BỘ CÔNG AN	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 47 /2026/TT-BCA	*Hà Nội, ngày 12 tháng 5 năm 2026*

THÔNG TƯ

Ban hành Quy chuẩn kỹ thuật quốc gia về an ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan Đảng, Nhà nước

Căn cứ Luật Tiêu chuẩn và quy chuẩn kỹ thuật số 68/2006/QH11 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật số 70/2025/QH15;

Căn cứ Luật Lưu trữ số 33/2024/QH15;

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Nghị định số 22/2026/NĐ-CP ngày 16 tháng 01 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp để tổ chức, hướng dẫn thi hành Luật Tiêu chuẩn và quy chuẩn kỹ thuật;

Căn cứ Nghị định số 02/2025/NĐ-CP ngày 18 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an được sửa đổi, bổ sung bởi Nghị định số 11/2025/NĐ-CP;

Theo đề nghị của Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao;

Bộ trưởng Bộ Công an ban hành Thông tư ban hành Quy chuẩn kỹ thuật quốc gia về an ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan Đảng, Nhà nước.

Điều 1. Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về an ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan Đảng, Nhà nước - QCVN 12:2026/BCA.

Điều 2. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2026.

Điều 3. Điều khoản thi hành

1. Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao có trách nhiệm theo dõi, kiểm tra, đôn đốc việc thực hiện Thông tư này.

2. Thủ trưởng các đơn vị thuộc cơ quan Bộ, Giám đốc Công an tỉnh, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

Trong quá trình thực hiện Thông tư, nếu có khó khăn, vướng mắc Công an các đơn vị, địa phương, tổ chức, cá nhân có liên quan báo cáo về Bộ Công an (qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để kịp thời hướng dẫn./.

Nơi nhận:
- Các đồng chí Thứ trưởng Bộ Công an;
- Văn phòng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố;
- Cục Kiểm tra văn bản và Tổ chức thi hành pháp luật Bộ Tư pháp;
- Các đơn vị thuộc cơ quan Bộ Công an;
- Công an các tỉnh, thành phố;
- Công báo;
- Cổng TTĐT Chính phủ;
- Cổng TTĐT Bộ Công an;
- Lưu: VT, A05.

BỘ TRƯỞNG

Đại tướng Lương Tam Quang

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 12:2026/BCA

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ AN NINH MẠNG CHO HỆ THỐNG THÔNG TIN LƯU TRỮ TÀI LIỆU ĐIỆN TỬ TRONG CÁC CƠ QUAN ĐẢNG, NHÀ NƯỚC

National technical regulation on Cybersecurity for Electronic document storage Information systems in party and state agencies

Hà Nội - 2026

Lời nói đầu

QCVN 12:2026/BCA do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Cục Khoa học, chiến lược và lịch sử Công an trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Công an ban hành theo Thông tư số /2026/TT-BCA ngày tháng năm 2026.

MỤC LỤC

QUY CHUẨN KỸ THUẬT QUỐC GIA
VỀ AN NINH MẠNG CHO HỆ THỐNG THÔNG TIN LƯU TRỮ TÀI LIỆU ĐIỆN TỬ TRONG CÁC CƠ QUAN ĐẢNG, NHÀ NƯỚC

National technical regulation

on Cybersecurity for Electronic document storage information systems in party and state agencies

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn này quy định các yêu cầu trong hoạt động quản lý, vận hành và bảo đảm an ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan Đảng, Nhà nước không chứa thông tin thuộc phạm vi bí mật nhà nước.

1.2. Đối tượng áp dụng

Quy chuẩn này áp dụng đối với các cơ quan, tổ chức, cá nhân có liên quan đến hoạt động quản lý, vận hành và bảo đảm an ninh mạng cho hệ thống thông tin thuộc phạm vi điều chỉnh của Quy chuẩn này.

Quy chuẩn này không áp dụng đối với các cơ quan, tổ chức, cá nhân có liên quan đến hoạt động quản lý, vận hành và bảo đảm an ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử có chứa bí mật nhà nước và giải pháp về bảo mật, xác thực trong hoạt động nghiệp vụ lưu trữ của các cơ quan Đảng, Nhà nước thuộc lĩnh vực quản lý nhà nước về cơ yếu, chữ ký số chuyên dùng công vụ.

1.3. Tài liệu viện dẫn

TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng;

TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Luật An ninh mạng số 116/2025/QH15;

NIST SP 800-88 Rev 2 - Guidelines for Media Sanitization.

1.4. Chữ viết tắt

ACL	Access Control List	Danh sách kiểm soát truy cập
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động
DLP	Data Leak Prevention	Chống thất thoát dữ liệu
DNS	Domain Name System	Hệ thống phân giải tên miền
FTP	File Transfer Protcol	Giao thức truyền tải tệp
HTTP	Hypertext Transfer Protocol	Giac thức truyền siêu văn bản
IP	Internet Protocol	Giao thức Internet

IPsec	Internet Protocol Security	Giao thức bảo mật mạng IP
MAC	Media Access Control	Điều khiển truy cập môi trường
MFA	Multi-factor Authentication	Xác thực đa nhân tố
SIEM	Security Information and Event Management	Hệ thống quản lý nhật ký và sự kiện tập trung
VPN	Virtual Private Network	Mạng riêng ảo
DMARC	Domain-based Message Authentication, Reporting & Conformance	Giao thức xác thực email
ISP	Internet Service Provider	Doanh nghiệp cung cấp dịch vụ Internet
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
NAC	Network Access Control	Kiểm soát truy cập mạng
SLA	Service Level Agreement	Thỏa thuận cung cấp dịch vụ
BCP	Business Continuity Plan	Kế hoạch duy trì hoạt động kinh doanh
DR	Disaster Recovery	Kế hoạch phục hồi sau thảm họa
NTP	Network Time Protocol	Giao thức đồng bộ thời gian trên mạng
PTP	Precision Time Protocol	Giao thức đồng bộ thời gian chính xác
EDR	Endpoint Detection and Response	Hệ thống phát hiện và phản hồi tại điểm cuối
URL	Uniform Resource Locator	Địa chỉ tài nguyên thống nhất
UTC	Coordinated Universal Time	Giờ phối hợp quốc tế
NGFW	Next-Generation Firewall	Tường lửa thế hệ mới
WAF	Web Application Firewall	Tường lửa ứng dụng web
WORM	Write Once Read Many	Ghi một lần, đọc nhiều lần
ANM		An ninh mạng
CNTT		Công nghệ thông tin

1.5. Giải thích từ ngữ

1.5.1. Lưu trữ

Lưu trữ là hoạt động lưu giữ tài liệu nhằm gìn giữ và phát huy các giá trị của tài liệu lưu trữ, phục vụ sự nghiệp xây dựng và bảo vệ Tổ quốc, bảo đảm quyền tiếp cận thông tin của công dân.

1.5.2. Tài liệu

Tài liệu là thông tin gắn liền với vật mang tin có nội dung và hình thức thể hiện không thay đổi khi chuyển đổi vật mang tin. Tài liệu bao gồm tài liệu giấy, tài liệu trên vật mang tin khác và tài liệu điện tử.

1.5.3. Tài liệu điện tử

Tài liệu điện tử là tài liệu tạo lập ở dạng thông điệp dữ liệu.

1.5.4. An ninh mạng

An ninh mạng là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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.

1.5.5. Hệ thống thông tin

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 không gian mạng.

1.5.6. Hệ thống thông tin lưu trữ tài liệu điện tử

Hệ thống thông tin lưu trữ tài liệu điện tử là hệ thống thông tin dùng để thu thập, quản lý, lưu trữ và truy cập tài liệu điện tử một cách an toàn, toàn vẹn và lâu dài.

1.5.7. Nhật ký hệ thống

Nhật ký hệ thống là những sự kiện được hệ thống ghi lại liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh mạng và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

1.5.8. Phần mềm độc hại

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

1.5.9. Phương tiện lưu trữ

Phương tiện lưu trữ là 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.

1.5.10. Vật mang tin

Vật mang tin là các thiết bị, phương tiện vật lý và kỹ thuật số được hệ thống sử dụng để ghi nhận, lưu giữ, bảo quản và truy xuất dữ liệu của tài liệu điện tử.

1.5.11. Vật mang tin khác

Vật mang tin khác là các thiết bị, phương tiện lưu trữ dữ liệu điện tử độc lập, di động, lưu trữ ngoại tuyến hoặc các công nghệ lưu trữ mới không thuộc hạ tầng lưu trữ tập trung của hệ thống.

1.5.12. Rủi ro an ninh mạng

Rủi ro an ninh mạng là khả năng bị lộ hoặc mất mát do một cuộc tấn công mạng hoặc vi phạm dữ liệu trong cơ quan, tổ chức, đơn vị. Rủi ro an ninh mạng không chỉ nằm ở khả

năng xảy ra một cuộc tấn công mạng mà còn là những hậu quả tiềm ẩn, ví dụ như tổn thất tài chính, thiệt hại về danh tiếng hoặc gián đoạn hoạt động.

1.5.13. Bản sao lưu dữ liệu

Bản sao lưu dữ liệu là bản sao của dữ liệu, thông tin được tạo ra và lưu trữ nhằm khôi phục hệ thống, ứng dụng hoặc dữ liệu khi xảy ra sự cố, mất mát hoặc hư hỏng.

1.5.14. Nhà cung cấp

Nhà cung cấp là tổ chức hoặc cá nhân thực hiện việc cung cấp sản phẩm, dịch vụ.

1.5.15. Gọi về máy chủ (call-home)

Gọi về máy chủ là việc phần mềm chủ động liên lạc với máy chủ nhà phát triển định kỳ hoặc theo sự kiện.

1.5.16. Ghi một lần, đọc nhiều lần (Write Once Read Many)

Ghi một lần, đọc nhiều lần là cơ chế lưu trữ cho phép ghi dữ liệu chỉ một lần, nhưng có thể đọc lại nhiều lần, giúp bảo vệ dữ liệu khỏi bị thay đổi hoặc bị xóa.

1.5.17. Tài sản công nghệ thông tin quan trọng

Tài sản công nghệ thông tin quan trọng là tài sản có vai trò thiết yếu đối với hệ thống thông tin, bao gồm: tài sản phần cứng, tài sản phần mềm, tài sản thông tin và các thành phần liên quan khác.

2. QUY ĐỊNH KỸ THUẬT

2.1. Yêu cầu chung

Chủ quản hệ thống thông tin có trách nhiệm xác định cấp độ hệ thống thông tin, áp dụng biện pháp bảo vệ theo cấp độ và thực hiện kiểm tra, đánh giá định kỳ đối với toàn bộ hệ thống thông tin thuộc phạm vi quản lý theo quy định tại Điều 8 Luật An ninh mạng số 116/2025/QH15. Đồng thời, chủ quản hệ thống thông tin có trách nhiệm rà soát hệ thống thông tin và áp dụng bổ sung các yêu cầu an ninh mạng theo TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng.

2.2. Yêu cầu kỹ thuật

2.2.1. Quản lý rủi ro

2.2.1.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.1. Quản lý rủi ro an ninh mạng.

2.2.1.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.1 Quản lý rủi ro an ninh mạng, trong đó:

2.2.1.2.1. Chủ quản hệ thống thông tin phải thực hiện quản lý rủi ro an ninh mạng và lưu trữ kết quả đánh giá rủi ro thành hồ sơ.

2.2.1.2.2. Đánh giá rủi ro phải xác định các tài sản thuộc sở hữu của chủ quản hệ thống thông tin, bao gồm nhưng không giới hạn: tài sản phần cứng, phần mềm, thông tin; từ đó, nhận diện các yếu tố rủi ro (dựa trên giá trị tài sản, lỗ hổng của hệ thống và các mối đe dọa). Đánh giá rủi ro dựa trên kết quả phân tích; từ kết quả của đánh giá rủi ro, thực hiện xử lý rủi ro (xây dựng chính sách, biện pháp kỹ thuật an ninh mạng). Thực hiện song song việc giám sát, cập nhật định kỳ và truyền thông rủi ro an ninh mạng với những thay đổi liên quan đến rủi ro đã được xác định.

2.2.1.2.3. Việc phân tích rủi ro phải bao gồm các yếu tố liên quan đến vật mang tin lưu trữ (cả vật mang tin chính và sao lưu), phù hợp với loại hình đang được sử dụng (ví dụ: vật mang tin có cơ chế WORM hoặc vật mang tin có khả năng ghi lại).

2.2.1.2.4. Việc đánh giá rủi ro phải cân nhắc đến sự cân bằng giữa chi phí triển khai và mức độ an toàn, bảo mật đạt được. Dựa trên kết quả phân tích, các biện pháp an toàn, bảo mật hiện có phải được xem xét lại về tính hiệu quả và thực hiện các điều chỉnh cần thiết.

