ĐẠI HỌC QUỐC GIA TP.HCM
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

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

TP. Hồ Chí Minh, ngày 17 tháng 7 năm 2019

QUY CHẾ
BẢO ĐẢM AN TOÀN THÔNG TIN

(Ban hành kèm theo quyết định số 408/QĐ-ĐHCNTT, ngày 17 Tháng 7 Năm 2019 của Hiệu trưởng Trường Đại học Công nghệ Thông tin)

CHƯƠNG I

NHỮNG QUI ĐỊNH CHUNG

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

1. Quy chế này quy định phạm vi tài nguyên thông tin và các nguyên tắc, chính sách, biện pháp cơ bản bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của trường Đại học Công nghệ Thông tin - ĐHQG-HCM (ĐHCNTT).
2. Đối tượng áp dụng đối với các đơn vị trực thuộc trường ĐHCNTT (sau đây gọi chung là đơn vị) và cán bộ, công chức, viên chức, giảng viên, nghiên cứu viên, người lao động trong các đơn vị, sinh viên, học viên cao học (sau đây gọi là cá nhân) tham gia vào hoạt động ứng dụng công nghệ thông tin của trường ĐHCNTT.

Điều 2. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu theo nghĩa như sau:

1. *Bảo đảm an toàn thông tin* là sự bảo vệ thông tin và các hệ thống thông tin 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. *Xâm phạm an toàn thông tin* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, hủy hoại trái phép thông tin và hệ thống thông tin.
3. *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.
4. *Hệ thống thông tin* là cơ sở dữ liệu, tập hợp phần cứng, phần mềm được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên môi trường mạng.

5. *Trang thông tin điện tử* là trang thông tin hoặc một tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin.
6. *Cổng thông tin điện tử* là điểm truy nhập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.
7. *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.
8. *Cổng giao tiếp* dùng để định danh các ứng dụng gửi và nhận dữ liệu. Mỗi ứng dụng sẽ được gắn tương ứng (không cố định) với một cổng giao tiếp. Những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.
9. *Bản ghi nhật ký hệ thống* là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: thiết bị bảo mật, thiết bị tính toán, máy chủ ứng dụng, ... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.
10. *Thiết bị lưu trữ dữ liệu di động* là thiết bị được sử dụng để đọc, ghi dữ liệu có thể được di chuyển tới nhiều nơi, nhiều người có thể sử dụng (ổ cứng di động, USB, máy tính xách tay, thẻ nhớ, CD, DVD, ...).
11. *Lưu trữ trên môi trường mạng* là phương thức lưu trữ sử dụng các ứng dụng lưu trữ của các nhà cung cấp. Dữ liệu được đưa lên máy chủ của nhà cung cấp dịch vụ lưu trữ.
12. *Người sử dụng* là cá nhân sử dụng máy tính, thiết bị di động có truy cập hệ thống mạng, hệ thống thông tin của trường.
13. *Tiêu chuẩn TCVN 7562:2005* là tiêu chuẩn Việt Nam về quy tắc thực hành quản lý an toàn thông tin (tương đương tiêu chuẩn ISO/IEC 17799:2000).

Điều 3. 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:

1. Hệ thống hạ tầng kỹ thuật:
   a) Mạng kết nối Internet của trường ĐHCNTT, mạng nội bộ (LAN) và thiết bị kết nối mạng, thiết bị bảo mật, thiết bị phụ trợ.
   b) Thiết bị tính toán, lưu trữ (máy chủ, máy trạm, SAN, NAS, …).
   c) Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hóa, thiết bị lưu trữ dữ liệu di động, …).
   d) Thiết bị công nghệ thông tin được kết nối mạng trong các đơn vị.

2. Phần mềm, ứng dụng và cơ sở dữ liệu:
   a) Trang/cổng thông tin điện tử của trường ĐHCNTT và các đơn vị, tổ chức.
   b) Phần mềm, ứng dụng phục vụ công tác quản lý, điều hành hoạt động của trường ĐHCNTT và các đơn vị, tổ chức.
   c) Phần mềm, ứng dụng cung cấp dịch vụ trực tuyến.
   d) Các dịch vụ mạng.
   e) Cơ sở dữ liệu dùng chung.
3. Thông tin, dữ liệu được trao đổi, truyền tải, xử lý và lưu trữ trên hạ tầng kỹ thuật của trường ĐHCNTT.

