TỔNG C.TY XD&TM HƯNG ĐÔ - CTCP
TRƯỜNG TRUNG CẤP NGHỀ HƯNG ĐÔ

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

Số: 33 /QĐ - TCNHĐ

Thiệu hoá; *ngày 11 tháng 02 năm 2025*

QUYẾT ĐỊNH

Đảm bảo an toàn an ninh thông tin, quy chế sử dụng phần cứng, phần mềm, tài khoản để đảm bảo sử dụng hệ thống thông tin an toàn, hiệu quả của trường TCN Hưng Đô

HIỆU TRƯỞNG TRƯỜNG TRUNG CẤP NGHỀ HƯNG ĐÔ

Căn cứ Luật Công nghệ thông tin ngày29/6/2006; Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015; Căn cứ Luật An ninh mạng ngày 12/06/2018;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 35/2024/TT-BGTVT ngày 15 tháng 11 năm 2024 của Bộ Giao thông vận tải quy định đào tạo, sát hạch, cấp giấy phép lái xe; cấp, sử dụng giấy phép lái xe quốc tế; đào tạo, kiểm tra, cấp chứng chỉ bồi dưỡng kiến thức pháp luật về giao thông đường bộ.

Theo đề nghị Trưởng Phòng Tổ chức - Hành Chính.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn hệ thống thông tin Hệ thống mạng nội bộ của trường TCN Hưng Đô.

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

Điều 3. Phòng TC - HC; Kỹ thuật viên; cán bộ, giáo viên, nhân viên trường TCN Hưng Đô, các bộ phận, tổ chức, cá nhân sử dụng hệ thống mạng nội bộ của trường TCN Hưng Đô và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lưu: VT.

K/T. HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

SỞ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI TỈNH THANH HÓA
TRƯỜNG TRUNG CẤP NGHỀ HƯNG ĐÔ

Chu Đình Tùng

TỔNG C.TY XD&TM HƯNG ĐÔ - CTCP
TRƯỜNG TRUNG CẤP NGHỀ HƯNG ĐÔ

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

QUY CHẾ

Đảm bảo an toàn an ninh thông tin, quy chế sử dụng phần cứng, phần mềm, tài khoản để đảm bảo sử dụng hệ thống thông tin an toàn, hiệu quả của trường TCN Hưng Đô

(Ban hành theo Quyết định số: 33 /QĐ-TCNHĐ ngày 11/02/2025 của Hiệu trưởng trường TCN Hưng Đô)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định về Đảm bảo an toàn an ninh thông tin, quy chế sử dụng phần cứng, phần mềm, tài khoản để đảm bảo sử dụng hệ thống thông tin an toàn, hiệu quả của trường TCN Hưng Đô

2. Đối tượng áp dụng:

a) Cán bộ, giáo viên, các bộ phận, tổ chức, cá nhân sử dụng hệ thống mạng nội bộ của trường TCN Hưng Đô; các tổ chức, cá nhân có liên quan và các đối tượng tham gia vận hành, khai thác các hệ thống thông tin mạng nội bộ của trường TCN Hưng Đô.

b) Các cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin mạng nội bộ của trường TCN Hưng Đô.

c) Các cơ quan, tổ chức, cá nhân cung cấp dịch vụ viễn thông, công nghệ thông tin và an toàn thông tin mạng cho hệ thống thông tin mạng nội bộ của trường TCN Hưng Đô.

Điều 2. Giải thích từ ngữ

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

1. An toàn thông tin mạng: là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Mạng: là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. 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 như: Hệ thống mạng nội bộ, hệ thống quản lý văn bản và điều hành, hệ thống thư điện tử, Dịch vụ công trực tuyến, Trang thông tin điện tử của trường TCN Hưng Đô.

4. Đơn vị vận hành hệ thống thông tin: là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

5. Cán bộ chuyên trách: Là cán bộ, công chức, viên chức, người lao động được tuyển dụng phụ trách an toàn thông tin/công nghệ thông tin tại các bộ phận.

6. Không gian mạng: Là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

7. Hạ tầng kỹ thuật: Là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng.

8. Sự cố an toàn thông tin mạng: Là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

9. 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 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin mạng nội bộ của trường TCN Hưng Đô tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Nguyên tắc

a) Hoạt động ứng dụng công nghệ thông tin thực hiện các nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật an toàn thông tin mạng năm 2015 và Điều 41 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.
- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn thông tin cho hệ thống thông tin mạng nội bộ

của trường TCN Hưng Đô được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Tài nguyên thông tin cần bảo đảm an toàn thông tin

Tài nguyên thông tin cần bảo đảm an toàn thông tin bao gồm các thành phần sau đây:

1) Hệ thống hạ tầng kỹ thuật:

a) Thiết bị tính toán, lưu trữ (máy chủ, máy trạm, SAN, NAS, ...nếu có).

b) Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hóa, camera, thiết bị lưu trữ dữ liệu di động, ...).

c) Đường truyền dữ liệu, đường kết nối Internet.

d) Mạng nội bộ (LAN), mạng diện rộng (WAN) và thiết bị kết nối mạng, thiết bị bảo mật, thiết bị phụ trợ.

đ) Thiết bị công nghệ thông tin, viễn thông khác được kết nối mạng trong cơ quan.

2. *Hệ thống thông tin, phần mềm, ứng dụng và cơ sở dữ liệu:*

a) Hệ thống thông tin, nền tảng số, cơ sở dữ liệu dùng chung (thư điện tử, quản lý văn bản và điều hành, thông tin nội bộ, quản lý nhân sự và thi đua khen thưởng, quản lý tài sản, hồ sơ hành chính điện tử, dữ liệu thống kê tổng hợp,...).

b) Hệ thống thông tin nghiệp vụ và các cơ sở dữ liệu chuyên ngành.

c) Phần mềm, ứng dụng phục vụ công tác quản lý, điều hành hoạt động của cơ quan Nhà nước.

