| | |
|---|---|
| **ỦY BAN NHÂN DÂN**<br>**XÃ VĨNH LẠI** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số: 602/QĐ-UBND | *Vĩnh Lại, ngày 01 tháng 8 năm 2025* |

# QUYẾT ĐỊNH
**Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn xã Vĩnh Lại**

## CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ VĨNH LẠI

*Căn cứ Luật Tổ chức chính quyền địa phương ngày 16/6/2025;*

*Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;*

*Căn cứ Luật An ninh mạng ngày 12/06/2018;*

*Căn cứ 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 584//QĐ-UBND, ngày 28/02/2025 của UBND thành phố Hải Phòng về việc chuyển chức năng, nhiệm vụ quản lý nhà nước về an toàn thông tin mạng từ Sở Thông tin và Truyền thông sang Công an thành phố,*

*Căn cứ Công văn số 916/CAHP-ANM, ngày 14/4/2025 của Công an thành phố Hải Phòng về việc thực hiện công tác bảo đảm an ninh mạng và an toàn thông tin;*

*Theo đề nghị của Trưởng Công an xã Vĩnh Lại.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này, Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn xã Vĩnh Lại.

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

**Điều 3.** Chánh Văn phòng HĐND và UBND xã, Giám đốc Trung tâm phục vụ hành chính công, Trưởng công an xã; Thủ trưởng các phòng, ban và các cơ quan, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***
- Như Điều 3;
- Sở KHCN;
- TT Đảng ủy, TT HĐND xã; (để b/c)
- Chủ tịch, các PCT UBND xã;
- Cổng TTĐT xã;
- Lưu: VT, CAX, VHXH.

**CHỦ TỊCH**



**Nguyễn Văn Hướng**

ỦY BAN NHÂN DÂN
XÃ VĨNH LẠI

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

# QUY CHẾ
## Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn xã Vĩnh Lại

*(Ban hành kèm theo Quyết định số 602/QĐ-UBND ngày 01/8/2025 của Ủy ban nhân xã Vĩnh Lại)*

## Chương I
## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh

Quy chế này quy định biện pháp, chính sách quản lý nhằm bảo đảm an toàn thông tin các hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn xã Vĩnh Lại.

### Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng với các cơ quan quản lý hành chính nhà nước và các đơn vị sự nghiệp thuộc Ủy ban nhân dân xã Vĩnh Lại; các tổ chức chính trị-xã hội được ngân sách nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin do Ủy ban nhân dân xã triển khai (sau đây gọi tắt là các cơ quan, đơn vị); cán bộ, công chức, viên chức, người lao động làm việc tại các cơ quan, đơn vị nêu trên (sau đây gọi tắt là cán bộ).

2. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các cơ quan, đơn vị thuộc khoản 1 Điều này.

### Điều 3. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là công tác 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. *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 của một cơ quan, tổ chức.

3. *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.

4. *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 chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

5. *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.

6. *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.

7. *Mạng ngang hàng* là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

8. *Đơn vị chuyên trách về công nghệ thông tin* là đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin do chủ quản hệ thống thông tin chỉ định.

9. *Đơn vị chuyên trách về an toàn thông tin* là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

10. *Cán bộ chuyên trách* là cán bộ, công chức, viên chức, người lao động được tuyển dụng phụ trách an toàn thông tin/công nghệ thông tin tại các cơ quan, đơn vị.

**Điều 4. Các hành vi bị nghiêm cấm**

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015. Cụ thể:

a) Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật;

b) Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng;

c) Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin;

d) Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo;

đ) Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân;

e) Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

2. Tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point) vào mạng máy tính của cơ quan, đơn vị và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card,

wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan, đơn vị;

3. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng; phá hại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại;

4. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

5. Tự ý tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

**Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền**

1. Phân công bộ phận phụ trách về an toàn an ninh mạng, an toàn thông tin:

UBND xã giao Công an xã là cơ quan phụ trách về an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn xã Vĩnh Lại.