Điều 4. Nguyên tắc chung về bảo đảm an toàn thông tin

1. Bảo đảm an toàn thông tin là yêu cầu bắt buộc, có tính xuyên suốt và phải thường xuyên, liên tục trong quá trình:
   a) Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.
   b) Thiết kế, xây dựng, vận hành, nâng cấp, cải tiến, hủy bỏ hệ thống thông tin.
2. Các đơn vị và cá nhân có trách nhiệm thực hiện đầy đủ, nghiêm túc các quy định của pháp luật, quy chế của trường ĐHCNTT về bảo đảm an toàn thông tin.
3. Các dự án ứng dụng công nghệ thông tin hoặc dự án có cấu phần công nghệ thông tin phải có ý kiến thẩm định nội dung liên quan đến an toàn thông tin trước khi được phê duyệt.
4. Khi thực hiện thuê hoặc sử dụng dịch vụ công nghệ thông tin do bên thứ ba cung cấp, đơn vị và cá nhân phải quản lý việc sở hữu thông tin, dữ liệu từ dịch vụ đó; yêu cầu nhà cung cấp dịch vụ có trách nhiệm bảo mật thông tin; không để nhà cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu mà chưa có sự cho phép của cá nhân, đơn vị.
5. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 5. Các hành vi bị nghiêm cấm

1. Vi phạm các quy định, quy trình về quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin đối hệ thống thông tin của trường ĐHCNTT.
2. Truy nhập, tác động trái phép, làm sai lệch, gây nguy hại đến thông tin, dữ liệu hoặc xâm phạm an toàn thông tin của cơ quan, đơn vị và cá nhân khác.
3. Tấn công, làm ảnh hưởng đến hoạt động bình thường của hệ thống thông tin hoặc ngăn chặn trái phép, gây gián đoạn truy nhập hợp pháp của người sử dụng tới hệ thống thông tin.
4. Sử dụng tài nguyên thông tin của trường ĐHCNTT để phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

CHƯƠNG II

CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. Bảo đảm an toàn thông tin mức vật lý

1. Bảo đảm an toàn thông tin mức vật lý là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động hệ thống.
2. Các biện pháp cơ bản bảo đảm an toàn thông tin mức vật lý bao gồm:
   a) Quản lý trung tâm dữ liệu/phòng máy chủ:
      - Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ SAN, NAS,... phải được đặt trong trung tâm dữ liệu/phòng máy chủ;
      - Trung tâm dữ liệu/phòng máy chủ phải được thiết lập cơ chế bảo vệ, theo dõi, phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp đối với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đấu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống;
      - Quá trình vào, ra trung tâm dữ liệu/phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu/phòng máy chủ. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào trung tâm dữ liệu/phòng máy chủ. Trang bị cơ chế kiểm tra xác thực nâng cao (thẻ, token, vân tay, ...) khi cần thiết;
      - Có phương án, kế hoạch phòng, chống và khắc phục sự cố ngập dột nước, sét, tĩnh điện, cháy nổ; áp dụng các quy chuẩn kỹ thuật về an toàn kỹ thuật nhiệt, độ ẩm, ánh sáng cho các thiết bị tính toán, lưu trữ; bảo đảm điều kiện hoạt động ổn định cho các hệ thống hỗ trợ như máy điều hòa nhiệt độ, nguồn cấp điện, dây dẫn;
      - Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 10 phút khi có sự cố mất điện.
   b) Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về độ sẵn sàng trong suốt thời gian lắp đặt, sử dụng.
   c) Các đường truyền dữ liệu, đường truyền Internet và hệ thống dây dẫn các mạng WAN, LAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng

tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các đơn vị.

d) Cá nhân sử dụng thiết bị lưu trữ dữ liệu di động để lưu trữ thông tin, dữ liệu của đơn vị mình có trách nhiệm bảo vệ thiết bị này và thông tin lưu trên thiết bị, tránh làm mất hoặc lộ thông tin, dữ liệu. Không mang ra nước ngoài thông tin, dữ liệu của đơn vị, của Nhà nước mà không liên quan tới nội dung công việc thực hiện ở nước ngoài.

e) Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ có chứa dữ liệu cần bảo vệ thì khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải được tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu). Khi thanh lý thiết bị thì phải xóa nội dung lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

3. Đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 7. Bảo đảm an toàn thông tin khi sử dụng máy tính

1. Cá nhân sử dụng máy tính để xử lý công việc tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng); không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu, ...), phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

d) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

e) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @ # ! ...) và thay đổi mật khẩu ít nhất 01 lần/ 3 tháng; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ cache và cookie trong trình duyệt trên máy tính.

f) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

2. Các đơn vị có trách nhiệm tập hợp, cập nhật tài liệu hướng dẫn, quy định về bảo đảm an toàn thông tin khi sử dụng máy tính (cho phù hợp với điều kiện môi trường hoạt động, tình hình phát triển công nghệ thông tin) và phổ biến đến tất cả cá nhân thuộc phạm vi đơn vị mình để tuân thủ thực hiện.

3. Tài khoản truy nhập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó. Các hệ thống thông tin dùng chung của trường ĐHCNTT sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, thôi học (với sinh viên, học viên sau đại học), trong vòng không quá 05 ngày làm việc, đơn vị quản lý cá nhân đó phải thông báo đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin. Với email sẽ được duy trì trong thời hạn 1 tháng, những trường hợp đặc biệt sẽ do Hiệu trưởng quyết định.

c) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

Điều 8. Bảo đảm an toàn thông tin đối với mạng máy tính

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng kết nối với mạng diện rộng (WAN) của trường ĐHCNTT; vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý giám sát bởi các hệ thống các thiết bị mạng, thiết bị bảo mật.

Căn cứ điều kiện, yêu cầu thực tế về bảo mật dữ liệu, cơ quan, đơn vị là chủ quản hệ thống mạng nội bộ chủ động triển khai xây dựng mô hình, giải pháp an toàn bảo mật, bao gồm các biện pháp kỹ thuật sau đây:

a) Kiểm soát truy nhập từ bên ngoài mạng (sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương).

b) Kiểm soát truy nhập từ bên trong mạng (quản lý các thiết bị đầu cuối, máy tính người sử dụng kết nối vào hệ thống mạng; giám sát, phát hiện và ngăn chặn truy nhập từ bên trong mạng đến các địa chỉ Internet bị cấm truy nhập).

c) Phòng, chống xâm nhập và phần mềm độc hại, bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ; có khả năng tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công. Vô hiệu hóa tất cả các dịch vụ không cần thiết tại từng vùng mạng.

d) Cấu hình chức năng xác thực trên các thiết bị kết nối mạng để xác thực người sử dụng quản trị thiết bị trực tiếp hoặc từ xa.

e) Mạng không dây phải có cơ chế bảo toàn tính toàn vẹn và bí mật của thông tin được truyền đưa trên môi trường mạng, có hướng dẫn bảo đảm an toàn thông tin dành cho các thiết bị đầu cuối khi kết nối vào mạng; được thiết lập các tham số: tên, nhận dạng dịch vụ (SSID), mật khẩu, cấp phép truy nhập đối với địa chỉ vật lý (MAC address), mã hóa dữ liệu. Thường xuyên thay đổi mật khẩu. Các điểm truy nhập không dây phải được bảo vệ, tránh bị tiếp cận trái phép.

f) Hệ thống máy chủ phải có chức năng tự động cập nhật bản ghi nhật ký hệ thống trong khoảng thời gian nhất định (tối thiểu là 03 tháng), lưu trữ thông tin kết nối mạng, quá trình đăng nhập vào máy chủ, các thao tác cấu hình hệ thống, lỗi phát sinh trong quá trình hoạt động và các thông tin liên quan về an toàn thông tin để phục vụ công tác khắc phục sự cố và điều tra về an toàn thông tin khi xảy ra. Xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Đơn vị tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN) của trường ĐHCNTT, có trách nhiệm:

a) Bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào hệ thống mạng diện rộng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về đơn vị vận hành hệ thống thông tin của trường ĐHCNTT để thống nhất xử lý.