3. Thông tin, dữ liệu được trao đổi, truyền tải, xử lý và lưu trữ tại trường TCN Hưng Đô.

Điều 5. Nguồn nhân lực bảo đảm an toàn thông tin

1. *Quy định đối với công tác tuyển dụng*

a) Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin cần có trình độ, chuyên ngành hoặc kiến thức, sự am hiểu về lĩnh vực công nghệ thông tin, an toàn thông tin hoặc phù hợp với vị trí tuyển dụng.

b) Xây dựng các quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ; xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.

2. *Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc:*

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với cán bộ quản lý và vận hành hệ thống.

+ Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

+ Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

+ Các cơ quan, địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

b) Định kỳ hàng năm người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 1907/QĐ-TTg ngày 23/11/2020 của Thủ tướng Chính phủ.

c) Định kỳ hàng năm, người sử dụng và bộ phận quản lý và vận hành hệ thống được tổ chức đào tạo các kỹ năng về an toàn thông tin theo chương trình, nội dung tại Quyết định số 21/QĐ-TTg ngày 06/01/2021 của Thủ tướng Chính phủ.

3. *Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:*

a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của cơ quan, tổ chức.

b) Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 6. Khi thiết kế, xây dựng hệ thống thông tin cần bảo đảm các yêu cầu như:

1. Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Xây dựng các tài liệu mô tả thiết kế, sơ đồ hệ thống và các thành phần của hệ thống thông tin.

3. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

4. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

Điều 7. Đối với phát triển phần mềm thuê khoán cần đáp ứng:

1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Các nhà phát triển cung cấp mã nguồn phần mềm.

3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

3.

Chương III
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG QUẢN LÝ, VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 9. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống:

a) Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn

và bảo mật. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

b) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

c) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

2. Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như: USB, DVD hoặc SAN...

b) Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

c) Xây dựng và triển khai quy trình kết nối thiết bị đầu cuối vào hệ thống quản trị. Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

d) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

4. Các thiết bị trong hệ thống cần được cấu hình tối ưu, tăng cường bảo mật, ưu tiên sử dụng thiết bị chuyên dụng trước khi đưa vào vận hành, khai thác.

Điều 10. Quản lý an toàn máy chủ và ứng dụng *(khi được trang bị)*

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Có phương án cập nhật bản vá lỗi, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. Người dùng không được can thiệp vào các phần mềm đã cài đặt (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận chuyên trách về công nghệ thông tin.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ

Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

3. Truy cập và quản trị máy chủ và ứng dụng

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

4. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5) Các máy chủ (khi được trang bị) trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

đ) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

Điều 11. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa

a) Đơn vị vận hành phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Có cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Sao lưu dự phòng và khôi phục dữ liệu

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Đơn vị vận hành xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ….

Điều 12. Quản lý an toàn thiết bị đầu cuối

1. Đơn vị vận hành cần thiết lập và cập nhật thường xuyên thông tin quản lý thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP…)

2. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

3. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 13. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy chủ, máy trạm phải được trang bị phần mềm phòng chống mã độc đáp ứng yêu cầu tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, …), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại

trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 14. Quản lý điểm yếu an toàn thông tin

Đơn vị vận hành có trách nhiệm:

1. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ...); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Báo cáo lãnh đạo/cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

5. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

6. Định kỳ 01 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

Điều 15. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.

3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

Điều 16. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia *(Quyết định 05)*; Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý

ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng: Cán bộ kỹ thuật cùng các đơn vị vận hành xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

3. Kế hoạch ứng phó sự cố an toàn thông tin mạng: Cán bộ kỹ thuật cùng các đơn vị vận hành xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin.

a. Cán bộ kỹ thuật cùng các đơn vị vận hành điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống.

b. Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của đơn vị khi phát hiện các sự cố gây mất ATTT 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.

5. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng: Cán bộ kỹ thuật cùng các đơn vị vận hành xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

6. Cán bộ kỹ thuật phụ trách về Thông tin quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của lãnh đạo.

7. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

8. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của lãnh đạo.

Điều 17. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo

nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 20. Bộ phận chuyên trách về an toàn thông tin

1. Giao cán bộ kỹ thuật phụ trách về công nghệ thông tin là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.

Trường TCN Hưng Đô là bộ phận vận hành Hệ thống thông tin.

2. Cán bộ kỹ thuật là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin như:

a) Sở Giao thông vận tải Thanh Hóa

- Người liên hệ/bộ phận: .....

+ Số điện thoại: .....

+ Email: .....

b) Công ty ECOTECK

- Người liên hệ/bộ phận: .....

- Số điện thoại: .....

- Email: .....

3. Cán bộ kỹ thuật có trách nhiệm phổ biến hướng dẫn triển khai Quy chế này và các quy định về an toàn thông tin có liên quan.

4. Cán bộ kỹ thuật tham mưu thực hiện chế độ báo cáo định kỳ theo quy định của pháp luật, báo cáo đột xuất theo yêu cầu của cấp trên.

Điều 21. Trách nhiệm của các bộ phận, tổ chức, cá nhân

1. Tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của Nhà nước đối với các cá nhân thuộc bộ phận, đơn vị mình về an toàn thông tin mạng.

1. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin mạng trong công việc của cá nhân do đơn vị quản lý.

2. Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ- CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 22. Tổ chức triển khai Quy chế

Quy định trong Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị

liên quan phản ánh kịp thời về bộ phận chuyên trách để xem xét, bổ sung, sửa đổi.

Điều 23. Rà soát, cập nhật, bổ sung Quy chế

Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung./.