2.2.2. An toàn vật lý

2.2.2.1. Chủ quản hệ thống thông tin phải xây dựng, ban hành và đảm bảo tuân thủ quy định, quy trình kiểm soát ra vào; trong đó, quy định, quy trình phải đáp ứng tối thiểu các yêu cầu sau:

2.2.2.1.1. Phải tạo yêu cầu, cấp quyền cho phép truy cập, ra, vào các khu vực quan trọng như khu vực máy chủ, nơi lưu trữ.

2.2.2.1.2. Ghi đầy đủ nhật ký hoạt động, hành vi.

2.2.2.1.3. Thực hiện xóa bỏ, thu hồi việc cấp quyền ngay khi hết nhiệm vụ.

2.2.2.1.4. Định kỳ rà soát quy định, quy trình tối thiểu 01 năm/lần hoặc khi có thay đổi ảnh hưởng đến quy định, quy trình này.

2.2.2.2. Phải triển khai các biện pháp bảo mật vật lý nhằm ngăn chặn việc truy cập trái phép vào hệ thống, tài sản, nhật ký kiểm toán và các bản sao lưu. Đối với khu vực làm việc chung hoặc khu vực yêu cầu truy cập liên tục, các thiết bị quan trọng lưu trữ dữ liệu phải được bố trí tách biệt về mặt vật lý hoặc có biện pháp bảo vệ riêng nhằm ngăn chặn việc tiếp cận trực tiếp từ môi trường bên ngoài.

2.2.3. Quản lý tài sản phần cứng

2.2.3.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.2. Quản lý tài sản phần cứng.

2.2.3.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.2 Quản lý tài sản phần cứng.

2.2.3.3. Phải quản lý toàn bộ tài sản phần cứng và lưu trữ kết quả kiểm kê thành hồ sơ.

2.2.4. Quản lý tài sản phần mềm

2.2.4.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.3 Quản lý tài sản phần mềm.

2.2.4.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 trở lên phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.3 Quản lý tài sản phần mềm.

2.2.4.3. Chủ quản hệ thống thông tin phải quản lý toàn bộ tài sản phần mềm và lưu trữ kết quả kiểm kê thành hồ sơ.

2.2.5. Quản lý tài sản thông tin

2.2.5.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu tại mục 4.4 Quản lý tài sản thông tin của TCVN 14423:2025.

2.2.5.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu tại mục 5.4 Quản lý tài sản thông tin của TCVN 14423:2025.

2.2.5.3. Chủ quản hệ thống thông tin phải thực hiện phân loại, kiểm kê và gán nhãn mức độ nhạy cảm cho toàn bộ tài sản thông tin, cập nhật định kỳ và lưu trữ kết quả kiểm kê thành hồ sơ.

2.2.5.4. Hệ thống thông tin lưu trữ tài liệu điện tử phải có cơ chế bảo đảm tính toàn vẹn của tài liệu, bao gồm:

2.2.5.4.1. Đảm bảo nội dung và cấu trúc của tài liệu không bị thay đổi trái phép kể từ khi tài liệu được tiếp nhận vào hệ thống cho đến khi tiêu hủy hoặc chuyển giao.

2.2.5.4.2. Sử dụng các thuật toán băm an toàn theo quy định để tạo ra giá trị băm duy nhất cho mỗi tài liệu; giá trị băm này phải được lưu trữ trong cơ sở dữ liệu và đảm bảo an toàn.

2.2.5.4.3. Tự động kiểm tra định kỳ để so sánh giá trị băm hiện tại của tập tin với giá trị băm gốc ban đầu, phát hiện sự thay đổi của tài liệu hoặc sự can thiệp trái phép.

2.2.5.4.4. Tự động phục hồi khi phát hiện tài liệu bị mất tính toàn vẹn.

2.2.5.5. Đối với các tài liệu điện tử có yêu cầu bảo mật, hạn chế truy cập khi lưu trữ ngoại tuyến hoặc truyền đưa trên môi trường mạng, hệ thống phải có chức năng thiết lập mật khẩu bảo vệ trực tiếp trên tệp tin hoặc mã hóa nội dung tài liệu.

2.2.6. Cấu hình an toàn phần cứng và phần mềm

2.2.6.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.5 Cấu hình an toàn cho phần cứng và phần mềm.

2.2.6.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.5 Cấu hình an toàn cho phần cứng và phần mềm; trong đó, trước khi đưa vào vận hành chính thức, phần mềm phải được đánh giá đảm bảo an ninh mạng và được đánh giá định kỳ hàng năm theo quy định pháp luật, cụ thể:

2.2.6.2.1. Việc đánh giá đảm bảo không ảnh hưởng đến tính sẵn sàng của hệ thống, dữ liệu phải được sao lưu đầy đủ trước khi thực hiện đánh giá để phục vụ khôi phục dữ liệu khi xảy ra sự cố.

2.2.6.2.2. Thực hiện đánh giá theo mục 2.2.19 Quản lý kiểm tra an ninh mạng trong Quy chuẩn này.

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

Chủ quản hệ thống thông tin phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.6 Quản lý tài khoản và quyền truy cập tài khoản của người dùng.

2.2.8. Quản lý lỗ hổng bảo mật

2.2.8.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.7 Quản lý lỗ hổng bảo mật.

2.2.8.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.7 Quản lý lỗ hổng bảo mật.

2.2.9. Quản lý nhật ký an ninh mạng

2.2.9.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.8 Quản lý nhật ký an ninh mạng.

2.2.9.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN

14423:2025 tại mục 5.8 Quản lý nhật ký an ninh mạng; ngoài ra, cần đáp ứng thêm các yêu cầu sau:

2.2.9.2.1. Bảo vệ tính toàn vẹn của nhật ký: Phải áp dụng công nghệ ghi một lần, đọc nhiều lần, khóa đối tượng hoặc lưu trữ bất biến để ngăn chặn việc sửa đổi nhật ký trái phép. Mọi thao tác xóa nhật ký hoặc thay đổi cấu hình lưu trữ nhật ký phải được kiểm soát chặt chẽ bằng biện pháp xác thực mạnh và cơ chế phê duyệt phù hợp.

2.2.9.2.2. Bảo vệ tính bí mật: Dữ liệu nhật ký phải được mã hóa ở trạng thái lưu trữ và trong quá trình truyền tải với mức độ mã hóa tương đương đối với thông tin nhạy cảm.

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

2.2.10.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử.

2.2.10.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.9 Bảo vệ cho trình duyệt web, dịch vụ thư điện tử.

2.2.11. Phòng chống phần mềm độc hại

2.2.11.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.10 Phòng chống phần mềm độc hại.

2.2.11.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.10 Phòng chống phần mềm độc hại.

2.2.12. Sao lưu và khôi phục dữ liệu

2.2.12.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.11 Sao lưu và khôi phục dữ liệu.

2.2.12.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.11 Sao lưu và khôi phục dữ liệu; ngoài ra, phải xây dựng, ban hành và tuân thủ quy trình, quy định quản lý vòng đời các bản sao lưu; định kỳ rà soát và cập nhật 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình, quy định, tối thiểu bao gồm:

2.2.12.2.1. Lập danh mục, thống kê toàn bộ các bản sao lưu bao gồm cả bản sao lưu, sao chép, bản sao theo thời gian, v.v.

2.2.12.2.2. Phải lưu giữ ít nhất 03 bản sao của cùng một thông tin, trong đó có 03 bản sao được bảo quản tại 02 phương tiện lưu trữ khác nhau tách biệt về mặt địa lý, ít nhất 01 bản sao phải được ghi trên vật mang tin không thể ghi đè đặt tại vị trí bên ngoài nơi lưu trữ dữ liệu chính và sử dụng kỹ thuật cách ly vật lý (air-gap).

2.2.12.2.3. Mỗi lần thực hiện sao lưu đều phải được ghi lại trong nhật ký sự kiện.

2.2.12.2.4. Quản lý khóa mã hóa phải tách biệt với hệ thống thông tin lưu trữ bản sao lưu để đảm bảo an toàn.

2.2.12.2.5. Rà quét mã độc định kỳ 01 lần/06 tháng trên toàn bộ các bản sao lưu chứa dữ liệu quan trọng, thông tin nhạy cảm và trước khi sử dụng. Ghi lại các công cụ chống phần mềm độc hại nào đã được sử dụng, được quét bằng phần mềm nào và kết quả quét.

2.2.12.2.6. Có phương án xóa, hủy bỏ dữ liệu an toàn và triệt để, đảm bảo không thể bị khôi phục, tuân thủ tiêu chuẩn NIST 800-88. Việc xóa, hủy bỏ dữ liệu phải được kiểm soát bằng MFA hoặc yêu cầu xác thực lại để bảo vệ dữ liệu nhằm ngăn chặn việc xóa

trái phép hoặc xóa nhầm. Việc xóa, hủy bỏ dữ liệu phải tuân thủ theo quy định của pháp luật về lưu trữ.

2.2.13. Quản lý hạ tầng mạng

2.2.13.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.12 Quản lý hạ tầng mạng.

2.2.13.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.12 Quản lý hạ tầng mạng; ngoài ra, cần xây dựng, ban hành và đảm bảo tuân thủ quy trình quản lý thay đổi; định kỳ rà soát tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình; quy trình phải đáp ứng tối thiểu các yêu cầu sau:

2.2.13.2.1. Thông báo cho các bên có thể bị ảnh hưởng về sự thay đổi;

2.2.13.2.2. Trước khi triển khai bất kỳ thay đổi nào trong môi trường hoạt động, phải thực hiện đánh giá các tác động liên quan đến an ninh mạng và khả năng tương thích của phần mềm đối với hệ thống, nền tảng và các thành phần khác có liên quan; đồng thời, thông báo đầy đủ cho các bên liên quan bị ảnh hưởng về nội dung và phạm vi thay đổi.

2.2.13.2.3. Khi gặp vấn đề trong hoặc sau khi thực hiện thay đổi cần đảm bảo hệ thống có thể khôi phục lại phiên bản trước khi thực hiện thay đổi. Trường hợp không thể quay về phiên bản trước phải xác định và chuẩn bị các phương án phục hồi, thay thế phù hợp.

2.2.13.2.4. Thực hiện đánh giá rủi ro trước, trong và sau khi thay đổi.

2.2.13.2.5. Cập nhật và ghi lại đầy đủ nhật ký trước, trong và sau khi thực hiện thay đổi.

2.2.14. Giám sát và phòng thủ an ninh mạng

Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.13 Giám sát và phòng thủ an ninh mạng; trong đó, giải pháp giám sát được sử dụng trong hệ thống thông tin lưu trữ tài liệu điện tử phải có khả năng kết nối, chia sẻ dữ liệu giám sát khi có yêu cầu của cơ quan có thẩm quyền theo quy định của pháp luật.

2.2.15. Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

2.2.15.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.13 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng.

2.2.15.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.14 Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng; ngoài ra, cần có cơ chế xác minh lý lịch nhân sự và đánh giá liên tục đối với cán bộ chuyên trách hoặc kiêm nhiệm quản trị hệ thống thông tin lưu trữ tài liệu điện tử.

2.2.16. Quản lý nhà cung cấp sản phẩm, dịch vụ

Chủ quản hệ thống thông tin phải xây dựng, phát triển và duy trì quy trình để đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng, lưu trữ, xử lý dữ liệu nhạy cảm hoặc chịu trách nhiệm về các quy trình, nền tảng quan trọng của hệ thống, tối thiểu bao gồm:

2.2.16.1. Định danh nhà cung cấp sản phẩm, dịch vụ

Xây dựng, ban hành và đảm bảo tuân thủ quy định về định danh đối với các nhà cung cấp dịch vụ, tối thiểu bao gồm:

2.2.16.1.1. Đáp ứng yêu cầu pháp lý theo quy định hiện hành;

2.2.16.1.2. Định danh điện tử doanh nghiệp;

2.2.16.1.3. Có đại diện pháp lý, chi nhánh hoặc văn phòng đại diện tại Việt Nam;

2.2.16.1.4. Đối với nhà cung cấp dịch vụ lưu trữ, phải đặt hạ tầng vật lý hoặc trung tâm dữ liệu tại Việt Nam.

2.2.16.2. An toàn truyền dữ liệu

2.2.16.2.1. Bảo mật đường truyền dữ liệu: Khi sử dụng mạng mở (Internet) để chuyển giao tài liệu giữa các bên, bắt buộc phải sử dụng các biện pháp kỹ thuật đảm bảo phù hợp để đáp ứng về tính xác thực, tính toàn vẹn và tính bảo mật của dữ liệu.

2.2.16.2.2. Mã hóa kết nối mạng mở rộng: Đối với các phân đoạn kết nối mở rộng giao tiếp mạng vượt ra ngoài ranh giới kiểm soát vật lý của chủ quản hệ thống thông tin (ví dụ: liên kết chuyển mạch giữa hai trung tâm dữ liệu tách biệt về mặt vật lý, lưu lượng IP truyền qua mạng WAN hoặc Internet), hệ thống bắt buộc phải kích hoạt tính năng mã hóa để ngăn chặn nguy cơ nghe lén và tấn công xen giữa.

