BỘ CÔNG AN
CỤC AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO
Số: 2009 /TB-A05-TTANMQG

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

Hà Nội, ngày 11 tháng 4 năm 2024

THÔNG BÁO

V/v hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

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

Căn cứ Nghị định số 01/NĐ-CP ngày 06/8/2018 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an;

Căn cứ Nghị quyết số 22/NQ-CP ngày 18/10/2019 của Chính phủ ban hành Chương trình hành động thực hiện Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia;

Căn cứ Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030;

Thời gian qua, tình hình an ninh mạng tại Việt Nam diễn biến hết sức phức tạp, hoạt động tấn công mạng nhằm vào các hệ thống thông tin trọng yếu của các cơ quan bộ, ngành, tổ chức, doanh nghiệp tại Việt Nam tiếp tục gia tăng về tần suất và mức độ nguy hiểm. Đáng chú ý, hình thức tấn công mạng bằng mã độc mã hóa dữ liệu đòi tiền chuộc (ransomware) đang ngày càng phổ biến và gây thiệt hại lớn về kinh tế và uy tín của cơ quan, tổ chức, doanh nghiệp; ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội. Trong khi đó, các cơ quan bộ, ban, ngành, tổ chức, doanh nghiệp chưa triển khai đầy đủ các biện pháp bảo vệ an ninh mạng cho các hệ thống thông tin theo quy định, gây khó khăn cho công tác điều tra, đấu tranh phòng, chống tội phạm của lực lượng Công an.

Từ tình hình trên, để tăng cường công tác bảo đảm an ninh mạng, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao ban hành tài liệu "*Hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia*" (gửi kèm theo) và đề nghị các cơ quan, đơn vị:

(1) Tham chiếu tài liệu "*Hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia*" để làm cơ sở đánh giá tổng thể, nghiên cứu cập nhật, bổ sung chính sách quản lý, quy trình quản trị, vận hành, các giải pháp bảo đảm an ninh mạng cho các hệ thống thông tin trọng yếu.

(2) Khẩn trương, ưu tiên tổ chức kiểm tra an ninh mạng; rà soát, gỡ bỏ mã độc trên máy tính (nếu có); sao lưu dự phòng dữ liệu quan trọng; tăng cường giám sát an ninh mạng để kịp thời phát hiện hoạt động tấn công mạng. Đồng thời, rà soát việc tuân thủ của bộ phận kỹ thuật, cán bộ, công nhân, viên chức đối với chính sách quản lý, quy chế bảo đảm an ninh mạng, quy trình quản trị, vận hành, ứng cứu sự cố, kiểm soát truy cập tài khoản quản trị đối với các hệ thống thông tin trọng yếu.

(3) Trao đổi kết quả kiểm tra, đánh giá tổng thể về an ninh mạng; kịp thời báo cáo về sự cố an ninh mạng nếu xảy ra trong quá trình vận hành về Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao để phối hợp triển khai các biện pháp bảo vệ an ninh mạng, hỗ trợ ứng cứu, xử lý, khắc phục sự cố.

Quá trình triển khai, thực hiện, nếu gặp khó khăn, vướng mắc, đề nghị các cơ quan, đơn vị liên hệ với*: Trung tâm An ninh mạng quốc gia - Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; hotline: 0593.505.999; thư điện tử: contact@nca.gov.vn* để được hỗ trợ, giải quyết.

Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thông báo các cơ quan, đơn vị để phối hợp thực hiện./.

Nơi nhận:
- Đ/c Bộ trưởng Tô Lâm
- Đ/c Thứ trưởng Lương Tam Quang | (để báo cáo);
- Văn phòng TW Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Văn phòng Quốc hội;
- Văn phòng Chính phủ;
- Các ban đảng Trung ương;
- Các bộ, cơ quan ngang bộ;
- Các cơ quan thuộc Chính phủ;
- Tỉnh ủy, UBND các tỉnh, thành phố trực thuộc TW;
- Các Tập đoàn, Tổng Công ty nhà nước;
- Công an các đơn vị, địa phương;
- Lưu: VT, A05(TTANMQG).

CỤC TRƯỞNG

CỤC AN NINH MẠNG VÀ P.C.T.P SỬ DỤNG CÔNG NGHỆ CAO

Trung tướng Nguyễn Minh Chính

HƯỚNG DẪN
CÁC BIỆN PHÁP TĂNG CƯỜNG BẢO ĐẢM AN NINH MẠNG CHO HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

(Ban hành kèm theo Thông báo số 1697/TB-A05-TTANMQG ngày 11/4/2024 của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an)

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

STT	Từ viết tắt	Giải thích
1	ANQG	An ninh quốc gia
2	CNTT	Công nghệ thông tin
3	DHCP	Dynamic Host Configuration Protocol - là một giao thức cho phép cấp phát địa chỉ IP một cách tự động.
4	DNS	Domain Name System - là máy chủ chứa cơ sở dữ liệu về địa chỉ IP công khai và các tên máy chủ được liên kết với chúng.
5	DMZ	Demilitarized Zone - là vùng mạng trung lập giữa mạng nội bộ và Internet.
6	URL	Uniform Resource Locator - là vị trí của một trang web trên Internet.
7	OT	Operation Technology - hay còn được gọi là Công nghệ Vận hành, là một khái niệm bao gồm tập hợp các phần cứng và phần mềm đóng vai trò phát hiện những thay đổi trong hệ thống thông qua việc quản lý, giám sát các thiết bị, máy móc, sự kiện trong quy trình vận hành công nghiệp.
8	IoT	Internet of Things - Internet vạn vật, là mạng kết nối các đồ vật và thiết bị thông qua cảm biến, phần mềm và các công nghệ khác, cho phép các đồ vật và thiết bị thu thập và trao đổi dữ liệu với nhau.
9	AAA	Xác thực (Authentication), Ủy quyền (Authorization) và Kiểm tra (Accounting).
10	VPN	Virtual Private Network - Mạng riêng ảo, là một mạng riêng để kết nối các máy tính của các đơn vị, tổ chức với nhau thông qua mạng Internet công cộng.
11	API	Application programming interface - giao diện lập trình ứng dụng, là một giao diện mà một hệ thống máy tính hay ứng dụng cung cấp để cho phép các yêu cầu dịch vụ có thể được tạo ra từ các chương trình máy tính khác để trao đổi dữ liệu.

