UBND TỈNH QUẢNG NGÃI **SỞ XÂY DỰNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1539 /QĐ-SXD	*Quảng Ngãi, ngày 05 tháng 11 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Xây dựng tỉnh Quảng Ngãi

GIÁM ĐỐC SỞ XÂY DỰNG TỈNH QUẢNG NGÃI

Căn cứ Quyết định số 132/2026/QĐ-UBND ngày 20 tháng 7 năm 2026 của Ủy ban nhân dân tỉnh Quảng Ngãi ban hành Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Quảng Ngãi;

Căn cứ Quyết định số 10/2025/QĐ-UBND ngày 01/7/2025 của UBND tỉnh ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Xây dựng tỉnh Quảng Ngãi;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Xây dựng tỉnh Quảng Ngãi.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng Sở, Trưởng các phòng chuyên môn, đơn vị thuộc Sở; công chức, viên chức, người lao động thuộc Sở và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Công an tỉnh (báo cáo);
- Các phòng CM,NV Sở;
- Các ĐVTT Sở;
- Lưu: VT,VP

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ XÂY DỰNG
TỈNH QUẢNG NGÃI

Võ Phiến

UBND TỈNH QUẢNG NGÃI
SỞ XÂY DỰNG

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

QUY CHẾ
Bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Xây dựng tỉnh Quảng Ngãi

(Kèm theo Quyết định số: /QĐ-SXD ngày /11/2026 của Sở 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 nguyên tắc, trách nhiệm và biện pháp tổ chức thực hiện công tác bảo đảm an ninh mạng trong quản lý, khai thác, sử dụng tài sản công nghệ thông tin và hệ thống thông tin thuộc phạm vi quản lý của Sở Xây dựng tỉnh Quảng Ngãi.

2. Đối tượng áp dụng

a) Công chức, viên chức, người lao động Sở Xây dựng tỉnh Quảng Ngãi.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống.

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

3. 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.

4. 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.

5. Chủ quản hệ thống thông tin là các phòng, đơn vị, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Sở Xây dựng là chủ quản các hệ thống thông tin do Sở Xây dựng 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 các phòng, đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin (trường hợp thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành là bên cung cấp dịch vụ).

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. 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.

10. 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.

11. 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.

12. 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.

13. Người sử dụng là công chức, viên chức, người lao động của các phòng, 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 phòng, đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an ninh mạng. Mỗi công chức, viên chức, người lao động tại các phòng, 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. Có sự phối hợp chặt chẽ, thống nhất, phân định rõ trách nhiệm giữa các phòng, đơn vị dưới sự chỉ đạo, điều phối của Sở Xây dựng và sự hướng dẫn của Công an tỉnh.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm thực hiện theo quy định của Luật An ninh mạng số 116/2025/QH15, Luật Bảo vệ bí mật nhà nước số 117/2025/QH15, Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, Luật Dữ liệu số 60/2024/QH15, Luật Giao dịch điện tử số 20/2023/QH15, Luật Chuyển đổi số số 148/2025/QH15 và các quy định khác của pháp luật có liên quan.

2. Tự ý kết nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây (Wi-Fi) vào mạng máy tính mà không có sự đồng ý của chủ quản hệ thống thông tin và hướng dẫn của đơn vị vận hành hệ thống thông tin.

3. Tự ý thay đổi, gỡ bỏ hoặc vô hiệu hóa làm mất tác dụng của các biện pháp bảo đảm an ninh mạng.

4. Ngăn chặn việc trao đổi thông tin trên mạng, can thiệp, truy cập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên hệ thống thông tin.

5. Gây ảnh hưởng, cản trở trái phép hoạt động bình thường của hệ thống thông tin hoặc khả năng truy cập hệ thống thông tin của người sử dụng.

6. Bẻ khóa, sử dụng trái phép mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Trao đổi, truyền đưa, lưu trữ các thông tin, tài liệu về hệ thống thông tin (tài khoản, mật khẩu, mã nguồn,...) trên môi trường mạng mà không có giải pháp bảo vệ gây mất an ninh mạng.

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

1. Các đơn vị thuộc Sở 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 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 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. Văn phòng Sở và các đơn vị thuộc Sở chủ trì, phối hợp với các đơn vị liên quan lập và cập nhật danh mục máy tính, máy chủ, thiết bị mạng, thiết bị lưu trữ thuộc phạm vi quản lý; xác định đơn vị, cá nhân được giao quản lý, sử dụng. Danh mục tài sản phần cứng được rà soát, cập nhật tối thiểu 02 lần/năm.