2.2.16.2.3. Giao tiếp giữa các thành phần của hệ thống thông tin phải được mã hóa để đảm bảo tính bảo mật, cụ thể:

2.2.16.2.3.1. Đối với kết nối người dùng: Các kết nối từ máy trạm đến hệ thống thông tin lưu trữ phải sử dụng các giao thức có hỗ trợ mã hóa.

2.2.16.2.3.2. Đối với kết nối nội bộ và quản trị: Các liên kết quản trị và liên kết đồng bộ dữ liệu giữa các hệ thống thông tin lưu trữ tài liệu điện tử phải được mã hóa.

2.2.16.2.3.3. Thực hiện việc di chuyển dữ liệu giữa các vật mang tin khi cần thiết để đảm bảo tính bảo mật, toàn vẹn và tài liệu luôn có thể đọc được.

2.2.16.3. An toàn khi sử dụng lưu trữ đám mây của nhà cung cấp dịch vụ

2.2.16.3.1. Lưu trữ toàn bộ tài liệu điện tử được ủy thác trong lãnh thổ Việt Nam và tuân thủ theo đúng các điều kiện đã thỏa thuận; đồng thời, phải đáp ứng yêu cầu về an ninh mạng theo quy định pháp luật hiện hành.

2.2.16.3.2. Cung cấp cơ chế truy cập an toàn cho tất cả các tài liệu được lưu trữ.

2.2.16.3.3. Khi nhà cung cấp dịch vụ sử dụng dịch vụ của các nhà cung cấp dịch vụ ngang hàng, nhà cung cấp có trách nhiệm đảm bảo độ tin cậy và mức độ bảo đảm an ninh mạng đối với khách hàng không thấp hơn so với khi không sử dụng các dịch vụ bên thứ ba.

2.2.16.3.4. Nhà cung cấp dịch vụ thực hiện xây dựng, ban hành và đảm bảo tuân thủ quy trình hủy bỏ dữ liệu triệt để. Định kỳ rà soát quy trình tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình.

2.2.16.3.5. Nhà cung cấp dịch vụ phải có phương án, biện pháp kỹ thuật đảm bảo việc dữ liệu được hủy bỏ một cách an toàn, không thể khôi phục và được ràng buộc bằng văn bản thỏa thuận. Việc xóa, hủy bỏ dữ liệu phải tuân thủ theo quy định của pháp luật về lưu trữ.

2.2.16.3.6. Duy trì nhật ký kiểm toán cho tất cả các hoạt động liên quan đến dịch vụ.

2.2.16.3.7. Đảm bảo an toàn và tính toàn vẹn trong suốt vòng đời của tài liệu và các nhật ký sự kiện liên quan.

2.2.16.4. Quản lý truy cập nhà cung cấp dịch vụ

2.2.16.5. Đảm bảo tuân thủ truy cập từ xa của nhà cung cấp dịch vụ

2.2.16.5.1. Tuân thủ quản lý truy cập tại mục 2.2.7 Quản lý tài khoản và quyền truy cập tài khoản của người dùng.

2.2.16.5.2. Giới hạn phạm vi dữ liệu được gửi ở mức tối thiểu cần thiết.

2.2.16.5.3. Triển khai cơ chế yêu cầu xác thực trước khi cho phép kết nối.

2.2.16.5.4. Đảm bảo đặc quyền tối thiểu khi nhà cung cấp thực hiện truy cập từ xa thông qua máy chủ hoặc thiết bị liên quan.

2.2.16.5.5. Vô hiệu hóa việc cập nhật phần mềm qua liên kết truy cập từ xa của nhà cung cấp: Trong môi trường nhạy cảm, không được phép tải xuống và triển khai các thành phần và bản cập nhật phần mềm (thủ công hoặc tự động) thông qua liên kết kết nối từ xa của nhà cung cấp.

2.2.16.5.6. Thực hiện kiểm tra định kỳ nhằm loại bỏ thông tin nhạy cảm khỏi các gói tin gửi đi và xác thực tính hợp lệ của địa chỉ IP đích thuộc nhà cung cấp.

2.2.16.6. Kiểm soát tính năng hỗ trợ từ xa và gửi dữ liệu chẩn đoán

Không cho phép thiết bị tự động gửi dữ liệu hoặc mở kết nối từ xa tới nhà sản xuất trừ trường hợp được cấp có thẩm quyền phê duyệt. Mọi kết nối phát sinh bắt buộc phải được cấp quyền, sử dụng MFA và phải được giám sát.

2.2.17. Phát triển ứng dụng an toàn

Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.16 Phát triển ứng dụng an toàn; yêu cầu này không bắt buộc đối với đơn vị sử dụng phần mềm thuê khoán, tuy nhiên, đơn vị phát triển phần mềm bắt buộc phải tuân thủ.

2.2.18. Quản trị ứng phó sự cố an ninh mạng

2.2.18.1. Chủ quản hệ thống thông tin cấp độ 1, 2 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 4.15 Quản trị ứng phó sự cố an ninh mạng.

2.2.18.2. Chủ quản hệ thống thông tin cấp độ 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.17 Quản trị ứng phó sự cố an ninh mạng; ngoài ra, cần xây dựng, ban hành và tuân thủ quy định về ứng phó sự cố an ninh mạng, tối thiểu bao gồm: phạm vi của sự cố an ninh mạng được phát hiện; phương án ứng phó sự cố trong mọi trường hợp; quy trình báo cáo sự cố an ninh mạng; thiết lập kênh liên lạc riêng biệt, an toàn phục vụ các vấn đề liên quan đến sự cố an ninh mạng; cơ chế phối hợp với các bên liên quan và cơ quan chức năng trong điều phối, ứng phó sự cố; thực hiện chia sẻ thông tin, báo cáo sự cố trong vòng 24 giờ kể từ khi phát hiện cho cơ quan có thẩm quyền theo quy định của pháp luật.

2.2.19. Quản lý kiểm tra an ninh mạng

2.2.19.1. Chủ quản hệ thống thông tin 3, 4, 5 phải tuân thủ yêu cầu trong TCVN 14423:2025 tại mục 5.18 Quản lý kiểm tra an ninh mạng.

2.2.19.2. Việc kiểm tra, đánh giá an ninh mạng và đánh giá rủi ro an ninh mạng độc lập đối với hệ thống thông tin cấp độ 3 trở lên phải do đơn vị sự nghiệp công lập có chức năng, nhiệm vụ phù hợp hoặc tổ chức chuyên môn được cấp phép bởi cấp có thẩm quyền.

2.2.20. Bảo trì hệ thống thông tin

Chủ quản hệ thống thông tin phải xây dựng, ban hành và tuân thủ quy định về bảo trì hệ thống thông tin lưu trữ tài liệu điện tử, tối thiểu gồm các yêu cầu sau:

2.2.20.1. Mọi hoạt động bảo trì, dù là phòng ngừa hay khắc phục đều phải được ghi lại trong nhật ký hệ thống.

2.2.20.2. Mọi thử nghiệm phải được thực hiện bằng vật mang tin chuyên dụng cho nhiệm vụ này. Nếu vật mang tin không thể tháo rời, các thử nghiệm không được làm thay đổi hoặc phá hủy thông tin đã ghi.

2.2.20.3. Bảo trì phòng ngừa phải được thực hiện thường xuyên theo khuyến nghị của nhà sản xuất để đảm bảo hệ thống hoạt động ổn định.

2.2.21. Đảm bảo phục hồi

2.2.21.1. Chủ quản hệ thống thông tin phải xây dựng, ban hành và tuân thủ quy trình khôi phục sau thảm họa (BCP/DR).

2.2.21.2. Hệ thống thông tin từ cấp độ 03 trở lên phải có quy trình khôi phục sau thảm họa đáp ứng tối thiểu các yêu cầu sau:

2.2.21.2.1. Khôi phục mà không làm mất mát dữ liệu, siêu dữ liệu, nhật ký hoặc bất kỳ thành phần nào khác.

2.2.21.2.2. Tự động ghi lại nhật ký của mọi quy trình khôi phục đã thực hiện và định kỳ rà soát, đánh giá các bản khôi phục.

2.2.22. Dấu thời gian

Việc sử dụng dấu thời gian phải tuân thủ các quy định pháp luật hiện hành và được cung cấp bởi tổ chức có thẩm quyền, tối thiểu bao gồm:

2.2.22.1. Nguồn thời gian tham chiếu: Hệ thống phải sử dụng chuẩn UTC.

2.2.22.2. Độ phân giải: Độ phân giải của thời gian phải đủ nhỏ để đảm bảo mỗi sự kiện trong hệ thống được gán một dấu thời gian là duy nhất và không trùng lặp.

2.2.22.3. Quy trình đồng bộ: Nguồn thời gian, phương pháp cập nhật và quy trình đồng bộ hóa thời gian toàn hệ thống phải được mô tả chi tiết trong hồ sơ thiết kế kỹ thuật.

3. PHƯƠNG PHÁP ĐÁNH GIÁ

3.1. Nhóm đánh giá 2.2.1

3.1.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin thiết lập và thực hiện quy trình quản lý rủi ro an ninh mạng tuân thủ TCVN 14423:2025 tương ứng với cấp độ của hệ thống thông tin; xác minh việc xác định, đánh giá, xử lý, giám sát và truyền thông rủi ro được thực hiện đầy đủ, cô xét đến các yếu tố đặc thù của vật mang tin lưu trữ và đảm bảo sự cân bằng giữa chi phí triển khai với hiệu quả bảo mật đạt được.

3.1.2. Phương pháp đánh giá

Người thực hiện đánh giá kiểm tra hồ sơ quản lý rủi ro, quy trình quản lý rủi ro được ban hành và các biên bản, báo cáo liên quan để xác minh các nội dung sau:

3.1.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.1.2.1.1. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định hoặc quy trình

quản lý rủi ro an ninh mạng, trong đó:

3.1.2.1.1.1. Nội dung quy trình bắt buộc phải bao gồm tối thiểu 05 bước: (1) Xác định, (2) Đánh giá, (3) Xử lý, (4) Giám sát và (5) Truyền thông rủi ro.

3.1.2.1.1.2. Có bằng chứng về việc rà soát, cập nhật quy trình này định kỳ tối thiểu 01 lần/năm.

3.1.2.1.1.3. Có hồ sơ hoặc danh sách rủi ro hiện hành, bao gồm đầy đủ các nhóm rủi ro: tài sản, lỗ hổng bảo mật, hạ tầng kỹ thuật và rủi ro từ bên thứ ba, nhà cung cấp.

3.1.2.1.1.4. Hồ sơ phải thể hiện việc đánh giá mức độ ảnh hưởng và khả năng xảy ra cho từng rủi ro cụ thể.

3.1.2.1.1.5. Có lịch sử cập nhật hồ sơ rủi ro định kỳ tối thiểu 01 lần/năm hoặc được cập nhật ngay khi có thay đổi lớn về hệ thống hoặc xảy ra sự kiện an ninh mạng.

3.1.2.1.2. Đối với mỗi rủi ro đã xác định, có quyết định xử lý rõ ràng (chấp nhận, giảm thiểu, chuyển giao, hoặc né tránh).

3.1.2.1.3. Có kế hoạch hoặc phương án xử lý cụ thể đối với các rủi ro vượt quá mức chấp nhận rủi ro; mức chấp nhận rủi ro phải được ban hành và cập nhật định kỳ, tối thiểu 01 lần/năm.

3.1.2.1.4. Có phương án ứng phó hoặc kiểm soát bổ sung đối với các rủi ro còn lại sau khi đã áp dụng biện pháp xử lý.

3.1.2.1.5. Có văn bản đánh giá hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro được; việc đánh giá được thực hiện định kỳ tối thiểu 01 lần/06 tháng.

3.1.2.1.6. Hồ sơ rủi ro phải thể hiện được tính cập nhật, tối thiểu bao gồm ngày cập nhật và những thay đổi liên quan đến rủi ro (thay đổi về khả năng xảy ra, mức độ ảnh hưởng, mức độ rủi ro, tài sản bị ảnh hưởng, biện pháp kiểm soát đã áp dụng).

3.1.2.1.7. Thông báo các thay đổi quan trọng liên quan đến rủi ro cho các bên liên quan.

3.1.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.1.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.1.2.1.

3.1.2.2.2. Về phạm vi đánh giá chuyên sâu: kết quả phân tích rủi ro phải bao gồm các yếu tố đe dọa đặc thù liên quan đến vật mang tin lưu trữ như rủi ro vật lý, lỗi phần cứng, tuổi thọ thiết bị lưu trữ.

3.1.2.2.3. Về phân tích chi phí lợi ích: trong báo cáo hoặc biên bản lựa chọn biện pháp xử lý rủi ro, phải có nội dung phân tích, xem xét giữa chi phí triển khai và mức độ an toàn đạt được để thể hiện tính hiệu quả của phương án được chọn.

