VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1263/QĐ-KHXH	*Hà Nội, ngày 19 tháng 11 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế Bảo đảm an toàn thông tin, an ninh mạng tại Viện Hàn lâm Khoa học xã hội Việt Nam

CHỦ TỊCH VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM

Căn cứ Luật an ninh mạng năm 2018;

Căn cứ Luật an toàn thông tin mạng năm 2018;

Căn cứ Nghị định số 108/2022/NĐ-CP ngày 28/12/2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Viện Hàn lâm Khoa học xã hội Việt Nam;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật an ninh mạng;

Theo đề nghị của Giám đốc Trung tâm Ứng dụng công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Bảo đảm an toàn thông tin, an ninh mạng tại Viện Hàn lâm Khoa học xã hội Việt Nam.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký, thay thế Quyết định số 2274/QĐ-KHXH ngày 07/11/2016 của Chủ tịch Viện Hàn lâm Khoa học xã hội Việt Nam ban hành Quy chế đảm bảo an toàn an ninh thông tin trong lĩnh vực công nghệ thông tin của Viện Hàn lâm Khoa học xã hội Việt Nam.

Điều 3. Giám đốc Trung tâm Ứng dụng công nghệ thông tin, Chánh Văn phòng Viện Hàn lâm, Trưởng ban Ban Kế hoạch - Tài chính, Thủ trưởng các đơn vị thuộc, trực thuộc Viện Hàn lâm Khoa học xã hội Việt Nam chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Viện Hàn lâm;
- Ban Chỉ đạo CĐS Viện Hàn lâm;
- Bộ Thông tin và Truyền thông (để biết);
- Lưu: VT, Trung tâm UDCNTT.

CHỦ TỊCH

VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM

Phan Chí Hiếu

VIỆN HÀN LÂM
KHOA HỌC XÃ HỘI VIỆT NAM

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

QUY CHẾ
Bảo đảm an toàn thông tin, an ninh mạng tại Viện Hàn lâm Khoa học xã hội Việt Nam

(Ban hành kèm theo Quyết định số 1263/QĐ-KHXH ngày 19 tháng 11 năm 2024 của Chủ tịch Viện Hàn lâm Khoa học xã hội Việt Nam)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về việc bảo đảm an toàn thông tin, an ninh mạng trong các hoạt động của Viện Hàn lâm Khoa học xã hội Việt Nam (sau đây gọi tắt là Viện Hàn lâm).

2. Quy chế này được áp dụng đối với: các đơn vị thuộc, trực thuộc Viện Hàn lâm (sau đây gọi tắt là đơn vị); viên chức, người lao động của các đơn vị; tổ chức, cá nhân có hoạt động, thiết bị kết nối vào hệ thống mạng của Viện Hàn lâm; tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin (CNTT) cho các đơn vị.

Điều 2. Mục đích, yêu cầu

Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm thiểu các nguy cơ gây mất an toàn thông tin, an ninh mạng trong các hoạt động của Viện Hàn lâm; thống nhất nguyên tắc, yêu cầu, cách thức, quy trình thực hiện bảo đảm an toàn thông tin, an ninh mạng tại Viện Hàn lâm; phân định vai trò, trách nhiệm của cá nhân, đơn vị thuộc, trực thuộc Viện Hàn lâm liên quan đến công tác bảo đảm an toàn thông tin, an ninh mạng.

Điều 3. Giải thích từ ngữ

1. *An toàn thông tin* là sự bảo vệ thông tin điện tử, hệ thống thông tin điện tử 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. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không 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.

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

4. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán (máy chủ, máy trạm), lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng...

5. *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 điện tử.

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. *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.

8. *Bộ phận chuyên trách CNTT* là bộ phận (hoặc cán bộ) được giao phụ trách công tác đảm bảo hạ tầng, ứng dụng và an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống CNTT.

9. *Đơn vị chủ quản hệ thống thông tin/đơn vị chủ quản trung tâm dữ liệu, phòng máy chủ* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Tại Viện Hàn lâm là các đơn vị thuộc và trực thuộc có hệ thống thông tin riêng của đơn vị.

10. *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 thì đơn vị vận hành là bên cung cấp dịch vụ.

