ỦY BAN NHÂN DÂN **XÃ HẢI HƯNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 804 /QĐ-UBND	*Hải Hưng, ngày 24 tháng 10 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành, khai thác hệ thống thông tin của Ủy ban nhân dân xã Hải Hưng

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ HẢI HƯNG

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 06 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 47/2020/NĐ-CP ngày 09 tháng 4 năm 2020 của Chính phủ quy định về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;

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 Nghị quyết số 203/2025/QH15 ngày 27 tháng 6 năm 2025 của Quốc hội về tổ chức chính quyền địa phương tại thành phố Hải Phòng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 749/QĐ-TTg ngày 03 tháng 6 năm 2020 của Thủ tướng Chính phủ về việc phê duyệt "Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030"

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông hướng dẫn xác định cấp độ an toàn hệ thống thông tin;

Theo đề nghị của Trưởng phòng Văn hóa – xã hội xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế quản lý, vận hành, khai thác hệ thống thông tin của Ủy ban nhân dân xã Hải Hưng".

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

Điều 3. Chánh Văn phòng HĐND&UBND xã, Trưởng phòng Văn hoá - Xã hội, Giám đốc Trung tâm phục vụ Hành chính công, các ban, ngành và Thủ trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Công an thành phố Hải Phòng;
- Thường trực Đảng uỷ;
- Thường trực HĐND xã;
- Chủ tịch, các Phó Chủ tịch UBND xã;
- Các phòng, ban, ngành, đoàn thể xã;
- Trang Thông tin điện tử xã;
- Lưu: VT

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ HẢI HƯNG T.P HẢI PHÒNG

Phạm Văn Hạnh

ỦY BAN NHÂN DÂN **XÃ HẢI HƯNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ
Quản lý, vận hành, khai thác hệ thống thông tin của Ủy ban nhân dân xã Hải Hưng

(Ban hành kèm theo Quyết định số: /QĐ-UBND ngày /10/2025 của Ủy ban nhân dân xã Hải Hưng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc quản lý, vận hành, khai thác hệ thống thông tin của Ủy ban nhân dân xã Hải Hưng.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với phòng, ban, ngành, đoàn thể thuộc Ủy ban nhân dân xã Hải Hưng (sau đây gọi tắt là đơn vị); cán bộ, công chức, viên chức và người lao động (sau đây viết tắt là CCVC) đang công tác tại các phòng, ban, ngành, đoàn thể tại xã.

Chương II
QUY TRÌNH QUẢN LÝ, VẬN HÀNH, KHAI THÁC HỆ THỐNG THÔNG TIN

Điều 3. Quy định về quản lý mật khẩu

1. Lãnh đạo Văn phòng Hội đồng nhân dân và Ủy ban nhân dân (VP) có trách nhiệm tiếp nhận mật khẩu quản trị các hệ thống sau khi hệ thống được bàn giao và đưa vào sử dụng; sau đó tiến hành bàn giao cho cán bộ, công chức, viên chức, người lao động quản lý hệ thống.

2. CCVC quản lý hệ thống phải thực hiện đổi mật khẩu trong vòng 01 ngày từ khi tiếp nhận. Việc đổi mật khẩu quản trị hệ thống phải tuân thủ theo đúng quy định hướng dẫn về mật khẩu do cơ quan quản lý ban hành.

3. Mật khẩu phải bảo đảm an toàn về độ dài, ký tự và thời gian sử dụng.

a) Độ dài của mật khẩu

- Đối với mật khẩu của CCVC và người sử dụng (dùng để đăng nhập thư điện tử, ứng dụng nghiệp vụ, máy tính cá nhân,...): tối thiểu là 8 ký tự.

- Đối với mật khẩu quản trị hệ thống (sử dụng cho quản trị các hệ thống mạng, bảo mật, máy chủ, thư điện tử, ứng dụng,...): tối thiểu là 11 ký tự.

b) Nội dung mật khẩu

- Không bao gồm các từ dễ nhớ như tên, ngày sinh, số điện thoại.

- Không được đặt theo ký tự chữ cái, ký tự chữ số tuần tự hoặc một dãy các ký tự giống nhau, ví dụ: ABCDEFGH, 98765432 hoặc !!!!!!!!,…

- Đối với mật khẩu quản trị hệ thống phải kết hợp các loại ký tự sau: chữ cái in thường (a, b,…), chữ cái in hoa (A, B,…), ký tự số (1, 2,…) và các ký tự đặc biệt (@, !, #...).

c) Thời gian sử dụng mật khẩu

- Đối với mật khẩu quản trị hệ thống phải được thay đổi định kỳ, ít nhất 03 tháng một lần.

- Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn an ninh thông tin thì phải thay đổi toàn bộ mật khẩu quản trị.

d) Quy định sử dụng và lưu trữ mật khẩu

- Người sử dụng phải thay đổi mật khẩu ngay từ lần đăng nhập đầu tiên.

- Không được lưu trữ mật khẩu trên máy tính cá nhân, các thiết bị điện tử.

- Mật khẩu tài khoản người dùng phải giữ bí mật, không chia sẻ mật khẩu với người khác.

- Khi kết thúc công việc phải thực hiện đăng xuất.

- Khi bị lộ mật khẩu hoặc nghi ngờ bị lộ mật khẩu phải đổi mật khẩu và báo cáo ngay với cán bộ quản trị để thực hiện khóa tài khoản, nhằm ngăn chặn các hành động phá hoại, lấy cắp thông tin.

- Nếu quên mật khẩu, người sử dụng thực hiện theo quy trình cấp mật khẩu mới.

- Các tài liệu liên quan đến mật khẩu được xem là tài liệu tối mật, không được soạn thảo trên máy tính có nối mạng Internet.

Điều 4. Quy định về kiểm soát truy nhập và xác thực

1. Việc quản lý, xác thực CCVC, người sử dụng truy nhập trên hệ thống phải có đầy đủ thông tin, bao gồm họ tên, chức vụ, phòng, ban, ngành, đoàn thể công tác, số điện thoại trên hệ thống xác thực người dùng (phải xây dựng quy trình đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng).

2. Mỗi người dùng chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

3. Tạm dừng quyền sử dụng đối với tài khoản đã được đăng ký trên hệ thống nhưng không làm việc trong hệ thống từ 30 ngày trở lên.

4. Giới hạn số lần đăng nhập không thành công vào hệ thống là 5 lần. Sau 5 lần không đăng nhập thành công, tài khoản sẽ bị khóa trong 30 phút.

5. CCVC quản lý hệ thống 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 viên chức quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

6. Thường xuyên kiểm tra, cập nhật tài khoản của người dùng hệ thống đã chuyển công tác, nghỉ hưu, hết hạn sử dụng hoặc không còn làm việc trên hệ thống.

Điều 5. 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 phải được thiết lập cấu hình đảm bảo an toàn 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 trường mạng.

3. 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.

4. 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.

5. Giới hạn và kiểm soát chặt chẽ những tiện ích hệ thống có khả năng ảnh hưởng đến hệ thống và chương trình ứng dụng khác.

6. Giới hạn thời gian kết nối với những ứng dụng có độ rủi ro cao.

7. Ngắt phiên làm việc sau một thời gian không sử dụng, nhằm ngăn chặn truy cập trái phép.

8. Thực hiện cài đặt và quản lý các bản vá lỗi, kích hoạt chức năng bảo mật (tường lửa), cài đặt các chương trình diệt virus.

9. Thực hiện theo dõi, giám sát nhật ký hệ thống.

Điều 6. 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. Triển khai các biện pháp kỹ thuật nhằm kiểm soát truy cập hệ thống, bao gồm:

a) Kiểm soát truy cập giữa các phân vùng mạng, bảo đảm chỉ cho phép kết nối, sử dụng các dịch vụ, ứng dụng theo đúng chức năng hoặc quyền truy

cập của cá nhân; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài.

b) Phòng chống xâm nhập để bảo vệ vùng DMZ; định kỳ hàng tháng thực hiện cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng trên các thiết bị tường lửa.

c) Giám sát kết nối mạng của thiết bị đầu cuối, máy tính người sử dụng bảo đảm phát hiện và ngăn chặn các hành vi truy cập, xâm nhập trái phép từ mạng nội bộ.

d) Quản lý truy nhập, xác thực, cấp quyền, lưu nhật ký truy nhập đối với các phiên truy nhập vào thiết bị mạng. Sử dụng các giao thức quản trị có mã hóa.

3. Triển khai các biện pháp kỹ thuật bảo vệ thiết bị hệ thống, bao gồm:

a) Cấu hình chức năng xác thực trên tất cả các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.

b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa.

