ĐẠI HỌC QUỐC GIA TP.HCM
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

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

DỰ THẢO

QUY CHẾ
Bảo đảm an toàn thông tin, an ninh mạng của Trường Đại học Khoa học tự nhiên

(Kèm theo Quyết định số: /QĐ-KHTN ngày..... tháng....năm 2025 của Hiệu trưởng Trường Đại học Khoa học tự nhiên)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi áp dụng

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm đảm bảo an toàn thông tin, an ninh mạng của Trường Đại học Khoa học tự nhiên (sau đây gọi tắt là Trường) bao gồm:

a) Phạm vi quản lý về vật lý và logic của hệ thống;

b) Các ứng dụng, dịch vụ hệ thống cung cấp;

c) Nguồn nhân lực đảm bảo an toàn thông tin.

2. Đối tượng áp dụng

a) Các đơn vị thuộc và trực thuộc Trường (sau đây gọi chung là các đơn vị thuộc Trường); viên chức, người lao động, sinh viên và học viên của Trường.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin của Trường.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và đảm bảo an toàn thông tin mạng, phục vụ hoạt động của hệ thống thông tin của Trường.

Điều 2. Giải thích từ ngữ

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

1. An ninh mạng là sự bảo đảm an toàn, ổn định, bền vững của thông tin, hệ thống thông tin, không gian mạng và phòng, chống các hoạt động trên không gian mạng gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

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. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

4. Hệ thống thông tin là tập hợp 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 trên không gian mạng.

5. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

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.

7. Phần cứng độc hại là các bộ phận vật lý của hệ thống máy tính, hệ thống thông tin có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống máy tính, hệ thống thông tin hoặc thực hiện các hoạt động không được quyền đối với dữ liệu lưu trữ trong hệ thống thông tin.

8. Nhật ký hệ thống là hệ thống được thiết lập có chức năng ghi nhận, lưu trữ và có thể trích xuất dữ liệu phản ánh những sự kiện liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh mạng của hệ thống và dữ liệu do người dùng tạo ra trong quá trình sử dụng hệ thống, truy cập dịch vụ Internet.

9. Tội phạm sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội quy định trong Bộ luật Hình sự được thực hiện thông qua việc sử dụng công nghệ thông tin, mạng máy tính, Internet hoặc các thiết bị số nhằm mục đích lừa đảo, chiếm đoạt tài sản, xâm nhập hệ thống máy tính, phát tán thông tin độc hại hoặc gây thiệt hại cho cá nhân, tổ chức và xã hội.

10. Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của không gian mạng.

11. Khủng bố mạng là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.

12. Gián điệp mạng là hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia nhằm chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên không gian mạng của cơ quan, tổ chức, cá nhân Việt Nam.

13. Tài sản số là sản phẩm công nghệ số được tạo ra, phát hành, chuyển giao và xác thực quyền sở hữu bằng công nghệ chuỗi khối, có giá và quyền tài sản theo quy định của pháp luật về dân sự và pháp luật có liên quan.

14. Sự cố an ninh mạng là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

15. Mật mã dân sự là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

16. Dịch vụ an ninh mạng là dịch vụ bảo vệ thông tin, hệ thống thông tin và không gian mạng.

17. Nhà cung cấp dịch vụ là các doanh nghiệp, tổ chức, các nhân cung cấp các sản phẩm, dịch vụ trên không gian mạng, gồm: dịch vụ Internet (ISP), dịch vụ bưu chính, viễn thông, dịch vụ lưu trữ, máy chủ, tên miền, mạng riêng ảo (Virtual Private Network), máy chủ trung gian (Proxy), dịch vụ điện toán đám mây (Cloud Computing), mạng xã hội, trang thông tin điện tử, dịch vụ viễn thông, các tổ chứ tài chính, tín dụng, ngân hàng, chi nhánh ngân hàng nước ngoài tại Việt Nam, ví điện tử, trung gian thanh toán, các sàn giao dịch chứng khoán, sàn giao dịch tài sản số, sàn thương mại điện tử, dịch vụ vận chuyển (logistic), truyền hình số, trò chơi trực tuyến và các loại sản phẩm, dịch vụ khác trên không gian mạng.

