ỦY BAN NHÂN DÂN **XÃ XUÂN HƯNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2998 /QĐ-UBND	*Xuân Hưng, ngày 23 tháng 12 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại UBND Xã Xuân Hưng

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ XUÂN HƯNG

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 12/6/2018;

Căn cứ Luật Dữ liệu ngày 30/11/2024;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 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 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Chánh Văn phòng HĐND-UBND xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế đảm bảo an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại UBND xã Xuân Hưng".

Điều 2. Quyết định này có hiệu lực kể từ ngày ký. Chánh Văn phòng HĐND-UBND xã; Thủ trưởng các cơ quan, đơn vị và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Lãnh đạo UBND xã;
- Như Điều 2;
- Trang TTĐT xã;
- Lưu: VT.

CHỦ TỊCH

U.B.N.D XÃ XUÂN HƯNG T.NINH BÌNH

Vũ Trường Khánh

QUY CHẾ
Đảm bảo an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại UBND Xã Xuân Hưng

(Kèm theo Quyết định số 2998 /QĐ-UBND, ngày 23 tháng 12 năm 2025 của Chủ tịch UBND Xã Xuân Hưng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi áp dụng

Quy chế này quy định về đảm bảo an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại UBND Xã Xuân Hưng.

Điều 2. Đối tượng áp dụng

1. Cán bộ, đảng viên, viên chức, người lao động đang làm việc tại UBND Xã Xuân Hưng;

2. Cơ quan, tổ chức, cá nhân có liên quan kết nối, sử dụng và khai thác các hệ thống thông tin tại UBND Xã Xuân Hưng;

3. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ viễn thông, công nghệ thông tin, internet và có tham gia kết nối vào các hệ thống thông tin tại UBND Xã Xuân Hưng.

Điều 3. Mục tiêu và nguyên tắc bảo đảm an toàn thông tin mạng

1. Mục tiêu

Bảo vệ thông tin, hệ thống thông tin của UBND Xã Xuân Hưng tránh bị truy cập, 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 thông tin.

2. Nguyên tắc

a) Bảo đảm an toàn thông tin đối với hệ thống thông tin của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố an toàn thông tin đối với các hệ thống thông tin tại xã.

b) Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Bảo đảm an toàn thông tin, an ninh mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng, Điều 4 Luật An ninh mạng, 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.

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

d) Cá nhân có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của cơ quan.

e) Xử lý sự cố an toàn thông tin, an ninh mạng phải phù hợp với trách nhiệm, quyền hạn, bảo đảm lợi ích hợp pháp của đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị nghiêm cấm

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

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập internet bằng thiết bị kết nối internet của cá nhân (như điện thoại di động, máy tính bảng, máy tính xách tay, USB 3G/4G/5G...).

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

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy cập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG TỔ CHỨC

Điều 5. Bộ phận chuyên trách về an toàn thông tin tại xã.

1. Văn phòng HĐND-UBND xã là bộ phận tham mưu triển khai các giải pháp đảm bảo an toàn thông tin, an ninh mạng của Xã Xuân Hưng; thực hiện chức năng của bộ phận chuyên trách về an toàn thông tin mạng theo quy định của pháp luật.

a) Đầu mối với các cơ quan quản lý nhà nước, các đơn vị ngoài về hoạt động thuộc lĩnh vực an toàn thông tin;

b) Nghiên cứu, tham mưu, xây dựng chiến lược, mô hình tổ chức; kế hoạch hành động về an toàn thông tin.

c) Chủ trì xây dựng, đề xuất ban hành văn bản chính sách; xây dựng tiêu chuẩn an toàn thông tin; xây dựng cơ chế vận hành đảm bảo tuân thủ các quy định có liên quan của pháp luật.

d) Điều hành, hướng dẫn, kiểm tra, giám sát và đánh giá việc thực hiện an toàn thông tin tại các phòng, ban. Đề xuất hình thức xử lý các vi phạm quy định, quy trình, hướng dẫn về an toàn thông tin tại phòng, ban.

e) Quy hoạch và triển khai các giải pháp kỹ thuật đảm bảo an toàn thông tin. Quản lý, theo dõi việc triển khai việc ứng dụng giải pháp an toàn thông tin.

f) Xây dựng kế hoạch đào tạo, kiểm tra, đánh giá nhân sự về an toàn thông tin.

g) Điều phối và tham gia trực tiếp xử lý các sự cố an toàn thông tin. Điều tra sự cố, rò rỉ thông tin (nếu có) tại xã.

2. Các phòng, ban và cá nhân có liên quan tại Xã Xuân Hưng

a) Tiếp nhận và triển khai thực hiện các văn bản chính sách liên quan đến an toàn thông tin. Đề xuất các chính sách an toàn thông tin phù hợp với cấp phòng, ban.

b) Phối hợp triển khai các giải pháp kỹ thuật phục vụ công tác an toàn thông tin tại phòng, ban.

c) Thực hiện đánh giá, giám sát hệ thống công nghệ thông tin tại phòng, ban; kịp thời phát hiện những điểm yếu, lỗ hổng và lỗi an toàn thông tin.

d) Sẵn sàng, chủ động phối hợp trong công tác ứng cứu sự cố an toàn thông tin.

e) Báo cáo kết quả thực hiện công tác an toàn thông tin khi được yêu cầu.

f) Chủ động đề xuất các ý kiến và giải pháp kỹ thuật để cải thiện tình hình an toàn thông tin tại phòng, ban.

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

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

Lãnh đạo xã giao cán bộ phụ trách công nghệ thông tin là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống thông tin trong xã.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) UBND Xã Xuân Hưng

Đầu mối liên hệ: Chủ tịch UBND Xã Xuân Hưng

b) Công an tỉnh - Đơn vị chuyên trách về an toàn thông tin mạng

- Đầu mối liên hệ: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

c) Bộ Công an/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam

- Bộ phận: Ban Giám sát và ứng cứu sự cố

3. Thường xuyên tham dự các lớp diễn tập đảm bảo an toàn thông tin mạng; lớp đào tạo, tập huấn chuyên sâu về an toàn thông tin mạng khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 7. Đảm bảo an toàn thông tin trong quản lý nguồn nhân lực

1. Tuyển dụng

a) Quy định cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

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

2. Quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin của người sử dụng

- Người sử dụng có trách nhiệm tuân thủ các quy định, hướng dẫn đảm bảo an toàn và các quy định của pháp luật, đảm bảo an toàn thông tin đối với từng vị trí công việc.

- Thông báo ngay cho bộ phận chuyên trách về an toàn thông tin khi nghi ngờ hoặc phát hiện sự cố, hiện tượng bất thường của hệ thống thông tin.

- Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về an toàn thông tin, an ninh mạng.

- Chịu trách nhiệm trước pháp luật về các hành vi làm lộ, lọt thông tin, nội dung bí mật của cơ quan.

- Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp hoặc mang thiết bị ra ngoài đơn vị; có trách nhiệm bàn giao lại các trang thiết bị khi chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ việc.

b) Trách nhiệm bảo đảm an toàn thông tin với cán bộ quản lý và vận hành hệ thống

- Phân rõ trách nhiệm quản lý, vận hành hệ thống thông tin đến từng cá nhân.

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

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

- Quản trị viên hệ thống khi giám sát, điều khiển hệ thống thông tin phải thông qua điều hành, không dùng thiết bị cá nhân để giám sát, điều khiển hệ thống thông tin.

- Máy tính dùng để quản trị hệ thống thông tin phải được cài đặt các chương trình quản trị hệ thống thông tin, không kết nối mạng internet và được cài đặt chương trình diệt virus có bản quyền.

