ỦY BAN NHÂN DÂN HUYỆN NHƠN TRẠCH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1307 /QĐ-UBND	*Nhơn Trạch, ngày 15 tháng 4 năm 2021*

QUYẾT ĐỊNH

V/v 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 huyện Nhơn Trạch

CHỦ TỊCH ỦY BAN NHÂN DÂN HUYỆN NHƠN TRẠCH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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

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 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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 03/2017/TT-BTTTT ngày 24/4/2017 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của 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 20/10/2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, 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 Quyết định số 48/2018/QĐ-UBND ngày 07/11/2018 của UBND tỉnh 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 Đồng Nai;

Xét đề nghị của Phòng Văn hóa và Thông tin huyện Nhơn Trạch tại Tờ trình số 57/VHTT-CNTT ngày 01 tháng 4 năm 2021.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này 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 huyện Nhơn Trạch.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 2208/QĐ-UBND ngày 23/6/2015 của Chủ tịch UBND huyện Nhơn Trạch về ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước trên địa bàn huyện Nhơn Trạch.

Điều 3. Chánh Văn phòng HĐND và UBND huyện, Thủ trưởng các cơ quan, ban, ngành, đoàn thể huyện, Chủ tịch UBND các xã, thị trấn, các đơn vị trường học và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- Như Điều 3 (thực hiện);
- UBND tỉnh (báo cáo);
- Sở Thông tin và Truyền thông;
- Chủ tịch, các Phó Chủ tịch UBND huyện;
- Ban Chỉ đạo CQĐT tỉnh;
- Chánh, Phó VP HĐND và UBND huyện;
- Lưu VT, TH (NN).

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lương Hữu Ích

ỦY BAN NHÂN DÂN
HUYỆN NHƠN TRẠCH

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

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 huyện Nhơn Trạch

(Ban hành kèm theo Quyết định số 1307/QĐ-UBND ngày 15 tháng 4 năm 2021 của UBND huyện Nhơn Trạch)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT), bao gồm:

- Bảo vệ thông tin cá nhân;
- Bảo vệ hệ thống thông tin mạng;
- Giám sát an toàn hệ thống thông tin;
- Ngăn chặn xung đột thông tin trên mạng;
- Đảm bảo an toàn thông tin nội bộ;
- Quy trình khắc phục sự cố mạng;
- Quản lý và sử dụng thiết bị công nghệ thông tin phục vụ công tác soạn thảo và lưu trữ văn bản, tài liệu mật của các cơ quan nhà nước trên địa bàn huyện Nhơn Trạch.

Điều 2. Đối tượng áp dụng

1. Các cơ quan, ban, ngành cấp huyện; các đơn vị sự nghiệp công lập trực thuộc UBND huyện; UBND các xã, thị trấn trên địa bàn huyện (gọi tắt là các cơ quan, đơn vị).

2. Các cán bộ, công chức, viên chức, người lao động (gọi tắt là công chức viên chức) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác hệ thống thông tin tại cơ quan, đơn vị quy định tại Khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, mạng internet, công nghệ thông tin; các tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của cơ quan, đơn vị thuộc Khoản 1 Điều này.

4. Khuyến khích các cơ quan, đơn vị khác có hoạt động ứng dụng và phát triển công nghệ thông tin trên địa bàn huyện áp dụng quy chế 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 sự bảo vệ thông tin, hệ thống thông tin trên không gian mạng tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm đảm bảo 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 các thiết bị 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. Xâm phạm an toàn thông tin mạng: Là hành vi truy cập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin.

5. Nguy cơ mất an toàn thông tin: Là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái hệ thống an toàn thông tin.

6. 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, toàn vẹn thông tin, tính bảo mật hoặc tính khả dụng.

7. Xung đột thông tin: Là việc hai hoặc nhiều tổ chức trong nước, ngoài nước sử dụng biện pháp công nghệ, kỹ thuật thông tin gây nhiễu thông tin, tổn hại đến thông tin, hệ thống thông tin trên mạng.

8. 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 việc sao chép, sửa đổi, xóa bỏ trái phép thông tin được lưu trữ trong hệ thống thông tin.

9. Hệ thống lọc phần mềm độc hại: Là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc, cảnh báo và thống kê phần mềm độc hại truy cập trái phép vào hệ thống thông tin mạng.