2. Trách nhiệm của bộ phận phụ trách về an toàn thông tin:

a. Là đầu mối liên hệ, tiếp nhận, phối hợp với các cơ quan, tổ chức (có thẩm quyền quản lý về an toàn thông tin) trong công tác đảm bảo an toàn thông tin, hỗ trợ điều phối xử lý sự cố an toàn thông tin;

b. Là đầu mối liên hệ, phối hợp với Công an thành phố và 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 các Hệ thống Thông tin do UBND xã triển khai;

c. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền;

d. Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ UBND xã;

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

e. Phối hợp chặt chẽ với Công an thành phố, Sở Khoa học và Công nghệ và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng;

f. Định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Công an thành phố (theo hướng dẫn của Công an thành phố).

**Điều 6. Bảo đảm nguồn nhân lực**

1. Tuyển dụng

a. Cán bộ được tuyển dụng vào vị trí việc 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;

b. Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ;

c. Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a. Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b. Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

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

3. Chấm dứt thay đổi công việc

a. Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, 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 (nếu có) thuộc UBND xã sở hữu của tổ chức;

b. Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c. Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

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

**Điều 7. Thiết kế an toàn hệ thống thông tin**

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

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

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

4. Có 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. Có phương án quản lý và bảo vệ hồ sơ thiết kế.

7. Có bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế hệ

thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện.

**Điều 8. Phát triển phần mềm thuê khoán**

1. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

5. Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm.

6. Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

**Điều 9. Thử nghiệm và nghiệm thu hệ thống**

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

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

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

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

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

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

**Điều 10. Quản lý an toàn mạng**

1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật;

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

4. Quản lý, vận hành hoạt động bình thường của hệ thống:

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 phục vụ cho việc gia hạn.

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

h. Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

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

k. Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

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

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

b. Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c. Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d. Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

6. 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 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.

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

8. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trườngmạng;

9. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sửdụng;

10. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học, thư rác cho những hệ thống xung yếu (máy chủ thư điện tử, máy chủ website, máy chủ tên miền, v.v...) và tại các máy chủ, máy trạm khác trong hệthống;

11. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy;

12. Đối với các thiết bị mạng chính

a. Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét: một cho đường cung cấp điện và một cho đường mạng nội bộ (LAN);

b. Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin học của cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network

Administration Security);

c. Tường lửa (firewall): Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu vào, ra và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS);

13. Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng;

14. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảmhọa.

**Điều 11. Quản lý an toàn máy chủ và ứng dụng**

1. Hạ tầng mạng triển khai hệ thống phải được thiết kế theo các phân vùng chức năng, tách biệt và có biện pháp kỹ thuật để hạn chế và giám sát được truy cập giữa các phân vùng mạng, tuân theo thiết kế đã được phê duyệt, bao gồm tối thiểu 03 phân vùng mạng:

a) Vùng mạng nội bộ (LAN - local area network): được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống.

b) Vùng mạng biên (outsize zone): được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

c) Vùng DMZ (demilitarized zone): được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet

2. 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.

3. 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.

4. 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; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

d. Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

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

e. Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

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

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

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

b. Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c. Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d. Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

6. Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

7. Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…).

**Điều 12. 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. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động;

5. 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;

6. 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;

7. 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 13. 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 14. Quản lý điểm yếu an toàn hệ thống thông tin**

1. Đơn vị/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 giám 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;

đ. 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/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT.

**Điều 15. Quản lý an toàn dữ liệu**

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

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

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

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

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

4. 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).

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

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

7. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

8. 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 theo yêu cầu của đơn vị vận hành.

9. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

10. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn;

11. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

**Điều 16. Quản lý an toàn người sử dụng đầu cuối**

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích kinh doanh của công ty. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

3. Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Đơn vị chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

5. Đơn vị chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.

6. Đơn vị chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

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

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, tổchức.

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 thôngtin.

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.

d. Đối với hệ thống thông tin có cấp độ 3 trở lên, 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 hệthống.

8. Quản lý truy cập mạng và tài nguyên trên Internet:

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 thành phố hoặc đơn vị chuyên môn tổ chức.

