UBND TỈNH THỪA THIÊN HUẾ
SỞ Y TẾ

Số: 321 /QĐ-SYT

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

Thừa Thiên Huế, ngày 25 tháng 4 năm 2024

QUYẾT ĐỊNH
Ban hành Quy chế quản lý và sử dụng mạng máy tính nội bộ của Sở Y tế

GIÁM ĐỐC SỞ Y TẾ

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 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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

Căn cứ Thông tư số 12/2019/TT-BTTTT ngày 05/11/2019 của Bộ trưởng Bộ Thông tin và Truyền thông về việc sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 Quy định về quản lý, vận hành, kết nối, sử dụng và đảm bảo an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Quyết định 4159/QĐ-BYT ngày 13/10/2014 của Bộ Y tế về việc ban hành Quy định về đảm bảo an toàn thông tin Y tế điện tử tại các đơn vị trong ngành Y tế;

Căn cứ Quyết định số 4495/QĐ-BYT ngày 30/10/2015 của Bộ Y tế về việc ban hành Hướng dẫn xây dựng nội quy an toàn, an ninh thông tin trong các đơn vị trong ngành y tế;

Căn cứ Quyết định số 34/2022/QĐ-UBND ngày 03/8/2022 của Uỷ ban nhân dân tỉnh Thừa Thiên Huế về việc ban hành Quy định quản lý, vận hành và khai thác mạng tin học diện rộng tỉnh Thừa Thiên Huế;

Căn cứ Quyết định số 26/2022/QĐ-UBND ngày 02/6/2022 của Uỷ ban nhân dân tỉnh Thừa Thiên Huế về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Y tế tỉnh Thừa Thiên Huế;

Xét theo đề nghị của Phó Chánh Văn phòng phụ trách Sở Y tế.

QUYẾT ĐỊNH:

Điều 1. Ban hành "Quy chế quản lý và sử dụng mạng máy tính nội bộ của Sở Y tế" *(có Quy chế đính kèm)*.

Điều 2. Các ông, bà: Phó Chánh Văn phòng phụ trách Sở Y tế, Trưởng các phòng chuyên môn của Sở Y tế, Giám đốc/Thủ trưởng các đơn vị trong ngành Y tế và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 2;
- Sở TT&TT;
- Công an tỉnh;
- Giám đốc Sở Y tế (báo cáo);
- Các PGĐ Sở Y tế (báo cáo);
- Lưu: VT, VP.

GIÁM ĐỐC

SỞ Y TẾ

Trần Kiêm Hảo

QUY CHẾ QUẢN LÝ VÀ SỬ DỤNG MẠNG MÁY TÍNH NỘI BỘ

(Ban hành kèm theo Quyết định số 321 /QĐ - SYT ngày 25 /4/2024)

CHƯƠNG I

NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

1. Quy chế quản lý và sử dụng mạng máy tính nội bộ của Sở Y tế (*gọi tắt là mạng nội bộ*).

2. Quy chế áp dụng đối với công chức, viên chức & người lao động công tác tại các Phòng của Sở, các đơn vị trực thuộc Sở trong việc quản lý, sử dụng hệ thống mạng nội bộ (LAN), mạng Internet và kết nối mạng WAN của UBND tỉnh.

Điều 2. Thống nhất sử dụng các thuật ngữ

1. Thiết bị công nghệ thông tin: là toàn bộ các máy móc, thiết bị có liên quan đến CNTT như: máy vi tính (PC, Laptop, Sever), máy in, máy quét, máy chiếu, các loại ổ ghi đĩa CD và DVD, ổ cứng, thẻ nhớ (USB), camera số, máy ảnh số, thiết bị chuyển mạch (hub, switch), tường lửa (firewall), modem, hệ thống cáp mạng.

2. Tài nguyên mạng: là toàn bộ các phần mềm dùng chung chạy trên mạng nội bộ của Sở, gồm: Trang thông tin điện tử, các phần mềm dùng chung của UBND tỉnh và Bộ Y tế, email công vụ, các phần mềm được cài đặt trên hệ thống máy tính, các phần mềm chuyên môn, chuyên ngành,...

3. Người sử dụng: cán bộ công chức, viên chức Sở Y tế, sử dụng các thiết bị công nghệ thông tin (CNTT); được cấp tài khoản (Account) gồm tên người sử dụng (Username) và mật khẩu (Password) để khai thác mạng LAN và các tài nguyên mạng nội bộ của Sở thông qua mạng LAN, mạng internet và kết nối mạng WAN của UBND tỉnh.