10. Tính toàn vẹn: Là bảo vệ sự chính xác và đầy đủ của thông tin và các phương pháp xử lý.

11. Tính sẵn sàng của hệ thống thông tin: Là đảm bảo cho người dùng được cấp quyền có thể truy nhập thông tin, truy cập ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: sự cố mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống hoặc từ chối dịch vụ của hệ thống mạng cung cấp.

12. Cấu hình chuẩn: Là cấu hình được các nhà sản xuất thiết bị phần cứng, phần mềm khuyến nghị áp dụng nhằm loại bỏ các xung đột kỹ thuật, lỗ hổng có thể xảy ra trong quá trình cấu hình thiết bị.

13. Cổng giao tiếp (Port) là để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước nhằm định danh duy nhất các ứng dụng đó. Khi người dùng máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ được mở để truyền tải dữ liệu.

14. Bản ghi nhật ký hệ thống (Log file): Là tệp được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng..., chứa tất cả các thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và kết quả để có các biện pháp xử lý thích hợp.

15. Mạng ngang hàng (mạng nội bộ): là mạng trong đó các máy tính có quyền ngang hàng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

16. Mạng internet: là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau thông qua nhà mạng cung cấp dịch vụ internet.

17. Thông tin cá nhân: Là thông tin gắn với việc xác định danh tính của một người, một đối tượng cụ thể.

18. Xử lý thông tin cá nhân: Là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

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. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. 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.

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

Điều 5. Các hành vi nghiêm cấm

1. Ngăn chặn trái phép việc truyền tải thông tin trên mạng; can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa, làm sai lệch thông tin trên mạng với mọi hình thức.

2. Cản trở trái phép, gây ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc cản trở trái phép, gây ảnh hưởng tới khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

3. Tấn công, vô hiệu hóa trái phép làm mất tác dụng của các thiết bị bảo vệ an toàn thông tin cho hệ thống thông tin; lợi dụng sơ hở, nhược điểm của hệ thống thông tin để truy cập, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin.

4. Phát tán thư, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo trên môi trường mạng để lừa đảo.

5. Lợi dụng mạng để truyền bá thông tin nhằm thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia, các tổ chức, cá nhân; phá hoại khối đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố, gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và các thành phần xã hội.

6. Lợi dụng mạng để truyền bá trái phép các tài liệu, hình ảnh, âm thanh hoặc các dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của các tổ chức, cá nhân.

CHƯƠNG II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Bảo vệ thông tin cá nhân

1. Công chức viên chức có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại Khoản 1, 2 Điều 10; Khoản 1, 4 Điều 16; Khoản 3 Điều 17; Khoản 1 Điều 18 của Luật An toàn thông tin mạng; Điều 5 của Quy chế này và trong các văn bản pháp luật có liên quan.

Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của tỉnh và huyện, có trách nhiệm:

a. Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào hệ thống thông tin, các phần mềm, ứng dụng dùng chung của tỉnh, huyện triển khai.

b. Phải thực hiện thay đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, huyện triển khai.

c. Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh, huyện tại các điểm truy cập Internet công cộng tuyệt đối không được đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng và phải đăng xuất ra ngay khi không sử dụng.

2. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định tại Khoản 2, 3, 4, 5 Điều 16; Khoản 1, 2 Điều 17; Khoản 3 Điều 18 và Điều 19 của Luật An toàn thông tin mạng và các quy định sau:

a. Quản lý và phân quyền truy cập trên hệ thống thông tin, các phần mềm ứng dụng, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác và sử dụng.

b. Ngay sau khi công chức viên chức đã nghỉ hưu, thôi việc hoặc chuyển công tác các cơ quan, đơn vị phải thực hiện thu hồi các thiết bị công nghệ thông tin liên quan, đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị hệ

thống thông tin, phần mềm ứng dụng, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc thu hồi tài khoản người dùng.