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

**Điều 17. Quản lý sự cố an toàn thông tin**

1. Phân nhóm sự cố an toàn thông tin, baogồm:

a. Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị như: máy tính trạm bị nhiễm phần mềm độc hại, phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi;

b. Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 (một) phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban;

c. Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như: hệ thống quản lý văn bản và điều hành, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng;

d. Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống Cổng/Trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin:

Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a. Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Khoa học và Công nghệ quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu thành phố) thì thực hiện tiếp Bước 3;

b. Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước3;

c. Bước 3: Báo sự cố đến Công an thành phố, Sở Khoa học và Công nghệ theo mẫu tại Phụ lục 1 kèm Quy chế và thực hiện tiếp Bước 4;

d. Bước 4: Phối hợp với Công an thành phố, Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Khoa học và Công nghệ và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ. Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu tại Phụ lục 2 kèm Quy chế, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Công an thành phố.

Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Công an thành phố để được hướng dẫn, hỗ trợ.

3. Bộ phận phụ trách về an toàn thông tin có trách nhiệm

a. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP 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 số 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;

b. 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.

c. Phối hợp với các đơn vị chức năng xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số05/2017/QĐ-TTg;

d. Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám

sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống.

e. 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 số05/2017/QĐ-TTg;

f. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an 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;

g. 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;

h. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an 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.

4. Trách nhiệm của người dùng

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

**Điều 18. Quản lý an toàn thông tin của các cơ quan, đơn vị đối với người sử dụng**

Đối với các phòng quản lý nhà nước, các đơn vị sự nghiệp trực thuộc UBND xã:

1. Khi tiếp nhận nhân sự mới phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị;

2. Phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng của từng cá nhân trong cơ quan, đơn vị;

3. Đối với cán bộ chấm dứt hoặc thay đổi công việc thực hiện theo điểm a, khoản 3, Điều 6 tại Quy định này.

**Điều 19. Quản lý truy cập**

1. Đối với phòng quản lý nhà nước, các đơn vị sự nghiệp trực thuộc, người sử dụng có trách nhiệm

a. Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài

khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị;

b. Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng;

c. Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả hệ thống máy chủ, máy trạm của người sử dụng;

d. Hệ thống mạng không dây (wifi) của các cơ quan, đơn vị phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây;

đ. Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %) và phải được thay đổi ít nhất 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng;

e. Các đơn vị cần rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.

2. Đối với các hệ thống thông tin

a. Bảo đảm mỗi tài khoản của tổ chức, cá nhân truy cập vào hệ thống thông tin là duy nhất;

b. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản;

c. Đơn vị quản lý, vận hành các hệ thống dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người dùng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

**Điều 20. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin**

1. Đối với phòng quản lý nhà nước, các đơn vị sự nghiệp trực thuộc phải thực hiện việc ghi nhật ký 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 và lưu giữ. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết;

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

3. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và

các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

**Điều 21. Quản lý rủi ro an toàn thông tin**

1. Xác định tài sản:

a) Lập danh mục thiết bị, máy chủ, phần mềm, dịch vụ, ứng dụng thuộc hệ thống;

b) Kịp thời cập nhật danh mục, nội dung hồ sơ đề xuất cấp độ an toàn thông tin của hệ thống khi có thay đổi.

2. Đánh giá rủi ro:

a) Xác định rủi ro: Định kỳ hàng tháng, Công an xã chủ trì, phối hợp với Văn phòng HĐND và UBND xã, Phòng Văn hoá – Xã hội tiến hành rà soát, xác định các mối đe dọa, điểm yếu, lỗ hổng bảo mật có thể ảnh hưởng, gây mất an toàn thông tin (ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn sàng) đối với các thành phần của hệ thống theo danh mục tài sản đã được xác định hoặc các yêu cầu về chính sách về quản lý, kỹ thuật được khuyến nghị thực hiện để bảo đảm an toàn thông tin nhưng chưa thể thực hiện được;

b) Phân tích tác động của rủi ro: Làm rõ mức độ tác động, ảnh hưởng của từng rủi ro được xác định và đề xuất phương án xử lý;

c) Phân loại rủi ro theo mức độ ảnh hưởng:

- Mức thấp: Rủi ro mất an toàn thông tin có thể xử lý thông qua cập nhật miễn phí bản vá của hệ điều hành, phần mềm, ứng dụng, dịch vụ;

- Mức cao: Rủi ro mất an toàn thông tin không thể xử lý thông qua cập nhật hoặc phải trả phí để được cập nhật bản vá của hệ điều hành, phần mềm, ứng dụng, dịch vụ.

