩm định, phê duyệt hồ sơ đề xuất cấp độ 1, cấp độ 2 đối với các hệ thống thông tin do Bộ Xây dựng làm chủ quản.

Điều 44. Trình tự, thủ tục xác định cấp độ hệ thống thông tin

1. Trình tự, thủ tục xác định cấp độ đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin thực hiện theo quy định tại Điều 19 Nghị định số 331/2026/NĐ-CP.

2. Trình tự, thủ tục xác định cấp độ đối với hệ thống thông tin đang vận hành thực hiện theo quy định tại Điều 20 Nghị định số 331/2026/NĐ-CP.

3. Trình tự, thủ tục xác định lại cấp độ đối với hệ thống thông tin đã được phê duyệt cấp độ thực hiện theo quy định tại Điều 25 Nghị định số 331/2026/NĐ-CP.

Mục 9

TRAO ĐỔI THÔNG TIN VÀ BÁO CÁO

Điều 45. Trao đổi thông tin

Khi trao đổi thông tin, đơn vị có trách nhiệm:

1. Bảo đảm tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

2. Thông tin, dữ liệu phải bảo mật theo quy định của pháp luật và được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính. Đối với thông tin, dữ liệu chứa bí mật nhà nước, thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

Điều 46. Chế độ báo cáo

Cơ quan, đơn vị thuộc Bộ có trách nhiệm gửi báo cáo về Bộ Xây dựng (qua Trung tâm Công nghệ thông tin) như sau:

1. Báo cáo định kỳ hằng năm.

- Thời hạn gửi báo cáo: trước ngày 15 tháng 12 hằng năm.

- Nội dung và biểu mẫu báo cáo thực hiện theo Phụ lục II kèm theo Quy chế này.

2. Báo cáo đột xuất

a) Báo cáo sự cố an ninh mạng: Khi phát hiện sự cố an ninh mạng, đơn vị phát hiện thông báo ngay cho chủ quản hệ thống thông tin, đơn vị vận hành và Trung tâm Công nghệ thông tin để phối hợp xử lý. Chủ quản hệ thống thông tin thực hiện thông báo, báo cáo cơ quan có thẩm quyền theo thời hạn và nội dung quy định tại điểm d khoản 2 Điều 31 Nghị định số 331/2026/NĐ-CP; đồng thời gửi Trung tâm Công nghệ thông tin để phối hợp, tổng hợp. Đơn vị vận hành và các đơn vị có liên quan cung cấp kịp thời thông tin, kết quả xác minh, xử lý và tài liệu phục vụ báo cáo. Trung tâm Công nghệ thông tin tiếp nhận thông tin, phối hợp xử lý và tổng hợp, báo cáo Bộ theo nhiệm vụ được giao. Các thông tin chưa xác định được tiếp tục cập nhật trong quá trình xử lý.

Nội dung báo cáo:

- Nội dung vụ, việc.

- Thời gian, địa điểm phát sinh vụ, việc.

- Nguyên nhân xảy ra vụ, việc (nếu có).

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống thông tin và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan.

- Các biện pháp đơn vị đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro.

- Kiến nghị, đề xuất (nếu có).

b) Các trường hợp đột xuất khác theo chuyên đề, đơn vị thực hiện theo nội dung, thời hạn và biểu mẫu kèm theo yêu cầu.

Chương III

ĐIỀU KHOẢN THI HÀNH

Điều 47. Trách nhiệm thi hành

1. Trung tâm Công nghệ thông tin có trách nhiệm:

a) Theo dõi, tổng hợp báo cáo Bộ Xây dựng tình hình thực hiện công tác bảo đảm an ninh mạng của các đơn vị theo quy định tại Quy chế này.

b) Hằng năm lập kế hoạch và kiểm tra việc thực hiện Quy chế này tại các đơn vị.

c) Chủ trì, phối hợp với các đơn vị liên quan thuộc Bộ Xây dựng xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Quy chế này.

2. Các đơn vị thuộc Bộ có trách nhiệm:

a) Tổ chức thực hiện Quy chế này.

b) Các đơn vị (không bao gồm các Vụ tham mưu giúp việc Bộ trưởng) rà soát, cập nhật, ban hành quy định bảo đảm an ninh mạng riêng của đơn vị, phù hợp với Quy chế này.

3. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị phản ánh kịp thời về Bộ Xây dựng (qua Trung tâm Công nghệ thông tin) để xem xét, bổ sung, sửa đổi./.