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

3. Chấm dứt hoặc thay đổi công việc

a) Khi cán bộ, viên chức, người lao động nghỉ việc, chấm dứt hợp đồng hoặc chuyển sang vị trí công tác khác, Văn phòng HĐND-UBND phải thu hồi, thay đổi

hoặc điều chỉnh quyền truy cập hệ thống, các thiết bị máy móc, phần cứng, phần mềm và các tài khoản khác (nếu có) thuộc sở hữu của UBND xã.

b) Bộ phận phụ trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ, viên chức, người lao động thôi việc.

c) Việc thu hồi, thay đổi hoặc điều chỉnh quyền truy cập phải có văn bản xác nhận của trưởng phòng, ban nơi cá nhân đó làm việc, lưu hồ sơ tại phòng, ban và Văn phòng HĐND-UBND xã để theo dõi, giám sát.

d) Phòng, ban có trách nhiệm theo dõi, đảm bảo việc thực hiện đầy đủ, kịp thời các biện pháp nêu trên, không để xảy ra tình trạng nhân sự đã nghỉ hoặc chuyển vị trí vẫn còn quyền truy cập vào hệ thống thông tin của xã.

e) Cán bộ, viên chức và người lao động nghỉ việc hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Chương III
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 8. Thiết kế an toàn hệ thống thông tin

1. Đơn vị được giao chủ trì xây dựng hệ thống thông tin có trách nhiệm phối hợp với đơn vị tư vấn triển khai xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin và phương án đảm bảo an toàn thông tin theo cấp độ để triển khai đồng thời quá trình triển khai dự án theo đúng các quy định 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.

2. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin:

a) Tài liệu phân tích lựa chọn kiến trúc, công nghệ;

b) Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống;

c) Các vùng mạng trong hệ thống;

d) Các giải pháp, thiết bị của hệ thống thông tin.

3. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

4. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ; có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

5. Khi hệ thống thông tin có thay đổi thiết kế cần đánh giá lại tính phù hợp của phương án đảm bảo an toàn thông tin để kịp thời sửa đổi, bổ sung.

6. Trường hợp hệ thống xây dựng theo hình thức thuê khoán yêu cầu phải có 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 và yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm trong hợp đồng thuê phải có điều kiện liên quan đến bảo đảm hệ thống thông tin theo cấp độ.

7. Đối với hệ thống thông tin cấp độ 3 trở lên phải thực hiện kiểm thử phần mềm, kiểm tra an toàn thông tin trước khi đưa vào sử dụng hoặc cấp dịch vụ Internet.

8. Tài liệu kiểm thử phần mềm, kiểm thử an toàn thông tin, thử nghiệm, nghiệm thu kỹ thuật phải được đảm bảo an toàn thông tin.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Thử nghiệm và nghiệm thu hệ thống trước khi đưa vào sử dụng

Khi phát triển phần mềm nội bộ, các sản phẩm, thiết bị, hệ thống thông tin phải được kiểm định an toàn thông tin trước khi đưa vào sử dụng:

- Kiểm tra phiên bản phần mềm cho phần cứng (firmware) các thiết bị mạng quan trọng như: tường lửa, Switch, IDS/IPS... xem có lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo ATTT;

- Các thiết bị hệ thống trước khi được đưa vào sử dụng phải được qua kiểm định về an ninh, an toàn, cháy nổ của các cơ quan chức năng; thực hiện nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng;

- Không cài cắm mã độc vào máy chủ; thực hiện gỡ bỏ các hệ điều hành cũ đối với máy chủ và thực hiện xóa dữ liệu (Format) đối với các ổ cứng trước khi đưa vào sử dụng.

- Các hệ thống hạ tầng kỹ thuật khác phải tuân thủ vận hành thử, nghiệm thu trước khi đưa vào sử dụng, đơn vị chủ trì có trách nhiệm phối hợp với đơn vị tư vấn triển khai và các tổ chức, cá nhân liên quan tổ chức vận hành thử và nghiệm thu.

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

a) Hệ thống được thử nghiệm tổng thể trước khi đưa vào sử dụng và định kỳ hàng năm để đảm bảo tính an toàn, thống nhất của hệ thống.

b) Quy trình thử nghiệm hệ thống như sau:

- Phân tích yêu cầu;

- Lập kế hoạch kiểm thử;

- Xây dựng tình huống, kịch bản cho quy trình kiểm thử;

- Thiết lập và duy trì môi trường kiểm thử;

- Thực hiện kiểm thử;

- Lập báo cáo kết quả kiểm thử;

- Đóng chu trình kiểm thử.

c) Nội dung, kế hoạch và quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 24/2020/TT-BTTTT ngày 09/09/2020 của Bộ Thông tin và Truyền

thông (nay là Bộ Khoa học và Công nghệ) quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

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

a) Chủ quản hệ thống thông tin đảm nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống như sau:

- Kiểm thử, nghiệm thu chức năng của hệ thống;

- Kiểm thử, nghiệm thu bảo đảm an toàn thông tin;

- Kiểm thử, nghiệm thu hệ thống nội bộ của đơn vị phát triển.

b) Chủ đầu tư phối hợp với đơn vị thiết kế, xây dựng hệ thống thông tin triển khai và các bên có liên quan. Trường hợp thuê đơn vị kiểm thử độc lập: đơn vị kiểm thử độc lập phối hợp với đơn vị thiết kế, xây dựng hệ thống thông tin triển khai và các bên có liên quan.

c) Báo cáo nghiệm thu được ký xác nhận của Văn phòng và phê duyệt của Chủ tịch UBND xã trước khi đưa vào sử dụng.

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

Điều 10. Tiêu chuẩn an toàn thông tin cho các hệ thống công nghệ thông tin

1. Các hệ thống công nghệ thông tin (bao gồm tất cả các thiết bị mạng lõi, truyền dẫn, tài nguyên vật lý, hệ thống máy chủ, hệ điều hành, cơ sở dữ liệu...) được triển khai, ứng dụng cho mục đích quản lý, vận hành, sử dụng trong UBND xã.

2. Hệ thống công nghệ thông tin trong xã phải được triển khai, thiết lập, cấu hình bảo mật đảm bảo an toàn thông tin tương ứng với từng loại tiêu chuẩn cho hệ thống, thiết bị, giải pháp, dịch vụ (như tiêu chuẩn an toàn thông tin cho máy chủ, hệ điều hành, cơ sở dữ liệu...).

Điều 11. Yêu cầu về tài liệu, văn bản vận hành, triển khai theo kế hoạch

1. Tất cả hệ thống mạng phải có tài liệu quy hoạch được Chủ tịch UBND xã phê duyệt.

2. Tất cả các máy chủ/thiết bị phải được lắp đặt, triển khai và vận hành theo các tài liệu quy hoạch đã được Văn phòng HĐND-UBND xã phê duyệt.

3. Tất cả các hệ thống phải có tài liệu, hồ sơ mô tả và quản lý hệ thống, tài liệu hồ sơ này phải được cập nhật ngay khi có sự thay đổi thông tin, bao gồm:

a) Mô hình kết nối của các thiết bị mạng, máy chủ, mô hình mạng bao gồm cả sơ đồ luận lý và vật lý.

b) Thông tin quản lý thiết bị mạng trong hệ thống (tên, loại thiết bị, mục đích sử dụng, cấu hình phần cứng...)

c) Thông tin quản lý các máy chủ (tên/loại máy chủ, chức năng trong hệ thống, cấu hình vật lý, hệ điều hành và các phần mềm, dịch vụ đang được cài đặt...)

d) Thông tin quản lý ứng dụng (tên ứng dụng, loại ứng dụng, module ứng dụng...)

e) Thông tin quản lý sự cố (tên sự cố, thời điểm xảy ra sự cố, biện pháp xử lý...)

f) Thông tin quản lý rủi ro do hệ thống (loại rủi ro gây ảnh hưởng, lỗ hổng...)

g) Thông tin liên lạc của những cá nhân quản lý/ chịu trách nhiệm về hệ thống, ứng dụng.

h) Các tài liệu, quy trình, hướng dẫn khai thác, vận hành hệ thống.