3. Xử lý rủi ro:

a) Công an xã chủ trì, phối hợp với Văn phòng HĐND và UBND, Phòng Văn hoá – Xã hội chủ động, kịp thời xử lý các rủi ro ở mức độ thấp;

b) Báo cáo Lãnh đạo đơn vị, Công an thành phố quyết định phương án xử lý đối với các rủi ro ở mức cao.

4. Chấp nhận rủi ro: Việc xử lý sớm toàn bộ các rủi ro là khó khả thi. Đối với các rủi ro ở mức thấp hoặc rủi ro ở mức cao được phát hiện nhưng được đánh giá không làm tổn hại đến hoạt động bình thường của hệ thống hoặc đã có các biện pháp khác hạn chế rủi ro thì có thể chấp nhận sự tồn tại của rủi ro trên hệ thống. Tuy nhiên, cần từng bước có biện pháp xử lý triệt để các rủi ro.

5. Trường hợp sự cố mất an toàn thông tin xảy ra:

a) Công an xã chủ trì, phối hợp với Văn phòng HĐND và UBND xã, Phòng Văn hoá – Xã hội chủ động thực hiện các biện pháp nghiệp vụ cần thiết để kịp thời xử lý.

b) Trong trường hợp sự cố mất an toàn thông tin vượt quá khả năng xử

lý, Công an xã chủ trì, phối hợp với Văn phòng HĐND và UBND xã, Phòng Văn hoá -Xã hội kịp thời báo cáo Lãnh đạo đơn vị, Công an thành phố để xử lý.

**Điều 22. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

1. Trường hợp hệ thống phải kết thúc vận hành, khai thác, thanh lý, hủy bỏ, Công an xã chủ trì, phối hợp với Văn phòng HĐND và UBND xã, Phòng Văn hoá – Xã hội tham mưu Lãnh đạo đơn vị báo cáo Công an thành phố, UBND thành phố phương án thực hiện, trong đó làm rõ:

a) Lý do kết thúc vận hành, khai thác, thanh lý, hủy bỏ và phương án thay thế (nếu có);

b) Phương án xử lý xóa bỏ các thông tin, dữ liệu: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối, phương tiện lưu trữ chứa thông tin, dữ liệu cần xóa. Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung cần đề xuất xử lý, các thư mục chứa dữ liệu sao lưu cần xóa dữ liệu…, phương thức xóa bỏ thông tin, dữ liệu, bảo đảm thông tin, dữ liệu được xóa hoàn toàn, không thể khôi phục trên các máy chủ, thiết bị, phương tiện lưu trữ;

c) Phương án gỡ bỏ các phần mềm, ứng dụng hoặc dịch vụ có liên quan: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối có cài đặt phần mềm, ứng dụng hoặc dịch vụ có liên quan đến hệ thống cần thực hiện gỡ bỏ. Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung đề xuất xử lý, phương thức xử lý bảo đảm phần mềm, ứng dụng, dịch vụ được xóa hoàn toàn, không thể phục hồi trên các máy chủ, thiết bị mạng, thiết bị đầu cuối có liên quan;

d) Danh mục các máy chủ, thiết bị mạng, thiết bị đầu cuối, thiết bị lưu trữ cần thanh lý (nếu có), làm rõ phương án thanh lý. Các máy chủ, thiết bị mang, thiết bị đầu cuối, thiết bị lưu trữ cần được xử lý xóa bỏ thông tin, dữ liệu, gỡ bỏ phần mềm, ứng dụng, dịch vụ trước khi tiến hành thanh lý;

2. Trình tự, thủ tục thực hiện: Sau khi được sự đồng ý bằng văn bản của UBND thành phố, Công an thành phố. Công an xã chủ trì, phối hợp với Văn phòng HĐND và UBND xã, Phòng Văn hoá - Xã hội tham mưu Lãnh đạo đơn vị thực hiện thanh lý, hủy bỏ hệ thống theo đúng các quy định tại Điều 29, Điều 30 Nghị định số 151/2017/NĐ-CP ngày 26/12/2017 của Chính phủ quy định chi tiết một số điều của Luật quản lý, sử dụng tài sản công1.