2. Tài sản phải được bảo quản, bảo trì phù hợp; không tự ý mang ra khỏi

trụ sở, sửa chữa bên ngoài, thanh lý hoặc chuyển đổi mục đích sử dụng khi chưa được cấp có thẩm quyền chấp thuận.

3. Trước khi thanh lý, chuyển giao hoặc sửa chữa thiết bị có lưu dữ liệu, phải sao lưu dữ liệu cần thiết và xóa dữ liệu an toàn hoặc áp dụng biện pháp tiêu hủy phù hợp, bảo đảm không thể khôi phục trái phép.

Điều 8. Quản lý tài sản phần mềm

1. Với mỗi hệ thống thông tin, các phòng, 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. Các phòng thuộc Sở gửi danh sách tài sản phần mềm về Văn phòng Sở tổng hợp. Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 02 lần/năm.

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. Văn phòng Sở chủ trì, phối hợp với các phòng, 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 phòng, 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, Luật Cơ yếu 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 thực hiện xác định cấp độ hệ thống thông tin theo Điều 13 Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

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. Hệ thống thông tin phải có tài liệu hướng dẫn sử dụng; quy trình quản lý, vận hành; quy chế hoạt động; phương án bảo đảm an ninh mạng; kế hoạch ứng cứu sự cố an ninh mạng thể hiện vai trò, trách nhiệm của tổ chức, cá nhân trong quá trình quản lý, vận hành, sử dụng và ứng cứu sự cố.

2. Tổ chức xây dựng tiêu chuẩn, định mức, yêu cầu kỹ thuật để bảo đảm hoạt động bình thường đối với tất cả các hệ thống thông tin hiện có và các hệ thống thông tin mới trước khi đưa vào hoạt động chính thức.

3. Căn cứ các tiêu chuẩn, định mức, yêu cầu kỹ thuật đã xây dựng, tổ chức giám sát, tối ưu hiệu suất của hệ thống thông tin; đánh giá khả năng đáp ứng, tình trạng hoạt động, cấu hình hệ thống của hệ thống thông tin để dự báo, lập kế hoạch mở rộng, nâng cấp bảo đảm khả năng đáp ứng về an ninh mạng hệ thống thông tin trong tương lai.

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

a) Các phòng, 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.

5. 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 các phòng, đơn vị chủ trì trong quá trình thuê dịch vụ công nghệ thông tin.

a) Quản lý chặt chẽ thông tin, dữ liệu phát sinh từ dịch vụ thuê, không cho phép bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

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

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

d) Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an ninh mạng phải tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm; thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ cho cơ quan chức năng 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.

đ) 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 85/2016/NĐ-CP.

e) 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 Quảng Ngãi, Khung kiến trúc số tỉnh Quảng Ngãi.

3. Trách nhiệm của các phòng, 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 chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết 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.

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. Bên cung cấp dịch vụ khi có thay đổi về mặt hệ thống, ứng dụng, mã nguồn và chức năng hệ thống phần mềm phục vụ kết nối các hệ thống thông tin quan trọng về an ninh quốc gia cần báo cáo về Công an tỉnh để phối hợp đơn vị nghiệp vụ Bộ Công an thực hiện kiểm tra an ninh thông tin bảo đảm đáp ứng các tiêu chí theo hướng dẫn của Bộ Công an, chủ quản hệ thống thông tin quan trọng quốc gia và quy định pháp luật.

Điều 13. Quản lý phòng máy chủ

1. Các thiết bị tường lửa, máy chủ, hệ thống lưu trữ... phải được đặt trong 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 phòng máy chủ để lắp đặt hoặc sửa chữa phải có sự chấp thuận của thủ trưởng cơ quan, đơn vị quản lý, vận hành.

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 về 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 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 phòng, 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, có nguồn gốc rõ ràng.

2. Chỉ cài đặt các phần mềm nằm trong danh mục được phép sử dụng do cơ quan có thẩm quyền ban hành (nếu có). 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.

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 tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt phổ biến; 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. Người sử dụng phải khóa màn hình máy tính khi rời khỏi vị trí làm việc và tắt hoàn toàn máy tính khi hết giờ làm việc. Đối với thiết bị phục vụ tác vụ kỹ thuật, sao lưu hoặc vận hành liên tục, được phép áp dụng ngoại lệ phù hợp với yêu cầu công việc và bảo đảm an toàn thông tin.