18. Các thuật ngữ, tên công nghệ phổ biến được nêu trong Quy chế này:

– SSL (Secure Sockets Layer): Giao thức mã hóa kênh truyền thông tin nhằm thiết lập kết nối an toàn giữa máy chủ web (host) và trình duyệt web (client).

– TLS (Transport Layer Security): Giao thức Bảo mật tầng vận chuyển, giao thức mật mã cung cấp bảo mật đầu cuối cho dữ liệu được gửi giữa các ứng dụng qua Internet.

– SSH (Secure Shell): đây là một giao thức hỗ trợ các nhà quản trị mạng truy cập vào máy chủ từ xa thông qua mạng internet không bảo mật.

– VPN (Virtual Private Network): mạng riêng ảo, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu, để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

– LAN (Local Area Network - Mạng nội bộ): là hệ thống kết nối các thiết bị máy tính và thiết bị đầu cuối trong phạm vi địa lý hạn chế như văn phòng, tòa nhà hoặc khuôn viên, cho phép các thiết bị trao đổi dữ liệu và chia sẻ tài nguyên với nhau. Mạng nội bộ bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

– Địa chỉ IP (Internet Protocol) là một chuỗi số được gán cho mỗi thiết bị kết nối với mạng Internet hoặc mạng nội bộ, dùng để nhận diện và giao tiếp giữa các thiết bị.

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

1. Mục tiêu đảm bảo an toàn thông tin

Bảo vệ thông tin và hệ thống thông tin trên mạng khỏi các hành vi xâm nhập bất hợp pháp, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép, nhằm đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của hệ thống thông tin của Trường.

2. Nguyên tắc

a) Đơn vị, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm đảm bảo an toàn thông tin vào hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, theo hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Đảm bảo an toàn thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình thu thập, xây dựng, xử lý, truyền tải, lưu trữ và khai thác thông tin, dữ liệu; quá trình thiết kế, triển khai, vận hành, nâng cấp và tháo dỡ hệ thống thông tin.

c) Việc đảm bảo an toàn hệ thống thông tin của Trường 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 và lãng phí.

d) Các đơn vị thuộc Trường có trách nhiệm đảm bảo an toàn thông tin, an ninh mạng của đơn vị mình; bố trí nhân sự chịu trách nhiệm đảm bảo an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của Trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác đảm bảo an toàn thông tin, an ninh mạng.

Điều 4. Những hành vi nghiêm cấm

1. Sử dụng không gian mạng để thực hiện hành vi sau đây:

a) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm lãnh tụ, anh hùng dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

c) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng và các thông tin có nội dung vi phạm pháp luật khác;

đ) Xúi giục, lôi kéo, kích động người khác phạm tội.

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm sử dụng công nghệ cao.

3. Thực hiện các hành vi sau đây:

a) Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng;

b) Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an ninh mạng của hệ thống thông tin;

c) Tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin;

d) Phát tán thư rác, nội dung vi phạm quy định về quảng cáo, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo;

đ) Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin cá nhân của người khác;

e) Lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân;

g) Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân;

h) Tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự;

i) Sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

4. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của không gian mạng; phát tán chương trình tin học gây hại cho hoạt động của không gian mạng; xâm nhập trái phép vào thông tin, hệ thống thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

5. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

6. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

7. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ IP, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ.

8. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

9. Hành vi khác vi phạm quy định của Luật An ninh mạng.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Phòng Thông tin - Truyền thông là đơn vị vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung đặt tại phòng dữ liệu của Trường.

2. Phòng Thông tin - Truyền thông là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc đảm bảo an toàn, an ninh

mạng cho hệ thống thông tin của Trường.

3. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

Phòng Thông tin - Truyền thông:

+ Số điện thoại: (028).38300986

+ Email: netadmin@hcmus.edu.vn

Điều 6. Đảm bảo nguồn nhân lực

1. Trong quá trình làm việc

a) Trách nhiệm đảm bảo an toàn thông tin đối với người quản lý và vận hành hệ thống:

- 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.
- Tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Trách nhiệm đảm bảo an toàn thông tin đối với người sử dụng hệ thống:

- Có trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc.
- Phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin.
- 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.

c) Định kỳ hằng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức và đào tạo kỹ năng cơ bản về an toàn thông tin cho người sử dụng do đơn vị chức năng tổ chức.