**Điều 23. Bảo đảm an toàn trong xây dựng hệ thống thông tin**

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng 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 thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của 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 01/7/2016 của Chính phủ về bảo đảm an

[1] Trường hợp hệ thống thông tin không phải là tài sản công thì tham chiếu đến các quy định có liên quan về thanh lý, hủy bỏ tài sản của doanh nghiệp hoặc ghi rõ trình tự, thủ tục thực hiện nếu chưa có văn bản quy định chính thức.

toàn hệ thống thông tin theo cấp độ;

2. Nhiệm vụ quản lý về hướng dẫn xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng; tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017;

3. Các phòng ban, đơn vị trực thuộc UBND xã chủ quản hệ thống thông tin phải tổ chức kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý;

4. Công an thành phố tổ chức kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin do UBND thành phố phê duyệt hồ sơ đề xuất cấp độ; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin.

5. Đối với các hệ thống thông tin đã được phê duyệt cấp độ: tiến hành rà soát Hồ sơ đề xuất cấp độ và Phương án đảm bảo an toàn thông tin đã được phê duyệt, trong trường hợp cần điều chỉnh, phê duyệt lại hồ sơ đề xuất cấp độ và Phương án đảm bảo an toàn thông tin, thì gửi về Công an thành phố để tổng hợp, thẩm định và thực hiện các thủ tục phê duyệt theo quy định. Triển khai đầy đủ các phương án đảm bảo an toàn thông tin đã được phê duyệt.

**Điều 24. Sao lưu dữ liệu dự phòng**

1. Đối với các phòng quản lý nhà nước, các đơn vị sự nghiệp trực thuộc và người sử dụng:

a. Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng. Khi lưu trữ, trao đổi thông tin, dữ liệu quan trọng phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng;

b. Phải lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ ít nhất một lần trong tháng các dữ liệu quan trọng, bao gồm: cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh, các tập tin dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (như: đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

2. Đối với đơn vị chủ quản các hệ thống thông tin

a. Có trách nhiệm ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu;

b. Xây dựng 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;

c. Phải lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và được kiểm tra thường xuyên, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

## Chương III

## BÁO CÁO, CHIA SẺ THÔNG TIN

### Điều 25. Chế độ báo cáo

1. Báo cáo định kỳ

Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 03/2017/TT-BTTTT, cụ thể như sau:

- Tình hình an toàn thông tin của hệ thống thông tin trong kỳ báo cáo;

- Tiến độ triển khai, áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

- Hiệu quả áp dụng phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

- Đề xuất thay đổi cấp độ, phương án bảo đảm an toàn hệ thống thông tin (nếu có);

- Nội dung khác phục vụ công tác bảo đảm an toàn hệ thống thông tin theo cấpđộ.

2. Báo cáo độtxuất

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, phê duyệt báocáo

- Công an xã lập báo cáo an toàn thông tin theo quy định tại khoản 1 điều này, gửi Công an thành phố theo quy định;

- Báo cáo đột xuất theo hướng dẫn của Công an thành phố và UBND thành phố.

## Chương IV

## TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

### Điều 26. Trách nhiệm của Công an xã

- Tham mưu giúp Lãnh đạo UBND xã về công tác bảo đảm an toàn thông tin mạng UBND xã và chịu trách nhiệm trước Lãnh đạo UBND xã trong việc bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của UBND xã;

- Thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và bảo đảm

an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của UBND xã theo quy định;

- Tổng hợp các Đề án, Dự án về bảo đảm an toàn thông tin mạng của các phòng, đơn vị; Chủ trì, phối hợp các đơn vị liên quan tham mưu Lãnh đạo UBND xã xây dựng dự trù kinh phí thực hiện các Đề án, Dự án về bảo đảm an toàn thông tin mạng;

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan thanh tra, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trong phạm vi của UBND xã;