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

1. Chữ ký số và chứng thư chữ ký số chuyên dùng trong các cơ quan nhà nước được cấp bởi tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (Ban Cơ yếu Chính phủ) hoặc các tổ chức được cấp phép.

2. Cá nhân được cấp chữ ký số, chứng thư chữ ký số chuyên dùng 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 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.

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

1. Các phòng, 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 phòng, 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 phòng, 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 phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an ninh mạng đối với từng hệ thống thông tin được quản lý, sử dụng; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, cơ quan, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

2. Các phòng, 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, các phòng, đơn vị có trách nhiệm

a) Xác định rõ trách nhiệm của 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. Văn phòng Sở và các đơn vị thuộc Sở 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 phòng, đơn vị xác định nhu cầu đào tạo cho nguồn nhân lực về bảo đảm an ninh mạng tại cơ quan, đơn vị mình gửi Văn phòng Sở tổng hợp, tham mưu tổ chức đào tạo.

3. Văn phòng Sở và các đơn vị thuộc Sở cử công chức, viên chức, người lao động tham gia các chương trình đào tạo, bồi dưỡng nghiệp vụ về an ninh mạng dành cho cán bộ chuyên trách, phụ trách công tác an ninh mạng; đồng thời, chủ động tổ chức hoặc phối hợp tổ chức đào tạo, bồi dưỡng kiến thức cơ bản về an ninh mạng cho công chức, viên chức, người lao động thuộc phạm vi quản lý nhằm nâng cao nhận thức, kỹ năng và trách nhiệm trong bảo đảm an

ninh mạng.

4. Các phòng, 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 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 phòng, đơn vị 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 7 đến Điều 11 của Nghị định số 85/2016/NĐ-CP.

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 hồ sơ đề xuất cấp độ hệ thống thông tin

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 15 của Nghị định số 85/2016/NĐ-CP, bao gồm: Tài liệu mô tả tổng quan về hệ thống thông tin, thiết kế hệ thống thông tin, thuyết minh đề xuất cấp độ hệ thống thông tin, thuyết minh phương án bảo đảm an ninh mạng 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 19 Nghị định số 85/2016/NĐ-CP và các điều kiện an ninh mạng theo Tiêu chuẩn quốc gia TCVN 14423:2026 về An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

3. Văn phòng Sở có trách nhiệm hướng dẫn, đôn đốc, kiểm tra việc triển khai phương án bảo đảm an ninh mạng tại các phòng, đơn vị.

Mục 4

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

Điều 24. Kiểm tra, giám sát và đánh giá

1. Văn phòng Sở chủ trì, phối hợp các phòng, đơn vị tổ chức tự kiểm tra việc chấp hành Quy chế; kiểm tra đột xuất khi phát hiện nguy cơ hoặc theo chỉ đạo của lãnh đạo Sở.

2. Nội dung kiểm tra gồm: quản lý tài sản, tài khoản và quyền truy cập; cập nhật phần mềm; sao lưu dữ liệu; quản lý nhật ký; bảo vệ bí mật nhà nước, dữ liệu cá nhân; thực hiện phương án cấp độ và xử lý sự cố.

3. Phòng, đơn vị được kiểm tra có trách nhiệm cung cấp thông tin, tài liệu liên quan và thực hiện khắc phục tồn tại theo thời hạn được yêu cầu.

Điều 25. Tiếp nhận và xử lý sự cố an ninh mạng

1. Văn phòng Sở là đầu mối tiếp nhận thông tin sự cố đối với các hệ thống thông tin tại cơ quan Sở; phối hợp với các phòng, đơn vị liên quan xác minh, đánh giá sơ bộ, đề xuất biện pháp xử lý và báo cáo lãnh đạo Sở. Giám đốc Sở phân công cụ thể công chức hoặc đơn vị phụ trách kỹ thuật, an ninh mạng bằng văn bản.

2. Đối với các hệ thống thông tin do đơn vị thuộc Sở trực tiếp quản lý, vận hành, đơn vị có trách nhiệm chủ động tiếp nhận, xác minh, xử lý ban đầu và triển khai các biện pháp khắc phục sự cố trong phạm vi thẩm quyền, khả năng kỹ thuật; đồng thời thông báo Văn phòng Sở để theo dõi, phối hợp xử lý theo quy định, nhất là đối với các sự cố nghiêm trọng, vượt khả năng xử lý hoặc có nguy cơ ảnh hưởng đến các hệ thống thông tin khác.