Điều 12. Quản lý an toàn mạng

1. Quản lý an toàn thông tin

a) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

b) 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. Nhân sự quản trị tường lửa phải thực hiện lưu hồ sơ theo dõi các chính sách được thiết lập trên tường lửa. Thể hiện đầy đủ các thông tin sau: địa chỉ IP nguồn, địa chỉ IP đích, cổng sử dụng dịch vụ, thời hạn hiệu lực chính sách yêu cầu, mô tả mục đích sử dụng.

c) 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.

d) Cán bộ, đảng viên, viên chức, người lao động trong UBND xã khi sử dụng máy tính nội bộ không được tự ý thay đổi địa chỉ IP và địa chỉ default gateway đã được mặc định.

đ) Không được tự ý lắp đặt thiết bị thu, phát sóng Wifi (Access Point Route Wifi) vào mạng khi chưa thống nhất với Văn phòng HĐND-UBND.

e) Thiết bị không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố.

g) Không cung cấp mật khẩu của các thiết bị phát sóng Wifi trong mạng nội bộ ra bên ngoài, trừ các đoàn trực tiếp đến làm việc tại xã.

h) Việc sử dụng mạng riêng ảo (VPN- Vitual Private Network) khi có nhu cầu cần làm việc từ xa, bắt buộc phải đặt mật khẩu với độ an toàn cao và thay đổi mật khẩu tối thiểu 03 lần/tháng.

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. Cập nhật, sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống 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 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.

4. Truy cập và quản lý cấu hình hệ thống:

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

b) Quản trị viên 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 quản lý cấp trên để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

Điều 13. Quản lý an toàn máy chủ và ứng dụng

1. 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 thảm họa cho hệ thống máy chủ.

c) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phương 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.

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 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.

h) Có vùng mạng quản trị riêng, giới hạn địa chỉ IP quản trị để người quản trị truy cập vào quản trị các máy chủ.

i) Người quản trị chỉ được cấp quyền truy cập vào các máy chủ có thẩm quyền. Để được cấp tài khoản quản trị phải gửi công văn xin cấp bao gồm các thông tin tối thiểu: tên, căn cước công dân, số điện thoại, phòng ban đơn vị công tác, mục đích, phạm vi máy chủ cần truy cập... và được phê duyệt bởi đơn vị quản lý hệ thống thông tin.

k) Ghi nhật ký, quy định thời gian về hoạt động tác động vào các máy chủ, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra giám sát về sau.

l) 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 như bên ngoài vào hệ thống.

2. 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.

đ) Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của cán bộ, viên chức, người lao động và phải được phê duyệt từ cấp trên.

3. Quản lý, vận hành, duy trì hoạt động bình thường của hệ thống máy chủ và ứng dụng:

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.

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

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

d) 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…).

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

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

Điều 14. Quản lý an toàn dữ liệu

1. 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.

2. 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.

3. 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.

4. Các phòng, ban được giao chủ trì quản lý, sử dụng thông tin nào có trách nhiệm tự sao lưu dữ liệu phục vụ công tác đó.

5. Với các dữ liệu của hệ thống thông tin nghiệp vụ dùng chung trong toàn xã, Văn phòng HĐND-UBND có trách nhiệm sao lưu dự phòng vào thiết bị lưu trữ chuyên dụng.

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

7. 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.

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

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

10. 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.

Điều 15. Quản lý an toàn người sử dụng và thiết bị đầu cuối

1. Quản lý an toàn thiết bị đầu cuối

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

b) 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.

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

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

đ) Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng và thực hiện quy trình trước khi đưa vào hệ thống sử dụng

- Máy tính người dùng trước khi đưa vào sử dụng phải được đánh giá, rà soát các điểm yếu an toàn thông tin. Cài đặt hoặc cập nhật các bản vá cho hệ điều hành.

- Gỡ bỏ các phần mềm không cần thiết, cài đặt chương trình diệt virus. Không cấp tài khoản quản trị máy tính cho người dùng, không để người dùng tự ý cài đặt các phần mềm độc hại trên máy tính.

e) Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối

trước khi đưa vào sử dụng.

g) 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.

h) Khi 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 hệ thống cần có sự đồng ý của Ban Giám đốc và được bộ phận chuyên trách về an toàn thông tin kiểm tra. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

i) Máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng. Trường hợp không sử dụng trong thời gian quá 01 giờ trở lên phải tắt máy để bảo đảm an toàn.

2. Quản lý an toàn người sử dụng đầu cuối

a) Quản lý truy cập, sử dụng tài nguyên nội bộ

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

- Bộ phận 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.

- Mỗi công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các 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 và ký tự đặc biệt như !, @, #, $, %, ...) và thường xuyên thay đổi để tăng cường công tác bảo mật (đối với những máy cá nhân).

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

- 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.

b) Quản lý truy cập mạng và tài nguyên trên Internet

- Người sử dụng khi truy cập, sử dụng Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

- Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của quản trị viên hệ thống.

- 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.

c) Cài đặt và sử dụng máy tính an toàn

- 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, xử lý.

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

- Công chức, viên chức và người lao động có trách nhiệm triển khai các biện pháp phòng chống mã độc theo hướng dẫn của Văn phòng HĐND-UBND xã, cán bộ phụ trách CNTT. Không tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.

- Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 16. Quản lý sự cố

1. Phân nhóm sự cố an toàn thông tin mạng

a) Hệ thống bị gián đoạn dịch vụ.

b) Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ.

c) Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được.

d) Hệ thống bị mất quyền điều khiển.

đ) Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin cấp độ 3 hoặc cấp độ 4 hoặc cấp độ 5 khác.

e) Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng: Bộ phận phụ trách công nghệ thông tin khi phát hiện hoặc nhận được thông báo sự cố đối với hệ thống thông tin của đơn vị, phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình;

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố;

- Chủ trì, phối hợp cùng đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có) và các đơn vị chức năng liên quan tiến hành phân tích, xác minh, đánh giá tình hình, sơ bộ phân loại sự cố và triển khai ngay các hoạt động ứng cứu sự cố và báo cáo theo quy định;

- Báo cáo về sự cố, diễn biến tình hình ứng cứu sự cố, đề xuất hỗ trợ ứng cứu sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản hệ thống thông tin.

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

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

a) Chủ quản hệ thống thông tin phối hợp với các đơn vị liên quan xây dựng các công cụ giám sát phát hiện và cảnh báo sự cố an toàn thông tin mạng.

b) 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 an toàn thông tin đưa ra cảnh báo sớm về nguy cơ mất an toàn thông tin trong hệ thống.

c) Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về an toàn thông tin của cơ quan khi phát hiện các sự cố gây mất an toàn thông tin 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.

5. Quy trình ứng cứu sự cố an toàn thông tin thông thường

Thực hiện đầy đủ các nội dung quy định tại Điều 14, Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

a) Phát hiện hoặc tiếp nhận thông tin sự cố.

b) Xác minh, phân tích, đánh giá và phân loại sự cố.

c) Xử lý sự cố

d) Kết quả xử lý sự cố

đ) Tổng kết đánh giá kết quả.

e) Báo cáo kết quả ứng cứu sự cố và lưu hồ sơ.

6. Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng

Thực hiện đầy đủ các nội dung quy định tại Điều 14, Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

a) Phát hiện hoặc tiếp nhận thông tin sự cố.

b) Xác minh, phân tích, đánh giá và phân loại sự cố

c) Báo cáo sự cố

d) Lựa chọn phương án điều phối ứng cứu sự cố

đ) Điều phối ứng cứu sự cố

e) Báo cáo kết quả xử lý sự cố

g) Tổng kết đánh giá kết quả

h) Báo cáo kết quả ứng cứu sự cố và lưu hồ sơ

7. 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.

Điều 17. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro

Mức ảnh hưởng	Tính bảo mật (C)	Tính toàn vẹn (I)	Tính sẵn sàng (A)
Đặc biệt nghiêm trọng (5)	Việc bị lộ thông tin trái phép làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh	Việc sửa đổi hoặc phá hủy trái phép thông tin làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh
Nghiêm trọng (4)	Việc bị lộ thông tin trái phép làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia
Vừa phải (3)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia
Nhỏ (2)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá

		cộng	nhân hoặc làm tổn hại tới lợi ích công cộng
Không đáng kể (1)	Việc bị lộ thông tin trái phép làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân

2. Quy trình đánh giá và quản lý rủi ro

a) Bước 1: Thiết lập bối cảnh

- Cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ.

b) Bước 2: Đánh giá rủi ro an toàn thông tin

- Cần xác định tài sản, điểm yếu, mối đe dọa, hậu quả và mức ảnh hưởng đối với cơ quan, tổ chức khi rủi ro xảy ra đối với hệ thống thông tin.

- Cần xác định rõ phạm vi thực hiện đánh giá và quản lý rủi ro để bảo toàn tài sản được bảo vệ trong quy trình thực hiện.

- Cần xây dựng phương án, kế hoạch thực hiện quản lý rủi ro an toàn thông tin. Nội dung phương án, kế hoạch, trách nhiệm của các đơn vị, bộ phận liên quan cần đưa vào quy chế bảo đảm an toàn thông tin của cơ quan, tổ chức để thực hiện.

- Phân tích rủi ro để xác định ra các mức ảnh hưởng, các hậu quả đối với cơ quan, tổ chức trên cơ sở thực hiện bước nhận biết rủi ro

- Ước lượng rủi ro để xác định ra các rủi ro và mức rủi ro tương ứng mà cơ quan, tổ chức phải xử lý.

c) Bước 3: Xử lý rủi ro an toàn thông tin

- Cần xác định các phương án xử lý rủi ro, bao gồm các biện pháp quản lý và kỹ thuật để có thể xử lý, giảm thiểu các mối đe dọa có thể xảy ra đối với tài sản, dẫn tới hậu quả cho cơ quan, tổ chức.

- Có thể lựa chọn các phương án xử lý rủi ro khác nhau để bảo đảm đạt được các mục tiêu bảo đảm an toàn thông tin của đơn vị mình.

- Xử lý rủi ro có thể được thực hiện bởi một hoặc kết hợp nhiều phương án sau:

+ Thay đổi rủi ro: thực hiện các biện pháp xử lý, khắc phục nhằm giảm mức rủi ro đã được xác định sao cho các rủi ro tồn đọng được đánh giá lại ở mức chấp nhận được.

+ Duy trì rủi ro: chấp nhận rủi ro đã xác định mà không đưa ra các phương án xử lý để giảm thiểu rủi ro. Việc xác định rủi ro nào có thể được chấp nhận dựa vào mức rủi ro và tiêu chí chấp nhận rủi ro

+ Tránh rủi ro: xử lý khi cơ quan, tổ chức phải đối mặt với mức rủi ro quá cao

bằng cách làm thay đổi, loại bỏ hoặc dừng hoạt động của hệ thống, quy trình nghiệp vụ hoặc hoạt động của cơ quan, tổ chức để không phải đối mặt với rủi ro đã xác định. Tránh rủi ro là phương án thích hợp khi rủi ro được xác định vượt quá khả năng chấp nhận rủi ro của tổ chức.

+ Chia sẻ rủi ro: chuyển rủi ro, một phần rủi ro phải đối mặt cho cơ quan, tổ chức khác. Phương án chia sẻ rủi ro thường được thực hiện khi cơ quan, tổ chức xác định rằng việc giải quyết rủi ro yêu cầu chuyên môn hoặc nguồn lực được cung cấp tốt hơn bởi các tổ chức khác.

d) Bước 4: Chấp nhận rủi ro an toàn thông tin

- Xem xét, đánh giá các rủi ro tồn đọng, chưa được xử lý hoàn toàn để đánh giá lại mức rủi ro sau xử lý có thể được chấp nhận hay không. Bởi vì có thể hệ thống tồn tại những rủi ro không có phương án xử lý triệt để mà chỉ có thể giảm thiểu.

đ) Bước 5: Truyền thông và tư vấn rủi ro an toàn thông tin

- Cần trao đổi, tham vấn ý kiến của các bên liên quan để có thông tin đầu vào khi thực hiện các bước ở trên; thực hiện tuyên truyền, phổ biến các nguy cơ, rủi ro có thể xảy ra.

- Nhằm đào tạo, tuyên truyền nâng cao nhận thức cho các bên liên quan đến hoạt động đánh giá và quản lý rủi ro.

- Cơ quan, tổ chức cần xây dựng kế hoạch truyền thông rủi ro định kỳ hoặc đột xuất. Hoạt động truyền thông rủi ro phải được thực hiện liên tục và thường xuyên.

e) Bước 6: Giám sát và soát xét rủi ro

- Giám sát và đánh giá tuân thủ, tính hiệu quả của việc thực hiện việc quản lý rủi ro.

- Nhằm bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được thực hiện thường xuyên liên tục theo quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức và được cấp có thẩm quyền phê duyệt.

- Cần bảo đảm các yếu tố sau:

+ Quản lý được các tài sản mới, sự thay đổi của tài sản, giá trị của tài sản;

+ Sự thay đổi, xuất hiện mới các mối đe dọa;

+ Sự thay đổi, xuất hiện mới các điểm yếu;

+ Sự thay đổi, xuất hiện mới các rủi ro;

+ Kết quả của việc giám sát và soát xét các yếu tố rủi ro là việc cập nhật thường xuyên, liên tục sự thay đổi đối với các yếu tố rủi ro được đề cập ở trên.

Điều 18. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Quy định hủy bỏ các thông tin/dữ liệu bảo mật khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

2. Quy định về xử lý và hủy bỏ phương tiện lưu trữ điện tử

a) Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ...) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt, lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Quy định về xử lý thông tin trên các phương tiện và thiết bị công nghệ thông tin:

a) Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

b) Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu)

4. Hệ thống thông tin khi kết thúc vận hành, khai thác hoặc thanh lý, hủy bỏ phải tuân thủ các quy định của pháp luật về quản lý tài sản. Thông tin, dữ liệu trên các hệ thống thông tin phải được sao lưu và chuyển sang các hệ thống khác (nếu còn giá trị sử dụng). Thực hiện các biện pháp xóa, hủy dữ liệu trước khi thanh lý, hủy bỏ tài sản.

Chương V
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG QUẢN LÝ VÀ SỬ DỤNG TÀI KHOẢN

Điều 19. Phân loại tài khoản

Tài khoản truy cập hệ thống thông tin tại xã được phân loại theo mục đích sử dụng và đối tượng sử dụng, cụ thể như sau:

1. Tài khoản cấp cho cá nhân: Tài khoản cấp cho cá nhân sử dụng, phục vụ theo nhiệm vụ được giao.

2. Tài khoản quản trị hệ thống công nghệ thông tin là các tài khoản có quyền truy cập cao (quản trị), phục vụ cho việc cài đặt, cấu hình, vận hành, bảo trì các hệ thống, thiết bị công nghệ thông tin: tài khoản quản trị thiết bị bảo mật, tài khoản truy cập hệ thống máy chủ, thiết bị lưu trữ camera, thiết bị mạng, thiết bị bảo mật, cơ sở dữ liệu (database), tài khoản quản trị phần mềm (admin), tài khoản truy cập giao diện quản trị hệ thống… Việc cấp, sử dụng, giám sát tài khoản quản trị phải tuân thủ quy trình đặc biệt, có phân quyền rõ ràng, kiểm soát nghiêm ngặt và nhật ký hoạt động (log).