Điều 7. Quy định bảo vệ hệ thống thông tin mạng

1. Đối với cơ quan nhà nước.

a. Trang bị đầy đủ các kiến thức bảo mật cơ bản cho công chức viên chức trước khi cho phép truy cập và sử dụng hệ thống thông tin.

b. Phân công công chức viên chức chuyên trách hoặc phụ trách công nghệ thông tin để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại đơn vị.

c. Thủ trưởng cơ quan, đơn vị tạo điều kiện để công chức viên chức chuyên trách hoặc phụ trách công nghệ thông tin học tập, tiếp thu công nghệ, kiến thức an toàn thông tin.

d. Hàng năm, xác định các nhiệm vụ bảo đảm an toàn thông tin cho hệ thống thông tin (mở rộng, nâng cấp, đầu tư, thay thế trang thiết bị phần cứng, phần mềm phục vụ cho công tác đảm bảo an toàn thông tin, đào tạo, bồi dưỡng kiến thức công nghệ thông tin,...) phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả.

e. Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật công nghệ thông tin, hệ thống thông tin của cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng, đồng thời phải tuân thủ các điều kiện sau:

- Phòng đặt máy chủ hệ thống thông tin phải được bố trí ở khu vực có điều kiện an ninh tốt, khô ráo, có điều hòa không khí, nguồn cung cấp điện ổn định và dự phòng, có các thiết bị phòng cháy chữa cháy, chống sét, nội quy, camera giám sát ra vào,...Thiết lập cơ chế bảo vệ mạng nội bộ, đảm bảo an toàn thông tin khi kết nối với mạng bên ngoài bằng các công cụ, thiết bị bảo vệ (tường lửa, hệ thống chống xâm nhập trái phép, hệ thống giám sát, cảnh báo);

- Khuyến nghị các cơ quan, đơn vị, tổ chức, địa phương trang bị hệ thống mạng nội bộ (LAN) theo hướng sử dụng máy chủ (Server/client) để quản lý các máy trạm trong hệ thống mạng, hạn chế sử dụng mô hình mạng ngang hàng (hệ thống mạng không có máy chủ quản lý) trang bị hệ thống tường lửa (Firewall) để bảo vệ hệ thống mạng. Các máy chủ, máy trạm, hệ thống lưu trữ (SAN), thiết bị mạng, mạng không dây (wifi) phải được bảo vệ bởi mật khẩu an toàn. Tất cả các máy tính tại các cơ quan, đơn vị phải được cài đặt các phần mềm bảo vệ, phòng chống mã độc, vi-rút có bản quyền;

- Các thiết bị công nghệ thông tin dùng để soạn thảo, in ấn, lưu trữ thông tin, tài liệu, văn bản bí mật nhà nước trong các cơ quan, đơn vị phải được kiểm duyệt và bố trí riêng ở nơi đảm bảo an ninh, bí mật, an toàn. Bắt buộc thiết lập mật khẩu phức tạp, cơ chế mã hóa dữ liệu và phân quyền, quy trách nhiệm người dùng được giao sử dụng để đảm bảo an toàn, bảo mật thông tin;

- Khi thực hiện di chuyển các trang thiết bị công nghệ thông tin lưu trữ dữ liệu, thông tin thuộc danh mục bí mật nhà nước phải được tổ chức quản lý, giám sát chặt chẽ theo quy định của pháp luật về bảo vệ bí mật nhà nước;

- Khi thuê dịch vụ công nghệ thông tin phải đặt tiêu chí đảm bảo an toàn thông lên hàng đầu;

- Các cơ quan, đơn vị, cá nhân tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về đảm bảo an toàn thông tin trên mạng truyền số liệu chuyên dùng được quy định tại Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và đảm bảo an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

f. Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, thu hồi các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin, triển khai các công cụ hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

g. Hệ thống thông tin phải cài đặt chế độ giới hạn số lần đăng nhập sai tài khoản (không quá 05 lần nhập sai liên tiếp), hệ thống tự động khóa hoặc cô lập tài khoản trong một khoảng thời gian nhất định mới cho phép người dùng tiếp tục đăng nhập cho lần kế tiếp.

h. Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa, phát hiện kịp thời việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu.

i. Thiết lập hệ thống thông tin ghi nhận và lưu vết các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống,...Ghi nhận đầy đủ các thông tin trong bản ghi nhật ký, thời gian lưu trữ các bản ghi nhật ký hệ thống tối thiểu 01 năm. Thường xuyên kiểm tra bản ghi nhật ký để kịp thời phát hiện dấu hiệu bất thường, có nguy cơ mất an toàn thông tin.

j. Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập lại cấu hình hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin và kiểm soát quá trình cài đặt trên máy chủ.

k. Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng, thiết lập các chế độ phân quyền truy cập theo chức năng, nhiệm vụ của người dùng.

l. Định kỳ hàng tuần sao lưu (backup) thông tin (không ghi đè thông tin, sao lưu dự phòng các thông tin thay đổi), dữ liệu của đơn vị và lưu trữ thông tin sao lưu trên thiết bị ở nơi an toàn theo quy định. Thường xuyên kiểm tra thông tin, dữ liệu sao lưu để đảm bảo tính sẵn sàng và toàn vẹn.

m. Thiết lập ràng buộc của hệ thống thông tin về cách đặt mật khẩu phức tạp cho tài khoản sử dụng trên hệ thống (mật khẩu có độ dài ít nhất 08 ký tự bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt). Người dùng không được tiết lộ, chia sẻ mật khẩu tài khoản cho người khác, khi kết thúc công việc hoặc chuyển giao máy tính cho người khác sử dụng phải thực hiện đăng xuất ra khỏi tài khoản đang dùng trên các hệ thống thông tin, các phần mềm, cơ sở dữ liệu đang tác nghiệp.

2. Đối với các đơn vị, doanh nghiệp cung cấp các dịch vụ viễn thông, công nghệ thông tin, internet cho cơ quan quản lý nhà nước trên địa bàn huyện.

Thực hiện các nội dung liên quan đến hoạt động bảo đảm an toàn thông tin mạng theo Điều 22 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; Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông và các quy định sau:

a. Thực hiện các quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của các cơ quan, đơn vị. Áp dụng và tổ chức thực hiện các biện pháp ngăn chặn việc gửi thông tin vi phạm quy định của pháp luật khi nhận được thông báo của cơ quan, đơn vị. Cung cấp các điều kiện kỹ thuật và nghiệp vụ cần thiết để thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng theo yêu cầu của cơ quan nhà nước có thẩm quyền.

b. Phải có hệ thống lọc phần mềm độc hại trong quá trình thực hiện các dịch vụ gửi, nhận, lưu trữ thông tin trên hệ thống của mình quản lý. Có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền, quản lý, phối hợp ngăn chặn mất an toàn thông tin trên không gian mạng internet, từ khách hàng của mình, phối hợp, kết nối định tuyến để đảm bảo hệ thống máy chủ có tên miền quốc gia Việt Nam hoạt động an toàn, ổn định.

3. Nguồn kinh phí thực hiện nhiệm vụ chuyên môn thuộc công tác bảo đảm an toàn thông tin do ngân sách nhà nước bảo đảm, theo quy định của Luật Ngân sách nhà nước và các văn bản pháp luật khác có liên quan.

4. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại.

a. Tất cả các máy trạm, máy chủ, các thiết bị công nghệ thông tin trong mạng và hệ thống thông tin phải được cài đặt phần mềm chống vi-rút phù hợp. Các phần mềm phòng chống vi-rút phải được thiết lập chế độ tự động cập nhật, chế độ tự động dò, quét mã độc, vi-rút khi thực hiện sao chép, lưu trữ, mở các tệp tin.

b. Các công chức viên chức trong cơ quan, đơn vị phải được hướng dẫn về phòng chống mã độc, vi-rút, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan, đơn vị.

c. Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình vô hiệu hoá tính năng tự động thực thi các tệp tin trên các thiết bị lưu trữ.

d. Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại, vi-rút trên máy chủ, máy trạm, thiết bị công nghệ thông tin như: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống vi-rút, mất dữ liệu, tăng dung lượng ổ đĩa cứng bất thường, mất điều khiển và những dấu hiệu bất thường khác,... người sử dụng nhanh chóng rút cáp mạng ra khỏi máy tính hoặc tắt máy tính (có thể ngắt nguồn điện máy tính trong trường hợp này) và thông báo đến bộ phận hoặc người quản lý trực tiếp hệ thống thông tin mạng của cơ quan, đơn vị để xử lý.

e. Phòng ngừa hư hỏng, sự cố máy tính, hệ thống thông tin qua các sự cố bất khả kháng như: Hư hỏng thiết bị đột ngột, chập điện, cháy nổ, sét đánh, trộm cắp, khủng bố, hỏa hoạn, lũ lụt...

