BỘ NỘI VỤ	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
———	**Độc lập – Tự do – Hạnh phúc**
Số: 1260 /QĐ-BNV	*Hà Nội, ngày 27 tháng 10 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng của Bộ Nội vụ

BỘ TRƯỞNG BỘ NỘI VỤ

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 6 năm 2006;

Căn cứ Luật an toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015;

Căn cứ Luật an ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14, ngày 15 tháng 11 năm 2018;

Căn cứ Luật Viễn thông số 24/2023/QH15 ngày 24 tháng 11 năm 2023;

Căn cứ Nghị định số 25/2025/NĐ-CP ngày 21 tháng 2 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nội vụ;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 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 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

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

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

Theo đề nghị của Giám đốc Trung tâm 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 của Bộ Nội vụ.

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

Quyết định này thay thế Quyết định số 309/QĐ-BNV ngày 21 tháng 4 năm 2023 của Bộ trưởng Bộ Nội vụ ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng của Bộ Nội vụ; Quyết định số 674/QĐ-BNV ngày 26 tháng 9 năm 2024 của Bộ trưởng Bộ Nội vụ bổ sung một số Phụ lục của Quyết định số 309/QĐ-BNV ngày 21 tháng 4 năm 2023 của Bộ trưởng Bộ Nội vụ ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng của Bộ Nội vụ; Quyết định số 234/QĐ-BLĐTBXH ngày 06 tháng 3 năm 2024 của Bộ trưởng Bộ Lao động - Thương binh và Xã hội ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin và chuyển đổi số của Bộ Lao động - Thương binh và Xã hội.

Điều 3. Chánh Văn phòng Bộ, Giám đốc Trung tâm Công nghệ thông tin, Thủ trưởng các cơ quan, đơn vị thuộc, trực thuộc Bộ, cán bộ, công chức, viên chức, người lao động thuộc Bộ Nội vụ và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để b/cáo);
- Các đ/c Thứ trưởng;
- Bộ Khoa học và Công nghệ;
- Bộ Công an;
- Bộ Quốc phòng;
- Các đơn vị thuộc, trực thuộc Bộ (để t/h);
- Cổng thông tin điện tử Bộ Nội vụ (đăng tin);
- Lưu: VT, TTCNTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ NỘI VỤ

Trương Hải Long

BỘ NỘI VỤ	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ

Bảo đảm an toàn thông tin, an ninh mạng của Bộ Nội vụ

(Ban hành kèm theo Quyết định số 1260/QĐ-BNV ngày 27 tháng 10 năm 2025 của Bộ trưởng Bộ Nội vụ)

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 nguyên tắc quản lý và các biện pháp nhằm bảo đảm an toàn thông tin (ATTT) mạng và an ninh mạng trong hoạt động chuyển đổi số, ứng dụng công nghệ thông tin (CNTT), quản lý, quản trị, vận hành, khai thác hệ thống, hạ tầng kỹ thuật CNTT, hệ thống thông tin (HTTT), phần mềm, cơ sở dữ liệu thuộc phạm vi quản lý của Bộ Nội vụ, các hệ thống CNTT dùng chung, chuyên ngành, liên thông với bên ngoài.

2. Đối tượng áp dụng

a) Các đơn vị thuộc, trực thuộc Bộ (sau đây gọi tắt là các đơn vị); công chức, viên chức, người lao động làm việc tại các đơn vị (sau đây gọi tắt là người sử dụng).

b) Các cơ quan, tổ chức, đơn vị, cá nhân không thuộc thẩm quyền quản lý của Bộ Nội vụ có nhu cầu truy cập, khai thác dữ liệu, sử dụng dịch vụ hoặc chức năng trên các HTTT thuộc Bộ Nội vụ.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ CNTT và ATTT (nhà cung cấp dịch vụ) phục vụ cho hoạt động ứng dụng CNTT tại các đơn vị thuộc Bộ Nội vụ.

Điều 2. Giải thích từ ngữ

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

1. *Bảo đảm ATTT mạng* là việc bảo vệ thông tin, HTTT trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *Bảo đảm an ninh mạng* là việc thực hiện các biện pháp nhằm bảo vệ không gian mạng và các HTTT trên không gian mạng khỏi các hành vi xâm phạm, qua đó bảo đảm không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã

hội, cũng như bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức và cá nhân.

3. *HTTT* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. *HTTT dùng chung* là HTTT đã được Bộ đầu tư, xây dựng để thu thập, xử lý, lưu trữ và phân phối thông tin và dữ liệu phục vụ cho nhu cầu chung của Bộ và các đơn vị thuộc Bộ như: Cổng thông tin điện tử, Cổng dữ liệu, Cổng dịch vụ công, Hệ thống thư điện tử, Hệ thống quản lý văn bản và chỉ đạo, điều hành v.v...

5. *Trung tâm điều hành mạng, phòng vận hành trung tâm (Network Operation Center - NOC)*: là phòng tại đó quản trị viên hệ thống thực hiện việc quản lý, quản trị, vận hành, giám sát toàn bộ hệ thống mạng.

6. *Chủ quản HTTT* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với HTTT.

7. *Sự cố ATTT mạng* là việc thông tin, HTTT bị tấn công, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Ứng cứu các sự cố ATTT mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất ATTT mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, kiểm tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của HTTT.

9. *Lỗ hổng bảo mật* là điểm yếu về ATTT trên phần mềm hoặc phần cứng, bị tin tặc khai thác để truy cập trái phép vào HTTT.

10. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ HTTT hoặc thực hiện mã hóa dữ liệu, sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong HTTT.

11. *Phần mềm diệt virus* là phần mềm có tính năng phát hiện, loại bỏ các virus máy tính, khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus mới.

12. *Mạng riêng ảo (Virtual Private Network - VPN)* là dịch vụ mạng dùng riêng để kết nối máy tính của các cơ quan, đơn vị hoặc máy tính cá nhân truy cập vào mạng nội bộ để đảm bảo an toàn, an ninh thông tin trên đường truyền.

13. *Tường lửa (Firewall)* có thể là phần cứng hoặc phần mềm, sử dụng các quy tắc để giám sát, kiểm soát lưu lượng truy cập vào, ra hệ thống.

14. *Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS)* là phần mềm ứng dụng hoặc thiết bị được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống.

15. *Hệ thống ngăn ngừa xâm nhập (Intrusion Prevention System - IPS)* là hệ thống phát hiện xâm nhập có khả năng theo dõi, giám sát và ngăn chặn kịp thời các hoạt động xâm nhập không mong muốn đối với HTTT.

16. *Vùng mạng nội bộ (Local Area Network - LAN)* là một hệ thống mạng nội bộ kết nối các thiết bị như máy tính, máy in, và các thiết bị khác trong một khu vực nhỏ. Mạng LAN cho phép các thiết bị trong mạng LAN chia sẻ tài nguyên như máy in, dữ liệu, và kết nối internet.

17. *Vùng mạng biên* được thiết kế nhằm mục đích kết nối HTTT với các mạng bên ngoài và mạng Internet, đồng thời đóng vai trò bảo vệ HTTT trước các truy cập không hợp lệ từ Internet.

18. *Vùng mạng DMZ* là vùng mạng trung lập giữa mạng nội bộ và mạng Internet, là nơi chứa các thông tin cho phép người dùng từ Internet truy xuất vào và chấp nhận các rủi ro tấn công từ Internet.

19. *Vùng máy chủ nội bộ* đặt các máy chủ nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống.

20. *Mật khẩu mạnh là* mật khẩu bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt (!,@,#,$,...) có độ dài tối thiểu 8 ký tự trở lên.

21. *Mã kiểm tra tính toàn vẹn (checksum)* là một giá trị được tạo ra từ dữ liệu thông qua một thuật toán xác định, nhằm mục đích kiểm tra và xác minh tính toàn vẹn của dữ liệu trong quá trình truyền tải hoặc lưu trữ.

Điều 3. Mục tiêu, nguyên tắc bảo đảm ATTT, an ninh mạng

1. Mục tiêu

Việc ban hành Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm thiểu các nguy cơ gây mất ATTT, an ninh mạng; bảo vệ thông tin, HTTT trong quá trình ứng dụng CNTT trong hoạt động của Bộ và các đơn vị thuộc và trực thuộc Bộ.

2. Nguyên tắc

a) Hoạt động ứng dụng CNTT của các đơn vị phải tuân thủ theo nguyên tắc bảo vệ ATTT mạng được quy định tại Điều 41 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước, Điều 4 Luật An ninh mạng và Điều 4 Luật An toàn thông tin mạng.

b) Bảo đảm ATTT, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, xuyên suốt quá trình thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu; thiết kế, xây dựng, quản lý vận hành, nâng cấp, hủy bỏ HTTT.

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

d) Công chức, viên chức, người lao động của Bộ Nội vụ có trách nhiệm bảo đảm ATTT, an ninh mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Bộ, nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp bảo đảm ATTT mạng.

3. Phạm vi quản lý ATTT, an ninh mạng

Phạm vi quản lý ATTT tại quy chế này bao gồm:

a) Thiết lập các quy tắc ATTT.

b) Tổ chức bảo đảm ATTT.

c) Bảo đảm nguồn nhân lực.

d) Quản lý thiết kế, xây dựng hệ thống.

đ) Quản lý vận hành hệ thống.

e) Ứng phó, khắc phục sự cố an ninh mạng.

g) Kiểm tra, đánh giá an ninh mạng.

Điều 4. Những hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 12 Luật Công nghệ thông tin, Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Cơ quan, đơn vị, người sử dụng tự ý đấu nối thiết bị mạng, máy tính cá nhân, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng không dây của cá nhân vào mạng nội bộ và lắp đặt các thiết bị tiếp sóng Wifi (Wireless Card, Wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng Wifi bên ngoài.

3. Tự ý thay đổi, gỡ bỏ biện pháp ATTT đã cài đặt trên thiết bị CNTT phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi linh kiện máy tính của cơ quan, đơn vị.

4. Chia sẻ thông tin cho người ngoài cơ quan, đơn vị như: mật khẩu, tài khoản truy cập vào các HTTT của Bộ như: tài khoản hệ thống quản lý văn bản và chỉ đạo, điều hành (Voffice), thư điện tử công vụ (Email), hệ thống mạng Internet không dây (Wifi), hệ thống VPN.

5. Sử dụng hộp thư điện tử công vụ (@moha.gov.vn) cho mục đích cá nhân như: đăng ký các trang mạng xã hội, dịch vụ thương mại, dịch vụ trao đổi chia sẻ thông tin cá nhân.

6. Soạn thảo, lưu trữ văn bản có chứa nội dung bí mật nhà nước trên máy tính có kết nối Internet, thiết bị ngoại vi không đúng quy định của pháp luật về

bảo vệ bí mật nhà nước; chia sẻ văn bản mật thông qua Internet; kết nối máy tính chứa tài liệu có nội dung bí mật nhà nước với mạng Internet.

7. Cài đặt các phần mềm không có bản quyền, các phần mềm đã bị bẻ khóa.

8. Người sử dụng ngăn cản, gây khó khăn, không hợp tác khi công chức, viên chức chuyên trách về CNTT, ATTT cài đặt các phần mềm diệt virus, giám sát ATTT trên máy tính người sử dụng.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG TỔ CHỨC

Điều 5. Đơn vị chuyên trách và phối hợp trong công tác bảo đảm ATTT, an ninh mạng

1. Trung tâm Công nghệ thông tin, Bộ Nội vụ là đơn vị chuyên trách về ATTT của Bộ Nội vụ.

2. Trung tâm Công nghệ thông tin là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền trong công tác tiếp nhận, xử lý sự cố ATTT mạng và triển khai các biện pháp bảo đảm ATTT, an ninh mạng cho các HTTT thuộc Bộ Nội vụ.

3. Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan tổ chức kiểm tra công tác bảo đảm ATTT, an ninh mạng định kỳ hàng năm hoặc theo chỉ đạo của Lãnh đạo Bộ.

4. Trung tâm Công nghệ thông tin và các đơn vị có liên quan có trách nhiệm phối hợp với cơ quan chức năng trong công tác hỗ trợ điều phối xử lý sự cố ATTT, an ninh mạng khi có yêu cầu.

5. Trung tâm Công nghệ thông tin có trách nhiệm tham gia các hoạt động, nhiệm vụ bảo đảm ATTT, an ninh mạng theo yêu cầu của cơ quan, tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

Công chức, viên chức, người lao động được tuyển dụng vào vị trí việc làm ATTT có trình độ, chuyên ngành về lĩnh vực CNTT, ATTT, phù hợp với vị trí tuyển dụng, đáp ứng được các quy định của cơ quan nhà nước có thẩm quyền.

Điều 7. Quy định về việc thực hiện bảo đảm ATTT trong quá trình làm việc

1. Đối với người sử dụng:

- Có trách nhiệm tuân thủ các quy định, hướng dẫn bảo đảm ATTT và các quy định của pháp luật, đảm bảo ATTT đối với từng vị trí công việc. Máy tính, thiết bị mạng trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp

ứng các yêu cầu về ATTT;

- Thông báo ngay cho đơn vị chủ quản HTTT khi nghi ngờ hoặc phát hiện sự cố, hiện tượng bất thường của HTTT;

- Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về ATTT, an ninh mạng;

- Chịu trách nhiệm trước pháp luật về các hành vi làm lộ, lọt thông tin, nội dung bí mật nhà nước do không tuân thủ, quy định của pháp luật, Bộ Nội vụ;

- Đổi mật khẩu ngay sau khi được cấp tài khoản đăng nhập các dịch vụ, ứng dụng của Bộ Nội vụ (Thư điện tử công vụ; hệ thống quản lý văn bản; cơ sở dữ liệu về công chức, viên chức của Bộ Nội vụ...). Giữ bí mật tài khoản cá nhân khi tham gia khai thác, sử dụng mạng Bộ Nội vụ;

- Chịu trách nhiệm quản lý, sử dụng trang thiết bị CNTT được giao, bảo đảm ATTT; không được giao cho các tổ chức, cá nhân khác sử dụng trang thiết bị CNTT đã được giao sử dụng; không được sử dụng trang thiết bị CNTT cá nhân để kết nối, truy cập vào các HTTT nội bộ nếu chưa được phép của đơn vị chủ quản; không tự thay thế, lắp mới, tráo đổi linh kiện của máy tính công vụ; không mang tài sản CNTT của đơn vị ra ngoài nếu chưa được phép của thủ trưởng đơn vị; có trách nhiệm bàn giao cho đơn vị quản lý các trang thiết bị CNTT khi chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ việc.

