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

QUY CHẾ

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

(Ban hành kèm theo Quyết định số 309 /QĐ-BNV ngày 21 tháng 04 năm 2023 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 chính sách 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, phần mềm, cơ sở dữ liệu thuộc phạm vi quản lý của Bộ Nội vụ.

2. Đối tượng áp dụng

a) Các cơ quan, đơn vị thuộc, trực thuộc Bộ; cán bộ, công chức, viên chức, người lao động của Bộ Nội vụ.

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

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm ATTT mạng phục vụ hoạt động của hệ thống thông tin 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 an toàn thông tin mạng* là việc bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *An ninh mạng* là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

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

4. *Chính sách an toàn thông tin là* các quy tắc, quy trình cho tất cả các tổ chức, cá nhân truy cập và sử dụng tài nguyên trong hệ thống thông tin của tổ chức nhằm đảm bảo tính an toàn cho hệ thống thông tin và chống lại các hoạt động tấn công của tội phạm.

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

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

7. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Ứng cứu các sự cố an toàn thông tin 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 hệ thống thông tin.

9. *Lỗ hổng bảo mật (Security vulnerability)* là điểm yếu về ATTT trên phần mềm hoặc phần cứng, bị tin tặc khai thác để truy cập trái phép vào hệ thống thông tin.

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

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)* là hệ thống an ninh mạng, có thể là phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát lưu lượng truy cập (traffic) 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 ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động xâm nhập không mong muốn đối với hệ thống thông tin.

16. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

17. *Vùng mạng nội bộ (Local Area Network - LAN)* là vùng mạng đặt các thiết bị mạng, máy trạm và máy chủ dùng trong khu vực giới hạn nhất định, tốc độ truyền tải cao.

18. *Vùng mạng biên* được thiết kế để kết nối hệ thống thông tin ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống thông tin từ bên ngoài Internet.

19. *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. Các dịch vụ thường được triển khai trong vùng DMZ là: máy chủ Web, máy chủ Mail, máy chủ DNS, máy chủ FTP,…

20. *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.

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

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

1. Mục tiêu bảo đảm an toàn thông tin

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

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm ATTT và an ninh mạng cho các hệ thống thông tin của cơ quan, tổ chức theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm ATTT là yêu cầu bắt buộc, phải được thực hiện trong quá trình:

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

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

c) Việc bảo đảm an toàn hệ thống thông tin phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

3. Phạm vi chính sách an toàn thông tin

Phạm vi chính sách ATTT tại quy chế này bao gồm:

a) Thiết lập chính sách an toàn thông tin.

b) Tổ chức bảo đảm an toàn thông tin.

c) Bảo đảm nguồn nhân lực.

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

e) Quản lý vận hành hệ thống.

Điều 4. Những hành vi nghiêm cấm

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

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin đã cài đặt trên thiết bị CNTT phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần máy tính của cơ quan, đơn vị.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG TỔ CHỨC

Điều 5. Đơn vị chuyên trách về an toàn thông tin

Trung tâm Thông tin, Bộ Nội vụ là đơn vị chuyên trách về ATTT của Bộ Nội vụ có nhiệm vụ:

- Chủ trì, phối hợp với các đơn vị có liên quan thực hiện bảo đảm an ninh, an toàn thông tin mạng; triển khai, ứng dụng chứng thư số, chữ ký số trong hoạt động của Bộ theo quy định của pháp luật;

- Hướng dẫn, kiểm tra, giám sát, đánh giá công tác bảo đảm an toàn, an ninh mạng tại Bộ theo quy định; tổ chức ứng cứu sự cố an toàn thông tin mạng; phối hợp với các cơ quan nghiệp vụ triển khai các phương án bảo vệ, ngăn chặn xung đột các hệ thống thông tin và khắc phục xung đột thông tin mạng trong phạm vi quản lý của Bộ;

- Phối hợp tổ chức tập huấn nghiệp vụ, kiến thức, kỹ năng công nghệ thông tin, Chính phủ điện tử, Chính phủ số, kinh tế số, xã hội số, hành chính số, an toàn, an ninh mạng... theo phương thức kết hợp truyền thông và trực tuyến (e-Learning) cho cán bộ, công chức, viên chức trong Bộ, ngành Nội vụ.

