| | |
|---|---|
| **ỦY BAN NHÂN DÂN**<br>**XÃ EA KNỐP** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số :405 /QĐ-UBND | *Ea Knốp, ngày 07 tháng 9 năm 2026* |

# QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị thuộc phạm vi quản lý của UBND xã Ea Knốp**

**ỦY BAN NHÂN DÂN XÃ EA KNỐP**

*Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15;*

*Căn cứ Luật An ninh mạng số 116/2025/QH15;*

*Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;*

*Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;*

*Căn cứ Luật Dữ liệu số 60/2024/QH15;*

*Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;*

*Căn cứ Luật Chuyển đổi số số 148/2025/QH15;*

*Căn cứ Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ Nghị định số 147/2024/NĐ-CP của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;*

*Căn cứ Nghị định số 68/2024/NĐ-CP của Chính phủ quy định về chữ ký số chuyên dùng công vụ;*

*Căn cứ Nghị định số 356/2025/NĐ-CP của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;*

*Căn cứ 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;*

*Căn cứ Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;*

*Căn cứ Thông tư số 31/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;*

*Căn cứ Thông tư số 12/2022/TT-BTTTT 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;*

*Căn cứ Quyết định số 93/2026/QĐ-UBND ngày 22/08/2026 của Ủy ban nhân dân tỉnh Đắk Lắk ban hành Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk;*

*Theo đề nghị của Chánh Văn phòng HĐND và UBND xã tại Tờ trình số 30/TTr-VP ngày 27 tháng 8 năm 2026.*

## 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 của các cơ quan, đơn vị thuộc phạm vi quản lý của UBND xã Ea Knốp.

**Điều 2.** Quyết định này có hiệu lực thi hành kể từ ngày 03 tháng 9 năm 2026.

**Điều 3.** Chánh Văn phòng HĐND và UBND xã; Trưởng Công an xã; Chỉ huy trưởng Ban Chỉ huy Quân sự xã; Trưởng các phòng chuyên môn, người đứng đầu các trung tâm, đơn vị thuộc xã và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***
- TT Đảng ủy; TT HĐND xã (b/c);
- UBMTTQ Việt Nam xã;
- Chủ tịch, các PCT UBND xã;
- Các phòng chuyên môn, trung tâm thuộc xã;
- Công an xã;
- Ban chỉ huy Quân sự xã;
- Trạm y tế;
- Lưu: VT

**TM. ỦY BAN NHÂN DÂN**
**CHỦ TỊCH**

U.B.N.D XÃ EA KNỐP T. ĐẮK LẮK

**Lê Anh Vũ**

ỦY BAN NHÂN DÂN
XÃ EA KNỐP

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 của các cơ quan, đơn vị thuộc phạm vi quản lý của UBND xã Ea Knốp**

*(Ban hành kèm theo Quyết định số 405/QĐ-UBND, ngày 07/9/2026 của UBND xã Ea Knốp)*

## Chương I
## QUY ĐỊNH CHUNG

**Điều 1. Phạm vi điều chỉnh**

Quy chế này quy định nguyên tắc, nội dung, trách nhiệm và biện pháp bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin; quản lý, vận hành và sử dụng hệ thống thông tin, nền tảng số, cơ sở dữ liệu, thiết bị công nghệ thông tin thuộc phạm vi quản lý của Ủy ban nhân dân xã Ea Knốp.

**Điều 2. Đối tượng áp dụng**

1. Các phòng chuyên môn, Trung tâm Phục vụ hành chính công, Trung tâm Cung ứng dịch vụ sự nghiệp công và các cơ quan, đơn vị thuộc phạm vi quản lý của Ủy ban nhân dân xã Ea Knốp (sau đây gọi chung là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động và các cá nhân được giao quản lý, vận hành, khai thác, sử dụng hệ thống thông tin, nền tảng số, cơ sở dữ liệu và thiết bị công nghệ thông tin của các cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các tổ chức, doanh nghiệp, cá nhân cung cấp sản phẩm, dịch vụ công nghệ thông tin, an toàn thông tin, an ninh mạng, điện toán đám mây, nền tảng số, dịch vụ số hoặc tham gia thiết kế, xây dựng, quản trị, vận hành, bảo trì, kết nối, tích hợp và chia sẻ dữ liệu đối với hệ thống thông tin thuộc phạm vi quản lý của Ủy ban nhân dân xã Ea Knốp (sau đây gọi chung là bên cung cấp dịch vụ).

4. Các cơ quan, tổ chức và cá nhân khác có liên quan đến hoạt động ứng dụng công nghệ thông tin và công tác bảo đảm an ninh mạng thuộc phạm vi quản lý của Ủy ban nhân dân xã Ea Knốp.

**Điều 3. Nguyên tắc bảo vệ an ninh mạng**

1. Việc bảo vệ an ninh mạng phải tuân thủ các nguyên tắc quy định tại Điều 4 Luật An ninh mạng số 116/2025/QH15 và các quy định pháp luật có liên quan.

2. Bảo đảm an ninh mạng là trách nhiệm của các cơ quan, đơn vị và từng cán bộ, công chức, viên chức, người lao động trong quá trình quản lý, vận hành,

khai thác và sử dụng hệ thống thông tin, nền tảng số, cơ sở dữ liệu, thiết bị công nghệ thông tin thuộc phạm vi quản lý của UBND xã.

3. Thông tin, tài liệu thuộc danh mục bí mật nhà nước phải được quản lý, bảo vệ nghiêm ngặt trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước; không lưu trữ, truyền đưa, trao đổi hoặc xử lý bí mật nhà nước trên hệ thống thông tin, thiết bị không đáp ứng yêu cầu bảo mật.

4. Công tác bảo vệ an ninh mạng phải được thực hiện thường xuyên, liên tục; chủ động phòng ngừa, kịp thời phát hiện, ngăn chặn và xử lý hành vi xâm phạm an ninh mạng.

5. Việc xử lý sự cố an ninh mạng phải kịp thời, đúng thẩm quyền, tuân thủ quy trình và bảo đảm quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân có liên quan; trường hợp vượt quá khả năng hoặc thẩm quyền xử lý, phải báo cáo UBND xã và cơ quan có thẩm quyền để được hướng dẫn, phối hợp xử lý theo quy định.

