SỞ Y TẾ THÀNH PHỐ ĐÀ NẴNG
TRUNG TÂM Y TẾ
QUẬN THANH KHÊ

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

Thanh khê, ngày 16 tháng 1 năm 2017

QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TẠI TRUNG TÂM Y TẾ QUẬN THANH KHÊ

Điều 1. Đảm bảo an toàn mạng và hạ tầng kỹ thuật

1. Phòng máy chủ:

a) Phòng máy chủ độc lập, phân công bộ phận chuyên trách hoặc cán bộ phụ trách CNTT trực tiếp quản lý. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ;

b) Phòng máy chủ phải đảm bảo các điều kiện cho những thiết bị đặt trong đó hoạt động ổn định, các điều kiện tối thiểu gồm: 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 có dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét;

c) Trường hợp đặc biệt không bố trí được phòng máy chủ độc lập, có thể ghép chung với các bộ phận khác nhưng phải bố trí, lắp đặt hệ thống máy chủ và thiết bị mạng dùng chung trong tủ mạng (Rack) và đảm bảo các điều kiện cho các thiết bị này hoạt động theo quy định tại Điểm b Khoản 1 Điều này.

2. Thiết lập các cơ chế bảo vệ mạng nội bộ:

a) Khi có kết nối mạng nội bộ với mạng ngoài (như: internet, mạng cơ quan khác) cần sử dụng hệ thống phòng thủ, bảo vệ mạng nội bộ (như: thiết bị tường lửa chuyên dụng, phần mềm tường lửa);

b) Hệ thống mạng không dây (Wifi) phải được thiết lập mật khẩu truy cập đủ mạnh và phân lớp mạng riêng cho các máy tính truy cập mạng không dây, định kỳ thay đổi mật khẩu, chậm nhất ba tháng phải đổi một lần;

c) Tổ chức mô hình mạng nội bộ theo hướng sử dụng máy chủ để quản lý các máy trạm trong mạng, hạn chế sử dụng mô hình mạng không có máy chủ quản lý các máy trạm. Các cơ quan, đơn vị khi có nhu cầu kết nối mạng LAN của các đơn vị, bộ phận trực thuộc ở xa, không nằm trong cùng một khu vực cần sử dụng đường truyền riêng để tăng cường bảo mật dữ liệu trao đổi trên mạng;

d) Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động và quản lý hạ tầng kỹ thuật, hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy cập trái phép;

đ) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an toàn mạng. Thường xuyên kiểm tra nhằm kịp thời phát hiện những dấu hiệu bất thường gây mất an toàn cho hệ thống mạng nội bộ của cơ quan, đơn vị;

e) Kiểm soát chặt chẽ việc cài đặt các phần mềm lên các máy chủ và máy trạm, đảm bảo tuân thủ quy định quản lý an toàn, an ninh thông tin của cơ quan, đơn vị và các quy định khác có liên quan;

g) Theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại khỏi hệ thống thông tin.

3. An toàn cho máy chủ:

a) Thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành và các phần mềm ứng dụng được cài đặt trên máy chủ; đóng tất cả các cổng (Port) dịch vụ khi không sử dụng; thiết lập chính sách ghi lưu tập trong quá trình hoạt động (Log file) của mỗi máy chủ theo định kỳ từ 3 tháng trở lên;

b) Khi cần kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa (ví dụ: SSH, VPN,...);

c) Các máy chủ chỉ dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt các phần mềm không rõ nguồn gốc, phần mềm không có nhu cầu sử dụng. Không sử dụng máy chủ để duyệt web đọc báo, xem tin tức, chơi điện tử,...;

d) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy chủ, đồng thời đảm bảo các phần mềm phòng, chống virus, mã độc này luôn được cập nhật khả năng nhận dạng virus, mã độc mới từ nhà sản xuất.

4. An toàn khi sử dụng các thiết bị lưu trữ ngoài:

a) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB phải quét virus trước khi đọc hoặc sao chép dữ liệu;

b) Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 2. An toàn dữ liệu, cơ sở dữ liệu

1. Các hệ thống phần mềm, cơ sở dữ liệu phải có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn, đồng thời phải thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi khi có sự cố xảy ra.

2. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã.

3. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, nhất là các thông tin thuộc danh mục bí mật Nhà nước.

4. Quản lý và phân quyền truy cập phần mềm và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

5. Phần mềm hệ quản trị cơ sở dữ liệu phải được thiết lập cơ chế tự động và thường xuyên cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

Điều 3. Đảm bảo an toàn trong hoạt động trao đổi thông tin trên mạng

1. Việc gửi thông tin trên mạng phải đảm bảo:

a) Không giả mạo nguồn gốc của thông tin;

b) Tuân thủ quy định này và quy định của pháp luật có liên quan.

