VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập -Tự do - Hạnh phúc
Số: 1304/QĐ-KHXH	*Hà Nội, ngày 31 tháng 10 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh mạng cho Hệ thống Trung tâm dữ liệu của Viện Hàn lâm Khoa học xã hội Việt Nam

CHỦ TỊCH VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/218;

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

Căn cứ 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;

Căn cứ Nghị định số 32/2025/NĐ-CP ngày 25/02/2025 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 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP.

Theo đề nghị của Chánh Văn phòng Viện Hàn lâm Khoa học xã hội Việt Nam.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế Bảo đảm an toàn, an ninh mạng cho Hệ thống Trung tâm dữ liệu của Viện Hàn lâm Khoa học xã hội Việt Nam".

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

Điều 3. Chánh Văn phòng, Thủ trưởng các đơn vị thuộc, trực thuộc Viện Hàn lâm Khoa học xã hội Việt Nam và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Viện Hàn lâm;
- Lưu: VT, VP.

CHỦ TỊCH

VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM

Lê Văn Lợi

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, an ninh mạng cho Hệ thống Trung tâm dữ liệu của Viện Hàn lâm Khoa học xã hội Việt Nam

(Ban hành kèm theo Quyết định số 1504/QĐ-KHXH ngày 31 tháng 10 năm 2025 của Chủ tịch Viện Hàn lâm Khoa học xã hội Việt Nam)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các yêu cầu trong công tác quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống Trung tâm dữ liệu của Viện Hàn lâm Khoa học xã hội Việt Nam (Viện Hàn lâm) bao gồm: Phạm vi quản lý về vật lý và logic tại Trung tâm dữ liệu của Viện Hàn lâm; Các ứng dụng, dịch vụ hệ thống cung cấp; Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

a) Các đơn vị thuộc, trực thuộc Viện Hàn lâm; viên chức, người lao động của đơn vị.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống Trung tâm dữ liệu

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

Điều 2. Giải thích từ ngữ

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

STT	Thuật ngữ viết tắt	Giải thích
1	Viện Hàn lâm	Viện Hàn lâm Khoa học xã hội Việt Nam
2	Văn phòng	Văn phòng Viện Hàn lâm
3	Bộ KHCN	Bộ Khoa học và Công nghệ
4	ATTT	An toàn thông tin
5	CNTT	Công nghệ thông tin

6	VPN (Virtual Private Network)	Mạng riêng ảo
7	NOC (Network Operation Center)	Trung tâm điều hành mạng
8	SOC (Security Operation Center)	Trung tâm điều hành an ninh mạng
9	MAC (Media Access Control Address)	Địa chỉ kiểm soát truy cập
10	IP (Internet Protocol)	Giao thức Internet
11	CPU (Central Processing Unit)	Bộ xử lý trung tâm
12	RAM (Random Access Memory)	Bộ nhớ truy cập ngẫu nhiên
13	DNS (Domain Name System)	Hệ thống tên miền
14	NTP (Network Time Protocol)	Giao thức đồng bộ thời gian mạng
15	DHCP (Dynamic Host Configuration Protocol)	Giao thức cấp phát địa chỉ IP động

Điều 3. Mục đích, yêu cầu

1. Mục đích bảo đảm an toàn thông tin.

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin Hệ thống Trung tâm dữ liệu

2. Yêu cầu

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

b) Bảo đảm ATTT là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong các quá trình như sau:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm ATTT Hệ thống được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

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

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

a) Viện Hàn lâm giao Văn phòng Viện Hàn lâm là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống Trung tâm dữ liệu của Viện Hàn lâm Khoa học xã hội Việt Nam.

b) Văn phòng Viện Hàn lâm làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống Trung tâm dữ liệu.

2. Đơn vị chuyên trách có trách nhiệm bố trí 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: Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

3. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

a) Văn phòng Viện Hàn lâm chịu trách nhiệm phối hợp với Ban Tổ chức cán bộ về việc tuyển dụng cán bộ vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;

b) Việc tuyển dụng phải thực hiện theo đúng quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

2. Trong quá trình làm việc

a) Cán bộ phụ trách, chuyên trách chịu trách nhiệm thực hiện theo đúng nội quy, quy chế bảo đảm an toàn thông tin trong việc quản lý và vận hành hệ thống;

b) Đơn vị chuyên trách chịu trách nhiệm xây dựng kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

c) Văn phòng chịu trách nhiệm xây dựng kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống của Viện Hàn lâm.

3. Chấm dứt thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi tài khoản, 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 tổ chức;

b) Cán bộ quản lý thực hiện quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c) Cán bộ chấm dứt hoặc thay đổi công việc phải cam kết giữ bí mật thông tin liên quan đến tổ chức 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. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

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

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

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.

Điều 8. Phát triển phần mềm thuê khoán

1. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

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.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

4. Có 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 và 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.

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

Điều 10. Quản lý an toàn mạng

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

a) Bộ phận NOC thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của các thiết bị hệ thống;

b) Giải pháp giám sát hệ thống thông tin tập trung phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thiết bị hệ thống bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của thiết bị hệ thống, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực.

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

a) Định kỳ hàng tháng hoặc khi có thay đổi cấu hình thiết bị hệ thống, toàn bộ tập tin cấu hình thiết bị hệ thống được sao lưu dự phòng trên thiết bị và hệ thống lưu trữ độc lập;

b) Tệp tin cấu hình của toàn bộ thiết bị hệ thống phải được sao lưu dự phòng theo từng phiên bản khác nhau, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn;

c) Sơ đồ thiết kế hệ thống về logic và vật lý phải được cập nhật khi có sự thay đổi về thiết kế và được sao lưu dự phòng theo từng phiên bản khác nhau, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn;

d) Có thiết bị hoặc thiết lập hệ thống, phân vùng lưu trữ độc lập để lưu trữ tệp tin cấu hình, sơ đồ hệ thống và các dữ liệu khác phục vụ quản lý an toàn mạng; dữ liệu được lưu trữ phải được phân loại và gán nhãn dữ liệu, được mã hóa và lưu trữ cùng mã kiểm tra tính nguyên vẹn.

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

a) Chỉ cho phép truy cập, cấu hình thiết bị hệ thống từ vùng mạng quản trị;

b) Truy cập, cấu hình thiết bị hệ thống từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng;

d) Toàn bộ thao tác thay đổi, thiết lập cấu hình thiết bị hệ thống phải được ghi nhật ký hệ thống;

đ) Hệ thống thông tin cấp độ 2 trở lên, khi thực hiện truy cập, cấu hình thiết bị hệ thống phải thông qua hệ thống quản lý tài khoản đặc quyền.

4. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào vận hành, khai thác.

5. Hoạt động quản lý an toàn mạng thực hiện theo Quy trình quản lý điểm yếu an toàn thông tin, ban hành kèm theo Quy chế này tại Phụ lục I.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

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

a) Bộ phận NOC thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của hệ thống máy chủ và ứng dụng;

b) Tối thiểu các thông tin về hoạt động của máy chủ và ứng dụng, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU, RAM, Storage) và lưu lượng mạng xử lý theo thời gian thực.

2. Truy cập mạng của máy chủ:

a) Tường lửa hệ thống và tường lửa máy chủ phải được thiết lập để quản lý kết nối mạng từ các địa chỉ bên ngoài vào máy chủ theo ứng dụng, dịch vụ máy

chủ cung cấp và địa chỉ nguồn truy cập. Các dịch vụ khác, không sử dụng phải vô hiệu hóa và chặn kết nối từ bên ngoài;

b) Tường lửa hệ thống và tường lửa máy chủ phải được thiết lập để quản lý kết nối mạng từ máy chủ đi ra các mạng bên ngoài; chỉ mở truy cập máy chủ theo hướng đi ra đối với các dịch vụ cơ bản như DNS, NTP, các kết nối khắc phục cập nhật hệ điều hành và các dịch vụ nghiệp vụ cụ thể mà máy chủ yêu cầu phải kết nối ra bên ngoài.

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

a) Chỉ cho phép truy cập, cấu hình máy chủ từ vùng mạng quản trị; cấu hình ứng dụng từ vùng mạng quản trị hoặc nghiệp vụ;

b) Truy cập, cấu hình máy chủ và ứng dụng từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng.