4. Quy định với máy chủ

a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục.

b) 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 sau sự cố cho hệ thống máy chủ.

c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao.

d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.

e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.

g) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

5. Quy định với ứng dụng

a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật.

b) Ứng dụng phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

Điều 7. Quản lý an toàn dữ liệu

1. Sao lưu dữ liệu

a) Thực hiện lưu trữ đầy đủ các dữ liệu của người dùng, ứng dụng vào hệ thống. Tùy theo từng loại dữ liệu, thực hiện lưu trữ đúng và đủ thời hạn theo các quy định tại quy trình sao lưu và phục hồi dữ liệu.

b) Dữ liệu phải được phân loại để lưu trữ theo thứ tự ưu tiên về mức độ quan trọng, sao lưu theo thời gian, loại thông tin, nơi lưu trữ. Đối với các dữ liệu quan trọng phải được lưu trữ tối thiểu tại hai địa điểm cách biệt nhau, thực hiện sao lưu dữ liệu tối thiểu một tuần một lần.

c) Bản dữ liệu sao lưu phải được lưu trữ tối thiểu trong 07 ngày làm việc tại máy chủ độc lập với máy chủ cơ sở dữ liệu của hệ thống, bảo đảm sẵn sàng sử dụng để khôi phục dữ liệu của hệ thống khi gặp sự cố.

d) Dữ liệu phải được kiểm soát và đối chiếu sau khi sao lưu.

2. Bảo mật dữ liệu

- Có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

- Thực hiện phân quyền và có quy định chặt chẽ đối với các cá nhân truy cập đến cơ sở dữ liệu, ghi nhật ký đối với các truy cập, thao tác cấu hình cơ sở dữ liệu.

- Rà soát, cập nhật các bản vá, các bản sửa lỗi hệ quản trị cơ sở dữ liệu tối thiểu 03 tháng một lần hoặc ngay sau khi có khuyến cáo của nhà cung cấp.

- Kiểm soát, phân quyền truy nhập vật lý và truy nhập xa tới bản sao dữ liệu.

- Hủy bỏ các thiết bị lưu trữ bản sao dữ liệu không còn khả năng sử dụng.

Điều 8. Quản lý an toàn thiết bị đầu cuối

1. Kiểm tra thiết bị

a) Đơn vị được giao vận hành cần phải lập danh sách chính xác các thiết bị phần cứng và các hệ thống phần mềm (bao gồm cả cơ sở hạ tầng) hiện đang được giao quản lý.

b) Quản trị viên thường xuyên theo dõi và kiểm tra các ứng dụng và thiết bị đầu cuối để đánh giá tình trạng hoạt động.

2. Theo dõi quá trình và kết thúc

a) Triển khai bản vá tự động.

b) Thông tin chính xác và hành động trên hệ thống thời gian thực.

Điều 9. Quản lý phòng chống phần mềm độc hại

1. Duy trì, cập nhật thường xuyên đối với hệ thống bảo mật (Tường lửa, phòng chống mã độc, phát hiện và ngăn chặn xâm nhập,…) để bảo đảm an toàn, bảo mật cho dữ liệu.

2. Tất cả các máy chủ, máy trạm phải được cài đặt phần mềm diệt mã độc được cơ quan quản lý phê duyệt.

3. Chương trình diệt mã độc phải luôn được cập nhật kịp thời các bản vá, các mẫu mã độc mới và phải được đặt ở chế độ quét thường xuyên, quét khi có kết nối với các thiết bị ngoại vi (usb, ổ cứng cắm ngoài,…).

4. Những máy tính được phát hiện có mã độc phải được cách ly ngay khỏi hệ thống để tránh lây nhiễm sang các máy tính khác.

Điều 10. Quản lý giám sát an toàn hệ thống thông tin

Các hệ thống thông tin được thiết lập các công cụ theo dõi, giám sát, ghi nhật ký hệ thống nhằm đánh giá tình trạng hoạt động của hệ thống làm cơ sở cho việc ra các yêu cầu điều hành thích hợp.

1. Văn phòng Hội đồng nhân dân và Ủy ban nhân dân phối hợp với các đơn vị liên quan thực hiện giám sát mạng và các hệ thống thông tin.

2. Kết quả của việc theo dõi, giám sát, ghi nhật ký hệ thống phải được tổng hợp, báo cáo cùng với các báo cáo quý, nằm nhằm đánh giá và làm sở cứ cho việc phát triển và quy hoạch mạng lưới.

Điều 11. Quản lý điểm yếu an toàn thông tin

1. Phân loại mức nguy hiểm: Điểm yếu an toàn thông tin (ATTT) được phân loại làm 4 mức nguy hiểm (từ mức 1 đến mức 4). Đơn vị vận hành cần rà soát và xác định đúng mức độ điểm yếu để áp dụng biện pháp xử lý cho phù hợp.

