UBND TỈNH HÒA BÌNH
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 849/QĐ-SGD&ĐT

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

Hòa Bình, ngày 10 tháng 6 năm 2016

QUYẾT ĐỊNH
Về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin của Sở Giáo dục và Đào tạo Hòa Bình

GIÁM ĐỐC SỞ GIÁO DỤC VÀ ĐÀO TẠO TỈNH HÒA BÌNH

Căn cứ Luật Công nghệ thông tin ngày 26 tháng 6 năm 2006;

Căn cứ Luật Giao dịch Điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 64/2007/NĐ-CP, ngày 10 tháng 4 năm 2007 của Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam về việc Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Quyết định số 04/2012/QĐ-UBND ngày 30/3/2012 của Ủy ban nhân dân tỉnh Hòa Bình về việc ban hành quy định vị trí, chức năng, quyền hạn, cơ cấu tổ chức bộ máy Sở GD&ĐT Hòa Bình;

Xét đề nghị của Chánh Văn phòng Sở Giáo dục và Đào tạo Hòa Bình,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế đảm bảo an toàn, an ninh thông tin của Sở Giáo dục và Đào tạo Hòa Bình".

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

Điều 3. Chánh Văn phòng Sở, Chánh Thanh tra Sở, Trưởng phòng chức năng, chuyên môn nghiệp vụ Sở, Hiệu trưởng, Giám đốc các đơn vị trực thuộc Sở, Trưởng phòng GD&ĐT huyện, thành phố, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- GĐ, các PGĐ Sở;
- Website ngành;
- Lưu: VT, VP, CNTT.(NVH80).

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HÒA BÌNH

Bùi Trọng Đắc

UBND TỈNH HÒA HÒA BÌNH
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin của Sở Giáo dục và Đào tạo Hòa Bình

(Ban hành kèm theo Quyết định số 849 /QĐ-SGD&ĐT, ngày 10 /6/2016 của Giám đốc Sở 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 nội dung, biện pháp bảo đảm an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT) phục vụ cho công tác điều hành và quản lý hành chính nhà nước của ngành Giáo dục và Đào tạo tỉnh Hòa Bình.

2. Quy chế này áp dụng cho tất cả cán bộ, công chức, viên chức cơ quan Sở Giáo dục và Đào tạo và các đơn vị, trường học trực thuộc Sở, các Phòng GD&ĐT huyện, thành phố trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại cơ quan, đơn vị.

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

Điều 2. Về quản lý tài khoản người dùng

1. Quản trị mạng Sở có trách nhiệm tạo, lập và cung cấp tài khoản truy nhập hệ thống mạng nội bộ, hệ thống email cho cán bộ, công chức, viên chức của Sở.

Đối với công chức, viên chức tiếp nhận mới hoặc luân chuyển, ngừng công tác ở Sở: Quản trị mạng căn cứ Quyết định của cơ quan tạo mới hoặc hủy bỏ các tài khoản liên quan cho các cá nhân đó.

2. Cán bộ, công chức, viên chức phải cài đặt mật khẩu cho máy tính cá nhân của mình, có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của mình như: thư công vụ, quản lý hồ sơ công việc, kế toán, cơ sở dữ liệu…; không tự ý xâm nhập các tài khoản khác; đồng thời không cho thông tin tài khoản của mình cho các cá nhân không có liên quan.

- Mật khẩu phải thay đổi thường xuyên hoặc định kỳ 3 tháng 1 lần.

- Không dùng một mật khẩu trong nhiều tài khoản.

Điều 3. Về quản lý, sử dụng hệ thống

1. Đối với thiết bị công nghệ thông tin

Cán bộ, công chức Sở có trách nhiệm quản lý trang thiết bị công nghệ thông tin (máy vi tính, máy in, thiết bị ngoại vi,...) được giao, tự quản lý dữ liệu trên máy tính của mình, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy định. Ngoài ra, đối với cơ sở dữ liệu có tính chất "Mật" khi chia sẻ dữ liệu phải có ý kiến của lãnh đạo cơ quan và quản lý, lưu trữ theo quy định của ngành Giáo dục và Đào tạo.

- Quản trị mạng 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; ghi nhật ký báo lỗi của mạng, các thiết bị công nghệ thông tin để thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN Sở.

- Máy tính và các thiết bị công nghệ thông tin để nơi an toàn, tránh ảnh hưởng các tác nhân bên ngoài (ánh nắng, mưa...), không để các tài liệu giấy gần máy tính và các thiết bị ngoại vi nhằm tránh cháy nổ xảy ra, thường xuyên vệ sinh cho máy; hàng ngày kiểm tra theo dõi sự hoạt động của máy tính, thiết bị ngoại vi... Khi không sử dụng máy tính nên tắt máy nhằm tiết kiệm điện và phòng, chống các xâm nhập trái phép.