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

a) Khi có thay đổi, cập nhật cấu hình, mã nguồn ứng dụng, toàn bộ tập tin cấu hình, mã nguồn ứng dụng phải được sao lưu dự phòng trên thiết bị và hệ thống lưu trữ độc lập;

b) Thực hiện lưu trạng thái ảnh của hệ điều hành ảo hóa (take snapshot) tại thời điểm trước và sau khi cập nhật máy chủ và ứng dụng;

c) Định kỳ hàng tháng lưu trữ ảnh của hệ điều hành máy chủ trên thiết bị và hệ thống lưu trữ độc lập.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng.

a) Trước khi cài đặt hệ điều hành, dịch vụ, phần mềm trên hệ thống chính phải thực hiện cài đặt trên môi trường thử nghiệm để đánh giá mức độ an toàn, ổn định;

b) Dịch vụ, phần mềm trên máy chủ ứng dụng không phục vụ hoạt động của máy chủ theo chức năng phải gỡ bỏ;

c) Thực hiện lưu trạng thái ảnh của hệ điều hành ảo hóa (take snapshot) tại thời điểm trước và sau khi gỡ bỏ dịch vụ, phần mềm;

d) Xóa sạch dữ liệu của hệ điều hành, dịch vụ, phần mềm sau khi được gỡ bỏ.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.

a) Máy chủ hệ thống phải được kiểm tra, đánh giá và xử lý các điểm yếu an toàn thông tin; không còn tồn tại điểm yếu mở mức trung bình trở lên, trước khi kết nối vào hệ thống;

b) Máy chủ phải được cấu hình tối ưu và tăng cường bảo mật trước khi kết nối vào hệ thống;

c) Khi gỡ bỏ máy chủ khỏi hệ thống, toàn bộ chính sách bảo mật, cấu hình hệ thống phải được gỡ bỏ;

d) Toàn bộ dữ liệu, hệ điều hành máy chủ phải được xóa bỏ trước khi gỡ bỏ máy chủ khỏi hệ thống.

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

8. Hoạt động quản lý an toàn máy chủ và ứng dụng thực hiện theo Quy trình quản lý rủi ro an toàn thông tin, Quy trình quản lý điểm yếu an toàn thông tin, Quy trình kết thúc vận hành, khai thác, thanh lý hệ thống thông tin, ban hành kèm theo Quy chế này tại các Phục lục I, V, VI.

Điều 12. Quản lý an toàn dữ liệu

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

a) Toàn bộ cơ sở dữ liệu, dữ liệu nghiệp vụ của hệ thống khi lưu trữ trên thiết bị và hệ thống lưu trữ độc lập phải được mã hóa và kèm theo mã kiểm tra tính toàn vẹn;

b) Dữ liệu được sao lưu dự phòng theo từng phiên bản và có nhật ký ghi lại thông tin dữ liệu sau mỗi lần thực hiện sao lưu, dự phòng;

c) Độ dài của khóa bí mật dùng để mã hóa dữ liệu tối thiểu 128 bit.

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

a) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu hệ thống (tệp tin cấu hình, ảnh hệ điều hành,…) được quản lý bởi bộ phận kỹ thuật quản trị hệ thống;

b) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu nghiệp vụ (tệp tin dữ liệu, cơ sở dữ liệu,…) được quản lý bởi bộ phận nghiệp vụ tương ứng;

c) Thông tin khóa bí mật phải được lưu trữ mã hóa, kèm theo mã kiểm tra tính toàn vẹn trên thiết bị và hệ thống lưu trữ độc lập;

d) Chỉ có bộ phận/cán bộ có chức năng có quyền quản lý và truy cập khóa bí mật;

đ) Thông tin mỗi khóa bí mật phải có thông tin nhật ký quản lý, cán bộ quản lý tại mỗi thời điểm.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu không được sử dụng không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Khoa học và Công nghệ công bố.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ phải được mã hóa đáp ứng yêu cầu ở trên.

5. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ phải được đồng bộ theo thời gian thực;

6. Định kỳ hàng 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 và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có) theo quy định tại điểm 5 Điều này.

7. Hoạt động quản lý an toàn dữ liệu thực hiện theo Quy trình quản lý an toàn người sử dụng đầu cuối, ban hành kèm theo Quy chế này tại Phụ lục IV.

Điều 13. Quản lý an toàn thiết bị đầu cuối

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối

a) Thiết bị đầu cuối (máy trạm và thiết bị ngoại vi) của cán bộ thuộc tổ chức khi kết nối vào mạng nghiệp vụ phải được quản lý truy cập theo địa chỉ IP và địa chỉ MAC;

b) Trạng thái hoạt động (UP/DOWN) của thiết bị đầu cuối phải được quản lý bởi hệ thống quản lý truy cập lớp mạng tập trung;

c) Ngăn chặn toàn bộ các thiết bị đầu cuối chưa được quản lý kết nối vào mạng nghiệp vụ.

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa

a) Chỉ cho phép truy cập, sử dụng thiết bị đầu cuối từ bên ngoài hệ thống phải thông qua kết nối VPN;

b) Tất cả truy cập từ các thiết bị đầu cuối từ các mạng khác nhau trong hệ thống phải được kiểm soát truy cập bởi tường lửa lớp mạng;

c) Mọi máy trạm trong mạng phải thiết lập chức năng tường lửa của hệ điều hành;

đ) Mọi máy trạm trong mạng phải cài đặt phần mềm phòng chống mã độc trước khi kết nối vào hệ thống.

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống

b) Máy trạm phải được cấu hình tối ưu và tăng cường bảo mật trước khi kết nối vào hệ thống;

c) Toàn bộ dữ liệu, hệ điều hành máy trạm phải được xóa bỏ trước khi gỡ bỏ máy chủ khỏi hệ thống.

4. Hoạt động quản lý an toàn thiết bị đầu cuối thực hiện theo Quy trình quản lý an toàn thiết bị đầu cuối, ban hành kèm theo Quy chế này tại Phụ lục IV.

Điều 14. Quản lý phòng chống phần mềm độc hại

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động

a) Máy tính, máy chủ và thiết bị di động phải được cập nhật phần mềm phòng chống mã độc trước khi kết nối vào hệ thống;

b) Phần mềm phòng, chống mã độc trên máy tính, máy chủ và thiết bị di động phải được thiết lập chế độ tự động cập nhật dấu hiệu mã độc từ nhà cung cấp và chế độ bảo vệ theo thời gian thực;

c) Triển khai giải pháp phòng, chống mã độc có chức năng quản lý tập trung.

2. Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng

a) Phần mềm trước khi cài đặt trên máy tính, thiết bị di động phải kiểm tra mã độc;

b) Phần mềm trước khi cài đặt trên máy tính, thiết bị di động phải xác thực nguồn gốc từ nhà sản xuất theo mã kiểm tra tính toàn vẹn;

c) Phần mềm sau khi cài đặt phải được xử lý điểm yếu an toàn thông tin và cập nhật lên phiên bản mới nhất;

d) Hệ thống phải được trang bị giải pháp kỹ thuật để quản lý và ngăn chặn truy cập đến các trang thông tin độc hại trên mạng.

3. Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động phải thực hiện qua kênh kết nối an toàn sử dụng giao thức mã hóa, xác thực không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Khoa học và Công nghệ công bố.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

5. Hoạt động quản lý phòng chống phần mềm độc hại thực hiện theo Quy trình quản lý rủi ro an toàn thông tin, ban hành kèm theo Quy chế này tại Phục lục V.

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

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

a) Bộ phận NOC thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của các thành phần của hệ thống giám sát;

b) Giải pháp giám sát hệ thống thông tin tập trung phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thành phần của hệ thống giám sát bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của các thành phần của hệ thống giám sát, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực;

2. Đối tượng giám sát bao gồm tối thiểu bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ;

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

4. Truy cập và quản trị hệ thống giám sát chỉ được thực hiện từ vùng mạng quản trị; trường hợp truy cập và quản trị từ mạng bên ngoài thì phải thông qua kênh kết nối VPN.

5. Loại thông tin cần được giám sát bao gồm tối thiểu các loại sau: Thông tin giám sát lớp mạng, lớp máy chủ, lớp ứng dụng, cơ sở dữ liệu và thiết bị đầu cuối.

6. Lưu trữ và bảo vệ thông tin giám sát phải được lưu trữ tập trung đầy đủ các loại thông tin tại khoản 5 Điều này theo thời gian thực.

7. Toàn bộ thành phần trong hệ thống giám sát, máy chủ, thiết bị hệ thống và ứng dụng phải được đồng bộ thời gian;

8. Bộ phận SOC thực hiện giám sát giám sát an toàn hệ thống thông tin 24/7 để thực hiện theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.

9. Hoạt động giám sát được thực hiện theo Quy trình quản lý rủi ro an toàn thông tin, ban hành kèm theo Quy chế này tại Phục lục V.

Điều 16. Quản lý điểm yếu an toàn thông tin

1. Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống nếu có.

2. Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định

a) Cán bộ quản trị hệ thống ATTT định kỳ ngày 01 lần truy cập và cập nhật thông tin về điểm yếu an toàn thông tin được cung cấp bởi tối thiểu 02 tổ chức trong nước và quốc tế;

b) Điểm yếu an toàn thông tin được phân nhóm theo mức độ nghiêm trọng (Critical, High, Medium, Low);

c) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Critical Cán bộ quản trị hệ thống ATTT phải xử lý trong vòng 06 giờ;

d) Khi phát hiện điểm yếu an toàn thông tin ở mức độ High Cán bộ quản trị hệ thống ATTT phải xử lý trong vòng 09 giờ;

đ) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Medium Cán bộ quản trị hệ thống ATTT phải xử lý trong vòng 24 giờ.

3. Cơ chế 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

a) Bên cung cấp phần mềm, giải pháp, ứng dụng phải có trách nhiệm hỗ trợ xử lý điểm yếu an toàn thông tin theo yêu cầu của bên sử dụng;

b) Phòng CNTT và Kỹ thuật là đầu mối phối hợp với các bên việc phối hợp xử lý điểm yếu an toàn thông tin từ các nhóm chuyên gia, bên cung cấp dịch vụ.

4. 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.

5. Định kỳ hàng 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.

6. Khi phát hiện điểm yếu an toàn thông tin tồn tại trong hệ thống thực hiện theo Quy trình Quản lý điểm yếu an toàn thông tin, Quy trình truyền thông khủng hoảng, ban hành theo Quy chế này tại các Phụ lục I, VII.

Điều 17. Quản lý sự cố an toàn thông tin

1. Đơn vị chuyên trách chịu trách nhiệm xây dựng phương án quản lý sự cố an toàn thông tin bao gồm các nội dung sau:

a) 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.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;

c) Xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng;

d) Thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

đ) Thực hiện quy trình ứng cứu sự cố an toàn thông tin mạng thông thường (khi sự cố ở mức độ thông thường);

e) Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng (khi sự cố ở mức độ nghiêm trọng);

g) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin;

2. Khi xảy ra sự cố an toàn thông tin thông thường thực hiện xử lý theo Quy trình xử lý sự cố an toàn thông tin thông thường, Quy trình truyền thông khủng hoảng ban hành theo Quy chế này tại Phụ lục II và Phụ lục VII .

3. Khi xảy ra sự cố an toàn thông tin nghiêm trọng thực hiện xử lý theo Quy trình xử lý sự cố an toàn thông tin nghiêm trọng, Quy trình truyền thông khủng hoảng ban hành theo Quy chế này tại Phụ lục III và Phụ lục VII .

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

Điều 18. Quản lý an toàn người sử dụng đầu cuối

1. Quản lý truy cập, sử dụng tài nguyên nội bộ

a) Người sử dụng đầu cuối phải tuân thủ các quy định của pháp luật và quy định tại Quy chế này khi truy cập, sử dụng tài nguyên nội bộ;

b) Không truy cập từ xa vào trực tiếp các máy tính trong mạng nội bộ của đơn vị. Trường hợp, người sử dụng cần truy cập từ xa thì phải truy cập gián tiếp qua giao thức mạng an toàn, có hỗ trợ mã hóa bảo mật thông tin như VPN;

c) Không kết nối các thiết bị lưu trữ di động của khách bên ngoài vào các

máy tính để bàn của đơn vị. Trường hợp, người sử dụng cần thiết phải kết nối các thiết bị lưu trữ di động của khách bên ngoài thì phải đề nghị và được bộ phận chuyên trách kiểm tra an toàn thông tin trước khi thực hiện.

2. Quản lý truy cập mạng và tài nguyên trên Internet

a) Không truy cập trang thông tin theo đường link, mở tệp tin đính kèm từ những thư điện tử lần đầu tiên nhận được, không rõ nguồn gửi hoặc nghi ngờ có thể gây hại. Trường hợp, người sử dụng cần thiết phải truy cập hoặc mở tệp tin đính kèm thì đề nghị bộ phận chuyên trách kiểm tra an toàn thông tin trước khi truy cập hoặc mở tệp tin.

b) Không truy cập các trang thông tin không rõ nguồn gốc hoặc có nội dung độc hại;

c) Thiết bị di động của người sử dụng được kết nối vào mạng không dây công cộng của đơn vị nhưng không kết nối thiết bị di động vào mạng ngang hàng với mạng máy tính để bàn của cán bộ. Trường hợp, người sử dụng cần thiết phải kết nối vào mạng ngang hàng thì phải đề nghị bộ phận chuyên trách kiểm tra an toàn thông tin cho thiết bị di động trước khi thực hiện;

d) Thiết bị di động khi kết nối vào mạng nội bộ của đơn vị phải được quản lý truy cập ra các vùng mạng khác của hệ thống và mạng Internet.

đ) Thiết bị di động phải được quản lý cấp phát DHCP theo địa chỉ MAC (trừ các thiết bị kết nối vào mạng không dây công cộng).

3. Cài đặt và sử dụng máy tính an toàn

a) Đặt mật khẩu cho các tài khoản của hệ điều hành theo quy tắc: tối thiểu 08 ký tự; bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt. Định kỳ 06 tháng thay đổi mật khẩu.

b) Khóa máy tính và các thiết bị có tính năng tương tự máy tính khi tạm thời rời khỏi vị trí làm việc. Đóng các phiên làm việc của ứng dụng khi đã hoàn tất, trừ khi đã có cơ chế bảo vệ thích hợp.

c) Không tự ý thay đổi cấu hình thiết bị đã được thiết lập, việc thay đổi phải thông báo đến bộ phận chuyên trách

4. Hoạt động quản lý an toàn người sử dụng đầu cuối thực hiện theo Quy trình Quản lý an toàn người sử dụng đầu cuối, ban hành kèm theo Quy chế này tại Phụ lục IV.

Điều 19. Quản lý rủi ro an toàn thông tin

1. Hệ thống phải được xây dựng phương án Quản lý rủi ro an toàn thông tin.

2. Phương án Quản lý an toàn thông tin phải được ban hành cùng Quy chế bảo đảm an toàn thông tin trước khi đưa hệ thống vào vận hành, khai thác.

3. Thực hiện đánh giá và xây dựng phương án xử lý rủi ro cho hệ thống trước khi đưa vào vận hành, khai thác.

4. Thực hiện đánh giá và quản lý rủi ro an toàn thông tin cho hệ thống theo Quy trình Quản lý rủi ro an toàn thông tin, được ban hành kèn theo Quy chế này tại Phụ lục V.

Điều 20. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Yêu cầu đối với việc thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin:

a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ 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.

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

c) Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), 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.

2. Thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin thực hiện theo Quy trình kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin, được ban hành kèn theo Quy chế này tại Phụ lục VI.

Chương IV
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 21. Trách nhiệm của Phòng CNTT và Kỹ thuật

1. Phòng CNTT và Kỹ thuật có trách nhiệm: Tham mưu cho Lãnh đạo Văn phòng, Lãnh đạo Viện Hàn lâm trong việc xây dựng, ban hành chính sách, quy định, quy trình liên quan đến bảo đảm an toàn, an ninh mạng; Đề xuất kế hoạch đầu tư, nâng cấp, duy trì hệ thống bảo mật và các giải pháp ATTT. Tổ chức giám sát nội bộ việc tuân thủ quy định an toàn thông tin đối với toàn bộ hệ thống, bao

gồm: giám sát kỹ thuật (hạ tầng, mạng, máy chủ, ứng dụng) và giám sát tuân thủ (quy trình, hành vi người dùng).

2. Tổ chức thực hiện các hoạt động bảo đảm ATTT cho hệ thống Trung tâm dữ liệu; Thiết lập, vận hành và giám sát 24/7 hệ thống NOC, SOC, cảnh báo sớm và phát hiện bất thường; Kiểm tra, đánh giá định kỳ mức độ an toàn hệ thống, xử lý điểm yếu, lỗ hổng ATTT.

3. Tiếp nhận, phân loại và xử lý sự cố an toàn thông tin theo quy trình ứng phó đã được phê duyệt; Kịp thời cô lập, khắc phục, khôi phục hệ thống và điều phối các lực lượng khi xảy ra sự cố; Phối hợp với các cơ quan chuyên trách như VNCERT, Cục ATTT khi xử lý sự cố nghiêm trọng.

4. Quản lý tài khoản, phân quyền truy cập hệ thống, cấp/thu hồi quyền quản trị và truy cập tài nguyên mạng. Đảm bảo mọi hoạt động truy cập được kiểm soát, giám sát và ghi nhật ký đầy đủ.

