UBND TỈNH THỪA THIÊN HUẾ
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 1885/QĐ-SGD&ĐT

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

Thừa Thiên Huế, ngày 19 tháng 8 năm 2016

QUYẾT ĐỊNH
Ban hành Quy định đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các đơn vị ngành Giáo dục và Đào tạo Thừa Thiên Huế

GIÁM ĐỐC SỞ GIÁO DỤC VÀ ĐÀO TẠO

Căn cứ Quyết định số 08/2016/QĐ-UBND ngày 21/01/2016 của UBND tỉnh về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của ngành Giáo dục và Đào tạo tỉnh Thừa Thiên Huế;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

Căn cứ Quyết định 2072/QĐ-UBND ngày 16 tháng 10 năm 2014 của UBND tỉnh quy định việc đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Thừa Thiên Huế;

Theo đề nghị của Ban Công nghệ thông tin ngành Giáo dục và Đào tạo,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các đơn vị ngành Giáo dục và Đào tạo Thừa Thiên Huế.

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

Điều 3. Chánh Văn phòng; Chánh Thanh tra; Trưởng các Phòng Ban của Sở; Trưởng Phòng Giáo dục và Đào tạo các huyện, thị xã và thành phố; Thủ trưởng các trường, các trung tâm trên địa bàn tỉnh Thừa Thiên Huế chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- Như điều 3;
- Lãnh đạo Sở;
- Lưu: VT, CNTT.

GIÁM ĐỐC

(Đã ký)

Phạm Văn Hùng

UBND TỈNH THỪA THIÊN HUẾ
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các đơn vị ngành Giáo dục và Đào tạo Thừa Thiên Huế

(Ban hành kèm theo Quyết định số /QĐ-SGD&ĐT, ngày 19/8/2016 của Giám đốc Ngành giáo dục và đào tạo)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các đơn vị ngành Giáo dục và Đào tạo (GD&ĐT) Thừa Thiên Huế bao gồm: Công tác quản lý đảm bảo an toàn, an ninh thông tin mạng; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin.

2. Quy chế này áp dụng đối với các Phòng chuyên môn của Sở, các Phòng GD&ĐT, các trường, các trung tâm và toàn thể công chức, viên chức (CCVC) ngành GD&ĐT tỉnh Thừa Thiên Huế.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin (CNTT) trong hoạt động của ngành GD&ĐT.

2. Các hoạt động ứng dụng CNTT của các đơn vị ngành GD&ĐT phải tuân thủ theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Quyết định 2072/QĐ-UBND ngày 16 tháng 10 năm 2014 của UBND tỉnh quy định về đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Thừa Thiên Huế.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 3. Quy định sử dụng máy tính cá nhân

1. Máy tính cá nhân bao gồm máy bàn và máy xách tay chỉ cài đặt các phần mềm rõ nguồn gốc và phục vụ trong công tác, không cài đặt các phần mềm không rõ nguồn gốc để hạn chế lỗ hổng bảo mật khi sử dụng internet.

2. Hệ điều hành máy tính luôn bật tường lửa (firewall) nhằm giảm thiểu được nguy cơ tấn công máy tính cá nhân.

3. Thường xuyên cập nhật các bản nâng cấp của hệ điều hành và các bản nâng cấp các phần mềm cài đặt trên máy tính.

4. Máy tính luôn thực thi phần mềm phòng chống virus, chống mã độc, đồng thời luôn để chế độ bảo vệ và phải được thiết lập chế độ tự động cập nhật.

5. Sử dụng các trình duyệt uy tín, an toàn như: Mozilla Firefox, Google Chrome, Internet Explorer để duyệt web.

6. Tất cả các tập tin, thư mục ở các thiết bị bên ngoài (như: USB, ổ cứng ngoài,…) phải được quét virus trước khi sao chép máy tính.