2. Áp dụng các biện pháp để kiểm tra và xử lý các điểm yếu ATTT theo các bước:

- Bước 1: Xác định phiên bản hệ điều hành và các ứng dụng có khả năng bị ảnh hưởng.

- Bước 2: Xác định các điểm yếu cụ thể tương ứng với phiên bản hệ điều hành và các ứng dụng đã được xác định ở bước 1, được liệt kê ở trên.

- Bước 3: Kiểm tra thông tin mã của các bản vá đã được cài đặt trong hệ điều hành xem trong tài liệu hướng dẫn "Hướng dẫn cấu hình tự động cập nhật Windows" phần Hướng dẫn kiểm tra thông tin các bản vá đã được cập nhật, tệp tin "WindowUpdateGuide.pdf".

3. Xem xét để có biện pháp nâng cấp hoặc cài đặt các bản vá (cho Hệ điều hành, CSDL và các ứng dụng) để xử lý điểm yếu an toàn thông tin.

4. Rà soát: kiểm tra lại thông tin các điểm yếu sau khi đã xử lý.

Điều 12. Quản lý sự cố an toàn thông tin

1. Khi phát hiện có sự cố, đơn vị vận hành thực hiện các biện pháp cô lập và xác định nguyên nhân xảy ra sự cố theo nguyên tắc hạn chế tối đa ảnh hưởng

tới hoạt động của hệ thống; đồng thời phải thông báo cho bộ phận sử dụng và các cơ quan, đơn vị có liên quan về tình hình sự cố.

2. Tùy thuộc vào mức độ ảnh hưởng của sự cố, đánh giá và phân loại theo 03 mức: sự cố thông thường, sự cố nghiêm trọng và sự cố đặc biệt nghiêm trọng.

3. Đối với các sự cố thông thường: Đơn vị vận hành nhanh chóng xử lý sự cố. Trường hợp không xử lý được, thông báo cơ quan quản lý để phối hợp giải quyết.

4. Đối với các sự cố nghiêm trọng (các sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố liên quan đến an ninh thông tin, mất mát dữ liệu): Ngay sau khi phát hiện sự cố đơn vị vận hành cần đánh giá ảnh hưởng của sự cố và thực hiện báo cáo về cơ quan quản lý để được hướng dẫn xử lý.

5. Đối với các sự cố đặc biệt nghiêm trọng: Đơn vị vận hành và cơ quan quản lý phải có đánh giá ảnh hưởng của sự cố và thực hiện báo cáo ngay về cơ quan chủ sở hữu để có chỉ đạo xử lý.

6. Yêu cầu đối với việc xử lý sự cố cần tuân thủ các nguyên tắc:

a) Phải tuân thủ quy trình xử lý sự cố do cơ quan quản lý phê duyệt và ban hành.

b) Đảm bảo tuyệt đối an toàn cho người và thiết bị của hệ thống.

c) Các dữ liệu quan trọng phải được sao lưu trước khi xử lý sự cố.

d) Ghi nhật ký sự cố kỹ thuật phát sinh tại chỗ.

e) Trường hợp sự cố vượt quá khả năng tự xử lý, thông báo cho trung tâm VNCERT phối hợp ngăn chặn, khắc phục sự cố.

f) Thông báo cho các bên liên quan về thời gian khắc phục xong sự cố.

g) Lập báo cáo sự cố gửi cơ quan quản lý đối với các sự cố nghiêm trọng và đặc biệt nghiêm trọng trong vòng 24 giờ kể từ khi phát hiện sự cố.

Điều 13. 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. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

2. 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.

3. 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.

4. Cán bộ 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 CCVC đã nghỉ việc.

5. Cán bộ phụ 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.

Điều 14. Quản lý rủi ro an toàn thông tin

1. Xác định tài sản: Dựa vào loại hình hệ thống thông tin là loại thông tin mà hệ thống đó xử lý.

2. Xác định điểm yếu và mối đe dọa: Việc xác định điểm yếu và mối đe dọa ở bước này là cơ sở để xác định khả năng xảy ra cũng như các biện pháp kiểm soát ở các bước tiếp theo.

