ỦY BAN NHÂN DÂN XÃ THIỆN TÍN	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 trên địa bàn xã Thiện Tín

(Ban hành kèm theo Quyết định số 1256 /QĐ-UBND ngày 28/08/2026 của Chủ tịch UBND xã Thiện Tín)

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 công tác bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn xã Thiện Tín.

2. Đối tượng áp dụng

a) Các ban, ngành; các tổ chức, đơn vị trực thuộc Ủy ban nhân dân xã, Hội đồng nhân dân, các tổ chức chính trị - xã hội trên địa bàn xã (viết tắt là cơ quan, đơn vị).

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

c) Các tổ chức, đơn vị, cá nhân cung cấp dịch vụ công nghệ thông tin, an ninh mạng tham gia triển khai, kết nối các hệ thống thông tin của xã (viết tắt là bên cung cấp dịch vụ) hoặc có liên quan trực tiếp đến công tác bảo đảm an ninh mạng trên địa bàn xã.

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

6. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Ủy ban nhân dân xã là chủ quản các hệ thống thông tin do ủy ban nhân dân xã quyết định chủ trương đầu tư sử dụng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

7. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin (trường hợp thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành là bên cung cấp dịch vụ).

8. 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.

9. 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.

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

11. 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.

12. 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.

13. 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.

14. 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.

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

Điều 3. Nguyên tắc chung

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

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

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

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

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

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

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

8. Có sự phối hợp chặt chẽ, thống nhất, phân định rõ trách nhiệm giữa các cơ quan, đơn vị dưới sự chỉ đạo, điều phối của Ủy ban nhân dân xã và sự tham mưu, hướng dẫn của bộ phận phụ trách công nghệ thông tin UBND xã và Công an xã.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm thực hiện theo quy định của Luật An ninh mạng 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.

Chương II
BẢO ĐẢM AN NINH MẠNG

Mục 1
QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 5. 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 6. Quản lý tài sản phần cứng

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị phải lập danh sách tài sản phần cứng gồm các thông tin cơ bản sau: Tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, vị trí lắp đặt, chủ thể quản lý, mục đích sử dụng, hệ thống thông tin tương ứng, tình trạng sử dụng, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có). Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần cứng định kỳ tối thiểu 02 lần/năm.

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

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

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

5. Không tự ý sửa chữa tài sản phần cứng ở các cơ sở, dịch vụ ngoài cơ quan, đơn vị. Trường hợp cấp bách phải sửa chữa ở các cơ sở bên ngoài, thì phải được sự đồng ý, phê duyệt của Thủ trưởng cơ quan, đơn vị đồng thời có biện pháp

xóa dữ liệu an toàn hoặc lưu giữ lại bộ phận lưu trữ dữ liệu trước khi thực hiện sửa chữa. Trong quá trình sửa chữa, bảo trì hệ thống, thiết bị công nghệ thông tin do bên thứ ba thực hiện, đơn vị chủ quản, vận hành hệ thống thông tin phải cử bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng giám sát và ghi nhật ký đầy đủ.

Điều 7. Quản lý tài sản phần mềm

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị lập danh sách tài sản phần mềm với các thông tin cơ bản gồm: tên tài sản, mục đích, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin tương ứng. 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. Cơ quan, đơn vị định kỳ rà soát, cập nhật, khắc phục các điểm yếu, lỗ hổng bảo mật có nguy cơ gây mất an ninh mạng.

Điều 8. Quản lý tài sản thông tin

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

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

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

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

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

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

2. 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 9. 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 10. 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 cơ quan, đơn vị phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận, lưu giữ và bảo vệ nhằm phục vụ công tác phân tích, kiểm tra, điều tra, giám sát an ninh mạng.

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

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

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 11. Quản lý thuê dịch vụ công nghệ thông tin

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

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

a) 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 xã; tuân thủ Khung kiến trúc Chính phủ số Việt Nam; Khung kiến trúc Chính quyền điện tử hướng đến Chính quyền số xã Thiện Tín, Khung kiến trúc số xã Thiện Tín.

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

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản công nghệ thông tin khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ 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 12. 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 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Dữ liệu trao đổi giữa các vùng mạng phải được kiểm soát chặt chẽ bởi thiết bị tường lửa và các thiết bị bảo mật khác.

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

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

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

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

6. Mạng truyền số liệu chuyên dùng trên địa bàn xã 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 13. Quản lý, sử dụng máy tính, thiết bị ngoại vi và phần mềm

1. Máy tính và các thiết bị ngoại vi tại các cơ quan, đơn vị phải được cài đặt hệ điều hành, phần mềm ứng dụng có bản quyền hoặc sử dụng phần mềm mã nguồn mở hợp pháp, 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 (sử dụng tính năng có sẵn của hệ điều hành) khi rời khỏi vị trí làm việc và tắt hoàn toàn máy tính khi hết giờ làm việc.