5. Báo cáo định kỳ hoặc đột xuất tình hình ATTT, sự cố, điểm yếu, kết quả giám sát cho Lãnh đạo Văn phòng, Lãnh đạo Viện Hàn lâm và cơ quan có thẩm quyền; Lưu trữ hồ sơ, nhật ký hệ thống, tài liệu đánh giá, xử lý sự cố theo quy định.

6. Rà soát, cập nhật các quy trình, giải pháp kỹ thuật nhằm nâng cao năng lực bảo vệ hệ thống; Thực hiện kiểm tra nội bộ, kiểm thử bảo mật và đánh giá hiệu quả các biện pháp đang áp dụng.

Điều 22. Trách nhiệm của Văn phòng Viện Hàn lâm

1. Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ;

2. Thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin;

3. Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin, báo cáo chủ quản hệ thống thông tin Điều chỉnh nếu cần thiết;

4. Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

Điều 23. Chế tài xử lý vi phạm

1. Cán bộ, viên chức, người lao động và các tổ chức/cá nhân có liên quan vi phạm Quy chế này tùy theo tính chất, mức độ sẽ bị:

a) Nhắc nhở, cảnh cáo, hoặc xử lý kỷ luật theo quy định;

b) Thu hồi, hạn chế quyền truy cập hệ thống;

c) Bồi thường thiệt hại nếu gây ra mất mát dữ liệu, gián đoạn dịch vụ;

d) Chuyển hồ sơ sang cơ quan có thẩm quyền nếu có dấu hiệu vi phạm pháp luật.

2. Trách nhiệm xử lý vi phạm do Văn phòng Viện Hàn lâm chủ trì, phối hợp với Phòng CNTT và Kỹ thuật và các đơn vị có liên quan.

Điều 24. Quy trình kiểm toán định kỳ

1. Hệ thống Trung tâm dữ liệu phải được kiểm toán an toàn thông tin định kỳ ít nhất 01 lần/năm; kiểm toán đột xuất khi có sự cố nghiêm trọng hoặc theo yêu cầu của Lãnh đạo Viện Hàn lâm.

2. Kiểm toán do bộ phận kiểm toán nội bộ của Viện Hàn lâm hoặc đơn vị kiểm toán độc lập có năng lực thực hiện, bảo đảm tính khách quan.

3. Nội dung kiểm toán gồm: tuân thủ chính sách, quy chế an toàn thông tin; hiệu quả các biện pháp kỹ thuật, công nghệ; quản lý nhật ký hệ thống; quản lý sự cố và rủi ro; mức độ đáp ứng tiêu chuẩn, quy chuẩn quốc gia và quốc tế (ISO/IEC 27001, NIST, …).

4. Kết quả kiểm toán phải được lập thành báo cáo, kiến nghị khắc phục, gửi Lãnh đạo Viện Hàn lâm và các đơn vị có liên quan để thực hiện. Việc khắc phục sau kiểm toán phải được theo dõi, báo cáo kết quả hoàn thành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 25. Xây dựng và công bố

1. Quy chế này gồm 05 Chương, 26 Điều và có hiệu lực kể từ ngày ký ban hành. Tất cả viên chức, người lao động trong Viện Hàn lâm có trách nhiệm thực hiện nghiêm chỉnh và đầy đủ các điều khoản của Quy chế này.

2. Quy chế này được công bố trước khi áp dụng.

3. Văn phòng Viện Hàn lâm chịu trách nhiệm tuyên truyền, phổ biến Quy chế này cho toàn bộ cán bộ trong Viện Hàn lâm.

Điều 26. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin, Văn phòng Viện Hàn lâm kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế này.

Trong quá trình tổ chức thực hiện, nếu có vấn đề phát sinh mới hoặc khó khăn, vướng mắc, các đơn vị cần phản ánh kịp thời về Văn phòng Viện Hàn lâm để tập hợp, báo cáo Chủ tịch Viện Hàn lâm sửa đổi, bổ sung cho phù hợp.

2. Văn phòng Viện Hàn lâm phải 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 và sau mỗi lần cập nhật, bổ sung Quy chế.

3. Văn phòng Viện Hàn lâm hướng dẫn, đôn đốc và kiểm tra việc thực hiện Quy chế này, hàng năm tổng kết và đánh giá báo cáo Chủ tịch Viện Hàn lâm./.

PHỤ LỤC I
QUY TRÌNH QUẢN LÝ ĐIỂM YẾU AN TOÀN THÔNG TIN

1. Mục đích

Quy trình này nhằm phát hiện, đánh giá, xử lý và khắc phục các điểm yếu an toàn thông tin trong hệ thống công nghệ thông tin của Viện Hàn lâm KHXH Việt Nam, đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của hệ thống thông tin.

2. Phạm vi áp dụng

Áp dụng cho toàn bộ hệ thống thông tin, máy chủ, thiết bị mạng, ứng dụng, phần mềm và cơ sở dữ liệu thuộc phạm vi quản lý của Trung tâm dữ liệu Viện Hàn lâm.

3. Căn cứ thực hiện

- Luật An toàn thông tin mạng năm 2015;
- Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ;
- Quyết định số 05/2017/QĐ-TTg về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT quốc gia;
- Các tiêu chuẩn, hướng dẫn của Bộ KHCN.

4. Quy trình thực hiện

4.1. Theo dõi và cập nhật điểm yếu

Bộ phận chuyên trách (Phòng CNTT & Kỹ thuật) thực hiện theo dõi hệ thống 24/7, thường xuyên rà soát, cập nhật hàng ngày thông tin điểm yếu ATTT từ:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT)
- Cục An toàn thông tin
- Bộ KHCN
- Các tổ chức quốc tế (US-CERT, NIST, CVE, v.v.).

4.2. Phân loại và đánh giá mức độ nghiêm trọng

Mỗi điểm yếu được đánh giá theo 4 mức độ:

STT	Mức độ	Mô tả
1.	Critical	Điểm yếu dễ khai thác, ảnh hưởng nghiêm trọng đến toàn bộ hệ thống, gây gián đoạn hoặc rò rỉ dữ liệu quy mô lớn.
2.	High	Điểm yếu có khả năng bị khai thác cao, ảnh hưởng lớn đến tính bảo mật, toàn vẹn hoặc sẵn sàng của hệ thống.

3.	Medium	Điểm yếu có mức độ khai thác trung bình, ảnh hưởng hạn chế hoặc cần điều kiện đặc biệt để khai thác.
4.	Low	Điểm yếu khó khai thác có tác động nhỏ hoặc ít ảnh hưởng đến hệ thống.

Phân loại dựa trên các yếu tố: khả năng khai thác, ảnh hưởng đến hệ thống, mức độ thiệt hại, độ phổ biến của hệ thống bị ảnh hưởng.

4.3. Xử lý điểm yếu theo mức độ

STT	Thang điểm	Mức độ	Thời gian xử lý tối đa	Trách nhiệm
1.	9.0-10.0	Critical	04-06 giờ	Bộ phận chuyên trách thực hiện ngay
2.	7.0-8.9	High	Trong 24 giờ	Bộ phận chuyên trách phối hợp đơn vị vận hành
3.	4.0-6.9	Medium	Trong 3 ngày	Lên lịch vá lỗi định kỳ
4.	0.1-3.9	Low	Trong 7 ngày	Gộp vào đợt cập nhật hệ thống

4.4. Biện pháp xử lý điểm yếu

- Áp dụng bản vá bảo mật, cập nhật hệ thống/ứng dụng
- Cấu hình lại hệ thống, đóng các cổng/rủi ro truy cập
- Cô lập tạm thời thiết bị/ứng dụng bị ảnh hưởng
- Nâng cấp hoặc thay thế thiết bị/phần mềm không còn được hỗ trợ

4.5. Ghi nhật ký và báo cáo

- Tất cả các điểm yếu, hành động xử lý phải được ghi vào hệ thống quản lý sự cố và điểm yếu
- Báo cáo định kỳ hàng quý hoặc đột xuất theo yêu cầu của lãnh đạo Viện Hàn lâm hoặc cơ quan quản lý nhà nước

4.6. Kết nối với quy trình xử lý sự cố

- Trong trường hợp điểm yếu đã bị khai thác và dẫn đến sự cố an toàn thông tin, việc xử lý sẽ được chuyển sang quy trình xử lý sự cố an toàn thông tin của Viện Hàn lâm.

- Tùy theo mức độ sự cố, bộ phận chuyên trách có trách nhiệm kích hoạt quy trình sự cố ngay khi phát hiện, đồng thời duy trì việc khắc phục điểm yếu sự cố để ngăn chặn tái diễn.

5. Trách nhiệm thực hiện

- Phòng CNTT & Kỹ thuật: Là đầu mối cập nhật, đánh giá và tổ chức xử lý điểm yếu.