Đơn vị chuyên trách CNTT của các đơn vị trực thuộc Bộ có trách nhiệm phối hợp với Trung tâm Thông tin trong việc bảo đảm ATTT, an ninh mạng của các hệ thống thông tin do các đơn vị trực thuộc Bộ quản lý, quản trị, vận hành.

Điều 6. Phối hợp với cơ quan, tổ chức có thẩm quyền

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

a) Trung tâm Thông tin - Bộ Nội vụ làm đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng của Bộ Nội vụ.

b) Trung tâm Thông tin - Bộ Nội vụ chủ trì, phối hợp với các đơn vị liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Lãnh đạo Bộ đối với các hệ thống thông tin của Bộ Nội vụ.

2. Đầu mối liên hệ, phối hợp với các cơ quan trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Bộ Tư lệnh 86 - Bộ Quốc phòng; Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an; Cục An toàn thông tin - Bộ Thông tin và Truyền thông và các đơn vị có liên quan, hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

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

Điều 7. Bảo đảm nguồn nhân lực

1. Công chức, viên chức, người lao động được tuyển dụng vào vị trí làm về ATTT có trình độ, chuyên ngành về lĩnh vực CNTT, ATTT, phù hợp với vị trí tuyển dụng:

- Có bằng tốt nghiệp đại học chuyên ngành máy tính, CNTT hoặc ATTT;

- Đáp ứng được các quy định của Thông tư số 45/2017/TT-BTTTT của Bộ Thông tin và Truyền thông Quy định tiêu chuẩn chức danh nghề nghiệp viên chức chuyên ngành CNTT;

- Có ít nhất 2 năm kinh nghiệm;

- Có cam kết giữ bí mật thông tin liên quan đến công việc.

2. Chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng

Công tác tuyển dụng thực hiện theo theo Nghị định 115/2020/NĐ-CP ngày 25/9/2020 của Chính phủ quy định về tuyển dụng, sử dụng và quản lý viên chức; Nghị định số 138/2020/NĐ-CP ngày 27/11/2022 của Chính phủ quy định về tuyển dụng, sử dụng và quản lý công chức và điều kiện tuyển dụng công chức, viên chức, người lao động về làm việc tại Bộ Nội vụ, theo đó trong quá trình tuyển dụng có thành lập Hội đồng tuyển dụng, bao gồm các chuyên gia có trình độ chuyên môn để kiểm tra, đánh giá ứng viên. Các chuyên gia cần đáp ứng các yêu cầu sau:

- Đã tốt nghiệp đại học các ngành nhân sự, quản trị nhân lực, ATTT hoặc các ngành có liên quan;

- Kinh nghiệm tối thiểu trong lĩnh vực tuyển dụng 2 năm;

- Có kiến thức và kinh nghiệm trong việc tìm kiếm nguồn nhân sự thông qua các kênh tuyển dụng, mạng xã hội hay các trang thông tin điện tử (trang web) tuyển dụng.

Điều 8. Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc

1. Quy định về thực hiện nội quy, quy chế bảo đảm ATTT cho người sử dụng, công chức, viên chức, người lao động quản lý và vận hành hệ thống

a) 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 và được dán tem ATTT;

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

- Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về an toàn thông tin, 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 cán bộ, 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, không ghi mật khẩu ra những nơi người khác có thể biết; không lưu trữ, truyền, gửi mật khẩu khi chưa được mã hóa an toàn và chia sẻ mật khẩu của cá nhân cho người khác;

- 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 hệ thống thông tin nội bộ nếu chưa được phép của đơn vị chủ quản; không tự thay thế, lắp mới, tráo đổi thành phần 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.

b) Đối với đội ngũ quản lý, vận hành hệ thống:

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

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

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

- Kết nối từ xa vào hệ thống thông tin phải thông qua VPN của thiết bị tường lửa (Firewall), có sự giám sát của quản trị viên hệ thống;

- Thực hiện chặt chẽ việc kiểm soát thay đổi của hệ thống thông tin: 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.

