SỞ Y TẾ VĨNH PHÚC
TTYT HUYỆN YÊN LẠC

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

QUY ĐỊNH
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại Trung tâm

(Kèm theo Quyết định số 128/QĐ-TTYT ngày 13 tháng 02 năm 2018 của Giám đốc TTYT huyện Yên Lạc)

I./ NHỮNG QUY ĐỊNH CHUNG

1. Phạm vi áp dụng

Quy định này quy định về nội dung, biện pháp đảm bảo an toàn, an ninh thông tin (viết tắt là AT-ANTT) trong lĩnh vực ứng dụng công nghệ thông tin (viết tắt là CNTT) phục vụ cho công tác điều hành và quản lý hệ thống mạng tại Trung tâm y tế huyện Yên Lạc.

2. Đối tượng áp dụng

Quy định này áp dụng đối với cán bộ, viên chức sử dụng máy vi tính trong các khoa, phòng tại Trung tâm y tế huyện Yên Lạc

3. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

- *An toàn thông tin:* Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin tại Trung tâm nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.
- ***Website:*** Là một **tập hợp các trang web** bao gồm văn bản, hình ảnh, video vv… Trang web được lưu trữ trên máy chủ có thể truy cập thông qua Internet.
- *An ninh thông tin:* Là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.
- *Hệ thống mạng LAN:* Là hệ thống mạng nội bộ dùng để kết nối các máy tính trong một phạm vi nhỏ *(phòng làm việc, khoa,…).* Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.
- *Địa chỉ IP:* Là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.
- *Bên thứ ba:* Là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ công nghệ thông tin.
- *Thiết bị lưu trữ ngoài:* Là các ổ cứng di động, USB, đĩa CD, DVD,..
- *Tài sản công nghệ thông tin:*Là các trang thiết bị, thông tin dịch vụ thuộc hệ thống công nghệ thông tin của đơn vị, bao gồm:

+*Tài sản vật lý:* Là các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thông thông tin

+ *Tài sản thông tin:* Là các dữ liệu, tài liệu liên quan đến hệ thống công nghệ thông tin. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dự liệu điện tử .

+ *Tài sản phần mềm:* Bao gồm các chương trình ứng dụng, phần mềm hệ thống cơ sở dữ liệu và công cụ hỗ trợ..

+ *Dịch vụ:* Là các dịch vụ công nghệ thông tin thuê bên thứ ba cung cấp

II./ QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

1. Bộ phận phụ trách đảm bảo an toàn, an ninh thông tin

Tổ Truyền thông-Công nghệ thông tin là bộ phận được Giám đốc giao nhiệm vụ trực tiếp chủ trì, phối hợp với các khoa phòng liên quan tham mưu cho Giám đốc Trung tâm về công tác quản lý và đảm bảo AT-ANTT trong ứng dụng CNTT trong Trung tâm.

2. Quản lý tài khoản người dùng

2.1. Tổ Truyền thông-Công nghệ thông tin có trách nhiệm tham mưu cho Giám đốc, tạo lập và cung cấp tài khoản truy nhập, tài khoản người dùng cho phòng khám và các khoa, phòng; tạo mới hoặc hủy bỏ tài khoản của phòng khám hay các khoa phòng khi có yêu cầu của Giám đốc.

2.2. Mỗi cá nhân, khoa, phòng phải có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của cá nhân, khoa, phòng và của cơ quan như: Hòm thư điện tử, phần mềm Quản lý…; không tự ý xâm nhập các tài khoản của người khác để sử dụng; không cung cấp thông tin tài khoản của cá nhân, khoa, phòng cho các tổ chức, cá nhân không có liên quan.

Mật khẩu phải thay đổi thường xuyên hoặc định kỳ mỗi tháng 01 lần; không dùng một mật khẩu trong nhiều tài khoản.

3. Quy định đăng bài lên Website Trung tâm.

- Nội dung bài viết, hình ảnh về các hoạt động của của Trung tâm cần phải được duyệt của Ban giám đốc Trung tâm, sau đó tổ TT-CNTT mới được đăng bài lên Website của Trung tâm.