- Tự bảo quản dữ liệu cá nhân, sao lưu dữ liệu cá nhân ra các thiết bị lưu trữ như ổ USB, ổ cứng di động (không sao lưu dữ liệu có nội dung thuộc phạm vi bí mật nhà nước vào thiết bị lưu trữ cá nhân).

- Không được phép cung cấp, chia sẻ hoặc tiết lộ các thông tin đã được tiếp cận trong quá trình thực hiện nhiệm vụ cho bất kỳ tổ chức, cá nhân nào khi chưa có ý kiến chấp thuận hoặc văn bản cho phép của người có thẩm quyền.

- 2. Đối với đội ngũ quản lý, vận hành hệ thống:

- Phân rõ trách nhiệm quản lý, vận hành HTTT đến từng cá nhân; không giao cho một người quản trị tất cả chức năng về ATTT, an ninh mạng của HTTT;

- Quản trị viên hệ thống khi giám sát, điều khiển HTTT phải thông qua Trung tâm điều hành - NOC, không dùng thiết bị cá nhân để giám sát, điều khiển HTTT;

- Máy tính dùng để quản trị HTTT phải được đặt trong phòng NOC; máy tính được cài đặt các chương trình quản trị HTTT và không kết nối mạng Internet, được cài đặt chương trình diệt virus có bản quyền;

- Kết nối từ xa vào HTTT phải thông qua VPN, có sự giám sát của quản trị viên hệ thống;

- Thực hiện chặt chẽ việc kiểm soát thay đổi của HTTT: Phiên bản phần mềm, cấu hình phần cứng, tài liệu, quy trình vận hành; ghi đầy đủ thông tin mạng trong các bản ghi nhật ký hệ thống và lưu trữ nhật ký tối thiểu 06 tháng để phục vụ việc quản lý, kiểm soát thông tin mạng.

- Không được phép cung cấp, chia sẻ hoặc tiết lộ các thông tin đã được tiếp cận trong quá trình thực hiện nhiệm vụ cho bất kỳ tổ chức, cá nhân nào khi chưa có ý kiến chấp thuận hoặc văn bản cho phép của người có thẩm quyền.

Điều 8. Quy định đối với công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc

1. Công chức, viên chức, người lao động khi nghỉ việc hoặc chuyển công tác có trách nhiệm thực hiện đầy đủ việc bàn giao tài sản CNTT, dữ liệu, tài khoản truy cập và các nội dung liên quan theo quy định của cơ quan, đơn vị. Việc bàn giao phải được lập thành biên bản có xác nhận của các bên liên quan và lưu tại đơn vị quản lý. Cá nhân có trách nhiệm cam kết bảo mật thông tin mà mình đã tiếp cận, quản lý trong quá trình công tác tại cơ quan, đơn vị.

2. Quy trình chấm dứt hoặc thay đổi công việc theo Phụ lục I.

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

Điều 9. Quản lý thiết kế, xây dựng HTTT

1. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành HTTT:

- Tài liệu phân tích lựa chọn kiến trúc, công nghệ;

- Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống;

- Các giải pháp, thiết bị của HTTT đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ (Thông tư số 12/2022/TT-BTTTT).

2. Đơn vị thiết kế, xây dựng HTTT phải cung cấp các tài liệu "Kiến trúc hệ thống" trong đó có mô tả thiết kế và các thành phần của HTTT thông qua một số mô hình kiến trúc khác nhau nhằm miêu tả hệ thống dưới nhiều góc nhìn khác nhau, bao gồm:

- Thiết kế kiến trúc ứng dụng;

- Thiết kế kiến trúc dữ liệu;

- Thiết kế kiến trúc vật lý.

3. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả phương án bảo đảm ATTT theo cấp độ được quy định tại Thông tư số 12/2022/TT-BTTTT.

4. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT, trong đó cần đảm bảo các tiêu chí:

- Đảm bảo có từ 2 - 3 công nghệ được phân tích và đưa ra phương án lựa chọn;

- Phân tích các ưu, nhược điểm của từng công nghệ để từ đó chọn ra công nghệ áp dụng phù hợp nhất.

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

Khi có thay đổi thiết kế, đơn vị thiết kế, xây dựng HTTT, cần phối hợp với các đơn vị liên quan đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, xây dựng kế hoạch trước khi có thay đổi, kèm theo các tài liệu sau:

- Căn cứ thực hiện thay đổi (công văn, tờ trình);

- Kế hoạch chi tiết các bước thực hiện.

6. Phương án quản lý và bảo vệ hồ sơ thiết kế

Hồ sơ thiết kế được sắp xếp một cách khoa học để dễ quản lý, dễ nộp lưu và dễ tìm khi cần. Hồ sơ thiết kế được giữ gìn bí mật, bảo quản theo chế độ tài liệu mật, không được mang hồ sơ thiết kế ra khỏi cơ quan hoặc tùy tiện cung cấp hồ sơ thiết kế cho cá nhân, đơn vị khác.

Điều 10. Phát triển phần mềm

1. Đối với các nội dung liên quan đến việc phát triển phần mềm, đơn vị được thuê khoán phải đảm bảo có các tài liệu sau:

- Biên bản làm việc;

- Biên bản thống nhất nội dung công việc;

- Hợp đồng giữa các đơn vị;

- Hồ sơ liên quan đến ATTT, bảo mật của phần mềm, cơ sở dữ liệu; các cam kết đảm bảo ATTT, an ninh mạng.

2. Nhà phát triển phần mềm phải cung cấp mã nguồn sản phẩm cho đơn vị xây dựng phần mềm theo hình thức ghi đĩa DVD hoặc USB; yêu cầu tệp trên DVD, USB cần phải đặt mật khẩu để đảm bảo ATTT

- Mã nguồn đã được nhà phát triển tự đánh giá và có biên bản kiểm thử, đánh giá Đạt trước khi bàn giao cho đơn vị thuê.

- Phối hợp với đơn vị chủ quản HTTT đánh giá mã nguồn và có phương án xử lý lỗi (nếu có).

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

Đơn vị thuê và đơn vị phát triển phối hợp thực hiện kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng:

- Mã nguồn phải được đánh giá ATTT trước khi đưa vào môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.

- Tất cả các lỗi liên quan đến mã nguồn (nếu có) sau khi được khắc phục, phải được đánh giá ATTT và có biên bản đánh giá trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng

Hệ thống được đầu tư phải được kiểm định ATTT trước khi đưa vào vận hành khai thác:

- Kiểm tra hệ thống, mã nguồn có các lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá ATTT hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo vá hoàn toàn các lỗ hổng bảo mật.

- Thực hiện nâng cấp, xử lý điểm yếu ATTT của thiết bị hệ thống trước khi đưa vào sử dụng.

- Máy chủ phải được cài đặt hệ điều hành, phần mềm, phần mềm diệt virus có bản quyền.

5. Kiểm tra, đánh giá ATTT cho phần mềm khi thay đổi mã nguồn, kiến trúc phần mềm

Khi có thay đổi thiết kế, đơn vị thuê và đơn vị phát triển phần mềm phối hợp đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, cần xây dựng kế hoạch trước khi có thay đổi bao gồm tối thiểu các tài liệu sau:

- Căn cứ thực hiện thay đổi (công văn, tờ trình);

- Kế hoạch chi tiết các bước thực hiện.

6. Cam kết đảm bảo tính bí mật của mã nguồn và bản quyền của phần mềm phát triển:

- Bên phát triển phải có cam kết về bảo đảm tính bí mật của mã nguồn, không cung cấp cho tổ chức hoặc cá nhân khác.

- Bên phát triển có cam kết không có tranh chấp về bản quyền phát triển của phần mềm.

- Các cá nhân tham gia phát triển, triển khai HTTT phải ký biên bản cam kết bảo mật ATTT.

Điều 11. Thử nghiệm và nghiệm thu hệ thống

1. Thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

Các sản phẩm, thiết bị được đầu tư trong hệ thống phải được kiểm định ATTT trước khi đưa vào vận hành khai thác:

- Kiểm tra phiên bản phần mềm cho phần cứng (firmware) các thiết bị mạng quan trọng như: Tường lửa, Switch, IDS/IPS,... có lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo ATTT;

- Các thiết bị hệ thống trước khi được đưa vào sử dụng phải được qua kiểm định về an ninh, an toàn, cháy nổ theo quy định của các cơ quan chức năng; thực hiện nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng;

- Đảm bảo máy chủ không chứa mã độc; thực hiện gỡ bỏ các hệ điều hành cũ đối với máy chủ và thực hiện xóa dữ liệu (Format) đối với các ổ cứng trước khi đưa vào sử dụng.

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

a) Hệ thống được thử nghiệm tổng thể trước khi đưa vào sử dụng và định kỳ hàng năm để đảm bảo tính an toàn, thống nhất của hệ thống.

b) Nội dung, kế hoạch và quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước.

c) Quy trình thử nghiệm và nghiệm thu hệ thống theo Phụ lục II.

3. Cơ quan có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống

Chủ quản HTTT đảm nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống như sau:

- Kiểm thử, nghiệm thu chức năng của hệ thống;

- Kiểm thử, nghiệm thu bảo đảm ATTT;

- Kiểm thử, nghiệm thu hệ thống nội bộ của đơn vị phát triển.

4. 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. Báo cáo nghiệm thu được ký xác nhận của Trung tâm Công nghệ thông tin, Bộ Nội vụ và phê duyệt của chủ quản HTTT trước khi đưa vào sử dụng.

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

Điều 12. Quản lý an toàn mạng

1. Quản lý, vận hành, duy trì hoạt động bình thường của HTTT:

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

b) Hằng tháng kiểm tra cấu hình, các tệp nhật ký hoạt động của hệ điều hành, phần mềm, các thiết bị mạng nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

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

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm, các thiết bị mạng. Đối với các bản vá lỗ hổng bảo mật nghiêm trọng, phải thực hiện trong vòng 48 giờ kể từ khi nhận được thông báo từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

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

g) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

h) Sử dụng các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

i) Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng, thiết bị lưu trữ, máy chủ.

k) Triển khai thiết bị cảnh báo môi trường, đồng thời tích hợp chức năng gửi cảnh báo trực tiếp đến người quản trị hệ thống thông qua tin nhắn điện thoại (SMS) hoặc qua ứng dụng cài đặt trên điện thoại di động (App), khi nhiệt độ tại Trung tâm tích hợp dữ liệu tăng cao, có nguy cơ ảnh hưởng đến hoạt động của các thiết bị.

l) Thực hiện kiểm tra, bảo dưỡng hệ thống điều hòa và máy hút ẩm trong

Trung tâm tích hợp dữ liệu định kỳ hằng tháng, đảm bảo hệ thống điều hòa và máy hút ẩm vận hành liên tục 24/7.

m) Duy trì ít nhất 02 đường truyền mạng Internet từ các nhà cung cấp dịch vụ Internet khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

n) Mật khẩu của các tài khoản thiết bị, ứng dụng, phần mềm, cơ sở dữ liệu phải được đặt mật khẩu mạnh.

o) Các hệ thống phát mạng không dây (wifi) phải được đặt mật khẩu và tách biệt với mạng nội bộ.

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

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

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c) Triển khai hệ thống, phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d) Triển khai hệ thống, phương tiện chống thất thoát dữ liệu trong hệ thống.

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

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

b) Quản trị viên hệ thống có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho công chức, viên chức quản lý cấp trên để tiến hành ngăn chặn, thu hồi quyền truy cập của các tài khoản vi phạm.

c) Thiết lập quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) hệ thống và nghiêm chỉnh thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

4. Quy trình quản lý an toàn mạng theo Phụ lục III.

Điều 13. Quản lý an toàn máy chủ

1. 1. ệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục.

2. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho toàn bộ HTTT.

3. Máy chủ phải được thiết lập cơ chế xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung để cảnh báo các hoạt động bất thường của máy chủ (CPU, RAM, ổ cứng quá tải,…); thực hiện biện pháp phòng chống xâm nhập; phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao.

4. Máy chủ phải được nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng.

5. Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.

6. Phần mềm, hệ điều hành cài trên máy chủ phải có bản quyền hoặc phần mềm, hệ điều hành mã nguồn mở phổ biến được kiểm định về bảo mật trong nước hoặc quốc tế.

7. Có tài liệu liệt kê các phần mềm cài trên máy chủ.

8. Có vùng mạng quản trị riêng, giới hạn địa chỉ IP quản trị để người quản trị truy cập vào quản trị các máy chủ.

9. Người quản trị chỉ được cấp quyền truy cập vào các máy chủ có thẩm quyền. Để được cấp tài khoản quản trị phải gửi công văn xin cấp bao gồm các thông tin tối thiểu: Tên, căn cước công dân, số điện thoại, phòng ban đơn vị công tác, mục đích, phạm vi máy chủ cần truy cập... và được phê duyệt bởi đơn vị quản lý HTTT.