3. Xác định mức ảnh hưởng.

4. Xác định khả năng xảy ra.

5. Xác định mức rủi ro: việc xác định khả năng xảy ra sự cố cần dựa vào giá trị tài sản, mức ảnh hưởng, khả năng xảy ra.

6. Xác định biện pháp xử lý rủi ro và kiểm soát: Trước hết cần lựa chọn biện pháp xử lý rủi ro. Các biện pháp kiểm soát chỉ được đưa ra khi lựa chọn biện pháp xử lý rủi ro là thay đổi rủi ro. Trường hợp việc lựa chọn các biện pháp kiểm soát cần nguồn lực bỏ ra lớn hơn lợi ích mang lại thì biện pháp xử lý rủi ro nên được lựa chọn là chấp nhận rủi ro.

Điều 15. Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, viên chức quản lý và vận hành hệ thống

1. Cá nhân sử dụng máy tính tham gia hệ thống để xử lý công việc phải tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) trên máy tính được cơ quan cấp để phục vụ công việc; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm phòng chống mã độc có chức năng quản lý tập trung và thiết lập chế độ tự động cập nhật cho phần mềm; thực hiện kiểm tra, rà quét bằng phần mềm phòng chống mã độc khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy tính phải tắt máy và báo trực tiếp cho bộ phận phụ trách về an toàn thông tin mạng hoặc đơn vị chuyên trách về an toàn thông tin để được xử lý kịp thời.

d) Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình. Không truy cập, mở các trang thông tin, thư điện tử không rõ nguồn gốc.

đ) Cá nhân có trách nhiệm quản lý, bảo vệ tài khoản và mật khẩu đã được cấp để đăng nhập, sử dụng hệ thống, không chia sẻ mật khẩu với người khác. Đặt mật khẩu với độ an toàn cao và thay đổi mật khẩu định kỳ theo quy định; tài

khoản đăng nhập hệ thống phải được đăng xuất khi không sử dụng. Thực hiện các biện pháp mã hóa đối với các tài khoản, mật khẩu được lưu trữ trên thiết bị.

e) Khóa máy tính khi tạm thời rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

h) Báo cáo và phải được thủ trưởng cơ quan đồng ý, cho phép trước khi mang máy tính, thiết bị công nghệ thông tin có kết nối mạng của cá nhân đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định được nêu ở trên.

2. Đối với cán bộ quản lý, vận hành hệ thống:

a) Tuân thủ các quy định như đối với các cá nhân tham gia sử dụng hệ thống được quy định tại Khoản 1 ở trên.

b) Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị; phân quyền sử dụng tài khoản quản trị theo chức năng nhiệm vụ của cá nhân trong công tác vận hành hệ thống.

c) Chỉ sử dụng các máy tính quản trị, trong mạng nội bộ để truy cập, thực hiện quản trị, cấu hình, cập nhật hoặc gỡ lỗi hệ thống. Trường hợp cần truy cập, thực hiện quản trị, cấu hình, cập nhật hoặc gỡ lỗi hệ thống từ xa thì chỉ sử dụng tài khoản VPN của hệ thống để thực hiện và có biện pháp thu hồi tài khoản VPN ngay sau khi kết thúc truy cập; tuyệt đối không sử dụng các phần mềm truy cập hệ thống từ xa của các bên thứ ba.

d) Việc truy cập hệ thống từ xa phải có báo cáo và được sự đồng ý của trưởng bộ phận vận hành hoặc Lãnh đạo cơ quan trước khi thực hiện.

Điều 16. 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, Bộ phận được giao vận hành hệ thống tham mưu Lãnh đạo xã phương án thực hiện. Trong đó cần 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 Sở Y tế, đơn vị vận hành hệ thống 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 công.

Điều 17. Quy định về quản lý thiết bị

1. Thiết bị công nghệ thông tin phải đặt tên và dán nhãn theo đúng quy định.

2. Đơn vị vận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị CNTT hàng quý.

3. Đơn vị vận hành đề xuất mua thêm thiết bị CNTT và các thiết bị phụ trợ khác trong trường hợp thiết bị hết bảo hành bị hỏng. Thiết bị được trang bị phải tuân theo các tiêu chuẩn (theo yêu cầu của từng hệ thống).

4. Đối với thiết bị hỏng còn bảo hành, đơn vị vận hành, khai thác yêu cầu đơn vị cung cấp sửa chữa. Thiết bị hỏng đã hết bảo hành, đơn vị vận hành báo cáo cơ quan quản lý về phương án sửa chữa.

5. Trường hợp thiết bị hỏng là thiết bị quan trọng (máy chủ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị tường lửa), đơn vị vận hành phải báo cáo ngay về cơ quan quản lý để có biện pháp khắc phục nhanh.