- Trong quá trình sử dụng các thiết bị công nghệ thông tin, nếu có sự cố xảy ra, cán bộ, công chức, viên chức lập tờ trình yêu cầu sửa chữa, chuyển đến Quản trị mạng. Trong trường hợp xảy ra sự cố lớn phiếu sửa chữa phải được xác nhận của lãnh đạo Sở.

- Các công việc sửa chữa hàng ngày đều được ghi vào nhật ký sửa chữa của Quản trị mạng sau mỗi lần sửa chữa.

2. Hệ thống mạng LAN

- Cán bộ, công chức, viên chức Sở khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng. Trường hợp cần thiết phải thay đổi tham số mạng, hãy báo cho Quản trị mạng để xử lý.

- Quản trị mạng 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 khác theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu; ghi nhật ký báo lỗi của mạng, các thiết bị công nghệ thông tin để thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN Sở.

- Quản trị mạng chịu tránh nhiệm cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; cài đặt hệ thống tự động cập nhật mẫu Virus mới và tự động diệt Virus khi phát hiện có Virus xâm nhập máy tính; thường xuyên kiểm tra, quét Virus định kỳ cho tất cả các máy chủ, máy trạm; xử lý, khắc phục kịp thời khi

xảy ra sự cố máy tính bị Virus xâm nhập; đảm bảo hệ thống mạng máy tính luôn sạch Virus để đảm bảo máy tính của cán bộ, công chức hoạt động tốt.

- Hàng năm phải tham mưu đề xuất kế hoạch mua sắm thiết bị, máy móc, phần mềm an toàn, an ninh thông tin trang bị trong cơ quan Sở.

Điều 4. Cơ chế sao lưu dữ liệu

1. Phân loại dữ liệu sao lưu

- Dữ liệu hệ thống: bao gồm các loại thông tin, dữ liệu cài đặt như: cấp phát tài khoản và địa chỉ IP mạng, phân giải tên miền, cung cấp thông tin internet,….

- Dữ liệu các ứng dụng dùng chung được cài đặt trên máy chủ như: Quản lý hộp thư điện tử, đường truyền số liệu, phần mềm dùng chung…

- Các dữ liệu khác cài đặt trên máy tính cá nhân như: số liệu quản lý thu chi kế toán, quản lý hồ sơ một cửa, công văn đi, công văn đến,… do cán bộ công chức, viên chức thuộc các phòng chức năng, chuyên môn, nghiệp vụ của Sở soạn thảo, tạo lập trên các máy trạm trong mạng nội bộ của Sở.

- Các hệ thống thông tin quản lý giáo dục, hệ thống thông tin quản lý chất lượng giáo dục tiểu học, hệ thống thông tin quản lý nhân sự, hệ thống thông tin phổ cập giáo dục, hệ thống thông tin đánh giá chất lượng giáo dục, hệ thống thông tin quản lý nhà trường... được quản lý và lưu trữ trên các hệ thống điện toán đám mây thuộc Bộ Giáo dục và Đào tạo, các Phòng chức năng, chuyên môn, nghiệp vụ Sở chịu trách nhiệm sao lưu theo quy định của Bộ GD&ĐT.

2. Quy định thiết bị sao lưu

- Đối với dữ liệu hệ thống: Sử dụng chức năng sao lưu dự phòng của các ứng dụng, kết hợp với sử dụng thiết bị lưu trữ tập trung tại phòng Quản trị mạng của Sở.

- Đối với các dữ liệu khác: Các dữ liệu cần lưu trữ, các phòng, đơn vị thuộc Sở chép lên ổ đĩa mạng của máy chủ để sao lưu tập trung.

Ngoài ra, căn cứ vào các mức độ quan trọng của dữ liệu, các phòng, đơn vị thuộc Sở sử dụng các thiết bị gắn ngoài (ổ cứng di động, USB, đĩa CD, DVD…) nhằm lưu trữ dữ liệu an toàn, bảo mật.

3. Định kỳ sao lưu

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

- Đối với dữ liệu hệ thống: Sao lưu định kỳ: 3 tháng/lần

- Đối với các hệ thống thông tin: Sao lưu thường xuyên.

- Đối với các dữ liệu khác: sao lưu khi có thay đổi thông tin

4. Quy định về khôi phục dữ liệu đã sao lưu

- Khi cần khôi phục lại dữ liệu đã sao lưu, các phòng chức năng, chuyên môn, nghiệp vụ Sở báo cho Quản trị mạng biết, xem xét thực hiện khôi phục dữ liệu.

- Thời kỳ dữ liệu yêu cầu khôi phục phải phù hợp với quy định khoản 3 Điều này.

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

1. Đối với cán bộ, công chức

- Thông tin báo cáo kịp thời cho Quản trị mạng và Văn phòng khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong hệ thống mạng Sở.

- Xử lý khẩn cấp: khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: hệ thống máy vi tính hoạt động chậm khác thường, nội dung bị thay đổi,…cần thực hiện các bước sau:

- Ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet.

- Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu ngoài (CD, USB, ổ cứng di động,…).