3. Tài khoản cấp cho ứng dụng công nghệ thông tin: tài khoản được dùng cho ứng dụng công nghệ thông tin tự động, kết nối vào hệ thống để phục vụ các hoạt động nghiệp vụ của ứng dụng; tài khoản kết nối từ ứng dụng vào cơ sở dữ liệu..., tài khoản cấp cho ứng dụng phải cấp cho người chịu trách nhiệm quản lý cụ thể và chỉ được dùng thông qua ứng dụng công nghệ thông tin từ các địa chỉ IP được xác định.

Điều 20. Quy định đặt tên tài khoản

1. Tài khoản cấp cho cá nhân

- Tên tài khoản phải đảm bảo thể hiện yếu tố định danh cá nhân, không trùng lặp, dễ quản lý và truy xuất.

- Trường hợp có nhiều người trùng tên, có thể bổ sung mã nhân viên, viết tắt đơn vị hoặc số thứ tự phân biệt.

- Không sử dụng tên tài khoản chung cho nhiều người, không sử dụng ký tự đặc biệt gây lỗi khi tích hợp hệ thống.

2. Tài khoản cấp cho ứng dụng công nghệ thông tin: tên tài khoản được đặt đảm bảo yếu tố định danh được ứng dụng sử dụng tài khoản.

3. Quy định đặt tên tài khoản cấp cho nhân viên đối tác: Tên tài khoản được đặt phải đảm bảo yếu tố định danh được nhân sự sử dụng tài khoản và thời hạn sử dụng tài khoản.

Điều 21. Đối tượng được cấp tài khoản

1. Đối tượng được cấp tài khoản chính thức bao gồm cán bộ, viên chức, người lao động thuộc quản lý của UBND xã, được phân công nhiệm vụ có liên quan đến việc sử dụng hệ thống công nghệ thông tin:

a) Được cấp tài khoản cá nhân để thực hiện công việc chuyên môn;

b) Trường hợp là cán bộ phụ trách kỹ thuật, quản trị hệ thống, có thể được cấp tài khoản quản trị phù hợp với phạm vi công việc;

c) Cá nhân có trách nhiệm quản lý tài khoản ứng dụng tự động hoặc tài khoản dùng chung trong đơn vị (nếu có).

2. Việc cấp tài khoản truy cập cho các đối tác, đơn vị hoặc cá nhân bên ngoài (ví dụ: chuyên gia, kỹ thuật viên bảo trì, nhân viên hợp đồng, nhà cung cấp dịch vụ...) chỉ được thực hiện trong các trường hợp thật sự cần thiết, đáp ứng các điều kiện sau:

a) Phải được sự chấp thuận bằng văn bản của Chủ tịch UBND xã;

b) Văn phòng HĐND-UBND xã là đơn vị đầu mối tiếp nhận đề nghị, thẩm định nhu cầu, xin ý kiến phê duyệt và chịu trách nhiệm giám sát, quản lý trong suốt thời gian tài khoản được sử dụng;

c) Tài khoản cấp cho đối tác phải có thời gian hiệu lực rõ ràng**,** phạm vi truy cập giới hạn và được theo dõi chặt chẽ trong nhật ký hệ thống;

d) Trường hợp tài khoản bị sử dụng sai mục đích, Văn phòng HĐND-UBND

xã phải chịu trách nhiệm chính trong công tác kiểm soát, xử lý.

Điều 22. Quy định về cấp phát tài khoản truy cập hệ thống công nghệ thông tin

Việc cấp phát tài khoản truy cập vào hệ thống công nghệ thông tin tại xã được thực hiện theo quy trình chặt chẽ, đảm bảo nguyên tắc phân quyền hợp lý, bảo mật và truy trách nhiệm. Cụ thể như sau:

1. Trách nhiệm xây dựng và quản lý quy trình cấp phát: Văn phòng HĐND-UBND xã

a) Chủ trì xây dựng, ban hành và cập nhật quy trình quản lý cấp phát, phân quyền và thu hồi tài khoản**;** tiếp nhận, thẩm định và phê duyệt yêu cầu cấp phát tài khoản cho người dùng theo đề xuất của các phòng, ban.

b) Tổ chức triển khai thực hiện đúng quy trình này.

c) Lập, lưu trữ và duy trì hồ sơ theo dõi việc cấp phát, thu hồi, thay đổi thông tin tài khoản, thông tin nhóm quyền trên hệ thống. Đảm bảo tất cả các tài khoản, nhóm quyền khai báo trên hệ thống đều hợp lệ so với hồ sơ theo dõi, không tồn tại trên hệ thống những tài khoản không sử dụng hoặc đã hết hạn.

d) Thông báo cho người sử dụng về các quyền truy cập, thời gian sử dụng tài khoản. Yêu cầu người sử dụng xác nhận quyền truy cập của mình khi được cấp/thay đổi thông tin tài khoản.

e) Phối hợp thu hồi hoặc điều chỉnh tài khoản khi người dùng có thay đổi công việc theo đúng quy trình do xã ban hành.

f) Đối với các tài khoản ngắn hạn được cấp để phục vụ nhiệm vụ có thời hạn, cán bộ Công nghệ thông tin thực hiện thu hồi/vô hiệu hóa tài khoản theo đúng thời hạn ghi trong phiếu đề nghị.

g) Ứng dụng các công cụ công nghệ thông tin vào việc giám sát, phân tích, cảnh báo và đánh giá việc sử dụng tài khoản**,** nhằm đảm bảo đúng mục đích, đúng quyền hạn và phát hiện kịp thời các rủi ro an ninh thông tin.

2. Nguyên tắc cấp phát tài khoản: Tài khoản được cấp cho từng cá nhân cụ thể, gắn với nhiệm vụ công việc được giao, không cấp tài khoản dùng chung, kể cả tài khoản chỉ có quyền giám sát.

3. Quy định về cấp tài khoản cho ứng dụng công nghệ thông tin: tài khoản cấp cho các ứng dụng công nghệ thông tin tích hợp, tự động hóa (API, kết nối hệ thống...) phải có:

a) Văn bản đề xuất của đơn vị sử dụng;

b) Phải có cá nhân chịu trách nhiệm quản lý tài khoản trong suốt thời gian hiệu lực.

4. Quy định về cấp tài khoản cho nhân sự ngoài UBND xã: việc cấp tài khoản cho đối tác, đơn vị khác, nhân viên hợp đồng... phải kèm theo:

a) Văn bản cam kết của đơn vị/đối tác về việc sử dụng tài khoản đúng mục

đích, đúng thời hạn;

b) Xác định người đại diện chịu trách nhiệm giám sát sử dụng tài khoản;

c) Có thời hạn sử dụng rõ ràng và cơ chế thu hồi khi hết hiệu lực.

5. Nguyên tắc phân quyền khi cấp tài khoản

a) Việc cấp phát tài khoản và phân quyền phải tuân thủ nguyên tắc "quyền hạn tối thiểu – vừa đủ để hoàn thành công việc"

b) Phòng, ban đề xuất cấp tài khoản phải xác định rõ quyền cần cấp và thời hạn hiệu lực cụ thể (ngày, tháng, năm hoặc thời gian hiệu lực).

