UỶ BAN NHÂN DÂN **XÃTRƯỜNG SƠN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 118/QĐ-UBND	*Trường Sơn, ngày 05 tháng 12 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế Bảo đảm an toàn, an ninhhệ thống thông tin của UBND xã Trường Sơn

ỦY BAN NHÂN DÂN XÃ TRƯỜNG SƠN

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH-13 ngày 19/11/2015;

Căn cứ 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;

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sữa đổi bổ sung một số điều của Luật tổ chức chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

Căn cứ Quyết định số 01/2021/QĐ-UBND ngày 19/01/2021 của UBND tỉnh về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh;

Theo đề nghị của Văn phòng-Thống kê, công chức Văn hóa-Xã hội xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Ban hành Quy chế Bảo đảm an toàn, an ninh hệ thống thông tin của UBND xã Trường Sơn.

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

Điều 3. Công chức Văn phòng-Thống kê, Công chức Văn hóa-Xã hội, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận: - Như điều 3; - Phòng VH-TT huyện; - Chủ tịch, PCT UBND xã; - BCĐ Chuyển đổi số xã; - Trang TTĐT xã; - Lưu: VP, VH.	**TM. ỦY BAN NHÂN DÂN** **CHỦ TỊCH** **Lê Đình Tài**

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

QUY CHẾ
Ban hành Quy chế Bảo đảm an toàn, an ninh hệ thống thông tin của UBND xã Trường Sơn

(Ban hành kèm theo 118/QĐ-UBND ngày 05 tháng12 năm 2023 của UBND Trường Sơn)

Chương I:
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho các Hệ thống thông tin do UBND xã Trường Sơn quản trị, vận hành (sau đây gọi tắt là các Hệ thống thông tin), bao gồm:

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

2. Đối tượng áp dụng

a) Cán bộ viên chức và người lao động thuộc UBND xã Trường Sơn;

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các Hệ thống thông tin tại UBND xã Trường Sơn;

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của các Hệ thống thông tin tại UBND xã Trường Sơn.

Điều 2. Giải thích từ ngữ

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

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

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

3. Hệ thống thông tin: là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. Chủ quản hệ thống thông tin: là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

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

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

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

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

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

1. Mục tiêu bảo đảm an toàn thông tin

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

2. Nguyên tắc

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

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

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

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

c) Việc bảo đảm an toàn Hệ thống thông tin tại UBND xã Trường Sơn 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.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm được quy định tại Điều 7 Luật An toàn thông tin mạng 2015 và Điều 8 Luật An ninh mạng 2018, cụ thể:

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

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

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

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

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

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

7. Hành vi quy định tại khoản 1 Điều 18 của Luật An ninh mạng số 24/2018/QH14.

8. Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

9. Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc.

10. Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

11. Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng.

12. Xúi giục, lôi kéo, kích động người khác phạm tội.

13. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

14. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

15. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

16. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

17. Hành vi khác vi phạm quy định của Luật An ninh mạng 2018.

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

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

a) Công chức văn hóa-xã hội phối hợp với Văn phòng UBND tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin đối với các Hệ thống thông tin của đơn vị.

b) Văn phòng UBND, Công chức văn hóa-xã hội có trách nhiệm phối hợp với phòng Văn hóa-Thông tin, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh và các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin bảo đảm an toàn thông tin, an ninh mạng cho các Hệ thống thông tin của đơn vị.

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 Trường Sơn

- Người liên hệ: Bà Nghiêm Thị Thu Hằng - Công chức Văn phòng-Thống kê

+Số điện thoại: 0978 710 362

+ Email: thuhang03062010@gmail.com

- Người liên hệ: Bà Nguyễn Thị Hoa - Công chức văn hóa-xã hội

+ Số điện thoại: 0985 457 123

+ Email: hoadung.ts@gmail.com

b) UBND huyện Đức Thọ

- Người liên hệ: Vương Thị Huyền

- Chuyên viên phòng Văn hóa Thông tin huyện

+ Số điện thoại: 0974372525

+ Email: huyenvt.dt@hatinh.gov.vn

c) Sở Thông tin và Truyền thông tỉnh Hà Tĩnh

- Điện thoại: 02393606789

- Email: ttcntt-tt@hatinh.gov.vn

- Địa chỉ: Số 18, đường 26/3, Thành phố Hà Tĩnh.

- Thành viên thường trực: Ông Nguyễn Thanh Lâm - Phó Giám đốc Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông Hà Tĩnh.