Điều 18. Quy định về quản lý, khai thác sử dụng Internet

1. Hạ tầng kết nối Internet phải có các giải pháp bảo mật đảm bảo hệ thống không bị tấn công xâm nhập, lây lan virus từ bên ngoài.

2. Đơn vị vận hành chịu trách nhiệm giám sát, kiểm tra nội dung và băng thông truy cập, ngăn chặn, đề xuất xử lý các hành vi vi phạm.

Điều 19. Quy định về quản lý bản quyền phần mềm

1. Các phần mềm, chương trình ứng dụng cài đặt tại máy chủ, máy trạm phải có bản quyền sử dụng theo đúng quy định của pháp luật.

2. Chỉ được cài đặt và sử dụng các phần mềm đã mua bản quyền. Các phần mềm có bản quyền khác, phần mềm mã nguồn mở, phần mềm miễn phí phải được cơ quan quản lý phê duyệt trước khi sử dụng.

3. Đơn vị vận hành phải tổ chức quản lý, theo dõi sử dụng các bản quyền phần mềm.

4. Không phát tán, chia sẻ phần mềm có bản quyền ra bên ngoài.

Điều 20. Quy định về quản lý hồ sơ

1. Danh sách các loại hồ sơ lưu trữ:

a) Các quy trình vận hành kỹ thuật, bảo trì, bảo dưỡng các hệ thống.

b) Hồ sơ thiết kế, thuyết minh kỹ thuật, hoàn công.

c) Hồ sơ quản trị các hệ thống thông tin (báo cáo định kỳ, báo cáo sự cố, nhật ký vận hành).

d) Bảng thống kê danh sách thiết bị; Danh sách các thiết bị hỏng, hết khấu hao sử dụng chờ thanh lý, thanh hủy; Biên bản bàn giao thiết bị.

e) Tài liệu, biên bản kiểm tra, đánh giá.

f) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ phải được lưu bằng văn bản, tập tin bản mềm trên máy tính và phải được cập nhật khi có sự thay đổi.

Điều 21. Quy định về bảo trì, bảo dưỡng

1. Đơn vị vận hành có trách nhiệm

a) Xây dựng, tham mưu cơ quan quản lý phê duyệt và ban hành quy trình bảo trì, bảo dưỡng hệ thống.

b) Trực tiếp thực hiện hoặc thuê dịch vụ để thực hiện bảo trì, bảo dưỡng các hệ thống.

2. Yêu cầu về bảo trì, bảo dưỡng

a) Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến tình hình cung cấp dịch vụ của các hệ thống CNTT.

b) Quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, quy trình và ghi nhật ký về tình trạng hoạt động trước và sau khi thực hiện.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 22. CCVC thuộc Ủy ban nhân dân xã Hải Hưng có trách nhiệm thi hành Quy định này nhằm đảm bảo sự hoạt động thông suốt của hệ thống thông tin và đảm bảo an toàn an ninh dữ liệu, thông tin trên mạng; chịu trách nhiệm trước Lãnh đạo xã về công tác quản lý, bảo quản và sử dụng các trang thiết bị công nghệ thông tin được giao quản lý.

Điều 23. Trách nhiệm của Văn phòng Hội đồng nhân dân và Ủy ban nhân dân

1. Theo dõi, kiểm tra, kiểm soát toàn diện việc thực hiện các quy định tại Quy chế này.

2. Là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin và các đơn vị trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin. Phối hợp với các đơn vị có liên quan tham mưu các biện pháp quản lý, vận hành và bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy định an toàn thông tin của cơ quan có thẩm quyền.

3. Phân công viên chức phụ trách bảo đảm an toàn thông tin cho hệ thống thông tin; Cán bộ được phân công phụ trách, được tuyển dụng vào vị trí làm về ATTT có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, ATTT, phù hợp với vị trí tuyển dụng.

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

Điều 24. Rà soát, sửa đổi, bổ sung Quy chế

1. Định kỳ 02 năm hoặc khi có thay đổi về chính sách ATTT, phòng Văn phòng Hội đồng nhân dân và Ủy ban nhân dân 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.

2. Trong quá trình thực hiện Quy chế này, nếu có vướng mắc hoặc phát sinh mới, đề nghị các phòng trực thuộc cần kịp thời phản ánh về Văn phòng Hội đồng nhân dân và Ủy ban nhân dân để tổng hợp và trình Lãnh đạo xã xem xét, quyết định./.