2. Chấm dứt thay đổi công việc

a) Viên chức, người lao động chấm dứt hoặc thay đổi công việc phải thu hồi tài khoản 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 (nếu có) thuộc sở hữu của Trường.

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi viên chức thôi việc.

c) Lập biên bản bàn giao tài sản và tài khoản công nghệ thông tin (nếu có).

d) Cam kết giữ bí mật thông tin liên quan đến Trường sau khi nghỉ việc.

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

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Xây dựng 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 tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Xây dựng tài liệu mô tả phương án đảm bảo an toàn thông tin theo cấp độ.

4. Xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ đảm bảo an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

5. 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, báo cáo Lãnh đạo quyết định trước khi thực hiện

thay đổi.

Điều 8. Phát triển phần mềm

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với nhà thầu/bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.

5. Các quy định tại Điều này áp dụng chủ yếu cho các phần mềm được phát triển hoặc mua sắm để phục vụ công tác quản lý, vận hành chung của Nhà trường. Đối với các phần mềm, công cụ do cá nhân, nhóm nghiên cứu tự phát triển phục vụ trực tiếp cho hoạt động nghiên cứu, người phát triển cần tuân thủ các nguyên tắc lập trình an toàn và chịu trách nhiệm về an toàn thông tin của sản phẩm do mình tạo ra.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung, quy trình, có bộ phận chịu trách nhiệm 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. Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, có báo cáo nghiệm thu được chủ quản hệ thống thông tin phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

4. Bộ phận chuyên trách phối hợp với đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm nghiệm thu hệ thống.

5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Điều 10. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án đảm bảo an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và 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.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản có trách nhiệm thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ phù hợp theo quy định; triển khai các phương án đảm bảo an toàn hệ thống thông tin đáp ứng đầy đủ các yêu cầu cơ bản quy định tại tiêu chuẩn, quy chuẩn kỹ thuật về đảm bảo an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát tình trạng an toàn của hệ thống; tuân thủ đầy đủ quy trình vận hành và quy trình xử lý sự cố đã được ban hành; đồng thời thực hiện ghi nhật ký và lưu trữ đầy đủ thông tin hệ thống nhằm phục vụ công tác quản lý, giám sát và kiểm soát an toàn thông tin.

4. Các đơn vị thuộc Trường, các đơn vị có máy chủ đặt tại phòng dữ liệu phải có trách nhiệm yêu cầu các đối tác (nếu có) tuân thủ các quy định về đảm bảo an toàn thông tin của quy chế này cho toàn bộ hệ thống thông tin của Trường, tránh lộ, lọt dữ liệu, tài liệu

thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

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

Điều 11. Quản lý an toàn mạng

1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, đảm bảo tính sẵn sàng của hệ thống.

2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần hoặc theo quy định từng nội dung liên quan.

3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

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

a) Định kỳ hằng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như: ổ cứng di động hoặc thiết bị lưu trữ mạng (SAN), thiết bị lưu trữ gắn trực tiếp vào hệ thống (NAS) và các thiết bị lưu trữ khác.

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

6. Truy cập và quản lý cấu hình hệ thống:

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

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN và được mã hóa trên giao thức đường truyền theo đúng các quy định về bảo mật truy cập từ xa.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

d) Thiết lập, phân quyền đối với các tài khoản truy cập hệ thống và được sự đồng ý từ quản trị hệ thống.

đ) Ghi và lưu trữ nhật ký hệ thống trong thời gian tối thiểu 90 ngày với những thông tin cơ bản: tên tài khoản, địa chỉ, nhật ký hoạt động và thao tác, các lỗi phát sinh trong quá trình hoạt động...