- Cử cán bộ tham gia các khóa đào tạo, hội nghị tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước do Công an thành phố tổ chức;

- Tham mưu lãnh đạo xã thực hiện phổ biến, tuyên truyền, quán triệt các văn bản, quy định về ATTT nhằm nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức, người lao động bằng các hình thức: gửi tài liệu tuyên truyền qua Hệ thống quản lý văn bản và điều hành, đăng tải thông tin, tài liệu trên Cổng TTĐT của xã, ban hành văn bản, quán triệt tại các cuộc họp giao ban của Lãnh đạo xã, cuộc họp của các phòng, đơn vị...

- Hướng dẫn về nghiệp vụ quản lý vận hành, kỹ thuật bảo đảm an toàn thông tin mạng; hỗ trợ giải quyết sự cố khi có yêu cầu;

- Hướng dẫn, giám sát các các đơn vị xây dựng quy định nội bộ và thực hiện việc bảo đảm an toàn thông tin mạng cho hệ thống thông tin theo quy định của Nhà nước;

- Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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;

- Hàng năm, căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an toàn thông tin mạng của các đơn vị đề xuất Lãnh đạo UBND xã xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành;

- Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho gửi Công an thành phố và các cơ quan, đơn vị có liên quan;

**Điều 27. Trách nhiệm Phòng Văn hoá – Xã hội**

- Phối hợp với Công an xã có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các Cổng/trang thông tin điện tử, mạng xã hội.

- Phối hợp Công an xã thực hiện việc tuyên truyền, hướng dẫn các cơ quan, đơn vị, ban, ngành, đoàn thể thuộc xã thực hiện nghiêm túc theo quy định của Luật an toàn an ninh mạng, an toàn thông tin.

- Phối hợp với Công an xã thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Phối hợp với Công an xã tiến hành thanh tra, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trong phạm vi của UBND xã;

- Phối hợp Công an xã hướng dẫn, giám sát các các đơn vị xây dựng quy định nội bộ và thực hiện việc bảo đảm an toàn thông tin mạng cho hệ thống thông tin theo quy định của Nhà nước;

- Phối hợp Công an xã, hàng năm căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an toàn thông tin mạng của các đơn vị đề xuất Lãnh đạo UBND xã xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành;

- Cử cán bộ tham gia các khóa đào tạo, hội nghị tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước do UBND thành phố tổ chức.

**Điều 27. Trách nhiệm của Văn phòng HĐND và UBND xã**

Tham mưu UBND xã vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

Chỉ đạo, phân công cán bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) phối hợp với Công an xã triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Phối hợp với Công an xã và Phòng Văn hóa - Xã hội thực hiện biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các Cổng/trang thông tin điện tử, mạng xã hội.

Cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng theo yêu cầu.

**Điều 28. Trách nhiệm của các cơ quan, đơn vị thuộc UBND xã.**

Thủ trưởng các cơ quan, đơn vị thuộc UBND xã có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình; quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

Phân công cán bộ thực hiện việc bảo đảm an toàn thông tin của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị.

Thực hiện bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

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

Phối hợp chặt chẽ với Công an xã, Phòng Văn hóa - Xã hội và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch mua phần mềm chống virus có bản quyền phần mềm... nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi để triển khai thực hiện.

Phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

7. Thực hiện các báo cáo về an toàn thông tin mạng khi UBND xã, Công an thành phố, UBND thành phố yêu cầu.

**Điều 29. Trách nhiệm của cán bộ công chức, viên chức và người lao động trong các cơ quan đơn vị**

Trách nhiệm của cán bộ phụ trách về an toàn thông tin/công nghệ thôngtin tại cơ quan, đơn vị

Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị;

Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, pháthiện và khắc phục các sự cố an toàn thông tin mạng;

đ)Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

Trách nhiệm của người sử dụng

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;

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

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;

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

**Điều 30. Tổ chức thực hiện**

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.

Công an xã chủ trì, phối hợp Văn phòng HĐND&UBND, 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 hằng năm hoặc đột xuất theo yêu cầu của UBND xã và cơ quan có thẩm quyền của thành phố.