10. Lưu trữ nhật ký (log) ít nhất là 12 tháng đối với các hoạt động tác động đến máy chủ của người sử dụng, bao gồm lỗi phát sinh và sự cố, nhằm hỗ trợ công tác điều tra và giám sát sau này.

11. Quy trình quản lý an toàn máy chủ theo Phụ lục IV.

Điều 14. Quản lý an toàn với ứng dụng

1. Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật.

2. Ứng dụng phải được thiết lập cơ chế xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

3. Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

4. Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

5. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

6. Quy định sử dụng hộp thư điện tử:

a) Không sử dụng các hộp thư điện tử công cộng trong công việc; không sử dụng thư điện tử công vụ vào mục đích cá nhân.

b) Mỗi cá nhân cần đặt mật khẩu mạnh cho hộp thư điện tử của mình.

c) Thời hạn thu hồi hộp thư điện tử cá nhân như sau:

- Đối với Lãnh đạo cấp phòng, ban trở xuống sẽ khóa ngay chức năng gửi, nhận thư từ hộp thư cá nhân và tự động thu hồi sau 03 tháng kể từ thời điểm cá nhân đó chính thức nghỉ hưu, nghỉ việc hoặc chuyển công tác;

- Đối với Lãnh đạo cấp Vụ, Cục và tương đương trở lên sẽ khóa chức năng gửi, nhận thư từ hộp thư cá nhân sau 01 tháng và tự động thu hồi sau 06 tháng kể từ thời Điểm cá nhân đó chính thức nghỉ hưu, nghỉ việc hoặc chuyển công tác.

d) Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án bảo đảm an toàn, duy trì khả năng truy cập hệ thống thư điện tử cả trong nội bộ và trên Internet, đồng thời triển khai giải pháp phòng chống thư rác hiệu quả.

đ) Bảo đảm an toàn cho hệ thống thư điện tử: Thực hiện theo hướng dẫn của Bộ Công an và các đơn vị có liên quan.

7. Quy định đối với Cổng, trang thông tin điện tử

a) Quản lý toàn bộ các phiên bản của mã nguồn, tổ chức mô hình Cổng, trang thông tin điện tử hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu HTTT của Cổng, trang thông tin điện tử phải có các hệ thống phòng vệ như tường lửa, thiết bị phát hiện, phòng chống xâm nhập (IDS/IPS), tường lửa web (WAF- Web Application Firewall).

b) Trước khi đưa vào sử dụng hoặc tích hợp thêm chức năng mới, Cổng,

trang thông tin điện tử cần được đánh giá, kiểm định để phát hiện và phòng tránh các lỗ hổng bảo mật thường gặp.

c) Xây dựng phương án sao lưu, phục hồi cho Cổng, trang thông tin điện tử, trong đó cần lưu ý: thực hiện sao lưu dữ liệu hàng ngày; định kỳ hàng tháng tiến hành sao lưu toàn bộ nội dung của Cổng, trang thông tin điện tử, bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... nhằm bảo đảm khả năng khôi phục hệ thống trong vòng 24 giờ khi xảy ra sự cố.

8. Quy trình quản lý an toàn ứng dụng theo Phụ lục V.

Điều 15. Quản lý an toàn dữ liệu

1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố ATTT mạng xảy ra.

3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống.

4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

7. Định kỳ 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.

8. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ, phương tiện lưu trữ.

9. Quy trình quản lý an toàn dữ liệu theo Phụ lục VI.

Điều 16. Quản lý an toàn thiết bị đầu cuối

Các thiết bị đầu cuối khi kết nối vào hệ thống phải được quản lý như sau:

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

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

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

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

5. Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng và thực hiện quy trình quản lý an toàn thiết bị đầu cuối khi đưa vào sử dụng trong hệ thống.

a) Máy tính người dùng trước khi đưa vào sử dụng phải được đánh giá, rà soát các điểm yếu ATTT. Cài đặt hoặc cập nhật các bản vá cho phần mềm, hệ điều hành.

b) Gỡ bỏ các phần mềm không cần thiết, cài đặt chương trình diệt virus. Không cấp tài khoản quản trị máy tính cho người dùng, không để người dùng tự ý cài đặt các phần mềm trên máy tính.

6. Kiểm tra, đánh giá, xử lý điểm yếu ATTT cho thiết bị đầu cuối trước khi đưa vào sử dụng.

7. Quy trình quản lý an toàn thiết bị đầu cuối theo Phụ lục VII.

Điều 17. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm diệt virus có bản quyền. Các phần mềm diệt virus phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tệp.

2. Văn bản điện tử gửi qua hệ thống thư điện tử phải sử dụng định dạng phù hợp, các định dạng này bao gồm các loại tệp văn bản, bảng tính, trình chiếu và hình ảnh phổ biến. Tuyệt đối không gửi các tệp có khả năng thực thi.

3. Công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp trên các thiết bị lưu trữ di động.

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

6. Trước khi cài đặt và sử dụng, phần mềm ứng dụng phải được kiểm tra, đảm bảo không có phần mềm độc hại. Toàn bộ tệp tin và thư mục liên quan phải được quét mã độc trước khi thực hiện sao chép hoặc sử dụng.

7. 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.

8. Quy trình quản lý phòng chống phần mềm độc hại theo Phụ lục VIII.

Điều 18. Quản lý giám sát an toàn HTTT

1. Công tác triển khai: Hệ thống giám sát trung tâm; thông tin giám sát và danh mục các đối tượng giám sát; thực thi nhiệm vụ giám sát; nâng cao năng lực hoạt động giám sát; trách nhiệm giám sát ATTT của các HTTT Bộ Nội vụ được thực hiện theo Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn HTTT.

2. Chủ quản HTTT quan trọng về an ninh quốc gia phối hợp với Cục An ninh mạng và phòng chống tội phạm công nghệ cao của Bộ Công an triển khai giám sát an ninh mạng đối với HTTT quan trọng về an ninh quốc gia theo quy định tại khoản 3 Điều 15 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.

3. Các đơn vị trực thuộc Bộ có trách nhiệm phối hợp với Trung tâm Công nghệ thông tin, Bộ Nội vụ; Vụ Kế hoạch - Tài chính lập dự toán, trình phê duyệt, phân bổ kinh phí thực hiện nhiệm vụ giám sát từ nguồn ngân sách nhà nước và các nguồn vốn hợp pháp khác theo quy định của pháp luật và hướng dẫn của cơ quan chức năng.

4. Quy trình quản lý giám sát an toàn HTTT theo Phụ lục IX.

Điều 19. Quản lý điểm yếu ATTT

1. Chủ quản HTTT có trách nhiệm:

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

b) Quản trị viên hệ thống báo cáo lãnh đạo, công chức, viên chức quản lý ngay khi phát hiện điểm yếu ATTT ở mức độ nghiêm trọng; thực hiện cảnh báo và xử lý điểm yếu ATTT theo chỉ đạo. Việc xử lý điểm yếu ATTT phải bảo đảm không làm ảnh hưởng, gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu ATTT chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống, hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu ATTT cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

3. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu ATTT cho toàn bộ HTTT; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu ATTT thông tin khi có thông tin hoặc nhận được cảnh báo.

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ.

a) Đơn vị chủ quản HTTT có trách nhiệm chỉ đạo, tổ chức thực hiện kiểm tra, đánh giá ATTT và quản lý rủi ro ATTT trong phạm vi cơ quan, tổ chức mình, cụ thể như sau:

- Định kỳ 02 năm thực hiện kiểm tra, đánh giá ATTT và quản lý rủi ro ATTT tổng thể trong hoạt động của cơ quan, tổ chức mình;

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá ATTT và quản lý rủi ro ATTT đối với các hệ thống cấp độ 3 và cấp độ 4;

- Việc kiểm tra, đánh giá ATTT và đánh giá rủi ro ATTT đối với hệ thống từ cấp độ 3 trở lên phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

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

- Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống là việc thực hiện dò quét, phát hiện lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập hệ thống và đánh giá nguy cơ, thiệt hại có thể có của HTTT khi bị đối tượng tấn công xâm nhập.

- Đơn vị chủ trì đánh giá là một trong những tổ chức sau đây:

+ Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (A05), Bộ Công an;

+ Trung tâm Công nghệ thông tin, Bộ Nội vụ;

+ Tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp;

+ Doanh nghiệp đã được cấp phép cung cấp dịch vụ kiểm tra, đánh giá ATTT mạng hoặc tổ chức khác được chủ quản HTTT cho phép thực hiện đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

- Đơn vị chủ trì đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống có trách nhiệm:

+ Thông báo cho chủ quản HTTT về điểm yếu ATTT phát hiện ra nhằm khắc phục, phòng tránh các sự cố ATTT;

+ Thực hiện công tác bảo đảm an toàn cho dữ liệu liên quan đến hệ thống được đánh giá, không công bố dữ liệu liên quan khi chưa được sự đồng ý của chủ quản HTTT;

+ Việc đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống phải bảo đảm không ảnh hưởng đến hoạt động bình thường của hệ thống.

5. Quy trình quản lý điểm yếu ATTT theo Phụ lục X.

Điều 20. Quản lý sự cố ATTT

1. Thành lập đội ứng cứu sự cố an ninh mạng, ATTT của Bộ Nội vụ

Đội ứng cứu sự cố an ninh mạng, ATTT của Bộ Nội vụ có Quy chế hoạt động riêng quy định về tổ chức, nhiệm vụ, quyền hạn, nguyên tắc hoạt động và cơ chế phối hợp của đội ứng cứu sự cố an ninh mạng, ATTT của Bộ Nội vụ (Đội). Đội có nhiệm vụ theo dõi, phát hiện, cảnh báo, xử lý và khắc phục các sự cố mất ATTT trong các đơn vị thuộc, trực thuộc Bộ Nội vụ. Cơ quan thường trực của Đội là Trung tâm Công nghệ thông tin.

Đội hoạt động theo nguyên tắc phối hợp liên ngành, xử lý sự cố theo quy trình thống nhất, bảo đảm bí mật và hiệu quả. Thành viên đội làm việc theo chế độ kiêm nhiệm, có trách nhiệm tham gia đầy đủ các cuộc họp, diễn tập và hoạt động xử lý sự cố khi có yêu cầu.

Kinh phí hoạt động được đảm bảo từ ngân sách nhà nước. Các cơ quan, tổ chức, cá nhân liên quan có trách nhiệm phối hợp và tạo điều kiện để Đội thực hiện nhiệm vụ.

2. Phân nhóm sự cố ATTT mạng

a) Hệ thống bị gián đoạn dịch vụ.

b) Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ.

c) Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được.

d) Hệ thống bị mất quyền điều khiển.

đ) Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các HTTT cấp độ 3 hoặc cấp độ 4 hoặc cấp độ 5 khác.

e) Chủ quản HTTT không đủ khả năng tự kiểm soát, xử lý được sự cố.

3. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng

Đơn vị vận hành HTTT khi phát hiện hoặc nhận được thông báo sự cố đối với HTTT do mình quản lý, phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình;

- Ngay sau khi nhận được thông báo hoặc báo cáo ban đầu về sự cố, các tổ chức, cá nhân có liên quan có trách nhiệm phản hồi kịp thời cho Trung tâm Công nghệ thông tin, Bộ Nội vụ để xác nhận việc đã tiếp nhận thông báo hoặc báo cáo sự cố;

- Chủ trì, phối hợp với Trung tâm Công nghệ thông tin, Bộ Nội vụ và các đơn vị chức năng liên quan tiến hành phân tích, xác minh, đánh giá tình hình, sơ bộ phân loại sự cố và triển khai ngay các hoạt động ứng cứu sự cố và báo cáo theo quy định;

- Báo cáo về sự cố, diễn biến tình hình ứng cứu sự cố, đề xuất hỗ trợ ứng cứu sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản HTTT.

4. Kế hoạch ứng cứu sự cố ATTT mạng

a) Xác định sự cố ATTT và nguyên tắc, phương châm ứng cứu sự cố.

b) Các lực lượng tham gia ứng cứu sự cố.

c) Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng tham gia ứng cứu sự cố.

5. Giám sát, phát hiện và cảnh báo sự cố ATTT

a) Chủ quản HTTT phối hợp với các đơn vị liên quan xây dựng các công cụ giám sát phát hiện và cảnh báo sự cố ATTT mạng.

b) Chủ quản HTTT phối hợp với các đơn vị liên quan cử nhân sự ATTT trực giám sát 24/7 hoạt động của hệ thống. Các hoạt động cần giám sát: ATTT mạng, ATTT máy chủ, ATTT ứng dụng, ATTT cơ sở dữ liệu thông qua hệ thống giám sát tập trung.

c) Khi phát hiện sự cố ATTT, nhân sự ATTT trực giám sát có trách nhiệm gọi điện và email cảnh báo tới các đầu mối đơn vị, chỉ huy đơn vị trong vòng 24h tùy thuộc vào mức độ nghiêm trọng của sự cố.

6. Quy trình ứng cứu sự cố ATTT thông thường

a) Phát hiện hoặc tiếp nhận sự cố.

b) Xác minh, phân tích, đánh giá và phân loại sự cố.

c) Chủ quản HTTT lựa chọn phương án tối ưu; lập kế hoạch ứng cứu và phân công thực hiện ứng cứu.

d) Phục hồi hệ thống.

đ) Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp đảm bảo ATTT. Thực hiện báo cáo và tài liệu hóa quá trình ứng cứu sự cố để áp dụng trong tương lai.

e) Rút ra bài học kinh nghiệm phục vụ huấn luyện đào tạo.

g) Kết thúc.

7. Quy trình ứng cứu sự cố ATTT nghiêm trọng

Thực hiện đầy đủ các nội dung quy định tại Điều 14, 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 ATTT mạng quốc gia.

a) Phát hiện hoặc tiếp nhận sự cố.

b) Xác minh, phân tích, đánh giá và phân loại sự cố.

c) Cơ quan thường trực quyết định lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp.

d) Triển khai phương án ứng cứu ban đầu.