6. Trách nhiệm của cá nhân được cấp tài khoản

a) Thiết lập và sử dụng mật khẩu mạnh, không chia sẻ tài khoản với bất kỳ ai. Đảm bảo an toàn tuyệt đối thông tin đăng nhập cá nhân. Trường hợp đặc biệt (chia sẻ tạm thời) phải có sự phê duyệt của Trưởng phòng, ban và sau đó người sử dụng phải đổi lại mật khẩu.

b) Chịu trách nhiệm trước Chủ tịch UBND và Trưởng phòng, ban về việc bảo vệ, sử dụng đúng mục đích và bảo mật tài khoản cá nhân được cấp.

c) Phải cam kết sử dụng tài khoản đúng với chức năng, nhiệm vụ công việc được giao. Không được lạm dụng quyền truy cập để thực hiện các hành vi trái quy định. Trường hợp được cấp quyền vượt quá chức năng, nhiệm vụ, người sử dụng phải báo cáo ngay cho Văn phòng HĐND-UBND xã để điều chỉnh phù hợp.

d) Khi phát hiện bị lộ mật khẩu hoặc nghi ngờ có hành vi xâm nhập trái, người sử dụng phải đổi ngay mật khẩu, trong trường hợp không thể tự đổi phải làm thủ tục khôi phục mật khẩu theo quy trình quản lý cấp phát tài khoản tương ứng.

e) Khi được cung cấp mật khẩu mới hoặc được khôi phục lại mật khẩu, người dùng cần phải đổi ngay mật khẩu mới ngay sau đó.

f) Người sử dụng không sử dụng chức năng mặc định lưu trữ các thông tin về mật khẩu trên trình duyệt web và các công cụ (SQL navigator…) kết nối vào mạng lưới, hệ thống/ứng dụng, database của xã, ngoại trừ trong trường hợp sử dụng Master Password hay các phần mềm chuyên dụng có mã hóa để bảo vệ mật khẩu và được Văn phòng HĐND-UBND xã phê duyệt.

Điều 23. Quy định về quản lý nhóm quyền, phân quyền cho tài khoản

1. Các nhóm quyền quản trị hệ thống phải được phân công và phê duyệt từ Văn phòng HĐND-UBND xã.

2. Các nhóm quyền trên các hệ thống phải được định nghĩa chi tiết, bao gồm: tên nhóm quyền, mục đích của nhóm quyền, các quyền được thực hiện, đối tượng được cấp tài khoản thuộc nhóm quyền đã định nghĩa.

3. Phòng, ban phải quản lý thông tin nhóm quyền (lưu thông tin đồng thời bằng văn bản được phê duyệt và trên hệ thống phân quyền), chỉ được phân quyền tài khoản theo các nhóm quyền đã được định nghĩa.

Điều 24. Quy định về thu hồi tài khoản

1. Khi tài khoản đến thời điểm hết hiệu lực theo hồ sơ đăng ký ban đầu, phòng, ban phải chủ động rà soát và đề nghị Văn phòng HĐND-UBND tiến hành thu hồi hoặc xóa bỏ tài khoản trên hệ thống. Việc thu hồi cần thực hiện chậm nhất trong vòng 03 ngày làm việc kể từ khi tài khoản hết hiệu lực.

2. Đối với các tài khoản trong hệ thống: Văn phòng HĐND-UBND đưa ra quy định về việc tài khoản không dùng sau bao nhiêu ngày sẽ bị khóa, xóa khỏi hệ thống. Thời gian tối đa không quá 90 ngày.

3. Trường hợp nhân sự chuyển công tác, nghỉ việc, thay đổi nhiệm vụ, bị đình chỉ... phòng, ban phải làm thủ tục đề nghị Văn phòng HĐND-UBND thu hồi/hủy tài khoản. Trường hợp chậm trễ dẫn đến rò rỉ, lạm dụng tài khoản, Trưởng phòng, ban phải liên đới trách nhiệm.

Điều 25. Kiểm soát truy cập hệ thống công nghệ thông tin

1. Văn phòng HĐND-UBND phải xác định và lập danh sách các hệ thống quan trọng, các tài khoản có đặc quyền, tài khoản có quyền thực hiện các chức năng quan trọng trong hệ thống (tài khoản quan trọng).

2. Không dùng các kết nối truy cập trực tiếp từ internet đến máy tính, hệ thống mạng nội bộ, các công cụ hỗ trợ truy cập như Ultraview, Teamviewer, VNC, Anydesk... Chỉ sử dụng các công cụ truy cập từ xa được Văn phòng kiểm duyệt, kiểm soát, có khả năng mã hóa và ghi nhật ký truy vết.

3. Đối với các tài khoản quan trọng trong hệ thống, chỉ được thực hiện kết nối, truy cập từ địa chỉ IP đã được đăng ký.

4. Văn phòng HĐND-UBND phải lưu hồ sơ quản lý các địa chỉ IP được phép kết nối, tác động đến các hệ thống quan trọng. Định kỳ hàng tháng rà soát, đối chiếu với thực tế kết nối và nhật ký truy cập các địa chỉ IP được phép truy cập tới các hệ thống quan trọng. Xử lý, thu hồi quyền truy cập từ IP không còn hợp lệ hoặc đã quá hạn đăng ký.

Điều 26. Giám sát truy cập hệ thống công nghệ thông tin

1. Văn phòng HĐND-UBND phải có các giải pháp kỹ thuật để kiểm soát, giám sát các tài khoản có thể kết nối đến các hệ thống quan trọng. Thiết lập cơ chế giám sát theo thời gian thực (real-time) hoặc theo lô (batch), phù hợp với đặc điểm từng hệ thống.

2. Phải thực hiện ghi nhật ký (log) tác động, log thực hiện các chức năng quan trọng trên hệ thống. Thời gian lưu log tối thiểu 6 tháng đối với các hệ thống thông thường, và tối thiểu 12 tháng đối với hệ thống trọng yếu hoặc chứa thông tin bí mật. Đối với từng hệ thống, Lãnh đạo UBND xã và Văn phòng HĐND-UBND phê duyệt đảm bảo đáp ứng theo yêu cầu nghiệp vụ, chức năng cụ thể.

3. Văn phòng HĐND-UBND xã có trách nhiệm:

a) Định kỳ rà soát nhật ký truy cập để phát hiện bất thường;

b) Thiết lập cảnh báo tự động (nếu có) khi phát hiện truy cập trái phép hoặc

thao tác bất thường;

c) Lưu trữ và bảo vệ log đúng quy định, không để mất, rò rỉ, chỉnh sửa log trái phép;

d) Hỗ trợ cung cấp log khi có yêu cầu điều tra, xử lý sự cố an toàn thông tin hoặc theo yêu cầu của các cơ quan chức năng.

Chương VI
ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI SẢN PHẨM PHẦN MỀM/THIẾT BỊ

Điều 27. Tiêu chuẩn an toàn thông tin cho các sản phẩm phần mềm/thiết bị

1. Đối tượng áp dụng: Bao gồm tất cả phần mềm, thiết bị do xã triển khai, ứng dụng, sản xuất, hợp tác hoặc mua sắm; cũng như phần mềm, thiết bị được trang cấp nhưng được đưa vào vận hành trong hệ thống.

2. Yêu cầu an toàn thông tin: Tất cả các phần mềm, thiết bị nêu trên phải đáp ứng các tiêu chuẩn an toàn thông tin theo quy định, bao gồm cả các ứng dụng web, phần mềm di động (mobile app) và các thiết bị phần cứng chuyên dụng.