b) Phối hợp với đơn vị vận hành hệ thống thông tin của trường ĐHCNTT rà soát đánh giá tính hợp lệ cấu hình địa chỉ IP kết nối mạng diện rộng trong quá trình vận hành và sử dụng các hệ thống thông tin, máy chủ, thiết bị công nghệ thông tin của mình có kết nối với hệ thống mạng diện rộng.

c) Định kỳ sao lưu thông tin, dữ liệu dùng chung lưu trữ trên mạng diện rộng.

d) Không tiết lộ phương thức (tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) để truy nhập vào hệ thống mạng diện rộng cho tổ chức, cá nhân khác; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

3. Các đơn vị phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau:

a) Có hệ thống tường lửa và hệ thống bảo vệ kiểm soát truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu ra, vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DoS/DDoS).

b) Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

c) Không mở trang tin hoặc ứng dụng Internet trên máy tính chứa dữ liệu quan trọng hoặc có khả năng tiếp cận các dữ liệu, ứng dụng quan trọng; chỉ thiết lập kết nối Internet cho các máy chủ và thiết bị công nghệ thông tin cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; thiết bị cập nhật bản quyền và hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

Điều 9. Bảo đảm an toàn thông tin mức phần mềm, ứng dụng

1. Các đơn vị xây dựng, vận hành và sử dụng phần mềm, ứng dụng phải đáp ứng các yêu cầu sau:

a) Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

b) Cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian chờ để đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa thông trên môi trường mạng; hạn chế truy nhập tới mã nguồn của

phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

e) Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu là 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

f) Thực hiện quy trình kiểm soát việc cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

g) Kiểm tra phát hiện và khắc phục điểm yếu của ứng dụng trước khi đưa vào sử dụng và trong quá trình sử dụng (khi có thông tin xuất hiện điểm yếu mới trên môi trường hoạt động của ứng dụng; tối thiểu mỗi năm một lần).

2. Đơn vị vận hành hệ thống thông tin của trường ĐHCNTT có trách nhiệm phối hợp với các đơn vị chủ quản hệ thống thông tin, cơ sở dữ liệu dùng chung của trường ĐHCNTT thực hiện:

a) Xây dựng, thống nhất kế hoạch, các phương án bảo đảm an toàn thông tin cho các phần mềm.

b) Thường xuyên theo dõi, giám sát an toàn thông tin và kiểm tra, rà soát hoạt động của các phần mềm.

c) Xây dựng phương án sao lưu, ứng cứu, khắc phục sự cố.

Điều 10. Bảo đảm an toàn thông tin mức dữ liệu

1. Các đơn vị được giao nhiệm vụ bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai như sau:

a) Thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; giám sát, cảnh báo khi có thay đổi hoặc phát hiện, ngăn chặn các tác động truy nhập, gửi, nhận dữ liệu trái phép; khuyến khích áp dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu, đặc biệt trong trường hợp cần bảo đảm chống từ chối nguồn gốc dữ liệu.

b) Mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống lưu trữ/thiết bị lưu trữ dữ liệu bằng giải pháp do đơn vị chuyên trách về công nghệ thông tin của trường ĐHCNTT chấp nhận sử dụng; thiết lập phân vùng lưu trữ mã hóa, chỉ cho phép cá nhân có quyền, trách nhiệm truy nhập, lưu trữ dữ liệu trên phân vùng mã hóa.

c) 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.

2. Các đơn vị phải thường xuyên kiểm tra, giám sát hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.
3. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, các đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài phải cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi; yêu cầu bên ngoài đáp ứng các thỏa thuận kết nối, bảo vệ thông tin phù hợp với quy định về bảo đảm an toàn thông tin của trường ĐHCNTT; thiết lập chức năng phát hiện dữ liệu đính kèm có phần mềm độc hại, cơ chế bảo mật truyền thông không dây, mã hóa thông tin, dữ liệu trước khi truyền đưa, trao đổi trên môi trường mạng theo quy định của pháp luật.
4. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 11. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định các rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

Một số yêu cầu như sau:

a) Có phương án bảo đảm an toàn thông tin mạng được bộ phận/đơn vị chuyên trách về công nghệ thông tin thẩm định khi phát triển, mở rộng hoặc nâng cấp hệ thống thông tin.