- Các đơn vị vận hành hệ thống: Phối hợp xử lý và khắc phục các điểm yếu trên hệ thống mình quản lý.

- Đơn vị cung cấp dịch vụ phần mềm/hạ tầng: Phối hợp cung cấp bản vá, hướng dẫn kỹ thuật khi có yêu cầu.

6. Giám sát và kiểm tra

Các hoạt động quản lý, đánh giá và xử lý điểm yếu được giám sát bởi Tổ Giám sát và hỗ trợ xử lý sự cố. Tổ Giám sát và hỗ trợ xử lý sự cố thực hiện kiểm tra định kỳ hoặc đột xuất nhằm bảo đảm tính khách quan, tránh bỏ sót hoặc đánh giá sai mức độ điểm yếu.

Tổ Giám sát và hỗ trợ xử lý sự cố thực hiện báo cáo kết quả giám sát/kiểm tra gửi trực tiếp cho Lãnh đạo Viện Hàn lâm và các cơ quan quản lý nhà nước có thẩm quyền (khi có yêu cầu).

Các khuyến nghị từ Tổ Giám sát và hỗ trợ xử lý sự cố phải được cập nhật vào quy trình quản lý điểm yếu để liên tục cải tiến.

7. Rà soát và cải tiến

- Quy trình được rà soát định kỳ 6 tháng/lần, hoặc khi có thay đổi về công nghệ, hệ thống hoặc yêu cầu pháp lý.

- Hồ sơ xử lý điểm yếu phải được lưu trữ tối thiểu 03 năm.

PHỤ LỤC II
QUY TRÌNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN THÔNG THƯỜNG

1. Mục đích

Quy trình này quy định các bước xử lý các sự cố an toàn thông tin thông thường xảy ra trong hệ thống công nghệ thông tin thuộc phạm vi quản lý của Viện Hàn lâm KHXH Việt Nam, nhằm đảm bảo nhanh chóng kiểm soát, khôi phục hệ thống và giảm thiểu thiệt hại.

2. Phạm vi áp dụng

Áp dụng cho các sự cố an toàn thông tin có mức độ ảnh hưởng thấp hoặc trung bình, không gây gián đoạn nghiêm trọng đến hoạt động chung của hệ thống thông tin và không ảnh hưởng đến an ninh, bí mật nhà nước.

3. Căn cứ thực hiện

- Luật An toàn thông tin mạng năm 2015
- Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ
- Quy chế bảo đảm an toàn, an ninh mạng hệ thống Trung tâm dữ liệu

4. Quy trình xử lý sự cố

4.1. Tiếp nhận và ghi nhận sự cố

- Cá nhân, bộ phận phát hiện sự cố phải lập tức thông báo cho bộ phận chuyên trách (Phòng CNTT & Kỹ thuật).

- Bộ phận chuyên trách ghi nhận sự cố vào hệ thống quản lý sự cố, ghi rõ thời gian, địa điểm, mô tả ban đầu.

4.2. Phân loại sự cố

Bộ phận chuyên trách tiến hành đánh giá sơ bộ dựa theo các tiêu chí định lượng của sự cố thông thường gồm:

- Thời gian gián đoạn dịch vụ: 2h≥ sự cố thông thường ≥30'
- Phạm vi ảnh hưởng: Chỉ ảnh hưởng đến 1 hệ thống không ảnh hưởng đến các hệ thống khác. Số lượng người dùng bị ảnh hưởng 100 ≥ sự cố thông thường ≥10 người.

- Các sự cố thông thường bao gồm: lỗi hệ điều hành, tấn công dò quét đơn lẻ, mất kết nối ngắn hạn, lỗi phần mềm cục bộ,…

4.3. Xử lý sự cố

- Bộ phận chuyên trách phối hợp với đơn vị vận hành khẩn trương áp dụng các biện pháp cô lập, ngăn chặn sự cố lan rộng.

- Tiến hành khôi phục hệ thống về trạng thái ổn định hoặc cấu hình an toàn gần nhất.

- Áp dụng bản vá, cập nhật hoặc cấu hình lại hệ thống nếu cần thiết.

- Bộ phận chuyên trách có trách nhiệm xử lý sự cố trong khoảng 24-72h.

Cụ thể đối với các sự cố thông thường phổ biến như:

• Sự cố mất kết nối: Bộ phận chuyên trách cần thực hiện kiểm tra hạ tầng mạng (switch, router), xác minh kết nối vật lý, khởi động lại thiết bị, kiểm tra cấu hình IP/DNS và khôi phục dịch vụ.

• Sự cố lỗi phần mềm: Bộ phận chuyên trách cần xác định ứng dụng bị lỗi, ghi nhận thông báo lỗi, thử khởi động lại ứng dụng/dịch vụ, cài đặt bản vá hoặc cập nhật phiên bản mới nhất.

• Sự cố tấn công dò quét: Bộ phận chuyên trách cần xác định nguồn IP tấn công, chặn trên firewall, kiểm tra log hệ thống, rà soát lỗ hổng bảo mật và áp dụng biện pháp gia cố (vá lỗi, thay đổi mật khẩu, tăng cường giám sát).

4.4. Ghi nhật ký và phục hồi

- Toàn bộ quá trình xử lý phải được ghi lại trong hệ thống nhật ký.

- Khôi phục dữ liệu, dịch vụ về trạng thái bình thường, đảm bảo tính toàn vẹn và liên tục.

4.5. Báo cáo và đánh giá sau xử lý

- Lập báo cáo tổng kết sự cố bao gồm nguyên nhân, diễn biến, biện pháp xử lý và khuyến nghị.

- Phân tích điểm yếu hệ thống và đề xuất giải pháp phòng ngừa sự cố tương tự.

- Trình báo cáo lên lãnh đạo Viện Hàn lâm hoặc cơ quan có thẩm quyền nếu cần thiết.

5. Trách nhiệm thực hiện

- Phòng CNTT & Kỹ thuật: Đầu mối tiếp nhận, đánh giá và xử lý sự cố.

- Các đơn vị vận hành, đầu mối quản trị: Phối hợp xử lý và cung cấp thông tin hỗ trợ.

- Người dùng cuối: Báo cáo kịp thời khi phát hiện sự cố, phối hợp xác minh.

6. Rà soát và cải tiến

- Quy trình được rà soát định kỳ 6 tháng/lần hoặc khi có sự cố đặc biệt phát sinh.

- Đề xuất cập nhật quy trình khi có thay đổi về công nghệ hoặc chính sách liên quan.

PHỤ LỤC III
QUY TRÌNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN NGHIÊM TRỌNG

1. Mục đích

Quy trình này quy định các bước xử lý sự cố an toàn thông tin nghiêm trọng nhằm đảm bảo kịp thời kiểm soát, khoanh vùng, hạn chế thiệt hại và khôi phục hoạt động hệ thống thông tin trong thời gian sớm nhất.

2. Phạm vi áp dụng

Áp dụng đối với các sự cố an toàn thông tin có mức độ nghiêm trọng như:

- Làm gián đoạn hoạt động của hệ thống trọng yếu;
- Mất, lộ lọt dữ liệu quan trọng;
- Tấn công có chủ đích vào hệ thống mạng;
- Các sự cố ảnh hưởng đến an ninh, bí mật nhà nước hoặc thuộc nhóm sự cố theo quy định tại Quyết định 05/2017/QĐ-TTg.

3. Căn cứ thực hiện

- Luật An toàn thông tin mạng năm 2015;
- Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ;
- Quy chế bảo đảm an toàn, an ninh mạng hệ thống Trung tâm dữ liệu.

4. Quy trình xử lý sự cố nghiêm trọng

4.1. Phát hiện và cảnh báo

- Trong vòng 15 phút – 1 giờ kể từ khi phát hiện dấu hiệu bất thường, người sử dụng hoặc hệ thống giám sát phải thông báo cho bộ phận chuyên trách ATTT.
- Bộ phận chuyên trách sau khi nhận cảnh báo cần khẩn cấp thông báo đến lãnh đạo đơn vị và các bộ phận liên quan.

4.2. Kích hoạt quy trình khẩn cấp

- Trong vòng 1 giờ kể từ khi nhận thông báo, bộ phận chuyên trách phải đánh giá, xác nhận sự cố và kích hoạt phương án ứng cứu. Nếu xác định là sự cố nghiêm trọng thì kích hoạt phương án ứng cứu khẩn cấp.
- Triệu tập nhóm ứng cứu sự cố gồm các thành viên kỹ thuật, quản lý và truyền thông (nếu cần).

