UBND TỈNH HƯNG YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

Số: 201 /QĐ-SGD&ĐT

Hưng Yên, ngày 06 tháng 4 năm 2016

QUYẾT ĐỊNH

Ban hành Quy chế quản lý và sử dụng mạng máy tính nội bộ và các thiết bị CNTT của 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 đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực CNTT 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 Trưởng phòng Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo Quyết định này Quy chế Quản lý và sử dụng mạng máy tính nội bộ và các thiết bị CNTT Sở Giáo dục và Đào tạo Hưng Yên.

Điều 2: Chánh Văn phòng Sở, Trưởng các phòng chức năng 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
Quản lý và sử dụng mạng máy tính nội bộ và các thiết bị CNTT của Sở Giáo dục và Đào tạo Hưng Yên

(Ban hành theo Quyết định số 201 /QĐ-SGD&ĐT ngày 06 /4/2016 của Giám đốc Sở Giáo dục và Đào tạo Hưng Yên

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

1. Quy chế này quy định việc quản lý và sử dụng hệ thống mạng máy tính nội bộ tại Sở Giáo dục và Đào tạo Hưng Yên.

2. Quy chế này áp dụng đối với công chức, viên chức, công tác tại các phòng ban thuộc Sở trong việc quản lý, sử dụng mạng nội bộ (LAN) và mạng Internet.

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 và Server), 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: Cổng thông tin điện tử (portal), Hệ thống văn bản điều hành (VBĐH), Hệ thống thư điện tử công vụ (email); các phần mềm được cài đặt trên hệ thống máy chủ (server); hệ thống cơ sở dữ liệu dùng chung của Sở; tài nguyên có nội dung chuyên môn, nghiệp vụ,... được lưu trữ trên máy tính cá nhân (PC).

3. Người sử dụng: Cán bộ, công chức, viên chức Sở GD&ĐT, 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.

4. Quản trị mạng 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; hướng dẫn người sử dụng thiết bị CNTT và khai thác tài nguyên phục vụ công tác.

CHƯƠNG II
QUẢN LÝ, SỬ DỤNG MẠNG MÁY TÍNH

Điều 3: Quản lý mạng máy tính

Phòng CNTT tham mưu giúp Giám đốc Sở quản lý hệ thống cơ sở dữ liệu (CSDL), hệ thống mạng trong Sở.

Quản trị mạng là cán bộ của phòng CNTT có trách nhiệm quản lý trang 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 Sở để khai thác, 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.

2. Việc đặt tên, đặt địa chỉ IP cho máy tính phải tuân 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, tiết lộ để lọt 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, cơ quan 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 phải bảo đảm 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, email công vụ, Văn bản điều hành.

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 CSDL, 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 được cung cấp mật khẩu cho người khác. Các thư mục chia sẻ file dùng chung phải đặt mật khẩu riêng để bảo đảm an toàn file dữ liệu.

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. Nghiêm cấm việc truy cập và truyền bá thông tin có hại.

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 lãnh đạo Sở đồng ý.

5. Sử dụng dịch vụ "Thư điện tử":

a. Hệ thống thư công vụ (email công vụ) của Sở có địa chỉ:

http://mail.hungyen.gov.vn/

b. Danh sách email công vụ của đơn vị, cá nhân thuộc Sở do Phòng CNTT quản lý, cung cấp theo quy định về bảo mật thông tin. Mọi vấn đề phát sinh đều phải thông qua Phòng CNTT kiểm duyệt theo quy định.

c. Email công vụ được sử dụng để gửi thư, các văn bản, tài liệu điện tử cần gửi tới người đã đăng ký hộp thư điện tử, tham gia sử dụng, trao đổi thông tin trên mạng nội bộ của Sở và Internet; tuyệt đối không sử dụng địa chỉ email công vụ để đăng ký dịch vụ trên mạng xã hội.

d. Các đơn vị, cá nhân có trách nhiệm thường xuyên kiểm tra hộp thư điện tử công vụ của đơn vị, cá nhân mình để tiếp nhận và xử lý kịp thời các thông tin, các ý kiến của lãnh đạo Sở, các phòng, đơn vị và cá nhân khác gửi đến ***(tối thiểu một ngày 02 lần: buổi sáng vào lúc 8h00, buổi chiều vào lúc 14h00)***