2. Định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức và ATTT cho người sử dụng.

3. Định kỳ hàng năm tổ chức đào tạo về ATTT cho cán bộ kỹ thuật, cán bộ quản lý, người sử dụng trong hệ thống.

Các đơn vị liên quan có trách nhiệm phối hợp với đơn vị chuyên trách ATTT xây dựng, triển khai kế hoạch đào tạo, bồi dưỡng, tập huấn về công tác bảo đảm ATTT, an ninh mạng cho đội ngũ công chức, viên chức của cơ quan, đơn vị.

Điều 9. 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 nghỉ việc hoặc thay đổi công việc phải tuân thủ:

- Phải bàn giao lại công việc, tài khoản truy cập hệ thống thông tin, tài sản CNTT của cơ quan, đơn vị; phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc;

- Quản trị viên hệ thống phải 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 thôi việc.

2. 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 thôi 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 thôi việc để đảm bảo đã hoàn toàn được gỡ bỏ khỏi hệ thống.

3. Cán bộ, công chức, viên chức nghỉ việc hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. Các thông tin bắt buộc cần giữ bí mật, tối thiểu bao gồm:

- Không tiết lộ thông tin được tiếp xúc trong quá trình công tác tại đơn vị cho các cá nhân, tổ chức gây ảnh hưởng bất lợi đến lợi ích của đơn vị;

- Không sử dụng các thông tin được tiếp xúc trong quá trình công tác tại đơn vị vào mục đích trục lợi cá nhân.

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

Điều 10. Thiết kế, xây dựng hệ thống thông tin

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

- Tài liệu 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 vùng mạng trong hệ thống: Vùng mạng nội bộ; vùng mạng biên; vùng mạng DMZ; vùng máy chủ nội bộ; vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; vùng mạng máy chủ cơ sở dữ liệu; vùng quản trị; vùng quản trị thiết bị hệ thống;

- Các giải pháp, thiết bị của hệ thống thông tin đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư số 12/2022/TT-BTTTT).

2. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp các tài liệu "Kiến trúc hệ thống" trong đó có mô tả thiết kế và các thành phần của hệ thống thông tin 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 hệ thống thông tin phải cung cấp tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ 3 trở lên được quy định tại Thông tư số 12/2022/TT-BTTTT.

4. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin, 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 hệ thống thông tin, 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 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.

Hồ sơ thiết kế phải được cất vào tủ có khóa. Những đợt nghỉ lễ, tết dài ngày phải niêm phong tủ đựng văn bản, tài liệu và phòng làm việc.

Hồ sơ thiết kế được sắp xếp một cách khoa học để dễ quản lý, dễ nộp lưu và dễ tìm khi cần. Phải có những cặp khác nhau để đựng những loại hồ sơ, văn bản, tài liệu khác nhau.

7. Bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện

Các đơn vị liên quan phối hợp và thành lập bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin trước khi triển khai thực hiện đảm bảo đầy đủ thông tin.

Điều 11. Phát triển phần mềm thuê khoán

1. Đối với các nội dung liên quan đến việc phát triển phần mềm thuê khoán, 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 phải cung cấp mã nguồn sản phẩm cho đơn vị thuê theo hình thức ghi đĩa DVD hoặc USB; yêu cầu 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 hệ thống thông tin 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 an toàn thông tin, trước khi đưa vào sử dụng

Hệ thống được đầu tư phải được kiểm định an toàn thông tin 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 an toàn thông tin 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 an toàn thông tin 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 bên thứ 3.

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 hệ thống thông tin phái ký biên bản cam kết bảo mật ATTT.