I. PHẠM VI, ĐỐI TƯỢNG VÀ NGUYÊN TẮC ÁP DỤNG

1. Phạm vi áp dụng

Hướng dẫn này đưa ra các biện pháp, yêu cầu quản lý cần thiết để tăng cường bảo đảm an ninh mạng, nâng cao khả năng phòng thủ cho hệ thống thông tin quan trọng về an ninh quốc gia; đồng thời tạo thuận lợi cho công tác của lực lượng chuyên trách bảo vệ an ninh mạng (*như: giám sát bảo vệ, điều phối ứng phó sự cố, thẩm định, kiểm tra, đánh giá điều kiện an ninh mạng...*) và hoạt động bảo vệ hệ thống của cơ quan chủ quản, bao gồm: (1) Quản lý tài sản phần cứng; (2) Quản lý tài sản phần mềm; (3) Quản lý tài sản thông tin; (4) Cấu hình an toàn cho thiết bị và phần mềm; (5) Quản lý tài khoản và quyền truy cập tài khoản của người dùng; (6) Quản lý lỗ hổng bảo mật; (7) Quản lý nhật ký an ninh mạng; (8) Bảo vệ cho trình duyệt web, dịch vụ thư điện tử; (9) Phòng chống phần mềm độc hại; (10) Sao lưu và khôi phục dữ liệu; (11) Quản lý hạ tầng mạng; (12) Giám sát và phòng thủ an ninh mạng; (13) Nâng cao nhận thức và đào tạo kỹ năng an ninh mạng; (14) Quản lý nhà cung cấp dịch vụ; (15) Quản lý an ninh cho phần mềm ứng dụng; (16) Quản trị ứng phó sự cố an ninh mạng; (17) Kiểm thử xâm nhập.

2. Đối tượng áp dụng

Hướng dẫn này khuyến cáo áp dụng cho các hệ thống thông tin, gồm:

- Hệ thống thông tin đã được xác định, nằm trong Danh mục Hệ thống thông tin quan trọng về an ninh quốc gia do Thủ tướng Chính phủ phê duyệt; hoặc các hệ thống thông tin đã được cấp có thẩm quyền phê duyệt, nộp hồ sơ đề nghị đưa vào Danh mục Hệ thống thông tin quan trọng về an ninh quốc gia;

- Hệ thống thông tin đáp ứng các căn cứ xác lập danh mục hệ thống thông tin quan trọng về an ninh quốc gia quy định tại Điều 3 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; được chủ quản hệ thống thông tin tự xác định và tuân thủ.

- Hệ thống thông tin đã được xác định cấp độ 4, 5 theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; nhưng cần tham chiếu, bổ sung để tăng cường bảo đảm an ninh mạng khi chưa có Tiêu chuẩn mới, cập nhật thay thế Tiêu chuẩn quốc gia TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

- Khuyến khích áp dụng rộng rãi cho các hệ thống thông tin khác ngoài các trường hợp nói trên.

3. Nguyên tắc áp dụng

a) Tuân thủ quy định của pháp luật.

b) Hướng dẫn mang tính chất khuyến cáo áp dụng, không thay thế phương án bảo đảm an toàn hệ thống thông tin đang áp dụng (nếu đã xây dựng, phê duyệt Hồ

sơ đề xuất cấp độ an toàn thông tin) mà nhằm giúp chủ quản các hệ thống thông tin rà soát, đối chiếu để tổ chức triển khai, tăng cường bảo đảm an ninh mạng.

c) Để hiệu quả bảo đảm an ninh mạng ở mức cao nhất, khuyến khích chủ quản của hệ thống thông tin quan trọng về an ninh quốc gia triển khai các biện pháp bảo đảm an ninh mạng đáp ứng toàn bộ các yêu cầu (bao gồm cả các yêu cầu khuyến khích thực hiện).

II. GIẢI THÍCH THUẬT NGỮ VÀ ĐỊNH NGHĨA

1. An ninh mạng: là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Hệ thống thông tin quan trọng về an ninh quốc gia

Được quy định tại Khoản 1, Khoản 2 Điều 10 Luật An ninh mạng, bao gồm:

a) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu;

b) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước;

c) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng;

d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái;

đ) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia;

e) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương;

g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí;

h) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

3. Trung tâm An ninh mạng quốc gia (National Cyber Security Agency – viết tắt là NCA): là đơn vị trực thuộc thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an; có chức năng giám sát, phân tích, cảnh báo sớm các nguy cơ đe dọa an ninh mạng quốc gia; tham gia bảo vệ an ninh mạng đối với các cơ quan, đơn vị trọng yếu.

4. Hệ thống thông tin (Information System): 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 của cơ quan, tổ chức.

5. Tài sản công nghệ thông tin: Các trang thiết bị, thông tin thuộc hệ thống CNTT của đơn vị; bao gồm:

a) Tài sản phần cứng: là các thiết bị CNTT, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống CNTT.

b) Tài sản phần mềm: bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

c) Tài sản thông tin: là các dữ liệu, tài liệu liên quan đến hệ thống CNTT, được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử.

6. Phần mềm trái phép (Unauthorized Software): Những phần mềm không nằm trong danh sách phần mềm được phép sử dụng hoặc đã hết thời gian hỗ trợ của nhà cung cấp.

7. An ninh thông tin (Information Security): Sự bảo vệ thông tin, hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bí mật và tính khả dụng của thông tin.

8. Dữ liệu quan trọng (Important Data): Dữ liệu trong hệ thống, được cơ quan, tổ chức xác định là quan trọng, cần được ưu tiên bảo vệ. Dữ liệu quan trọng bao gồm, nhưng không giới hạn các loại dữ liệu chứa các thông tin sau: thông tin nghiệp vụ, thông tin bí mật nhà nước, thông tin riêng và các loại thông tin quan trọng khác (nếu có).

9. Giám sát hệ thống thông tin (Information System Monitoring): Biện pháp giám sát, theo dõi trạng thái hoạt động của hệ thống để phát hiện, cảnh báo sớm các sự cố có thể gây gián đoạn hoạt động của hệ thống và làm mất tính khả dụng của hệ thống thông tin.