Điều 28. Quy định an toàn thông tin trên thiết bị, máy tính, thiết bị di động người dùng cuối

Tất cả các thiết bị di động, máy tính người dùng cuối sử dụng hệ thống phải đảm bảo các tiêu chuẩn an toàn thông tin theo tiêu chuẩn về an toàn thông tin trên các loại thiết bị, máy tính người dùng cuối.

Điều 29. Quy định kiểm soát, đánh giá an toàn thông tin trước khi triển khai, nâng cấp, sử dụng sản phẩm phần mềm/ thiết bị

Tất cả các sản phẩm phần mềm/ thiết bị trước khi triển khai, nâng cấp hay đưa vào sử dụng đều phải đáp ứng các tiêu chuẩn an toàn thông tin theo quy định.

Chương VII
ĐẢM BẢO AN TOÀN THÔNG TIN KHI LÀM VIỆC VỚI ĐỐI TÁC

Điều 30. An toàn thông tin khi làm việc với đối tác

1. Hợp đồng với các đối tác có kết nối đến hệ thống thông tin, cung cấp triển khai các ứng dụng công nghệ thông tin cho xã phải bao gồm các điều khoản về bảo mật và nghĩa vụ về an toàn thông tin:

a) Cam kết không tiết lộ thông tin;

b) Trách nhiệm xử lý lỗ hổng, khắc phục sự cố;

c) Có điều khoản xử phạt và bồi thường nếu vi phạm an toàn thông tin;

d) Quy định này áp dụng cho cá nhân, tổ chức liên quan của đối tác bao gồm nhân viên của đối tác và các nhà thầu phụ của đối tác trong trường hợp đối tác ký kết hợp đồng với nhà thầu phụ.

2. Văn phòng HĐND-UBND xã là đầu mối làm việc với các đối tác, phải lập hồ sơ nhật ký giám sát dịch vụ của đối tác cung cấp, bao gồm tối thiểu các

thông tin sau:

- Tên đối tác

- Dịch vụ cung cấp

- Ngày thực hiện

- Các vấn đề an toàn thông tin (sự cố gây gián đoạn, mất hay lộ thông tin, lỗ hổng phần mềm, thời gian khắc phục lỗ hổng…)

- Các thay đổi trong dịch vụ/ nhân sự (nếu có)

Điều 31. Tiêu chuẩn an toàn thông tin cho đối tác

1. Tất cả các hệ thống, dịch vụ, sản phẩm do đối tác cung cấp, chuyển giao cho UBND xã phải đáp ứng các tiêu chuẩn an toàn thông tin theo quy định.

2. Tất cả các hợp đồng ký kết với đối tác phải có điều khoản cam kết việc tuân thủ tiêu chuẩn an toàn thông tin. Điều khoản cam kết phải nêu rõ trách nhiệm, phương án xử lý, thời gian xử lý với các vi phạm tiêu chuẩn an toàn thông tin của đối tác.

Chương VIII
ĐẢM BẢO AN TOÀN THÔNG TIN CỦA THIẾT BỊ CÓ KHẢ NĂNG LƯU TRỮ THÔNG TIN/DỮ LIỆU

Các quy định trong mục này áp dụng cho việc cấp phát, quản lý vào/ra, luân chuyển thu hồi tất cả các thiết bị điện tử, công nghệ thông tin, viễn thông có chứa hoặc có khả năng lưu trữ thông tin thông tin, dữ liệu thuộc UBND xã phụ trách, quản lý.

Điều 32. Quy định sử dụng thiết bị lưu trữ cá nhân

Nghiêm cấm viên chức và người lao động sử dụng USB, thẻ nhớ, bộ nhớ trong điện thoại, ổ cứng di động, thiết bị lưu trữ cá nhân để sao chép dữ liệu từ máy tính nội bộ. Trường hợp đặc biệt, phải được sự đồng ý bằng văn bản của Lãnh đạo UBND xã hoặc người được uỷ quyền, đồng thời phải đảm bảo các biện pháp bảo mật theo quy định.

Điều 33. Quy định đối với các thiết bị lưu trữ của phòng, ban được cấp phép

1. Các thiết bị lưu trữ di động (như USB, ổ cứng, thẻ nhớ...) được cấp phép sử dụng tại phòng, ban phải được dán nhãn nhận diện và chỉ định rõ cá nhân quản lý, chịu trách nhiệm sử dụng và bảo quản**.**

2. Khi sử dụng thiết bị lưu trữ để kết nối với máy chủ hoặc hệ thống nội bộ, thiết bị phải được kiểm tra, quét mã độc (virus/malware) trước khi kết nối và sử dụng.

Điều 34. An toàn khi thu hồi, luân chuyển, thanh lý thiết bị

1. Các thiết bị công nghệ thông tin (máy tính, phương tiện lưu trữ...) khi thu hồi, luân chuyển hoặc thanh lý phải được xóa sạch dữ liệu, ghi đè hoặc phá hủy vật lý, đảm bảo không thể khôi phục thông tin.

2. Đối với phương tiện lưu trữ chứa dữ liệu quan trọng, việc xử lý dữ liệu

(xóa, ghi đè, tiêu hủy) phải có phương án được Lãnh đạo UBND hoặc người được ủy quyền phê duyệt**.**

3. Đối với **t**hiết bị mạng khi bàn giao hoặc thay đổi mục đích sử dụng phải được Văn phòng HĐND-UBND xã loại bỏ hoàn toàn cấu hình hiện tại, khôi phục về trạng thái mặc định của nhà sản xuất**.**

4. Đối với máy chủ khi thay đổi mục đích sử dụng phải được bộ phận quản trị xóa toàn bộ dữ liệu, thư mục ứng dụng, cấu hình, mã nguồn... trước khi bàn giao hoặc sử dụng lại.

5. Tất cả thiết bị công nghệ thông tin vào/ra cơ quan phải được kiểm soát và phê duyệt theo đúng quy định hiện hành.

Chương IX
QUY ĐỊNH VỀ AN TOÀN THÔNG TIN ĐỐI VỚI CÁN BỘ, NHÂN VIÊN

Điều 35. Quy định bảo vệ thông tin/ dữ liệu

1. Cán bộ, viên chức và người lao động trong xã có trách nhiệm tuyệt đối bảo mật các thông tin và dữ liệu theo chức trách, nhiệm vụ được giao.

2. Nghiêm cấm các hành vi sau, dưới bất kỳ hình thức nào:

a) Thu thập, cung cấp, trao đổi, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép các loại thông tin, dữ liệu nội bộ;

b) Tải lên (upload), chia sẻ, phát tán thông tin, tài liệu, phần mềm lên các nền tảng Internet như: mediafire, 4share, gmail, yahoo mail, Dropbox, Google Drive... hoặc các ứng dụng mạng xã hội như: Facebook, Zalo, Viber, Telegram...

c) Sao chép, sử dụng, phát tán mã nguồn phần mềm (source code), cơ sở dữ liệu hoặc các tài sản số của cơ quan mà không được phép.

3. Việc cung cấp thông tin nội bộ trong trường hợp đặc biệt (phục vụ công việc, phối hợp liên ngành, báo cáo theo yêu cầu cơ quan chức năng...) phải được sự chấp thuận bằng văn bản của Chủ tịch UBND hoặc người được ủy quyền.

4. Chỉ được sử dụng các công cụ chia sẻ dữ liệu đã được UBND cấp phát và phê duyệt để phục vụ công việc. Việc sử dụng công cụ cá nhân để lưu trữ, chia sẻ dữ liệu nội bộ không được phép, trừ khi có văn bản đồng ý từ cấp có thẩm quyền.

Điều 36. Quy định về việc truy cập, sử dụng máy tính an toàn

1. Nghiêm cấm **c**án bộ, viên chức và người lao động truy cập các website không lành mạnh, các website có nội dung vi phạm pháp luật, các website chứa nội dung crack, keygen phần mềm ….