đ) Triển khai phương án ứng cứu khẩn cấp.

e) Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia.

g) Kết thúc.

8. Cơ chế phối hợp với cơ quan chức năng, các chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố ATTT

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

- 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 ATTT; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

- Trách nhiệm của người dùng: Thông tin, báo cáo kịp thời cho công chức, viên chức chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào HTTT của đơn vị; phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

9. Định kỳ tổ chức diễn tập phương án xử lý sự cố ATTT

- Tổ chức diễn tập phương án xử lý sự cố ATTT, tối thiểu 01 lần/năm. Trung tâm Công nghệ thông tin, Bộ Nội vụ lập kế hoạch diễn tập, phối hợp với

các đơn vị liên quan tổ chức triển khai thực hiện.

- Chương trình diễn tập được mô phỏng các tấn công trên thực tế vào hệ quản trị nội dung gồm các pha khai thác lỗ hổng, thực hiện chiếm quyền máy chủ, tải mã độc lên hệ thống và thực hiện các hành vi độc hại. Các đơn vị tham gia phải thực hiện các yêu cầu phát hiện sự cố, phân tích, khắc phục và đưa ra các biện pháp phòng ngừa kịp thời.

- Kết thúc diễn tập thực hiện tài liệu hóa các trường hợp tấn công và biện pháp phòng chống ngăn chặn, ứng cứu tạm thời hoặc triệt để tránh bị khai thác sâu lây lan vào các hệ thống bên trong. Rút kinh nghiệm và nhìn ra điểm yếu ATTT còn tồn tại trong hệ thống.

Điều 21. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro

Các mức độ rủi ro ATTT được xác định trong bảng sau:

Mức ảnh hưởng	Tính bảo mật (C)	Tính toàn vẹn (I)	Tính sẵn sàng (A)
Đặc biệt nghiêm trọng (5)	Việc bị lộ thông tin trái phép làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh	Việc sửa đổi hoặc phá hủy trái phép thông tin làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh	Việc gián đoạn truy cập hoặc sử dụng thông tin/HTTT làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh
Nghiêm trọng (4)	Việc bị lộ thông tin trái phép làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/HTTT làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia
Vừa phải (3)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/HTTT làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia
Nhỏ (2)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới quyền và lợi ích hợp	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới	Việc gián đoạn truy cập hoặc sử dụng thông tin/HTTT làm tổn hại nghiêm trọng tới quyền

Mức ảnh hưởng	Tính bảo mật (C)	Tính toàn vẹn (I)	Tính sẵn sàng (A)
	pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng
Không đáng kể (1)	Việc bị lộ thông tin trái phép làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân	Việc gián đoạn truy cập hoặc sử dụng thông tin/HTTT làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân

2. Quy trình đánh giá và quản lý rủi ro

a) Bước thiết lập bối cảnh, cơ quan, tổ chức cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ.

Bước này, cơ quan, tổ chức cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ, bao gồm nhưng không giới hạn các thông tin sau:

(1) Thông tin Chủ quản HTTT;

(2) Thông tin Đơn vị vận hành;

(3) Chức năng, nhiệm vụ, cơ cấu tổ chức của đơn vị vận hành;

(4) Các cơ quan, tổ chức liên quan;

(5) Phạm vi, quy mô của hệ thống.

b) Bước đánh giá rủi ro, cơ quan, tổ chức cần thực hiện nhận biết rủi ro, phân tích rủi ro và ước lượng rủi ro. Kết quả của việc thực hiện nội dung này là cần xác định tài sản, điểm yếu, mối đe dọa, hậu quả và mức ảnh hưởng đối với cơ quan, tổ chức khi rủi ro xảy ra đối với tài sản.

- Tiêu chí chấp nhận rủi ro: Việc xử lý toàn bộ rủi ro được xác định là khó khả thi với bất kỳ cơ quan, tổ chức nào. Do đó, các rủi ro có thể xem xét giảm thiểu đến mức chấp nhận được; tiêu chí chấp nhận rủi ro phụ thuộc vào các định hướng, mục đích, mục tiêu bảo đảm ATTT của cơ quan, tổ chức và các lợi ích của các bên liên quan; mỗi tổ chức cần phải xác định mức chấp nhận rủi ro của riêng tổ chức mình. Việc xác định các tiêu chí chấp nhận rủi ro cần xem xét đến các yếu tố như: Nguồn lực để xử lý rủi ro so với hiệu quả mang lại sau khi rủi ro được xử lý, khả năng xử lý rủi ro theo điều kiện thực tế của cơ quan, tổ chức của mình.

- Tiêu chí chấp nhận rủi ro có thể bao gồm nhiều ngưỡng với các tiêu chí tương ứng, căn cứ theo mục tiêu bảo đảm ATTT mà tổ chức đưa ra, như sau:

+ HTTT cấp độ 5, có xử lý thông tin bí mật nhà nước, không chấp nhận tổn

tại rủi ro. Chỉ chấp nhận tồn tại các rủi ro ở mức thấp đối với HTTT cấp độ 5 không xử lý thông tin bí mật nhà nước. Đối với HTTT cấp độ 5, để bảo đảm tính khả thi trong việc xử lý hết các rủi ro của hệ thống, cơ quan, tổ chức cần làm rõ phạm vi của hệ thống để có biện pháp xử lý phù hợp;

+ HTTT cấp độ 3 hoặc cấp độ 4, có xử lý thông tin bí mật nhà nước, chỉ chấp nhận tồn tại các rủi ro ở mức thấp. Chỉ chấp nhận tồn tại các rủi ro mức trung bình đối với HTTT cấp độ 3 hoặc cấp độ 4, không xử lý thông tin bí mật nhà nước;

+ HTTT cấp độ 1 hoặc cấp độ 2, chỉ chấp nhận tồn tại các rủi ro mức trung bình.

- Cơ quan, tổ chức cần xác định rõ phạm vi thực hiện đánh giá và quản lý rủi ro để bảo toàn tài sản được bảo vệ trong quy trình thực hiện. Để xác định phạm vi, giới hạn, cơ quan, tổ chức cần xác định rõ thông tin liên quan sau:

+ Phạm vi quản lý ATTT: Các mục tiêu bảo đảm ATTT của cơ quan, tổ chức; các quy định pháp lý phải tuân thủ; quy chế, quy tắc bảo đảm ATTT của tổ chức;

+ Phạm vi kỹ thuật: Sơ đồ tổng thể (vật lý, logic) và các thành phần trong hệ thống (thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối…); xác định các HTTT khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của HTTT được đề xuất; trong đó, xác định rõ mức độ ảnh hưởng đến HTTT đang được đề xuất cấp độ khi các hệ thống này bị mất ATTT; danh mục các nguy cơ tấn công mạng, mất ATTT đối với hệ thống và các ảnh hưởng.

- Cơ quan, tổ chức cần xây dựng phương án, kế hoạch thực hiện quản lý rủi ro ATTT. Nội dung phương án, kế hoạch, trách nhiệm của các đơn vị, bộ phận liên quan cần đưa vào quy chế bảo đảm ATTT của cơ quan, tổ chức để thực hiện. Dưới đây là một số nội dung cơ bản cần thực hiện để tổ chức thực hiện quản lý rủi ro ATTT:

+ Phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro;

+ Quy trình tổ chức thực hiện đánh giá và quản lý rủi ro;

+ Cơ chế phối hợp với các bên liên quan trong quá trình thực hiện;

+ Phương án, kế hoạch giám sát quy trình đánh giá và quản lý rủi ro.

- Nhận biết rủi ro là các bước để xác định ra các rủi ro, hậu quả và mức thiệt hại tương ứng. Để xác định được rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

+ Nhận biết về tài sản để xác định danh mục các tài sản của cơ quan, tổ chức cần bảo vệ bao gồm thông tin, HTTT;

+ Nhận biết về mối đe dọa để xác định các mối đe dọa đối với mỗi tài sản;

+ Nhận biết về điểm yếu để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản;

+ Kết quả của bước nhận biết rủi ro là danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định.

- Phân tích rủi ro để xác định ra các mức ảnh hưởng, các hậu quả đối với cơ quan, tổ chức trên cơ sở thực hiện bước nhận biết rủi ro ở trên. Để phân tích rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

+ Đánh giá các hậu quả để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối đe doạ;

+ Đánh giá khả năng xảy ra đối với từng loại sự cố;

+ Kết quả của bước phân tích rủi ro là xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý.

- Ước lượng rủi ro để xác định ra các rủi ro và mức rủi ro tương ứng mà cơ quan, tổ chức phải xử lý. Mức rủi ro được xác định dựa vào 03 tham số được xác định ở bước trên.

c) Bước xử lý rủi ro, cơ quan, tổ chức cần xác định các phương án xử lý rủi ro, bao gồm các biện pháp quản lý và kỹ thuật để có thể xử lý, giảm thiểu các mối đe dọa có thể xảy ra đối với tài sản, dẫn tới hậu quả cho cơ quan, tổ chức.

Cơ quan, tổ chức có thể lựa chọn các phương án xử lý rủi ro khác nhau để bảo đảm đạt được các mục tiêu bảo đảm ATTT của đơn vị mình. Xử lý rủi ro có thể được thực hiện bởi một hoặc kết hợp nhiều phương án sau: thay đổi rủi ro, duy trì rủi ro, tránh rủi ro và chia sẻ rủi ro, cụ thể như dưới đây:

- Thay đổi rủi ro:

+ Thay đổi rủi ro là phương án thực hiện các biện pháp xử lý, khắc phục nhằm giảm mức rủi ro đã được xác định sao cho các rủi ro tồn đọng được đánh giá lại ở mức chấp nhận được;

+ Để thực hiện phương án này, cơ quan, tổ chức cần xây dựng một hệ thống các biện pháp kiểm soát phù hợp. Các biện pháp được lựa chọn căn cứ vào các tiêu chí liên quan đến chi phí, đầu tư và thời gian triển khai, trên cơ sở cân đối giữa nguồn lực bỏ ra và lợi ích đem lại đối với tổ chức khi thực hiện xử lý rủi ro đó.

- Duy trì rủi ro: Duy trì rủi ro là phương án chấp nhận rủi ro đã xác định mà không đưa ra các phương án xử lý để giảm thiểu rủi ro. Việc xác định rủi ro nào có thể được chấp nhận dựa vào mức rủi ro và tiêu chí chấp nhận rủi ro;

- Tránh rủi ro: Tránh rủi ro là phương án xử lý khi cơ quan, tổ chức phải đối mặt với mức rủi ro quá cao bằng cách làm thay đổi, loại bỏ hoặc dừng hoạt động của hệ thống, quy trình nghiệp vụ hoặc hoạt động của cơ quan, tổ chức để không phải đối mặt với rủi ro đã xác định. Tránh rủi ro là phương án thích hợp

khi rủi ro được xác định vượt quá khả năng chấp nhận rủi ro của tổ chức;

- Chia sẻ rủi ro: Chia sẻ rủi ro là phương án chuyển rủi ro, một phần rủi ro phải đối mặt cho cơ quan, tổ chức khác. Phương án chia sẻ rủi ro thường được thực hiện khi cơ quan, tổ chức xác định rằng việc giải quyết rủi ro yêu cầu chuyên môn hoặc nguồn lực được cung cấp tốt hơn bởi các tổ chức khác;

- Chấp nhận rủi ro: Chấp nhận rủi ro là việc xem xét, đánh giá các rủi ro tồn đọng, chưa được xử lý hoàn toàn để đánh giá lại mức rủi ro sau xử lý có thể được chấp nhận hay không. Bởi vì có thể hệ thống tồn tại những rủi ro không có phương án xử lý triệt để mà chỉ có thể giảm thiểu.

d) Quá trình truyền thông và tư vấn rủi ro là quá trình cơ quan, tổ chức cần trao đổi, tham vấn ý kiến của các bên liên quan để có thông tin đầu vào khi thực hiện các bước ở trên; thực hiện tuyên truyền, phổ biến các nguy cơ, rủi ro có thể xảy ra.

- Truyền thông và tư vấn rủi ro ATTT là hoạt động nhằm đào tạo, tuyên truyền nâng cao nhận thức cho các bên liên quan đến hoạt động đánh giá và quản lý rủi ro. Bên cạnh đó, việc này cũng nhằm đạt được sự thống nhất giữa các bên liên quan. Ví dụ trong trường hợp lựa chọn phương án chia sẻ rủi ro.

- Cơ quan, tổ chức cần xây dựng kế hoạch truyền thông rủi ro định kỳ hoặc đột xuất. Hoạt động truyền thông rủi ro phải được thực hiện liên tục và thường xuyên.

đ) Quá trình giám sát và soát xét rủi ro, cơ quan, tổ chức giám sát và đánh giá tuân thủ, tính hiệu quả của việc thực hiện việc quản lý rủi ro.

- Giám sát và soát xét rủi ro ATTT nhằm bảo đảm hoạt động đánh giá và quản lý rủi ro ATTT được thực hiện thường xuyên liên tục theo quy chế, quy tắc bảo đảm ATTT của cơ quan, tổ chức và được cấp có thẩm quyền phê duyệt.

- Giám sát và soát xét các yếu tố rủi ro, việc giám sát và soát xét các yếu tố rủi ro cần bảo đảm các yếu tố sau:

+ Quản lý được các tài sản mới, sự thay đổi của tài sản, giá trị của tài sản;

+ Sự thay đổi, xuất hiện mới các mối đe dọa;

+ Sự thay đổi, xuất hiện mới các điểm yếu;

+ Sự thay đổi, xuất hiện mới các rủi ro;

+ Kết quả của việc giám sát và soát xét các yếu tố rủi ro là việc cập nhật thường xuyên, liên tục sự thay đổi đối với các yếu tố rủi ro được đề cập ở trên.

