| | |
|---|---|
| **ỦY BAN NHÂN DÂN**<br>**XÃ HÀ BẮC** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số:644 /QĐ-UBND | *Hà Bắc, ngày 14 tháng 4 năm 2026* |

# QUYẾT ĐỊNH
## Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Hà Bắc

## ỦY BAN NHÂN DÂN XÃ HÀ BẮC

*Căn cứ Luật tổ chức Chính quyền địa phương ngày 16 tháng 6 năm 2025;*

*Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006; Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;*

*Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018; Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;*

*Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng; Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Theo đề nghị của Chánh Văn phòng HĐND và UBND xã Hà Bắc.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Hà Bắc.

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

**Điều 3.** Chánh Văn phòng HĐND và UBND xã, Thủ trưởng các cơ quan thuộc UBND xã, các đơn vị liên quan chịu trách nhiệm thi hành quyết định này./.

***Nơi nhận:***
- Công an Thành phố;(Để báo cáo)
- TT Đảng ủy; TT HĐND xã;
- Chủ tịch, các PCT UBND;
- Như Điều 3;
- Lưu: VT.

**TM. ỦY BAN NHÂN DÂN**
**CHỦ TỊCH**

U.B.N.D XÃ HÀ BẮC T.P HẢI PHÒNG

**Nguyễn Anh Tuấn**

| | |
|---|---|
| **ỦY BAN NHÂN DÂN**<br>**XÃ HÀ BẮC** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |

# QUY CHẾ
## Bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Hà Bắc

*(Ban hành kèm theo Quyết định số: 644 /QĐ-UBND ngày 14 /4/2026 của Ủy ban nhân dân xã Hà Bắc)*

## Chương I
## NHỮNG QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống mạng nội bộ và các hệ thống thông tin của UBND xã Hà Bắc, bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức;
- Các ứng dụng, dịch vụ hệ thống cung cấp;
- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

- Cán bộ, công chức, viên chức và người lao động thuộc UBND xã Hà Bắc;
- Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ tại UBND xã Hà Bắc;
- Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống mạng nội bộ.

**Điều 2. Giải thích từ ngữ**

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

*1. An toàn thông tin mạng*: Là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

*2. Mạng*: Là môi trường, trong đó thông tin được cung cấp, truyền đưa, thu thập,xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

*3. Hệ thống thông tin*: Là tập hợp phần cứng, phần mềm và cơ sở 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 mạng.

*4. 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.

*5. Xâm phạm an toàn thông tin mạng*: Là hành vi truy nhập, sử dụng, tiết lộ,làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

*6. Sự cố an toàn thông tin mạng*: Là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

*7. Rủi ro an toàn thông tin mạng*: Là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

*8. Đánh giá rủi ro an toàn thông tin mạng*: Là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

*9. Quản lý rủi ro an toàn thông tin mạng*: Là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

*10. Phần mềm độc hại*: Là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép,sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

*11. Hệ thống lọc phần mềm độc hại*: Là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

*12. Địa chỉ điện tử*: Là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

*13. Xung đột thông tin*: Là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin,hệ thống thông tin trên mạng.

*14. Thông tin cá nhân*: Là thông tin gắn với việc xác định danh tính của mộtngười cụ thể.

*15. Xử lý thông tin cá nhân*: Là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

*16. Sản phẩm an toàn thông tin mạng*: Là phần cứng, phần mềm có chức năngbảo vệ thông tin, hệ thống thông tin.

*17. Dịch vụ an toàn thông tin mạng*: Là dịch vụ bảo vệ thông tin, hệ thống thông tin.

**Điều 3. Chủ quản hệ thống thông tin; đơn vị chuyên trách về an toàn thông tin; đơn vị vận hành hệ thống thông tin**

1. Chủ quản hệ thống thông tin

- Là cấp có thẩm quyền quyết định đầu tư, xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

- Trong trường hợp cần thiết, chủ quản hệ thống thông tin ủy quyền cho một tổ chức trực thuộc có đủ năng lực để thay mặt thực hiện trách nhiệm của chủ quản

hệ thống thông tin quy định tài khoản 2, Điều 20 Nghị định 85/2016/NĐ-CP. Việc ủy quyền trách nhiệm chủ quản hệ thống thông tin phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi của hệ thống, trách nhiệm của tổ chức được ủy quyền và thời hạn ủy quyền.