**Điều 4. Xây dựng quy định bảo đảm an ninh mạng**

1. Các cơ quan, đơn vị căn cứ Quy chế này và tình hình thực tế để tổ chức thực hiện các biện pháp bảo đảm an ninh mạng phù hợp với chức năng, nhiệm vụ, cơ cấu tổ chức và hệ thống thông tin được giao quản lý, khai thác, sử dụng.

2. Cơ quan, đơn vị được giao trực tiếp quản lý, vận hành hệ thống thông tin có trách nhiệm xây dựng hoặc tham mưu cấp có thẩm quyền ban hành quy định bảo đảm an ninh mạng phù hợp với cấp độ của hệ thống thông tin, tiêu chuẩn, quy chuẩn kỹ thuật và quy định của pháp luật có liên quan.

3. Quy định bảo đảm an ninh mạng phải xác định rõ trách nhiệm của tổ chức, cá nhân trong quản lý, vận hành và sử dụng hệ thống thông tin; biện pháp phòng ngừa, phát hiện, ngăn chặn và xử lý sự cố an ninh mạng.

4. Các cơ quan, đơn vị thường xuyên kiểm tra, rà soát việc thực hiện; kịp thời đề xuất sửa đổi, bổ sung quy định bảo đảm an ninh mạng khi có thay đổi về pháp luật, tổ chức bộ máy, hệ thống thông tin hoặc phát sinh nguy cơ 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**

Tài sản công nghệ thông tin thuộc phạm vi quản lý của UBND xã và các cơ quan, đơn vị bao gồm:

**1. Tài sản phần cứng:** Máy chủ, máy tính để bàn, máy tính xách tay; thiết bị lưu trữ, vật mang tin như USB, ổ cứng, đĩa CD/DVD; thiết bị mạng và thiết bị bảo mật như bộ định tuyến, bộ chuyển mạch, tường lửa; thiết bị ngoại vi như máy in, máy quét; hệ thống cáp mạng, thiết bị cung cấp nguồn điện và các thiết bị khác phục vụ hoạt động của hệ thống thông tin.

**2. Tài sản phần mềm:** Phần mềm hệ thống, phần mềm ứng dụng, phần mềm tiện ích, phần mềm bảo đảm an ninh mạng, hệ quản trị cơ sở dữ liệu, mã nguồn, công cụ phát triển phần mềm và các tài khoản được cấp để quản trị, khai thác, sử dụng hệ thống thông tin, nền tảng số.

**3. Tài sản thông tin:** Dữ liệu, thông tin dưới dạng số được tạo lập, thu thập, tiếp nhận, xử lý, lưu trữ, khai thác, chia sẻ hoặc truyền đưa thông qua hệ thống thông tin thuộc phạm vi quản lý của UBND xã và các cơ quan, đơn vị.

**4. Tài sản, thành phần liên quan khác:** Tài liệu kỹ thuật, hồ sơ thiết kế, sơ đồ mạng, quy trình vận hành, thông tin cấu hình hệ thống, khóa bảo mật, chứng thư số, chữ ký số và các tài sản khác phục vụ hoạt động ứng dụng công nghệ thông tin.

**Điều 6. Quản lý tài sản phần cứng**

1. Đối với mỗi hệ thống thông tin thuộc phạm vi quản lý của UBND xã, cơ quan, đơn vị được giao quản lý, vận hành 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 hoặc mã nhận diện, số sê-ri; vị trí lắp đặt; cơ quan, bộ phận hoặc cá nhân 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 đối với toàn bộ tài sản phần cứng định kỳ tối thiểu 02 lần/năm.

2. Tài sản phần cứng được giao và gắn trách nhiệm cho cơ quan, 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 nhằm giảm thiểu rủi ro do các mối đe dọa, hiểm họa từ môi trường và hành vi xâm nhập trái phép.

3. Tài sản phần cứng thuộc hệ thống thông tin từ cấp độ 3 trở lên do UBND xã quản lý phải được kiểm tra, đánh giá an ninh, an toàn thông tin trước khi đưa vào sử dụng; bảo đảm 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 hoặc thay đổi mục đích sử dụng phải được tiêu hủy về mặt vật lý hoặc xóa dữ liệu an toàn, bảo đảm không có khả năng phục hồi. Trường hợp không thực hiện được việc xóa hoặc ghi đè dữ liệu thì 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 tại các cơ sở, dịch vụ bên ngoài cơ quan, đơn vị. Trường hợp cấp bách phải sửa chữa tại cơ sở bên ngoài thì phải được sự đồng ý, phê duyệt của người đứng đầu cơ quan, đơn vị; đồng thời, phải có biện pháp xóa dữ liệu an toàn hoặc 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, cơ quan, đơn vị được giao quản lý, vận hành phải cử người giám sát và phối hợp với chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin để theo dõi, ghi nhật ký đầy đủ.

**Điều 7. Quản lý tài sản phần mềm**

1. Đối với mỗi hệ thống thông tin thuộc phạm vi quản lý của UBND xã, cơ quan, đơn vị được giao quản lý, vận hành phải lập danh sách tài sản phần mềm với các thông tin cơ bản gồm: tên tài sản; mục đích, phạm vi sử dụng; cơ quan, bộ phận hoặc cá nhân quản lý; thông tin về bản quyền; phiên bản và hệ thống thông tin tương ứng. Thực hiện kiểm kê, rà soát và cập nhật danh sách đối với toàn bộ tài sản phần mềm định kỳ tối thiểu 02 lần/năm.

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

3. Các cơ quan, đơn vị định kỳ rà soát, cập nhật và khắc phục các điểm yếu, lỗ hổng bảo mật có nguy cơ gây mất an ninh mạng đối với tài sản phần mềm được giao quản lý, sử dụng.

**Điều 8. Quản lý tài sản thông tin**

1. Đối với mỗi hệ thống thông tin thuộc phạm vi quản lý của UBND xã, cơ quan, đơn vị được giao quản lý, vận hành phải lập danh sách tài sản thông tin với các thông tin cơ bản gồm: tên tài sản; mức độ tiếp cận; cơ quan, bộ phận hoặc cá nhân quản lý; phạm vi truy cập thông tin; thời gian lưu trữ và hệ thống thông tin tương ứng. Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/năm hoặc khi có thay đổi trong cơ quan, đơn vị làm 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 số 117/2025/QH15.