- Tổ Truyền thông-Công nghệ thông tin có trách nhiệm đăng tải nội dung đăng trên Website.

4. Quy định về quản lý và kiểm soát truy cập vật lý

4.1. Đối với thiết bị CNTT

a) Mỗi cá nhân, khoa phòng có trách nhiệm quản lý trang thiết bị CNTT (máy vi tính, máy in, thiết bị ngoại vi,…) được giao sử dụng, tự quản lý dữ liệu trên máy tính của cá nhân, tự quyết định việc chia sẻ tài nguyên với các máy tính khác trong mạng lan theo đúng quy định.

b) Tổ Truyền thông-Công nghệ thông tin chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu thường xuyên; các thiết bị CNTT phải thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật.

c) Máy vi tính chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus có bản quyền; có cơ chế bảo vệ thư mục và tập tin khi chia sẻ tài nguyên dùng chung.

d) Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng của các tác nhân bên ngoài như nắng, mưa…; không để các tài liệu, vật liệu dễ cháy gần máy tính và các thiết

bị CNTT để tránh xảy ra cháy nổ; thường xuyên vệ sinh cho máy vi tính; kiểm tra theo dõi sự hoạt động của máy vi tính và các thiết bị... Khi không sử dụng nên tắt máy vi tính và các thiết bị nhằm tiết kiệm điện và phòng, chống các xâm nhập trái phép.

e) Trong quá trình sử dụng các thiết bị CNTT, khi có sự cố xảy ra đối với các thiết bị CNTT , người sử dụng thiết bị CNTT thông báo với Tổ Truyền thông-Công nghệ thông tin; nếu sự cố nhỏ, không phải thay thế hoặc sửa chữa linh kiện thì cán bộ được giao phụ trách CNTT xử lý trực tiếp. Nếu có sự cố lớn, cần phải thay thế linh kiện để sửa chữa thì cá nhân khoa, phòng trực tiếp quản lý và sử dung thiết bị CNTT phải lập dự trù, có xác nhận của lãnh đạo khoa, phòng, cán bộ trực tiếp kiểm tra tình trạng máy gửi về Tổ Truyền thông-Công nghệ thông tin để được hướng dẫn sửa chữa, thay thế, tuyệt đối không được chuyển cho các tập thể, cá nhân khi chưa được sự thống nhất và đồng ý của BGĐ.

4.2. Hệ thống mạng LAN

a) CBVC của Trung tâm khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng, nếu tự ý thay đổi tham số mạng thì người thay đổi phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số mạng, phải báo cán bộ phụ trách CNTT của Trung tâm biết để xử lý.

b) Tổ Truyền thông-Công nghệ thông tin chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng, máy in và các thiết bị khác theo đúng tiêu chuẩn kỹ thuật; thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm tối đa các sự cố kỹ thuật; kết nối mạng Internet cho các khoa phòng khi có yêu cầu của cấp trên.

c) Tổ Truyền thông-Công nghệ thông tin chịu trách nhiệm hướng dẫn, cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; thường xuyên kiểm tra, quét virus cho tất cả các máy tính, xử lý khắc phục kịp thời khi xảy ra sự cố, đảm bảo hệ thống mạng máy tính hoạt động ổn định, liên tục.

d) Hàng tháng/quý Tổ Truyền thông-Công nghệ thông tin phải đề xuất kế hoạch mua sắm các thiết bị CNTT để thay thế sửa chữa kịp thời đảm bảo an toàn cho các máy tính và mạng máy tính luôn trong tạng thái hoạt động ổn định nhất .