4. Quản trị cơ quan: là công chức, viên chức được giao nhiệm vụ quản lý hệ thống thiết bị CNTT, duy trì sự hoạt động mạng máy tính nội bộ tại Văn phòng Sở Y tế hoặc tại các đơn vị trực thuộc; hướng dẫn người sử dụng thiết bị CNTT và khai thác tài nguyên mạng phục vụ công tác.

1. Mạng tin học diện rộng (WAN) tỉnh Thừa Thiên Huế (sau đây gọi tắt là mạng diện rộng) là mạng tin học được thiết lập bằng cách kết nối giữa Trung tâm Giám sát, điều hành đô thị thông minh Thừa Thiên Huế (HueIOC) với các mạng nội bộ (LAN) của các cơ quan, đơn vị thông qua mạng viễn thông; đồng thời kết nối với mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng và Nhà nước nhằm phục vụ công tác chỉ đạo, điều hành của lãnh đạo tỉnh; việc trao đổi thông tin phục vụ công tác chuyên môn nghiệp vụ và công tác quản lý hành chính nhà nước trên địa bàn tỉnh.

5. Hạ tầng kỹ thuật: là tập hợp thiết bị công nghệ thông tin (thiết bị định tuyến, thiết bị chuyển mạch, thiết bị lưu trữ dữ liệu, các thiết bị giám sát, bảo mật,

máy chủ, máy trạm, máy tính cá nhân), thiết bị điện (điều hòa chính xác, tủ điện, chống sét, UPS, máng cáp điện), thiết bị phòng cháy, chữa cháy, thiết bị viễn thông, thiết bị ngoại vi, mạng nội bộ, mạng diện rộng và các thiết bị kỹ thuật chuyên dùng khác.

6. Phần mềm ứng dụng triển khai trong mạng WAN: là các phần mềm ứng dụng, hệ thống thông tin, nền tảng số cung cấp dịch vụ cho các cơ quan, đơn vị và người sử dụng được UBND tỉnh thống nhất triển khai đưa vào hoạt động tại Trung tâm Giám sát, điều hành đô thị thông minh.

7. An toàn, an ninh thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin trước các nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, thiết bị mạng, tài sản và con người trong hệ thống thông tin nhằm đảm bảo cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn, an ninh 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.

CHƯƠNG II

QUẢN LÝ, SỬ DỤNG MẠNG MÁY TÍNH

Điều 3. Quản lý mạng máy tính

Quản trị mạng của Văn phòng Sở, đơn vị trực thuộc có trách nhiệm quản lý thiết bị, dữ liệu trên máy tính của đơn vị; trực tiếp theo dõi, giám sát việc sử dụng các dịch vụ mạng máy tính cơ quan; cấp quyền, phân quyền truy cập cho công chức, viên chức kết nối máy tính vào mạng máy tính của Sở hoặc các đơn vị khác, sử dụng thông tin phục vụ yêu cầu công tác theo hướng dẫn kỹ thuật của quản trị mạng.

Điều 4. Truy cập vào mạng nội bộ

1. Việc truy cập vào mạng nội bộ phải xuất phát từ yêu cầu phục vụ công tác quản lý, điều hành tác nghiệp của Sở và các đơn vị trực thuộc.

2. Việc đặt tên, đặt địa chỉ IP cho máy tính phải tuân thủ theo quy định tại khoản 4 Điều 7 của quy chế này.

3. Trường hợp có sự thay đổi vị trí làm việc của phòng, cá nhân, việc giữ nguyên hoặc thay đổi các tham số đã cài đặt trên máy tính phải thông báo đến Quản trị mạng để phối hợp và báo cáo Lãnh đạo sau khi thực hiện.

4. Việc sử dụng các ứng dụng trên mạng nội bộ được quy định tại Điều 6 của quy chế này.

5. Cá nhân truy cập từ xa vào mạng nội bộ Sở có trách nhiệm bảo mật thông tin, thông số kỹ thuật kết nối mạng. Nghiêm cấm việc cung cấp, để lộ, truyền thông tin ra bên ngoài.

6. Đối với các nút mạng và máy tính nối mạng có nhiều người sử dụng thì mỗi người sử dụng phải có tài khoản riêng bao gồm:

- Tên người sử dụng (Username).
- Mật khẩu (Password).
- Chức năng và phạm vi sử dụng được quy định cụ thể, rõ ràng để quản lý.