7. Tuyệt đối không cắm USB không rõ nguồn gốc vào máy tính.

8. Khi không sử dụng máy tính trong thời gian quá 02 giờ trở lên cần tắt máy, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

9. Khi phát hiện ra các dấu hiệu liên quan đến việc bị nhiễm mã độc trên máy tính (ví dụ: máy hoạt động chậm bất thường, cảnh báo liên tục từ phần mềm diệt virus, mất dữ liệu,…), người sử dụng phải tắt máy, không nên cố sử dụng để truy xuất dữ liệu trên máy tính hoặc copy dữ liệu qua máy tính khác, mà phải báo ngay cho cán bộ, giáo viên được giao phụ trách CNTT của đơn vị mình để kịp thời xử lý.

10. Không tải và cài đặt các phần mềm lạ, không rõ nguồn gốc, xuất xứ làm ảnh hưởng đến máy tính.

11. Sao lưu dữ liệu thường xuyên để có thể khôi phục lại khi dữ liệu bị mất hoặc bị mã hóa.

Điều 4. Quy định sử dụng các phần mềm ngành giáo GD&ĐT và hộp thư điện tử (email)

1. Mỗi tài khoản truy cập các hệ thống phần mềm chỉ được cấp cho một người quản lý và sử dụng. Người sử dụng phải có trách nhiệm bảo mật tài khoản truy cập của mình.

2. CCVC đặt mật khẩu cho tài khoản đăng nhập phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, gồm ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và phải thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Không xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của đơn vị, cá nhân khác.

4. Không được truy cập vào các website hoặc các đường link lạ.

5. Không đọc những thư điện tử không rõ nguồn gốc người gửi và kích hoạt các đường liên kết có dấu hiệu không rõ ràng.

6. Không sử dụng email công vụ do cơ quan cấp trên cấp cho mục đích cá nhân như: Đăng ký dịch vụ thương mại, trao đổi chia sẻ thông tin cá nhân, tham gia vào các diễn đàn.

7. Không tải những file đính kèm trên thư điện tử và các Trang thông tin khác không rõ nguồn gốc, đặc biệt là các tập tin đính kèm có phần mở rộng (đuôi) zip, rar (file nén).

8. Đối với CCVC nghỉ hưu, chuyển công tác hoặc chấm dứt hợp đồng lao động thì các của đơn vị chủ động khóa ngay tài khoản đăng nhập các phần mềm ngành GD&ĐT, đồng thời gửi Sở danh sách các tài khoản email đề nghị khóa hoặc thiết lập lại nhằm đảm bảo đúng quy định.

Điều 5. Quản lý, vận hành hệ thống thông tin của đơn vị

1. Hệ thống mạng không dây (wireless) của đơn vị phải được thiết lập khóa khi truy cập tối thiểu 8 ký tự và định kỳ thay đổi mật khẩu.

2. Mạng riêng ảo (VPN) của đơn vị (nếu có) kết nối để truy cập vào hệ thống thông tin phải được bảo mật; quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng.

3. Tất cả các tài khoản truy cập vào hệ thống thông tin, thiết bị mạng, máy tính, các ứng dụng của các đơn vị phải được thiết lập mật khẩu; mật khẩu phải được đặt ở mức bảo mật cao (tương tự như quy định ở khoản 2, điều 4 nêu trên) và phải thường xuyên thay đổi mật khẩu với tần suất phù hợp; danh sách tài khoản phải được quản lý, kiểm tra và cập nhật kịp thời; quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng cá nhân.

4. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing) ngoại trừ máy in, khi sử dụng chức năng này cần có chức năng bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này sau khi sử dụng xong.

Điều 6. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng CNTT

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

a) 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 Trang thông tin điện tử.

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

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật thì cá nhân, đơn vị phải báo cơ quan có thẩm quyền, không được để người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính, các đơn vị phải xoá bỏ vĩnh viễn toàn bộ dữ liệu trong ổ cứng máy tính.

Điều 7. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

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

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán hay đình trệ hoạt động chính của các phòng, đơn vị.

c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của các đơn vị.

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của các phòng, đơn vị thuộc Sở.