5. Cơ chế sao lưu dữ liệu

5.1. Phân loại dữ liệu sao lưu

a) Dữ liệu hệ thống bao gồm các loại thông tin, dữ liệu cài đặt như: Cấp phát tài khoản và địa chỉ IP mạng, đưa thông tin lên Website của Trung tâm,...

b) Dữ liệu các ứng dụng dùng chung được cài đặt trên máy chủ dữ liệu tỉnh đảm bảo AT-ANTT như: phần mềm quản lý tổng thể Trung tâm Medissoft, phần mềm kế toám Misa, Website Trung tâm...

c) Các dữ liệu khác cài đặt trên máy tính cá nhân do các CBVC thuộc các khoa, phòng soạn thảo, tạo lập trên các máy tính trong mạng nội bộ.

5.2. Quy định thiết bị sao lưu

a) Đối với dữ liệu hệ thống: Sử dụng chức năng sao lưu dự phòng của các ứng dụng.

b) Đối với các dữ liệu khác: Các dữ liệu cần lưu trữ, của các khoa, phòng tự sao chép vào các thiết bị lưu trữ để đảm bảo dữ liệu ít nhất lưu trữ ở hai nơi đề phòng ổ đĩa cứng của máy tính bị hỏng.

5.3. Định kỳ sao lưu

Tùy vào mức độ qui định thời hạn mỗi loại thông tin, dữ liệu cần sao lưu.

a) Đối với dữ liệu hệ thống (Dữ liệu máy chủ): Sao lưu hàng ngày vào thời điểm cuối ngày làm việc.

b) Đối với các dữ liệu khác: Sao lưu khi có thay đổi thông tin.

6. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

6.1. Đối với CBVC

a) Thông báo kịp thời cho cán bộ Tổ Truyền thông-Công nghệ thông tin của Trung tâm khi phát hiện các sự cố gây mất AT-ANTT trong hệ thống mạng.

b) Xử lý khẩn cấp: Khi phát hiện hệ thống gặp sự cố, thông qua các dấu hiệu khác thường như: Hệ thống máy tính hoạt động chậm khác thường, nội dung bị thay đổi,… cần báo ngay cho cán bộ Tổ Truyền thông-Công nghệ thông tin Trung tâm để có hướng xử lý kịp thời

6.2. Đối với Tổ Truyền thông-Công nghệ thông tin.

a) Quản lý việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi...) .

b) Hướng dẫn người dùng nắm được những nguyên tắc hoạt động cơ bản nhất của máy vi tính và một số giải pháp khắc phục sự cố đơn giản mà hệ thống CNTT hay gặp phải; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời thông tin ngay với cán bộ phòng CNTT đồng thời phối hợp với các đơn vị có liên quan để cùng phối hợp khắc phục.

d) Thường xuyên theo dõi, tổng hợp, nắm tình hình, tham mưu các văn bản chỉ đạo về AT-ANTT.

e)Tham mưu cho BGĐ các phương án nâng cấp và xử lý đảm bảo hệ thống CNTT luôn hoạt động trong trạng thái ổn định và an toàn. Căn cứ Bộ tiêu chí ứng dụng công nghệ thông tin, hướng dẫn xác định mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh.

7. **Các quy định về an toàn thông tin**

7.1. Đối với người sử dụng

a) Những điều phải thực hiện

1. Tắt máy tính trước khi về.
2. Quét virus ổ cứng di động, thẻ nhớ ngay sau khi gắn vào máy tính.
3. Quét virus trước khi gửi và nhận tài liệu qua email.
4. Xóa dữ liệu trên ổ cứng di động, thẻ nhớ trước khi cho người khác dùng.
5. Đặt mật khẩu truy cập vào máy vi tính. Mật khẩu phải nhiều hơn 8 ký tự và bao gồm số, chữ cái và các ký tự đặc biệt.
6. Thay đổi mật khẩu đăng nhập mỗi 03 tháng/ lần.
7. Phải thiết lập chế độ tự động bảo vệ màn hình máy vi tính khi không sử dụng trong thời gian từ 15 phút trở lên.

b) Những điều không được làm

1. Không lưu trữ các tài liệu quan trọng lên ổ cứng di động, thẻ nhớ.
2. Không chia sẽ mật khẩu của cá nhân cho người khác, không đăng nhập mật khẩu khi có người bên cạnh.
3. Không lưu mật khẩu trên máy vi tính, điện thoại, sổ tay cá nhân…
4. Không sử dụng chế độ tự động đăng nhập thư điện tử, phần mềm.
5. Không truy cập các trang web và các tập tin không rõ nguồn gốc hoặc có nội dung xấu.