11. *Thiết bị CNTT* là các thiết bị bao gồm các máy chủ, máy tính, laptop, thiết bị tường lửa, thiết bị định tuyến, thiết bị lưu trữ, thiết bị chuyển mạch, thiết bị wifi, thiết bị ngoại vi (máy in, máy photo, máy Scan, máy chiếu,...).

Điều 4. Nguyên tắc bảo đảm an toàn thông tin, an ninh mạng

1. Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn thông tin, an ninh mạng thông tin tuân thủ các nguyên tắc chung quy định tại Luật An toàn thông tin mạng, Luật An ninh mạng, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về quy định chi tiết một số điều của Luật An ninh mạng (sau đây gọi tắt là Nghị định số 53/2022/NĐ-CP) và 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 (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP) và các quy định pháp luật khác có liên quan.

2. Tuân thủ các quy định và hướng dẫn về bảo đảm an toàn thông tin, an ninh mạng của cơ quan có thẩm quyền.

3. Trách nhiệm bảo đảm an toàn thông tin và an ninh mạng gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan. Cá nhân quản lý, sử dụng có trách nhiệm đảm bảo an toàn thông tin mạng trong phạm vi xử lý công việc của mình theo quy định pháp luật, quy định của đơn vị và Viện Hàn lâm.

Cá nhân quản lý, sử dụng có trách nhiệm đảm bảo an toàn thông tin mạng trong phạm vi xử lý công việc của mình theo quy định pháp luật, quy định của đơn vị và Viện Hàn lâm.

4. Việc bảo đảm an toàn hệ thống thông tin 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. Các nhiệm vụ, dự án ứng dụng CNTT hoặc có cấu phần CNTT thuộc phạm vi quy định tại khoản 1 và khoản 2 Điều 1 của Nghị định 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước phải có ý kiến thẩm định nội dung liên quan đến an toàn thông tin, an ninh mạng, phê duyệt hồ sơ cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước khi được phê duyệt.

5. Quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước.

6. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 5. Các hành vi bị cấm

1. Làm ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc khả năng truy nhập hệ thống thông tin.

2. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin, phá hoại hệ thống thông tin.

3. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

4. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

5. Các hành vi bị nghiêm cấm quy định tại Điều 8 Luật An ninh mạng.

Chương II
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 6. Bảo đảm an toàn thông tin đối với thiết bị công nghệ thông tin

1. Các đơn vị phải giao, gắn trách nhiệm cho cá nhân hoặc tập thể trực tiếp quản lý, sử dụng thiết bị CNTT.

2. Các đơn vị phải quy định các quy tắc sử dụng, bảo vệ thiết bị CNTT trong các trường hợp như: mang thiết bị ra khỏi cơ quan, cài đặt và cấu hình thiết bị.

3. Khi thay đổi mục đích sử dụng hoặc thanh lý thiết bị CNTT có lưu trữ dữ liệu quan trọng, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên thiết bị CNTT.

4. Thiết bị CNTT có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài đơn vị hoặc ngừng sử dụng phải 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).

5. Các đơn vị có trách nhiệm 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 CNTT 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 đối với trung tâm dữ liệu, phòng máy chủ

1. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong trung tâm dữ liệu, phòng máy chủ tuân thủ tiêu chuẩn kỹ thuật liên quan và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập, biện pháp kiểm soát truy nhập. Đơn vị chủ quản trung tâm dữ liệu, phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

2. Trung tâm dữ liệu, phòng máy chủ là khu vực hạn chế tiếp cận 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. Việc vào, ra khu vực này phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học,...).

3. 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 15 phút khi có sự cố mất điện.

4. Trung tâm dữ liệu, phòng máy chủ phải có hệ thống làm mát điều hòa không khí, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp. Đơn vị chủ quản phải phân công cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu, phòng máy chủ.

Điều 8. Bảo đảm an toàn thông tin đối với hạ tầng mạng

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản với các chính sách an toàn thông tin riêng, bao gồm: 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 hệ thống các thiết bị mạng, thiết bị bảo mật.

