

Số: /QĐ-UBND

Ea H'Leo, ngày tháng năm 2024

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của UBND huyện Ea H'Leo

CHỦ TỊCH ỦY BAN NHÂN DÂN HUYỆN

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

Căn cứ Nghị định số 27/2018/NĐ-CP ngày 01 tháng 03 năm 2018 của Chính phủ về sửa đổi Nghị định 72/2013/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 09 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 20/2016/QĐ-UBND ngày 17 tháng 5 năm 2016 của UBND tỉnh ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk;

Theo đề nghị của Phòng Văn hóa và Thông tin huyện Ea H'Leo tại Tờ trình số 44/TTr, ngày 25/11/2024.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này “Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của UBND huyện Ea H’Leo”.

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

Điều 3. Chánh Văn phòng HĐND và UBND huyện; Thủ trưởng các cơ quan, đơn vị; Chủ tịch UBND các xã, thị trấn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- UBND tỉnh Đắk Lắk;
- Sở TTTT tỉnh Đắk Lắk;
- Phòng CNTT Sở TTTT tỉnh Đắk Lắk;
- Thường trực Huyện ủy;
- TT HĐND huyện;
- CT, các PCT UBND huyện;
- Các cơ quan, đơn vị;
- UBND các xã, thị trấn;
- Cổng Thông tin điện tử huyện;
- Lưu: VT, VHTT.

CHỦ TỊCH**Nguyễn Văn Hà**

QUY CHẾ
Bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công
nghe thông tin của UBND huyện Ea H'Leo
(Ban hành kèm theo Quyết định số /ngày tháng năm 2024
của Ủy ban nhân dân huyện Ea H'Leo)

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 Hệ thống Mạng nội bộ của UBND huyện Ea H'Leo quản trị, vận hành (sau đây gọi tắt là Hệ thống mạng nội bộ), 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) Các đơn vị thuộc UBND huyện Ea H'Leo; cán bộ thuộc các đơn vị thuộc UBND huyện Ea H'Leo
- b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ tại UBND huyện Ea H'Leo
- 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 Hệ thống mạng nội bộ.

Điều 2: Giải thích từ ngữ

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

- 1. *An toàn thông tin mạng*: là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.
- 2. *Mạng*: là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính

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

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

5. *Sự cố an toàn thông tin mạng*: Là việc thông tin, Hệ thống mạng nội bộ 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 mạng nội bộ.

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 Hệ thống Mạng nội bộ.

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 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.

Điều 4. Những hành vi nghiêm cấm

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

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

3. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập 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 (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

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:

UBND huyện Ea H'Leo giao Phòng Văn hóa và 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 Mạng nội bộ.

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 huyện Ea H'Leo

- Đơn vị liên hệ: Phòng Văn hóa và Thông tin huyện

- Người liên hệ: Nguyễn Huy Dũng

+ Chức vụ: Trưởng Phòng

+ Số điện thoại: 0944005588

+ Email: dungnh@eahleo.daklak.gov.vn

b) Sở Thông tin và Truyền thông tỉnh Đắk Lắk

- Liên hệ: Phòng Công nghệ Thông tin - Sở Thông tin và Truyền thông tỉnh Đắk Lắk

+ Email: phongcntt@tttt.daklak.gov.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>

Điều 6: Bảo đảm nguồn nhân lực

1. Tuyển dụng

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

2. 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:

+ Công chức 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.

+ Công chức 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 chức năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Công 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) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

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. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

Điều 8: Phát triển phần mềm thuê khoán

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.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.
2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

Chương III:

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

Điều 10. Quản lý an toàn mạng

1. Hệ thống mạng phải được thiết kế thống nhất, có sơ đồ logic và vật lý về hệ thống mạng, tổ chức 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.
2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (trường hợp chưa trang bị thiết bị tường lửa chuyên dụng thì có thể tích hợp tường lửa trên Router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.
3. Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng
4. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

Điều 11. 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 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.

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

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

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

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

Điều 13. Quản lý sự cố an toàn thông tin

1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác khi xảy ra sự cố an toàn thông tin trong mạng.

2. Xây dựng và triển khai phương án giám sát, phát hiện và cảnh báo sự cố an toàn thông tin trong quy trình ứng cứu sự cố an toàn thông tin mạng nhằm khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

3. Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

4. Liên hệ với đầu mối ứng cứu sự cố theo thông tin đưa ra dưới đây:

a) Sở Thông tin và Truyền thông tỉnh Đắk Lắk

- Liên hệ: Phòng Công nghệ Thông tin – Sở Thông tin và Truyền thông tỉnh Đắk Lắk

Email: phongcntt@tttt.daklak.gov.vn

b) 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>

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

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

a. 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.

b. 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.

c. 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

d. 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.

e. 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.

f. 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.

g. 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.

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

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

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

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

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

Điều 15. Quản lý rủi ro an toàn thông tin mạng

1. Xây dựng danh mục tài sản thông tin, dữ liệu có trong hệ thống. 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.

2. 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.

3. 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.

4. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại 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 bao gồm các mức thấp, trung bình, cao, rất cao, cực cao.

5. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 16. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành 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.

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

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

4. 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)

5. 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. 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.

Chương IV:

TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 17. Trách nhiệm của UBND huyện Ea H'Leo

Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 18. Trách nhiệm của Phòng Văn hóa và Thông tin huyện

1. Là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.

2. Giao Phòng Văn hóa và Thông tin huyện làm nhiệm vụ tham mưu vận hành, quản lý hệ thống mạng nội bộ của đơn vị.

3. Có trách nhiệm xây dựng và tổ chức thực thi chính sách bảo đảm an toàn thông tin cho hệ thống mạng nội bộ của đơn vị.

4. 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 19. 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 20. Xây dựng và công bố

1. Chính sách được thông qua và công bố công khai trước khi áp dụng.
2. Tổ chức tuyên truyền, phổ biến cho toàn thể công chức, viên chức, người lao động trong cơ quan để triển khai thực hiện

Điều 21. 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 chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.
3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Bộ phận chuyên trách về ATTT để tổng hợp báo cáo, điều chỉnh, bổ sung.