Điều 12. 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 an toàn thông tin 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,... xem 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 của các cơ quan chức năng; thực hiện nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng;

- Không cài cắm mã độc vào máy chủ; 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) Quy trình thử nghiệm hệ thống như sau:

- Phân tích yêu cầu;

- Lập kế hoạch kiểm thử;

- Thiết kế kịch bản cho quy trình kiểm thử;

- Thiết lập môi trường kiểm thử;

- Thực hiện kiểm thử;

- Đóng chu trình kiểm thử.

c) Nội dung, kế hoạch và quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 24/2020/TT-BTTTT ngày 09/09/2020 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 công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

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

Chủ quản hệ thống thông tin 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 an toàn thông tin;

- 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

Chủ quản hệ thống thông tin có trách nhiệm phối hợp với Trung tâm Thông tin - Bộ Nội vụ thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống trước khi đưa vào sử dụng.

5. Báo cáo nghiệm thu được ký xác nhận của Trung tâm Thông tin - Bộ Nội vụ và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

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

Điều 13. Quản lý an toàn mạng

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

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

b) Thường xuyên kiểm tra cấu hình, các tệp nhật ký hoạt động của hệ điều hành, phần mềm 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.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm 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 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.

k) 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).

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

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, khóa 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.

Điều 14. Quản lý an toàn máy chủ và ứng dụng

1. Quy định với máy chủ

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

b) 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 hệ thống máy chủ.

c) Máy chủ phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; 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.

d) Máy chủ phải được nâng cấp, xử lý điểm yếu ATTT trên máy chủ trước khi đưa vào sử dụng.

đ) 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.

e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.

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

h) 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.

i) 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 hệ thống thông tin.

k) Ghi nhật ký, quy định thời gian về hoạt động tác động vào các máy chủ, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra giám sát về sau.

2. Quy định với ứng dụng:

a) 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.

b) Ứng dụng phải được thiết lập chính sách 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.

c) 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.

d) 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.

đ) 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.

3. Quy định với ứng dụng 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 đủ mạnh cho hộp thư điện tử của mình.

c) Khi công chức, viên chức, người lao động nghỉ việc thì hộp thư điện tử sẽ bị khóa và xóa bỏ khỏi hệ thống thư điện tử.

d) Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án đảm bảo an toàn và tính khả dụng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử.

đ) Bảo đảm an toàn cho hệ thống thư điện tử: Thực hiện theo hướng dẫn tại công văn số 430/BTTTT-CATTT ngày 09 tháng 2 năm 2015 của Bộ Thông tin và Truyền thông về việc hướng dẫn đảm bảo an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước.

4. 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 hệ thống thông tin 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 (WAP- Web Application Firewall).

b) Cổng, trang thông tin điện tử khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss),...

c) Xây dựng phương án sao lưu, phục hồi Cổng, trang thông tin điện tử, trong đó chú ý mỗi tháng thực hiện việc sao lưu dữ liệu toàn bộ nội dung Cổng, trang thông tin điện tử một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

d) Bảo đảm an toàn cho Cổng, trang thông tin điện tử: Thực hiện theo hướng dẫn tại công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 của Bộ Thông tin và Truyền thông về việc hướng dẫn đảm bảo an toàn thông tin cho các Cổng, trang thông tin điện tử.

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.

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 trước khi đưa vào hệ thống sử dụng

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 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 độc hại trên máy tính.

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

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. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các tệp thực thi (.com),(.bat),(.exe)….

3. Cán bộ, 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. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tệp, thư mục phải được quét mã độc trước khi sao chép, 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.

Điều 18. Quản lý giám sát an toàn hệ thống thông tin

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 an toàn thông tin của các Hệ thống thông tin 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 hệ thống thông tin.

2. Các đơn vị trực thuộc Bộ có trách nhiệm phối hợp với Trung tâm Thông tin, 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.

Điều 19. Quản lý điểm yếu an toàn thông tin

1. Chủ quản hệ thống thông tin 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, cán bộ 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 hệ thống thông tin; 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

a) Đơn vị chủ quản hệ thống thông tin 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 hệ thống thông tin khi bị đối tượng tấn công xâm nhập.