6. Sử dụng phần mềm "Quản lý văn bản điều hành"

a. Hệ thống văn bản điều hành của Sở có địa chỉ: http://113.160.133.4:8281/

b. Các đơn vị, cá nhân phải tổ chức triển khai và ứng dụng có hiệu quả phần mềm VBĐH để quản lý, gửi, nhận và xử lý văn bản đi, đến. Thực hiện quy trình xử lý văn bản đi, đến; quản lý, lưu trữ hồ sơ công việc của đơn vị, cá nhân trên mạng máy tính.

c. Tăng cường sử dụng văn bản, tài liệu điện tử lưu hành trong đơn vị thông qua phần mềm, CSDL trên mạng thay thế văn bản giấy; hạn chế tối đa việc in ấn, sao chụp, nhân bản văn bản giấy.

d. Các đơn vị, cá nhân có trách nhiệm thường xuyên truy cập, sử dụng phần mềm VBĐH theo quyền hạn được phân công để tiếp nhận, xử lý kịp thời văn bản chỉ đạo, văn bản dự thảo của Lãnh đạo Sở, các phòng, đơn vị và cá nhân khác gửi đến ***(tối thiểu một ngày 02 lần: buổi sáng vào lúc 7h30, buổi chiều vào lúc 14h00).***

e. Tên truy cập vào hệ thống VBĐH của đơn vị, cá nhân thuộc Sở do Phòng CNTT quản lý, cung cấp theo đúng quy định về bảo mật thông tin; thông tin của các đơn vị, cá nhân khi được tạo lập được lưu trữ tại máy chủ của Sở. Mọi vấn đề phát sinh phải thông qua phòng CNTT kiểm duyệt theo quy định.

7. Cập nhật, khai thác CSDL dùng chung, CSDL chuyên ngành, dịch vụ hành chính công, thông tin trên mạng Internet:

Các đơn vị căn cứ vào chức năng, nhiệm vụ của đơn vị, chỉ đạo chuyên viên phụ trách cập nhật, sử dụng 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.

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 hiện theo hướng dẫn sử dụng thiết bị, hạn chế tối đa việc tắt đột ngột thiết bị (ví dụ: ngắt nguồn điện). Thường xuyên vệ sinh máy tính và 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 trình, 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.

5. Không được tự ý thay đổi tên máy, workgroup, domain, địa chỉ IP máy tính nếu không được 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 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 vào các trang web không 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 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 theo đúng quy trình, tắt nguồn điện cung cấp cho hệ thống máy tính. Hàng tháng máy chủ và các thiết bị phải được kiểm tra, bảo dưỡng định kỳ.

10. Quản trị mạng chịu trách nhiệm bảo đảm an toàn thông tin truyền dẫn và dữ liệu lưu trên mạng máy tính. Áp dụng các biện pháp bảo đảm 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 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 tại Công văn số 648/VPCP-QTTV ngày 14/08/2006 của Văn phòng Chính phủ.

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 sẻ đường truyền mạng LAN cơ quan, đơn vị ra ngoài cơ quan, đơn vị đề phòng để lộ, lọt thông tin nội bộ và xâm nhập trái phép vào máy chủ.

3. Người sử dụng phải đổi mật khẩu cá nhân ngay sau khi nhận được tên và mật khẩu đăng nhập do quản trị mạng cung cấp. 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 đĩa cứng (HDD) và ổ cứng ngoài (có chứa dữ liệu) ra khỏi cơ quan, đơn vị trừ trường hợp ổ cứng hỏng cần sửa chữa phải được phép của quản trị mạng. Đối với những máy tính 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. Trong trường hợp ổ đĩa cứng của máy tính này bị hư hỏng không còn khả năng sử dụng thì cơ quan tự hủy để bảo đảm 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, bảo đảm 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 dữ liệu dự phòng 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, khi có sự cố xảy ra các đơn vị, cá nhân phải kịp thời tách rời và cô lập thiết bị khỏi mạng LAN; 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.

CHƯƠNG IV
KHEN THƯỞNG, KỶ LUẬT

Điều 10. Các cá nhân, đơn vị thuộc cơ quan 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 đúng 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 của Sở và có hiệu lực kể từ ngày ký ban hành.

Điều 13. Trong quá trình thực hiện nếu cần bổ sung chỉnh sửa, các cá nhân, đơn vị gửi kiến nghị về Phòng Công nghệ thông tin để tổng hợp, trình Giám đốc Sở xem xét, quyết định.

Điều 14. Chánh văn phòng Sở, Trưởng các phòng chức năng Sở có trách nhiệm chỉ đạo, hướng dẫn và đôn đốc thực hiện Quy chế này./.

GIÁM ĐỐC

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

Nguyễn Văn Phê