6. Không được lưu trữ, tải xuống hoặc phát tán các chương trình, mã độc hại, thông tin xấu.

7. Không cài đặt và sử dụng các phần mềm ngoài danh sách phần mềm do cơ quan quy định.

7.2. Đối với bộ phận quản trị mạng (IT)

a) Trách nhiệm chung

- Tuân thủ đầy đủ các quy định về: "Các quy định về an toàn thông tin đối với người sử dụng" ;

- Sửa chữa hệ thống phần cứng, thiết bị thông tin trong mạng nội bộ của cơ quan theo yêu cầu;

- Thực hiện chính sách hạn chế quyền cài đặt phần mềm tại các máy trạm;

- Hỗ trợ hướng dẫn sử dụng các ứng dụng phần mềm tại Trung tâm và phối hợp với các đơn vị phát triển phần mềm chỉnh sửa, nâng cấp trong trường hợp phát sinh yêu cầu hoặc lỗi;

- Xây dựng, thực hiện và giám sát chính sách ATTT tại Trung tâm.

- Thực hiện các nhiệm vụ liên quan đến hệ thống công nghệ thông tin của cơ quan do Lãnh đạo Trung tâm chỉ đạo thực hiện;

- Cung cấp số điện thoại riêng về danh sách các thành viên bộ phận quản trị IT (mail, di động, điện thoại bàn) để nhận phản hồi từ cán bộ viên chức về các tình huống ảnh hưởng đến ATTT hoặc các sự cố về thông tin;

b) Tác nghiệp hàng ngày

- Phải ghi lại nhật ký hoạt động (NKHĐ) về phòng máy chủ: kiểm soát việc ra vào của nhân viên tại phòng máy, hiện tượng sai lệch và bất bình thường của hệ thống vận hành, thời gian xảy ra lỗi, cảnh báo hiện tượng nguy cấp, xác định máy trạm hay phân vùng mạng có khả năng là nguyên nhân, lỗi trong quá trình hoạt động của các thiết bị và trong quá trình bảo trì...;

- Ghi nhận nhật ký các hoạt động sửa chữa, hỗ trợ thực hiện trực tiếp tại các phòng/ khoa về hệ thống mạng, máy chủ, các hệ thống phần mềm ứng dụng của Trung tâm.

- Kiểm tra hệ thống điện, nhiệt độ phòng máy, toàn bộ máy chủ, các thiết bị mạng, các hệ thống bảo mật (router, switch, firewall, hệ thống phòng chống phần mềm độc hại,..), giao diện Cổng thông tin, phần mềm ứng dụng của Trung tâm tối thiểu 01 lần/ ngày để phát hiện kịp thời những thay đổi, bất thường;

- Kiểm tra, giám sát an toàn an ninh thông tin thông qua các camera quan sát trong Trung tâm;

c) Tác nghiệp hàng tuần

- Kiểm tra và cập nhật các bản và lỗi, bản cập nhật cho các hệ thống bảo mật (thiết bị phần cứng, phần mềm, Firewall, Antirus,…);

- Kiểm tra các điều kiện phòng cháy chữa cháy, điều kiện nhiệt độ hoạt động và nguồn điện cho phòng máy chủ;

- Theo dõi nhật ký hệ thống, trang web, phần mềm ứng dụng và các hệ thống thông tin (logfile) trong cơ quan 02 lần/ tuần để phát hiện kịp thời những trường hợp bất thường;