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

+ Cục An toàn thông tin;

+ Trung tâm 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 hệ thống thông tin 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 hệ thống thông tin về điểm yếu ATTT phát hiện ra nhằm khắc phục, phòng tránh các sự cố an toàn thông tin;

+ 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 hệ thống thông tin;

+ 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.

Điều 20. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin 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 hệ thống thông tin cấp độ 3 hoặc cấp độ 4 hoặc cấp độ 5 khác.

e) Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

Đơn vị vận hành hệ thống thông tin khi phát hiện hoặc nhận được thông báo sự cố đối với hệ thống thông tin 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;

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố;

- Chủ trì, phối hợp cùng đơn vị cung cấp dịch vụ ATTT mạng (nếu có) 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 hệ thống thông tin.

3. Kế hoạch ứng cứu sự cố an toàn thông tin 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.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

a) Chủ quản hệ thống thông tin 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 hệ thống thông tin 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.

5. Quy trình ứng cứu sự cố an toàn thông tin 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 hệ thống thông tin 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 phướng án ứng cứu khẩn cấp đảm bảo an toàn thông tin. 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.

6. Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng

Thực hiện đầy đủ các nội dung quy định tại Điều 14, Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

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.

d) Triển khai phương án ứng cứu khẩn cấp.

đ) Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

e) Kết thúc.

7. 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 an toàn thông tin

- Chủ quản hệ thống thông tin, quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về an toàn thông tin; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất an toàn thông tin; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về an toàn thông tin; 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 an toàn thông tin; 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 cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

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

- Tổ chức diễn tập phương án xử lý sự cố ATTT, tối thiểu 1 lần/năm. Trung tâm 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

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/hệ thống thông tin 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/hệ thống 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
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/hệ thống 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
Nhỏ (2)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới quyền 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/hệ thống thông tin 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 hệ thống thông tin;

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 chính sách, mục đích, mục tiêu bảo đảm an toàn thông tin 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 an toàn thông tin mà tổ chức đưa ra, như sau:

+ Hệ thống thông tin cấp độ 5, có xử lý thông tin bí mật nhà nước, không chấp nhận tồn tại rủi ro. Chỉ chấp nhận tồn tại các rủi ro ở mức thấp đối với hệ thống thông tin cấp độ 5 không xử lý thông tin bí mật nhà nước. Đối với hệ thống thông tin 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.

+ Hệ thống thông tin 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 hệ thống thông tin cấp độ 3 hoặc cấp độ 4, không xử lý thông tin bí mật nhà nước;

+ Hệ thống thông tin 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 an toàn thông tin:Các mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức; các quy định pháp lý phải tuân thủ; quy chế, chính sách bảo đảm an toàn thông tin 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 hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất; trong đó, xác định rõ mức độ ảnh hưởng đến hệ thống thông tin đang được đề xuất cấp độ khi các hệ thống này bị mất an toàn thông tin; danh mục các nguy cơ tấn công mạng, mất an toàn thông tin 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 an toàn thông tin. Nội dung phương án, kế hoạch, trách nhiệm của các đơn vị, bộ phận liên quan cần đưa vào quy chế bảo đảm an toàn thông tin 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 an toàn thông tin:

+ 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, hệ thống thông tin.

+ 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 an toàn thông tin 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 an toàn thông tin 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 an toàn thông tin nhằm bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được thực hiện thường xuyên liên tục theo quy chế, chính sách bảo đảm an toàn thông tin 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 an toàn thông tin được mang lại hiệu quả, việc giám sát, soát xét và cải tiến quy trình quản lý rủi ro an toàn thông tin 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 an toàn thông tin.

c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, 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 an toàn thông tin, 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 công nghệ thông tin 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.

Điều 23. Kết thúc vận hành, khai thác, sửa chữa, 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 hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản hệ thống thông tin 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 hệ thống thông tin 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.

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 hệ thống thông tin theo cấp độ.

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

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

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

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin.

