UBND TỈNH HƯNG YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 202 /QĐ-SGD&ĐT

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

Hưng Yên, ngày 06 tháng 4 năm 2016

QUYẾT ĐỊNH
Ban hành Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động nội bộ Sở Giáo dục và Đào tạo Hưng Yên

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng CNTT trong hoạt động của cơ quan Nhà nước;

Căn cứ Quyết định số 05/2016/QĐ-UBND ngày 17/3/2016 v/v Ban hành Quy chế bảo đảm an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Hưng Yên;

Căn cứ Quyết định số 575/QĐ-UBND ngày 23/3/2009 của UBND tỉnh Hưng Yên, quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Giáo dục và Đào tạo;

Xét đề nghị của ông Trưởng phòng Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo Quyết định này Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động nội bộ Sở Giáo dục và Đào tạo Hưng Yên.

Điều 2: Chánh Văn phòng Sở, Trưởng các phòng Sở chịu trách nhiệm thi hành Quyết định này kể từ ngày ký.

Nơi nhận:
- Như điều 2;
- Ban giám đốc;
- Lưu: VT, CNTT.

GIÁM ĐỐC

CỘNG HÒA XH CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HƯNG YÊN

Nguyễn Văn Phê

UBND TỈNH HƯNG YÊN
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 trong hoạt động nội bộ Sở Giáo dục và Đào tạo Hưng Yên

(Ban hành theo Quyết định số 202 /QĐ-SGD&ĐT ngày 6 /4/2016 của Giám đốc Sở Giáo dục và Đào tạo Hưng Yên

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin (CNTT) trong hoạt động nội bộ của Sở Giáo dục và Đào tạo (GD&ĐT) Hưng Yên.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với cơ quan Sở GD&ĐT (sau đây gọi tắt là cơ quan).

2. Cán bộ, công chức, viên chức đang làm việc trong cơ quan Sở GD&ĐT và những tổ chức, cá nhân có liên quan áp dụng Quy chế này trong việc đảm bảo an toàn thông tin tại cơ quan.

Điều 3. Mục đích, nguyên tắc đảm bảo an toàn, an ninh thông tin

1. Tăng cường khả năng phòng chống nguy cơ tấn công, xâm nhập hệ thống thông tin và ngăn chặn, khắc phục kịp thời các sự cố gây mất an toàn thông tin trên môi trường mạng.

2. Công tác đảm bảo an toàn, bảo mật thông tin trên môi trường mạng là yêu cầu bắt buộc trong quá trình thiết kế, vận hành, nâng cấp và hủy bỏ hạ tầng kỹ thuật, hệ thống thông tin của cơ quan nhà nước.

3. Thông tin số được quy định trong danh mục bí mật nhà nước, văn bản điện tử có nội dung mật không được truyền đưa trên môi trường mạng và phải được phân loại, lưu trữ, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng phải được Lãnh đạo Sở cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu.

Điều 4. Giải thích từ ngữ

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

1. Hệ thống thông tin là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

2. An toàn thông tin là 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 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.

3. 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.

4. Trung tâm tích hợp dữ liệu là nơi tập trung nhiều thành phần máy chủ, thiết bị mạng, thiết bị bảo mật và các thiết bị phụ trợ khác (hệ thống giám sát, hệ thống lưu điện, máy phát điện, điều hòa, chống cháy nổ, chống sét) để lưu trữ, xử lý, trao đổi và quản lý tập trung dữ liệu cho các hệ thống thông tin của tỉnh.

5. Thông tin số là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

6. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn trái pháp luật việc truyền tải thông tin trên mạng; can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sửa chữa, sao chép, làm sai lệch trái phép thông tin trên mạng.

2. Cản trở trái pháp luật hoạt động của hệ thống thông tin, phá hoại cơ sở hạ tầng thông tin, thông tin trên môi trường mạng, gây ảnh hưởng tới khả năng truy nhập hợp pháp của người sử dụng tới hệ thống thông tin.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin cho hệ thống thông tin; tạo, cài đặt, phát tán phần mềm độc hại, vi rút máy tính, thư rác; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin.

4. Lợi dụng mạng để tuyên truyền, chống phá Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết toàn dân.

5. Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm.

6. Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định.

7. Các hành vi bị nghiêm cấm khác theo quy định của pháp luật.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 6. Các biện pháp quản lý vận hành trong công tác đảm bảo an toàn, an ninh thông tin

1. Đối với cơ quan

a) Trang bị đầy đủ các kiến thức an toàn, bảo mật thông tin cho cán bộ, công chức, viên chức;

b) Bố trí cán bộ chuyên trách về an toàn thông tin của đơn vị (gọi tắt là cán bộ chuyên trách); tạo điều kiện để cán bộ chuyên trách được học tập, nâng cao kiến thức về an toàn thông tin;

c) Bố trí máy tính riêng, không kết nối mạng nội bộ và mạng internet để quản lý, lưu trữ, soạn thảo văn bản tài liệu mật theo quy định khi cần thiết;

d) Kiểm tra việc thực hiện các nội dung quy định tại Điều 7 Quy chế này.

2. Đối với cán bộ chuyên trách tại cơ quan

a) Triển khai, thực hiện các nội dung tại Điều 7 Quy chế này;

b) Tham mưu về chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị; triển khai các biện pháp đảm bảo an toàn, an ninh thông tin cho cán bộ, công chức, viên chức trong đơn vị mình;

c) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật nhà nước; thường xuyên nghiên cứu, cập nhật kiến thức về an toàn, an ninh thông tin; các nguy cơ tiềm ẩn có thể gây mất an toàn thông tin và biện pháp kỹ thuật phòng ngừa;

d) Thực hiện giám sát, đánh giá, báo cáo các rủi ro và nguy cơ mất an toàn thông tin có thể xảy ra và mức độ nghiêm trọng của các rủi ro đó;

e) Thường xuyên theo dõi bản ghi nhật ký trên các thiết bị mạng máy tính, hệ điều hành, phần mềm ứng dụng, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ; các sự kiện đó có thể do sự truy cập trái phép để sử dụng trái phép hoặc gây mất, thay đổi thông tin;

f) Kiểm soát chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm; theo dõi hoạt động của cổng/trang thông tin điện tử của đơn vị bảo đảm thông tin chính xác, không bị thay đổi; phối hợp với các cá nhân, đơn vị liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

3. Đối với cán bộ, công chức, viên chức

a) Thường xuyên cập nhật chính sách, quy trình đảm bảo an toàn thông tin của đơn vị, hướng dẫn của cán bộ chuyên trách;

b) Việc sử dụng, chia sẻ và lưu trữ dữ liệu, thông tin số trên mạng nội bộ, mạng Internet phải tuân thủ các quy định của cơ quan, đơn vị và quy định của pháp luật về viễn thông, công nghệ thông tin;

c) Không cài đặt phần mềm không rõ nguồn gốc hoặc can thiệp tới các phần mềm ứng dụng khác trên hệ thống thông tin của cơ quan khi chưa được cấp có thẩm quyền cho phép;

d) Sử dụng các biện pháp kỹ thuật để mã hóa dữ liệu khi cần thiết bảo đảm không bị thay đổi trước khi truyền trên môi trường mạng. Các tệp tin đính kèm thư điện tử hoặc được tải xuống từ mạng Internet hay từ các thiết bị lưu trữ ngoài khi thực hiện sao chép, kết nối với máy tính cần được kiểm tra để phòng chống vi rút, phần mềm độc hại;

e) Không sử dụng tên tài khoản thư điện tử công vụ trên các trang mạng xã hội, diễn đàn và các trang thông tin tổng hợp khác trên mạng Internet, Thư điện tử công vụ được phép sử dụng trong các hoạt động công vụ; tuân thủ các quy định theo quy chế sử dụng thư điện tử công vụ của tỉnh;

f) Sử dụng các thiết bị lưu trữ gắn ngoài và thiết bị điện tử khác an toàn, đúng quy định. Thực hiện tắt máy tính khi không sử dụng trong thời gian dài hoặc hết thời gian làm việc để tránh các nguy cơ tấn công, xâm nhập trái phép.