10. Nhật ký hệ thống (System Log): Những sự kiện được hệ thống ghi lại liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh thông tin và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

11. Phần mềm độc hại (Malware): 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.

12. Phương tiện lưu trữ (Media Storage): Các thiết bị, phương tiện được sử dụng để lưu trữ, sao chép, trao đổi thông tin giữa các thiết bị, máy tính một cách gián tiếp.

13. Xác thực đa yếu tố (Multi-Factor Authentication): Phương pháp xác thực không chỉ dựa vào một mà là kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập...), những thông tin mà người dùng sở hữu (chứng thư số, thẻ thông minh...) hoặc những thông tin về sinh trắc học của người dùng (vân tay, mống mắt...).

14. Tiến trình (Process): Một thực thể chương trình đang được chạy trong hệ thống.

15. Khôi phục (Rollback): Thao tác đưa hệ thống về một trạng thái cũ.

16. Kiểm soát (Control): Quá trình thiết lập các tiêu chuẩn đo lường kết quả thực hiện, so sánh kết quả với các tiêu chuẩn, phát hiện sai lệch và nguyên nhân, tiến hành các điều chỉnh nhằm làm cho kết quả cuối cùng phù hợp với mục tiêu đã được xác định.

III. CÁC BIỆN PHÁP TĂNG CƯỜNG BẢO ĐẢM AN NINH MẠNG

1. Quản lý tài sản phần cứng

a) Yêu cầu chung

- Lập danh sách, theo dõi, cập nhật trạng thái của tất cả các tài sản công nghệ thông tin nội bộ và các tài sản không thuộc quyền kiểm soát của tổ chức nhưng có kết nối vào hệ thống nội bộ, xác định danh sách tài sản cần được giám sát, bảo vệ.

- Xác định các tài sản vô chủ, tài sản trái phép để loại bỏ hoặc đưa ra phương án quản lý.

- Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả các tài sản định kỳ tối thiểu 02 lần/năm.

- Khai báo và cập nhật đầy đủ tình trạng tài sản phần cứng trên hệ thống quản lý của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao để phục vụ công tác quản lý, đánh giá an ninh, an toàn, ứng phó sự cố đối với các hệ thống thông tin quan trọng về an ninh quốc gia.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
1.1	Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng	- Lập danh sách, theo dõi, cập nhật trạng thái của tất cả các tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị văn phòng, thiết bị mạng, thiết bị OT/IoT và máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây. - Tất cả tài sản vật lý phải được kiểm tra an ninh bởi cơ quan, tổ chức có thẩm quyền theo quy định của pháp luật trước khi đưa vào sử dụng. - Danh sách tài sản phần cứng phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có), vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống	Cần thiết

		mạng, mục đích sử dụng, tình trạng sử dụng. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng. - Các thiết bị di động kết nối vào hệ thống mạng nội bộ của tổ chức phải được đăng ký để kiểm soát. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.	
1.2	Xử lý các tài sản phần cứng chưa được quản lý	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào mạng nội bộ của cơ quan, tổ chức định kỳ tối thiểu 01 lần/tuần. - Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.	Cần thiết
1.3	Rà soát các tài sản kết nối vào mạng nội bộ	- Xây dựng, ban hành và bảo đảm tuân thủ quy định rà quét để phát hiện tài sản kết nối vào mạng nội bộ định kỳ tối thiểu 01 lần/tuần. - Thực hiện cập nhật danh sách tài sản dựa trên kết quả rà quét.	Cần thiết
1.4	Sử dụng DHCP Logging để cập nhật bản kiểm kê tài sản công nghệ thông tin nội bộ	- Sử dụng tính năng ghi nhận ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có). - Tiến hành rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin định kỳ tối thiểu 01 lần/tuần.	Cần thiết
1.5	Quản lý tài sản thanh lý/ hư hỏng	Xây dựng, ban hành và bảo đảm tuân thủ quy trình thanh lý/ tiêu hủy tài sản CNTT, bảo đảm xóa không thể khôi phục toàn bộ dữ liệu của cơ quan, tổ chức trước khi tiến hành thanh lý/ tiêu hủy.	Cần thiết

2. Quản lý tài sản phần mềm

a) Yêu cầu chung

- Lập danh sách, theo dõi, cập nhật trạng thái của tất cả các tài sản phần mềm của cơ quan, tổ chức, bảo đảm chỉ những phần mềm đã phê duyệt mới được phép cài đặt và sử dụng.

- Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả các tài sản phần mềm định kỳ tối thiểu 02 lần/năm.

- Khai báo và cập nhật đầy đủ tình trạng tài sản phần mềm trên hệ thống quản lý của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao để phục vụ công tác quản lý, đánh giá an ninh, an toàn, ứng phó sự cố đối với các hệ thống thông tin quan trọng về an ninh quốc gia.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
2.1	Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm	- Lập danh sách, theo dõi, cập nhật trạng thái của tất cả các tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng của cơ quan, tổ chức. - Danh sách tài sản phần mềm phải bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm phải được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.	Cần thiết
2.2	Thiết lập và duy trì danh sách các tài sản phần mềm được phép sử dụng	- Lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong toàn cơ quan, tổ chức. - Danh sách phần mềm được phép sử dụng phải bao gồm cả các thư viện phần mềm (như các file có định dạng .dll, .ocx…) và các đoạn mã lệnh thực thi (các script có định dạng .py, .ps1, .bat…) - Xây dựng, ban hành và bảo đảm tuân thủ quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép, bảo đảm giới hạn đặc quyền tối thiểu các quyền quản trị trên các tài sản CNTT; ngăn chặn các tác vụ thực thi, vô hiệu hóa, cài đặt và gỡ bỏ phần mềm, thư viện, đoạn mã lệnh trái phép trên hệ thống; có phương án kỹ thuật để theo dõi hoạt động cài đặt chương trình phần mềm trên các tài sản CNTT. - Định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng tối thiểu 02 lần / năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến danh sách.	Cần thiết