3. Khi phát hiện sự cố, người phát hiện phải thông báo ngay cho lãnh đạo trực tiếp và đầu mối phụ trách. Đầu mối phụ trách tổ chức cô lập thiết bị hoặc tài khoản bị ảnh hưởng khi cần thiết, bảo vệ nhật ký và chứng cứ, xác định phạm vi ảnh hưởng, triển khai khắc phục trong khả năng.

4. Trường hợp sự cố nghiêm trọng, có dấu hiệu tấn công mạng, lộ lọt dữ liệu, ảnh hưởng đến hệ thống dùng chung hoặc vượt khả năng xử lý, lãnh đạo Sở báo cáo ngay cơ quan chuyên trách theo quy định, trong đó phối hợp Công an tỉnh và đơn vị vận hành hệ thống liên quan; không tự ý công bố thông tin sự cố.

5. Sau sự cố, đầu mối phụ trách lập hồ sơ ghi nhận diễn biến, nguyên nhân, phạm vi ảnh hưởng, biện pháp đã thực hiện và kiến nghị phòng ngừa tái diễn.

Mục 5

BẢO VỆ BÍ MẬT NHÀ NƯỚC, DỮ LIỆU CÁ NHÂN

Điều 26. Bảo vệ bí mật nhà nước trên không gian mạng

1. Cơ quan Sở và các đơn vị thuộc Sở 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 Internet hoặc mạng máy tính, mạng viễn thông, trừ trường hợp pháp luật về bảo vệ bí mật nhà nước có quy định khác. Không sử dụng máy tính, thiết bị đã kết nối Internet hoặc mạng máy tính, mạng viễn thông để soạn thảo, lưu giữ bí mật nhà nước.

3. Tài sản phần cứng, phần mềm phục vụ xử lý thông tin bí mật nhà nước phải được cơ quan chức năng kiểm tra, dán tem bảo đảm an ninh, an toàn thông tin trước khi đưa vào sử dụng (kể cả sau khi sửa chữa, bảo hành).

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 27. Yêu cầu chung trong xử lý dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân tại các phòng, đơn vị phải tuân thủ đầy đủ các nguyên tắc bảo vệ dữ liệu cá nhân quy định tại Điều 3 Luật số 91/2025/QH15.

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 phòng, 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 28. Quyền và nghĩa vụ của các bên liên quan trong bảo vệ dữ liệu cá nhân

1. Chủ thể dữ liệu là công chức, viên chức, người lao động và công dân có các quyền và nghĩa vụ theo quy định tại Điều 4 Luật số 91/2025/QH15.

2. Thủ trưởng các phòng, 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 phòng, đơn vị mình.

3. 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 29. Trách nhiệm bảo vệ dữ liệu cá nhân

1. Các phòng, 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 hoặc sự cố về dữ liệu cá nhân, các phòng, đơn vị phải tiến hành các biện pháp khắc phục ngay lập tức và thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất 72 giờ kể từ khi phát hiện hành vi vi phạm hoặc sự cố dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác.

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

1. Trách nhiệm của các phòng, 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 14 Nghị định số 85/2016/NĐ-CP.

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.

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.

2. Trường hợp hệ thống thông tin thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Bên cung cấp dịch vụ đóng vai trò là đơn vị vận hành hệ thống thông tin, có trách nhiệm thực hiện các quy định tại khoản 1 Điều này; phối hợp chặt chẽ với đơn vị chủ quản hệ thống thông tin trong quá trình thực hiện.

Điều 31. Trách nhiệm của công chức, viên chức và người lao động

1. Trách nhiệm của 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) 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.

2. Trách nhiệm của cán bộ chuyên trách/phụ trách về an ninh mạng: Ngoài các quy định tại khoản 1 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 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 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 32. Trách nhiệm của tổ chức, đơn vị, cá nhân liên quan

Các tổ chức, đơn vị, cá nhân liên quan đến sử dụng, khai thác các hệ thống thông tin của tỉnh hoặc có liên quan trực tiếp đến công tác bảo đảm an ninh mạng trên địa bàn tỉnh phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về an ninh mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 33. Trách nhiệm thi hành

1. Căn cứ Quy chế này, Thủ trưởng các phòng, đơn vị và các tổ chức, 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 phòng, đơn vị phản ánh kịp thời về Văn phòng Sở để tổng hợp, báo cáo Giám đốc Sở xem xét sửa đổi, bổ sung.

2. Các nội dung không quy định tại Quy chế này thực hiện theo Quy chế ban hành kèm theo Quyết định số 132/2026/QĐ-UBND và các quy định khác có liên quan.

3. 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.

4. Văn phòng Sở chủ trì, theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế này./.