3. Tài sản thông tin thuộc danh mục bí mật nhà nước phải được quản lý theo quy định của Luật Bảo vệ bí mật nhà nước số 117/2025/QH15, Luật Cơ yếu số 05/2011/QH13 và các quy định khác có liên quan trong 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 mở rộng, nâng cấp hệ thống thông tin do UBND xã làm chủ quản, cơ quan, đơn vị được giao chủ trì thực hiện phải xác định cấp độ hệ thống thông tin theo Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ; đồng thời, tuân thủ các quy định về phân loại và nhiệm vụ bảo vệ hệ thống thông tin tại Điều 8 và Điều 10 Luật An ninh mạng số 116/2025/QH15.

2. Khi triển khai các sản phẩm bảo đảm an ninh mạng trong hệ thống thông tin thuộc phạm vi quản lý của UBND xã phải đáp ứng các tiêu chuẩn, quy chuẩn Việt Nam và 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 cơ quan, tổ chức, doanh nghiệp trong nước.

**Điều 10. Yêu cầu quản lý, vận hành, hủy bỏ hệ thống thông tin**

1. Hệ thống thông tin thuộc phạm vi quản lý của UBND xã 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, trong đó xác định rõ vai trò, trách nhiệm của cơ quan, tổ chức, cá nhân trong quá trình quản lý, vận hành, sử dụng và ứng cứu sự cố.

2. Áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng theo quy định của pháp luật để bảo đảm hoạt động bình thường đối với tất cả hệ thống thông tin hiện có và hệ thống thông tin mới thuộc phạm vi quản lý của UBND xã trước khi đưa vào hoạt động chính thức.

3. Căn cứ tiêu chuẩn, định mức và yêu cầu kỹ thuật theo quy định của pháp luật, cơ quan, đơn vị được giao quản lý, vận hành 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 để dự báo, lập kế hoạch mở rộng, nâng cấp, bảo đảm khả năng đáp ứng yêu cầu về an ninh mạng của hệ thống thông tin trong tương lai.

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

a) Cơ quan, đơn vị được giao quản lý, vận hành hệ thống thông tin phải thực hiện 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, phục vụ công tác phân tích, kiểm tra, điều tra, giám sát an ninh mạng.

b) Các sự kiện tối thiểu 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 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 của 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. Việc hủy bỏ hệ thống thông tin thuộc phạm vi quản lý của UBND xã do UBND xã quyết định bằng văn bản và thông báo đến các cơ quan, tổ chức, cá nhân có liên quan và đơn vị chuyên trách về an ninh mạng của tỉnh. Quá trình hủy bỏ được 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. Trước khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan, đơn vị chủ trì phải 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.

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; chỉ cho phép truy cập trong phạm vi được cấp quyền và chịu sự giám sát của UBND xã.

b) Yêu cầu bên cung cấp dịch vụ 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 thuộc phạm vi quản lý của UBND xã.

d) Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định về bảo đảm an ninh mạng, phải tạm dừng hoặc đình chỉ việc cung cấp dịch vụ tùy theo mức độ vi phạm; thông báo chính thức hành vi vi phạm của bên cung cấp dịch vụ cho cơ quan chức năng để phối hợp xử lý theo quy định của pháp luật; thu hồi ngay quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ; kiểm tra, xác định, lập báo cáo về 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, 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 và phương án kỹ thuật theo quy định tại Nghị định số 85/2016/NĐ-CP.

e) Yêu cầu bên cung cấp dịch vụ bảo đảm 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 số tỉnh Đắk Lắk và các tiêu chuẩn, quy chuẩn kỹ thuật có liên quan.

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 có liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ 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 liên tục, kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

4. Hợp đồng ký kết với bên cung cấp dịch vụ phải quy định chặt chẽ trách nhiệm của các bên và có cơ chế quản lý đối với các tài khoản thuộc 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 của hệ thống.

5. Khi có thay đổi về hệ thống, ứng dụng, mã nguồn hoặc chức năng của phần mềm phục vụ kết nối với hệ thống thông tin quan trọng về an ninh quốc gia, bên cung cấp dịch vụ có trách nhiệm phối hợp với UBND xã báo cáo Công an tỉnh để phối hợp với đơn vị nghiệp vụ thuộc 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, cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia và quy định của pháp luật.

**Điều 12. Quản lý Trung tâm dữ liệu/Phòng máy chủ**

1. Trường hợp UBND xã hoặc các cơ quan, đơn vị có Trung tâm dữ liệu, phòng máy chủ, các thiết bị tường lửa, máy chủ, hệ thống lưu trữ và các thiết bị có liên quan phải được đặt trong Trung tâm dữ liệu, phòng máy chủ; đồng thời, 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 được quản lý thống nhất, tập trung. Nhật ký hoạt động của thiết bị, phần mềm phải được lưu giữ trong thời gian phù hợp với cấp độ an toàn của hệ thống thông tin.

3. Việc mang thiết bị vào, ra Trung tâm dữ liệu, phòng máy chủ để lắp đặt hoặc sửa chữa phải được sự chấp thuận của người đứng đầu cơ quan, đơn vị được giao quản lý, vận hành.

**Điều 13. Quản lý Hệ thống mạng máy tính**

1. Hệ thống mạng máy tính thuộc phạm vi quản lý của UBND xã và các cơ quan, đơn vị 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 bằng 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 thông tin được xác định có chứa mã độc hoặc nội dung không phù hợp.

3. Việc 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 và được 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 cập Internet công cộng tại trụ sở UBND xã và các cơ quan, đơn vị phải niêm yết công khai nội quy sử dụng dịch vụ Internet tại nơi dễ nhận biết; được thiết lập thành vùng mạng riêng biệt, không kết nối với vùng mạng nội bộ chứa dữ liệu chuyên môn; sử dụng 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 tại UBND xã và các cơ quan, đơn vị phải được quản lý, vận hành và sử dụng theo quy định của Thủ tướng Chính phủ và hướng dẫn của Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ. Mạng truyền số liệu chuyên dùng chỉ được sử dụng cho mục đích công vụ, không được kết nối trực tiếp với Internet.