2.3	Đảm bảo toàn bộ các tài sản phần mềm được phép sử dụng đang trong thời gian hỗ trợ của nhà cung cấp	Thực hiện định kỳ rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng để bảo đảm tất cả tài sản phần mềm đang trong thời gian hỗ trợ của nhà cung cấp, tối thiểu 02 lần / năm.	Cần thiết
2.4	Xử lý các tài sản phần mềm trái phép	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình phát hiện và xử lý các phần mềm trái phép định kỳ tối thiểu 01 lần / quý. - Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức phải được đưa vào danh sách ngoại lệ để quản lý. Danh sách ngoại lệ này phải thể hiện chi tiết các biện pháp kiểm soát giảm thiểu các nguy cơ an ninh mạng ảnh hưởng đến hệ thống. - Những phần mềm trái phép không nằm trong danh sách ngoại lệ phải có kế hoạch để xóa/ gỡ bỏ hoàn toàn khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.	Cần thiết

3. Quản lý tài sản thông tin

a) Yêu cầu chung

Thực hiện quản lý tài sản thông tin và thực hiện các biện pháp kiểm soát để phát hiện, phân loại, xử lý, lưu giữ và loại bỏ tài sản thông tin một cách an toàn.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
3.1	Thiết lập và duy trì quy trình quản lý tài sản thông tin	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình quản lý tài sản thông tin. Trong quy trình, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin. - Mức độ nhạy cảm của tài sản thông tin có thể được quy định như sau:	Cần thiết

		+ Mức 1: Công khai. Tài sản thông tin công khai không yêu cầu về bảo mật. + Mức 2: Nội bộ. Tài sản thông tin nội bộ yêu cầu chỉ những người trong tổ chức mới có quyền truy cập. + Mức 3: Hạn chế. Tài sản thông tin bị hạn chế yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế sẽ ảnh hưởng đến hoạt động của các đơn vị. + Mức 4: Bí mật nhà nước. Thông tin có nội dung quan trọng, do cơ quan, tổ chức có thẩm quyền xác định; chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc (*thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước*). - Xây dựng quy trình yêu cầu truy cập, thêm mới, sửa, xoá dữ liệu để kiểm soát nhật ký truy cập dữ liệu. - Kiểm tra cấp độ phân quyền của các nguồn dữ liệu định kỳ tối thiểu 01 lần/tháng. - Đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ tối thiểu 01 lần/ năm hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình.	
3.2	Thiết lập và duy trì bản danh sách tài sản thông tin	- Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin. - Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách.	Cần thiết
3.3	Xây dựng danh sách kiểm soát truy cập tài sản thông tin	Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.	Cần thiết
3.4	Mã hoá dữ liệu quan trọng	- Mã hoá dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của tổ chức. - Mã hoá dữ liệu quan trọng trong quá trình truyền gửi để bảo đảm tính toàn vẹn của dữ liệu.	Cần thiết

		- Thực hiện bảo vệ và quản lý vòng đời mã khóa sử dụng để mã hóa dữ liệu.	
3.5	Tài liệu hoá luồng dữ liệu	- Có tài liệu mô tả các luồng dữ liệu quan trọng. - Xây dựng và tuân thủ quy định quản lý phiên bản tài liệu tại tổ chức. - Đánh giá và cập nhật định kỳ tối thiểu 01 lần/năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến tài liệu.	Cần thiết
3.6	Tách biệt quá trình xử lý và lưu trữ dữ liệu theo mức độ nhạy cảm	- Xây dựng, ban hành và bảo đảm tuân thủ quy định về việc xử lý dữ liệu nhạy cảm. - Tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao với dữ liệu có độ nhạy cảm thấp. Không sử dụng các tài sản/ môi trường dành cho dữ liệu nhạy cảm thấp để lưu trữ và xử lý dữ liệu có mức độ nhạy cảm cao.	Cần thiết
3.7	Triển khai giải pháp phòng chống thất thoát dữ liệu	Xây dựng và triển khai giải pháp chống thất thoát dữ liệu đối với dữ liệu có độ nhạy cảm mức 03 trở lên trong toàn tổ chức.	Cần thiết
3.8	Lưu trữ nhật ký truy cập dữ liệu quan trọng	- Ghi lại nhật ký hành vi đối dữ liệu có độ nhạy cảm mức 03 trở lên, bao gồm các hành vi truy cập, chỉnh sửa, huỷ bỏ dữ liệu. - Rà soát nhật ký thường xuyên, tối thiểu định kỳ 01 lần/ tháng để phát hiện sớm những hành vi truy cập trái phép.	Cần thiết

4. Cấu hình an toàn cho thiết bị và phần mềm

a) Yêu cầu chung

Thiết lập và duy trì cấu hình an toàn cho thiết bị (như thiết bị người dùng cuối bao gồm thiết bị di động và cầm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ) và phần mềm (như hệ điều hành, ứng dụng…).

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
4.1	Thiết lập và duy trì quy định, quy trình cấu	- Xây dựng, ban hành và bảo đảm tuân thủ quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Cần thiết

	hình an toàn cho tài sản phần cứng và phần mềm	- Xây dựng, ban hành và bảo đảm tuân thủ các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập phần mềm tường lửa trên máy chủ/ máy trạm và có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng. - Đánh giá và cập nhật quy trình quản lý cấu hình an toàn và các tài liệu liên quan tối thiểu 01 lần/năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.	
4.2	Cấu hình tự động khoá phiên làm việc trên các tài sản phần cứng và phần mềm	- Tự động khoá phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng. + Đối với máy tính người dùng, thời gian này không vượt quá 15 phút. + Đối với các thiết bị mạng, thời gian này không vượt quá 05 phút. + Đối với thiết bị di động, thời gian này không vượt quá 02 phút. + Đối với các phần mềm nghiệp vụ xử lý dữ liệu quan trọng, thời gian này không vượt quá 15 phút. - Tự động khoá thiết bị di động sau một số lần đăng nhập thất bại. + Đối với máy tính xách tay, số lần đăng nhập thất bại tối đa 10 lần. + Đối với điện thoại, số lần đăng nhập thất bại tối đa 10 lần. + Đối với các phần mềm nghiệp vụ xử lý và lưu trữ dữ liệu quan trọng, số lần đăng nhập thất bại tối đa 05 lần.	Cần thiết
4.3	Gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm	Xây dựng, ban hành và bảo đảm tuân thủ quy định gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.	Cần thiết

4.4	Cấu hình máy chủ DNS tin cậy	Thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.	Tuỳ chọn
4.5	Thiết lập khả năng xoá sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng	Xây dựng và triển khai giải pháp xoá sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.	Cần thiết
4.6	Phân tách các không gian làm việc riêng biệt trên các thiết bị di động cấp cho người dùng	- Xây dựng, ban hành và bảo đảm tuân thủ quy định tách biệt các không gian làm việc riêng biệt trên thiết bị di động cấp cho người dùng. - Xây dựng giải pháp kỹ thuật cho phép quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối tới các hệ thống của tổ chức.	Tuỳ chọn

5. Quản lý tài khoản và quyền truy cập tài khoản của người dùng

a) Yêu cầu chung

- Thiết lập, tuân thủ và duy trì quy trình, công cụ để chỉ định và quản lý việc cấp quyền tài khoản người dùng bao gồm tài khoản quản trị, tài khoản dịch vụ trên các tài sản công nghệ thông tin và phần mềm.