2. 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: có hệ thống tường lửa và hệ thống bảo vệ truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng; có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ; Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

3. Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập, đơn vị vận hành phải thiết lập các tham số mật khẩu truy cập có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %), cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

Điều 9. Bảo đảm an toàn thông tin đối với máy tính và thiết bị công nghệ thông tin

1. Các phần mềm, ứng dụng được cài đặt trên máy tính, thiết bị CNTT phải có nguồn gốc rõ ràng, chính thống. Các phần mềm, ứng dụng phải được cài đặt chế độ

tự động cập nhật thường xuyên. Các cá nhân không được tự ý cài đặt hay gỡ bỏ các phần mềm, ứng dụng trên máy tính, thiết bị CNTT dùng chung mà không được sự đồng ý của lãnh đạo đơn vị hoặc bộ phận chuyên trách về CNTT.

2. Tất cả các máy tính, thiết bị CNTT phải được cài đặt phần mềm phòng chống mã độc, thiết lập mật khẩu truy nhập, thiết lập chế độ tự động bảo vệ màn hình sau khoảng thời gian không sử dụng, sử dụng trình duyệt an toàn.

3. Khi phát hiện dấu hiệu liên quan đến nhiễm phần mềm độc hại trên các máy tính, thiết bị CNTT, cá nhân sử dụng phải thực hiện ngắt mạng nội bộ, thông báo trực tiếp cho bộ phận chuyên trách về CNTT để được hỗ trợ kịp thời.

4. Cá nhân sử dụng máy tính, thiết bị CNTT chỉ truy cập vào các website chính thống để trao đổi thông tin theo đúng nhiệm vụ, quyền hạn của mình; đồng thời, có trách nhiệm bảo mật thông tin tài khoản cá nhân trên mạng xã hội, thư điện tử, ứng dụng trên mạng internet.

Điều 10. Bảo đảm an toàn thông tin mức ứng dụng

1. 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 nội bộ tại các đơn vị.

2. Các phần mềm, ứng dụng nội bộ của các đơn vị phải đáp ứng các yêu cầu sau:

a) Có cấu hình xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống.

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

c) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách CNTT quản lý.

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

đ) Được kiểm tra, phát hiện và khắc phục các điểm yếu về an toàn, an ninh

thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.

Điều 11. Bảo đảm an toàn thông tin mức dữ liệu

1. Các đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động nghiệp vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên thiết bị lưu trữ dữ liệu; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

2. Các đơn vị cần triển khai hệ thống 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 theo từng loại, nhóm thông tin; 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, thông tin nghiệp vụ.

3. Các đơn vị phải bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ thông tin, dữ liệu và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

4. Các đơn vị 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 khích việc sử dụng mật khẩu bảo vệ khi chia sẻ, gửi, nhận thông tin, dữ liệu trên môi trường mạng.

5. 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. 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 12. Bảo đảm an toàn thông tin mức hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin, bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và trình tự, thủ tục xác định cấp độ hệ thống thông tin tuân thủ theo quy định tại Nghị định số 85/2016/NĐ-CP.

2. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện 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; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

3. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, đơn vị chủ quản hệ thống thông tin phải rà soát cấp độ, phương án bảo đảm 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.

4. Các đơn vị liên quan đến việc phát triển phần mềm, ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác đảm bảo an toàn thông tin, 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.

5. Quản lý tài khoản truy cập

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 sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu.

Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì cơ quan, đơn vị quản lý cá nhân đó phải thông báo cơ quan, 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.

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 hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

Mật khẩu đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc

biệt như !, @, #, $, %,...).

Điều 13. Giám sát, kiểm tra, đánh giá an toàn thông tin mạng

1. Các đơn vị chủ quản hệ thống thông tin phải thực hiện giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý; phối hợp với Trung tâm Ứng dụng CNTT và các đơn vị chức năng của Bộ Thông tin và Truyền thông thực hiện giám sát theo quy định.