4.3. Khoanh vùng và ngăn chặn

- Thực hiện trong vòng 2 giờ kể từ khi kích hoạt quy trình khẩn cấp, nhằm ngăn chặn sự cố lan rộng.
- Cô lập các hệ thống, phân vùng mạng bị ảnh hưởng để ngăn sự cố lan rộng.
- Ngắt kết nối Internet, dừng các dịch vụ có liên quan nếu cần thiết.
- Giữ nguyên hiện trạng để phục vụ phân tích nguyên nhân.

4.4. Phân tích và xử lý sự cố

- Sau khi cô lập, khoanh vùng sự cố phải xác định nguyên nhân gốc rễ trong vòng 24 giờ.
- Phân tích nhật ký hệ thống, truy vết mã độc hoặc hành vi bất thường.
- Xác định loại bỏ tác nhân tấn công.
- Cập nhật bản vá, khôi phục hệ thống từ bản sao lưu an toàn.

4.5. Phối hợp với các đơn vị có thẩm quyền

- Phối hợp với Cục ATTT, VNCERT hoặc các cơ quan nhà nước có liên quan theo quy định.
- Trường hợp sự cố ảnh hưởng đến an ninh quốc gia, phải báo cáo và phối hợp xử lý theo cơ chế đặc biệt.

4.6. Khôi phục hệ thống

- Khôi phục dần từng phần hệ thống theo mức độ ưu tiên, đảm bảo khôi phục dịch vụ thiết yếu trong vòng 24-48h tùy theo mức độ nghiêm trọng của sự cố.
- Kiểm tra tính toàn vẹn và an toàn của dữ liệu, dịch vụ.
- Theo dõi sát sau khi khôi phục để phát hiện bất thường.

4.7. Báo cáo và cải tiến sau sự cố

- Lập báo cáo nhanh trong vòng 2-4h kể từ khi xác nhận sự cố nghiêm trọng; Báo cáo chi tiết về sự cố gửi lãnh đạo Viện Hàn lâm và cơ quan có thẩm quyền trong vòng 05 ngày làm việc sau khi khắc phục sự cố.
- Rút kinh nghiệm, cập nhật chính sách và quy trình phòng chống sự cố.
- Tổ chức diễn tập hoặc đào tạo lại nếu cần thiết.

5. Trách nhiệm thực hiện

Phòng CNTT & Kỹ thuật:

- Tổng hợp diễn biến sự cố, báo cáo nhanh và báo cáo chi tiết cho lãnh đạo

- Chủ trì phân tích nguyên nhân, khoanh vùng và khắc phục sự cố.
- Triển khai các biện pháp kỹ thuật (cô lập, khôi phục, vá lỗi, giám sát).
- Thông báo lỗi sự cố và dự kiến thời gian khắc phục tới các bộ phận và người dùng liên quan.

Lãnh đạoVăn phòng phụ trách Phòng CNTT & Kỹ thuật:

- Đảm bảo các hoạt động ứng cứu tuân thủ quy định pháp luật, quy chế nội bộ.
- Điều phối hoạt động giữa các bộ phận kỹ thuật và truyền thông
- Tham mưu, báo cáo với Lãnh đạo Văn phòng, Viện Hàn lâm về xử lý trách nhiệm pháp lý (nếu có).

6. Bảo mật và pháp lý

- Tất cả thông tin liên quan đến sự cố nghiêm trọng phải được bảo mật tuyệt đối.
- Không tự ý cung cấp thông tin cho báo chí hoặc bên thứ ba khi chưa được phép.
- Tuân thủ quy định pháp luật về bảo vệ thông tin, dữ liệu cá nhân và bí mật nhà nước.

PHỤ LỤC 3A
KỊCH BẢN XỬ LÝ SỰ CỐ MẪU

1. Sự cố tấn công từ chối dịch vụ (DDoS)

• Kiểm tra, phát hiện: Lưu lượng tăng đột biến, hệ thống chậm hoặc tê liệt.

• Các bước xử lý:

- Kích hoạt tường lửa/chống DDoS, lọc lưu lượng bất thường.
- Phối hợp ISP để chặn lưu lượng từ nguồn tấn công.
- Cô lập dịch vụ bị tấn công, chuyển sang hệ thống dự phòng (nếu có).

• Thời gian phản ứng:

- 15 phút: cảnh báo, báo cáo nội bộ.
- 1 giờ: áp dụng biện pháp lọc chặn, phối hợp ISP.
- 24 giờ: khôi phục dịch vụ ở trạng thái ổn định.

2. Sự cố mã độc tống tiền (Ransomware)

• Kiểm tra, phát hiện: Máy chủ/máy trạm bị mã hóa dữ liệu, xuất hiện thông báo đòi tiền chuộc.

• Các bước xử lý:

- Ngắt kết nối ngay máy bị nhiễm khỏi mạng.
- Phân tích biến thể ransomware, loại bỏ mã độc.
- Khôi phục dữ liệu từ bản sao lưu an toàn.
- Vá lỗ hổng và tăng cường giám sát.

• Thời gian phản ứng:

- 30 phút: cô lập hệ thống bị nhiễm.
- 4 giờ: triển khai khôi phục dữ liệu từ backup.
- 24–48 giờ: khôi phục toàn bộ dịch vụ.

3. Sự cố mất điện tại trung tâm dữ liệu

• Kiểm tra, thát hiện: Toàn bộ hệ thống/dịch vụ ngừng hoạt động do mất nguồn.

• Các bước xử lý:

- Kích hoạt UPS và máy phát điện dự phòng.
- Ưu tiên duy trì hệ thống trọng yếu (mạng lõi, máy chủ dịch vụ công).
- Thông báo cho đơn vị quản lý cơ sở hạ tầng để xử lý sự cố nguồn điện chính.

• Thời gian phản ứng:

- Ngay lập tức: chuyển sang nguồn dự phòng.

- 1 giờ: xác nhận khả năng duy trì bằng nguồn dự phòng.

- Trong vòng 24 giờ: khôi phục điện lưới ổn định, đưa hệ thống vận hành bình thường.

4. Sự cố mất dữ liệu quan trọng

• Kiểm tra, phát hiện: Hệ thống báo lỗi, dữ liệu bị xóa nhầm hoặc hỏng do sự cố lưu trữ.

• Các bước xử lý:

- Kiểm tra hệ thống sao lưu gần nhất.

- Khôi phục dữ liệu từ backup.

- Rà soát nguyên nhân và ngăn chặn lặp lại (quyền truy cập, cấu hình lưu trữ).

• Thời gian phản ứng:

- 1 giờ: xác định phạm vi mất dữ liệu.

- 4 giờ: khôi phục dữ liệu từ backup.

- 24 giờ: kiểm tra toàn vẹn, đưa hệ thống về trạng thái bình thường.

5. Sự cố lộ lọt tài khoản quản trị

• Kiểm tra, phát hiện: Tài khoản quản trị bị truy cập trái phép hoặc xuất hiện log đăng nhập bất thường.

• Các bước xử lý:

- Ngay lập tức khóa tài khoản bị lộ.

- Thay đổi mật khẩu, triển khai xác thực đa yếu tố.

- Kiểm tra log để xác định hành vi truy cập trái phép.

- Vá các lỗ hổng liên quan.

• Thời gian phản ứng:

- 30 phút: khóa tài khoản, thay đổi mật khẩu.

- 4 giờ: rà soát log, ngăn chặn truy cập bất thường.

- 24 giờ: khôi phục vận hành an toàn.

6. Sự cố tấn công khai thác lỗ hổng ứng dụng web

• Kiểm tra, phát hiện: Hệ thống ứng dụng có log tấn công SQL Injection, XSS hoặc hành vi bất thường.

• Các bước xử lý:

- Ngắt kết nối ứng dụng bị tấn công khỏi Internet (nếu cần).

- Vá lỗ hổng hoặc cập nhật bản vá an ninh.

- Khôi phục hệ thống từ bản sao lưu an toàn.
- Tăng cường giám sát và cập nhật tường lửa ứng dụng web (WAF).

• Thời gian phản ứng:

- 1 giờ: ngắt kết nối hoặc chặn tấn công.
- 4 giờ: triển khai bản vá, kiểm tra tính toàn vẹn dữ liệu.
- 24 giờ: đưa ứng dụng hoạt động trở lại an toàn.

PHỤ LỤC IV
QUY TRÌNH QUẢN LÝ AN TOÀN NGƯỜI SỬ DỤNG ĐẦU CUỐI

1. Mục đích

Quy trình này quy định các biện pháp đảm bảo an toàn thông tin đối với người sử dụng đầu cuối trong quá trình truy cập, sử dụng hệ thống mạng, tài nguyên và thiết bị thuộc Trung tâm dữ liệu của Viện Hàn lâm KHXH Việt Nam.