- Xây dựng và thực thi quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng, tài khoản quản trị và tài khoản dịch vụ cho tài sản công nghệ thông tin và phần mềm. Quyền truy cập của tài khoản người dùng, quản trị viên và dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, bảo đảm người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

- Ghi nhật ký và giám sát tài khoản người dùng.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
5.1	Thiết lập và duy trì hệ thống quản lý tài khoản	- Lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.	Cần thiết

		- Danh sách tài khoản phải bao gồm các loại tài khoản sau: tài khoản người dùng, tài khoản quản trị và tài khoản dịch vụ. - Danh sách tài khoản phải bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hoá tài khoản (nếu có). Đảm bảo tất cả tài khoản đang hoạt động là hợp lệ. - Danh sách tài khoản phải được rà soát định kỳ 01 lần / quý.	
5.2	Xây dựng và tuân thủ quy định sử dụng mật khẩu	- Xây dựng, ban hành và bảo đảm tuân thủ quy định sử dụng mật khẩu an toàn trong tổ chức, đáp ứng các yêu cầu sau: + Sử dụng mật khẩu duy nhất cho mỗi tài sản. + Thay đổi mật khẩu định kỳ 01 lần/ 02 tháng. + Đối với các hệ thống sử dụng xác thực đa yếu tố, quy định mật khẩu có tối thiểu 08 ký tự. + Đối với các hệ thống không sử dụng xác thực đa yếu tố, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số. + Mật khẩu mới không được trùng với 10 mật khẩu trước đó.	Cần thiết
5.3	Xây dựng và tuân thủ quy định quản lý tài khoản	- Xây dựng, ban hành và bảo đảm tuân thủ quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau: + Quản lý tài khoản tập trung. + Quản lý tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ). + Quản lý tách biệt giữa các loại tài khoản: tài khoản người dùng, tài khoản quản trị và tài khoản dịch vụ. + Xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý tài khoản.	Cần thiết
5.4	Xây dựng và tuân thủ quy định	- Xây dựng, ban hành và bảo đảm tuân thủ quy định về quản lý truy cập đáp ứng các yêu cầu sau:	Cần thiết

	quản lý truy cập	+ Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản. + Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức. + Yêu cầu xác thực đa yếu tố đối với các ứng dụng có kết nối ra bên ngoài tổ chức, kết nối đến đối tác/ bên thứ ba, kết nối internet; các truy cập từ xa đến hệ thống mạng nội bộ và các tài khoản có quyền quản trị hệ thống. + Định kỳ rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần / năm.	
5.5	Xây dựng và tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức. - Định kỳ rà soát quy trình và công tác thực hiện cấp quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức tối thiểu 01 lần / năm.	Cần thiết

6. Quản lý lỗ hổng bảo mật

a) Yêu cầu chung

- Xây dựng, phát triển kế hoạch đánh giá và theo dõi các lỗ hổng bảo mật thường xuyên để khắc phục và giảm thiểu nguy cơ bị tấn công.

- Theo dõi, cập nhật thông tin về các mối đe doạ, lỗ hổng bảo mật mới từ nhiều nguồn.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
6.1	Thiết lập, tuân thủ và duy trì quy trình quản lý lỗ hổng bảo mật	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình quản lý lỗ hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức. Các nội dung tối thiểu bao gồm: + Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai các giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức. Định kỳ thực hiện rà soát tổng thể	Cần thiết

		hệ thống tối thiểu 01 lần/ quý và rà soát đối với các tài sản quan trọng tối thiểu 01 lần / tháng. + Đánh giá mức độ nghiêm trọng của lỗ hổng: Xây dựng và triển khai phương pháp đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng. + Báo cáo/ chia sẻ thông tin lỗ hổng: Chia sẻ thông tin về lỗ hổng bảo mật với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao và các bên liên quan. Thiết lập và duy trì cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác. + Triển khai các biện pháp khắc phục: Xây dựng phương án, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và các bước đánh giá lại hệ thống để bảo đảm lỗ hổng đã được khắc phục hoàn toàn. - Rà soát và cập nhật quy trình tối thiểu 01 lần / năm hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này.	
6.2	Thiết lập, tuân thủ và duy trì quy trình quản lý bản vá	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình quản lý bản vá. Các nội dung tối thiểu bao gồm: + Xây dựng và triển khai máy chủ quản lý bản vá tập trung cho toàn bộ tài sản phần cứng và phần mềm của cơ quan, tổ chức. + Đánh giá tác động, tiến hành kiểm thử và xây dựng phương án phục hồi trước khi triển khai bản vá trên các hệ thống thông tin có xử lý hoặc lưu trữ dữ liệu quan trọng. + Thực hiện cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/tháng. + Giám sát và duy trì hệ thống để bảo đảm không có lỗ hổng mới xuất hiện và các bản vá vẫn hoạt động tốt.	Cần thiết

7. Quản lý nhật ký an ninh mạng

a) Yêu cầu chung

- Có chính sách thu thập, phân tích, giám sát và lưu trữ nhật ký an ninh mạng để phát hiện sớm và ứng phó sự cố tấn công mạng.