- Giám sát soát xét và cải tiến quản lý rủi ro:

+ Để bảo đảm hoạt động quản lý rủi ro ATTT được mang lại hiệu quả, việc

giám sát, soát xét và cải tiến quy trình quản lý rủi ro ATTT cần được thực hiện thường xuyên, liên tục;

+ Các tiêu chí được sử dụng để giám sát soát xét và cải tiến quản lý rủi ro có thể bao gồm, nhưng không giới hạn các yếu tố sau: Các yếu tố liên quan đến quy định pháp lý; phương pháp tiếp cận đánh giá rủi ro; các loại tài sản và giá trị tài sản; tiêu chí tác động; tiêu chí ước lượng rủi ro; tiêu chí chấp nhận rủi ro; các nguồn lực cần thiết.

Điều 22. Quản lý an toàn người sử dụng đầu cuối

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

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT.

c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

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

a) Người sử dụng khi truy cập, sử dụng Internet phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của quản trị viên hệ thống.

c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

3. Cài đặt và sử dụng máy tính an toàn

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất ATTT mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách CNTT của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được cơ quan chức năng, đơn vị chuyên môn tổ chức.

4. Quy trình quản lý an toàn người sử dụng đầu cuối theo Phụ lục XI.

Điều 23. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản HTTT khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ HTTT. Trong trường hợp thông tin, dữ liệu của HTTT lưu trữ trên tài sản vật lý, đơn vị chủ quản HTTT thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

2. Đối với các HTTT có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

3. Quy trình kết thúc vận hành, khai thác, thanh lý, hủy bỏ theo Phụ lục XII.

Chương V
KIỂM TRA, ĐÁNH GIÁ

Điều 24. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ quy định của pháp luật và theo quy chế của Bộ Nội vụ về bảo đảm an toàn HTTT theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn HTTT.

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

d) Kiểm tra, đánh giá khác do chủ quản HTTT quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản HTTT.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Trung tâm Công nghệ thông tin, Bộ Nội vụ.

b) Bộ Công an; Bộ Quốc phòng.

4. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

5. Đối tượng kiểm tra, đánh giá là các đơn vị có HTTT hoặc đơn vị vận hành HTTT và các HTTT có liên quan.

Điều 25. Kiểm tra việc tuân thủ quy định về ATTT và hiệu quả của biện pháp bảo đảm ATTT

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn HTTT và triển khai phương án bảo đảm ATTT; kiểm tra hiệu quả của các biện pháp bảo đảm ATTT.

b) Kiểm tra công tác giám sát ATTT; ứng cứu sự cố ATTT.

c) Kiểm tra các nội dung khác tại quy chế này.

2. Thẩm quyền kiểm tra

Trung tâm Công nghệ thông tin, Bộ Nội vụ chịu trách nhiệm kiểm tra các đơn vị thuộc, trực thuộc Bộ Nội vụ.

Chương VI
CHẾ ĐỘ BÁO CÁO

Điều 26. Quy định về chế độ báo cáo

1. Phương thức gửi, nhận báo cáo:

a) Gửi qua hệ thống quản lý văn bản và điều hành.

b) Gửi qua hệ thống thư điện tử.

c) Các phương thức khác theo quy định của pháp luật (gửi trực tiếp, gửi qua bưu chính, gửi qua Fax, ...).

2. Thực hiện báo cáo:

Thực hiện báo cáo theo đề nghị của cơ quan có thẩm quyền (Bộ Công an; Bộ Quốc phòng; Trung tâm Công nghệ thông tin, Bộ Nội vụ).

Điều 27. Nội dung báo cáo

1. Thông tin chung về chủ quản HTTT; đơn vị chuyên trách về CNTT; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử).

2. Danh sách các HTTT thuộc phạm vi quản lý, gồm: Tên hệ thống, đơn vị vận hành, cấp độ đề xuất.

3. Danh sách HTTT được phê duyệt Hồ sơ đề xuất cấp độ theo quy định.

4. Danh sách HTTT đã triển khai đầy đủ, mới triển khai một phần hoặc chưa triển khai các biện pháp bảo vệ đáp ứng các yêu cầu an toàn theo phương án bảo đảm ATTT theo cấp độ đã được phê duyệt.

5. Danh sách HTTT có phương án bảo đảm ATTT theo quy định.

6. Danh sách HTTT tuân thủ các quy định, quy trình trong Quy chế bảo

đảm ATTT trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ HTTT.

7. Danh sách HTTT được kiểm tra, đánh giá theo quy định.

8. Đánh giá về việc triển khai các biện pháp bảo đảm ATTT theo phương án bảo đảm ATTT được phê duyệt trong Hồ sơ đề xuất cấp độ theo từng tiêu chí, yêu cầu.

9. Thông tin Quyết định phê duyệt Hồ sơ đề xuất cấp độ, phương án bảo đảm ATTT được phê duyệt trong Hồ sơ đề xuất cấp độ theo từng tiêu chí, yêu cầu (đã đáp ứng đầy đủ hoặc chưa đáp ứng đầy đủ; kế hoạch hoặc lộ trình hoàn thiện tiêu chí, yêu cầu chưa đáp ứng,…).

10. Báo cáo số lượng sự cố về ATTT, các thông tin khác theo yêu cầu của cơ quan có thẩm quyền (Bộ Công an; Bộ Quốc phòng; Trung tâm Công nghệ thông tin, Bộ Nội vụ).

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 28. Trách nhiệm của Trung tâm Công nghệ thông tin, Bộ Nội vụ

1. Chủ trì, làm đầu mối hướng dẫn, theo dõi, giám sát, đôn đốc việc triển khai, tổ chức thực hiện Quy chế này.

2. Tiếp nhận và đưa ra các cảnh báo về an toàn, an ninh thông tin, áp dụng các biện pháp để khắc phục và hạn chế tối đa thiệt hại do sự cố mất an toàn, an ninh thông tin trong mạng Bộ Nội vụ.

3. Nhắc nhở, tạm dừng cung cấp các dịch vụ trong mạng Bộ Nội vụ đối với đơn vị, người sử dụng có liên quan để kiểm tra, khắc phục sự cố. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục phải báo cáo Lãnh đạo Bộ và thông báo cho các tổ chức hỗ trợ xử lý sự cố mất ATTT để cùng phối hợp giải quyết.

4. Hàng năm, phối hợp với các đơn vị liên quan kiểm tra về công tác bảo đảm an toàn, an ninh thông tin mạng đối với các đơn vị thuộc, trực thuộc Bộ Nội vụ.

5. Thực hiện việc cấp mới, chỉnh sửa, thu hồi tài khoản, mật khẩu, quyền truy cập và quyền khai thác tài nguyên mạng của Bộ Nội vụ cho người sử dụng khi có yêu cầu bằng văn bản.

6. Định kỳ hằng năm tiến hành rà soát Quy chế bảo đảm ATTT, an ninh mạng của Bộ Nội vụ nhằm kiểm tra tính phù hợp, đồng thời cập nhật, chỉnh sửa và bổ sung khi cần thiết.

Điều 29. Trách nhiệm của các đơn vị thuộc và trực thuộc Bộ Nội vụ

1. Thủ trưởng các đơn vị thuộc, trực thuộc Bộ có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức, người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. Thủ trưởng các cơ quan, tổ chức, đơn vị có trách nhiệm tổ chức triển khai, chỉ đạo, kiểm tra và giám sát việc thực hiện các quy định về bảo đảm ATTT

tại cơ quan, đơn vị thuộc phạm vi phụ trách; chịu trách nhiệm trước pháp luật và trước cấp có thẩm quyền nếu để xảy ra vi phạm trong lĩnh vực ATTT thuộc phạm vi quản lý.

3. Cung cấp thông tin người sử dụng của đơn vị khi có sự thay đổi để Trung tâm Công nghệ thông tin, Bộ Nội vụ thực hiện cấp mới, sửa đổi, thu hồi thiết bị, tài khoản, mật khẩu truy cập và quyền khai thác tài nguyên mạng Bộ Nội vụ.

4. Bảo vệ, quản lý các trang thiết bị và tài nguyên mạng Bộ Nội vụ được lắp đặt tại đơn vị.

5. Chịu trách nhiệm về nội dung, thông tin truyền tải trong mạng Bộ Nội vụ theo quy định của pháp luật, Bộ Nội vụ.

6. Trường hợp phát hiện sự cố mất an toàn, an ninh thông tin phải thông báo kịp thời tới Trung tâm Công nghệ thông tin, Bộ Nội vụ bằng văn bản và các hình thức liên lạc khác để phối hợp giải quyết.

7. Tạo điều kiện thuận lợi cho Trung tâm Công nghệ thông tin, Bộ Nội vụ và các đơn vị liên quan triển khai công tác kiểm tra, khắc phục sự cố khi xảy ra tình trạng mất an toàn, an ninh thông tin trong mạng Bộ Nội vụ.

8. Phối hợp với Trung tâm Công nghệ thông tin, Bộ Nội vụ thẩm định về mặt kỹ thuật và công nghệ đối với các dự án, kế hoạch ứng dụng CNTT do đơn vị chủ trì.

9. Các đơn vị có HTTT có trách nhiệm đảm bảo ATTT mạng đối với HTTT của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố ATTT mạng đối với các HTTT do đơn vị mình quản lý.

Điều 30. Kinh phí thực hiện

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

Điều 31. Khen thưởng, kỷ luật

1. Việc thực hiện đúng Quy chế này là một trong những tiêu chí bắt buộc để đánh giá kết quả công tác hằng năm của cá nhân và đơn vị, đồng thời là căn cứ xem xét thi đua, khen thưởng và xét tặng các danh hiệu đối với tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật.

Điều 32. Sửa đổi, bổ sung Quy chế

Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh bằng văn bản về Trung tâm Công nghệ thông tin, Bộ Nội vụ để tổng hợp, báo cáo Lãnh đạo Bộ xem xét điều chỉnh, bổ sung Quy chế cho phù hợp./.

Phụ lục I
Quy trình chấm dứt hoặc thay đổi công việc
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Quy trình chấm dứt hoặc thay đổi công việc, cụ thể như sau:

Bước 1: Công chức, viên chức, người lao động nghỉ việc bàn giao lại công việc, tài khoản truy cập HTTT, tài sản CNTT của cơ quan, đơn vị.

Bước 2: Quản trị viên hệ thống tiến hành quy trình thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động nghỉ việc:

a) Thu hồi tài khoản truy cập, các trang thiết bị máy móc, phần cứng và các tài sản khác thuộc sở hữu của đơn vị quản lý.

b) Vô hiệu hóa các thông tin của công chức, viên chức, người lao động thôi việc được lưu trên các phương tiện lưu trữ, phần mềm.

c) Vô hiệu hóa tất cả các quyền ra vào trung tâm dữ liệu của công chức, viên chức, người lao động thôi việc tại các trụ sở làm việc của đơn vị quản lý.

d) Vô hiệu hóa tất cả các quyền truy cập của công chức, viên chức, người lao động thôi việc vào tài nguyên, hệ thống phần mềm của đơn vị quản lý.

đ) Kiểm tra lại các quyền ra vào, truy cập tài nguyên, quản trị hệ thống đã cấp cho công chức, viên chức, người lao động nghỉ việc để đảm bảo đã hoàn toàn được gỡ bỏ khỏi hệ thống.

Phụ lục II
Quy trình thử nghiệm và nghiệm thu hệ thống
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

I. QUY TRÌNH THỬ NGHIỆM HỆ THỐNG

1. Nội dung thực hiện

Trách nhiệm	Trình tự thực hiện	Mô tả
Đơn vị chuyên môn	Xác định nhu cầu	Đơn vị chuyên môn xác định nhu cầu kiểm thử theo Dự án
Đơn vị chuyên môn	Lập kế hoạch kiểm thử	Lập kế hoạch kiểm thử theo Dự án
Trưởng dự án	Thông qua	Xem xét kế hoạch kiểm thử
Đơn vị chuyên môn	Thiết kế kịch bản cho quy trình kiểm thử	
Trưởng dự án	Thông qua	Xem xét thiết kế kịch bản cho quy trình kiểm thử
Đơn vị chuyên môn	Thiết lập môi trường kiểm thử	
Đơn vị chuyên môn	Thực hiện kiểm thử	
Đơn vị chuyên môn	Báo cáo kiểm thử	
Trưởng dự án	Thông qua	
	Kết thúc kiểm thử	

2. Diễn giải

Bước 1: Đơn vị chuyên môn sẽ xác định các yêu cầu kiểm thử. Dựa trên việc phân tích các tài liệu đặc tả, thiết kế chi tiết của Dự án

Bước 2: Đơn vị chuyên môn sẽ xây dựng kế hoạch kiểm thử:

Nội dung thực hiện: Lập kế hoạch kiểm thử, xác định yêu cầu, phạm vi, chiến lược, các mốc thời gian quan trọng và lịch trình thực hiện các bước từ đầu đến khi kết thúc kiểm thử.

Bước 3: Trưởng dự án sẽ xem xét kế hoạch kiểm thử, sau khi kế hoạch kiểm thử được chấp thuận, chuyển sang bước 4

Bước 4: Đơn vị chuyên môn thiết kế kịch bản kiểm thử:

Nội dung thực hiện:

- Xác định phạm vi kiểm thử của hệ thống bao gồm các chức năng của phần cứng, phần mềm, nghiệp vụ phần mềm,…

- Phân tích các tài liệu đầu vào để nắm vững yêu cầu, phạm vi kiểm thử, xác định các tính năng cần kiểm thử và các kỹ thuật kiểm thử;

- Xây dựng các tình huống kiểm thử: số ký hiệu của tình huống, đặt tên tình huống và xác định điều kiện, dữ liệu đầu vào, các bước thực hiện, kết quả mong đợi, kết quả thực tế dựa vào yêu cầu đầu vào;

- Xây dựng các kịch bản kiểm thử tương ứng với các tình huống kiểm thử bảo đảm đáp ứng được việc đánh giá đầy đủ các yêu cầu chức năng và phi chức năng.