3.1.3. Kết luận

3.1.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.1.2.

3.1.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.2. Nhóm đánh giá 2.2.2

3.2.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin có quy định, quy trình kiểm soát ra vào chặt chẽ từ cấp quyền, giám sát, ghi nhật ký đến thu hồi; quy định, quy trình phải được rà soát

định kỳ và triển khai các biện pháp vật lý tương ứng để ngăn chặn truy cập trái phép vào các tài sản công nghệ thông tin quan trọng.

3.2.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy định, quy trình được ban hành và nhật ký hoạt động để xác minh các nội dung sau:

3.2.2.1. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định, quy trình kiểm soát ra vào; quy định, quy trình được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy định, quy trình, trong đó:

3.2.2.1.1. Có quy trình cấp quyền truy cập, bao gồm đầy đủ 03 bước: (1) Tạo yêu cầu, cấp quyền truy cập, (2) Ghi nhật ký hoạt động, hành vi và (3) Thu hồi quyền truy cập.

3.2.2.1.2. Có nhật ký (sổ ghi chép hoặc nhật ký hệ thống) ghi lại đầy đủ thông tin hoạt động ra, vào khu vực hạn chế, tối thiểu bao gồm: họ và tên, số giấy tờ tuỳ thân hợp pháp, thời gian vào và ra, mục đích.

3.2.2.1.3. Có bằng chứng (biên bản bàn giao, phiếu yêu cầu kỹ thuật) chứng minh việc xóa bỏ, thu hồi quyền truy cập vật lý (thẻ từ, vân tay, chìa khóa) được thực hiện ngay lập tức khi nhân sự hết nhiệm vụ hoặc chấm dứt thỏa thuận lao động.

3.2.2.2. Các khu vực chứa tài sản công nghệ thông tin quan trọng đã được trang bị các biện pháp ngăn chặn truy cập trái phép (tối thiểu gồm: khóa cửa từ hoặc vân tay, camera giám sát hoặc nhân viên bảo vệ). Khu vực chứa tài sản công nghệ thông tin quan trọng phải bao gồm: Khu vực đặt hệ thống máy chủ và thiết bị mạng, khu vực lưu trữ các tài sản công nghệ thông tin, hệ thống thông tin lưu trữ nhật ký, khu vực lưu trữ các bản sao lưu dự phòng.

3.2.2.3. Đối với các khu vực làm việc chung có yêu cầu truy cập liên tục, hệ thống thông tin lưu trữ dữ liệu hoặc các thiết bị vận hành quan trọng đã được thiết kế, bố trí tách biệt về mặt vật lý hoặc có biện pháp bảo vệ riêng để ngăn chặn việc tiếp cận trực tiếp từ môi trường mở.

3.2.3. Kết luận

3.2.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.2.2.

3.2.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.3. Nhóm đánh giá 2.2.3

3.3.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin kiểm soát toàn diện vòng đời của tài sản phần cứng: từ việc lập danh sách chi tiết, kiểm tra an ninh đầu vào, kiểm soát thiết bị di động, phát hiện thiết bị lạ định kỳ hàng tháng, đến việc xử lý an toàn dữ liệu khi thanh lý hoặc tiêu hủy thiết bị.

3.3.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên danh mục tài sản và quy trình quản lý tài sản để xác minh các nội dung sau:

3.3.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.3.2.1.1. Chủ quản hệ thống thông tin đã thiết lập và duy trì "Danh sách tài sản phần

cứng" có khả năng lưu trữ, xử lý dữ liệu, tối thiểu bao gồm: thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, thiết bị OT/IoT, máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây, trong đó:

3.3.2.1.1.1. Thông tin cho mỗi tài sản trong danh sách tài sản phần cứng tối thiểu bao gồm các trường: (1) Tên tài sản, (2) Địa chỉ IP (đối với thiết bị đặt địa chỉ IP tĩnh), (3) Địa chỉ phần cứng MAC hoặc số sê-ri, (4) Thời gian ngừng hỗ trợ kỹ thuật của hãng, (5) Vị trí lắp đặt địa lý, (6) Vị trí lắp đặt trong hệ thống mạng, (7) Mục đích sử dụng và (8) Tình trạng sử dụng hiện tại.

3.3.2.1.1.2. Mỗi tài sản trong danh sách phải được gán tên cá nhân hoặc bộ phận chịu trách nhiệm quản lý, sử dụng.

3.3.2.1.2. Có tài liệu, chứng cứ chứng minh việc tất cả tài sản phần cứng đáp ứng yêu cầu về an ninh của cơ quan, tổ chức có thẩm quyền cấp theo quy định của pháp luật trước khi đưa vào sử dụng.

3.3.2.1.3. Có danh sách đăng ký các thiết bị di động được phép kết nối vào hệ thống thông tin.

3.3.2.1.4. Có quy định về trách nhiệm của cá nhân khi sử dụng thiết bị di động cho mục đích công việc.

3.3.2.1.5. Chủ quản hệ thống thông tin đã ban hành 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 hệ thống thông tin.

3.3.2.1.6. Có bằng chứng (nhật ký, báo cáo kết quả rà quét) về việc thực hiện rà quét định kỳ, tối thiểu 01 lần/tháng đối với hệ thống thông tin để phát hiện các tài sản phần cứng không có trong danh sách quản lý.

3.3.2.1.7. Chủ quản hệ thống thông tin đã thực hiện các biện pháp (loại bỏ, từ chối kết nối hoặc cách ly) đối với tài sản phần cứng không có trong danh sách quản lý được phát hiện.

3.3.2.1.8. Chủ quản hệ thống thông tin đã ban hành quy trình thanh lý, tiêu hủy tài sản CNTT, trong đó các thiết bị lưu trữ đã thanh lý, tiêu hủy phải có văn bản xác nhận không thể khôi phục dữ liệu nhạy cảm trên thiết bị lưu trữ trước khi tiến hành thanh lý, tiêu hủy.

3.3.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.3.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.3.2.1.

3.3.2.2.2. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin định kỳ tối thiểu 01 lần/tháng; có bằng chứng chứng minh việc thực hiện cập nhật danh sách tài sản dựa trên kết quả rà quét.

3.3.2.2.3. Hệ thống phải bật tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc sử dụng công cụ quản lý địa chỉ mạng IP.

3.3.2.2.4. Có bằng chứng về việc thực hiện rà soát nhật ký DHCP để cập nhật danh sách tài sản công nghệ thông tin định kỳ với tần suất tối thiểu 01 lần/tháng.

3.3.3. Kết luận

3.3.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.3.2.

3.3.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.4. Nhóm đánh giá 2.2.4

3.4.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin duy trì một danh sách tài sản phần mềm, chính xác với đầy đủ thông tin quản lý; thực hiện rà soát định kỳ để phát hiện phần mềm trái phép và có cơ chế xử lý phù hợp.

3.4.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên danh sách tài sản phần mềm, các báo cáo rà quét, danh sách ngoại lệ và nhật ký xử lý để xác minh các nội dung sau:

3.4.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.4.2.1.1. Chủ quản hệ thống thông tin phải thiết lập và duy trì danh sách tài sản phần mềm đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin, trong đó:

3.4.2.1.1.1. Thông tin cho mỗi phần mềm trong danh sách tài sản phần mềm tối thiểu bao gồm các trường: (1) Tên tài sản, (2) Mục đích sử dụng, (3) Thời gian ngừng hỗ trợ kỹ thuật, (4) Phạm vi sử dụng, (5) Chủ thể quản lý, (6) Thông tin bản quyền, (7) Phiên bản và (8) Hệ thống thông tin thành phần mà phần mềm được cái đặt.

3.4.2.1.1.2. Mỗi phần mềm phải được gán tên cá nhân hoặc bộ phận chịu trách nhiệm quản lý, sử dụng.

3.4.2.1.2. Chủ quản hệ thống thông tin đã ban hành quy trình phát hiện phần mềm trái phép; có bằng chứng về việc thực hiện rà soát theo quy trình trên toàn hệ thống với tần suất tối thiểu 01 lần/quý.

3.4.2.1.3. Có danh sách các phần mềm ngoại lệ (không thuộc danh sách tài sản phần mềm) được phê duyệt riêng. Với mỗi phần mềm trong danh sách ngoại lệ, phải có tài liệu mô tả chi tiết các biện pháp kiểm soát kỹ thuật được áp dụng để giảm thiểu rủi ro an ninh mạng.

3.4.2.1.4. Có kế hoạch hoặc phương án xử lý cụ thể (xóa, gỡ bỏ) khi phát hiện phần mềm trái phép.

3.4.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.4.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.4.2.1.

3.4.2.2.2. Chủ quản hệ thống thông tin đã thiết lập "Danh sách phần mềm được phép sử dụng" trong hệ thống thông tin; danh sách này phải bao gồm cả các phần mềm được cung cấp bởi nhà cung cấp dịch vụ, các môi trường thực thi cần cài đặt cho ứng dụng; danh sách phần mềm được phép sử dụng được định kỳ đánh giá và cập nhật tối thiểu 01 lần/06 tháng hoặc khi xảy ra các thay đổi trong hệ thống thông tin ảnh hưởng đến danh sách.

3.4.2.2.3. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép, trong đó: 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.

3.4.2.2.4. Có báo cáo kết quả 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 đảm bảo tất cả tài sản pbần mềm đang trong thời gian hỗ trợ của nhà cung cấp, tối thiểu 01 lần/06 tháng.

3.4.3. Kết luận

3.4.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.4.2.

3.4.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.5. Nhóm đánh giá 2.2.5

3.5.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã ban hành quy định quản lý tài sản thông tin, quy định việc phân loại, kiểm soát truy cập, duy trì danh sách tài sản thông tin và áp dụng các biện pháp kỹ thuật như mã hóa dữ liệu quan trọng và quản lý vòng đời mã khóa được sử dụng để mã hóa dữ liệu.

3.5.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy định quản lý tài sản thông tin, danh sách tài sản thông tin, phân loại mức độ nhạy cảm của tài sản thông tin và kiểm tra cấu hình hệ thống để xác minh các nội dung sau:

3.5.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định quản lý tài sản thông tin, trong đó:

3.5.2.1.1. Nội dung quy định phải bao gồm các yêu cầu về: xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, quy trình xử lý, thời gian lưu trữ và quy định việc tiêu hủy, xóa bỏ đối với tài sản thông tin.

3.5.2.1.2. Có quy định về phân loại mức độ nhạy cảm, tối thiểu gồm 04 mức (hoặc tương đương): Mức 1 (Công khai), Mức 2 (Nội bộ), Mức 3 (Hạn chế truy cập), Mức 4 (Bí mật).

3.5.2.1.3. Có danh sách tài sản thông tin hiện hành, tối thiểu bao gồm các trường thông tin được quy định tại quy định quản lý tài sản thông tin; danh sách này phải được cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến danh sách.

3.5.2.1.4. Quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu phải có bước phê duyệt của cấp có thẩm quyền.

3.5.2.1.5. Có danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.

3.5.2.1.6. Có bằng chứng (văn bản hoặc nhật ký hệ thống) chứng minh việc rà soát cấp độ phân quyền dữ liệu được thực hiện định kỳ tối thiểu 01 lần/tháng.

3.5.2.1.7. Các quy trình, quy định về việc quản lý tài sản thông tin đã được đánh giá và cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi về cơ cấu tổ chức ảnh hưởng đến quy trình, quy định.

3.5.2.1.8. Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức trong nước, quốc tế công bố điểm yếu, lỗ hổng bảo mật) để mã hóa dữ liệu quan trọng được lưu trữ trên các tài sản phần cứng, phần mềm.

3.5.2.1.9. Có quy trình quản lý vòng đời mã khóa tối thiểu bao gồm các bước: tạo khóa, lưu trữ an toàn, xoay vòng khóa và hủy khóa.

3.5.2.1.10. Hệ thống có tính năng tự động tạo giá trị băm duy nhất cho mỗi tài liệu ngay khi tiếp nhận. Giá trị băm phải được lưu trữ trong cơ sở dữ liệu và có cơ chế bảo vệ kỹ

thuật để ngăn chặn sửa đổi trái phép.

3.5.2.1.11. Hệ thống đã cấu hình tự động kiểm tra định kỳ để phát hiện thay đổi dữ liệu hcặc can thiệp trái phép.

3.5.2.1.12. Hệ thống có cơ chế tự động phục hồi tài liệu về trạng thái toàn vẹn ban đầu khi phát hiện sai lệch.

3.5.2.1.13. Thuật toán băm sử dụng phải bảo đảm an toàn theo quy định.

3.5.2.1.14. Cơ sở dữ liệu băm đã được thiết lập cơ chế bảo vệ "Chỉ đọc" hoặc WORM đối với tài khoản quản trị thông thường.