2. Đơn vị chuyên trách về an toàn thông tin, Bộ phận chuyên trách về an toàn thông tin

Đơn vị/Bộ phận phụ trách hệ thống thông tin là đơn vị được chủ quản hệ thống thông tin chỉ định; có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

3. Đơn vị vận hành hệ thống thông tin

- 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.

- Trong trường hợp hệ thống thông tin gồm nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin có trách nhiệm chỉ định một đơn vị chủ trì thực hiện quyền và nghĩa vụ của đơn vị vận hành hệ thống thông tin theo quy định của pháp luật.

- Trong trường hợp thuê dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin được xác định như sau:

+ Trường hợp chưa xác định được đơn vị cung cấp dịch vụ theo quy định của pháp luật, đơn vị chủ trì thuê dịch vụ đóng vai trò là đơn vị vận hành.

+ Trường hợp đã xác định được đơn vị cung cấp dịch vụ theo quy định của pháp luật thì đơn vị vận hành là đơn vị cung cấp dịch vụ.

+ Trường hợp hết thời hạn cung cấp dịch vụ, nếu hệ thống thông tin được thiết lập qua hình thức thuê dịch vụ vẫn tiếp tục duy trì hoạt động, đơn vị vận hành được xác định là đơn vị chủ trì thuê dịch vụ.

**Điều 4. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin**

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của hệ thống thông tin.

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn hệ thống thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

3. Phạm vi chính sách an toàn thông tin

a) Thiết lập chính sách an toàn thông tin.

b) Tổ chức bảo đảm an toàn thông tin.

c) Bảo đảm nguồn nhân lực.

d) Quản lý thiết kế, xây dựng hệ thống.

e) Quản lý vận hành hệ thống.

**Điều 5. Những hành vi nghiêm cấm**

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phátsóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng mộtthiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, trao đổi thành phần của máy tính phục vụ công việc.

**Điều 6. Phối hợp với những cơ quan, tổ chức có thẩm quyền**

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin.

a) UBND xã Hà Bắc công chức chuyên trách chuyển đổi số, an toàn thông tin mạng, an ninh mạng là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống mạng nội bộ.

- Công chức được giao nhiệm vụ có trách nhiệm tham gia đầy đủ các hoạt động phối hợp, đào tạo, tập huấn, các chương trình công tác bảo đảm an toàn 3 thông tin khi có yêu cầu của tổ chức có thẩm quyền.

**Điều 7. Bảo đảm nguồn nhân lực**

1. Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Xây dựng kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

3. Trách nhiệm bảo đảm an toàn thông tin cho cán bộ quản lý và vận hành hệ thống.

a) Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

b) Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

c) Các cơ quan, địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

4. Với người sử dụng

- Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

- Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mìnhđược giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc.

a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức.

b) Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

## Chương II
## BẢO ĐẢM AN TOÀN THÔNG TIN TRONG THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

### Điều 8. Thiết kế, xây dựng hệ thống thông tin

1. Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Xây dựng các tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

4. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

6. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin phải xây dựng phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin

thẩm định (hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân thành phố) trước khi trình cấp có thẩm quyền phê duyệt dự án.

7. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin.

a) Chủ quản hệ thống thông tin có trách nhiệm tổ chức đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) và Thông tư 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông để áp dụng phương án bảo đảm an toàn thông tin phù hợp.

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân thành phố thẩm định, trình cấp có thẩm quyền phê duyệt.

8. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, Chủ quản hệ thống thông tin phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10 Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

**Điều 9. Phát triển phần mềm thuê khoán**

1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Các nhà phát triển cung cấp mã nguồn phần mềm.

3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trướckhi đưa vào sử dụng.

**Điều 10. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin**

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng thông tin điện tử, Trang thông tin điện tử.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

c) Phải bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

## Chương III
## BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

### Điều 11. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

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

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

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

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

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

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

3. Truy cập và quản lý cấu hình hệ thống

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

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo

cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

**Điều 12. Quản lý an toàn máy chủ và ứng dụng**

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

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

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

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. - Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp. - Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

- Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụcho việc gia hạn.

2. Truy cập mạng của máy chủ Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

3. Truy cập và quản trị máy chủ và ứng dụng

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

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

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

4. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông

tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng. Bộ phận chuyên trách về công nghệ thông tin của đơn vị chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận công nghệ thông tin của đơn vị.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủtrước khi đưa vào vận hành, khai thác.