b) Chỉ tiếp nhận và đưa vào vận hành hệ thống thông tin sau khi đã thực hiện nghiệm thu và kiểm thử hệ thống (được thẩm định, xác nhận của bộ phận/đơn vị chuyên trách về công nghệ thông tin và phê duyệt của chủ quản hệ thống thông tin).

c) Hệ thống thông tin được tiếp nhận phải đi kèm:

- Tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;
- Tài liệu mô tả các thành phần của hệ thống thông tin, gồm: các vùng mạng chức năng, hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin.

d) Xem xét tính tương thích với các phần mềm, ứng dụng hiện có, bảo đảm hoạt động ổn định, an toàn trước khi quyết định thay đổi hoặc nâng cấp hệ điều hành lên phiên bản mới hơn; kiểm soát chặt chẽ việc nâng cấp, mở rộng phần mềm, ứng dụng trong hệ thống. Việc bổ sung các thiết bị vào hệ thống thông tin cần có kế hoạch, quy trình bảo đảm việc tiếp nhận không làm gián đoạn hoạt động của hệ thống đang vận hành.

e) Bảo trì hệ thống thông tin phải có kế hoạch từ trước và được thực hiện thường xuyên.

2. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống cần thực hiện:

a) Đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Thường xuyên kiểm tra, giám sát việc tuân thủ các quy định về an toàn thông tin, cập nhật đầy đủ các lỗ hổng bảo mật, áp dụng cơ chế sao lưu dự phòng, bảo đảm an toàn truy nhập, đăng nhập hệ thống.

c) Giám sát an toàn hệ thống thông tin, cảnh báo hành vi xâm phạm an toàn thông tin hoặc hành vi có khả năng gây ra sự cố an toàn thông tin đối với hệ thống thông tin; tiến hành phân tích yếu tố then chốt ảnh hưởng tới trạng thái an toàn thông tin; đề xuất thay đổi biện pháp kỹ thuật.

d) Giám sát hiệu năng hệ thống và thực hiện các biện pháp bảo trì cần thiết (dọn dẹp hệ thống, điều chỉnh thông số kỹ thuật và bổ sung mua sắm) để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin theo yêu cầu.

e) Tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi đầy đủ thông tin trong các bản ghi nhật ký hệ thống và lưu trữ nhật ký trong khoảng thời gian nhất định, để phục vụ việc quản lý, kiểm soát thông tin.

3. Đối tác phát triển phần mềm, ứng dụng cho đơn vị có trách nhiệm bảo đảm an toàn thông tin cho công tác phát triển, vận hành, bảo hành, bảo trì phần mềm, ứng dụng, tránh lộ lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

4. Các biện pháp kỹ thuật bảo đảm an toàn thông tin cho trang/cổng thông tin điện tử:

a) Xác định cấu trúc thiết kế trang/cổng thông tin điện tử: quản lý toàn bộ các phiên bản của mã nguồn của phần mềm, ứng dụng trang/cổng thông tin điện tử; phối hợp với đơn vị quản lý máy chủ tổ chức mô hình trang/cổng thông tin điện tử hợp lý tránh khả năng tấn công leo thang đặc quyền; yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa, thiết bị phát hiện/phòng, chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF - Web Application Firewall);

b) Vận hành phần mềm, ứng dụng trang/cổng thông tin điện tử: các trang/ cổng thông tin điện tử khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng thực hiện dịch vụ công trực tuyến mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web (như SQL Injection, Cross-Site Scripting, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Security Misconfiguration, Failure to Restrict URL Access, Insecure Cryptoeraphic Storage, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards và các lỗi bảo mật khác);

c) Thiết lập và cấu hình cơ sở dữ liệu của trang/cổng thông tin điện tử:
   - Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu;
   - Gỡ bỏ các cơ sở dữ liệu không còn sử dụng;
   - Có cơ chế sao lưu dữ liệu tự động theo định kỳ tối thiểu 1 lần / ngày, nên sao lưu vào thiết bị lưu trữ / máy chủ khác với máy chủ cơ sở dữ liệu.

d) Phối hợp với các đơn vị quản lý máy chủ xây dựng phương án phục hồi trang/cổng thông tin điện tử, trong đó chú ý ít nhất mỗi tháng thực hiện việc sao lưu toàn bộ nội dung trang/cổng thông tin điện tử 01 lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc để bảo đảm khi có sự cố có thể khắc phục trong thời gian ngắn nhất.