3.5.2.1.15. Tần suất kiểm tra toàn vẹn được cấu hình phù hợp với khối lượng và mức độ quan trọng của dữ liệu.

3.5.2.1.16. Đối với cáo tài liệu điện tử có yêu cầu bảo mật, hạn chế truy cập khi lưu trữ ngoại tuyến hoặc truyền đưa trên môi trường mạng, hệ thống phải có chức năng thiết lập mật khẩu bảo vệ trực tiếp trên tệp tin hoặc mã hóa nội dung tài liệu.

3.5.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.5.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.5.2.1.

3.5.2.2.2. Hệ thống sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức trong nước, quốc tế công bố điểm yếu, lỗ hổng bảo mật) để mã hóa dữ liệu quan trọng trong quá trình truyền gửi để đảm bảo tính toàn vẹn của dữ liệu.

3.5.2.2.3. Có tài liệu kỹ thuật mô tả chi tiết các luồng dữ liệu quan trọng.

3.5.2.2.4. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định quản lý phiên bản tài liệu;

3.5.2.2.5. Hoạt động đánh giá và cập nhật tài liệu được thực hiện định kỳ tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến tài liệu.

3.5.2.2.6. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định về việc xử lý dữ liệu nhạy cảm.

3.5.2.2.7. Chủ quản hệ thống thông tin đã thực hiện tách biệt môi trường lưu trữ giữa dữ liệu nhạy cảm mức độ 04, mức độ 03 và dữ liệu nhạy cảm mức độ 01, mức độ 02.

3.5.2.2.8. Chủ quản hệ thống thông tin triển khai giải pháp chống thất thoát dữ liệu đối với dữ liệu có độ nhạy cảm mức 03 trở lên được lưu trữ, xử lý trong hệ thống thông tin

3.5.2.2.9. Hệ thống đã ghi nhật ký hành vi chi tiết đối với dữ liệu có mức độ nhạy cảm:

Mức 03: Ghi nhận hành vi chỉnh sửa, hủy bỏ.

Mức 04: Ghi nhận hành vi xem, chỉnh sửa, hủy bỏ.

3.5.2.2.10. Có bằng chứng rà soát nhật ký để phát hiện hành vi truy cập trái phép với tần suất tối thiểu 01 lần/tháng.

3.5.2.2.11. Việc sử dụng chữ ký số trong trao đổi thông tin, dữ liệu quan trọng đã đáp ứng quy định tại mục 8.2.3.5 của TCVN 11930:2017, cụ thể:

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

3.5.2.2.11.2. Chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép;

3.5.2.2.11.3. Có phương án bảo đảm an toàn trong việc quản lý và sử dụng chữ ký số.

3.5.3. Kết luận

3.5.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.5.2.

3.5.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.6. Nhóm đánh giá 2.2.6

3.6.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định, quy trình về cấu hình an toàn tài sản phần cứng, phần mềm.

3.6.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên hồ sơ thiết kế, tài liệu cấu hình, thỏa thuận thuê khoán và kiểm tra cấu hình thực tế trên thiết bị để xác minh các nội dung sau:

3.6.2.1. Đối với hệ thống thông tin cấp đô 1, 2:

3.6.2.1.1. Có hồ sơ thiết kế và tài liệu phát triển phần mềm nội bộ được phê duyệt.

3.6.2.1.2. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định, quy trình cấu hình an toàn cho các tài sản phần cứng, phần mềm thuộc hệ thống thông tin.

3.6.2.1.3. Chủ quản hệ thống thông tin đã ban hành và tuân thủ các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật cho các tài sản phần cứng, phần mềm.

3.6.2.1.4. Có bằng chứng chứng minh quy định, quy trình cấu hình an toàn, các tài liệu cấu hình được rà soát và cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy định, quy trình, tài liệu.

3.6.2.1.5. Hệ thống đã được cấu hình sử dụng các giao thức mạng an toàn và vô hiệu hóa các giao thức không an toàn.

3.6.2.1.6. Tường lửa đã được thiết lập cho máy chủ và máy trạm.

3.6.2.1.7. Có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng.

3.6.2.1.8. Hệ thống đã cấu hình tự động khóa phiên làm việc sau một khoảng thời gian không hoạt động, cụ thể:

3.6.2.1.8.1. Đối với máy tính người dùng: không quá 15 phút.

3.6.2.1.8.2. Đối với các phiên quản trị phần mềm, máy chủ, thiết bị mạng, thiết bị IoT: không quá 05 phút.

3.6.2.1.8.3. Đối với thiết bị di động: không quá 02 phút.

3.6.2.1.8.4. Đối với phần mềm nghiệp vụ xử lý và lưu trữ dữ liệu quan trọng: không quá 15 phút.

3.6.2.1.9. Các tài sản phần cứng, phần mềm đã được cấu hình tự động khóa sau một số lần đăng nhập hoặc mở khóa thất bại, cụ thể:

3.6.2.1.9.1. Đối với máy tính xách tay và điện thoại: tối đa 10 lần nhập sai liên tiếp.

3.6.2.1.9.2. Đối với phần mềm nghiệp vụ xử lý và lưu trữ dữ liệu quan trọng: tối đa 05 lần nhập sai liên tiếp.

3.6.2.1.9.3. Thời gian tự động mở khóa tài sản phần cứng, phần mềm sau khi bị khóa được cấu hình tối thiểu 12 giờ và tối đa 30 ngày (trừ trường hợp mở khóa bởi quản trị viên).

3.6.2.1.10. Có biên bản, hợp đồng và cam kết bảo mật các nội dung liên quan đến phát triển phần mềm thuê khoán.

3.6.2.1.11. Trong hợp đồng thuê khoán phải yêu cầu đơn vị phát triển phần mềm cung cấp mã nguồn phần mềm cho bên thuê khoán.

3.6.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.6.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.6.2.1.

3.6.2.2.2. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định gỡ bỏ hoặc vô hiệu hóa các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm; kết quả kiểm tra thực tế phải thể hiện các dịch vụ không an toàn hoặc không sử dụng đã được gỡ bỏ hoặc vô hiệu hóa hoàn toàn trên hệ thống.

3.6.2.2.3. Chủ quản hệ thống thông tin đã thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng.

3.6.2.2.4. Chủ quản hệ thống thông tin đã triển khai giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.

3.6.2.2.5. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định tách biệt các không gian làm việc riêng biệt trên thiết bị di động cấp cho người dùng. Đã áp dụng 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.

3.6.3. Kết luận

3.6.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.6.2.

3.6.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.7. Nhóm đánh giá 2.2.7

3.7.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin kiểm soát chặt chẽ danh tính và quyền truy cập thông qua việc duy trì danh sách tài khoản chính xác, áp dụng chính sách mật khẩu mạnh, thực hiện nguyên tắc cấp quyền tối thiểu và tuân thủ quy trình vòng đời tài khoản.

3.7.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên danh sách tài khoản, chính sách mật khẩu và nhật ký hệ thống để xác minh các nội dung sau:

3.7.2.1. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy trình phân quyền và quản lý quyền truy cập của tài khoản người dùng, bao gồm các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm.

3.7.2.2. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng.

3.7.2.3. Quyền truy cập của tài khoản người dùng phải nhất quán dựa trên vai trò và yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp.

3.7.2.4. Có nhật ký giám sát tài khoản người dùng; bảo đảm ghi nhận đầy đủ các hành vi đăng nhập, đăng xuất, đăng nhập không thành công, khóa và mở khóa tài khoản, tạo, sửa, xóa tài khoản, thay đổi quyền truy cập và các hành vi quản trị liên quan.

3.7.2.5. Chủ quản hệ thống thông tin đã thiết lập và duy trì danh sách tài khoản trên các tài sản phần cứng và phần mềm trong hệ thống thông tin, trong đó:

3.7.2.5.1. Danh sách tài khoản phải bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật và các trường thông tin: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản và ngày vô hiệu hóa tài khoản (trong trường hợp tài khoản bị vô hiệu hóa).

3.7.2.5.2. Có bằng chứng chứng minh đã thực hiện rà soát danh sách tài khoản định kỳ (tối thiểu 01 lần/quý) để phát hiện những tài khoản lạ tồn tại trong hệ thống; kết quả rà soát phải chỉ ra tất cả thay đổi về danh sách tài khoản và đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.

3.7.2.6. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định sử dụng mật khẩu an toàn, đáp ứng các yêu cầu:

3.7.2.6.1. Phải sử dụng mật khẩu duy nhất cho mỗi tài sản phần cứng, phần mềm hoặc sử dụng giải pháp xác thực và quản lý tập trung.

3.7.2.6.2. Các tái sản phần cứng, phần mềm đã được cấu hình bắt buộc thay đổi mật khẩu ngay trong lần đăng nhập đầu tiên.

3.7.2.6.3. Đối với hệ thống sử dụng MFA: mật khẩu phải có độ dài tối thiểu 08 ký tự.

3.7.2.6.4. Đối với hệ thống không sử dụng MFA: mật khẩu phải có độ dài tối thiểu 14 ký tự, bao gồm kỹ tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số.

3.7.2.6.5. Đối với tài khoản quản trị: phải thay đổi mật khẩu định kỳ tối thiểu 01 lần/02 tháng và mật khẩu mới không được trùng với 10 mật khẩu đã sử dụng gần nhất.

3.7.2.7. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định quản lý tài khoản, đáp ứng các yêu cầu:

3.7.2.7.1. Quản lý tài khoản tập trung.

3.7.2.7.2. Thay đổi tên đăng nhập mặc định, đổi mật khẩu mặc định hoặc vô hiệu hóa toàn bộ các tài khoản mặc định trên phần mềm, thiết bị (tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ); trường hợp không thể thay đổi hoặc vô hiệu hóa tài khoản mặc định, phải có văn bản phê duyệt của chủ quản hệ thống thông tin và quy định trách nhiệm quản lý, sử dụng tài khoản cho cá nhân, đơn vị cụ thể.

3.7.2.7.3. Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ; không dùng một loại tài khoản cho mọi mục đích mà phải phân loại để quản lý riêng.

3.7.2.7.4. Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung phải có văn bản phê duyệt của chủ quản hệ thống và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng.

3.7.2.7.5. Quy định về việc quản lý thiết bị lưu khóa bí mật và khóa bí mật.

3.7.2.7.6. Cấu hình tự động vô hiệu hóa hoặc xóa các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý tài khoản; trường hợp không thể cấu hình tự động, phải thông báo cho quản trị viên để thực hiện vô hiệu hóa hoặc xóa tài khoản.

3.7.2.7.7. Định kỳ rà soát và cập nhật quy định quản lý tài khoản tối thiểu 01 lần/năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến quy định này.

3.7.2.8. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định về quản lý truy cập đáp ứng các yêu cầu:

3.7.2.8.1. Việc cấp quyền phải tuân thủ nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản.

3.7.2.8.2. Có tài liệu mô tả các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong việc quản lý, vận hành hệ thống thông tin.

3.7.2.8.3. MFA phải được kích hoạt cho các trường hợp: truy cập của người dùng từ mạng bên ngoài; từ đối tác, bên thứ ba; từ Internet và trường hợp truy cập vào các tài khoản có quyền quản trị hệ thống.

3.7.2.8.4. Định kỳ rà soát và cập nhật quy định về quản lý truy cập và các tài liệu trong quy định này tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy định, tài liệu.

3.7.2.9. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy trình quản lý quyền truy cập, bao gồm việc cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT; việc cấp mới, thay đổi và thu hồi quyền truy cập phải được ghi vào nhật ký hệ thống và trùng khớp với những thay đổi về nhân sự (nhân sự mới, nghỉ việc). Quy trình này được rà soát, đánh giá lại tối thiểu 01 lần/năm.

3.7.3. Kết luận

3.7.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.7.2.

3.7.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.8. Nhóm đánh giá 2.2.8

3.8.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin có khả năng chủ động phát hiện và xử lý các lỗ hổng bảo mật theo mức độ ưu tiên; duy trì hệ thống quản lý bản vá tập trung, đảm bảo bản vá được kiểm thử an toàn trước khi triển khai và được cập nhật định kỳ cho thiết bị người dùng.

3.8.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy trình quản lý lỗ hổng, quản lý bản vá, báo cáo rà quét, nhật ký cập nhật và kiểm tra cấu hình hệ thống để xác minh các nội dung sau:

3.8.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.8.2.1.1. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy trình quản lý lỗ hổng bảo mật cho các tài sản CNTT thuộc hệ thống thông tin, bao gồm tối thiểu 04 bước: (1) Phát hiện lỗ hổng bảo mật, (2) Đánh giá mức độ nghiêm trọng của lỗ hổng bảo mật, (3) Chia sẻ thông tin lỗ hổng bảo mật và (4) Triển khai các biện pháp khắc phục; quy trình được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi trong cơ cấu tổ chức

ảnh hưởng đến quy trình này, trong đó:

3.8.2.1.1.1. Triển khai giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng, phần mềm của hệ thống thông tin.

3.8.2.1.1.2. Có hồ sơ theo dõi xử lý lỗ hổng, trong đó thể hiện rõ: Các lỗ hổng được phát hiện và phân loại theo mức độ nghiêm trọng và có kế hoạch khắc phục theo thứ tự ưu tiên.