Điều 7. Các biện pháp quản lý kỹ thuật trong công tác đảm bảo an toàn, an ninh thông tin

1. Máy chủ, máy tính cá nhân, hệ thống lưu trữ, thiết bị mạng, thiết bị bảo mật, các ứng dụng của cơ quan phải được bảo vệ bởi mật khẩu an toàn, có độ phức tạp cao (mật khẩu có tối thiểu 6 ký tự bao gồm chữ in hoa, chữ in thường, chữ số và ký tự đặc biệt) và không sử dụng mật khẩu ngắn, mặc định.

2. Tất cả các máy tính tại cơ quan, đơn vị phải được cài đặt và bảo vệ bởi phần mềm phòng chống vi rút, phần mềm độc hại.

3. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm: Tiến hành sao lưu định kỳ dữ liệu hệ điều hành, phần mềm chuyên ngành, cơ sở dữ liệu quan trọng bằng các thiết bị sao lưu và phần mềm chuyên dụng nhằm phục vụ công tác phục hồi dữ liệu một cách nhanh nhất.

4. Tổ chức quản lý tài khoản, định danh người dùng trong các hệ thống thông tin bao gồm: Tạo mới, kích hoạt, sửa đổi và loại bỏ tài khoản. Đối với cán bộ công chức, viên chức đã nghỉ việc, chuyển công tác phải có biện pháp khóa tài khoản, hủy quyền truy cập, thu hồi các thiết bị liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, công cụ ký số và thiết bị khác có liên quan) nhưng vẫn đảm bảo khả năng truy cập vào các hồ sơ được tạo ra bởi tài khoản đó.

5. Đối với tài khoản người dùng sử dụng để đăng nhập các hệ thống thông tin, phần mềm ứng dụng, cơ sở dữ liệu và các ứng dụng chuyên ngành khác phải thiết lập mật khẩu có mức bảo mật cao, không sử dụng mật khẩu ngắn, mặc định nhằm đảm bảo an toàn, bảo mật thông tin của người dùng.

6. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

7. Hệ thống thông tin cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DOS, DDOS). Sử dụng thiết bị tường lửa, xây dựng giải pháp phù hợp để có thể ngăn chặn, phòng tránh bị ảnh hưởng trực tiếp và bảo vệ thiết bị, máy chủ.

8. Quản lý nhật ký hệ thống (Logfile): Hệ thống thông tin cần ghi nhận các bản ghi nhật ký (quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, truy xuất hệ thống). Thường xuyên kiểm tra, lưu giữ nội dung nhật ký trong khoảng thời gian nhất định để phục vụ quản lý, kiểm soát trên hệ thống.

9. Trường hợp có sự cố máy tính nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cơ quan cấp trên quản lý trực tiếp, phối hợp với Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ khắc phục.

Điều 8. Đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin

Phòng CNTT có trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin, bao gồm:

a) Nghiên cứu, đề xuất xây dựng các hệ thống thông tin dùng chung trên địa bàn tỉnh để tăng hiệu quả sử dụng, tiết kiệm đầu tư, đảm bảo tính liên thông giữa cơ quan và thuận tiện trong việc đảm bảo an toàn thông tin;

b) Tổ chức thực hiện giám sát, đánh giá và đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung, cơ sở dữ liệu quan trọng của ngành, cổng/trang thông tin điện tử, hệ thống thư điện tử, quản lý văn bản điều hành, một cửa điện tử, quản lý nhân sự và các hệ thống thông tin quan trọng khác;

c) Chủ trì phối hợp với các phòng ban xây dựng phương án, tổ chức sao lưu và phục hồi dữ liệu khi xảy ra sự cố đối với các hệ thống thông tin của ngành; hướng dẫn sao lưu dự phòng các dữ liệu quan trọng khác;

d) Tham mưu Lãnh đạo Sở, hướng dẫn việc sử dụng các thiết bị viễn thông, điện tử, máy tính dùng để lưu giữ và truyền đưa thông tin bí mật nhà nước.

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

Điều 9. Trách nhiệm của cơ quan

1. Thủ trưởng cơ quan có trách nhiệm tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND tỉnh trong công tác đảm bảo an toàn thông tin của cơ quan.

2. Ưu tiên nguồn kinh phí thường xuyên cho việc triển khai các biện pháp đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan.