2. Trung tâm Ứng dụng CNTT và bộ phận chuyên trách về an toàn thông tin của các đơn vị thực hiện việc kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

Điều 14. Ứng cứu sự cố an toàn thông tin mạng

1. Ban chỉ đạo, đơn vị chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

a) Ban Chỉ đạo chuyển đổi số Viện Hàn lâm đảm nhiệm chức năng Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của Viện Hàn lâm. Trách nhiệm và quyền hạn liên quan đến ứng cứu khẩn cấp sự cố an toàn thông tin mạng của Ban Chỉ đạo chuyển đổi số Viện Hàn lâm được quy định tại Khoản 2, Điều 5 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 Thủ tướng Chính phủ: Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg).

b) Trung tâm Ứng dụng CNTT là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Viện Hàn lâm. Bộ phận chuyên trách về an toàn thông tin mạng tại các đơn vị đảm nhiệm vai trò chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý CNTT của đơn vị. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

2. Kế hoạch ứng phó sự cố an toàn thông tin mạng

a) Các đơn vị tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố an toàn thông tin mạng cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định, đơn vị lấy ý kiến của Trung tâm Ứng dụng CNTT, Ban Kế hoạch - Tài chính (đối với các nội dung yêu cầu có kinh phí), báo cáo Viện Hàn lâm xem xét, quyết định.

b) Các kế hoạch ứng phó sự cố an toàn thông tin mạng sau khi được phê duyệt phải gửi Trung tâm Ứng dụng CNTT tổng hợp thành kế hoạch chung của

Viện Hàn lâm. Trung tâm Ứng dụng CNTT có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Viện Hàn lâm, trình Lãnh đạo Viện Hàn lâm phê duyệt.

c) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn, an ninh thông tin năm tiếp theo.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng

a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công mạng hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin liên quan và Trung tâm Ứng dụng CNTT. Trung tâm Ứng dụng CNTT có trách nhiệm cập nhật, công khai thông tin liên lạc, đường dây nóng của bộ phận tiếp nhận thông tin sự cố của Viện Hàn lâm và của các đơn vị trên Cổng thông tin điện tử Viện Hàn lâm.

b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a Khoản 1 Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9 Thông tư số 20/2017/TT-BTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc (sau đây gọi tắt là Thông tư số 20/2017/TT-BTTT), đồng thời thông báo Trung tâm Ứng dụng CNTT để tổng hợp, báo cáo Ban Chỉ đạo chuyển đổi số Viện Hàn lâm. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng tuân thủ quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

4. Diễn tập ứng cứu sự cố an toàn thông tin mạng

a) Đơn vị chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt.

b) Trung tâm Ứng dụng CNTT chủ trì, phối hợp với các đơn vị tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập ứng cứu sự cố trong phạm vi Viện Hàn lâm.

Điều 15. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng

1. Đơn vị chuyên trách an toàn thông tin mạng của chủ quản hệ thống thông tin phối hợp với đơn vị vận hành hệ thống thông tin thực hiện các nhiệm vụ sau trong phạm vi hệ thống thông tin thuộc quản lý của chủ quản hệ thống thông tin, theo quy định của Luật An ninh mạng và Nghị định số 53/2022/NĐ-CP:

a) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung: tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống cá nhân, tổ chức; xâm phạm trật tự quản lý kinh tế trên hệ thống thông tin.

b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hoạt động xâm nhập bất hợp pháp, hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này.

c) Áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng đối với hệ thống thông tin; Thường xuyên rà soát, kiểm tra hệ thống thông tin nhằm loại trừ nguy cơ khủng bố mạng.

d) Phối hợp, thực hiện yêu cầu của Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời tư trên hệ thống thông tin; về áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội; về gỡ bỏ các nội dung buộc phải gỡ bỏ theo quy định của pháp luật trên hệ thống thông tin; về thực hiện biện pháp phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

2. Đơn vị chuyên trách an toàn thông tin mạng của chủ quản hệ thống thông tin khi tiếp nhận tin báo về tình huống nguy hiểm về an ninh mạng hoặc khủng bố mạng liên quan đến hệ thống thông tin thuộc phạm vi quản lý của chủ quản hệ thống thông tin, cần thông báo kịp thời cho Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao.

3. Chủ quản hệ thống thông tin có trách nhiệm thông báo cho Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

Chương III
TRÁCH NHIỆM CỦA CÁC ĐƠN VỊ THUỘC, TRỰC THUỘC VIỆN HÀN LÂM

Điều 16. Trách nhiệm của các đơn vị thuộc, trực thuộc, các tổ chức chính trị, chính trị - xã hội của Viện Hàn lâm

1. Thực hiện các trách nhiệm được giao tại Quy chế này.

2. Thực hiện các báo cáo theo quy định, gửi Viện Hàn lâm (qua Trung tâm Ứng dụng Công nghệ thông tin).

3. Triển khai quy chế bảo đảm an toàn thông tin, an ninh mạng tại đơn vị bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.