3.8.2.1.1.3. Có bằng chứng đã thực hiện đánh giá lại hệ thống thông tin sau khi xử lý lỗ hổng và thể hiện việc lỗ hổng đã được khắc phục hoàn toàn theo thời gian trong kế hoạch.

3.8.2.1.1.4. Thiết lập cơ chế cụ thể để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ các bên liên quan hoặc nguồn bên ngoài như: cơ quan chức năng, hãng sản xuất, các tổ chức, hiệp hội về an ninh mạng...

3.8.2.1.2. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy trình quản lý bản vá, tối thiểu bao gồm:

3.8.2.1.2.1. Triển khai máy chủ quản lý bản vá tập trung và đẩy bản vá cho toàn bộ tài sản phần cứng và phần mềm thuộc hệ thống thông tin.

3.8.2.1.2.2. Có cơ chế giám sát để phát hiện các lỗ hổng mới xuất hiện và cập nhật bản vá.

3.8.2.1.2.3. Đối với hệ thống thông tin lưu trữ hoặc xử lý dữ liệu quan trọng, có bằng chứng chứng minh đã thực hiện đánh giá tác động, kiểm thử trong môi trường thử nghiệm và có phương án phục hồi trước khi triển khai lên hệ thống.

3.8.2.1.2.4. Có bằng chứng chứng minh việc kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn bộ máy tính, thiết bị di động cấp cho người dùng được thực hiện tối thiểu 01 lần/tháng.

3.8.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.8.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.8.2.1;

3.8.2.2.2. Có bằng chứng chứng minh việc thực hiện rà quét lỗ hổng bảo mật định kỳ tuân thủ tần suất: thực hiện rà soát tổng thể hệ thống tối thiểu 01 lần/quý và rà soát đối với các tài sản quan trọng tối thiểu 01 lần/tháng.

3.8.3. Kết luận

3.8.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.8.2.

3.8.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.9. Nhóm đánh giá 2.2.9

3.9.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã thiết lập và thực thi quy định quản lý nhật ký toàn diện từ việc đồng bộ thời gian, ghi nhận đầy đủ các trường thông tin bắt buộc trên các tài sản công nghệ thông tin quan trọng đến việc lưu trữ lâu dài và thực hiện rà soát định kỳ hàng tuần.

3.9.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy định quản lý nhật ký đã ban hành, cấu hình hệ thống và mẫu nhật ký thực tế để xác minh các nội dung sau:

3.9.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định quản lý nhật ký an ninh mạng; quy trình được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy trình, tối thiểu bao gồm:

3.9.2.1.1. Có quy định về cách thức ghi nhật ký.

3.9.2.1.2. Có quy định về việc thu thập, kiểm tra, lưu trữ nhật ký.

3.9.2.1.3. Có quy định về các loại nhật ký được thu thập và 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.

3.9.2.1.4. Nhật ký truy cập hệ thống tối thiểu bao gồm các thông tin: địa chỉ nguồn, địa chỉ đích, tài khoản đích và thời điểm xảy ra sự kiện.

3.9.2.1.5. Nhật ký tiến trình hoạt động tối thiểu bao gồm các thông tin: thông tin thiết bị, thông tin tiến trình, tài khoản thực thi và thời điểm xảy ra sự kiện.

3.9.2.1.6. Nhật ký cảnh báo tối thiểu bao gồm: tên cảnh báo, thiết bị phát sinh cảnh báo, mức độ nghiêm trọng, địa chỉ nguồn, loại cảnh báo và thời điểm xảy ra sự kiện.

3.9.2.1.7. Việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT lưu trữ hoặc xử lý dữ liệu nhạy cảm.

3.9.2.1.8. Các thiết bị mạng, máy chủ và thiết bị đầu cuối sinh nhật ký phải được cấu hình đồng bộ thời gian với một máy chủ thời gian.

3.9.2.1.9. Thời gian lưu trữ nhật ký đã được thiết lập tối thiểu 12 tháng.

3.9.2.1.10. Có công cụ hoặc tính năng tự động giám sát và cảnh báo cho quản trị viên khi dung lượng lưu trữ nhật ký đạt ngưỡng sắp đầy để ngăn chặn nguy cơ mất dữ liệu.

3.9.2.1.11. Có bằng chứng chứng minh việc thực hiện rà soát nhật ký an ninh mạng định kỳ được thực hiện tối thiểu 01 lần/tuần.

3.9.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.9.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.9.2.1;

3.9.2.2.2. Nhật ký hệ thống của các đối tượng giám sát phải được kết nối và gửi về hệ thống giám sát.

3.9.2.2.3. Nhật ký từ các nguồn khác nhau phải đảm bảo được gửi về đầy đủ và hiển thị đúng thời gian thực trên hệ thống giám sát trung tâm.

3.9.2.2.4. Chủ quản hệ thống thông tin đã xác định danh sách các dịch vụ thuê ngoài quan trọng; có bằng chứng thực tế cho thấy chủ quản hệ thống thông tin đã thực hiện thu thập hoặc có quyền truy cập để trích xuất đầy đủ nhật ký an ninh từ các nhà cung cấp này về hệ thống thông tin.

3.9.2.2.5. Hệ thống thông tin lưu trữ nhật ký được đặt tại một vùng mạng riêng biệt; có tường lửa kiểm soát truy cập, tách biệt luồng truy cập hệ thống lưu trữ nhật ký với vùng mạng của các hệ thống phát sinh nhật ký.

3.9.2.2.6. Hệ thống thông tin lưu trữ nhật ký có tính năng ghi lại lịch sử các hành động truy cập, xem, trích xuất nhật ký của chính quản trị viên hệ thống thông tin lưu trữ nhật ký.

3.9.2.2.7. Hệ thống thông tin lưu trữ đã kích hoạt cơ chế WORM, khóa đối tượng hoặc sử dụng hạ tầng lưu trữ bất biến; khi quản trị viên thứ sửa đổi hoặc ghi đè một tệp nhật

ký đã lưu trữ thì hệ thống phải từ chối hành động và hiển thị thông báo.

3.9.2.2.8. Chính sách MFA được áp dụng cho các hành động nhạy cảm trên nhật ký hệ thống; khi quản trị viên thực hiện lệnh xóa hoặc đổi cấu hình thì hệ thống bắt buộc yêu cầu nhập mã xác thực thứ hai; nếu hành động thực hiện thành công mà không yêu cầu MFA thì không đạt.

3.9.2.2.9. Đường truyền dữ liệu phục vụ giám sát phải được cấu hình để các tác vụ giám sát hoặc giao thức truyền tải sử dụng cơ chế mã hóa.

3.9.2.2.10. Phân vùng ổ cứng, cơ sở dữ liệu hoặc lưu trữ nhật ký phải được mã hóa.

3.9.2.2.11. Thuật toán mã hóa nhật ký phải tương đương với chuẩn mã hóa đang áp dụng cho "thông tin nhạy cảm" của chủ quản hệ thống thông tin.

3.9.3. Kết luận

3.9.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.9.2.

3.9.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.10. Nhóm đánh giá 2.2.10

3.10.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã thiết lập các biện pháp tăng cường bảo vệ và phát hiện các mối đe doạ từ dịch vụ thư điện tử, trình duyệt web.

3.10.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên danh sách các trình duyệt web, dịch vụ thư điện tử và quy định về quản lý được ban hành để xác minh các nội dung sau:

3.10.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.10.2.1.1. Chủ quản hệ thống thông tin đã ban hành "Danh sách trình duyệt web và dịch vụ thư điện tử" được phép sử dụng trong hệ thống thông tin; tất cả các trình duyệt web và dịch vụ thư điện tử trong danh sách này phải đang trong thời gian hỗ trợ kỹ thuật của nhà cung cấp.

3.10.2.1.2. Có bằng chứng chứng minh việc rà soát và cập nhật bản vá lỗ hổng bảo mật cho trình duyệt web, dịch vụ thư điện tử được thực hiện tối thiểu 01 lần/tháng.

3.10.2.1.3. Hệ thống đã được triển khai dịch vụ lọc tên miền để ngăn chặn truy cập đến các tên miền giả mạo, độc hại.

3.10.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.10.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các yêu cầu tại mục 3.10.2.1;

3.10.2.2.2. Các bộ lọc URL đã được triển khai để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận và có cơ chế cập nhật cơ sở dữ liệu định kỳ.

3.10.2.2.3. Hệ thống có cơ chế kỹ thuật để giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ nhằm chống quá tải.

3.10.2.2.4. Chủ quản hệ thống thông tin đã thiết lập danh sách tiện ích mở rộng được phép sử dụng trong trình duyệt web và dịch vụ thư điện tử, theo đó yêu cầu:

3.10.2.2.4.1. Kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử, bảo đảm chỉ cho phép cài đặt và sử dụng những tiện ích mở rộng thuộc danh sách tiện ích mở rộng được phép sử dụng.

3.10.2.2.4.2. Gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng đã cài đặt trước đó nhưng không nằm trong danh sách tiện ích mở rộng được phép sử dụng.

3.10.2.2.5. Hệ thống thư điện tử đã được triển khai giải pháp xác thực email thông qua giao thức DMARC để tăng cường bảo mật và ngăn chặn các cuộc tấn công giả mạo tên miền của hệ thống thông tin.

3.10.2.2.6. Chủ quản hệ thống thông tin đã xác định các loại tệp tin được phép gửi qua hệ thống thư điện tử.

3.10.2.2.7. Giải pháp kỹ thuật đã được kích hoạt để tự động ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm.

3.10.2.2.8. Máy chủ thư điện tử được triển khai phương án bảo vệ để phát hiện và ngăn chặn mã độc theo thời gian thực.

3.10.3. Kết luận

3.10.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.10.2.

3.10.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.11. Nhóm đánh giá 2.2.11

3.11.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã thiết lập các quy định về quản lý, phòng ngừa, phát hiện và xử lý việc cài đặt, lây nhiễm, thực thi của các phần mềm và đoạn mã độc hại; đồng thời, có giải pháp phòng chống mã độc phù hợp và tương thích với hệ thống thông tin thuộc phạm vi quản lý.

3.11.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy định về xây dựng, triển khai và quản lý phần mềm, giải pháp phòng chống mã độc đã ban hành để xác minh các nội dung sau:

3.11.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.11.2.1.1. Hệ thống được trang bị phần mềm, giải pháp phòng, chống mã độc trên toàn bộ máy chủ và máy tính người dùng; giải pháp này được kích hoạt tính năng bảo vệ theo thời gian thực và tự động cập nhật các mẫu nhận diện mã độc mới.

3.11.2.1.2. Hệ thống có cơ chế tự động rà quét mã độc khi kết nối các phương tiện lưu trữ di động.

3.11.2.1.3. Tính năng tự động thực thi đối với các phương tiện lưu trữ di động đã được vô hiệu hóa hoàn toàn trên hệ thống.

3.11.2.1.4. Các tài sản phần cứng và phần mềm quan trọng đã được kích hoạt các cơ chế kỹ thuật hoặc tính năng chuyên dụng để phòng chống việc khai thác các lỗ hổng bảo mật.

3.11.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.11.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.11.2.1;

3.11.2.2.2. Có phương án kỹ thuật để kiểm tra, dò quét và xử lý mã độc đối với mọi gói phần mềm trước khi cho phép cài đặt vào hệ thống.

3.11.2.2.3. Chủ quản hệ thống thông tin đã ban hành quy định và triển khai công cụ quản lý tập trung đối với các phần mềm phòng chống mã độc đã cài đặt trên máy chủ và máy tính người dùng (cho phép theo dõi trạng thái, cập nhật chính sách từ xa).

3.11.2.2.4. Hệ thống có cơ chế theo dõi, giám sát và tự động phát cảnh báo khi phát hiện sự xuất hiện của các tiến trình mới hoặc khi các tập tin hệ thống quan trọng trên máy chủ bị thay đổi nội dung.

3.11.2.2.5. Giải pháp EDR đã được triển khai trên máy chủ, máy tính người dùng.

3.11.2.2.6. Giải pháp phòng chống mã độc đã được kết nối, chuyển dữ liệu về hệ thống quản lý nhật ký và sự kiện an ninh mạng tập trung để phục vụ việc giám sát liên tục theo thời gian thực.

3.11.3. Kết luận

3.11.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.11.2.

3.11.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.12. Nhóm đánh giá 2.2.12

3.12.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã thiết lập phương án sao lưu, khôi phục dữ liệu, đảm bảo khôi phục các tài sản về trạng thái tin cậy trước khi có sự cố.