3. Khi xảy ra sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế mức thấp nhất thiệt hại có thể xảy ra, ưu tiên sử dụng cán bộ chuyên trách của cơ quan; thông báo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông.

4. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan thực hiện công tác kiểm tra, khắc phục sự cố nhanh chóng, kịp thời và hiệu quả; đồng thời cung cấp đầy đủ thông tin khi được yêu cầu.

5. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

6. Định kỳ hàng năm báo cáo tình hình, kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin gửi Sở Thông tin và Truyền thông trước ngày 15 tháng 11 để tổng hợp, báo cáo UBND tỉnh.

Điều 10. Trách nhiệm của Phòng Công nghệ thông tin

1. Tham mưu Lãnh đạo Sở về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động nội bộ cơ quan và chịu trách nhiệm trước Lãnh đạo Sở trong việc đảm bảo an toàn cho các hệ thống thông tin của cơ quan.

2. Hàng năm xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác đảm bảo an toàn, an ninh thông tin phục vụ cho hoạt động ứng dụng công nghệ thông tin tại cơ quan; vận hành, khai thác các hệ thống thông tin trong phạm vi quản lý.

3. Chủ trì, phối hợp với các đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc kiểm tra đột xuất công tác đảm bảo an toàn thông tin trong cơ quan khi phát hiện có các dấu hiệu, hành vi vi phạm an toàn thông tin.

4. Hỗ trợ tập huấn, hướng dẫn, tuyên truyền đảm bảo an toàn, an ninh thông tin trong hoạt động quản lý nhà nước; tham gia các khóa đào tạo nâng cao về an toàn thông tin cho cán bộ chuyên trách của cơ quan.

5. Là cơ quan đầu mối về ứng cứu sự cố máy tính, tham gia vào mạng lưới điều phối ứng cứu sự cố, tiếp nhận và xử lý các thông báo sự cố về an toàn thông tin. Tùy theo mức độ sự cố, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính của tỉnh, các đơn vị có liên quan hướng dẫn xử lý, ứng cứu sự cố mất an toàn thông tin.

6. Chủ trì, phối hợp với Sở Thông tin và Truyền thông triển khai giải pháp an toàn, bảo mật đối với hệ thống thông tin, cơ sở dữ liệu liên quan tới lưu trữ, truyền tải thông tin bí mật nhà nước trên Mạng truyền số liệu chuyên dùng của cơ quan Đảng, Nhà nước.

7. Hướng dẫn đơn vị trực thuộc xây dựng quy chế nội bộ bảo đảm an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

8. Tổng hợp báo cáo tình hình đảm bảo an toàn thông tin của tỉnh theo định kỳ, gửi Sở Thông tin và Truyền thông, UBND tỉnh và cơ quan có liên quan.

Điều 11. Trách nhiệm của cán bộ, công chức, viên chức trong cơ quan

1. Nghiêm chỉnh chấp hành các quy định tại quy chế nội bộ đảm bảo an toàn, an ninh thông tin của cơ quan, các quy định tại Quy chế này và 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, quyền hạn được giao.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và cán bộ chuyên trách của đơn vị để kịp thời ngăn chặn, xử lý.

3. Tham gia các chương trình đào tạo, tập huấn, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông hoặc cơ quan chuyên môn tổ chức.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 12. Khen thưởng và xử lý vi phạm

1. Hàng năm, lập báo cáo gửi Sở Thông tin và Truyền thông về công tác an toàn, an ninh thông tin của cơ quan làm căn cứ đánh giá xếp hạng an toàn, an ninh thông tin; trên cơ sở đó đề xuất UBND tỉnh xem xét, khen thưởng theo quy định hiện hành.

2. Tập thể, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

Điều 13. Điều khoản thi hành

Phòng CNTT có trách nhiệm chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn, triển khai và kiểm tra, đôn đốc việc thực hiện Quy chế này.

Trong quá trình thực hiện Quy chế này, nếu có vướng mắc, đề nghị cơ quan gửi văn bản về phòng CNTT để tổng hợp, báo cáo Lãnh đạo Sở xem xét, sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC

CỘNG HÒA XH CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HƯNG YÊN

Nguyễn Văn Phê