ỦY BAN NHÂN DÂN **HUYỆN NGỌC HỒI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1619/QĐ-UBND	*Ngọc Hồi, ngày 29 tháng 12 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo An toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện Ngọc Hồi

ỦY BAN NHÂN DÂN HUYỆN NGỌC HỒI

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015 và Luật Sửa 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 Luật Cơ yếu số 05/2011/QH13 ngày 26 tháng 11 năm 2011 của Quốc hội về Luật Cơ yếu;

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

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và truyền thông về quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Văn bản số 741/UBND-KGVX ngày 17/3/2023 của UBND tỉnh về việc triển khai nhiệm vụ trọng tâm về An toàn thông tin mạng năm 2023;

Xét đề nghị của Phòng Văn hoá và Thông tin huyện tại Tờ trình số 291/TTr-VHTT ngày 26/12/2023 về việc ban hành Quyết định phê duyệt cấp độ bảo đảm An toàn thông tin mạng đối với hệ thống thông tin trên địa bàn huyện.

QUYẾT ĐỊNH:

Điều 1. Quyết định này Ban hành kèm theo Quy chế đảm bảo An toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện Ngọc Hồi.

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

Điều 3. Chánh Văn phòng HĐND&UBND huyện, Thủ trưởng các phòng, ban, ngành huyện; Chủ tịch Ủy ban nhân dân các xã, thị trấn; các cơ quan, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Sở Thông tin và Truyền thông;
- CT, các PCT UBND huyện;
- Phòng VH và TT;
- Trang TTĐT huyện;
- Lưu: VT, TH.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Y Lan

ỦY BAN NHÂN DÂN HUYỆN NGỌC HỒI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Đảm bảo An toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện Ngọc Hồi

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày / /2023 của Ủy ban nhân dân huyện Ngọc Hồi)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

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

Điều 2. Đối tượng áp dụng

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

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

Điều 3. Giải thích từ ngữ

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

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

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

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

4. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ Công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

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

6. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

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

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

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

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

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm An toàn thông tin mạng. Hoạt động An toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Việc xử lý sự cố An toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

3. Hoạt động An toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Yêu cầu thiết kế, xây dựng hệ thống thông tin

1. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin phải xây dựng phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định trước khi trình cấp có thẩm quyền phê duyệt dự án.

2. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) Chủ quản hệ thống thông tin có trách nhiệm tổ chức đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống

theo cấp độ *(gọi tắt là Nghị định số 85/2016/NĐ-CP)* để áp dụng phương án bảo đảm an toàn thông tin phù hợp;

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân tỉnh thẩm định, trình cấp có thẩm quyền phê duyệt.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, Chủ quản hệ thống thông tin phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10 Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông 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.

Điều 6. Quản lý thuê dịch vụ Công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ Công nghệ thông tin, cơ quan, đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ Công nghệ thông tin

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý;

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan;

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

3. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm;

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ;

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ;

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại…

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin;

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 7. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng Công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử;

Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet;

Phải bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

2. 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.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách Công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 8. Quy định về cấp phát thu hồi cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó.

2. Cán bộ chuyên trách thực hiện quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các cơ quan, đơn vị. Hủy quyền truy cập hệ thống thông tin đối với cán bộ, công chức (CBCC) nghỉ chế độ, chuyển công tác và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi CBCC đó. Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

3. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao *(có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %,...).*

Điều 9. Bảo đảm nguồn nhân lực

1. Cán bộ chuyên trách được đảm bảo các điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

2. Cán bộ được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện 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; 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.

3. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho tổ chức, cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

Điều 10. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a) Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng Công nghệ thông tin của các cơ quan nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao;

b) Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. Trang bị thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan, đơn vị khi kết nối với hệ thống bên ngoài; cài đặt phần mềm phòng chống mã độc Viettel an toàn thông tin để kiểm soát, phát hiện truy cập trái phép vào hệ thống;

c) Đối với các phòng, ban, đơn vị trực thuộc không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết;

d) Khi thực hiện truy nhập từ xa vào mạng nội bộ thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin *(như: SSL/TLS, VPN...)* và thiết lập mật khẩu có độ phức tạp cao;

đ) Xây dựng 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 trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác;

e) Không 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 cơ quan, đơn vị;

g) Không tự ý thay đổi, gỡ bỏ biện pháp, giải pháp an toàn thông tin 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. Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý hệ thống mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập *(Access Point - AP)*, cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ *(Service Set Identifier - SSID),* mật khẩu có độ phức tạp cao *(có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %),* cấp phép truy nhập đối với địa chỉ vật lý *(MAC Address),* mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật;

c) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài, cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 11. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác *(ví dụ tài khoản thư điện tử, chữ ký số, chứng thư số)* để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu;

b) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm Quyết định có hiệu lực, cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho cơ quan, đơn vị vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số.

2. Khi thực hiện chia sẻ tài nguyên trên máy tính, các cơ quan, đơn vị phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

3. Cơ quan, đơn vị sử dung máy tính và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

4. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

Điều 12. Bảo đảm an toàn thiết bị đầu cuối

1. Trên máy tính cá nhân phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc; thiết lập chế độ tự động cập nhật phần mềm phòng chống mã độc, chế độ tự động rà quét mã độc khi sao chép, mở các tập tin, chế độ rà quét máy tính định kỳ hằng tuần.

2. Khuyến khích các cơ quan, đơn vị đầu tư, mua sắm thiết bị Công nghệ thông tin sản xuất trong nước. Nếu mua sắm thiết bị Công nghệ thông tin nhập khẩu thuộc danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông quy định.

3. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

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

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

4. Trong quá trình sử dụng thiết bị đầu cuối

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.

Điều 13. Quản lý giám sát an toàn hệ thống thông tin

1. Hệ thống thông tin phải triển khai hệ thống giám sát an toàn thông tin đáp ứng các yêu cầu tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm tích hợp dữ liệu tỉnh *(Sở Thông tin và Truyền thông)* thì có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ bảo đảm các yêu cầu giám sát an toàn hệ thống thông tin theo quy định của pháp luật.

3. Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại cơ quan, đơn vị. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

Điều 14. Ứng cứu sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả;

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin;

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin;

d) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị; cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân nhóm sự cố an toàn thông tin

a) Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật;

c) Sự cố do lỗi của người quản trị, vận hành hệ thống;

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

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

Hoạt động ứng cứu sự cố An toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

3. Phân loại mức độ nghiêm trọng sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị;

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị;

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp;

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ

thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp;

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Quy trình phối hợp ứng cứu xử lý sự cố

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

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3;

c) Bước 3: Báo sự cố về UBND huyện *(qua Phòng Văn hóa và Thông tin)* theo mẫu số 01 kèm theo Quy chế này;

d) Bước 4: Phối hợp với Phòng Văn hóa và Thông tin và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 02 kèm theo Quy chế này. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho UBND huyện *(qua Phòng Văn hóa và Thông tin)*.

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của Phòng Văn hóa và Thông tin, đơn vị tham mưu UBND huyện báo cáo ngay Sở Thông tin và Truyền thông tỉnh để được hướng dẫn, hỗ trợ.

6. Phòng Văn hóa và Thông tin là cơ quan chuyên trách về an toàn thông tin có trách nhiệm:

a) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố An toàn thông tin mạng, ứng phó sự cố An toàn thông tin mạng;

b) Thực hiện quy trình ứng cứu sự cố An toàn thông tin mạng thông thường và nghiêm trọng theo quy định;

c) 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;

d) Tham gia diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của ngành cấp trên.

Chương III

KIỂM TRA ĐÁNH GIA CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 15. Kế hoạch kiểm tra hằng năm

1. Phòng Văn hóa và Thông tin chủ trì, phối hợp với Văn phòng HĐND & UBND huyện, Công an huyện và các đơn vị liên quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn huyện theo Kế hoạch công tác hằng năm.

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin trên địa bàn huyện.

Điều 16. Nội dung hình thức kiểm tra đánh giá hệ thống thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực theo các nội dung theo Quy chế này; việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin; kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin;

b) Đánh giá hiệu quả của biện pháp bảo đảm an thông tin tại đơn vị; phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

c) Kiểm tra, đánh giá các nội dung khác theo quy định hệ thống an toàn thông tin.

2. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của UBND huyện và đơn vị chuyên trách về an toàn thông tin của tỉnh;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá

a) Đơn vị chuyên trách ATTT tại Trung ương;

b) Ủy ban nhân dân tỉnh hoặc Sở Thông tin và Truyền thông *(đơn vị chuyên trách về an toàn thông tin trên địa bàn tỉnh);*

c) UBND huyện giao nhiệm vụ kiểm tra về an toàn thông tin trên địa bàn huyện cho Phòng Văn hóa và Thông tin.

4. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

5. Đối tượng kiểm tra, đánh giá là các ban, ngành, đơn vị hoạt động sự nghiệp thuộc UBND huyện.

Chương IV

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

Điều 17. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Tham mưu Ủy ban nhân dân huyện về công tác bảo đảm an toàn thông tin trên địa bàn huyện và chịu trách nhiệm trước Ủy ban nhân dân huyện trong việc bảo đảm an toàn thông tin.

2. Tham mưu Ủy ban nhân dân huyện xây dựng hồ sơ đề xuất cấp độ an toàn thông tin và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

3. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm An toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Ủy ban nhân dân huyện đối với các cơ quan nhà nước đóng trên địa bàn huyện.

4. Hàng năm, cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm An toàn thông tin mạng cho cán bộ phụ trách An toàn thông tin mạng. Tổ chức tuyên truyền về An toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn huyện.

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

6. Là cơ quan đầu mối thực hiện việc tiếp nhận và xử lý các sự cố về An toàn thông tin mạng trên địa bàn huyện.

Điều 18. Trách nhiệm của Văn phòng HĐND & UBND huyện

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

2. Chỉ đạo, phân công cán bộ triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

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

4. Cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm An toàn thông tin mạng.

Điều 19. Trách nhiệm của các cơ quan, đơn vị và UBND các xã, thị trấn

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

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

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

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

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

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

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

8. Thực hiện các báo cáo về An toàn thông tin mạng khi UBND huyện có yêu cầu.

Điều 20. Trách nhiệm của cán bộ công chức, viên chức và người lao động trong các cơ quan đơn vị

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

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

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

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

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố An toàn thông tin mạng;

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

2. Trách nhiệm của người sử dụng

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;

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

Điều 21. Trách nhiệm của các tổ chức, cá nhân liên quan

Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do UBND huyện triển khai hoặc liên quan đến hoạt động ứng dụng Công nghệ thông tin của các cơ quan nhà nước của huyện phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Điều 22. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn huyện và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Phòng Văn hóa và Thông tin có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo UBND huyện theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của UBND huyện và cơ quan có thẩm quyền của tỉnh.

3. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Phòng Văn hóa và Thông tin để tổng hợp báo cáo Ủy ban nhân dân huyện xem xét điều chỉnh, bổ sung./.