Điều 15. 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 16. 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 xã.

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

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

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

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

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

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

4. Bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng phối hợp với các cơ quan, đơn vị có liên quan thực hiện phân loại tài sản thông tin, phần mềm, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có. Các nội dung thực

hiện gồm: Lập danh sách các dữ liệu (thông tin cấu hình của mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ thống được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; thực hiện quy trình sao lưu dự phòng và phục hồi.

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

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

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

Điều 18. Bảo đảm an ninh mạng đối với người sử dụng

1. Các cơ quan, đơn vị phải xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, cơ quan, đơn vị 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 cơ quan, đơn vị phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản công nghệ thông tin liên quan đến hệ thống thông tin đối với các cá nhân do cơ quan, đơn vị quản lý. Người sử dụng phải kiểm tra thông tin, dữ liệu được lưu giữ trên các tài sản công nghệ thông tin trước khi tiếp nhận.

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

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

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

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

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

Mục 3
BẢO ĐẢM HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 19. Phân loại và xác định cấp độ hệ thống thông tin

1. Tất cả các hệ thống thông tin do các cơ quan, đơn vị trong xã 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.

4. 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, trình cấp có thẩm quyền phê duyệt.

Mục 4
KIỂM TRA, GIÁM SÁT, CẢNH BÁO VÀ ỨNG CỨU SỰ CỐ

Điều 20. Kiểm tra, đánh giá an ninh mạng

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

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng

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

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

4. Việc kiểm tra, đánh giá được thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP, như sau:

a) Định kỳ 02 năm đối với hệ thống thông tin cấp độ 1 và cấp độ 2.

b) Định kỳ hằng năm đối với hệ thống thông tin cấp độ 3 và cấp độ 4.

c) Định kỳ 06 tháng một lần đối với hệ thống thông tin cấp độ 5.

5. Nội dung, hình thức kiểm tra, đánh giá quy định tại Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và quy định có liên quan. Đơn vị chuyên trách về an ninh mạng có trách nhiệm thông báo kế hoạch, thành lập đoàn kiểm tra, lập biên bản và thông báo kết quả kiểm tra, đánh giá cho đơn vị được kiểm tra, đánh giá.

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

Điều 21. Giám sát, cảnh báo an ninh mạng

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

2. Các hệ thống thông tin của các cơ quan, đơn vị phải được kết nối, chia sẻ thông tin, dữ liệu giám sát về Trung tâm An ninh mạng tỉnh (nếu có) để thực hiện giám sát tập trung, phân tích, cảnh báo sớm các nguy cơ, mối đe dọa trên toàn tỉnh và kết nối, chia sẻ kết quả giám sát về Trung tâm An ninh mạng quốc gia (thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao -

Bộ Công an).

Điều 22. Ứng cứu sự cố an ninh mạng

1. Chủ quản hệ thống thông tin thành lập hoặc chỉ định bộ phận là Đội ứng cứu sự cố an ninh mạng nội bộ để thực hiện nhiệm vụ giám sát, phát hiện, xử lý và phối hợp khắc phục sự cố an ninh mạng trong phạm vi quản lý.

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

Điều 23. Quy trình ứng cứu sự cố an ninh mạng

1. Quy trình ứng cứu sự cố an ninh mạng tuân thủ quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, Thông tư số 20/2017/TT-BTTTT của Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng và phương án ứng cứu sự cố an ninh mạng của xã, bao gồm: Phát hiện, tiếp nhận, phân loại, xử lý ban đầu, phân tích, khắc phục, điều tra và tổng kết, đánh giá.

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

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

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

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

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

e) Kịp thời phối hợp Đội ứng cứu sự cố an ninh mạng tỉnh triển khai xác minh và xử lý sự cố an ninh mạng, ngăn chặn nguồn tấn công, lọc lưu lượng độc hại.

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

Mục 5
BẢO VỆ BÍ MẬT NHÀ NƯỚC, DỮ LIỆU CÁ NHÂN

Điều 24. Bảo vệ bí mật nhà nước trên không gian mạng

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

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

3. 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.

Điểu 25. Yêu cầu chung trong xử lý dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân tại các cơ quan, đơn vị phải tuân thủ đầy đủ các nguyên tắc bảo vệ dữ liệu cá nhân quy định tại Điều 3 Luật sô 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 cơ quan, đơn vị áp dụng các biện pháp quản lý và kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân trong suốt quá trình xử lý, lưu trữ và hủy bỏ.