Điều 8. Giám sát an toàn hệ thống thông tin mạng

1. Đối với cơ quan đơn vị: Tổ chức thực hiện giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trực tiếp quản lý. Nội dung và đối tượng giám sát thực hiện theo quy định tại các Khoản 1, 2 Điều 24 của Luật An toàn thông tin mạng; thực hiện việc lưu trữ nhật ký tình trạng hoạt động của hệ thống thông tin tại máy chủ ít nhất là 30 ngày để phục vụ công tác đảm bảo an toàn thông tin.

2. Đối với các doanh nghiệp cung cấp các dịch vụ viễn thông, công nghệ thông tin, internet: Có trách nhiệm thực hiện theo các quy định tại Khoản 3 Điều 24 của Luật An toàn thông tin mạng.

Điều 9. Ngăn chặn xung đột thông tin trên mạng

1. Cá nhân, tổ chức có trách nhiệm ngăn chặn các thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của các tổ chức, cá nhân trong và ngoài nước.

2. Cá nhân, tổ chức có trách nhiệm ngăn chặn các hành vi của tổ chức, cá nhân trong và ngoài nước với mục đích phá hoại tính nguyên vẹn của hệ thống mạng.

3. Cá nhân, tổ chức chủ động và có trách nhiệm thực hiện việc loại trừ các hoạt động trái pháp luật trên không gian mạng có ảnh hưởng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong và ngoài nước.

4. Cá nhân, tổ chức thực hiện quy định tại Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng.

5. Các cơ quan, đơn vị chức năng trên địa bàn huyện có trách nhiệm thực hiện nghiêm các quy định trong Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng.

Điều 10. Xây dựng quy chế đảm bảo an toàn thông tin nội bộ

Trên cơ sở Quy chế này và các hướng dẫn của bộ, ngành, UBND tỉnh và các sở, ban, ngành cấp tỉnh, các cơ quan, đơn vị, địa phương ban hành quy chế đảm bảo an toàn thông tin trong nội bộ tại cơ quan, đơn vị, địa phương mình, quy định rõ các vấn đề cơ bản sau:

1. Phân công cụ thể công chức viên chức chuyên trách hoặc phụ trách công nghệ thông tin, số điện thoại liên hệ khi có sự cố về an toàn thông tin.

2. Phân công công chức viên chức chịu trách nhiệm quản lý máy tính để dự thảo các văn bản, tài liệu có tính mật; việc sử dụng và vận hành máy tính này phải đảm bảo tuân thủ các quy định của pháp luật về bảo mật và an toàn thông tin.

3. Thiết lập quy tắc vào ra; quản lý phòng máy chủ; quy tắc cài đặt phần mềm lên máy chủ, máy trạm của người dùng.

4. Quy tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, thiết bị CNTT,…).

5. Kiểm tra, rà soát và khắc phục sự cố an toàn của hệ thống thông tin, áp dụng hiệu quả các các quy định trong Điều 6 của Quy chế này.

6. Quy tắc quản lý bảo đảm an toàn hệ thống thông tin tại đơn vị; đảm bảo tính toàn vẹn, tính tin cậy, tính thống nhất và tính sẵn sàng của dữ liệu trong quản lý và vận hành, trao đổi thông tin.

7. Xây dựng quy trình xử lý các sự cố ảnh hưởng đến an toàn hệ thống tại đơn vị.

8. Thực hiện đầy đủ các chế độ báo cáo tổng hợp tình hình an toàn của hệ thống thông tin.

Điều 11. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm an toàn thông tin trên địa bàn huyện

1. Quy trình xử lý khẩn cấp:

Khi phát hiện hệ thống có nguy cơ mất an toàn thông tin như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng (trang) thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan,… thực hiện các bước cơ bản:

a. Bước 1: Ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị, khẩn trương thông báo về các cơ quan chức năng (Phòng Văn hóa và Thông tin, Sở Thông tin và Truyền thông).

b. Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

c. Bước 3: Khẩn trương khắc phục hệ thống; sử dụng hệ thống dự phòng hoặc chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động (nếu có);

d. Bước 4: Tổng hợp, báo cáo sự cố và nội dung khắc phục gửi về các cơ quan chức năng liên quan (Phòng Văn hóa và Thông tin, Sở Thông tin và Truyền thông).