7. Việc truy cập vào mạng nội bộ thông qua thiết bị Wireless (Wifi) từ các thiết bị di động (Laptop, Smartphone, máy tính bảng,...) chỉ phục vụ cho các đối tượng trong nội bộ phòng, đơn vị trực thuộc Sở. Trường hợp cần phục vụ hội nghị, hội thảo phải báo Quản trị mạng cơ quan để phối hợp và đề xuất biện pháp giải quyết.

Điều 5. Truy xuất ra bên ngoài

1. Xuất phát từ nhu cầu quản lý, điều hành và tác nghiệp của Sở, quản trị mạng có trách nhiệm tổng hợp trình Lãnh đạo Sở về mục đích, lý do, phạm vi, người chịu trách nhiệm, địa điểm thực hiện và địa điểm mạng bên ngoài cần truy xuất đến.

2. Việc truy xuất ra bên ngoài cần phải đảm bảo các quy định sau:

- Không trao đổi, truyền dẫn thông tin nghiệp vụ thuộc Sở quản lý dưới bất kỳ hình thức nào ra bên ngoài khi chưa được Lãnh đạo Sở phê duyệt.
- Không trao đổi thông tin, dữ liệu lạ từ bên ngoài vào mạng nội bộ Sở nếu chưa được quản trị mạng kiểm tra độ an toàn thông tin đối với hệ thống mạng nội bộ và chưa được sự đồng ý của Lãnh đạo Sở.
- Đối với dịch vụ Internet: các đơn vị, cá nhân thuộc Sở phải tuân theo các quy định sử dụng dịch vụ Internet do các cơ quan nhà nước có thẩm quyền ban hành.

Điều 6. Sử dụng mạng máy tính, tài khoản người dùng

1. Công chức, viên chức khi truy cập mạng máy tính cơ quan sẽ được cấp tài khoản người dùng (Account), chịu trách nhiệm bảo đảm bí mật tài khoản được cấp; được quản trị mạng cơ quan phân quyền khai thác cơ sở dữ liệu , dịch vụ trên mạng theo chức năng, nhiệm vụ được phân quyền.

2. Máy tính cá nhân bắt buộc phải đặt mật khẩu của mỗi người dùng, không cung cấp mật khẩu cho người khác. Các thư mục chia sẽ file dùng chung phải đặt mật khẩu riêng để bảo đảm an toàn file dữ liệu. Máy tính phải được cài đặt phần mềm diệt virus theo đúng quy định.

3. Công chức, viên chức không sử dụng mạng máy tính cơ quan để khai thác, lưu trữ dữ liệu trò chơi, chương trình giải trí không lành mạnh, có nội dung đồi trụy.

4. Quản trị mạng cung cấp tài khoản, mật khẩu cho khách đến làm việc có nhu cầu khai thác mạng Wifi của Sở sau khi đượcLãnh đạo Sở đồng ý.

5. Sử dụng dịch vụ “Thư điện tử”

a. Hệ thống thư điện tử công vụ (email công vụ) của Sở có địa chỉ: http://mail.thuathienhue.gov.vn

b. Việc sử dụng tài khoản email công vụ phải tuân thủ theo Quyết định 1373/QĐ-UBND ngày 09/7/2009 của UBND tỉnh về việc ban hành Quy chế sử dụng Hệ thống Thư điện tử trong hoạt động của cơ quan nhà nước tỉnh Thừa Thiên Huế.

6. Cập nhật, khai thác các cơ sở dữ liệu (CSDL) dùng chung, CSDL chuyên ngành, dịch vụ hành chính công, thông tin trên mạng Internet, trang thông tin điện tử, các phần mềm dùng chung:

Các đơn vị căn cứ vào chức năng, nhiệm vụ của đơn vị, chỉ đạo chuyên viên phụ trách cập nhật, sử dụng và khai thác các CSDL dùng chung, CSDL chuyên ngành của Sở hiệu quả, đúng mục đích; tổ chức cung cấp các dịch vụ hành chính công trên môi trường mạng, sử dụng các phần mềm dùng chung theo đúng quy định.

CHƯƠNG III

QUY ĐỊNH VỀ BẢO MẬT VÀ AN TOÀN THÔNG TIN

Điều 7. Quy định về an toàn hệ thống

1. Việc bật, tắt máy tính, máy in,...phải thực theo hướng dẫn sử dụng thiết bị, hạn chế tối đa việc tắt đột ngột thiết bị.

2. Người trực tiếp sử dụng máy tính không được vận chuyển, di dời thiết bị CNTT trong đơn vị khi chưa được Lãnh đạo đơn vị đồng ý.