2. Phân loại tài sản thông tin theo các tiêu chí về giá trị, độ nhạy cảm và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ.

3. Thực hiện các biện pháp quản lý phù hợp với từng loại tài sản thông tin đã phân loại

4. Khuyến khích áp dụng công nghệ mã hóa, chữ ký số,... khi chia sẻ, lưu trữ, trao đổi thông tin trên môi trường mạng.

Điều 4. Bảo vệ bí mật Nhà nước trong công tác ứng dụng CNTT

1. Không được sử dụng máy tính nối mạng 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 mạng.

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

3. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo và có sự giám sát, quản lý chặt chẽ của cơ quan có thẩm quyền.

4. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Tuân thủ Pháp lệnh bảo vệ bí mật Nhà nước và các quy định khác có liên quan của Nhà nước về công tác bảo vệ bí mật nhà nước.

Điều 5. Giải quyết và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng:

a) Thông tin, báo cáo kịp thời cho người chuyên trách, phụ trách về công nghệ thông tin của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin của đơn vị.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với người chuyên trách, phụ trách về công nghệ thông tin:

a) Thông tin, báo cáo lãnh đạo cơ quan, đơn vị.

b) Xử lý khẩn cấp: Khi phát hiện hệ thống nội bộ bị tấn công, thông qua các dấu hiệu như luồng tin (traffic) tăng lên bất ngờ, nội dung bị thay đổi, hệ thống hoạt động chậm bất thường cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

Bước 2: Sao chép nhật ký (log file) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ;

Bước 3: Khôi phục lại hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại bình thường.

Lập biên bản ghi nhận sự cố gây ra mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị; đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có); đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

c) Trong trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông, Công an tỉnh và các đơn vị có liên quan.

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 6. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm trước Sở Y Tế, UBND Quận trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình.

2. Thực hiện và chỉ đạo CBCCVC và người lao động thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy định này.

3. Tạo điều kiện thuận lợi cho người chuyên trách về công nghệ thông tin được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn, an ninh thông tin mạng.

4. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

5. Hủy bỏ quyền truy nhập vào hệ thống thông tin, thu hồi lại các tài liệu, hồ sơ, thông tin liên quan tới tài khoản của CBCCVC chuyển công tác, nghỉ hưu hoặc chấm dứt hợp đồng.

6. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin mạng phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan có liên quan.

7. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi phạm an toàn, an ninh thông tin.

Điều 7. Người chuyên trách, phụ trách công nghệ thông tin tại các cơ quan đơn vị

1. Được đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

3. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị; hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

4. Triển khai áp dụng các giải pháp tổng thể đảm bảo an toàn, an ninh thông tin mạng trong toàn hệ thống; triển khai các giải pháp kỹ thuật phòng chống virus, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin.

5. Thường xuyên cập nhật các bản vá lỗi đối với hệ thống, cập nhật các phiên bản mới đối với chương trình chống virus.

6. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng, tin cậy và toàn vẹn.

7. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin mạng bao gồm: Hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét), truy cập trái phép, virus, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thểxảy ra.

Điều 8. Đối với cán bộ, công chức, viên chức tại các cơ quan, đơn vị

a) Thường xuyên cập nhật chính sách, thủ tục an toàn thông tin của đơn vị và thực hiện hướng dẫn về an toàn, an ninh thông tin của cán bộ phụ trách;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, nếu sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

d) Khi mở các tập tin đính kèm theo thư điện tử, nếu biết rõ người gửi thư thì phải lưu tập tin vào máy tính rồi quét virus trước khi mở, không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng để phòng, tránh virus, phần mềm gián điệp đính kèm theo thư;

đ) Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước;

e) Khi đặt các loại mật khẩu *(tệp tin, máy tính, thư điện tử, tài khoản phần mềm quản lý văn bản,...)* nên nhiều hơn 8 ký tự, có cả số và chữ; đồng thời các loại mật khẩu nên thay đổi sau một khoảng thời gian đưa vào sử dụng, nếu có dấu hiệu lộ phải thay đổi ngay;

f) Không cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi./.

TRUNG TÂM Y TẾ QUẬN THANH KHÊ

GIÁM ĐỐC

TRUNG TÂM Y TẾ QUẬN THANH KHÊ

Phan Thanh Phương