2. Nghiêm cấm truy cập internet trên các máy tính của UBND xã thông qua các thiết bị cá nhân (USB - 3G, USB 4G, bộ phát Wi-Fi di động) và các thiết bị không thuộc cơ quan, tổ chức quản lý. Trường hợp đặc biệt cần sử dụng thiết bị ngoài hệ thống, phải có sự phê duyệt bằng văn bản của Chánh Văn phòng HĐND-

UBND xã trước khi thực hiện

3. Tuyệt đối không mở các tập tin đính kèm (email attachment) hoặc nhấp vào các đường liên kết (link) không rõ nguồn gốc, đáng ngờ hoặc không có liên quan đến công việc chuyên môn. Trường hợp nghi ngờ có mã độc, phần mềm gián điệp, phải báo cáo ngay cho Văn phòng HĐND-UBND xã để được kiểm tra, xử lý.

Chương X
TỔ CHỨC THỰC HIỆN

Điều 37. Chính sách xây dựng quy chế an toàn thông tin

1. Quy chế được lấy ý kiến các cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng.

2. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Văn phòng HĐND-UBND xã để tổng hợp điều chỉnh, bổ sung.

4. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

Điều 38. Trách nhiệm của Lãnh đạo UBND xã

1. Chỉ đạo xây dựng, ban hành và tổ chức thực hiện Quy chế đảm bảo an toàn thông tin.

2. Phân công rõ trách nhiệm quản lý, giám sát an toàn thông tin cho các phòng, ban.

3. Đảm bảo bố trí nguồn lực (nhân sự, tài chính, thiết bị) phục vụ cho công tác bảo mật và an toàn thông tin.

4. Xem xét, xử lý các sai phạm về an toàn thông tin theo đúng quy định của pháp luật và Quy chế nội bộ.

Điều 39. Trách nhiệm của Văn phòng HĐND-UBND xã

1. Chủ trì tham mưu các nhiệm vụ về bảo đảm an toàn thông tin mạng trong triển khai ứng dụng công nghệ thông tin phục vụ hoạt động của xã.

2. Xây dựng, cập nhật, phổ biến các chính sách, quy trình kỹ thuật đảm bảo an toàn thông tin.

3. Quản lý hệ thống mạng, tài khoản, phân quyền truy cập, thiết bị lưu trữ, phần mềm... theo tiêu chuẩn an toàn thông tin.

4. Giám sát, phát hiện và ứng phó sự cố an toàn thông tin.

5. Phối hợp với các đơn vị liên quan tổ chức đào tạo, hướng dẫn, tuyên truyền nâng cao nhận thức về an toàn thông tin cho nhân viên.

6. Định kỳ đánh giá, kiểm tra, rà soát hệ thống và báo cáo Lãnh đạo UBND xã.

7. Cung cấp thông tin, dữ liệu phục vụ thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo về bảo đảm an toàn thông tin khi cấp có thẩm quyền yêu cầu.

8. Thường xuyên cập nhật các quy định mới về bảo đảm an toàn thông tin mạng trong quá trình vận hành hệ thống; đề xuất phương án bảo đảm an toàn thông tin cho hệ thống mạng và các hệ thống thông tin khi có thay đổi về thiết kế.

9. Tham mưu, đề xuất với Lãnh đạo UBND xã biện pháp quản lý, vận hành; nâng cấp hệ thống thông tin và triển khai các biện pháp bảo đảm an toàn thông tin đáp ứng nhiệm vụ chuyển đổi số phục vụ công tác của đơn vị.

10. Sau khi tuyển dụng, tiếp nhận nhân sự mới, có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn thông tin, an ninh mạng của xã.

11. Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

12. Giám sát, nhắc nhở công chức, viên chức, người lao động thay đổi mật khẩu thường xuyên.

13. Chủ trì phối hợp bộ phận phụ trách CNTT khi cán bộ, viên chức và người lao động chấm dứt hoặc thay đổi công việc; phải thu hồi các tài khoản, quyền truy cập hệ thống, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc quản lý của UBND xã.

Điều 40. Trách nhiệm của cán bộ, đảng viên, viên chức và người lao động

1. Lãnh đạo các phòng, ban có trách nhiệm tổ chức thực hiện Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin; thường xuyên quán triệt các quy định về an toàn thông tin, an ninh mạng để nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin.

2. Thực hiện các chính sách, quy trình, quy định, hướng dẫn các giải pháp kỹ thuật để đảm bảo an toàn thông tin trong quá trình sử dụng.

3. Nghiêm túc chấp hành quy định này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

4. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và Văn phòng HĐND-UBND để kịp thời ngăn chặn và xử lý.

5. Tham gia đầy đủ các chương trình diễn tập, tập huấn về an toàn thông tin, an ninh mạng do các cơ quan chuyên trách về an toàn, an ninh thông tin tổ chức.

6. Phối hợp, cung cấp thông tin và tạo điều kiện để Văn phòng HĐND-UBND hoặc bộ phận phụ trách CNTT triển khai công tác kiểm tra, khắc phục sự cố an toàn thông tin kịp thời, nhanh chóng và đạt hiệu quả.

Điều 41. Trách nhiệm của nhà cung cấp thiết bị/ phần mềm hệ thống công nghệ thông tin

1. Tuân thủ quy định của pháp luật về an toàn thông tin

Nhà cung cấp có trách nhiệm thực hiện đầy đủ các yêu cầu, tiêu chuẩn về an toàn thông tin theo quy định, đặc biệt đối với các sản phẩm có khả năng kết nối mạng, lưu trữ hoặc xử lý thông tin dữ liệu.

2. Cam kết về bảo mật và an toàn thông tin

Trong hợp đồng cung cấp thiết bị/phần mềm phải có điều khoản ràng buộc về bảo mật thông tin, bao gồm:

- Cam kết không tiết lộ, đánh cắp, hoặc chia sẻ dữ liệu.

- Cam kết xử lý kịp thời các lỗ hổng, sự cố kỹ thuật liên quan đến an toàn thông tin.

- Có trách nhiệm bồi thường thiệt hại nếu vi phạm dẫn đến rò rỉ, mất mát dữ liệu.

3. Hỗ trợ triển khai và vận hành hệ thống an toàn

- Cung cấp đầy đủ tài liệu kỹ thuật, hướng dẫn vận hành an toàn hệ thống/phần mềm thiết bị.

- Hỗ trợ kiểm tra bảo mật, thiết lập các cấu hình an toàn theo yêu cầu của .

- Phối hợp với Văn phòng HĐND-UBND xã giám sát, cập nhật, bảo trì hệ thống định kỳ.

4. Quản lý nhân sự và bảo mật khi làm việc

Chịu trách nhiệm nếu nhân sự vi phạm quy định bảo mật, an toàn thông tin trong quá trình làm việc.

5. Bàn giao sản phẩm đúng chuẩn an toàn thông tin

- Thiết bị phải được bàn giao trong tình trạng an toàn, không chứa mã độc, không thiết lập sẵn tài khoản, mật khẩu mặc định nguy hiểm.

- Phần mềm phải không có mã độc, backdoor và được cập nhật các bản vá bảo mật mới nhất.

6. Tham gia xử lý sự cố

Trong trường hợp xảy ra sự cố liên quan đến sản phẩm đã cung cấp, nhà cung cấp có trách nhiệm phối hợp kịp thời với UBND xã để điều tra, khắc phục và ngăn chặn tái diễn.

Trên đây là Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin tại UBND Xã Xuân Hưng. Trong quá trình thực hiện nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung, các tổ chức, cá nhân có liên quan phản ánh trực tiếp về Văn phòng HĐND-UBND xã để được hướng dẫn cụ thể./.