Điều 12. Quản lý an toàn máy chủ và ứng dụng

Quy định về quản lý an toàn máy chủ và ứng dụng:

1. Quy định với máy chủ

a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, đảm bảo tính sẵn sàng của ứng dụng.

b) Ảnh máy chủ ảo phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần.

c) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của lãnh đạo đơn vị và xóa sạch dữ liệu.

e) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

2. Quy định với ứng dụng:

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, đảm bảo tính sẵn sàng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp đảm bảo an toàn ứng dụng và mã nguồn.

c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin tối thiểu 01 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.

3. Truy cập mạng của máy chủ:

a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.

b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).

c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN. Các máy tính truy cập từ xa phải đảm bảo an toàn bảo mật thông tin trên đường truyền kết nối và cài đặt các phần mềm anti-virus.

d) Phân quyền, quy định thời gian kết nối đối với các tài khoản kết nối.

4. Truy cập và quản trị máy chủ và ứng dụng:

a) Định kỳ từ 03 đến 06 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho viên chức quản trị theo chức năng nhiệm vụ được giao.

c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.

d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.

e) Các máy tính quản trị hệ thống phải cài đặt các phần mềm phòng chống mã độc có bản quyền (anti-virus) và phải quét mã độc trước khi kết nối vào hệ thống.

f) Phân quyền, quy định thời gian kết nối đối với các tài khoản quản trị.

5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hằng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

6. Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác

a) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu.

b) Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo quy định của Trường.

7. Đối với các hệ thống các đơn vị thì việc áp dụng cấp độ ATTT sẽ được xem xét dựa trên đặc thù kỹ thuật. Đơn vị quản lý thiết bị phải phối hợp với Phòng Thông tin - Truyền thông để xây dựng phương án theo cấp độ phù hợp và được phê duyệt bởi cấp có thẩm quyền.

Điều 13. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hằng tháng phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau.

2. Định kỳ hằng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

4. Bố trí máy tính riêng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác đảm bảo an toàn thông tin khi lưu trữ và truy cập cơ sở dữ liệu hệ thống.

5. Nghiêm cấm các hành vi chia sẻ các tài liệu, dữ liệu liên quan đến Hệ thống thông tin của Trường khi chưa được sự cho phép của lãnh đạo có thẩm quyền và chưa được mã hóa.

6. **Quản lý vòng đời và lưu trữ dài hạn dữ liệu nghiên cứu:**

a) Các đơn vị, nhóm nghiên cứu có trách nhiệm xây dựng kế hoạch quản lý dữ liệu cho các dự án, đề tài của mình, trong đó xác định rõ yêu cầu về phân loại, bảo vệ, lưu trữ và hủy dữ liệu.

b) Đối với các dữ liệu nghiên cứu có yêu cầu lưu trữ dài hạn, cần có phương án lưu trữ riêng biệt, đảm bảo tính toàn vẹn và khả năng truy xuất trong suốt thời gian quy định. Phòng Thông tin - Truyền thông phối hợp với các đơn vị để tư vấn và cung cấp giải pháp kỹ thuật phù hợp.

Điều 14. Quản lý an toàn thiết bị đầu cuối

1. Thông tin về thiết bị đầu cuối (tên máy tính, tài khoản, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

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 15. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm, người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm 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 hằng 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 16. Quản lý giám sát an toàn hệ thống thông tin

1. Các hệ thống thông tin đặt tại phòng dữ liệu bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện

việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

2. Chủ quản hệ thống thông tin có hệ thống đặt tại phòng dữ liệu phải tuân thủ quy định về đảm bảo an toàn thông tin tại Quy chế này và phối hợp với Phòng Thông tin- Truyền thông trong trường hợp xảy ra sự cố liên quan đến vấn đề an toàn, an ninh thông tin hệ thống đang vận hành.

3. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo đúng quy định tại 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 và hướng dẫn triển khai theo Công văn số 2973/BTTTT-CATTT ngày 04/9/2019 của Bộ Thông tin và Truyền thông.

4. Đối tượng giám sát về cơ bản bao gồm máy chủ, thiết bị mạng, thiết bị bảo mật, máy chủ, dịch vụ, ứng dụng, các thiết bị đầu cuối và điểm giám sát đường truyền, cụ thể: giám sát lớp mạng, giám sát lớp máy chủ, giám sát lớp ứng dụng và giám sát lớp đầu cuối.