Điều 26. Quyền và nghĩa vụ của các bên liên quan trong bảo vệ dữ liệu cá nhân

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

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

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

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG

Điều 27. Trách nhiệm của Công an xã

1. Tham mưu, quản lý nhà nước

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

b) Xây dựng, trình Uỷ ban nhân dân xã ban hành và tổ chức thực hiện các Chương trình, Kế hoạch, Phương án về đảm bảo an ninh mạng.

2. Giám sát và cảnh báo

a) Tổ chức giám sát tập trung, phân tích, cảnh báo sớm các nguy cơ, mối đe dọa an ninh mạng.

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

3. Ứng cứu sự cố an ninh mạng

a) Là đơn vị thường trực của Đội ứng cứu sự cố an ninh mạng xã, giữ vai trò đầu mối tiếp nhận, điều phối các hoạt động ứng cứu sự cố an ninh mạng trên địa bàn xã

b) Tham mưu Uỷ ban nhân dân xã ban hành và tổ chức triển khai phương án ứng cứu sự cố an ninh mạng trên địa bàn xã.

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

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

mới của các loại tội phạm công nghệ cao.

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

c) Chủ trì triển khai các biện pháp bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

Điều 28. Trách nhiệm của chủ quản hệ thống thông tin

1. Ủy ban nhân dân xã có thể giao nhiệm vụ quản lý trực tiếp hệ thống thông tin thuộc lĩnh vực chuyên môn cho các cơ quan, đơn vị phụ trách và thực hiện đầy đủ trách nhiệm của chủ quản hệ thống thông tin.

2. Thủ trưởng các cơ quan, đơn vị là chủ quản hệ thống thông tin trực tiếp chỉ đạo và phụ trách công tác bảo đảm an ninh mạng; chịu trách nhiệm toàn diện trước uỷ ban nhân dân xã và trước pháp luật về công tác bảo đảm an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý của mình.

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

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

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

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

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

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

Điều 29. Trách nhiệm của đơn vị vận hành hệ thống thông tin

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

a) Thực hiện xác định cấp độ hệ thống thông tin theo quy định tại Điều 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.

f) 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 có chủ quản đóng vai trò là đơn vị vận hành hệ thống thông tin thực hiện các quy định tại khoản 1 Điều này.

3. Trường hợp hệ thống thông tin thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Bên cung cấp dịch vụ 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 30. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

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

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

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

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

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 cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin.

c) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo 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 31. 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 xã hoặc có liên quan trực tiếp đến công tác bảo đảm an ninh mạng trên địa bàn xã 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 32. Chế độ, nội dung báo cáo

Các cơ quan, đơn vị có trách nhiệm lập và gửi báo cáo cho Ủy ban nhân dân xã *(qua Công an xã)* về công tác an ninh mạng theo định kỳ và đột xuất:

1. Báo cáo định kỳ hằng năm về tình hình, kết quả thực hiện Quy chế này. Thời gian báo cáo trước ngày **05 tháng 12**.

2. Báo cáo đột xuất: Công tác khắc phục, xử lý các lỗ hổng, điểm yếu bảo mật, cảnh báo an ninh mạng và các báo cáo đột xuất khác theo yêu cầu của Công an xã hoặc yêu cầu của Ủy ban nhân dân xã.

3. Công an xã chịu trách nhiệm tập hợp, tổng hợp báo cáo của các cơ quan, đơn vị, trình Ủy ban nhân dân xã phê duyệt, gửi các cơ quan quản lý nhà nước về an ninh mạng.

Điều 33. Kinh phí thực hiện

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

2. Căn cứ Kế hoạch này hàng năm Công an xã phối hợp với Phòng Kinh tế xã và các cơ quan, đơn vị có liên quan dự trù, tham mưu cấp có thẩm quyền bố trí nguồn kinh phí cho hoạt động đảm bảo an ninh mạng theo quy định của Luật Ngân sách nhà nước số 89/2025/QH15, Luật 116/2025/QH15 và các quy định hiện

hành.

3. Các cơ quan, đơn vị bảo đảm bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng.

Điều 34. Khen thưởng, kỷ luật

1. Hằng năm, Công an xã dựa trên kết quả quản lý, báo cáo công tác bảo đảm an ninh mạng của các cơ quan, đơn vị tham mưu đề xuất Ủy ban nhân dân xã, xem xét khen thưởng cho tổ chức, cá nhân có thành tích xuất sắc trong công tác bảo đảm an ninh mạng theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác.

Điều 35. Trách nhiệm thi hành

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

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

3. Công an xã chủ trì phối hợp với Phòng Văn hóa - Xã hội, Văn phòng HĐND và UBND xã theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế này./.