2. Nguyên tắc phối hợp trong ứng cứu sự cố:

a. Thực hiện các bước khắc phục sự cố theo Khoản 1 điều này.

b. Các sự cố vượt quá khả năng xử lý, đơn vị thông báo đến cơ quan chức năng (Phòng Văn hóa và Thông tin – số điện thoại 0251.3521139, phòng Công nghệ thông tin Viễn thông - Sở Thông tin và Truyền thông qua số 0251.8825678) để được hỗ trợ.

c. Tổng hợp, báo cáo Đơn vị chuyên trách CNTT (Phòng Văn hóa và Thông tin, Sở Thông tin và Truyền thông) theo định kỳ 06 tháng một lần và báo cáo đột xuất khi có yêu cầu.

Điều 12. Mua sắm, trang bị máy tính, thiết bị công nghệ thông tin có liên quan đến an toàn thông tin mạng

1. Trong quá trình mua sắm trang thiết bị cho hệ thống, các cơ quan, đơn vị cần tuân thủ quy định tại Thông tư số 47/2016/TT-BTTTT ngày 26/12/2016 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết về ưu tiên đầu tư mua sắm sản phẩm, dịch vụ công nghệ thông tin sản xuất trong nước sử dụng nguồn vốn ngân sách nhà nước.

2. Việc đầu tư mua sắm các thiết bị, máy tính với mục đích soạn thảo, lưu trữ văn bản mật phải được kiểm định của Công an tỉnh trước khi đưa vào sử dụng.

Điều 13. Tiếp nhận thông tin báo cáo sự cố mất an toàn thông tin mạng, sự cố mạng truyền số liệu chuyên dùng

Địa chỉ tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin mạng; Sự cố tắc, nghẽn, đứt, rớt, không truy cập được của mạng truyền số liệu chuyên dùng, cơ quan, đơn vị thông báo ngay đến Phòng Văn hóa và Thông tin là bộ phận làm đầu mối liên lạc ứng cứu an toàn thông tin máy tính trên địa bàn huyện qua số **(0251)3521139**, trường hợp khẩn cấp liên hệ trực tiếp về Phòng Công nghệ thông tin Viễn thông – Sở Thông tin và Truyền thông qua các thông tin liên hệ sau: Điện thoại: **(0251).3810269, Fax: (0251).3827071, Email: attt@dongnai.gov.vn**.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 14. Tổ chức, cá nhân bên ngoài khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan Nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng công nghệ thông tin trên địa bàn huyện, chịu sự thanh tra, kiểm tra của các cơ quan Nhà nước có thẩm quyền về lĩnh vực an toàn thông tin (Tổ kiểm tra huyện hoặc Đoàn thanh tra của tỉnh).

Điều 15. Cán bộ, công chức, viên chức trong cơ quan nhà nước

Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin.

1. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay đến công chức viên chức chuyên trách CNTT của đơn vị và cơ quan chuyên trách CNTT của huyện (Phòng Văn hóa và Thông tin).

2. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và an toàn thông tin.

3. Công chức viên chức chuyên trách CNTT:

a. Triển khai hoặc tham mưu để triển khai thực hiện các nội dung tại khoản 1 Điều 6 và Điều 10 Quy chế này;

b. Theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin tại cơ quan, đơn vị;

c. Hướng dẫn, hỗ trợ người dùng tại cơ quan, đơn vị giải pháp phòng, chống vi rút máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro;

d. Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an toàn thông tin; tham gia khắc phục các sự cố mất an toàn thông tin.

Điều 16. Các cơ quan nhà nước trên địa bàn huyện

1. Cơ quan nhà nước nếu có sự cố về an toàn thông tin, thực hiện theo nội dung quy định tại Khoản 1 Điều 42 Nghị định số 64/2007/NĐ-CP.

2. Báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu của Ủy ban nhân dân huyện (qua phòng Văn hóa và Thông tin).

3. Tuân thủ và bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin, đảm bảo an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo quy định của quy chế này và các quy định khác của pháp luật có liên quan.

4. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm, quyền hạn của từng cơ quan, đơn vị.

5. Xác định và trình cấp có thẩm quyền phê duyệt cấp độ hệ thống thông tin của cơ quan, đơn vị (nếu có).

6. Khi được kiểm tra công tác đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị có trách nhiệm cử cán bộ, công chức, viên chức có chuyên môn về công nghệ thông tin tham gia đoàn kiểm tra; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo an toàn thông tin.