3.12.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy định về sao lưu, khôi phục dữ liệu đã ban hành để xác minh các nội dung sau:

3.12.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.12.2.1.1. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định sao lưu và khôi phục dữ liệu; quy định được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy định, tối thiểu bao gồm:

3.12.2.1.1.1. Có định nghĩa về các loại dữ liệu cần được sao lưu và khôi phục cơ bản, tối thiểu bao gồm: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu, thông tin nghiệp vụ.

3.12.2.1.1.2. Xác định tần suất, phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu được định nghĩa.

3.12.2.1.1.3. Quản lý vùng lưu trữ dữ liệu sao lưu, bảo đảm tính toàn vẹn của dữ liệu và khả năng khôi phục dữ liệu.

3.12.2.1.1.4. Có bằng chứng chứng minh việc định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu.

3.12.2.1.2. Xác định danh sách dữ liệu cần sao lưu và tần suất sao lưu tương ứng.

3.12.2.1.3. Chủ quản hệ thống thông tin đã triển khai các giải pháp sao lưu dữ liệu tự động cho dữ liệu cần sao lưu.

3.12.2.1.4. Có phương án bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu; thực hiện mã hóa đối với những bản sao lưu chứa dữ liệu quan trọng.

3.12.2.1.5. Các bản sao lưu dữ liệu đã được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng tách biệt với môi trường vận hành.

3.12.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.12.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.12.2.1;

3.12.2.2.2. Kiểm tra sơ đồ triển khai và trên thực tế, bảo đảm thiết bị lưu trữ bản sao lưu là hạ tầng tách biệt với hệ thống đang vận hành.

3.12.2.2.3. Có biện pháp bảo vệ vật lý và môi trường cho nơi lưu trữ bản sao lưu.

3.12.2.2.4. Có bằng chứng về việc diễn tập, khôi phục thử nghiệm.

3.12.2.2.5. Có bằng chứng chứng minh việc kiểm tra khả năng khôi phục của bản sao lưu dữ liệu được thực hiện định kỳ tối thiểu 01 lần/quý; kết quả kiểm tra phải thể hiện dữ liệu được khôi phục thành công.

3.12.2.2.6. Chủ quản hệ thống thông tin đã xây dựng và ban hành quy định quản lý vòng đời bản sao lưu; tần suất rà soát, cập nhật quy định tối thiểu phải thực hiện 01 lần/năm.

3.12.2.2.7. Có danh mục liệt kê tất cả bản sao lưu đang tồn tại.

3.12.2.2.8. Kiểm tra sơ đồ và cấu hình hệ thống để xác minh sự tuân thủ: có đủ 03 bản sao lưu dữ liệu; lưu trữ trên 02 phương tiện hoặc loại hình lưu trữ khác nhau; có sự tách biệt về vật lý vá địa lý.

3.12.2.2.9. Có ít nhất 01 bản sao lưu thỏa mãn 03 điều kiện: ghi trên vật mang tin không thể ghi đè; đặt tại vị trí bên ngoài hệ thống thông tin; sử dụng kỹ thuật cách ly vật lý hoặc logic nghiêm ngặt.

3.12.2.2.10. Kiểm tra nhật ký hệ thống sao lưu, đảm bảo mọi phiên sao lưu đều được ghi lại.

3.12.2.2.11. Hệ thống quản lý khóa mã hóa được thiết lập tách biệt với hệ thống thông tin lưu trữ bản sao lưu.

3.12.2.2.12. Chủ quản hệ thống thông tin đã xây dựng và ban hành quy trình kiểm tra an ninh bản sao lưu.

3.12.2.2.13. Kiểm tra báo cáo, nhật ký quét mã độc trên các bản sao lưu chứa dữ liệu quan trọng, dữ liệu nhạy cảm và tần suất rà quét; trong báo cáo phải ghi rõ công cụ được sử dụng, phiên bản phần mềm và kết quả quét.

3.12.2.2.14. Chủ quản hệ thống thông tin đã xây dựng và ban hành quy trình hủy bỏ dữ liệu, thanh lý tài sản lưu trữ phù hợp với quy định về lưu trữ.

3.12.2.2.15. Phương pháp xóa, hủy bỏ dữ liệu an toàn đã tuân thủ theo quy định của pháp luật về lưu trữ và tuân thủ tiêu chuẩn NIST SP 800-88.

3.12.2.2.16. Có biên bản hủy, xóa dữ liệu đối với các bản sao lưu đã hết vòng đời.

3.12.2.2.17. Hệ thống thông tin phải sử dụng MFA hoặc cơ chế phê duyệt nhiều lớp khi thực hiện các lệnh xóa, định dạng, hủy bỏ vùng dữ liệu (LUN hoặc Volume) hoặc xóa bản sao lưu.

3.12.2.2.18. Xác minh tính năng MFA hoặc xác thực lại đã được kích hoạt cho các tài khoản có quyền xóa dữ liệu bằng cách yêu cầu quản trị viên thực hiện một thao tác xóa đối với dữ liệu thử nghiệm và kiểm tra nhật ký hệ thống sau khi thực hiện thao tác xóa thử nghiệm; trường hợp cho phép xóa mà không yêu cầu MFA hoặc xác thực lại thì không đạt yêu cầu.

3.12,3. Kết luận

3.12.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.12.2.

3.12.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.13. Nhóm đánh giá 2.2.13

3.13.1. Mục đích đánh giá

Đảm bảo hệ thống mạng được thiết kế và vận hành theo kiến trúc an toàn gồm: phân vùng mạng, đặc quyền tối thiểu, dự phòng nóng; có đầy đủ hồ sơ tài liệu được cập nhật định kỳ; kiểm soát chặt chẽ truy cập từ xa (VPN, MFA) và có mạng quản trị tách biệt để đảm bảo an ninh cho công tác quản trị.

3.13.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên sơ đồ mạng, hồ sơ thiết kế, cấu hình thiết bị mạng và các biên bản kiểm thử (nếu có) để xác minh các nội dung sau:

3.13.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.13.2.1.1. Hệ thống thông tin có sơ đồ kiến trúc mạng tổng quan, sơ đồ kiến trúc mạng chi tiết và tài liệu mô tả phương án bảo đảm an ninh mạng.

3.13.2.1.2. Sơ đồ kiến trúc mạng phải thể hiện được việc áp dụng 03 nguyên tắc: phân vùng mạng, đặc quyền tối thiểu và tính sẵn sàng.

3.13.2.1.3. Sơ đồ kiến trúc mạng phải được xem xét và cập nhật tối thiểu 01 lần/06 tháng hoặc khi có thay đổi ảnh hưởng đến sơ đồ này.

3.13.2.1.4. Có phương án dự phòng cho các thiết bị mạng chính của hệ thống thông tin.

3.13.2.1.5. Có phương án kiểm soát truy cập giữa các vùng mạng, kiểm soát truy cập thiết bị đầu cuối, máy tính người dùng kết nối vào mạng trong hệ thống thông tin.

3.13.2.1.6. Việc thay đổi về cơ sở hạ tầng mạng phải thực hiện quản lý thay đổi.

3.13.2.1.7. Hệ thống mạng được chia tách thành các vùng mạng, tối thiểu bao gồm: 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; có vùng mạng nội bộ; có vùng mạng biên; có vùng mạng WAN diện rộng.

3.13.2.1.8. Chủ quản hệ thống thông tin đã thực hiện kiểm soát luồng truy cập giữa các vùng mạng nêu trên.

3.13.2.1.9. Có công cụ hoặc biện pháp theo dõi hiệu năng (CPU, RAM) của các tài sản phần cứng trong hệ thống thông tin.

3.13.2.1.10. Hệ thống phải sử dụng các giao thức truyền thông và quản trị mạng an toàn.

3.13.2.1.11. Chủ quản hệ thống thông tin phải thiết lập VPN và yêu cầu xác thực cho việc

truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống.

3.13.2.1.12. Hệ thống phải yêu cầu người dùng xác thực đa nhận tố để kết nối VPN và các dịch vụ xác thực khác trước khi truy cập vào hệ thống.

3.13.2.1.13. Các thiết bị được phép truy cập từ xa phải đảm bảo các yêu cầu về bảo mật: cài đặt phần mềm phòng chống mã độc, cấu hình bảo mật theo chính sách an ninh, an toàn đã ban hành của chủ quản hệ thống thông tin.

3.13.2.1.14. Chủ quản hệ thống thông tin đã ban hành quy trình thử nghiệm và nghiệm thu hệ thống.

3.13.2.1.15. Có bằng chứng chứng minh việc kiểm thử hệ thống đã được hoàn thành và đạt yêu cầu trước khi hệ thống được đưa vào vận hành, khai thác, sử dụng.

3.13.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.13.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.13.2.1;

3.13.2.2.2. Kiểm tra thỏa thuận cung cấp dịch vụ và cấu hình đường truyền Internet để đảm bảo đối với các hệ thống buộc phải có kết nối mạng Internet, đã triển khai phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.

3.13.2.2.3. Kiểm tra giải pháp quản lý xác thực tập trung đang hoạt động và bảo đảm giải pháp có đủ 03 chức năng: xác thực, cấp quyền và ghi nhật ký kiểm toán đối với các truy cập hệ thống thông tin.

3.13.2.2.4. Kiểm tra sơ đồ và cấu hình hệ thống để bảo đảm tài nguyên quản trị nằm trong vùng mạng tách biệt so với mạng người dùng/mạng chính.

3.13.2.2.5. Thực hiện thử nghiệm kết nối từ vùng mạng quản trị ra Internet bằng các công cụ truy cập mạng; kết quả đạt khi không thể thiết lập kết nối trực tiếp ra Internet.

3.13.2.2.6. Có quyết định thành lập tổ nghiệm thu hoặc thỏa thuận cung cấp dịch vụ, tư vấn giám sát độc lập với bộ phận/đơn vị trực tiếp triển khai.

3.13.2.2.7. Chủ quản hệ thống thông tin đã xây dựng, ban hành và tuân thủ quy trình quản lý thay đổi; tần suất rà soát, cập nhật quy trình tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình.

3.13.2.2.8. Kiểm tra hồ sơ thay đổi trên cơ sở chọn một số lần thay đổi gần nhất để xác minh các thông tin sau:

3.13.2.2.8.1. Có bằng chứng thông báo cho các bên liên quan trước khi thay đổi.

3.13.2.2.8.2. Có báo cáo đánh giá tác động an ninh mạng và tính tương thích trước khi thực hiện thay đổi.

3.13.2.2.8.3. Có phương án khôi phục hoặc phương án thay thế nếu thay đổi thất bại.

3.13.2.2.8.4. Có báo cáo đánh giá rủi ro tại 03 thời điểm: trước, trong và sau khi thay đổi.

3.13.2.2.8.5. Nhật ký hệ thống phải ghi lại đầy đủ các bước thực hiện thay đổi.

3.13.3. Kết luận

3.13.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.13.2.

3.13.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.14. Nhóm đánh giá 2.2.14

3.14.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin đã thiết lập hệ thống giám sát an ninh mạng tập trung hoạt động 24/7; triển khai lớp phòng thủ đa tầng; kiểm soát chặt chẽ các cổng kết nối vật lý/logic; thu thập đầy đủ dữ liệu lưu lượng mạng và thực hiện tinh chỉnh ngưỡng cảnh báo định kỳ hàng tháng.

3.14.2. Phương pháp đánh giá

Đối với các hệ thống thông tin cấp độ 3, 4, 5:

3.14.2.1. Chủ quản hệ thống thông tin đã triển khai giải pháp quản lý sự kiện an ninh mạng tập trung SIEM hoặc tương đương.

3.14.2.2. Hệ thống phải có các tập luật để liên kết các sự kiện rời rạc thành cảnh báo có ý nghĩa.

3.14.2.3. Kiểm tra lịch trực và nhật ký trực của đội ngũ giám sát để đảm bảo luôn có nhân sự giám sát hệ thống 24/7.

3.14.2.4. Kiểm tra trên các máy chủ, máy trạm quan trọng để xác minh tính năng tường lửa của hệ điều hành đã được bật; nếu hệ điều hành có tính năng tDS/IPS tích hợp, xác minh tính năng này đã được kích hoạt.

3.14.2.5. Chủ quản hệ thống thông tin đã triển khai cho hệ thống các giải pháp, thiết bị chuyên dụng có chức năng lọc gói tin giữa các phân đoạn mạng, lọc tầng ứng dụng, cảnh báo phát hiện và ngăn chặn xâm nhập trong hệ thống mạng (NGFW, WAF, IPS/IDS).

3.14.2.6. Hệ thống thông tin phải có chính sách lọc gói tin giữa các phân đoạn mạng.

3.14.2.7. Hệ thống thông tin phải có chính sách lọc tầng ứng dụng để chặn các tấn công web hoặc ứng dụng cụ thể.

3.14.2.8. Hệ thống thông tin phải có chính sách phát hiện và ngăn chặn xâm nhập đã được cập nhật, đồng thời, kích hoạt ở chế độ chặn, ngăn chặn.