7. Các máy chủ trước khi đưa vào vận hành khai thác cần triển khai một sốyêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

e) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

**Điều 13. Quản lý an toàn dữ liệu**

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

a) Đơn vị xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

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

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

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

a) Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin;chế độ bảo quản thông tin.

b) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

c) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến chocác tổ chức, cá nhân bên ngoài.

d) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

5. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

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 của hệ thống: Đơn vị quản trị hệ thống 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.

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

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

b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.

c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

**Điều 14. Quản lý an toàn thiết bị đầu cuối**

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

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực vàsử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

**Điều 15. Quản lý phòng chống phần mềm độc hại**

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như:

(.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe)…

3. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

5. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

6. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

**Điều 16. Quản lý giám sát an toàn hệ thống thông tin**

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

4. Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9 Thông tư số 31/2017/TT-BTTTT.

5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

**Điều 17. Quản lý điểm yếu an toàn thông tin**

1. Đơn vị hoặc Bộ phận chuyên trách về an toàn thông tin có trách nhiệm.

a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Báo cáo Lãnh đạo, cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không giảm ảnh hưởng/gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

3. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c, khoản 2, Điều 20 Nghị định số 85/2016/NĐCP và Điều 13 Thông tư số 03/2017/TT-BTTTT.

**Điều 18. Quản lý sự cố an toàn thông tin**

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

2. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05/2017/QĐ-TTg.

3. Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

5. Phối hợp với cơ quan chức năng, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

**Điều 19. Quản lý an toàn người sử dụng đầu cuối**

1. Kết nối máy tính, thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

2. Trong quá trình sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

## Chương IV
## KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

### Điều 20. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực hiện các nội dung tại quy chế này; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định và theo quy định của hệ thống an toàn thông tin.

2. Hình thức kiểm tra, đánh giá.

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin, theo kế hoạch của xã và đơn vị chuyên trách về an toàn thông tin của thành phố.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá.

a) Ủy ban nhân dân thành phố hoặc Sở Khoa học và Công nghệ thành phố (đơn vị chuyên trách CNTT của TP).

b) UBND xã giao nhiệm vụ kiểm tra về an toàn thông tin trên địa bàn xã cho Văn phòng HĐND và UBND phối hợp với Công an xã, phòng Văn hoá – xã hội.

4. 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 nhiệm vụ kiểm tra, đánh giá.

5. 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.

**Điều 21. Kế hoạch kiểm tra hàng năm**

1. Công chức chuyên trách chuyển đổi số, an toàn thông tin mạng, an ninh mạng chủ trì, phối hợp với các đơn vị liên quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn xã theo Kế hoạch công tác hàng năm.

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin trên địa bàn xã.

## Chương V
## BÁO CÁO, CHIA SẺ THÔNG TIN

**Điều 22. Chế độ báo cáo**

1. Báo cáo định kỳ.

a) Báo cáo an toàn thông tin định kỳ hằng năm gồm các nội dung quy định tại Điều 14 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT.

2. Báo cáo đột xuất.

Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, gửi và phê duyệt báo cáo.

- Các cơ quan, đơn vị nhà nước trên địa bàn xã chịu trách nhiệm.

- Đối với đơn vị chủ quản hệ thống thông tin.

+ Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi Bộ Thông tin và Truyền thông trước ngày 25 tháng 12 hàng năm.

+ Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi về UBND xã trước ngày 15 tháng 6 và 15 tháng 12 hàng năm. Đồng thời gửi Sở Khoa học và công nghệ, Công an thành phố Hải Phòng khi có yêu cầu.

- Báo cáo đột xuất theo hướng dẫn của đơn vị chủ quản hệ thống thông tin, UBND TP, Sở Khoa học và công nghệ và các đơn vị cấp trên theo quy định.

4. Phương thức gửi, nhận báo cáo. Phương thức gửi và nhận báo cáo được quy định tại khoản 1, Điều 13 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

5. Thời gian báo cáo.

- Đối với báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này: Tính từ ngày 15 tháng 12 năm trước kỳ báo cáo đến ngày 14 tháng 12 của kỳ báo cáo.