**Điều 14. Quản lý, sử dụng máy tính, thiết bị ngoại vi và phần mềm**

1. Máy tính và các thiết bị ngoại vi tại UBND xã và 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 thuộc danh mục được cơ quan có thẩm quyền cho phép sử dụng (nếu có). Nghiêm cấm tự ý cài đặt phần mềm không rõ nguồn gốc, phần mềm bẻ khóa, phần mềm không phục vụ công tác chuyên môn hoặc gỡ bỏ phần mềm khi chưa có sự đồng ý của người đứng đầu cơ quan, đơn vị và

ý kiến của chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin.

3. Tất cả máy tính phải được cài đặt phần mềm phòng, chống mã độc và thiết lập chế độ tự động cập nhật 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 như USB, ổ cứng ngoài trước khi sử dụng.

4. Khi phát hiện máy tính có dấu hiệu bất thường như hoạt động chậm, tự động mở các cửa sổ lạ, mất dữ liệu hoặc 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 người đứng đầu cơ quan, đơn vị, đồng thời thông báo cho chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin để phối hợp hỗ trợ, xử lý kịp thời.

5. Chỉ truy cập các trang thông tin điện tử, 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 các trình duyệt phổ biến; không truy cập, mở các trang thông 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 đối với tệp đính kèm tải về trước khi mở; 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 bằng 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 chuyên dùng công vụ và chứng thư chữ ký số chuyên dùng công vụ sử dụng trong hoạt động công vụ của UBND xã và các cơ quan, đơn vị được quản lý, cung cấp bởi tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ theo quy định của pháp luật về giao dịch điện tử, pháp luật về cơ yếu và pháp luật có liên quan.

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

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

4. Cơ quan, tổ chức, cá nhân được cấp chứng thư chữ ký số chuyên dùng công vụ phải thực hiện nghiêm trách nhiệm của thuê bao quy định tại Điều 39 Nghị định số 68/2024/NĐ-CP 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, cơ quan, đơn vị thuộc phạm vi quản lý của UBND xã 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 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. Nghiêm cấm việc sử dụng chung tài khoản.

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

4. Tài khoản người dùng phải sử dụng mật khẩu mạnh và thay đổi định kỳ tối thiểu 90 ngày/lần. Hệ thống phải 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 cho cá nhân làm công tác quản trị và phải sử dụng mật khẩu mạnh có tối thiểu 14 ký tự. Hệ thống phải 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. Cơ quan, đơn vị được giao quản lý, vận hành hệ thống thông tin có quyền khóa tài khoản truy cập trong trường hợp người sử dụng không tuân thủ các quy định về an ninh mạng hoặc phát hiện tài khoản có hành vi tấn công mạng, gây mất an ninh mạng.

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

1. Các cơ quan, đơn vị xây dựng và tổ chức thực hiện chính sách, quy trình quản lý dữ liệu gồm: phân loại dữ liệu, phân quyền truy cập, lưu trữ, sao lưu, khôi phục và tiêu hủy dữ liệu; 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. Khi thuê dịch vụ, các cơ quan, đơn vị phải yêu cầu bên cung cấp dịch vụ thiết lập giải pháp sao lưu tự động đối với dữ liệu trên máy chủ cơ sở dữ liệu và máy chủ ứng dụng; xây dựng các kịch bản có sẵn để khôi phục toàn bộ máy chủ hoặc các tệp tin, thư mục khi xảy ra sự cố.

2. Khuyến khích triển khai các giải pháp tăng tính sẵn sàng cho việc lưu trữ như RAID, nhân bản, cluster và các giải pháp phù hợp khác để giảm gián đoạn dịch vụ; các cơ chế này không thay thế việc sao lưu dữ liệu.

3. Đối với công tác sao lưu dự phòng và khôi phục dữ liệu, bao gồm 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 dữ liệu, phần mềm cần được sao lưu; phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra việc phục hồi hệ thống từ dữ liệu sao lưu.

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu, phục hồi dữ liệu. Cơ quan, đơn vị được giao quản lý hệ thống thông tin có trách nhiệm xây dựng tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành do mình quản lý.

4. Chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin phối hợp với các cơ quan, đơn vị có liên quan thực hiện phân loại tài sản thông tin, phần mềm và quy trình sao lưu dự phòng, phục hồi đối với các phần mềm, dữ liệu cần thiết theo quy định. Nội dung thực hiện gồm: lập danh sách dữ liệu, thông tin cấu hình mạng, máy chủ, phần mềm ứng dụng, cơ sở dữ liệu và tệp tin ghi nhật ký hệ thống cần sao lưu; 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, bảo đảm sẵn sàng sử dụng khi cần thiết. Việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu được thực hiện tối thiểu 06 tháng một lần hoặc khi có yêu cầu đột xuất.

6. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc máy trạm, cơ quan, đơn vị được giao vận hành hệ thống thông tin phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không chia sẻ toàn bộ ổ cứng; theo dõi, giám sát và kết thúc việc chia sẻ tài nguyên ngay sau khi hoàn thành. 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 được quản lý theo pháp luật về bảo vệ bí mật nhà nước; dữ liệu cá nhân được quản lý theo pháp luật về bảo vệ dữ liệu cá nhân và các 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 như máy tính xách tay, điện thoại thông minh, máy tính bảng và các thiết bị khác vào vùng mạng nội bộ của UBND xã, cơ quan, đơn vị để xử lý công việc phải được sự đồng ý của người đứng đầu cơ quan, đơn vị và tuân thủ các quy định về bảo đảm an ninh mạng tại Quy chế này; chịu sự theo dõi, giám sát của chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin.

**Điều 19. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến kiến thức về an ninh mạng**

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

2. Các cơ quan, đơn vị xác định nhu cầu đào tạo cho nguồn nhân lực về bảo đảm an ninh mạng tại cơ quan, đơn vị mình gửi Sở Nội vụ, Công an tỉnh tổng hợp, tham mưu tổ chức đào tạo.