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 Thông tin - Bộ Nội vụ.

b) Bộ thông Thông tin và Truyền thông; 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 hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

Điều 25. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

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

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

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

2. Thẩm quyền kiểm tra

a) Trung tâm Thông tin - Bộ Nội vụ chịu trách nhiệm kiểm tra các đơn vị thuộc, trực thuộc Bộ Nội vụ.

b) Các đơn vị khác tự kiểm tra trong nội bộ đơn vị.

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. Tần suất thực hiện báo cáo:

a) Định kỳ hàng năm.

b) Đột xuất theo đề nghị của cơ quan có thẩm quyền (Bộ Công an; Bộ Thông tin và Truyền thông; Bộ Quốc phòng; Trung tâm Thông tin - Bộ Nội vụ;).

3. Thời gian chốt số liệu báo cáo định kỳ hàng năm:

Tính từ ngày 15 tháng 12 năm trước kỳ báo cáo đến ngày 14 tháng 12 của kỳ báo cáo.

4. Thời hạn gửi báo cáo đối với báo cáo định kỳ hàng năm:

Đơn vị chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin gửi báo cáo tới Trung tâm Thông tin - Bộ Nội vụ trước ngày 20 tháng 12 hàng năm.

Điều 27. Nội dung báo cáo

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

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

3. Danh sách hệ thống thông tin được phê duyệt Hồ sơ đề xuất cấp độ theo quy định.

4. Danh sách hệ thống thông tin 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 hệ thống thông tin có phương án bảo đảm ATTT theo quy định.

6. Danh sách hệ thống thông tin 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 hệ thống thông tin.

7. Danh sách hệ thống thông tin 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. Các thông tin khác theo yêu cầu của cơ quan có thẩm quyền (Bộ Công an; Bộ Thông tin và Truyền thông; Bộ Quốc phòng; Trung tâm Thông tin - Bộ Nội vụ).

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 28. Trách nhiệm của Trung tâm 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. Thẩm định về mặt kỹ thuật, công nghệ, ATTT đối với các dự án, hoạt động ứng dụng công nghệ thông tin, chuyển đổi số; hướng dẫn công tác bảo đảm an toàn, an ninh thông tin cho các cơ quan, đơn vị thuộc và trực thuộc Bộ Nội vụ.

3. 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.

4. 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.

5. Lập kế hoạch hàng năm trình Bộ trưởng Bộ Nội vụ phê duyệt và tổ chức triển khai kế hoạch bảo đảm an toàn, an ninh mạng của Bộ Nội vụ và kế hoạch đào tạo, bồi dưỡng nghiệp vụ cho cán bộ chuyên trách công nghệ thông tin.

6. 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.

7. Cấp mới, sửa đổi, thu hồi tài khoản, mật khẩu, truy cập và quyền khai thác tài nguyên mạng Bộ Nội vụ cho người sử dụng khi có yêu cầu bằng văn bản.

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. Cung cấp thông tin người sử dụng của đơn vị khi có sự thay đổi để Trung tâm 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.

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

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

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

6. Tạo điều kiện thuận lợi cho Trung tâm Thông tin - Bộ Nội vụ 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.

7. Phối hợp với Trung tâm Thông tin - Bộ Nội vụ để lấy ý kiến thẩm định về mặt kỹ thuật và công nghệ đối với các dự án, kế hoạch ứng dụng công nghệ thông tin.

8. Hàng năm rà soát lại quy chế bảo đảm ATTT kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

Điều 29. 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.

Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng gửi Trung tâm Thông tin - Bộ Nội vụ để tổng hợp, gửi Vụ Kế hoạch - Tài chính thẩm định, trình Bộ phê duyệt.

Điều 30. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị đồng thời là tiêu chí bắt buộc để xem xét tình hình khen thưởng và danh hiệu thi đua đối với các tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

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 Thông tin - Bộ Nội vụ để tổng hợp, báo cáo Lãnh đạo Bộ điều chỉnh, bổ sung Quy chế cho phù hợp./.