Phụ lục I

QUY TRÌNH ỨNG CỨU SỰ CỐ AN NINH MẠNG BỘ XÂY DỰNG

1. Lưu đồ điều phối, ứng cứu sự cố an ninh mạng

Bước	Quy trình thực hiện	Đơn vị thực hiện
Bước 1	**Phát hiện, tiếp nhận thông tin nguy cơ, sự cố**	Người phát hiện; đơn vị vận hành; đầu mối an ninh mạng
Bước 2	**Xác minh sự cố** Kiểm tra thông tin, phạm vi và dấu hiệu ảnh hưởng Không phải sự cố → **Kết thúc** Có sự cố	Đơn vị vận hành; đơn vị chủ quản; Trung tâm CNTT khi cần
Bước 3	**Phân tích, phân loại sự cố** Đánh giá mức độ, phạm vi, dữ liệu và dịch vụ bị ảnh hưởng	Đơn vị chủ quản; đơn vị vận hành; Trung tâm CNTT và đơn vị liên quan
Bước 4	**Xử lý ban đầu, cô lập và bảo toàn** Hạn chế lan truyền; bảo vệ dữ liệu; lưu giữ nhật ký, dấu vết và chứng cứ điện tử	Đơn vị vận hành; người quản trị; đơn vị chủ quản
Bước 5	**Xác định phương án điều phối, ứng phó sự cố** Sự cố nghiêm trọng hoặc vượt khả năng xử lý? Có Không hoặc xử lý nội bộ	Đơn vị chủ quản; Trung tâm CNTT; cơ quan có thẩm quyền khi cần
Bước 6	**Khắc phục, khôi phục và kiểm tra kết quả** Xử lý nguyên nhân; khôi phục dữ liệu, cấu hình hoặc dịch vụ; đánh giá điều kiện an toàn trước khi vận hành bình thường	Đơn vị chủ quản; đơn vị vận hành; Trung tâm CNTT và bên liên quan
Bước 7	**Tổng kết, báo cáo và lưu hồ sơ sự cố** Đánh giá nguyên nhân, thiệt hại, biện pháp phòng ngừa tái diễn; cập nhật phương án và hồ sơ quản lý rủi ro **Kết thúc**	Đơn vị chủ quản; đơn vị vận hành; Trung tâm CNTT và đơn vị liên quan

2. Diễn giải lưu đồ

Bước	Đơn vị thực hiện	Nội dung và trình tự thực hiện	Sản phẩm
Bước 1. Phát hiện, tiếp nhận thông tin nguy cơ, sự cố	- Người phát hiện - Đơn vị vận hành - Đầu mối an ninh mạng	1. Người phát hiện nguy cơ, sự cố thông báo ngay cho người quản trị, đơn vị vận hành hoặc đầu mối an ninh mạng của đơn vị. 2. Đơn vị vận hành tiếp nhận, ghi nhận thông tin ban đầu về thời điểm, nguồn tin, hiện tượng, hệ thống hoặc thành phần có liên quan. 3. Thông tin tiếp nhận được kiểm tra, xác thực trước khi thực hiện các bước tiếp theo.	Thông tin sự cố được ghi nhận; hồ sơ hoặc nhật ký tiếp nhận ban đầu.
Bước 2. Xác minh sự cố	- Đơn vị vận hành - Chủ quản hệ thống thông tin - Trung tâm CNTT khi cần thiết	1. Đơn vị vận hành kiểm tra, xác minh tính chính xác của thông tin 2. Xác định sơ bộ thành phần bị ảnh hưởng, dấu hiệu mất an ninh mạng và khả năng ảnh hưởng đến hoạt động của hệ thống. 3. Trường hợp không phải sự cố, ghi nhận kết quả và kết thúc xử lý; trường hợp xác định có sự cố, chuyển sang Bước 3.	Kết quả xác minh sự cố.
Bước 3. Phân tích, phân loại sự cố	- Chủ quản hệ thống thông tin - Đơn vị vận hành - Trung tâm CNTT và đơn vị liên quan khi cần thiết	1. Phân tích nguyên nhân, phạm vi, mức độ ảnh hưởng, dữ liệu, dịch vụ và khả năng lan truyền của sự cố. 2. Xác định khả năng xử lý tại chỗ, nhu cầu phối hợp, điều phối hoặc đề nghị hỗ trợ theo quy định.	Kết quả phân tích, phân loại; đề xuất phương án xử lý.
Bước 4. Xử lý ban đầu, cô lập và bảo toàn	- Đơn vị vận hành - Người quản trị - Chủ quản hệ thống thông tin	1. Thực hiện ngay biện pháp phù hợp để hạn chế lan truyền, ngăn chặn truy cập trái phép, bảo vệ dữ liệu và duy trì hoạt động thiết yếu. 2. Bảo toàn nhật ký, dữ liệu, dấu vết và chứng cứ điện tử trước khi thực hiện biện pháp có thể làm thay đổi hiện trạng hệ thống, trừ trường hợp xử lý khẩn cấp.	Hệ thống hoặc thành phần bị ảnh hưởng được cô lập; nhật ký, dữ liệu, dấu vết liên quan được bảo toàn.
Bước 5. Xác định phương án điều phối, ứng cứu sự	- Chủ quản hệ thống thông tin - Trung tâm CNTT - Cơ quan có	1. Chủ quản quyết định hoặc đề xuất biện pháp xử lý thuộc thẩm quyền. 2. Trường hợp sự cố nghiêm trọng, có nguy cơ ảnh hưởng lớn hoặc vượt khả năng xử lý của đơn vị, phối hợp	Phương án xử lý, điều phối ứng phó sự cố.