Điều 12. Kiểm tra, khắc phục sự cố an toàn thông tin

1. Đơn vị quản lý hệ thống thông tin có trách nhiệm phối hợp với các đơn vị chuyên trách về công nghệ thông tin, an toàn thông tin của trường ĐHCNTT:
   a) Rà soát, đánh giá và xác định các sự cố an toàn thông tin, các rủi ro an toàn thông tin có thể xảy ra với từng thành phần hệ thống thông tin trong phạm vi quản lý của mình. Trên cơ sở đó, xây dựng và phê duyệt các phương án ứng cứu, xử lý sự cố phù hợp với các rủi ro an toàn thông tin có thể xảy ra;
   b) Chuẩn bị sẵn sàng các biện pháp, phương tiện kỹ thuật để phục vụ cho triển khai các phương án ứng cứu đã được xây dựng;
   c) Xây dựng và ban hành các hướng dẫn, quy trình xử lý sự cố an toàn thông tin đối với từng đối tượng người sử dụng cụ thể trong hệ thống thông tin;
   d) Thông báo công khai các phương án liên lạc với bộ phận xử lý sự cố cho toàn bộ cá nhân liên quan hệ thống thông tin đang quản lý;
   e) Thường xuyên kiểm tra, rà soát tính sẵn sàng của các phương án ứng cứu sự cố; thực hiện đúng các hướng dẫn, quy trình xử lý sự cố an toàn thông tin.
2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, thủ trưởng đơn vị thực hiện:

a) Chỉ đạo xác định nguyên nhân sự cố, có biện pháp khắc phục kịp thời, hạn chế thiệt hại;

b) Trường hợp gặp sự cố nghiêm trọng ở mức độ cao, khẩn cấp (hệ thống bị gián đoạn dịch vụ; dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; hệ thống bị mất quyền điều khiển) hoặc chủ quản hệ thống không đủ khả năng tự kiểm soát, xử lý được sự cố thì phải phối hợp chặt chẽ với các đơn vị chuyên trách về vận hành hệ thống thông tin, an toàn thông tin, cung cấp đầy đủ thông tin sự cố để được hướng dẫn, hỗ trợ cụ thể.

c) Chuẩn bị tài liệu báo cáo sự cố, gồm các nội dung sau:

- Tên, địa chỉ đơn vị vận hành hệ thống thông tin; chủ quản hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;
- Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;
- Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;
- đơn vị cung cấp dịch vụ hạ tầng kỹ thuật;
- Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;
- Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;
- Kết quả ứng cứu sự cố ban đầu;
- Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có);
- Bản cập nhật mới nhất của tài liệu mô tả các thành phần hệ thống thông tin, bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin (trong trường hợp sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin quan trọng khác).

3. Thủ trưởng đơn vị chủ quản hệ thống thông tin chủ trì, phối hợp với các đơn vị chuyên trách về vận hành hệ thống thông tin, an toàn thông tin của trường ĐHCNTT giám sát liên tục diễn biến sự cố (ở mức độ cao, khẩn cấp) và thông báo, cập nhật đến bên liên quan; tiến hành phân tích sự cố và khắc phục sự cố, gỡ bỏ phần mềm độc hại.

CHƯƠNG III
TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm của đơn vị

1. Chỉ đạo, bảo đảm việc tuân thủ các quy định của Quy chế này trong phạm vi tổ chức, quyền hạn của mình và thực hiện báo cáo việc thực hiện Quy chế này theo yêu cầu của đơn vị chuyên trách về công nghệ thông tin của trường ĐHCNTT.
2. Căn cứ Quy chế này và nhu cầu thực tế của đơn vị, xây dựng hoặc rà soát sửa đổi phương án quản lý an toàn thông tin đang áp dụng cho phù hợp.
3. Tuyên truyền, phổ biến nội dung Quy chế này tới từng cá nhân thuộc đơn vị; nâng cao nhận thức cho các cá nhân về các nguy cơ mất an toàn thông tin.
4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị chuyên trách về công nghệ thông tin, vận hành hệ thống thông tin và an toàn thông tin của trường ĐHCNTT triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