3. Các cơ quan, đơn vị cử cán bộ tham gia hoặc phối hợp tổ chức đào tạo, bồi dưỡng kiến thức về an ninh mạng khi cần thiết.

4. Các cơ quan, đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an ninh mạng đến toàn thể cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị.

## Mục 3
## BẢO ĐẢM HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

**Điều 20. Phân loại và xác định cấp độ hệ thống thông tin**

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

2. Việc phân loại cấp độ hệ thống thông tin được thực hiện theo 5 cấp độ, từ cấp độ 1 đến cấp độ 5, dựa trên các tiêu chí quy định từ Điều 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 21. Lập, thẩm định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin**

1. Đối với hệ thống thông tin thuộc phạm vi quản lý của UBND xã, cơ quan, đơn vị được giao quản lý, vận hành có trách nhiệm phối hợp với Văn phòng HĐND và UBND xã lập hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP.

2. Hồ sơ đề xuất cấp độ hệ thống thông tin gồm: tài liệu mô tả tổng quan về hệ thống thông tin; tài liệu thiết kế hệ thống thông tin; thuyết minh đề xuất cấp độ hệ thống thông tin và thuyết minh phương án bảo đảm an ninh mạng đối với hệ thống thông tin.

3. Văn phòng HĐND và UBND xã tham mưu UBND xã gửi hồ sơ đề xuất cấp độ hệ thống thông tin đến cơ quan có thẩm quyền để thẩm định, phê duyệt theo quy định của pháp luật.

4. Trong quá trình thẩm định, phê duyệt, cơ quan, đơn vị được giao quản lý, vận hành hệ thống thông tin có trách nhiệm phối hợp với chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin cung cấp đầy đủ hồ sơ, tài liệu, thông tin có liên quan; chỉnh sửa, hoàn thiện hồ sơ theo yêu cầu của cơ quan có thẩm quyền.

**Điều 22. Phương án bảo đảm an ninh mạng theo cấp độ**

1. UBND xã với vai trò chủ quản hệ thống thông tin có trách nhiệm chỉ đạo Văn phòng HĐND và UBND xã, cơ quan, đơn vị được giao quản lý, 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 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 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; TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng.

3. Văn phòng HĐND và UBND xã theo dõi, đôn đốc việc triển khai phương án bảo đảm an ninh mạng; phối hợp với Công an tỉnh và trong việc hướng dẫn, kiểm tra, đánh giá kết quả thực hiện theo quy định.

**Điều 23. Bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia trên địa bàn tỉnh**

1. Các cơ quan, đơn vị có trách nhiệm rà soát, xác định các hệ thống thông tin thuộc phạm vi quản lý có đủ tiêu chuẩn, khả năng thuộc danh mục

quan trọng cần ưu tiên bảo đảm an ninh mạng và lập hồ sơ đề nghị đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo quy định.

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

3. Đơn vị chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải tổ chức triển khai đầy đủ các giải pháp bảo đảm an ninh mạng theo TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng. Kết nối vào Trung tâm An ninh mạng quốc gia và Trung tâm An ninh mạng tỉnh (nếu có), chia sẻ dữ liệu, giám sát liên tục 24/7.

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

### Điều 24. Kiểm tra, đánh giá an ninh mạng

1. UBND xã với vai trò chủ quản hệ thống thông tin có trách nhiệm tổ chức hoặc đề nghị cơ quan có thẩm quyền kiểm tra, đánh giá an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý.

2. Cơ quan, đơn vị chủ trì kiểm tra, đánh giá là cơ quan, đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn theo quy định. Đối tượng kiểm tra, đánh giá là cơ quan, đơn vị được giao quản lý, 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 lỗ hổng, điểm yếu bảo mật và đánh giá việc tuân thủ các quy định về bảo đảm an ninh mạng.

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, cụ thể 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 thực hiện theo quy định tại Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT và các quy định có liên quan. Việc thông báo kế hoạch, thành lập đoàn kiểm tra, lập biên bản và thông báo kết quả kiểm tra, đánh giá do cơ quan có thẩm quyền thực hiện theo quy định.

6. Văn phòng HĐND và UBND xã chủ trì tham mưu UBND xã phối hợp với cơ quan có thẩm quyền trong quá trình kiểm tra, đánh giá; theo dõi, đôn đốc việc khắc phục các tồn tại, hạn chế sau kiểm tra.

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

**Điều 25. Giám sát, cảnh báo an ninh mạng**

1. Các hệ thống thông tin thuộc phạm vi quản lý của UBND xã phải được giám sát, cảnh báo an ninh mạng phù hợp với cấp độ, phạm vi, quy mô và tính chất xử lý thông tin. Hệ thống thông tin từ cấp độ 3 trở lên và hệ thống thông tin quan trọng phải được ưu tiên giám sát thường xuyên, liên tục theo quy định. Cơ quan, đơn vị được giao vận hành hệ thống thông tin có trách nhiệm phối hợp với cơ quan chuyên môn cấp trên thực hiện việc giám sát theo quy định tại Thông tư số 31/2017/TT-BTTTT quy định hoạt động giám sát an toàn hệ thống thông tin.

2. UBND xã phối hợp với cơ quan chuyên môn cấp trên triển khai giải pháp giám sát an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý; trường hợp cần thiết, thực hiện thuê dịch vụ giám sát an ninh mạng theo quy định.

3. Các hệ thống thông tin thuộc phạm vi quản lý của UBND xã phải thực hiện kết nối, chia sẻ thông tin, dữ liệu giám sát với hệ thống giám sát an ninh mạng của tỉnh khi có yêu cầu và theo hướng dẫn của cơ quan có thẩm quyền.

4. Đối với hệ thống thông tin của UBND xã được đặt tại hạ tầng dùng chung của tỉnh, cơ quan, đơn vị được giao quản lý, vận hành có trách nhiệm phối hợp với đơn vị quản lý hạ tầng dùng chung của tỉnh và cơ quan có thẩm quyền trong việc giám sát kỹ thuật, tiếp nhận cảnh báo và xử lý nguy cơ mất an ninh mạng.

**Điều 26. Ứng cứu sự cố an ninh mạng**

1. UBND xã phối hợp với Đội ứng cứu sự cố an ninh mạng tỉnh và cơ quan có thẩm quyền trong hoạt động ứng cứu sự cố an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý.

2. Chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin có trách nhiệm tiếp nhận thông tin, tham mưu và phối hợp thực hiện việc giám sát, phát hiện, xử lý, khắc phục sự cố an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của UBND xã.

3. Khi xảy ra sự cố an ninh mạng, cơ quan, đơn vị được giao quản lý, vận hành hệ thống thông tin phải ưu tiên xử lý tại chỗ; đồng thời, báo cáo ngay UBND xã qua chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin. Trường hợp sự cố vượt quá khả năng xử lý, chuyên viên đầu mối tham mưu UBND xã báo cáo, đề nghị cơ quan chuyên môn cấp trên hỗ trợ, phối hợp xử lý.

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

a) UBND xã tổ chức triển khai phương án ứng cứu sự cố an ninh mạng của tỉnh trong phạm vi quản lý.

b) Chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin tham mưu UBND xã triển khai kế hoạch ứng cứu sự cố an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý theo cấp độ được phê duyệt.

**Điều 27. Quy trình ứng cứu sự cố an ninh mạng**

1. Việc ứng cứu sự cố an ninh mạng tại UBND xã thực hiện theo quy định của pháp luật, phương án ứng cứu sự cố an ninh mạng của tỉnh và hướng dẫn của cơ quan chuyên môn cấp trên; gồm các bước: phát hiện, tiếp nhận, phân loại, xử lý ban đầu, phân tích, khắc phục, điều tra, tổng kết và đánh giá.

2. Khi phát hiện sự cố an ninh mạng, cơ quan, đơn vị và người sử dụng phải ngắt kết nối thiết bị, hệ thống có nguy cơ gây mất an ninh mạng khi cần thiết; bảo vệ hiện trạng, không tự ý xóa dữ liệu, nhật ký hoặc dấu vết có liên quan; đồng thời, báo cáo ngay UBND xã qua chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin để tham mưu xử lý.

3. Chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin có trách nhiệm:

a) Tiếp nhận thông tin, xác định sơ bộ nguyên nhân, phạm vi và mức độ ảnh hưởng của sự cố.

b) Phối hợp với cơ quan, đơn vị quản lý, vận hành hệ thống thông tin thực hiện các biện pháp xử lý ban đầu, ngăn chặn sự cố lan rộng và khôi phục hoạt động của hệ thống.

c) Tham mưu UBND xã báo cáo, đề nghị cơ quan chuyên môn cấp trên hỗ trợ xử lý khi sự cố vượt quá khả năng xử lý của xã.

d) Phối hợp thực hiện các biện pháp xử lý, khắc phục sự cố theo hướng dẫn của cơ quan có thẩm quyền.

đ) Tổng hợp, báo cáo diễn biến, kết quả xử lý và đề xuất biện pháp phòng ngừa sự cố tái diễn.

4. Các cơ quan, đơn vị và cá nhân có liên quan có trách nhiệm phối hợp, cung cấp đầy đủ, kịp thời thông tin, tài liệu, dữ liệu và nhật ký phục vụ việc xác minh, xử lý, khắc phục sự cố theo yêu cầu của UBND xã và cơ quan có thẩm quyền.

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

**Điều 28. Bảo vệ bí mật nhà nước trên không gian mạng**

1. UBND xã và các cơ quan, đơn vị có xử lý thông tin thuộc bí mật nhà nước phải bố trí máy tính, máy in và các thiết bị ngoại vi 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 đổi mục đích sử dụng tài sản phần cứng; không 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 thuộc 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. Việc mang tài sản phần cứng có lưu trữ thông tin, tài liệu bí mật nhà nước ra khỏi trụ sở UBND xã hoặc cơ quan, đơn vị phải được người có thẩm quyền cho phép và thực hiện đầy đủ các biện pháp bảo vệ thông tin, tài liệu bí mật nhà nước lưu trữ trên tài sản đó.

5. Thiết bị lưu trữ di động như USB, ổ cứng ngoài và các thiết bị khác 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 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 các quy định của pháp luật về cơ yếu, bảo vệ bí mật nhà nước và an ninh mạng.

**Điều 29. Yêu cầu chung trong xử lý dữ liệu cá nhân**

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

2. Việc 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 cá nhân chỉ được xử lý đúng mục đích đã đăng ký hoặc thông báo.

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

**Điều 30. 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, nghĩa vụ theo quy định tại Điều 4 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15.

2. Người đứng đầu 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 theo quy định của pháp luật.

**Điều 31. Trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, đơn vị**

1. UBND xã là Bên Kiểm soát dữ liệu hoặc Bên Kiểm soát và xử lý dữ liệu cá nhân thuộc phạm vi quản lý, có trách nhiệm:

a) Phân công chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin phối hợp tham mưu công tác bảo vệ dữ liệu cá nhân.

b) Xây dựng, ban hành và tổ chức thực hiện quy định nội bộ về bảo vệ dữ liệu cá nhân.

c) Thực hiện đánh giá tác động xử lý dữ liệu cá nhân, lập và gửi hồ sơ đến cơ quan có thẩm quyền theo quy định.

2. Các cơ quan, đơn vị có trách nhiệm phối hợp, cung cấp đầy đủ thông tin, tài liệu phục vụ việc đánh giá tác động xử lý dữ liệu cá nhân; thực hiện các biện pháp bảo vệ dữ liệu cá nhân thuộc phạm vi được giao quản lý, xử lý.

3. Khi phát hiện hành vi vi phạm hoặc sự cố về dữ liệu cá nhân, cơ quan, đơn vị phải thực hiện ngay các biện pháp khắc phục ban đầu và báo cáo UBND xã qua chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin. UBND xã thực hiện 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 về dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác.

4. UBND xã và các cơ quan, đơn vị áp dụng 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 có thẩm quyền.

## Chương III
## TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG

### Điều 32. Trách nhiệm của Văn phòng HĐND và UBND xã

1. Tham mưu UBND xã tổ chức triển khai các quy định, chương trình, kế hoạch và văn bản chỉ đạo của cấp trên về bảo đảm an ninh mạng, an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của UBND xã.