Bước 5: Trưởng dự án xem xét kịch bản kiểm thử, sau khi kịch bản kiểm thử được chấp thuận chuyển sang bước 6.

Bước 6: Đơn vị chuyên môn thiết lập môi trường kiểm thử tương đương với môi trường vận hành, khai thác thực tế, bao gồm các công cụ hỗ trợ kiểm thử (nếu có) để thực hiện kiểm thử và thông báo trạng thái sẵn sàng môi trường kiểm thử cho các bên liên quan.

Bước 7: Đơn vị chuyên môn thực hiện kiểm thử, khi tìm kiếm được lỗi, sẽ lập báo cáo về kết quả công việc thực hiện được, số lỗi đã tìm được. Khi các lỗi được sửa chữa bởi bên phát triển hoàn thành, đơn vị chuyên môn sẽ vào kiểm tra lại một lần nữa để đảm bảo các chức năng được sửa chữa chính xác.

- Nội dung thực hiện: Thực hiện kiểm thử theo kịch bản kiểm thử.

- Các hoạt động chính:

+ Thực thi toàn bộ các kịch bản kiểm thử.

+ Quan sát, ghi nhận kết quả thực tế, ghi nhận các sự cố, lỗi phần cứng, phần mềm xảy ra trong quá trình kiểm thử.

+ So sánh kết quả thực tế và kết quả mong đợi.

Bước 8: Trưởng dự án kiểm tra kết quả kiểm thử thông qua báo cáo kiểm thử và kiểm thử thực tế, nếu đạt yêu cầu thì chuyển bước tiếp theo, nếu chưa đơn

vị chuyên môn tiến hành kiểm thử lại.

Bước 9: Khi các lỗi đã được ghi nhận, đơn vị chuyên môn sẽ báo cáo kết quả kiểm thử đến Trưởng dự án và các đơn vị liên quan

Nội dung thực hiện: Lập báo cáo kết quả kiểm thử.

Các hoạt động chính:

- Đơn vị thực hiện kiểm thử lập báo cáo kết quả kiểm thử.

- Công bố kết quả kiểm thử và tuyên bố kết thúc kiểm thử. Trưởng dự án xem xét quyết định:

+ Yêu cầu nhà thầu triển khai tiếp nhận kết quả, chỉnh sửa, bổ sung và hoàn thiện hệ thống phần mềm trong trường hợp phần cứng, phần mềm có lỗi.

+ Thống nhất kế hoạch tổ chức nghiệm thu với các bên liên quan.

+ Tuyên bố kết thúc kiểm thử.

- Nhà thầu triển khai và các bên liên quan có trách nhiệm tiếp nhận và triển khai các công việc theo kết quả kiểm thử được công bố.

II. QUY TRÌNH NGHIỆM THU HỆ THỐNG

Quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng CNTT; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ CNTT theo yêu cầu riêng (Thông tư 16/2024/TT-BTTTT), cụ thể như sau:

Bước 1: Sản phẩm hoặc hạng mục công việc của dự án phải được kiểm thử hoặc vận hành thử tại ít nhất một đơn vị thụ hưởng trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng.

1. Đối với hệ thống hạ tầng kỹ thuật, thiết bị, phần mềm thương mại, nhà thầu triển khai chủ trì, phối hợp với chủ đầu tư tổ chức vận hành thử.

a) Nội dung và trình tự các bước vận hành thử theo mục I của Phụ lục III.

b) Kết quả vận hành thử được nhà thầu triển khai lập thành báo cáo.

2. Đối với phần mềm nội bộ, tùy theo mức độ yêu cầu chất lượng và các điều kiện thực tế, chủ đầu tư xem xét, quyết định áp dụng hình thức kiểm thử hoặc vận hành thử và chịu trách nhiệm với quyết định của mình.

a) Nội dung và trình tự các bước vận hành thử theo hướng dẫn tại Phụ lục số 2 của Phụ lục II ban hành kèm theo Thông tư 16/2024/TT-BTTTT. Quá trình vận hành thử phần mềm nội bộ, chủ đầu tư cần kiểm soát chất lượng phần mềm đối với

các yêu cầu phi chức năng trên cơ sở báo cáo kết quả kiểm thử do nhà thầu triển khai. Kết quả vận hành thử phần mềm nội bộ do chủ đầu tư lập thành báo cáo;

b) Nội dung, kết quả kiểm thử theo hướng dẫn tại Phụ lục số 3 của Phụ lục II ban hành kèm theo Thông tư 16/2024/TT-BTTTT. Kết quả kiểm thử do chủ đầu tư lập (nếu tự thực hiện) hoặc đơn vị kiểm thử độc lập (nếu thuê) lập thành báo cáo.

Bước 2: Nghiệm thu, bàn giao sản phẩm, hạng mục công việc hoàn thành của dự án

1. Yêu cầu sản phẩm, hạng mục công việc nghiệm thu

a) Sản phẩm hoặc hạng mục công việc được hoàn thành đầy đủ về khối lượng, chất lượng, tiến độ, các yêu cầu theo hợp đồng và thiết kế chi tiết được phê duyệt;

b) Sản phẩm hoặc hạng mục công việc được kiểm thử hoặc vận hành thử đáp ứng yêu cầu chất lượng theo quy định tại Điều 34 Nghị định số 73/2019/NĐ-CP và Điều 9 Thông tư 16/2024/TT-BTTTT.

2. Chủ đầu tư và các đơn vị có liên quan thỏa thuận về nội dung nghiệm thu, thời điểm, địa điểm nghiệm thu. Kết quả nghiệm thu được lập thành biên bản theo Mẫu số 6 của Phụ lục I ban hành kèm theo Thông tư 16/2024/TT-BTTTT.

Trên cơ sở các hồ sơ, tài liệu sau khi nghiệm thu, chủ đầu tư có trách nhiệm lập danh mục hồ sơ hoàn thành phục vụ lưu trữ và bảo quản hồ sơ, tài liệu của dự án theo quy định của pháp luật lưu trữ. Danh mục hồ sơ hoàn thành phục vụ lưu trữ theo Phụ lục III ban hành kèm theo Thông tư 16/2024/TT-BTTTT.

Phụ lục III
Quy trình quản lý an toàn mạng
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Quy trình quản lý an toàn mạng của HTTT được thực hiện thông qua các quy trình sau:

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

Bước 1: Kiểm tra, đánh giá thiết bị mạng, hệ điều hành, phần mềm cài đặt trên các máy chủ hoạt động liên tục, ổn định và an toàn:

- Kiểm tra nhật ký hoạt động (log) của thiết bị mạng, hệ điều hành, phần mềm nhằm phát hiện ra các hành vi mất an toàn, an ninh thông tin (kiểm tra, phát hiện, loại bỏ các tài khoản người dùng lạ trên thiết bị mạng, máy chủ, phần mềm; kiểm tra hành vi của các tài khoản đăng nhập vào thiết bị mạng, máy chủ, phần mềm).

- Kiểm tra tình trạng hoạt động của CPU, RAM, Ổ cứng của máy chủ. Nếu

- Kiểm tra lưu lượng truy cập mạng của máy chủ, phần mềm

Bước 2: Kiểm tra, cập nhật các bản và lỗi của thiết bị phần cứng, hệ điều hành, phần mềm, từ nhà cung cấp.

Bước 3: Kiểm tra, loại bỏ các thành phần không cần thiết hoặc không sử dụng của hệ điều hành, phần mềm.

Bước 4: Kiểm tra đường truyền Internet: tốc độ mạng; lưu lượng mạng.

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

a. Cập nhật bản vá

Bước 1: Kiểm tra các bản cập nhật mới, các nhà phát triển thường phát hành các bản cập nhật mới cho phần mềm, ứng dụng hoặc hệ điều hành thông qua các kênh chính thức như trang web của nhà phát triển.

Bước 2: Sao lưu hệ thống trước khi cập nhật bản vá để tránh các trường hợp khi cài bản cập nhật mới sẽ xảy ra lỗi hệ thống, gây gián đoạn hệ thống. Trong trường hợp xảy ra lỗi sẽ khôi phục lại hệ thống lúc chưa cài bản cập nhật.

Bước 3: Tải xuống và cài đặt bản cập nhật: Sau khi đã xác định được các bản cập nhật cần thiết, tải xuống và cài đặt bản cập nhật.

Bước 4: Kiểm tra các bản cập nhật sau khi cài đặt: Sau khi cài đặt bản cập nhật, cần phải kiểm tra hệ thống hoạt động bình thường hay không.

b. Quy trình sao lưu dữ liệu

Bước 1: Xác định nguồn dữ liệu sao lưu (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 dữ liệu quan trọng khác)

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện xác định nguồn dữ liệu cần lưu trữ để tiến hành sao lưu định kỳ.

Bước 2: Chuẩn bị, kiểm tra (Mạng, phương tiện lưu trữ, phần mềm lưu trữ,…).

Việc chuẩn bị nhằm bảo đảm an toàn, hạn chế tối đa lỗi có thể xảy ra trong quá trình tiến hành sao lưu.

Bước 3: Tiến hành sao lưu dữ liệu

Sau khi đã thực hiện xác định nguồn dữ liệu sao lưu và chuẩn bị các phương tiện lưu trữ, phần mềm để phục vụ việc sao lưu, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn tiến hành sao lưu dữ liệu cần thiết vào phương tiện lưu trữ.

Bước 4: Kiểm tra kết quả sao lưu dữ liệu

Sau khi hoàn thành quá trình sao lưu, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện kiểm tra kết quả sao lưu. Trường hợp kết quả sao lưu không đạt yêu cầu thì quay lại Bước 2 để kiểm tra, tìm hướng khắc phục lỗi và báo cáo Lãnh đạo; Trường hợp việc sao lưu đạt yêu cầu thì chuyển phương tiện lưu trữ chứa dữ liệu sao lưu vào nơi bảo quản.

Bước 5: Bảo quản phương tiện lưu trữ

Bước 6: Ghi nhật ký, lập hồ sơ

c. Quy trình khôi phục hệ thống

Bước 1: Xác định sự cố tin học

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn xác định nguyên nhân xảy ra sự cố tin học do lỗi phần cứng hoặc lỗi phần mềm để tìm hướng khắc phục.

Bước 2: Thực hiện cách ly, xử lý hệ thống, các dịch vụ bảo đảm an toàn, an ninh trước khi thực hiện phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện cách ly máy chủ, dịch vụ hay cơ sở dữ liệu bằng cách sửa chữa, thay thế thiết bị, chặn tấn công xâm nhập mạng, tắt tiến trình phần mềm, rà quét bóc gỡ mã độc,… bảo đảm cho hệ thống được vận hành bình thường.

Bước 3: Xác định trường hợp cần phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn cần xác định trường hợp phục hồi là do sự cố hệ thống, phần cứng hay dữ liệu, phần mềm quản trị cơ sở dữ liệu, phần mềm ứng dụng để từ đó đưa ra cách phục hồi nhanh chóng, chính xác.

Bước 4: Xác định nguồn cơ sở dữ liệu tài liệu lưu trữ phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn xác định và lấy bản sao lưu dự phòng gần nhất trước thời điểm xảy ra sự cố để tiến hành phục hồi.

Bước 5: Tiến hành phục hồi

Người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện khôi phục lại phần mềm ứng dụng bằng cách sử dụng phần mềm ứng dụng đã được sao lưu gần nhất trước thời điểm xảy ra sự cố.

Bước 6: Kiểm tra kết quả phục hồi

Khi hệ thống hoạt động trở lại bình thường, người được giao quản lý hệ thống, cơ sở dữ liệu, mã nguồn thực hiện kiểm tra dữ liệu để bảo đảm dữ liệu sau khi phục hồi hoàn toàn đầy đủ, chính xác so với trước thời điểm xảy ra sự cố. Trường hợp dữ liệu không đạt yêu cầu thì quay lại Bước 4 để kiểm tra nguồn dữ liệu phục hồi; trường hợp đạt yêu cầu thì tiến hành chuyển sang bước tiếp theo.

Bước 7: Ghi biên bản, lập hồ sơ.

3. Truy cập và quản lý cấu hình hệ thống

Bước 1: Xác định cấu hình:

- Xác định tất cả các thành phần cấu tạo nên HTTT, bao gồm phần cứng, phần mềm, mạng và dữ liệu.

- Thu thập thông tin chi tiết về từng thành phần, chẳng hạn như tên, nhà cung cấp, phiên bản, v.v.

- Lưu trữ thông tin cấu hình trong một kho lưu trữ trung tâm.

Bước 2: Theo dõi cấu hình:

- Theo dõi các thay đổi đối với cấu hình hệ thống.

- Ghi lại lịch sử thay đổi, bao gồm ai đã thực hiện thay đổi, khi nào thay đổi được thực hiện và thay đổi gì đã được thực hiện.

- Lưu trữ lịch sử thay đổi trong kho lưu trữ trung tâm.

Bước 3: Kiểm soát cấu hình:

- Xác định các quy định và quy trình để quản lý thay đổi đối với cấu hình hệ thống.

- Yêu cầu phê duyệt cho các thay đổi cấu hình trước khi được thực hiện.

- Kiểm tra các thay đổi cấu hình để đảm bảo rằng chúng đáp ứng các yêu cầu kinh doanh và không gây ra sự cố.

Triển khai các thay đổi cấu hình một cách có kiểm soát.