- Sao lưu dự phòng dữ liệu trên các máy chủ, sao lưu dữ liệu trên các hệ thống thông tin (quản lý hồ sơ công việc, Website, cấp phép, ..);

d) Tác nghiệp hàng tháng

- Tổng hợp báo cáo về việc tuân thủ quy định an toàn an ninh thông tin của toàn bộ cán bộ, nhân viên và những sự cố về ATTT trong cơ quan đồng thời đề xuất những biện pháp giải quyết thích hợp trình Lãnh đạo phụ trách;

- Giám sát và cập nhật phân quyền truy cập hệ thống thông tin trong Trung tâm và đưa ra những quy định chi tiết để hướng dẫn người sử dụng;

- Cập nhật danh sách các phần mềm, hệ điều hành khác mà các CBCNV trong cơ quan có thể cài đặt, chạy thử nghiệm các ứng dụng;

- Cập nhật danh sách các phần mềm bị cấm không được sử dụng đối với các nhân viên;

- Xây dựng chính sách sao lưu dữ liệu dung chung, cá nhân được lưu trên máy chủ FILE, dữ liệu của camera (nếu có), dữ liệu của các phần mềm ứng dụng, Cổng thông tin… định kỳ hàng tháng để bảo vệ là những dữ liệu chuyên môn, quan trọng phục vụ công tác của cơ quan, đơn vị. Các thiết bị lưu trữ thông tin này phải được bảo quản ở nơi an toàn và bảo mật.

e) Tác nghiệp hàng quý/ hàng năm

- Phối hợp các khoa/phòng trực thuộc Trung tâm thực hiện việc xây dựng, triển khai và cập nhật quy định ATTT trong Trung tâm. Làm báo cáo tổng hợp trong cuộc họp hàng quý với lãnh đạo đơn vị.

- Xây dựng các quy trình cụ thể để triển khai quy định ATTT đến tòan bộ CBCNV trong Trung tâm;

- Bộ phận quản trị IT có trách nhiệm tham mưu đề xuất việc đào tạo, nâng cao kiến thức về ATTT cho nhân viên Trung tâm;

- Phối hợp cùng đơn vị tư vấn độc lập, có uy tín về bảo mật, an toàn thông tin để thực hiện kiểm thử, đánh giá rủi ro đối với hệ thống thông tin trong cơ quan (ít nhất 01 lần/ năm hoặc khi có các thay đổi lớn) để nâng cấp thiết bị, phần mềm hoặc sửa đổi chính sách nhằm mục đích hoàn thiện hệ thống hơn.

g) Trường hợp đột xuất

- Bộ phận quản trị IT phải xây dựng Quy trình xử lý các tình huống đột xuất đối với hệ thống thông tin và Quy trình phối hợp ứng cứu đảm bảo vận hành hệ thống mạng, phần mềm của Trung tâm;

- Tuân thủ các quy định trong quy trình xử lý sự cố đột xuất;

- Trực tiếp xử lý những sự cố đột xuất về kỹ thuật theo khả năng và phạm vi được giao khi nhận được thông báo về sự cố;

- Bộ phận quản trị IT phải ghi nhận lại các mẫu tấn công, phạm vi bị ảnh hưởng, chi phí khắc phục...để rút kinh nghiệm cho những lần sau;

- Đối với các tình huống nằm ngoài thẩm quyền, bộ phận IT phải xin ý kiến chỉ đạo Lãnh đạo đơn vị về cách thức xử lý tiếp theo;

- Thực hiện công tác ứng cứu, xử lý sự cố về thông tin, sự cố máy tính trong Trung tâm theo yêu cầu của lãnh đạo khoa/phòng.

h) Bên thứ ba tham gia vào hệ thống thông tin trong Trung tâm

- Bộ phận quản trị IT phải xác định loại tài nguyên trong hệ thống thông tin (cơ sở dữ liệu, thông tin, thiết bị...) mà cộng tác viên có thể truy cập trách nhiệm của cộng tác viên khi xảy ra các sự cố về hệ thống thông tin của Trung tâm;

- Bộ phận quản trị IT phải giám sát, ghi lại toàn bộ các tác động của Bên thứ 3 vào hệ thống máy tính của Trung tâm.