2. Phân công chuyên viên làm đầu mối về an toàn thông tin; tiếp nhận, tổng hợp thông tin về nguy cơ, lỗ hổng, điểm yếu và sự cố an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của UBND xã.

3. Chủ trì, phối hợp với các cơ quan, đơn vị thực hiện quản lý, rà soát, cập nhật danh mục tài sản công nghệ thông tin; theo dõi việc quản lý, sử dụng máy tính, thiết bị ngoại vi, phần mềm, tài khoản, chữ ký số và các hệ thống thông tin dùng chung tại UBND xã.

4. Phối hợp với Công an xã và cơ quan chuyên môn cấp trên hướng dẫn, kiểm tra, giám sát việc thực hiện các quy định về bảo đảm an ninh mạng, an toàn thông tin; kịp thời cảnh báo nguy cơ, lỗ hổng và điểm yếu bảo mật đến các cơ quan, đơn vị, cá nhân có liên quan.

5. Tiếp nhận thông tin về sự cố an ninh mạng; tham mưu UBND xã triển khai biện pháp xử lý ban đầu, phối hợp khắc phục sự cố; trường hợp vượt quá khả năng xử lý của xã, tham mưu báo cáo, đề nghị cơ quan chuyên môn cấp trên hỗ trợ.

6. Phối hợp với cơ quan chuyên môn cấp trên tổ chức tập huấn, hướng dẫn, tuyên truyền, phổ biến kiến thức và kỹ năng bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức và người lao động thuộc UBND xã.

7. Theo dõi, đôn đốc các cơ quan, đơn vị thực hiện Quy chế này; tổng hợp tình hình, kết quả thực hiện, tham mưu UBND xã thực hiện chế độ báo cáo định kỳ, đột xuất theo quy định.

**Điều 33. Trách nhiệm của Phòng Văn hóa - Xã hội**

1. Chủ trì, tham mưu UBND xã triển khai các chương trình, đề án, kế hoạch về ứng dụng công nghệ thông tin, chuyển đổi số, phát triển chính quyền số, kinh tế số và xã hội số trên địa bàn xã; bảo đảm lồng ghép các yêu cầu về an toàn thông tin, an ninh mạng trong quá trình xây dựng và tổ chức thực hiện.

2. Phối hợp với Văn phòng HĐND và UBND xã, Công an xã và các cơ quan, đơn vị có liên quan trong việc tham gia ý kiến đối với các nội dung về công nghệ, hạ tầng số, hệ thống thông tin, nền tảng số thuộc phạm vi quản lý của UBND xã, bảo đảm tuân thủ yêu cầu về an toàn thông tin và an ninh mạng.

3. Chủ trì, phối hợp hướng dẫn, tuyên truyền, phổ biến các quy định của pháp luật về khoa học, công nghệ, chuyển đổi số, công nghệ số, an toàn thông tin và an ninh mạng cho các cơ quan, đơn vị, tổ chức và cá nhân trên địa bàn xã.

4. Phối hợp cung cấp thông tin, tài liệu thuộc lĩnh vực phụ trách khi có yêu cầu phục vụ việc kiểm tra, đánh giá hoặc ứng cứu sự cố an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của UBND xã.

5. Phối hợp với cơ quan chuyên môn cấp trên hướng dẫn các cơ quan, đơn vị triển khai, quản lý, khai thác hiệu quả hạ tầng số, nền tảng số dùng chung; thúc đẩy ứng dụng khoa học, công nghệ, đổi mới sáng tạo, trí tuệ nhân tạo, dữ liệu số và chuyển đổi số, bảo đảm tuân thủ các yêu cầu về an toàn thông tin, an ninh mạng trong hoạt động của cơ quan nhà nước.

**Điều 34. Trách nhiệm của Phòng Kinh tế**

1. Chủ trì, phối hợp với Văn phòng HĐND và UBND xã tham mưu UBND xã bố trí kinh phí thực hiện các nhiệm vụ, đề án, dự án về bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu theo quy định của Luật Ngân sách nhà nước số 89/2025/QH15 và các văn bản hướng dẫn có liên quan.

2. Tổng hợp, tham mưu UBND xã bố trí kế hoạch vốn trung hạn, hằng năm đối với các nhiệm vụ, đề án, dự án về bảo đảm an ninh mạng thuộc phạm vi quản lý của UBND xã khi đáp ứng đầy đủ điều kiện theo quy định.

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

1. UBND xã là chủ quản đối với các hệ thống thông tin thuộc phạm vi quản lý; có thể giao Văn phòng HĐND và UBND xã hoặc cơ quan, đơn vị có liên quan trực tiếp quản lý, vận hành hệ thống thông tin theo chức năng, nhiệm vụ được giao.

2. Chủ tịch UBND xã trực tiếp chỉ đạo công tác bảo đảm an ninh mạng và chịu trách nhiệm trước pháp luật, cơ quan có thẩm quyền về công tác bảo đảm an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của UBND xã.

3. Giao chuyên viên Văn phòng HĐND và UBND xã làm đầu mối về an toàn thông tin; tham mưu, phối hợp triển khai các nhiệm vụ bảo đảm an ninh mạng. Căn cứ khả năng cân đối ngân sách, UBND xã bố trí nhân lực, kinh phí, trang thiết bị để thực hiện nhiệm vụ theo quy định.

4. Chỉ đạo lập, hoàn thiện và trình cơ quan có thẩm quyền thẩm định, phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin; xây dựng và tổ chức thực hiện phương án bảo đảm an ninh mạng tương ứng với cấp độ được phê duyệt.

5. Ban hành và tổ chức thực hiện các quy định về bảo đảm an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của UBND xã.

6. Tổ chức hoặc phối hợp với cơ quan chuyên môn cấp trên thực hiện việc kiểm tra, đánh giá và quản lý rủi ro an ninh mạng định kỳ theo quy định.

7. Phối hợp với Công an xã, Công an tỉnh và các cơ quan, đơn vị có liên quan trong công tác phòng ngừa, phát hiện, đấu tranh, ngăn chặn các hành vi xâm phạm an ninh mạng.

8. Cung cấp thông tin, tài liệu và tạo điều kiện cho cơ quan có thẩm quyền thực hiện việc kiểm tra, đánh giá, ứng cứu và khắc phục sự cố an ninh mạng kịp thời, hiệu quả.