3. Không đặt các vật cứng đè lên hệ thống dây điện, cáp kết nối từ nút mạng đến máy tính. Người sử dụng không được tự ý cài đặt chương rình, phần mềm vào máy tính của cơ quan, nếu có nhu cầu phải báo cáo cho quản trị mạng cơ quan biết và phải được sự đồng ý của quản trị mạng mới được cài đặt.

4. Cấu hình mạng, vị trí thiết bị, quy định địa chỉ IP, tên máy trạm, máy chủ, nhóm làm việc (Workgroup), vùng làm việc (Domain) được quy định và thống nhất tại đơn vị mình quản lý do cán bộ quản trị mạng thiết lập.

5. Không tự ý thay đổi tên máy, workgroup, domain, địa chỉ IP máy tính nếu không có sự đồng ý của quản trị mạng. Trường hợp lắp đặt thêm máy tính mới hoặc máy tính bị lỗi phải cài đặt lại hệ điều hành phải liên hệ quản trị mạng để được hướng dẫn cài đặt thông số máy tính người sử dụng.

6. Các thông tin khi di chuyển từ ổ đĩa ngoài, USB, đĩa CD, VCD, DVD và các thư điện tử trước khi tải về phải kiểm tra, quét virus.

7. Không truy cập các trang web không biết rõ nguồn gốc. Nghiêm cấm mọi hành vi cài đặt hoặc phát tán virus vào hệ thống máy tính. Không được xâm nhập trái phép vào các máy trạm của các phòng, đơn vị và các máy trạm trong hệ thống của Sở, trừ trường hợp được sự thỏa thuận chia sẻ thông tin.

8. Các kết nối bất thường, không thuộc lớp IP, tên truy cập theo quy định của đơn vị khi phát hiện kết nối vào mạng sẽ bị ngắt ra ngoài.

9. Kết thúc ngày làm việc, yêu cầu người sử dụng phải thoát khỏi các chương trình phần mềm, tắt máy tính đúng quy trình. Hàng tháng máy chủ và các thiết bị phải được kiểm tra, bảo dưỡng định kỳ.

10. Quản trị mạng chịu trách nhiệm đảm bảo an toàn thông tin truyền dẫn và dữ liệu lưu trên mạng máy tính. Áp dụng các biện pháp đảm bảo an ninh, bảo mật những thông tin trên mạng máy tính.

Điều 8. Quy định về bảo mật và an toàn dữ liệu

1. Không kết nối mạng LAN, Internet, mạng WAN đối với máy tính cá nhân chuyên dùng sử dụng soạn thảo văn bản, lưu trữ tài liệu mật, tài liệu liên quan đến bí mật quốc gia theo quy định.

2. Nghiêm cấm hành vi để lộ thông tin máy chủ, máy tính cá nhân (mật khẩu, tên truy cập máy chủ, địa chỉ IP) cho các đối tượng khác. Không chia sẽ đường truyền LAN, WAN cơ quan, đơn vị ra ngoài cơ quan, đơn vị đề phòng để lộ, truyền thông tin nội bộ và xâm nhập trái phép vào máy chủ.

Cán bộ phụ trách Quản trị mạng và bộ phận Văn thư lưu trữ phải có cam kết về Bảo vệ bí mật Nhà nước theo quy định.

3. Người sử dụng phải đổi mật khẩu cá nhân ngay sau khi nhận được tên tài khoản và mật khẩu đăng nhập do quản trị mạng cung cấp, không để mật khẩu mặt định do quản trị mạng cung cấp. Khi đặt mật khẩu mới phải có tối thiểu là 8 ký tự, bao gồm: ký tự in hoa (A, B, C,...), ký tự số (1,2,3,4,5,6,7,8,9), và các ký tự đặc biệt ($, *,@,....). Nếu quên mật khẩu hoặc không đăng nhập được phải liên hệ với quản trị mạng để cấp mật khẩu mới. Tự chịu trách nhiệm việc bảo vệ dữ liệu máy tính được giao sử dụng, kể cả tài nguyên được chia sẻ. Không được xóa dữ liệu đang được chia sẻ trong hệ thống mạng.

4. Nếu công chức, viên chức nghỉ công tác hoặc chuyển công tác phải bàn giao thiết bị, tên truy cập, mật khẩu truy cập cho người thay thế. Người thay thế có trách nhiệm phối hợp với quản trị mạng để tiến hành thay đổi.