2. Phạm vi áp dụng

Áp dụng đối với tất cả cán bộ, viên chức, người lao động, tổ chức và cá nhân có quyền truy cập, sử dụng các thiết bị đầu cuối và tài nguyên mạng của hệ thống Trung tâm dữ liệu.

3. Căn cứ thực hiện

- Luật An toàn thông tin mạng năm 2015
- Quyết định 05/2017/QĐ-TTg ngày 16/3/2017
- Quy chế bảo đảm an toàn, an ninh mạng hệ thống Trung tâm dữ liệu

4. Nội dung quy trình

4.1. Quản lý truy cập và sử dụng tài nguyên

- Người sử dụng đầu cuối phải tuân thủ đầy đủ các quy định về bảo mật thông tin, không truy cập trái phép vào các tài nguyên không thuộc phạm vi trách nhiệm.
- Không truy cập từ xa trực tiếp vào máy tính nội bộ, chỉ được truy cập gián tiếp qua các giải pháp bảo mật như VPN.
- Không kết nối các thiết bị lưu trữ di động lạ khi chưa được kiểm tra an toàn bởi bộ phận chuyên trách (đảm bảo thiết bị có cài đặt phần mềm chống virus).
- Không truy cập các đường link, tệp tin đính kèm không rõ nguồn gốc hoặc đáng ngờ từ email.
- Không truy cập các website có nội dung độc hại hoặc không rõ nguồn gốc.

4.2. Quản lý truy cập mạng và Internet

- Việc cấp phát quyền truy cập dựa trên chức năng, nhiệm vụ và vai trò của từng người dùng trong hệ thống.
- Chỉ cấp quyền tối thiểu cần thiết để hoàn thành công việc (nguyên tắc least privilege).

Mọi quyền truy cập phải được quản lý tập trung và định kỳ rà soát, cụ thể:

- Người dùng thông thường: chỉ có quyền sử dụng ứng dụng, tài nguyên liên quan đến công việc.
- Quản trị hệ thống: có quyền cấu hình, quản lý thiết bị và hệ thống, nhưng phải được giám sát chặt chẽ.
- Quản trị an toàn thông tin: có quyền giám sát, kiểm tra nhật ký, điều tra sự cố, không can thiệp vào dữ liệu nghiệp vụ.
- Khách/đối tác: chỉ có quyền truy cập tạm thời, hạn chế vào các khu vực được phê duyệt.
- Trường hợp phát hiện người dùng có quyền vượt quá nhu cầu công việc phải xử lý và điều chỉnh ngay.

4.3. Cài đặt và sử dụng thiết bị an toàn

- Mật khẩu máy tính phải có độ mạnh tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt; thay đổi định kỳ 3 tháng (không đặt mật khẩu dễ đoán như 123456, password, ngày sinh). Không đặt mật khẩu cho nhiều tài khoản, hệ thống.
- Máy tính phải được khóa khi rời khỏi chỗ làm việc.
- Không tự ý thay đổi cấu hình thiết bị, phần mềm khi chưa được phép.

4.4. Trách nhiệm của người sử dụng

- Báo cáo ngay khi phát hiện hành vi nghi ngờ hoặc dấu hiệu vi phạm an toàn thông tin.
- Không chia sẻ tài khoản, mật khẩu hoặc thông tin truy cập cho người khác.
- Tuân thủ hướng dẫn của bộ phận chuyên trách trong suốt quá trình sử dụng hệ thống.
- Thường xuyên cập nhật phần mềm, hệ điều hành. Chỉ cài đặt ứng dụng từ các nguồn chính thống, nhà cung cấp chính hãng.
- Khi mất thiết bị, phải báo cáo ngay lập tức cho bộ phận ATTT để xử lý (khóa truy cập, thay đổi mật khẩu, xóa dữ liệu từ xa nếu có).

5. Xử lý vi phạm

- Người sử dụng vi phạm quy trình này tùy mức độ sẽ bị xử lý hành chính, kỷ luật hoặc truy cứu trách nhiệm theo quy định pháp luật.

6. Rà soát và cải tiến

- Quy trình này được rà soát, cập nhật định kỳ hàng quý hoặc khi có thay đổi chính sách về an toàn thông tin.
- Bộ phận ATTT định kỳ 3–6 tháng thực hiện kiểm tra danh sách người dùng và quyền truy cập.
- Nhật ký cấp phát, thay đổi và thu hồi quyền phải được lưu trữ để phục vụ kiểm tra, truy vết.

PHỤ LỤC V
QUY TRÌNH QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN

1. Mục đích

Quy trình này nhằm xác định, đánh giá, kiểm soát và giảm thiểu các rủi ro an toàn thông tin ảnh hưởng đến hệ thống công nghệ thông tin thuộc Trung tâm dữ liệu của Viện Hàn lâm Khoa học xã hội Việt Nam.

2. Phạm vi áp dụng

- Áp dụng cho toàn bộ hệ thống thông tin, máy chủ, thiết bị mạng, dữ liệu, phần mềm và các dịch vụ CNTT thuộc phạm vi quản lý của Viện Hàn lâm.

3. Căn cứ thực hiện

- Luật An toàn thông tin mạng năm 2015
- Nghị định 85/2016/NĐ-CP
- Tiêu chuẩn quốc gia TCVN ISO/IEC 27005:2011 về kỹ thuật an toàn – quản lý rủi ro an toàn thông tin
- Quy chế bảo đảm an toàn, an ninh mạng hệ thống Trung tâm dữ liệu

4. Các bước trong quy trình quản lý rủi ro

4.1. Xác định tài sản và mối đe dọa

- Liệt kê các tài sản thông tin quan trọng như: dữ liệu, phần mềm, phần cứng, dịch vụ.
- Xác định các mối đe dọa có thể gây tổn hại như: tấn công mạng, mã độc, lỗi hệ thống, thiên tai, yếu tố con người, rủi ro nội bộ,...

4.2. Đánh giá rủi ro

- Phân tích khả năng xảy ra và mức độ tác động của từng rủi ro.
- Xác định mức độ rủi ro theo ma trận: Thấp – Trung bình – Cao – Nghiêm trọng.
- Sử dụng các phương pháp đánh giá định tính (theo tiêu chí) và/hoặc định lượng (theo tổn thất ước tính).

4.3. Lựa chọn biện pháp kiểm soát

- Ưu tiên xử lý các rủi ro có mức cao và nghiêm trọng.
- Biện pháp kiểm soát có thể gồm:

- ❖ Giảm thiểu rủi ro (triển khai công nghệ, quy trình bảo vệ)
- ❖ Chấp nhận rủi ro (khi rủi ro nhỏ hoặc chi phí kiểm soát lớn hơn thiệt hại)
- ❖ Chuyển giao rủi ro (qua bảo hiểm, dịch vụ bên thứ ba)
- ❖ Tránh rủi ro (ngừng hoặc thay đổi quy trình gây ra rủi ro)

4.4. Thực hiện và giám sát

- Triển khai các biện pháp đã được lựa chọn.
- Giám sát hiệu quả thực tế của biện pháp thông qua hệ thống giám sát ATTT.
- Cập nhật danh sách rủi ro định kỳ hoặc khi có rủi ro mới phát sinh.

4.5. Đánh giá lại và cải tiến

- Định kỳ 6 tháng/lần hoặc sau mỗi sự cố nghiêm trọng, thực hiện đánh giá lại các rủi ro.
- Điều chỉnh hoặc nâng cấp các biện pháp kiểm soát nếu không còn phù hợp.
- Cập nhật Hồ sơ quản lý rủi ro và Báo cáo đánh giá rủi ro hàng quý.

5. Trách nhiệm thực hiện

Phòng Công nghệ thông tin và Kỹ thuật:

- ❖ Chủ trì đánh giá rủi ro, đề xuất và thực hiện các biện pháp kiểm soát.
- ❖ Phối hợp các đơn vị trong quá trình rà soát và xử lý rủi ro.

Các đơn vị sử dụng hệ thống:

- ❖ Phối hợp cung cấp thông tin, thực hiện các biện pháp tại đơn vị mình.

Người sử dụng cuối:

- ❖ Tuân thủ các quy định và hướng dẫn về an toàn thông tin.
- ❖ Báo cáo kịp thời khi phát hiện rủi ro hoặc sự cố bất thường.

6. Rà soát và cập nhật quy trình

- Quy trình này được rà soát định kỳ 1 năm/lần hoặc khi có:
- Thay đổi về công nghệ, tổ chức, quy định pháp lý;
- Sự cố ATTT nghiêm trọng;
- Kết quả kiểm tra, đánh giá nội bộ hoặc từ cơ quan chức năng.