2. Xử lý sự cố:

a) Đối với người sử dụng:

- Thông tin, báo cáo kịp thời cho cán bộ được phân công phụ trách CNTT 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.

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

b) Đối với cán bộ được đơn vị phân công phụ trách CNTT:

Xử lý khẩn cấp: Khi phát hiện hệ thống nội bộ bị tấn công, cần ngắt kết nối máy chủ ra khỏi mạng (nếu có), sao chép nhật ký (log file) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ; 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 đơn vị; thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có); báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng đơn vị.

Trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp, Sở GD&ĐT và Sở Thông tin và Truyền thông qua số điện thoại 054.3882333-25 để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 8. Trách nhiệm của thủ trưởng đơn vị

Trưởng các Phòng Ban của Sở, Trưởng Phòng GD&ĐT các huyện thị xã và thành phố, Thủ trưởng các đơn vị giáo dục trên địa bàn tỉnh Thừa Thiên Huế có trách nhiệm sau:

1. Tổ chức thực hiện Quy định này và chịu trách nhiệm trước Giám đốc Sở trong công tác đảm bảo an toàn thông tin của phòng, đơn vị mình.

2. Thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin.

3. Phân công một lãnh đạo đơn vị thường xuyên theo dõi để đảm bảo an toàn thông tin của đơn vị.

4. Thủ trưởng các đơn vị kiểm tra công tác xóa dữ liệu trong ổ đĩa máy tính đảm bảo không còn dữ liệu trước khi thanh lý.

5. 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.

Điều 9. Trách nhiệm của công chức, viên chức

1. Trách nhiệm của cán bộ được đơn vị phân công phụ trách CNTT:

- Có trách nhiệm thiết lập các thiết bị mạng, mạng không dây trong nội bộ đơn vị, đặt mật khẩu truy cập, chịu trách nhiệm thay đổi và quản lý mật khẩu.

- 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.

- Giám sát, nhắc nhở, khuyến cáo CCVC thay đổi mật khẩu thường xuyên.

- Thường xuyên cập nhật Quy định an toàn, an ninh thông tin trong quá trình vận hành hệ thống.

- Triển khai các giải pháp tổng thể bảo đảm an toàn, an ninh thông tin mạng trong toàn hệ thống; các giải pháp kỹ thuật phòng chống virus, mã độc, thư rác cho hệ thống và máy tính cá nhân cho CCVC trong đơn vị.

- Hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra cho CCVC trong toàn đơn vị.

- Tuân thủ theo sự hướng dẫn kỹ thuật của Sở GD&ĐT và Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

2. Trách nhiệm của CCVC tham gia sử dụng và khai thác hệ thống thông tin:

- Nghiêm túc thực hiện Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

- Mỗi CCVC phải có trách nhiệm tự quản lý, bảo quản thiết bị đã được giao sử dụng.

- Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo ngay với thủ trưởng đơn vị và cán bộ được đơn vị phân công phụ trách CNTT để kịp thời ngăn chặn và xử lý sự cố.

- Tham gia các chương trình tập huấn về an toàn, an ninh thông tin.

- Không cung cấp mật khẩu cho người ngoài hoặc cắm các thiết bị không rõ nguồn gốc vào máy tính trừ những đoàn công tác đến làm việc trực tiếp với đơn vị.

Chương IV
XỬ LÝ VI PHẠM

Điều 10. Xử lý vi phạm

Cá nhân, tập thể nào làm trái với các quy định của văn bản này và các quy định của pháp luật có liên quan thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 11. Tổ chức thực hiện

Các Phòng Ban của Sở; Phòng GD&ĐT các huyện, thị xã và thành phố, các trường và các trung tâm trên địa bàn tỉnh Thừa Thiên Huế triển khai thực hiện nghiêm túc Quy chế này. Trong quá trình thực hiện nếu gặp khó khăn, vướng mắc, kịp thời báo cáo về Sở GD&ĐT xem xét, giải quyết./.

GIÁM ĐỐC

(Đã ký)

Phạm Văn Hùng