5. Phải đảm bảo được thực hiện thường xuyên, liên tục. Chủ động theo dõi, phân tích, phòng ngừa nhằm kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

6. Đảm bảo ổn định, bí mật cho thông tin cung cấp, trao đổi trong quá trình giám sát.

Điều 17. Quản lý điểm yếu an toàn thông tin

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/Người 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 đảm bảo 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 18. 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; 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. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.

3. Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

4. Liên hệ với Phòng Thông tin - Truyền thông.

5. Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

Điều 19. Quản lý an toàn người sử dụng đầu cuối

1. Người sử dụng có trách nhiệm tự bảo vệ thông tin cá nhân của mình. Khi sử dụng, khai thác các hệ thống thông tin của đơn vị và các phần mềm ứng dụng dùng chung có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung, cơ quan, đơn vị.

c) Khi khai thác, sử dụng các phần mềm dùng chung tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

2. Đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các quy định:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi viên chức, người lao động đã nghỉ việc hoặc chuyển công tác, đơn vị phải thực hiện việc thu hồi các thiết bị công nghệ thông tin liên quan; đồng thời phải thông báo ngay bằng văn bản đến Phòng Thông tin - Truyền thông để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

3. Các đơn vị thuộc Trường phải thường xuyên kiểm tra, giám sát các 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.

4. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi.

Điều 20. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành hồ sơ quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Việc kiểm tra, đánh giá và quản lý rủi ro cần tuân thủ các nội dung sau:

a) Kiểm tra việc tuân thủ quy định của pháp luật về đảm bảo an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp đảm bảo an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản Hệ thống thông tin quy định.

Điều 21. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được viên chức vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra. giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị công nghệ thông tin: Máy tính cá nhân, máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 22. Trách nhiệm của Phòng Thông tin - Truyền thông

1. Thực hiện trách nhiệm theo quy định tại Điều 21, Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ. Đồng thời thực hiện các quy định cụ thể như sau:

a) Chủ trì, hướng dẫn các đơn vị triển khai thực hiện Quy chế này và các quy định có liên quan đến an toàn thông tin, an ninh mạng;

b) Xây dựng kế hoạch kiểm tra, đánh giá hàng năm tình hình an toàn thông tin, an ninh mạng tại đơn vị;

c) Là đầu mối đại diện cho Trường tham gia các hoạt động, công tác bảo đảm an toàn thông tin, an ninh mạng khi có yêu cầu của cấp trên;

d) Tổng hợp, báo cáo Trường về an toàn thông tin, an ninh mạng.

2. Giao Phòng Thông tin - Truyền thông thực hiện vai trò chuyên trách về an toàn thông tin,an ninh mạng. Phòng Thông tin - Truyền thông phối hợp với các đơn vị trong Trường thực hiện các công tác bảo đảm an toàn thông tin cho hệ thống công nghệ thông tin của Trường.

Điều 23. Trách nhiệm của viên chức, người lao động, người học của Trường

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về an toàn thông tin tại Quy chế này.

Điều 24. Trách nhiệm của các cơ quan, đơn vị, tổ chức có liên quan

Các cơ quan, đơn vị, tổ chức có liên quan khi thuê các dịch vụ phần mềm, cơ sở dữ liệu, hệ thống thông tin, dịch vụ vận hành, đặt chỗ máy chủ tại phòng dữ liệu phải tuân thủ theo các quy định tại quy chế này về quản lý tài khoản, phiên đăng nhập, phân quyền của Phòng Thông tin - Truyền thông; chịu trách nhiệm với nội dung, dữ liệu hệ thống do đơn vị mình tạo ra, cung cấp phát tán trên môi trường mạng theo quy định pháp luật.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 25. Trách nhiệm thi hành

1. Các cá nhân, bao gồm viên chức, người lao động, người học thuộc trường Trường chịu 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 đảm bảo 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.