- Chia sẻ dữ liệu nhật ký an ninh mạng với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao để hỗ trợ phát hiện, cảnh báo và khắc phục sự cố tấn công mạng đối với các hệ thống thông tin quan trọng về an ninh quốc gia.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
7.1	Thiết lập, tuân thủ và duy trì một quy trình quản lý nhật ký an ninh mạng	- Xây dựng, ban hành và bảo đảm tuân thủ quy định quản lý nhật ký an ninh mạng, trong đó bao gồm: + Quy định về cách thức ghi nhật ký. + Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký. + Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng, nhật ký cảnh báo của các thiết bị bảo mật. + Đảm bảo việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT chứa dữ liệu nhạy cảm của tổ chức. + Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 18 tháng. Triển khai hệ thống theo dõi tránh tình trạng đầy không gian lưu trữ, dẫn tới thất thoát dữ liệu. + Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần / tuần. - Chia sẻ nhật ký an ninh mạng của các hệ thống trọng yếu với Trung tâm An ninh mạng quốc gia để hỗ trợ phân tích, săn tìm, cảnh báo nguy cơ an ninh mạng nếu có. - Kiểm tra và cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình này.	Cần thiết
7.2	Thu thập nhật ký an ninh mạng của nhà cung cấp dịch vụ	Thực hiện thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối các dịch vụ mà tổ chức sử dụng.	Tuỳ chọn

7.3	Bảo vệ nhật ký an ninh mạng	- Kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng. - Đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ.	Cần thiết

8. Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

a) Yêu cầu chung

Tăng cường bảo vệ và phát hiện các mối đe doạ từ dịch vụ thư điện tử, trình duyệt web.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
8.1	Quản lý trình duyệt web và dịch vụ thư điện tử	- Ban hành danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan và tổ chức. - Đảm bảo danh sách trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp. - Đảm bảo chỉ sử dụng phiên bản trình duyệt và dịch vụ thư điện tử mới nhất được cung cấp thông qua nhà cung cấp.	Cần thiết
8.2	Sử dụng dịch vụ lọc tên miền (DNS Filtering)	Triển khai sử dụng dịch vụ lọc tên miền DNS Filtering trong toàn cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.	Cần thiết
8.3	Thực thi và cập nhật các bộ lọc URL	Triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản doanh nghiệp kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.	Cần thiết
8.4	Kiểm soát việc sử dụng các tiện ích mở rộng trong trình duyệt web và ứng dụng thư điện tử	- Xác định danh sách tiện ích mở rộng được phép sử dụng trong trình duyệt web, dịch vụ điện tử. - Kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử. - Gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.	Cần thiết

8.5	Triển khai giải pháp xác thực email	Triển khai giải pháp xác thực email thông qua DMARC (Domain-based Message Authentication, Reporting & Conformance) để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.	Cần thiết
8.6	Quản lý các loại tệp được phép đính kèm trong trong thư điện tử	- Xác định danh sách các loại tệp được phép gửi qua hệ thống thư điện tử. - Ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát các thư điện tử có chứa tệp đính kèm.	Cần thiết
8.7	Triển khai và duy trì biện pháp bảo vệ mã độc đối với máy chủ thư điện tử	Xây dựng và triển khai các phương án bảo vệ mã độc đối với máy chủ thư điện tử.	Cần thiết

9. Phòng chống phần mềm độc hại

a) Yêu cầu chung

- Xây dựng quy định để quản lý, phòng chống, khắc phục việc cài đặt, lây lan, thực thi các phần mềm và đoạn mã độc hại trong cơ quan, tổ chức.

- Triển khai hệ thống phòng chống mã độc trên tất cả các tài sản và các điểm kết nối giữa những hệ thống thông tin (bao gồm cả kết nối nội bộ và kết nối ra bên ngoài tổ chức). Hệ thống phòng chống mã độc phải phù hợp và tương thích với các hệ thống thông tin của cơ quan, tổ chức, đồng thời có khả năng tự động dò quét, ngăn chặn khi phát hiện mã độc, cập nhật kịp thời các mẫu nhận diện mã độc mới và tích hợp với quy trình quản lý lỗ hổng và ứng phó sự cố.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
9.1	Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc	- Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc trên hệ thống. - Sử dụng các giải pháp tổng thể gồm có phòng, chống mã độc, phát hiện mã độc dựa trên hành vi, bao gồm ít nhất các tính năng cơ bản như bảo vệ thời gian thực, tự động cập nhật các mẫu nhận diện mã độc mới…	Cần thiết

9.2	Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài	Triển khai rà quét mã độc và vô hiệu hoá tính năng tự động thực thi đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…	Cần thiết
9.3	Quản lý tập trung các phần mềm phòng, chống mã độc	Triển khai giải pháp quản trị tập trung phần mềm phòng, chống mã độc trong toàn cơ quan, tổ chức.	Cần thiết
9.4	Kích hoạt tính năng phòng chống khai thác lỗ hổng	Kích hoạt các tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm như Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), Apple® System Integrity Protection (SIP), Gatekeeper™…	Cần thiết
9.5	Xây dựng và triển khai giải pháp phòng chống mã độc theo hành vi	Triển khai giải pháp phòng và chống mã độc dựa trên hành vi (EDR - Endpoint Detection and Response).	Cần thiết

10. Sao lưu và khôi phục dữ liệu

a) Yêu cầu chung

Triển khai và duy trì phương án sao lưu, phục hồi dữ liệu, bảo đảm khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
10.1	Xây dựng và tuân thủ quy định sao lưu và khôi phục dữ liệu	- Xây dựng, ban hành và bảo đảm tuân thủ quy định sao lưu và khôi phục dữ liệu. Các nội dung tối thiểu bao gồm: + Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục.	Cần thiết

		+ Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa. + Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa. + Quản lý vùng lưu trữ dữ liệu sao lưu, bảo đảm tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh chóng và hiệu quả. + Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu. - Rà soát và cập nhật quy định tối thiểu 01 lần/năm hoặc khi xảy thay đổi trong tổ chức ảnh hưởng đến quy định.	
10.2	Thực hiện sao lưu dữ liệu tự động	- Xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm...) đối với từng loại dữ liệu. - Triển khai các giải pháp sao lưu dữ liệu tự động.	Cần thiết
10.3	Bảo vệ dữ liệu khôi phục	- Thực hiện bảo vệ dữ liệu khôi phục với các điều kiện như đối với dữ liệu gốc. - Thực hiện mã hoá đối với những dữ liệu quan trọng.	Cần thiết
10.4	Thiết lập và duy trì hạ tầng lưu trữ tách biệt cho dữ liệu khôi phục	Các dữ liệu khôi phục cần phải được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng tách biệt với môi trường vận hành.	Cần thiết
10.5	Kiểm tra khả năng khôi phục dữ liệu	Kiểm tra khả năng khôi phục bản sao lưu tối thiểu 01 lần/03 tháng.	Cần thiết