Bước 4: Báo cáo cấu hình:

- Tạo các báo cáo về cấu hình hệ thống.

- Sử dụng các báo cáo này để theo dõi trạng thái của HTTT và xác định các nguy cơ tiềm ẩn.

- Sử dụng các báo cáo này để cải thiện hiệu suất của HTTT.

Phụ lục IV
Quy trình quản lý an toàn máy chủ
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Vị trí máy chủ an toàn

Đặt máy chủ ở vị trí an toàn, kiểm tra điều kiện lý tưởng cho máy chủ như: nhiệt độ; khoảng cách giữa các máy chủ và thiết bị; hệ thống lưu điện đảm bảo cho hệ thống hoạt động liên tục không bị gián đoạn. Vị trí đặt máy chủ phải có khoá và giới hạn người được phép vào ra.

Bước 2: Kiểm soát quyền truy cập

Các quyền truy cập ứng dụng, cấu hình, phần mềm trên máy chủ chỉ được cấp cho một người quản trị duy nhất. Hạn chế quyền truy cập vào máy chủ sẽ hạn chế khả năng máy chủ bị xâm nhập trái phép.

Bước 3: Thiếp lập tường lửa

Trên thiết bị tường lửa chỉ mở cổng cần thiết cho máy chủ hoạt động đúng chức năng.

Bước 4: Quản lý cấu hình máy chủ

Trên máy chủ chỉ nên cài đặt các chức năng cần thiết cho máy chủ, không cài đặt nhiều chức năng trên cùng một máy chủ (AD, FTP Server, Web Server, DNS Server, …). Các máy chủ nên thống nhất về cách đặt tên, mật khẩu, các máy chủ cùng vùng mạng nên có cùng một dải IP

Bước 5: Bảo mật tài khoản quản trị, người dùng

Mật khẩu tài khoản quản trị, người dùng phải bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt, độ dài của mật khẩu phải trên 8 ký tự, không đặt mật khẩu dễ đoán (các ký tự liên tiếp nhau:123456, abcde, trùng với tên tài khoản, trùng với ngày sinh nhật của quản trị viên,…). Đảm bảo rằng tài khoản và mật khẩu chỉ duy nhất một quản trị viên biết.

Bước 6: Cài đặt các bản vá lỗ hổng bảo mật

Để đảm bảo an toàn cho máy chủ quản trị viên phải thường xuyên cập nhật bản vá lỗ hổng bảo mật cho hệ điều hành, ứng dụng, phần mềm theo khuyến cáo của các nhà cung cấp.

Bước 7: Gỡ bỏ các phần mềm không cần thiết

Việc cài đặt các phần mềm không cần thiết trên máy chủ sẽ dẫn đến mất ATTT, tin tặc rất dễ lợi dụng các lỗ hổng bảo mật của các phần mềm để tấn công hệ thống mạng, nên chỉ cài đặt các phần mềm thực sự cần thiết trên máy chủ.

Bước 8: Sao lưu dự phòng dữ liệu, cấu hình máy chủ

Sao lưu dự phòng dữ liệu, cấu hình máy chủ để đảm bảo các thông tin quan trọng không bị mất và dễ dàng phục hồi lại khi có sự cố về ATTT xảy ra.

Bước 9: Giám sát liên tục

Thường xuyên, liên tục giám sát các hoạt động của máy chủ, nhằm mục đích phát hiện các hành vi bất thường trên máy chủ như: Tài khoản lạ đăng nhập vào máy chủ, lưu lượng truy cập vào ra Internet tăng đột biến,…

Phụ lục V
Quy trình quản lý an toàn ứng dụng
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Xác thực

- Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

- Lưu trữ có mã hoá thông tin xác thực hệ thống;

- Thiếp lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu: Yêu cầu thay đổi mật khẩu mặc định; thiếp lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; thiếp lập thời gian yêu cầu thay đổi mật khẩu; thiếp lập thời gian mật khẩu hợp lệ;

- Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;

- Mã hoá thông tin xác thực trước khi gửi qua môi trường mạng;

- Thiếp lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu quan trọng trong hệ thống.

Bước 2: Kiểm soát truy cập

- Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

- Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

- Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa;

- Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

- Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp.

Bước 3: Nhật ký hệ thống

- Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: Thông tin truy cập ứng dụng; thông tin đăng nhập khi quản trị ứng dụng; thông tin các lỗi phát sinh trong quá trình hoạt động; thông tin thay đổi cấu hình ứng dụng.

- Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

- Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng.

Bước 4: Bảo mật thông tin liên lạc

- Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;

- Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.

Bước 5: Chống chối bỏ

Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng.

Bước 6: An toàn ứng dụng và mã nguồn

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý;

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;

- Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

- Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng.

Phụ lục VI
Quy trình quản lý an toàn dữ liệu
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Phân loại dữ liệu

- Lựa chọn dữ liệu quan trọng để sao lưu;
- Các tệp tin cấu hình của các thiết bị phần cứng;
- Bản sao ổ đĩa các máy ảo;
- Code phần mềm, Trang/Cổng thông tin điện tử, cơ sở dữ liệu;
- Tệp văn bản, ảnh, video.

Bước 2: Mã hoá dữ liệu

Dữ liệu được sao lưu phải được mã hóa là việc chuyển đổi dữ liệu từ định dạng có thể đọc được sang định dạng được mã hóa. Dữ liệu được mã hóa chỉ có thể được đọc hoặc xử lý sau khi được giải mã. Phương pháp mã hoá được sử dụng là phương pháp mã hoá dữ liệu đối xứng AES

Bước 3: Phân loại, quản lý và sử dụng khoá bí mật và dữ liệu mã hoá

- Phân loại dữ liệu: Chọn dữ liệu quan trọng để mã hoá, sử dụng phương pháp mã hoá dữ liệu đối xứng AES
- Khoá dữ liệu được giao cho quản trị viên HTTT quản lý.

Bước 4: Cơ chế mã hoá và kiểm tra tính nguyên vẹn của dữ liệu

Sử dụng phương pháp mã hoá dữ liệu đối xứng AES. Trước khi sao lưu dữ liệu phải kiểm tra tính nguyên vẹn của dữ liệu bằng cách kiểm tra mã MD5 và SH1.

Bước 5: Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ

- Khi trao đổi dữ liệu qua môi trường mạng phải sử dụng mã hoá dữ liệu đối xứng AES.
- Khoá dữ liệu phải được lưu vào thiết bị không có kết nối mạng, trao đổi khoá dữ liệu qua bưu điện hoặc giao trực triếp.
- Phương tiện lưu trữ dữ liệu phải đảm bảo đủ các điều kiện ATTT.

Bước 6: Sao lưu dự phòng và khôi phục dữ liệu

- Sao lưu dữ liệu dự phòng phải thực hiện ít nhất 01 tháng 01 lần, thời gian lưu trữ tối thiểu là 06 tháng đối với dữ liệu cũ của Trang/ Cổng thông tin điện tử, cơ sở dữ liệu; đối với dữ liệu về văn bản điện tử, ảnh, video lưu vĩnh viễn, tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống. Thiết bị lưu trữ dự

phòng phải không có kết nối Internet.

- Việc lấy dữ liệu ra khỏi phương tiện lưu trữ phải đảm bảo tuân thủ đảm bảo an toàn, bảo mật thông tin dữ liệu.

Bước 7: Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ

Phụ lục VII
Quy trình quản lý an toàn thiết bị đầu cuối
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Phân loại các thiết bị đầu cuối

- Thiết bị di động;
- Máy chủ;
- Mạy trạm;
- Thiết bị mạng;
- Thiết bị lưu trữ.

Bước 2: Dán nhãn và đặt tên cho các thiết bị đầu cuối

- Thông tin về thiết bị đầu cuối (Tên, chủng loại, địa chỉ MAC, địa chỉ IP, ngày mua, thời hạn bảo hành).

- Tên máy trạm được đặt theo quy tắc (vi dụ: Văn Sỹ Hùng, Vụ Chính quyền địa phương, phòng 625 thì tên máy tính sẽ được đặt là HungVS_CQDP_625).

- Tên máy chủ được đặt theo dịch vụ được cung cấp bởi máy chủ. Ví dụ: máy chủ cung cấp dịch vụ DNS được đặt tên là ServerDNS.

Bước 3: Kiểm tra, đánh giá, xử lý điểm yếu ATTT các thiết bị đầu cuối trước khi đưa vào sử dụng

- Quản lý theo địa chỉ IP, địa chỉ MAC

- Các thiết bị đầu cuối phải được rà quét điểm yếu về ATTT trước khi đưa vào sử dụng.

- Các thiết bị di động kết nối mạng không dây được quản lý bằng thiết bị quản lý truy cập mạng không dây tập trung. Người dùng không tự ý lắp đặt các thiết bị phát mạng di động.

- Các máy chủ, máy trạm phải được cài đặt chương trình diệt virus và cập nhật các bản vá cho hệ điệu hành, ứng dụng, phần mềm, gỡ bỏ các phần mềm không cần thiết.

- Các thiết bị mạng phải được cấu hình tối ưu cho hệ thống, rà soát các tài khoản quản trị (thay đổi thông tin tài khoản quản trị mặc định, rà soát các tài khoản lạ trên thiết bị, theo dõi lưu lượng bất thường trên thiết bị, cập nhật các bản vá lỗi về ATTT,…).

- Các thiết bị lưu trữ (USB, ổ cứng di động, SAN, …) phải được rà soát về ATTT trước khi sử dụng.

Bước 4: Cấp tài khoản cho người sử dụng thiết bị đầu cuối

- Các tài khoản máy chủ, máy trạm, thiết bị mạng được cấp theo tên người sử dụng, phải đặt mật khẩu mạnh cho các tài khoản. Không cấp tài khoản quản trị máy tính cho người dùng.

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

Bước 5: Lưu nhật ký sử dụng (Log)

- Các thiết bị đầu cuối phải được lưu log tập trung ít nhất là 3 tháng.

- Khi xảy ra sự cố các hành vi xoá log, xoá dữ liệu, xoá hệ điều hành, khôi phục hệ thống về trạng thái ban đầu là hành vi cản trở điều tra sự cố ATTT.

Bước 6: Cài đặt, kết nối, gỡ bỏ thiết bị đầu cuối

- Khi cài đặt, kết nối, gỡ bỏ thiết bị đầu cuối phải được sự cho phép của người có thẩm quyền.

- Cài đặt, kết nối thực hiện theo từ Bước 1 đến Bước 5.

- Gỡ bỏ thiết bị đầu cuối ngắt thiết bị ra khỏi hệ thống, xoá hết dữ liệu có trên thiết bị, khôi phục thiết bị về trạng thái ban đầu. Đối với thiết bị mạng khi gỡ bỏ phải đảm bảo trạng thái hoạt động bình thường của hệ thống. Đối với thiết bị phải huỷ bỏ phải đảm bảo khi huỷ bỏ thiết bị không còn sử dụng được, không có khả năng khôi phục được dữ liệu.

Phụ lục VIII
Quy trình quản lý phòng chống phần mềm độc hại
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Cài đặt chương trình diệt virus bản quyền cho máy chủ, máy trạm, thiết bị di động.

Bước 2: Thiết lập cơ chế tự động cập nhật; tự động quét phần mềm độc hại khi sao chép, mở các tệp; tự động quét các thiết bị lưu trữ lưu động (ổ USB, ổ cứng di động,…); tự động quét phần mềm độc hại định kỳ 01 tuần một lần.

Bước 3: Định kỳ cập nhật bản vá các lỗ hổng bảo mật trên hệ điều hành, phần mềm, ứng dụng theo khuyến cáo của nhà phát hành.

Bước 4: Gỡ bỏ các phần mềm không cần thiết trên máy chủ, máy trạm, thiết bị di động.

Bước 5: Tất cả các máy tính phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp trên các thiết bị lưu trữ di động.

Bước 6: Cảnh báo người dùng thực hiện nghiêm các biện pháp ngăn chặn các phần mềm độc hại, tin tặc xâm nhập vào máy tính.

- Đặt mật khẩu đăng nhập cho máy chủ, máy trạm, thiết bị di động.

- Xoá bỏ các tài khoản không dùng, tài khoản lạ.

- Không truy cập vào trang thông tin điện tử không rõ nguồn gốc, không mở thư điện tử lạ.

- Phải dùng chương trình diệt virus quét ổ USB, ổ cứng di động trước khi sử dụng.

- Không tự ý cài đặt các phần mềm, ứng dụng không rõ nguồn gốc.

Bước 7: Trong trường hợp người dùng phát hiện dấu hiệu bất thường trên máy tính (máy chậm, cảnh bảo từ chương trình diệt virus, mất dữ liệu,….) phải báo ngay cho bộ phận chịu trách nhiệm về ATTT.

Bước 8: 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.

Phụ lục IX
Quy trình quản lý giám sát an toàn HTTT
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Tiếp nhận, phân tích, đánh giá cảnh báo

- Nhân sự trực giám sát ATTT tiếp nhận cảnh báo từ: hệ thống vận hành ATTT; thông báo thông tin về cảnh báo sự cố cho nhân sự quản trị hệ thống.

- Đơn vị phụ trách hệ thống giám sát ATTT: Thu thập bổ sung các sự kiện, thông tin liên quan đến cảnh báo; phân tích, đánh giá xác định hệ thống có bị tấn công hay không.

Trong trường hợp xác định hệ thống không bị tấn công, chuyển Bước 2, hệ thống bị tấn công, chuyển Bước 3.

Bước 2: Đóng cảnh bảo

Đối với cảnh báo được nhân sự trực giám sát phân tích đánh giá:

- Không có tấn công do liên quan tới nghiệp vụ quản trị, tác động của quản trị viên hệ thống được thông báo trước.

- Các hành vi được phép và không được phép của hệ thống giám sát bắt rộng hoặc chưa tối ưu dẫn tới cảnh báo sai.