Điều 15. Trách nhiệm của các cá nhân

1. Cá nhân phụ trách an toàn thông tin có trách nhiệm:
   a) Tham mưu cho thủ trưởng đơn vị ban hành các quy định, quy trình nội bộ và chịu trách nhiệm triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin tại cơ quan, đơn vị theo Quy chế này.
   b) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó.
   c) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn thông tin.
2. Cá nhân là người sử dụng có trách nhiệm:
   a) Chấp hành nghiêm túc các quy định về an toàn thông tin của đơn vị, quy định này và các quy định khác của pháp luật về an toàn thông tin; nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.
   b) Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng. Khi phát hiện sự cố phải báo ngay với cấp trên và bộ phận chuyên trách về công nghệ thông tin để kịp thời ngăn chặn, xử lý.
   c) Tích cực tham gia các chương trình đào tạo, hội nghị về an toàn thông tin do các đơn vị chuyên môn tổ chức.

Điều 16. Trách nhiệm của Phòng Dữ liệu & CNTT

1. Phòng Dữ liệu & CNTT đồng thời là đơn vị chuyên trách về công nghệ thông tin, đơn vị vận hành hệ thống thông tin của trường ĐHCNTT, giúp Hiệu trưởng trường ĐHCNTT thực hiện quản lý an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của trường ĐHCNTT theo quy định của Quy chế này và các quy định của pháp luật có liên quan.
2. Phòng Dữ liệu & CNTT có trách nhiệm:
   a) Tham mưu cho Hiệu trưởng trường ĐHCNTT trong việc xây dựng mới, sửa đổi, bổ sung các quy định, chính sách an toàn thông tin trong trường ĐHCNTT.
   b) Chủ trì, phối hợp với các đơn vị liên quan tổ chức phổ biến, hướng dẫn triển khai, kiểm tra, đánh giá và giám sát việc thực hiện Quy chế này trong phạm vi trường ĐHCNTT; định kỳ báo cáo Hiệu trưởng trường ĐHCNTT về tình hình thực hiện; truyền thông, nâng cao nhận thức về gắn kết bảo đảm an toàn thông tin với triển khai ứng dụng công nghệ thông tin.
   c) Thực hiện xác định cấp độ an toàn hệ thống thông tin của trường ĐHCNTT và các đơn vị.
   d) Triển khai các biện pháp bảo đảm an toàn thông tin đối với hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu của trường ĐHCNTT.
   e) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin triển khai tại trường ĐHCNTT, báo cáo Hiệu trưởng trường ĐHCNTT điều chỉnh nếu cần thiết.
   f) Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn thông tin tại trường ĐHCNTT theo yêu cầu của Hiệu trưởng trường ĐHCNTT hoặc cơ quan quản lý nhà nước có thẩm quyền.
   g) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của nhà nước trong công tác bảo đảm an toàn thông tin.
   h) Các nhiệm vụ khác theo yêu cầu của Hiệu trưởng trường ĐHCNTT.
3. Phòng Dữ liệu & CNTT có trách nhiệm xây dựng kế hoạch và dự toán kinh phí thực hiện các nhiệm vụ nêu tại Khoản 2 Điều này trình Hiệu trưởng trường ĐHCNTT phê duyệt theo quy định.

Điều 18. Khen thưởng, xử lý vi phạm

1. Các đơn vị, cá nhân vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm có thể bị xử lý hành chính, xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định hiện

hành; nếu vi phạm gây thiệt hại lớn đến tài nguyên thông tin của trường ĐHCNTT thì phải chịu trách nhiệm về những thiệt hại gây ra theo quy định của pháp luật.

2. Việc giải quyết khiếu nại, tố cáo và tranh chấp được thực hiện theo quy định liên quan của pháp luật.

Điều 19. Điều khoản thi hành

Trong quá trình thực hiện Quy chế này, nếu có vướng mắc, các đơn vị, cá nhân phản ánh về Phòng Dữ liệu & CNTT để tổng hợp, báo cáo Hiệu trưởng trường ĐHCNTT xem xét sửa đổi, bổ sung Quy chế cho phù hợp.

HIỆU TRƯỞNG

Nguyễn Hoàng Tú Anh