Định kỳ 02 năm hoặc khi có thay đổi về chính sách ATTT, Công an xã kiểm tra tính phù hợp của Quy chế này và thực hiện rà soát, cập nhật bổ sung đảm bảo đúng với quy định của pháp luật.

Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Công an xã để tổng hợp báo cáo Ủy ban nhân dân xã xem xét điều chỉnh, bổ sung./.

**MẪUSỐ 01**

# BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

## THÔNG TIN VỀ TỔ CHỨC/ CÁ NHÂN BÁO CÁO SỰCỐ

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ:(*) .....
- Điện thoại(*).....Email (*).....

**NGƯỜI LIÊN HỆ**

- Họ và tên (*).....Chứcvụ:.....
- Điện thoại (*).....Email (*).....

## THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰCỐ

| | |
|---|---|
| Tên đơn vị vận hành hệ thống thông tin (*): | *Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin* |
| Cơ quan chủ quản: | *Điền tên cơ quan chủ quản* |
| Tên hệ thống bị sự cố | *Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan* |
| Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có) | *Điền tên nhà cung cấp ở đây* |
| Dải địa chỉ Public IP kết nối với hệthống bên ngoài: | *Điền thông tin ở đây* |
| Mô tả sơ bộ về sự cố (*): | |
| *Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:*..... ..... ..... ..... | |

| | | |
|---|---|---|
| Ngàyphátthiệnsựcố (*) (dd/mm/yy) | Thời gian phát hiện (*): | …..giờ….phút |

## HIỆN TRẠNG SỰ CỐ (*)

☐Đã được xử lý. ☐Chưa được xử lý.

**CÁCH THỨC PHÁT HIỆN** * (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

 Qua hệ thống phát hiện xâm nhập. Kiểm tra dữ liệu lưu lại (LogFile)

 Nhận được thông báo từ: .....

 Khác, đó là .....

**ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO ***

 Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

 ISP đang trực tiếp cung cấp dịch vụ

 Cơ quan điều phối

**THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ**

- Hệ điều hành.....Version.....
- Các dịch vụ có trên hệ thống(*Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

 Webserver Mailserver Databaseserver

 Dịch vụ khác, đól à.....

- Các biện pháp an toàn thông tin đã triển khai(*Đánh dấu những biện pháp đã triển khai)*

 Antivirus  Firewall  Hệ thống phát hiện xâm nhập

 Khác:.....

- Cá cđịa chỉ IP của hệt hống

*(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IPnội bộ)*

.....

- Các tên miền của hệ thống.....
- Mục đích chính sử dụng hệ thống.....
- Thôngtingửi kèm

 Nhậtkýhệthống Mẫuvirus/mãđộc

 Khác:…….

- Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:

 Có Không

**KIẾN NGHỊ ĐỀ XUẤT HỖ TRỢ**

| Mô tả về đề xuất, kiến nghị |
|---|
| Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có)<br>.....<br>.....<br>.....<br>..... |

**THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ**

(ngày/tháng/năm/giờ/phút):

**CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT**

**MẪUSỐ 02**

# BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

## THÔNG TIN VỀ TỔ CHỨC/ CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ: (*) .....
- Điện thoại (*).....Email(*).....

## KÝ HIỆU BÁO CÁO BAN ĐẦU SỰCỐ

Số ký hiệu..... Ngày báo cáo: / /202…

## THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

| | | |
|---|---|---|
| Tên đơn vị vận hành hệ thống thông tin(*): | *Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin* | |
| Cơ quan chủ quản: | *Điền tên cơ quan chủ quản* | |
| Tên hệ thống bị sự cố | *Điền tên hệ thống bị sự cố* | |
| Tên/Mô tả sơ bộ về sự cố (*) | | |
| Ngày phát hiện sự cố (*) (dd/mm/yy) | Thời gian phát thiện (*): | …..giờ….phút |
| **Kết quả xử lý sự cố** | | |
| *Cung cấp ,tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu sựcố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...* | | |
| Các tài liệu đính kèm | | |
| *Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố;phương án xử lý,log file…)* | | |

**CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT**

*(Ký tên, đóng dấu)*