9. Các cơ quan, đơn vị được giao quản lý, vận hành hoặc sử dụng hệ thống thông tin có trách nhiệm bảo đảm an ninh mạng đối với hệ thống được giao; phân công cán bộ, công chức, viên chức phối hợp với chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin trong quá trình quản lý, vận hành và xử lý sự cố. Trường hợp hệ thống thông tin thuộc diện phải bố trí lực lượng bảo vệ an ninh mạng thì thực hiện theo quy định của Chính phủ và hướng dẫn của cơ quan có thẩm quyền.

**Điều 36. Trách nhiệm của đơn vị vận hành hệ thống thông tin**

1. Cơ quan, đơn vị được UBND xã giao quản lý, vận hành hệ thống thông tin có trách nhiệm:

a) Phối hợp với chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin thực hiện việc xác định, đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP.

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

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng, báo cáo UBND xã xem xét, điều chỉnh khi cần thiết.

d) Phối hợp và thực hiện yêu cầu của cơ quan có thẩm quyền trong công tác bảo đảm an ninh mạng.

đ) Kịp thời triển khai phương án ứng cứu sự cố; thông báo ngay cho UBND xã qua chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin; phối hợp với các cơ quan, đơn vị có liên quan xử lý sự cố an ninh mạng.

e) Thực hiện chế độ báo cáo định kỳ hoặc đột xuất về công tác bảo đảm an ninh mạng đối với hệ thống thông tin theo yêu cầu của UBND xã và cơ quan có thẩm quyền.

2. Trường hợp UBND xã trực tiếp quản lý, vận hành hệ thống thông tin thì Văn phòng HĐND và UBND xã chủ trì, phối hợp với các cơ quan, đơn vị có liên quan thực hiện các trách nhiệm quy định tại khoản 1 Điều này.

3. Trường hợp thuê dịch vụ công nghệ thông tin theo hợp đồng, 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 và phối hợp chặt chẽ với UBND xã, Văn phòng HĐND và UBND xã trong quá trình thực hiện.

**Điều 37. Trách nhiệm của cán bộ, công chức, viên chức và người lao động**

**1.** Cán bộ, công chức, viên chức và người lao động có trách nhiệm:

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

b) Quản lý, bảo quản và bảo đảm an ninh mạng đối với tài sản công nghệ thông tin được giao quản lý, sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an ninh mạng, phải báo cáo ngay người đứng đầu cơ quan, đơn vị và thông báo cho chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin để kịp thời phối hợp ngăn chặn, xử lý.

d) Tham gia đầy đủ, nghiêm túc các chương trình đào tạo, tập huấn, diễn tập về an ninh mạng do cơ quan có thẩm quyền tổ chức.

đ) Bảo đảm an ninh mạng đối với hệ thống thông tin, tài khoản, dữ liệu và thiết bị công nghệ thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, của ngành và Quy chế này.

2. Ngoài trách nhiệm quy định tại khoản 1 Điều này, chuyên viên Văn phòng HĐND và UBND xã được giao làm đầu mối về an toàn thông tin có trách nhiệm:

a) Tham mưu lãnh đạo Văn phòng HĐND và UBND xã, UBND xã triển khai thực hiện Quy chế này và các quy định của pháp luật có liên quan đến an ninh mạng, an toàn thông tin.

b) Tham mưu hoặc phối hợp triển khai các biện pháp kỹ thuật bảo đảm an ninh mạng đối với hạ tầng kỹ thuật, hệ thống thông tin thuộc phạm vi quản lý của UBND xã; hướng dẫn cán bộ, công chức, viên chức và người lao động thực hiện các biện pháp bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin.

c) Phối hợp theo dõi, giám sát, đánh giá, ghi nhận thông tin; báo cáo kịp thời lãnh đạo Văn phòng HĐND và UBND xã, UBND xã về sự cố mất an ninh mạng và mức độ nghiêm trọng của sự cố.

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

**Điều 38. 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 39. Chế độ, nội dung báo cáo**

Các cơ quan, đơn vị có trách nhiệm báo cáo UBND xã về công tác bảo đảm an ninh mạng, an toàn thông tin theo định kỳ và đột xuất như sau:

1. Báo cáo định kỳ hằng năm về tình hình, kết quả thực hiện Quy chế này, gửi UBND xã qua Văn phòng HĐND và UBND xã trước ngày 15 tháng 12.

2. Báo cáo đột xuất về tình hình, kết quả ứng cứu sự cố an ninh mạng; việc khắc phục, xử lý lỗ hổng, điểm yếu bảo mật, cảnh báo an ninh mạng và các nội dung khác theo yêu cầu của UBND xã hoặc cơ quan có thẩm quyền. Khi xảy ra sự cố nghiêm trọng, phải báo cáo ngay, không chờ tổng hợp theo chế độ định kỳ.

3. Văn phòng HĐND và UBND xã chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổng hợp tình hình, kết quả thực hiện; tham mưu UBND xã báo cáo cơ quan có thẩm quyền theo quy định.

**Điều 40. Kinh phí thực hiện**

Kinh phí bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của UBND xã và các cơ quan, đơn vị được bố trí từ ngân sách nhà nước theo phân cấp ngân sách hiện hành và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

**Điều 41. Trách nhiệm thi hành**

1. Người đứng đầu các cơ quan, đơn vị và các tổ chức, cá nhân có liên quan chịu trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý. Trong quá trình thực hiện, nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị kịp thời phản ánh về UBND xã qua Văn phòng HĐND và UBND xã để tổng hợp, tham mưu xem xét, sửa đổi, bổ sung hoặc báo cáo cơ quan có thẩm quyền.

2. Văn phòng HĐND và UBND xã có trách nhiệm theo dõi, đôn đốc, kiểm tra và tổng hợp tình hình thực hiện Quy chế này; phối hợp với Công an xã, Phòng Văn hóa - Xã hội và các cơ quan, đơn vị có liên quan tham mưu UBND xã xử lý các vấn đề phát sinh.

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 văn bản sửa đổi, bổ sung hoặc thay thế đó.