- Khôi phục hệ thống bằng cách chuyển dữ liệu backup (sao lưu) mới nhất để hệ thống hoạt động ổn định.

2. Đối với cán bộ Quản trị mạng

- Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi) của Sở.

- Hướng dẫn người dùng các biện pháp kỹ thuật giải quyết và khắc phục sự cố; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với Lãnh đạo Sở; đồng thời phối hợp với cơ quan chuyên môn (Sở Thông tin và Truyền thông, Công An tỉnh Hòa Bình…) hướng dẫn khắc phục.

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

Điều 6. Trách nhiệm của Lãnh đạo Sở

1. Lãnh đạo Sở có trách nhiệm toàn diện trước UBND tỉnh trong công tác bảo vệ an toàn hệ thống thông tin của đơn vị.

2. Phân công cán bộ Quản trị mạng đảm bảo, an toàn thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin.

3. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin. Đào tạo, tuyển dụng nguồn nhân lực có kiến thức, trình độ về công nghệ thông tin.

4. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời cử cán bộ phối hợp chặt chẽ với cơ quan chuyên môn trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

Điều 7. Trách nhiệm của Tổ Công nghệ Thông tin

- Hàng năm, lập kế hoạch ứng dụng công nghệ thông tin, kế hoạch an toàn và an ninh thông tin trình lãnh đạo Sở GD&ĐT phê duyệt để thực hiện.

- Xây dựng các quy chế hoạt động của Hệ thống thông tin Quản lý giáo dục, quản lý Phổ cập giáo dục, quản lý chất lượng giáo dục, quản lý nhân sự, quản lý đánh giá chất lượng giáo dục...

- Kịp thời tham mưu cho Lãnh đạo Sở những quy định, hướng dẫn có liên quan đến công tác an toàn, an ninh thông tin do cơ quan chuyên môn cấp trên, UBND tỉnh ban hành.

- Đảm bảo an toàn, an ninh thông tin đối với các máy tính quản trị Website của Sở và Website của Phòng GD&ĐT huyện, thành phố, các đơn vị, trường học, các máy tính lưu trữ cơ sở dữ liệu của ngành giáo dục và đào tạo. Có kế hoạch trang bị thiết bị, phần mềm an toàn, an ninh thông tin đảm bảo hoạt động ổn định và an toàn.

Điều 8. Đối với trách nhiệm của quản trị mạng

1. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi), hệ thống mạng, thực hiện các báo cáo định kỳ về tình trạng hoạt động toàn hệ thống mạng, đề nghị hướng giải quyết khi có sự cố.

2. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

3. Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ, công chức, viên chức trong cơ quan.

4. Quản lý, theo dõi các hoạt động thường xuyên và định kỳ như vận hành, sửa chữa hệ thống máy chủ, máy trạm, các thiết bị khác...; xử lý các yêu cầu về thay đổi tài khoản sử dụng mạng của các phòng chức năng, chuyên môn, nghiệp vụ của Sở.

5. Sao lưu dữ liệu tại nơi an toàn, kiểm ra dữ liệu sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn.

6. Thực hiện việc đánh giá, báo cáo các rủi ro về mức độ nghiêm trọng có thể xảy ra do sự truy cập và sử dụng trái phép, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

Điều 9. Đối với cán bộ, công chức, viên chức và người lao động

1. Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, 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.

2. Các cán bộ, công chức, viên chức có trách nhiệm tự quản lý các thiết bị CNTT được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy vi tính khi chưa có sự đồng ý của quản trị mạng; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị máy tính.

3. Sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu nhạy

cảm như tài khoản, mật khẩu, các tập tin văn bản,... được mã hóa trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp gây mất mát thông tin.

4. Không được truy cập hoặc tải thông tin từ các trang Website độc hại, không được cài đặt các chương trình không rõ nguồn gốc…

5. Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn thông tin của cơ quan và các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn, an ninh thông tin tại cơ quan.

Chương IV
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 10. Khen thưởng

Các phòng chức năng, chuyên môn, nghiệp vụ Sở, các đơn vị, trường học trực thuộc; cán bộ, công chức, viên chức và người lao động thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá khen thưởng.

Điều 11. Xử lý vi phạm

Các phòng chức năng, chuyên môn, nghiệp vụ Sở, các đơn vị, trường học trực thuộc; cán bộ, công chức, viên chức có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 12. Trách nhiệm thi hành

Chánh Văn phòng Sở, Chánh Thanh tra Sở, Trưởng các phòng chức năng, chuyên môn nghiệp vụ Sở, Hiệu trưởng, Giám đốc các đơn vị, trường học trực thuộc, Trưởng phòng GD&ĐT huyện, thành phố chịu trách nhiệm tổ chức, triển khai thực hiện Quy chế này. Trong quá trình thực hiện, nếu có những vấn đề vướng mắc, phát sinh cần bổ sung, sửa đổi. Đề nghị các đơn vị báo cáo về Văn phòng Sở để kịp thời sửa đổi, bổ sung./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HÒA BÌNH

Bùi Trọng Đắc