4. Thực hiện việc quản lý thiết bị CNTT và viên chức, người lao động theo Quy chế này.

5. Phối hợp với Trung tâm Ứng dụng Công nghệ thông tin bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Viện Hàn lâm và các hệ thống thông tin do đơn vị quản lý, vận hành.

6. Thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn thông tin, an ninh mạng tại đơn vị, coi đây là nhiệm vụ trọng tâm của đơn vị.

8. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn thông tin, an ninh mạng đến toàn thể viên chức và người lao động tại đơn vị.

Điều 17. Trách nhiệm của Trung tâm Ứng dụng Công nghệ thông tin

1. Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP và Quy chế này.

2. Hướng dẫn triển khai Quy chế này và các quy định liên quan của Nhà nước.

3. Xây dựng kế hoạch, báo cáo về an toàn thông tin, an ninh mạng của Viện Hàn lâm.

4. Bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Viện Hàn lâm.

5. Đôn đốc, giám sát, kiểm tra và báo cáo Viện Hàn lâm việc thực hiện Quy chế này tại các đơn vị.

6. Xây dựng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin, an ninh mạng tại Viện Hàn lâm và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

7. Phối hợp với Ban Tổ chức - Cán bộ xây dựng, trình Viện Hàn lâm phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn thông tin, an ninh mạng cho viên chức và người lao động của Viện Hàn lâm và tổ chức đào tạo theo kế hoạch đã phê duyệt.

Điều 18. Trách nhiệm của chủ quản hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị chủ quản hệ thống thông tin theo quy

định tại Điều 20 Nghị định số 85/2016/NĐ-CP và Quy chế này.

2. Chỉ đạo, phân công các đơn vị vận hành các hệ thống thông tin triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 19. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 20. Trách nhiệm cá nhân

1. Thủ trưởng đơn vị có trách nhiệm: phổ biến tới từng viên chức, người lao động của đơn vị, tổ chức triển khai và thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Viện Hàn lâm về các vi phạm, thất thoát thông tin, dữ liệu bảo mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Viên chức, người lao động của Viện Hàn lâm có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin, an ninh mạng cho bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu bảo mật của Viện Hàn lâm do không tuân thủ Quy chế.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 21. Kinh phí thực hiện

Kinh phí bảo đảm an toàn thông tin, an ninh mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Viện Hàn lâm.

Căn cứ nhiệm vụ được giao, các đơn vị thực hiện lập dự toán, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin, an ninh mạng theo quy định của Luật Ngân sách Nhà nước.

Điều 22. Khen thưởng và xử lý vi phạm

1. Tổ chức, cá nhân thực hiện tốt nhiệm vụ bảo đảm an toàn thông tin, an ninh

mạng được xem xét để khen thưởng hàng năm theo quy định.

2. Đơn vị, tổ chức, cá nhân có hành vi vi phạm các quy định về bảo đảm an toàn thông tin, an ninh mạng, gây ảnh hưởng tới hoạt động của Viện Hàn lâm, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

Điều 23. Trách nhiệm thi hành và sửa đổi, bổ sung

Quy chế này gồm 04 Chương, 23 Điều và có hiệu lực kể từ ngày ký ban hành. Tất cả viên chức và người lao động trong Viện Hàn lâm có trách nhiệm thực hiện nghiêm chỉnh và đầy đủ các điều khoản của Quy chế này.

Trường hợp quy định tại các văn bản dẫn chiếu trong Quy chế này được sửa đổi, bổ sung, thay thế hoặc bãi bỏ bằng văn bản mới thì thực hiện theo quy định tại văn bản mới.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các đơn vị, tổ chức, cá nhân phản ánh về Trung tâm Ứng dụng Công nghệ thông tin để tổng hợp, báo cáo Chủ tịch Viện Hàn lâm xem xét, sửa đổi, bổ sung cho phù hợp./.