+ Đt: 0914237788

+ Email: ntlam.stttt@hatinh.gov.vn

d) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố

- Số điện thoại: 0869 100 317

- Email: ir@vncert.vn

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn

- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

3. Giao bộ phận chuyên trách 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 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

a) Công chức, Viên chức, người lao động được tuyển dụng làm nhiệm vụ về an toàn thông tin có trình độ, chuyên môn về lĩnh vực công nghệ thông tin, an toàn thông tin bảo đảm phù hợp với yêu cầu vị trí việc làm và tiêu chuẩn chức danh nghề nghiệp viên chức theo quy định.

b) Thực hiện tuyển dụng công chức, viên chức bảo đảm đúng quy trình, thủ tục pháp luật hiện hành và phân cấp tuyển dụng công chức, viên chức của tỉnh.

c) Thực hiện đánh giá năng lực của công chức, viên chức phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

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

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với cán bộ quản lý và vận hành hệ thống

+ Cán bộ quản lý và vận hành hệ thống 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 quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chắc năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Công chức, viên chức chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

b) Thực hiện đúng quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức thôi việc, nghỉ hưu.

c) Lập biên bản cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc, nghỉ hưu, chuyển công tác.

Chương II:

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

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Đối với hệ thống phải thông qua đặt hàng để thiết kế, không có sẵn dịch vụ công nghệ thông tin trên thị trường.

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

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

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

d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

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

2. Đối với dịch vụ công nghệ thông tin có sẵn trên thị trường

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê dịch vụ các nội dung liên quan đến việc đơn vị cung cấp dịch vụ là đơn vị vận hành hệ thống.

b) Có cam kết của đơn vị cung cấp dịch vụ về bảo đảm tính bí mật và bản quyền của dịch vụ.

c) Yêu cầu đơn vị cung cấp dịch vụ cung cấp các tài khoản quản trị, mã nguồn hệ thống. Hỗ trợ chỉnh sửa khi có yêu cầu.

Điều 8. Phát triển phần mềm thuê khoán

Đối với việc thuê dịch vụ phát triển phần mềm theo hình thức thuê khoán cần phải:

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

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

a) Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách.

b) Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

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

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

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

Điều 9. Thử nghiệm và nghiệm thu hệ thống

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

2. Có nội dung, kế hoạch thực hiện vận hành thử/kiểm thử theo quy định.

3. Có bộ phận có trách nhiệm thực hiện tham gia vận hành thử/kiểm thử và nghiệm thu hệ thống.

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

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

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

Điều 10. Quản lý truy cập

1. Chính sách truy cập thông tin nghiệp vụ

- Phân loại các ứng dụng, hệ thống mạng theo các mức độ an ninh: Thông tin bí mật, nhạy cảm, thông tin nội bộ, thông tin dùng chung.
- Phân quyền quản lý truy cập theo người dùng, nhóm người dùng.

2. Chính sách quản lý truy cập mạng

- Phân tách các dịch vụ khác nhau nằm trong các vùng mạng khác nhau. Đặc biệt, các ứng dụng nhạy cảm phải được tách riêng và kiểm soát chặt chẽ.
- Yêu cầu ràng buộc đối với người dùng khi truy cập dịch vụ:

+ Nhập đúng tên người dùng;
+ Đăng nhập đúng phạm vi sử dụng;
+ Thay đổi mật khẩu mặc định;
+ Chấp nhận cơ chế mã hóa dữ liệu của hệ thống;
+ Máy trạm cài đầy đủ các phần mềm bảo mật;
+ Địa chỉ máy trạm được phép truy cập.

- Lập hồ sơ ghi lại cách sử dụng các dịch vụ mạng: Lớp mạng và dịch vụ mạng nào được phép truy cập, ai là người được truy cập, quy trình kiểm soát truy cập như thế nào.

3. Chính sách quản lý kết nối từ xa

- Phải sử dụng những hệ thống, phương thức mã hóa trên đường truyền như OpenSSL, HTTPS, SSH…
- Sử dụng phương thức kết nối an toàn, đảm bảo khả năng bảo mật thông tin như VPN.
- Kiểm soát và hạn chế các kết nối hoặc truy cập đến các cổng điều khiển, quản lý: Cổng console, cổng cho phép remote access trên thiết bị mạng (telnet, ssh). Các cổng kết nối từ xa đến các máy chủ.
- Đặt mật khẩu bảo vệ, đóng các cổng không sử dụng trên thiết bị.

Điều 11. Quản lý an toàn mạng

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

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

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

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

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

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

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn và duy trì việc gia hạn bản quyền, dịch vụ bản quyền hàng năm.

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

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

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

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

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

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

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

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

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

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

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

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

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

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

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

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

Điều 13. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

2. Định kỳ hàng tháng 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.

3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.Thông tin về tất cả các lần sao lưu đều phải ghi rõ trong Nhật ký sao lưu dữ liệu. Các băng, đĩa sử dụng sao lưu phải có đánh số, dán nhãn và ghi chú cẩn thận để có thể tìm lại dễ dàng, tránh nhầm lẫn.