- Đối với báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b, khoản 1 điều này: Thời gian chốt số liệu 6 tháng đầu năm được tính từ ngày 15 tháng 12 năm trước kỳ báo cáo đến ngày 14 tháng 6 của kỳ báo cáo. Thời gian chốt số liệu 6 tháng cuối năm được tính từ ngày 15 tháng 6 đến ngày 14 tháng 12 của kỳ báo cáo.

**Điều 23. Chia sẻ thông tin**

Việc chia sẻ dữ liệu số của các hệ thống thông tin với các cơ quan nhà nước được thực hiện theo quy định tại Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về việc quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước.

## Chương VI
## TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

**Điều 24. Đơn vị chủ quản hệ thống thông tin**

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ định đơn vị vận hành, đơn vị/Bộ phận chuyên trách về an toàn thông tin của đơn vị mình.

**Điều 25. Đơn vị vận hành**

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo các đơn vị thuộc, trực thuộc thực hiện quản lý ứng dụng; quản lý dữ liệu và các đơn vị có liên quan vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật, triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

3. Lập hồ sơ đề xuất cấp độ, gửi về Đơn vị hoặc Bộ phận chuyên trách về ATTT của chủ quản hệ thống thông tin thẩm định (theo quy định tại Nghị định số 15/2016/NĐ-CP).

**Điều 26. Trách nhiệm của Đơn vị/Bộ phận chuyên trách về ATTT**

Thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng theo các quy định tại Quy chế này tại UBND xã và hướng dẫn các đơn vị thuộc, trực thuộc UBND xã triển khai đảm bảo an toàn, an ninh mạng trong hoạt động ứng dụng CNTT tại đơn vị mình.

**Điều 27. Trách nhiệm của đơn vị cung cấp dịch vụ**

1. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; thiết kế, thiết lập hệ thống đáp ứng các yêu cầu kỹ thuật các cấp độ theo tiêu chuẩn quy định.

2. Quản lý, vận hành, bảo đảm an toàn thông tin cho các thành phần hệ thống thuộc phạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

3. Lập hồ sơ cấp độ của hệ thống thông tin, gửi về đơn vị vận hành hệ thống để chuyển đến đơn vị, các cấp có thẩm quyền để thẩm định, phê duyệt hệ thống.

**Điều 28. Trách nhiệm của đơn vị, tổ chức, cá nhân sử dụng hệ thống**

Sử dụng hệ thống thông tin đảm bảo an toàn thông tin theo Quy chế này.

**Điều 29. Bảo đảm an ninh mạng**

Thực hiện theo Điều 12, Điều 13, Điều 14 của Quyết định số 1512/QĐ-BTTTT ngày 05/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Quy chế bảo đảm an toàn thông tin mạng và các quy định khác có liên quan.

## Chương VI
## TỔ CHỨC THỰC HIỆN

**Điều 30. Tổ chức triển khai Quy chế**

- Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

- Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Bộ phận chuyên trách để xem xét, bổ sung, sửa đổi.

**Điều 31. Khen thưởng và xử lý vi phạm**

1. Xem xét, khen thưởng cho các cá nhân, phòng ban có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng trong quản lý, vận hành, khai thác Hệ thống mạng nội bộ của đơn vị.

2. Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

**Điều 32. Xây dựng, rà soát, cập nhật, bổ sung Quy chế**

- Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.

- Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Bộ phận chuyên trách về ATTT để tổng hợp báo cáo điều chỉnh, bổ sung.

**Điều 33. Đơn vị hoặc Bộ phận chuyên trách về an toàn thông tin**

- Giao một Chuyên viên Văn phòng là bộ phận chuyên trách về ATTT cho hệ thống thông tin của UBND xã.

- Chuyên viên Phòng Văn hoá - xã hội phối hợp với các phòng, ban, ngành có liên quan nghiên cứu và tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo chỉ đạo của UBND xã.

- Triển khai các phương án đảm bảo an toàn thông tin tại cơ quan UBND xã.

**Điều 34. Các cơ quan, đơn vị trên địa bàn xã**

- Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn xã và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

- Phòng Văn hoá - xã hội có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân xã theo định kỳ hàng năm hoặc đột xuất theo yêu cầu của UBND xã và cơ quan có thẩm quyền của thành phố.

- Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Văn phòng HĐND và UBND hoặc Phòng Văn hoá - xã hội để tổng hợp báo cáo Ủy ban nhân dân xã xem xét điều chỉnh, bổ sung./.