Nhân sự trực giám sát thực hiện đóng cảnh báo với đầy đủ các thông tin đã xác minh. Hành động này để ghi nhận giúp đánh giá chất lượng của các các hành vi được phép và không được phép phát sinh cảnh báo, từ đó triển khai các hoạt động tối ưu các hành vi được phép và không được phép không đảm bảo chất lượng.

Bước 3: Xác định trường hợp cảnh báo ATTT mạng cần được xử lý

Chuẩn bị các trường hợp có thể xảy ra xác minh thêm thông tin về hành vi hoặc phản ứng ngăn chặn tấn công đang nhằm vào hệ thống nhưng chưa thành công hoặc các hành động khắc phục khi tấn công thành công.

Hệ thống có bị tấn công nhưng chưa thành công hoặc chưa xác định (cần xác minh thêm) chuyển Bước 4. Nếu hệ thống bị tấn công thành công, chuyển Bước 8.

Bước 4: Trên hệ thống giám sát tạo cảnh báo cho công chức, viên chức quản trị hệ thống

Bộ phận trực giám sát tạo cảnh báo mô tả rõ thông tin cho công chức, viên chức quản trị hệ thống cần thực hiện:

- Xác minh hành vi tác động vào hệ thống: Tuỳ theo thông tin cảnh báo, cần xác minh hành vi liên quan đến nghiệp vụ quản trị, khai thác hoặc tác động của công chức, viên chức quản trị hệ thống.

- Phản ứng tấn công: Căn cứ vào loại tấn công để đưa ra phương án ngăn chặn phù hợp, bao gồm các phương án:

+ Chặn IP đang thực hiện tấn công dò quét từ Internet;

+ Thiết lập luật chặn thư điện tử theo người gửi, tiêu đề,…

Bước 5: Xử lý cảnh báo

Công chức, viên chức quản trị hệ thống thực hiện xử lý cảnh báo trong phạm vi nghiệp vụ quản trị, vận hành theo yêu cầu của bộ phận trực giám sát được mô tả , hướng dẫn trong cảnh bảo.

Bước 6: Cập nhật kết quả xử lý và đóng cảnh báo

Công chức, viên chức quản trị hệ thống thực hiện xử lý cảnh báo theo nghiệp vụ quản trị và vận hành. Cập nhật chi tiết thông tin đã xác minh, xử lý vào cảnh báo. Đóng cản bảo xác nhận hoàn thành xử lý.

Bộ phận trực giám sát kiểm tra lại kế quả xử lý cảnh báo của công chức, viên chức quản trị hệ thống.

Trường hợp cảnh báo tấn công chưa được ngăn chặn triệt để, quay lại Bước 4. Nếu tấn công đã được ngăn chặn thành công, hoặc hành vi liên quan nghiệp vụ quản trị chuyển Bước 7.

Dựa vào kết quả xác minh nghiệp vụ của công chức, viên chức quản trị hệ thống, đánh giá có sự cố, chuyển Bước 8.

Bước 7: Đóng cảnh báo

Bộ phận trực giám sát thực hiện đóng cảnh bảo kết thúc quy trình xử lý cảnh báo.

Bước 8: Xác định mức độ sự cố

Mức độ nghiêm trọng của sự cố được quy định trong bảng dưới đây:

Phạm vi / **Mức độ**	**Toàn hệ thống**	**Nhiều hệ thống, dịch vụ hoặc toàn bộ hệ thống**	**Một hệ thống, dịch vụ**	**Người dùng cá nhân**
Gián đoạn dịch vụ/Lộ lọt thông tin	Nghiêm trọng	Nghiêm trọng	Cao	Trung bình
Ảnh hưởng hiệu năng dịch vụ	Cao	Cao	Trung bình	Thấp
Không ảnh hưởng dịch vụ	Trung bình	Trung bình	Thấp	Thấp

Bước 9: Báo cáo sự cố

Hàng tháng bộ phận giám sát ATTT lập báo cáo sự cố đã xảy ra trong tháng gửi Lãnh đạo Bộ, đơn vị liên quan.

Phụ lục X
Quy trình quản lý điểm yếu an toàn thông tin
(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Xác định các thành phần có trong hệ thống có khả năng tồn tại điểm yếu ATTT (thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác).

Bước 2: Rà quét các điểm yếu có trong hệ thống (tiến hành rà quét 03 tháng 01 lần) bằng các phần mềm chuyên dụng như: Acunetix, Nessus, Tenable,…

Bước 3: Phân loại, xử lý điểm yếu ATTT có trong hệ thống.

Các mức độ điểm yếu ATTT được xác định trong bảng sau:

Mức độ nguy hiểm	Mô tả	Xử lý
Nghiêm trọng	Là những điểm yếu khi bị khai thác cho phép tin tặc thực thi lệnh điều khiển mà không cần bất kỳ tác động nào của người sử dụng. Ví dụ: điểm yếu cho phép lây nhiễm mã độc hoặc thực hiện các lệnh điều khiển trên máy tính từ xa mà không đưa ra bất cứ thông báo nào cho người đang sử dụng máy tính.	Khi phát hiện có điểm yếu này thì người sử dụng cần có ngay biện pháp khắc phục hoặc cài đặt bản vá (Patch) do nhà sản xuất phần mềm cung cấp chính thức để ngăn chặn khả năng tin tặc khai thác điểm yếu.
Cao	Là những điểm yếu khi bị khai thác có thể gây ảnh hưởng đến: tính bí mật, toàn vẹn, sẵn sàng đối với dữ liệu của người sử dụng hoặc tài nguyên khác của hệ thống. Những điểm yếu này chỉ bị khai thác khi người sử dụng cố tình bỏ qua những cảnh báo của hệ điều hành hay ứng dụng. Ví dụ: người sử dụng truy cập vào những trang web có chứa mã độc được nhúng trong một đoạn Java Script mặc dù đã được trình duyệt cảnh báo.	Khi phát hiện các điểm yếu loại này người sử dụng cần có biện pháp khắc phục sớm nhất có thể. Trong trường hợp thực hiện nâng cấp hoặc cài đặt bản vá cho các ứng dụng người sử dụng cần xem xét mức độ ảnh hưởng của việc nâng cấp hoặc cài đặt tới các phần mềm và ứng dụng có liên quan.
Trung bình	Là những điểm yếu khi bị khai thác, ảnh hưởng xấu của nó có thể được hạn chế hay khắc phục bằng cách áp dụng biện pháp xác thực hoặc đôi khi chỉ là thay đổi cấu	Khi phát hiện các điểm yếu loại này người sử dụng chỉ thực hiện khi việc nâng cấp hay cài đặt bản vá khi đã xác định rõ bản vá không có ảnh hưởng tới các

Mức độ nguy hiểm	Mô tả	Xử lý
	hình mặc định của hệ điều hành, hoặc ứng dụng liên quan đến điểm yếu.	phần mềm, ứng dụng và hệ thống khác liên quan đang hoạt động. Khi chưa cập nhật bản vá hoặc nâng cấp theo hướng dẫn, thì cần có biện pháp bảo vệ và phòng ngừa các sự cố có thể xảy ra theo cảnh báo.
Thấp	Là những điểm yếu khi bị khai thác, ảnh hưởng của nó có thể khắc phục bằng cách thiết lập các thông số của hệ điều hành hoặc ứng dụng bị ảnh hưởng bởi điểm yếu.	Đối với các điểm yếu ở mức nguy hiểm này, việc lựa chọn các biện pháp khắc phục cũng giống như việc lựa chọn các biện pháp khắc phục đối với các điểm yếu có mức độ nguy hiểm Trung bình.

Bước 4: Lập báo cáo các điểm yếu của hệ thống đã xử lý, điểm yếu còn tồn tại trong hệ thống.

Phụ lục XI

Quy trình quản lý an toàn người sử dụng đầu cuối

(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Kiểm tra, cài đặt máy tính an toàn

Bộ phận chuyên trách về ATTT, kiểm tra máy tính của người sử dụng trước khi kết nối vào mạng chung:

- Kiểm tra chương trình diệt virus đã được cài đặt trên máy tính người sử dụng hay chưa;

- Kiểm tra máy tính còn tồn tại lỗ hổng bảo mật hay không;

- Cài đặt phần mềm theo dõi, giám sát ATTT trên máy người sử dụng.

- Vô hiệu hóa tính năng Autorun của ổ cứng di động;

- Vô hiệu hóa các tài khoản không sử dụng.

Bước 2: Đặt tên máy tính người sử dụng

Đặt tên máy tính người sử dụng phải thể hiện được tên người sử dụng, đơn vị, số phòng. Ví dụ: Nguyễn Văn An, Vụ Chính quyền địa phương, phòng 623 đặt tên máy tính là Annv-CQDP-623.

Bước 3: Cung cấp tài khoản sử dụng tài nguyên nội bộ

- Đơn vị thuộc, trực thuộc Bộ gửi công văn yêu cầu cung cấp tài khoản cho cá nhân, đơn vị sử dụng các phần mềm, cơ sở dữ liệu, thư điện tử đến đơn vị quản lý.

- Đơn vị quản lý phần mềm, cơ sở dữ liệu, thư điện tử tạo tài khoản và phân quyền cho tài khoản theo mục đích sử dụng của đơn vị yêu cầu.

- Thêm người sử dụng vào nhóm đơn vị gửi yêu cầu.

Bước 4: Theo dõi các diễn biến bất thường của máy tính người sử dụng

Quản trị viên mạng máy tính thường xuyên giám sát, theo dõi các hành vi bất thường của máy tính người sử dụng. Khi phát hiện sự cố phải xử lý ngay, tránh lây lan sang máy tính khác.

Phụ lục XII

Quy trình kết thúc vận hành, khai thác, thanh lý, hủy bỏ

(Kèm theo Quyết định số 1260/QĐ-BNV ngày 27/10/2025 của Bộ trưởng Bộ Nội vụ)

Bước 1: Lập danh sách và phân loại thiết bị

Công chức, viên chức kỹ thuật và công chức, viên chức có liên quan tiến hành lập danh sách và phân loại thiết bị:

- Thiết bị đang vận hành;

- Thiết bị hư hỏng không thể sửa chữa hoặc việc sửa chữa không hiệu quả (dự toán chi phí sửa chữa lớn hơn 30% giá trị của thiết bị), thiết bị cũ không bị hỏng nhưng có cấu hình thấp không đáp ứng nhu cầu sử dụng thì tiến hành thanh lý;

- Ổ cứng máy tính, thiết bị lưu trữ dữ liệu đã từng lưu trữ tài liệu mật khi không sử dụng phải hủy bỏ.

Bước 2: Ngắt thiết bị không sử dụng ra khỏi hệ thống

Đơn vị có liên quan gửi báo cáo bằng văn bản đến lãnh đạo đơn vị để báo cáo và xin ý kiến chỉ đạo về việc tháo, ngắt thiết bị không sử dụng ra khỏi hệ thống.

Bước 3: Thành lập hội đồng ra quyết định kết thúc vận hành, khai thác, thanh lý, hủy bỏ thiết bị (Hội đồng)

- Các đơn vị có liên quan lập danh sách các thiết bị thanh lý, hủy bỏ.

- Gửi Đơn đề nghị thanh lý, hủy bỏ thiết bị đến Lãnh đạo đơn vị hoặc Lãnh đạo Bộ để xin ý kiến chỉ đạo.

- Lãnh đạo đơn vị hoặc Lãnh đạo Bộ ra quyết định thanh lý thiết bị và thành lập hội đồng kiểm kê, đánh giá lại thiết bị.

- Thành phần Hội đồng bao gồm:

+ Lãnh đạo đơn vị hoặc Lãnh đạo Bộ: Chủ tịch Hội đồng;

+ Kế toán trưởng, kế toán tài sản;

+ Trưởng (hoặc phó) bộ phận cơ sở vật chất, công chức, viên chức phụ trách thiết bị;

+ Đại diện đơn vị trực tiếp quản lý thiết bị thanh lý;

+ Công chức, viên chức có hiểu biết về đặc điểm, tính năng kỹ thuật của thiết bị thanh lý.

Bước 4: Xử lý kỹ thuật

- Đối với thiết bị thanh lý công chức, viên chức kỹ thuật tiến hành xóa dữ liệu hoặc khôi phục thiết bị về trạng thái ban đầu của nhà sản xuất, đảm bảo không

thể khôi phục lại dữ liệu.

- Đối với các thiết bị hủy bỏ: Lập danh sách thiết bị hủy bỏ, xin ý kiến chỉ đạo của người có thẩm quyền để tiến hành hủy bỏ, thiết bị hủy bỏ cần phải xóa dữ liệu và đập vỡ.

Bước 5: Tiến hành thanh lý thiết bị

Tùy vào điều kiện và đặc điểm của thiết bị mà Hội đồng trình Thủ trưởng đơn vị hoặc Lãnh đạo Bộ xem xét, quyết định hình thức xử lý thiết bị như bán tài sản, hủy tài sản.

Hồ sơ cần chuẩn bị:

- Biên bản họp hội đồng: Biên bản ghi chép lại các nội dung đã được bàn và thống nhất trong buổi họp liên quan đến việc kiểm định chất lượng và giá trị của thiết bị, kết quả định giá, hình thức xử lý thiết bị.

- Biên bản kiểm kê thiết bị: Biên bản có mục đích xác nhận số lượng, hiện trạng của thiết bị và giá trị còn lại của tài sản.

Bước 6: Tổng hợp, xử lý kết quả thanh lý, hủy bỏ thiết bị của đơn vị

Hội đồng tiến hành lập Biên bản thanh lý, hủy bỏ thiết bị, sau đó bộ phận kế toán ghi giảm tài sản và giá trị tài sản theo quy định hiện hành của Nhà nước.