Điều 14. Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

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

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

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

4. Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi,

kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

5. 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.

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

Điều 15. Quản lý phòng chống phần mềm độc hại

- Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;
- Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;
- Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;
- Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

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

- Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;
- Đối tượng giám sát bao gồm: Thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có);
- Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;
- Truy cập và quản trị hệ thống giám sát;
- Loại thông tin cần được giám sát;
- Lưu trữ và bảo vệ thông tin giám sát (Nhật ký hệ thống);
- Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;
- Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;
- Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin đảm bảo hệ thống hoạt động ổn định, an toàn

Điều 17. Quản lý rủi ro an toàn thông tin mạng

1. Xác định mức rủi ro

a) Nhận biết tài sản thông qua xác định và thu thập thông tin đầy đủ về tài sản của mình đang quản lý, đặc biệt là các thông tin liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản. Đánh giá các nguy cơ, điểm yếu đối với tài sản đó, từ đó có thể đánh giá xem mỗi tài sản khi gặp rủi ro thì sẽ gây ra hậu quả, mức độ ảnh hưởng thế nào đối với cơ quan, tổ chức

b) Phân loại nhóm các điểm yếu: Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu an toàn thông tin trong hệ thống; Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: Không có quy định về sử dụng mật khẩu an toàn; không có quy định về lưu trữ có mã hóa, không có quy định về

quy trình xử lý sự cố, không có quy định về bảo đảm an toàn thông tin phía người sử dụng.v.v.; Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: Không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công.v.v.; Nhóm các điểm yếu khác liên quan đến các nguy cơ mất an toàn thông tin từ bên thứ ba.

c) Phân loại các mối đe dọa: Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật.

d) Đánh giá hậu quả và khả năng xảy ra sự cố, xác định mức rủi ro bao gồm các mức thấp, trung bình, cao, rất cao, cực cao.

2. Quy trình đánh giá và quản lý rủi ro bao gồm 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý rủi ro; (4) Chấp nhận rủi ro và 02 quá trình cần thực hiện song song: Truyền thông và tư vấn rủi ro, Giám sát và soát xét rủi ro.

3. Biện pháp kiểm soát rủi ro được thực hiện theo yêu cầu an toàn cơ bản trong Hồ sơ đề xuất cấp độ của Hệ thống thông tin được cấp có thẩm quyền phê duyệt.

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

Cá nhân hoặc tập thể có trách nhiệm bảo đảm an toàn thông tin mạng trong quản lý, sử dụng thiết bị công nghệ thông tin được giao.

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 CNTT 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 CNTT: 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.

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)

Chương IV:
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 19. Trách nhiệm của UBND xã Trường Sơn

1. Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định.

2. Thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin;

3. Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin, báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết;

4. Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền;

5. Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Bộ Thông tin và Truyền thông trong công tác bảo đảm an toàn thông tin.

Điều 20. Trách nhiệm của các đơn vị, tổ chức, cá nhân khi tham gia hỗ trợ vận hành các hệ thống, phần mềm tại UBND xã Trường Sơn

1. Thực hiện nghiêm túc quy chế làm việc tại UBND xã Trường Sơn và theo sự hướng dẫn của cán bộ quản lý, vận hành UBND xã Trường Sơn.

2. Sử dụng đúng tài khoản được cấp để truy cập từ xa. Thực hiện nghiêm túc Điều 4, Điều 10 Quy chế này.

Điều 21. Trách nhiệm của Văn phòng UBND, công chức Văn hóa-xã hội

1. Văn phòng UBND phối hợp với công chức văn hóa-xã hội, tổ ứng cứu của UBND huyện Đức Thọ, chuyên trách về an toàn thông tin của UBND huyện Đức Thọ và các đơn vị liên quan trong công tác bảo đảm an toàn, an ninh cho các hệ thống thông tin.

2. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách về an toàn thông tin được giao tại Quy chế này.

Điều 22.Trách nhiệm của người dùng

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về an toàn thông tin tại Điều 14 Quy chế này.

Chương V:
TỔ CHỨC THỰC HIỆN

Điều 23. Xây dựng và công bố

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

2. Quy chế được công bố trước khi áp dụng.

3. Tổ chức tuyên truyền, phổ biến cho toàn bộ công chức, viên chức trong tổ chức.

3. Tổ chức tuyên truyền, phổ biến cho toàn bộ công chức, viên chức trong tổ chức.

Điều 24. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng. Trong quá trình thực hiện, nếu có những vấn đề vướng mắc cần sửa đổi, bổ sung đề xuất Đơn vị xem xét, quyết định./.