Bước	Đơn vị thực hiện	Nội dung và trình tự thực hiện	Sản phẩm
cố	thẩm quyền và đơn vị liên quan khi cần thiết	với Trung tâm CNTT để tổ chức điều phối, báo cáo và đề nghị hỗ trợ theo quy định của pháp luật. 3. Việc xử lý tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động đã được cấp có thẩm quyền phê duyệt.	
Bước 6. Khắc phục, khôi phục và kiểm tra kết quả	- Chủ quản hệ thống thông tin - Đơn vị vận hành - Trung tâm CNTT và bên liên quan khi cần thiết	1. Xử lý nguyên nhân sự cố; loại bỏ thành phần gây mất an ninh mạng; vá lỗ hổng, thay đổi thông tin xác thực, khôi phục dữ liệu, cấu hình hoặc dịch vụ khi cần thiết. 2. Kiểm tra, đánh giá điều kiện an toàn cần thiết trước khi khôi phục hoạt động bình thường.	Hệ thống, dữ liệu hoặc dịch vụ được khắc phục, khôi phục; kết quả kiểm tra an toàn.
Bước 7. Tổng kết, báo cáo và lưu hồ sơ sự cố	- Chủ quản hệ thống thông tin - Đơn vị vận hành - Trung tâm CNTT và đơn vị liên quan	1. Đánh giá nguyên nhân, mức độ thiệt hại, kết quả xử lý và biện pháp phòng ngừa tái diễn. 2. Lập báo cáo, lưu trữ hồ sơ sự cố theo Điều 46 Quy chế này và quy định của pháp luật có liên quan. 3. Cập nhật phương án ứng phó sự cố, biện pháp bảo vệ và hồ sơ quản lý rủi ro của hệ thống.	Báo cáo kết quả xử lý; hồ sơ sự cố; nội dung cập nhật phương án, biện pháp bảo vệ.

Phụ lục II
BIỂU MẪU BÁO CÁO HẰNG NĂM

BỘ XÂY DỰNG **TÊN ĐƠN VỊ……**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /BC-…	*Hà Nội, ngày tháng năm 20…*

BÁO CÁO VỀ CÔNG TÁC BẢO ĐẢM AN NINH MẠNG
NĂM …

Kính gửi: Bộ Xây dựng (qua Trung tâm Công nghệ thông tin)

I. Thông tin chung

1. Tên đơn vị:

2. Đầu mối liên hệ về an ninh mạng:

- Họ và tên:
- Chức vụ:
- Số điện thoại:
- Thư điện tử:

II. Kết quả thực hiện công tác bảo đảm an ninh mạng

STT	Nội dung báo cáo	Kết quả thực hiện
1	Công tác chỉ đạo, điều hành về bảo vệ an ninh mạng	
2	Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng	
3	Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý	
4	Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng	
5	Bảo vệ an ninh mạng trong hoạt động cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của	

STT	Nội dung báo cáo	Kết quả thực hiện
	Chính phủ	
6	Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin	
7	Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng	
8	Triển khai giải pháp giám sát an ninh mạng	
9	Xây dựng, phê duyệt hồ sơ đề xuất cấp độ an ninh mạng hệ thống thông tin	
10	Diễn tập bảo đảm an ninh mạng	
11	Tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm bảo vệ an ninh mạng	
12	Phát triển nguồn nhân lực	
13	Các nhiệm vụ khác (nếu có)	

III. Khó khăn, vướng mắc

IV. Đề xuất, kiến nghị

Nơi nhận:
- Như trên;
- …;
- Lưu: ...

THỦ TRƯỞNG ĐƠN VỊ
(Ký, ghi họ tên)