PHỤ LỤC VI
QUY TRÌNH KẾT THÚC VẬN HÀNH, KHAI THÁC, THANH LÝ HỆ THỐNG THÔNG TIN

1. Mục đích

Quy trình này hướng dẫn các bước cần thiết để đảm bảo việc kết thúc vận hành, khai thác và thanh lý hệ thống thông tin được thực hiện an toàn, hiệu quả và tuân thủ quy định pháp luật, tránh thất thoát dữ liệu và rủi ro an toàn thông tin.

2. Phạm vi áp dụng

Áp dụng đối với:

- Các hệ thống thông tin, máy chủ, thiết bị mạng, lưu trữ, phần mềm,... thuộc hệ thống Trung tâm dữ liệu của Viện Hàn lâm;

- Các trường hợp kết thúc sử dụng, chuyển giao, thay thế hoặc thanh lý tài sản công nghệ thông tin.

3. Căn cứ thực hiện

- Luật An toàn thông tin mạng năm 2015;

- Luật Quản lý, sử dụng tài sản công năm 2017;

- Nghị định 85/2016/NĐ-CP;

- Quy chế bảo đảm an toàn, an ninh mạng Trung tâm dữ liệu;

- Quy định quản lý tài sản, thiết bị công nghệ thông tin nội bộ.

4. Quy trình thực hiện

4.1. Xác định hệ thống/thiết bị cần kết thúc sử dụng

- Đơn vị sử dụng đề xuất danh mục hệ thống, thiết bị hoặc phần mềm cần dừng khai thác, thanh lý.

- Lý do: hỏng hóc, lạc hậu, không còn phù hợp, chuyển đổi công nghệ, hoặc thực hiện theo kế hoạch đầu tư.

4.2. Đánh giá và phê duyệt

- Phòng CNTT & Kỹ thuật phối hợp đánh giá: tình trạng hoạt động, dữ liệu, mức độ ảnh hưởng khi dừng khai thác.

- Đề xuất biện pháp xử lý dữ liệu và tài nguyên liên quan.

- Trình Lãnh đạo Viện Hàn lâm phê duyệt kế hoạch kết thúc khai thác, thanh lý.

Bảng ma trận rủi ro:

STT	Mức độ ảnh hưởng	Dữ liệu	Vận hành	Dịch vụ
1	Thấp	Có bản sao lưu đầy đủ	Không làm ảnh hưởng hệ thống khác	Không ảnh hưởng dịch vụ
2	Trung bình	Có nguy cơ mất một phần dữ liệu	Gây gián đoạn tạm thời	Ảnh hưởng tới một nhóm người dùng, một dịch vụ
3	Cao	Nguy cơ mất dữ liệu quan trọng, rò rỉ bí mật	Gây gián đoạn nghiêm trọng, ảnh hưởng nhiều hệ thống	Dừng toàn bộ các dịch vụ, gián đoạn nghiệp vụ chính

4.3. Xử lý dữ liệu và tài nguyên thông tin

- Sao lưu và chuyển giao dữ liệu cần giữ lại sang hệ thống mới hoặc lưu trữ an toàn.

- Xóa toàn bộ dữ liệu trên thiết bị bằng phần mềm chuyên dụng, đảm bảo không thể phục hồi, bắt buộc tuân thủ theo chuẩn quốc tế (DoD 5220.22-M, NIST 800-88) hoặc sử dụng phần mềm/hệ thống xóa dữ liệu đã được Bộ Khoa học và Công nghệ công nhận.

- Thu hồi tài khoản, phân quyền truy cập, giấy phép phần mềm gắn với hệ thống.

- Đối với hệ thống thuê ngoài hoặc cloud: yêu cầu nhà cung cấp dịch vụ cung cấp chứng chỉ/xác nhận xóa dữ liệu, bàn giao đầy đủ nhật ký hệ thống (log) và các thông tin liên quan trước khi chấm dứt hợp đồng.

4.4. Gỡ bỏ và tháo dỡ hệ thống

- Ngắt kết nối thiết bị khỏi hệ thống mạng nội bộ.

- Thực hiện tháo dỡ thiết bị phần cứng, đảm bảo không gây ảnh hưởng tới các hệ thống đang hoạt động.

- Gỡ bỏ phần mềm, dịch vụ đã được cài đặt.

4.5. Thanh lý hoặc tiêu hủy thiết bị

- Trường hợp đủ điều kiện thanh lý theo quy định: tiến hành bàn giao cho bộ phận quản lý tài sản để thực hiện quy trình thanh lý tài sản công.

- Trường hợp thiết bị không còn giá trị sử dụng và chứa dữ liệu nhạy cảm: thực hiện tiêu hủy vật lý an toàn, có biên bản ghi nhận.

4.6. Lập hồ sơ và báo cáo

Hồ sơ kết thúc khai thác gồm:

+ Biên bản đánh giá, đề xuất;
+ Kế hoạch xử lý;
+ Biên bản xóa dữ liệu, gỡ bỏ phần mềm;
+ Biên bản thanh lý/tiêu hủy thiết bị;
+ Báo cáo tổng hợp gửi lãnh đạo Viện Hàn lâm.

5. Trách nhiệm thực hiện

- Phòng CNTT & Kỹ thuật**:** Chủ trì quy trình, đảm bảo ATTT trong suốt quá trình.

- Phòng Quản lý tài sản/Tài chính**:** Phối hợp thực hiện thanh lý, tiêu hủy theo đúng quy định về tài sản công.

- Đơn vị sử dụng thiết bị**:** Báo cáo đề xuất, hỗ trợ xử lý dữ liệu và kiểm kê tài sản liên quan.

- Hội đồng tiêu hủy (nếu có)**:** Giám sát và xác nhận việc tiêu hủy đúng quy trình.

6. Rà soát và cập nhật

- Quy trình được rà soát định kỳ 6 tháng/lần hoặc khi có sự thay đổi về quy định pháp luật, công nghệ, hoặc cơ cấu hệ thống thông tin.

PHỤ LỤC VII
QUY TRÌNH TRUYỀN THÔNG KHỦNG HOẢNG

1. Nguyên tắc chung

- Mọi thông tin liên quan đến sự cố an toàn thông tin nghiêm trọng phải được quản lý tập trung, tránh rò rỉ hoặc đưa tin sai lệch.

- Truyền thông phải đảm bảo chính xác – kịp thời – nhất quán, đồng thời tuân thủ quy định pháp luật về bảo mật và bí mật nhà nước.

2. Người phát ngôn chính thức

- Chỉ định 01 người phát ngôn chính thức (là Lãnh đạo Văn phòng hoặc Lãnh đạo Viện Hàn lâm được ủy quyền).

- Trong trường hợp cần thiết, có thể chỉ định thêm Trưởng phòng CNTT & Kỹ thuật để trả lời các câu hỏi chuyên môn.

- Nhân viên, bộ phận khác không tự ý phát ngôn hoặc cung cấp thông tin ra bên ngoài.

3. Cơ chế phối hợp nội bộ

- Nhóm ứng cứu sự cố phải cập nhật liên tục tình hình cho người phát ngôn và Ban lãnh đạo.

- Mọi thông cáo báo chí, nội dung gửi cơ quan quản lý, hoặc thông báo cho người dùng đều phải được phê duyệt trước khi phát hành.

- Bộ phận pháp chế rà soát các nội dung liên quan đến trách nhiệm pháp lý.

4. Phối hợp với báo chí và cơ quan quản lý

- Thông tin cho báo chí chỉ được công bố sau khi đã báo cáo và được sự đồng ý của Lãnh đạo.

- Khi có yêu cầu từ các cơ quan chức năng (Cục ATTT, VNCERT/CC, Bộ TT&TT, cơ quan công an), phải phối hợp cung cấp thông tin theo đúng quy định.

- Nội dung công bố tập trung vào: mức độ ảnh hưởng, biện pháp xử lý đang triển khai, cam kết khắc phục và bảo vệ người dùng.

5. Kênh công bố thông tin

Các kênh chính thức gồm:

+ Cổng thông tin điện tử/Website của Viện Hàn lâm.

+ Thông cáo báo chí chính thức (nếu cần).

+ Thông báo nội bộ qua email, hệ thống quản lý công việc.

Tuyệt đối không công bố thông tin qua mạng xã hội cá nhân hoặc kênh chưa được kiểm soát.

6. Đánh giá và cải tiến

- Sau khi kết thúc sự cố, tổ chức họp rút kinh nghiệm về công tác truyền thông.

- Cập nhật kịch bản truyền thông khủng hoảng để phù hợp với tình hình thực tiễn và các bài học mới.