2. Lãnh đạo các đơn vị thuộc Trường có trách nhiệm quán triệt, chỉ đạo và giám sát viên chức, người lao động và người học thuộc đơn vị mình thực hiện đúng nội dung Quy chế này:

a) Chỉ đạo, đảm bảo việc tuân thủ các quy định của Quy chế trong phạm vi tổ chức, quyền hạn của mình và thực hiện báo cáo theo yêu cầu của đơn vị chuyên trách về công nghệ thông tin của Trường.

b) Căn cứ vào Quy chế này và nhu cầu thực tế, xây dựng hoặc rà soát, sửa đổi phương án quản lý an toàn thông tin của đơn vị cho phù hợp.

c) Tuyên truyền, phổ biến nội dung Quy chế này đến từng cá nhân trong đơn vị, đồng thời nâng cao nhận thức của họ về các nguy cơ mất an toàn thông tin.

d) Phối hợp, cung cấp thông tin và tạo điều kiện thuận lợi để các đơn vị chuyên trách triển khai công tác kiểm tra, khắc phục sự cố một cách kịp thời và hiệu quả.

3. Trách nhiệm Phòng thông tin - Truyền thông:

a) Tham mưu cho Ban Giám hiệu trong việc xây dựng mới, sửa đổi, bổ sung các quy định, chính sách an toàn thông tin, an ninh mạng trong trường.

b) Chủ trì, phối hợp với các đơn vị liên quan để tổ chức phổ biến, hướng dẫn, kiểm tra và giám sát việc thực hiện Quy chế, định kỳ báo cáo Ban Giám hiệu về tình hình thực hiện.

c) Tổ chức tuyên truyền nhằm nâng cao nhận thức về việc gắn kết công tác đảm bảo an toàn thông tin với việc triển khai ứng dụng công nghệ thông tin.

d) Thực hiện xác định cấp độ an toàn hệ thống thông tin của Trường và các đơn vị.

e) Triển khai các biện pháp đảm bảo an toàn thông tin đối với hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu của Trường.

f) Định kỳ hoặc đột xuất đánh giá hiệu quả của các biện pháp đảm bảo an toàn thông tin đã triển khai, báo cáo Ban Giám hiệu điều chỉnh nếu cần thiết.

g) Thực hiện báo cáo công tác đảm bảo an toàn thông tin theo yêu cầu của Ban Giám hiệu hoặc cơ quan quản lý nhà nước có thẩm quyền.

h) Phối hợp và thực hiện các yêu cầu của cơ quan chức năng nhà nước trong công tác đảm bảo an toàn thông tin.

Điều 26. Khen thưởng và xử lý vi phạm

1. Khen thưởng

Các đơn vị, tổ chức, viên chức, người lao động, người học thuộc Trường có đóng góp, thành tích vào công tác xây dựng, triển khai, tuân thủ quy chế bảo mật, tùy theo mức độ đóng góp, sẽ được xem xét, đề xuất khen thưởng kịp thời theo quy định.

2. Xử lý vi phạm

Các đơn vị, tổ chức, viên chức, người lao động, người học thuộc Trường vi phạm Quy chế này hoặc các quy định pháp luật có liên quan về an toàn thông tin, thì tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật.

Nếu hành vi vi phạm gây thiệt hại đến tài sản, thiết bị, dữ liệu trên mạng Trường thì phải chịu trách nhiệm bồi thường theo quy định của pháp luật.

Điều 27. Rà soát, cập nhật, bổ sung Quy chế

Phòng Thông tin - Truyền thông xây dựng kế hoạch thực hiện:

1. Định kỳ 01 năm hoặc khi có quy định, chính sách mới cần điều chỉnh, bổ sung Quy chế bảo đảm an toàn thông tin, an ninh mạng, Phòng Thông tin - Truyền thông tham mưu rà soát, cập nhật, bổ sung quy chế phù hợp.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

3. Phổ biến đến toàn thể viên chức, người lao động, người học của Trường và cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin của Trường.

Trong quá trình tổ chức thực hiện, nếu có những khó khăn, vướng mắc, các đơn vị, cá nhân cần phản ánh ngay với Phòng Thông tin - Truyền thông để tổng hợp, trình Hiệu trưởng xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.