Điều 17. Phòng Văn hóa và Thông tin

1. Tham mưu Ủy ban nhân dân huyện về công tác đảm bảo an toàn thông tin trên địa bàn huyện và chịu trách nhiệm trong việc đảm bảo an toàn thông tin cho hệ thống thông tin, máy chủ của huyện.

2. Tham mưu Ủy ban nhân dân huyện thiết lập kênh thông tin để tiếp nhận kiến nghị, phản ánh của tổ chức, cá nhân liên quan đến bảo đảm an toàn thông tin cá nhân trên mạng.

3. Phối hợp phòng Nội vụ xây dựng và triển khai các kế hoạch, chương trình đào tạo về an toàn thông tin trong ứng dụng CNTT cho cán bộ, công chức, viên chức trên địa bàn huyện.

4. Tùy theo mức độ sự cố, phối hợp Sở Thông tin và Truyền thông, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn huyện; Thực hiện các cảnh báo các vấn đề về an toàn thông tin trong các cơ quan nhà nước trên địa bàn huyện.

5. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan nhà nước trên địa bàn huyện; Phối hợp các đơn vị liên quan xử lý các vấn đề liên quan sự cố mạng truyền số liệu chuyên dùng.

6. Hướng dẫn, giám sát các đơn vị xây dựng quy chế và thực hiện việc đảm bảo an toàn cho hệ thống thông tin theo quy định.

7. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền đến các phương tiện truyền thông đại chúng trên địa bàn huyện về công tác bảo đảm an toàn thông tin.

8. Phối hợp với Công an huyện đề xuất Công an tỉnh thẩm định, bảo hành-bảo trì đảm bảo an toàn thông tin của thiết bị CNTT phục vụ soạn thảo và lưu trữ văn bản, tài liệu mật của các cơ quan nhà nước.

9. Hỗ trợ, hướng dẫn các địa phương mô hình kết nối mạng nội bộ (LAN) đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT.

10. Tham mưu UBND huyện thành lập Tổ kiểm tra, kiểm tra công tác an toàn thông tin đối với tổ chức, cá nhân trong công tác đảm bảo an toàn thông tin; tổ chức thanh tra, kiểm tra đột xuất trong trường hợp cần thiết.

Điều 18. Văn phòng HĐND và UBND huyện

1. Phối hợp chặt chẽ với phòng Văn hóa và Thông tin, các cơ quan liên quan trong việc rà soát, đầu tư trang thiết bị phục vụ công tác đảm bảo an toàn thông tin cho hệ thống máy chủ huyện.

2. Cử nhân sự tham gia, phối hợp đoàn thanh, kiểm tra công tác đảm bảo an toàn thông tin, thẩm định, kiểm định thiết bị CNTT dùng soạn thảo và lưu trữ văn bản, tài liệu mật của các cơ quan nhà nước trên địa bàn huyện.

3. Cử nhân sự phối hợp chặt chẽ với phòng Văn hóa và thông tin trong việc rà soát, khắc phục các sự cố kỹ thuật, các nguy cơ mất an toàn thông tin trên hệ thống thông tin, máy chủ của huyện.

Điều 19. Công an huyện

1. Chủ trì, phối hợp với phòng Văn hóa và Thông tin, các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống mạng internet, các mạng xã hội đăng tải thông tin gây phương hại đến an ninh mạng trong cơ quan nhà nước và an ninh trật tự trên địa bàn huyện.

2. Chủ trì, phối hợp với phòng Văn hóa và Thông tin, các cơ quan, đơn vị có liên quan tổ chức Đoàn kiểm tra về an ninh mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo quy định của pháp luật.

3. Chủ trì, phối hợp các cơ quan chuyên môn huyện kiến nghị Công an tỉnh hỗ trợ kiểm định thiết bị CNTT dùng soạn thảo và lưu trữ văn bản, tài liệu mật của các cơ quan nhà nước trên địa bàn huyện; định kỳ thành lập đoàn kiểm tra thiết bị CNTT soạn thảo, lưu trữ văn bản, tài liệu mật tại các cơ quan nhà nước trên địa bàn huyện.

4. Cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị; Điều tra và xử lý các trường hợp vi phạm các quy định về an toàn thông tin mạng theo thẩm quyền.

5. Kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn thông tin và an ninh mạng theo đúng quy định của pháp luật.

CHỦ TỊCH