5. Không đem ổ cứng (HDD) và ổ cứng ngoài (có chứa dữ liệu) ra khỏi cơ quan, đơn vị, trừ trường hợp ổ cứng bị hỏng cần sửa chữa phải được phép của quản trị mạng. Đối với những máy có dữ liệu liên quan đến bí mật nhà nước, bí mật an ninh quốc gia, tài liệu có tính chất quan trọng, nhạy cảm tuyệt đối không được đưa ra khỏi cơ quan. Trường hợp ổ cứng của máy tính này bị hư hỏng không còn khả năng sử dụng thì cơ quan tự hủy để đảm bảo an toàn thông tin. Xóa dữ liệu liên quan đến công việc trong USB cá nhân trước khi đưa USB cho người khác sử dụng (trừ những dữ liệu được phép cung cấp, trao đổi).

6. Quản trị mạng có nhiệm vụ: Sử dụng thiết bị tường lửa (Firewall) được trang bị để thiết lập bảo mật, ngăn ngừa xâm nhập từ bên ngoài. Xử lý sự cố theo chức năng nhiệm vụ được giao, báo cáo kịp thời đến Lãnh đạo để có biện pháp khắc

phục sự cố xảy ra (nếu có). Có trách nhiệm bảo vệ hệ thống máy chủ và cơ sở dữ liệu cơ quan bằng mật khẩu quản trị, đảm bảo chức năng phục hồi tốt nhất khi hệ thống xảy ra sự cố.

7. Đối với máy vi tính có số liệu kế toán và các số liệu quan trọng, cần phải lưu trữ dữ liệu dự phòng. Công chức, viên chức có trách nhiệm tự lưu trữ dự phòng dữ liệu để đảm bảo an toàn dữ liệu khi có sự cố xảy ra và quản lý dữ liệu dự phòng đó.

Điều 9. Xử lý sự cố

Trong quá trình sử dụng và khai thác mạng nội bộ tại cơ quan, đơn vị khi có sự cố xảy ra các đơn vị, cá nhân phải kịp thời thông báo đến quản trị mạng về sự cố. Quản trị mạng tiến hành lập biên bản về sự cố, tìm hiểu nguyên nhân sự cố đồng thời báo cáo Lãnh đạo phương án xử lý. Trường hợp những lỗi sự cố không khắc phục được thì quản trị mạng báo cáo với thủ trưởng cơ quan, đơn vị và đề xuất giải pháp xử lý phù hợp.

CHƯƠNG IV

KHEN THƯỞNG, KỶ LUẬT

Điều 10. Các đơn vị, cá nhân trực thuộc Sở phải chấp hành nghiêm Quy chế này. Nếu vi phạm thì tùy theo tính chất, mức độ sẽ bị xử lý, kỷ luật theo quy định.

Điều 11. Các đơn vị, cá nhân thực hiện tốt Quy chế được xét thi đua khen thưởng hàng năm. Người phát hiện, ngăn chặn kịp thời các hành vi vi phạm sẽ được khen thưởng theo Quy chế thi đua khen thưởng của Sở.

CHƯƠNG V

ĐIỀU KHOẢN THI HÀNH

Điều 12. Quy chế này được phổ biến đến tất cả công chức, viên chức & người lao động của Sở và có hiệu lực kể từ ngày ký ban hành. Công chức, viên chức & người lao động tham gia vào hệ thống mạng nội bộ có trách nhiệm chấp hành nghiêm Quy định này. Lãnh đạo các đơn vị tham gia vào hệ thống mạng có trách nhiệm tổ chức kiểm tra việc thực hiện Quy định này và chịu trách nhiệm trước Giám đốc Sở về những vi phạm các quy định về an ninh, an toàn thông tin trong quá trình tham gia quản lý, vận hành, khai thác hệ thống mạng LAN, mạng WAN của công chức, viên chức & người lao dộng thuộc đơn vị.

Các cơ quan, tổ chức, cá nhân tham gia truy cập, khai thác, sử dụng các dịch vụ, ứng dụng có trách nhiệm chấp hành nghiêm túc Quy định này. Nếu xảy ra sai phạm tùy theo mức độ vi phạm, cán bộ vi phạm chịu kỷ luật, xử lý hành chính hoặc trách nhiệm hình sự theo quy định của pháp luật.

Điều 13. Trong quá trình thực hiện nếu cần bổ sung chính sửa, các cá nhân, đơn vị gửi kiến nghị về Văn phòng Sở Y tế để tổng hợp trình Giám đốc Sở xem xét, quyết định.

Điều 14. Phó Chánh Văn phòng phụ trách, Trưởng các Phòng của Sở, các đơn vị trực thuộc Sở, trong phạm vi chức năng, nhiệm vụ có trách nhiệm chỉ đạo, hướng dẫn, kiểm tra và đôn đốc thực hiện Quy chế này./.

GIÁM ĐỐC