11. Quản lý hạ tầng mạng

a) Yêu cầu chung

Thiết lập, thực thi và quản lý các thiết bị mạng để phòng ngừa tin tặc khai thác lỗ hổng dịch vụ mạng và các điểm truy cập dễ bị tấn công.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
11.1	Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng và kiến trúc mạng an toàn	- Thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng. - Triển khai và duy trì một kiến trúc hệ thống mạng an toàn, bảo đảm thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng. - Tài liệu hóa sơ đồ kiến trúc hệ thống mạng bao gồm: + Tổng quan kiến trúc hệ thống mạng; + Sơ đồ cấp chi tiết của hệ thống mạng; + Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê…; + Tài liệu mô tả phương án bảo đảm an ninh mạng. - Xem xét và cập nhật sơ đồ mạng 01 lần/06 tháng hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống.	Cần thiết
11.2	Quản lý an toàn cơ sở hạ tầng mạng	- Thực hiện quản lý an toàn cơ sở hạ tầng mạng. - Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu: có phân vùng mạng riêng cho máy chủ của hệ thống thông tin; có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây; có phân vùng mạng riêng đối với máy chủ cơ sở dữ liệu.	Cần thiết
11.3	Quản lý tập trung việc xác thực, cấp quyền và kiểm toán mạng.	Triển khai hệ thống AAA để quản lý tập trung việc xác thực, cấp quyền và kiểm toán cho toàn cơ quan, tổ chức.	Cần thiết
11.4	Sử dụng các giao thức truyền thông và quản trị	Sử dụng các giao thức truyền thông và quản trị mạng an toàn.	Cần thiết

	mạng an toàn		
11.5	Xây dựng và áp dụng chính sách quản lý truy cập từ xa	- Xây dựng và áp chính sách quản lý truy cập từ xa đáp ứng yêu cầu sau: + Sử dụng mạng riêng ảo VPN cho việc truy cập từ xa vào hệ thống. + Yêu cầu người dùng xác thực đa yếu tố để VPN và các dịch vụ xác thực khác trước khi truy cập vào hệ thống. + Các thiết bị được phép truy cập từ xa phải bảo đảm các yêu cầu về bảo mật: cài đặt phần mềm phòng chống mã độc, cấu hình bảo mật theo chính sách an toàn đã ban hành của tổ chức.	Cần thiết
11.6	Thiết lập và duy trì tài nguyên hệ thống dành riêng cho công tác quản trị	Thiết lập và duy trì các nguồn tài nguyên dành riêng, tách biệt về mặt vật lý và logic; được phân tách với mạng chính của hệ thống và không kết nối với Internet.	Cần thiết

12. Giám sát và phòng thủ an ninh mạng

a) Yêu cầu chung

- Xây dựng, vận hành các quy trình và công cụ để thiết lập, duy trì giám sát mạng toàn diện và bảo vệ hệ thống mạng khỏi các mối đe doạ.

- Kết nối các hệ thống quan trọng với hệ thống chỉ huy giám sát an ninh mạng của Trung tâm An ninh mạng quốc gia để triển khai giám sát, phát hiện và xử lý sự cố.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
12.1	Quản lý tập trung các cảnh báo và sự kiện an ninh mạng	- Triển khai giải pháp quản lý tập trung các sự kiện an ninh mạng để liên kết các sự kiện liên quan và phân tích theo hướng dẫn, yêu cầu của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao và quy định của cơ quan, tổ chức. - Kết nối với hệ thống chỉ huy giám sát an ninh mạng của Trung tâm An ninh	Cần thiết

		- Xem xét và cập nhật quy định tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy định này.	
14.3	Đảm bảo các hợp đồng cung cấp dịch vụ có kèm theo các yêu cầu bảo mật	- Đảm bảo các hợp đồng với nhà cung cấp dịch vụ bao gồm đầy đủ yêu cầu về bảo mật trong đó quy định trách nhiệm kết nối, chia sẻ thông tin giám sát an ninh mạng về Trung tâm An ninh mạng quốc gia để quản lý, hỗ trợ giám sát, điều phối ứng phó sự cố tấn công mạng nếu xảy ra. - Đánh giá và cập nhật hợp đồng của nhà cung cấp dịch vụ hàng năm để bảo đảm đầy đủ các yêu cầu bảo mật.	Cần thiết
14.4	Thực hiện theo dõi các nhà cung cấp dịch vụ	Giám sát các nhà cung cấp dịch vụ thực hiện quy định quản lý cung cấp dịch vụ của tổ chức.	Cần thiết
14.5	Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ	Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.	Cần thiết
14.6	Cấp phép hoặc kiểm tra an ninh đối với cá nhân, nhà cung cấp dịch vụ	Các cá nhân, nhà cung cấp dịch vụ cho chủ quản hệ thống thông tin quan trọng về ANQG phải được Bộ Công an thẩm tra lý lịch nhân sự.	Cần thiết

15. Quản lý an ninh cho phần mềm ứng dụng

a) Yêu cầu chung

Quản lý vòng đời bảo mật của các phần mềm ứng dụng để phòng ngừa, phát hiện và xử lý các điểm yếu, lỗ hổng bảo mật.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
15.1	Thiết lập và duy trì quy trình phát triển ứng dụng an toàn	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình phát triển ứng dụng an toàn. - Đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.	Cần thiết

15.2	Thiết lập và duy trì quy trình tiếp nhận và xử lý các lỗ hổng bảo mật phần mềm	- Xây dựng, ban hành và bảo đảm tuân thủ quy trình tiếp nhận và xử lý các báo cáo về lỗ hổng bảo mật phần mềm, bao gồm cả việc cung cấp phương tiện để các thực thể bên ngoài báo cáo. - Quản lý, theo dõi lỗ hổng bảo mật phần mềm bao gồm xếp hạng mức độ nghiêm trọng và chỉ số đo lường thời gian để xác định, phân tích và khắc phục các lỗ hổng. - Đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.	Cần thiết
15.3	Thực hiện phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật	Thực hiện phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật.	Cần thiết
15.4	Thiết lập và quản trị hệ thống kiểm kê các cấu thành phần mềm của bên thứ ba	- Thiết lập và quản lý một danh sách cập nhật các thành phần của bên thứ ba được sử dụng trong quá trình phát triển (thư viện, mô đun...) và các thành phần dự kiến sẽ sử dụng trong tương lai để phát triển phần mềm. - Danh sách bao gồm các nguy cơ an ninh mạng mà mỗi thành phần bên thứ ba có thể gây ra. - Đánh giá và cật nhật danh sách tối thiểu 01 lần/ tháng.	Cần thiết
15.5	Tách biệt môi trường cho các hoạt động phát triển, kiểm thử và vận hành	Duy trì việc tách biệt môi trường vận hành chính thức (Production), môi trường kiểm thử (Testing) và môi trường phát triển ứng dụng (Development).	Cần thiết
15.6	Đào tạo về bảo mật và lập trình an toàn	- Đảm bảo tất cả nhân viên phát triển phần mềm được đào tạo về trách nhiệm và phương thức phát triển phần mềm an toàn đối với từng môi trường/ giải pháp cụ thể. - Thực hiện đào tạo tối thiểu 01 lần/năm.	Cần thiết
15.7	Kết hợp các nguyên tắc bảo mật	Kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng.	Cần thiết

	trong kiến trúc ứng dụng		
15.8	Tận dụng các mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật ứng dụng	- Tận dụng các mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật của ứng dụng. - Chỉ sử dụng các thuật toán mã hoá được chuẩn hoá và đánh giá rộng rãi. - Ghi nhật ký kiểm toán các hành vi của người dùng trong sản phẩm.	Cần thiết
15.9	Tiến hành kiểm thử xâm nhập các ứng dụng	Kiểm thử xâm nhập và khắc phục các lỗ hổng trước khi đưa vào vận hành chính thức.	Cần thiết

16. Quản trị ứng phó sự cố an ninh mạng

a) Yêu cầu chung

Xây dựng kế hoạch, chương trình để phát triển và duy trì khả năng ứng phó sự cố bao gồm chính sách, kế hoạch, thủ tục, vai trò, đào tạo, kênh liên lạc.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
16.1	Thành lập lực lượng ứng phó sự cố an ninh mạng	- Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng. - Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố. Xác minh thông tin liên hệ hàng năm để bảo đảm rằng thông tin được cập nhật. - Phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.	Cần thiết
16.2	Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng	- Thiết lập và duy trì một quy trình nội bộ để báo cáo sự cố an ninh mạng. - Các sự cố an ninh mạng cần được báo cáo đầy đủ về Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao. - Đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.	Cần thiết

16.3	Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng	- Thiết lập và duy trì một quy trình ứng phó sự cố. - Quy trình ứng phó sự cố an ninh mạng cần đặt dưới sự chỉ huy của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao khi có yêu cầu. - Đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.	Cần thiết
16.4	Thiết lập cơ chế (kênh kỹ thuật) liên lạc trong quá trình xử lý sự cố	- Thiết lập cơ chế chính và cơ chế phụ sử dụng để giao tiếp và báo cáo trong xử lý sự cố an ninh mạng. - Đánh giá và cập nhật cơ chế liên lạc tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến cơ chế.	Cần thiết
16.5	Thực hiện đánh giá sau sự cố an ninh mạng	Thực hiện đánh giá sau sự cố an ninh mạng.	Cần thiết
16.6	Định kỳ diễn tập ứng phó sự cố an ninh mạng	Lập kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố định kỳ tối thiểu 01 lần/năm.	Cần thiết
16.7	Triển khai và duy trì các ngưỡng sự cố an ninh mạng	- Thiết lập và duy trì các ngưỡng sự cố an ninh mạng. - Đánh giá và cập nhật ngưỡng tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến ngưỡng.	Tuỳ chọn

17. Kiểm thử xâm nhập

a) Yêu cầu chung

Xác định tính hiệu quả trong năng lực phòng vệ và khả năng phục hồi của các tài sản, đặc biệt là hệ thống thông tin quan trọng về an ninh quốc gia thông qua việc khai thác các điểm yếu trong quy trình kiểm soát về con người, quy trình, công nghệ; mô phỏng lại các mục tiêu và hành động của kẻ tấn công.

b) Yêu cầu chi tiết

STT	Yêu cầu	Nội dung thực hiện	Khuyến cáo áp dụng
17.1	Thiết lập và duy trì một chương trình kiểm thử xâm nhập	- Thiết lập và duy trì một chương trình kiểm thử xâm nhập phù hợp với quy mô,	Cần thiết

		mức độ phức tạp và trạng thái của tổ chức. - Chương trình kiểm thử xâm nhập cần đáp ứng một số nội dung sau: 1. Về phạm vi tiến hành: kiểm thử hạ tầng mạng, ứng dụng web, API, các dịch vụ được sử dụng trong tổ chức; kiểm tra một phần hoặc toàn bộ tổ chức. 2. Về tính thường xuyên: các cuộc kiểm thử được tổ chức theo chu kì quý, nửa năm, một năm hoặc đột xuất. 3. Về các giới hạn: xác định thời gian thực hiện kiểm thử; các hành vi tấn công bị cấm (tấn công vật lý, tấn công lừa đảo, tấn công phi kỹ thuật...). 4. Về cách phản ứng của tổ chức: có thực hiện việc ngăn chặn hay không, cơ chế kiểm soát thông tin (về cuộc kiểm thử) trong nội bộ.	
17.2	Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài	- Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài tối thiểu 01 lần/năm. - Áp dụng với các ứng dụng, dịch vụ của tổ chức được công khai ra mạng Internet.	Cần thiết
17.3	Khắc phục các tồn tại phát hiện được qua việc kiểm thử xâm nhập	Khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập dựa trên chính sách của tổ chức về phạm vi và mức độ ưu tiên khắc phục.	Cần thiết
17.4	Rà soát các biện pháp bảo mật	Kiểm tra các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.	Tuỳ chọn
17.5	Định kỳ thực hiện kiểm thử xâm nhập từ bên trong	- Định kỳ thực hiện kiểm thử xâm nhập từ bên trong tối thiểu 01 lần/năm. - Áp dụng với các tài nguyên nội bộ trong hệ thống thông tin của tổ chức.	Cần thiết