3.14.2.9. Các cổng mạng không sử dụng phải ở trạng thái vô hiệu hóa.

3.14.2.10. Hệ thống thông tin đã được áp dụng các biện pháp kiểm soát như bảo mật cổng (giới hạn MAC), 802.1x, hoặc NAC để kiểm soát thiết bị cắm vào mạng.

3.14.2.11. Kiểm tra cấu hình thiết bị mạng để xác minh việc kích hoạt tính năng gửi nhật ký lưu lượng về hệ thống phân tích.

3.14.2.12. Kiểm tra trên hệ thống giám sát để bảo đảm hiển thị dữ liệu về luồng kết nối phục vụ cho việc điều tra và cảnh báo.

3.14.2.13. Kiểm tra nhật ký cấu hình hoặc yêu cầu bộ phận quản trị hệ thống SIEM/IDS cung cấp thông tin, bằng chứng chứng minh đã triển khai hoạt động rà soát và điều chỉnh ngưỡng cảnh báo định kỳ tối thiểu 01 lần/tháng.

3.14.3. Kết luận

3.14.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.14.2.

3.14.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.15. Nhóm đánh giá 2.2.15

3.15.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin có cơ cấu nhân sự tách biệt giữa vận hành và bảo vệ an ninh mạng; nhân sự có đủ năng lực và cam kết bảo mật; công tác đào tạo được thực hiện đầy đủ cho hai nhóm đối tượng: người dùng chung và nhân sự chuyên trách.

3.15.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên sơ đồ tổ chức, hồ sơ nhân sự, kế hoạch đào tạo và kết quả đào tạo để xác minh các nội dung sau:

3.15.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.15.2.1.1. Có quyết định thành lập các bộ phận riêng biệt vận hành, quản trị hệ thống vá bảo vệ an ninh mạng; quyết định thành lập phải thể hiện rõ cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

3.15.2.1.2. Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có văn bằng hoặc chứng chỉ về an ninh mạng (hoặc lĩnh vực tương đương), công nghệ thông tin; những nhân sự này đã được ký cam kết bảo mật thông tin trong quá trình làm việc và sau khi nghỉ việc.

3.15.2.1.3. Chủ quản hệ thống thông tin đã thiết lập và duy trì chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin; có bằng chứng chứng minh đã tổ chức đào tạo theo chương trình tối thiểu 01 lần/năm.

3.15.2.1.4. Chủ quản hệ thống thông tin đã thực hiện đào tạo kiến thức chuyên môn an ninh mạng theo từng vị trí, vai trò cụ thể, đào tạo nhận thức về quy định pháp luật liên quan, trách nhiệm pháp lý cho các cá nhân tham gia bảo vệ an ninh mạng; có bằng chứng chứng minh đã tổ chức đào tạo tối thiểu 01 lần/năm hoặc khi có thay đổi về các nhân sự.

3.15.2.1.5. Có bằng chứng chứng minh việc định kỳ tổ chức sát hạch các cá nhân tham gia bảo vệ an ninh mạng cho hệ thống thông tin.

3.15.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.15.2.2.1. Tuân thủ kế thừa: Đáp ứng đầy đủ các tiêu chí đánh giá tại mục 3.15.2.1;

3.15.2.2.2. Kiểm tra tài liệu về khung năng lực, mô tả công việc, trong đó:

3.15.2.2.2.1. Tài liệu mô tả các tiêu chuẩn năng lực cụ thể cho từng vị trí (vận hành, quản trị hệ thống, bảo vệ an ninh mạng).

3.15.2.2.2.2. Có các yêu cầu về bằng cấp, chứng chỉ và kinh nghiệm được quy định rõ ràng làm cơ sở tuyển dụng.

3.15.2.2.2.3. Hồ sơ của nhân sự đang làm việc phù hợp với khung năng lực được xác định trong tài liệu.

3.15.2.2.3. Kiểm tra hồ sơ xác minh lý lịch nhân sự và đảm bảo:

3.15.2.2.3.1. Có phiếu lý lịch tư pháp hoặc văn bản thẩm tra lý lịch tương đương.

3.15.2.2.3.2. Việc xác minh lý lịch phải bao gồm cả nhân sự chuyên trách và nhân sự kiêm nhiệm (đặc biệt là các vị trí có quyền quản trị hệ thống); việc xác minh phải được thực hiện trước hoặc ngay khi tiếp nhận nhiệm vụ.

3.15.2.2.4. Có bằng chứng chứng minh chủ quản hệ thống thông tin đã thực hiện đánh giá định kỳ đối với đạo đức nghề nghiệp và việc tuân thủ các quy định nội bộ của nhân sự liên quan.

3.15.3. Kết luận

3.15.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.15.2.

3.15.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.16. Nhóm đánh giá 2.2.16

3.16.1. Nhóm đánh giá 2.2.16.1

3.16.1.1. Mục đích đánh giá

Đảm bảo các nhà cung cấp dịch vụ cho hệ thống thông tin có tư cách pháp nhân minh bạch, tuân thủ đầy đủ các quy định pháp luật Việt Nam để đảm bảo an toàn dữ liệu và khả năng giải trình, xử lý khi xảy ra sự cố.

3.16.1.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên hồ sơ năng lực, hồ sơ pháp lý, thỏa thuận dịch vụ và các tài liệu liên quan của nhà cung cấp để xác minh các nội dung sau:

3.16.1.2.1. Kiểm tra tính tuân thủ pháp lý: Nhà cung cấp sản phẩm, dịch vụ/bên thứ ba phải cung cấp bản sao công chứng (hoặc tài liệu xác thực tương đương) của Giấy chứng nhận đăng ký doanh nghiệp hoặc Giấy phép hoạt động phù hợp với lĩnh vực cung cấp dịch vụ theo quy định hiện hành cho chủ quản hệ thống thông tin.

3.16.1.2.2. Kiểm tra định danh điện tử doanh nghiệp: Nhà cung cấp sản phẩm, dịch vụ/bên thứ ba phải sử dụng chữ ký số hợp lệ hoặc tài khoản định danh điện tử doanh nghiệp trên các hệ thống Cổng dịch vụ công quốc gia để thực hiện ký kết văn bản thỏa thuận và giao dịch điện tử.

3.16.1.2.3. Kiểm tra sự hiện diện pháp lý tại Việt Nam: Trong thỏa thuận cung cấp dịch vụ hoặc hồ sơ năng lực phải đầy đủ thông tin cụ thể về người đại diện theo pháp luật, địa chỉ trụ sở chính, chi nhánh hoặc văn phòng đại diện hợp pháp đang hoạt động trên lãnh thổ Việt Nam để liên hệ xử lý vấn đề pháp lý và kỹ thuật khi có yêu cầu.

3.16.1.2.4. Kiểm tra vị trí hạ tầng: Trong thỏa thuận dịch vụ hoặc cam kết chất lượng dịch vụ của nhà cung cấp dịch vụ lưu trữ phải có điều khoản rõ ràng, cam kết về việc hạ tầng vật lý (máy chủ, thiết bị lưu trữ) hoặc trung tâm dữ liệu lưu trữ dữ liệu của hệ thống được đặt tại lãnh thổ Việt Nam; nhà cung cấp sản phẩm, dịch vụ/bên thứ ba phải cung cấp các tài liệu để xác nhận vị trí của hạ tầng vật lý, trung tâm dữ liệu.

3.16.1.3. Kết luận

3.16.1.3.1. Đáp ứng: Đáp ứng đầy đủ các nội dung được liệt kê tại mục 3.16.1.2.

3.16.1.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên hoặc thông tin cung cấp không chính xác, không còn hiệu lực.

3.16.2. Nhóm đánh giá 2.2.16.2

3.16.2.1. Mục đích đánh giá

Đảm bảo tính bí mật, tính toàn vẹn và tính xác thực của dữ liệu trong quá trình truyền tải; ngăn chặn các nguy cơ nghe lén, can thiệp trái phép hoặc tấn công xen giữa khi dữ liệu di chuyển qua mạng Internet, mạng diện rộng hoặc giữa oác thánh phần nội bộ của hệ thống.

3.16.2.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên tài liệu thiết kế mạng, cấu hình thiết bị/hệ thống và kiểm tra thực tế để xác minh các nội dung sau:

3.16.2.2.1. Kiểm tra bảo mật đường truyền Internet nhằm xác nhận việc sử dụng các giao thức an toàn đối với các kênh truyền tải dữ liệu qua mạng mở, không sử dụng những giao thức đã lỗi thời hoặc tồn tại điểm yếu (như SSL 2.0, TLS 1.1 ...).

3.16.2.2.2. Kiểm tra chứng thư số được sử dụng cho các kết nối này hợp lệ và được cấp bởi tổ chức tin cậy theo quy định của pháp luật.

3.16.2.2.3. Kiểm tra mã hóa kết nối mạng mở rộng bằng cách rà soát sơ đồ kết nối mạng và cấu hình thiết bị định tuyến/tường lửa tại các điểm kết nối ra ngoài ranh giới vật lý của hệ thống thông tin (như kết nối WAN, liên kết giữa các trung tâm dữ liệu); xác nhận lưu lượng IP truyền qua các kết nối này được cấu hình sử dụng cơ chế mã hóa.

3.16.2.2.4. Kiểm tra mã hóa giao tiếp nội bộ và người dùng bằng cách thử nghiệm truy cập từ máy trạm vào hệ thống thông tin lưu trữ, xác nhận hệ thống bắt buộc sử dụng giao thức truyền thông có mã hóa và từ chối các kết nối không an toàn.

3.16.2.2.5. Đối với kết nối quản trị và đồng bộ: Kiểm tra cấu hình các giao diện quản trị và các kênh đồng bộ dữ liệu giữa các nút hoặc cụm lưu trữ để đảm bảo dữ liệu trao đổi được mã hóa.

3.16.2.2.6. Kiểm tra quy trình di chuyển dữ liệu: Rà soát quy trình và nhật ký thực hiện việc di chuyển dữ liệu giữa các vật mạng tin (ví dụ: từ ổ cứng cũ sang mới, từ hệ thống tại chỗ lên đám mây), xác nhận việc di chuyển được thực hiện tuân thủ theo quy trình và oó ghi lại bằng chứng chứng minh. Xác nhận việc áp dụng các biện pháp kiểm tra tính toàn vẹn trước vá sau khi di chuyển; đảm bảo dữ liệu tại đích đến vẫn an toàn và có thể đọc, truy xuất bình thường.

3.16.2.3. Kết luận

3.16.2.3.1. Đáp ứng: Khi hệ thống đáp ứng đầy đủ các nội dung được liệt kê tại mục 3.16.2.2.

3.16.2.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên hoặc phát hiện dữ liệu được truyền tải dưới dạng bản rõ ở các kênh bắt buộc phải mã hóa.

3.16.3. Nhóm đánh giá 2.2.16.3

3.16.3.1. Mục đích đánh giá

Đảm bảo nhà cung cấp dịch vụ tuân thủ các cam kết về chủ quyền dữ liệu, duy trì an ninh trong chuỗi cung ứng dịch vụ, cung cấp cơ chế truy cập an toàn, thực hiện quy trình hủy bỏ dữ liệu triệt để và duy trì đầy đủ nhật ký kiểm toán cho toán bộ vòng đời tài liệu.

3.16.3.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên thỏa thuận dịch vụ, quy trình nội bộ, hồ sơ năng lực và các bằng chứng kỹ thuật để xác minh các nội dung sau:

3.16.3.2.1. Kiểm tra yêu cầu về lưu trữ và tuân thủ pháp lý: Thỏa thuận cung cấp dịch vụ (SLA) phải cam kết lưu giữ toàn bộ tài liệu điện tử được ủy thác trong lãnh thổ Việt Nam.

3.16.3.2.2. Nhà cung cấp sản phẩm, dịch vụ/bên thứ ba đã đáp ứng các quy định pháp luật hiện hành về ANM.

3.16.3.2.3. Rà soát tài liệu kỹ thuật để xác nhận nhà cung cấp đã trang bị các cơ chế kiểm soát truy cập an toàn (như MFA, đường truyền mã hóa, phân quyền chi tiết) cho tất cả các tài liệu được lưu giữ.

3.16.3.2.4. Trường hợp nhà cung cấp sử dụng hạ tầng hoặc dịch vụ của bện thứ ba (nhá cung cấp ngang hàng), đảm bảo các thỏa thuận liên kết giữa hai bên đáp ứng quy định hiện hánh về bảo đảm an ninh mạng và độ tin cậy cung cấp cho khách hàng không thấp hơn mức độ cam kết trong thỏa thuận gốc.

3.16.3.2.5. Chủ quản hệ thống thông tin có quy trình hủy bỏ dữ liệu được ban hánh chính thức và thực hiện rà soát, cập nhật định kỳ 01 lần/năm.

3.16.3.2.6. Trong thỏa thuận phải có điều khoản cam kết áp dụng biện pháp kỹ thuật đảm bảo dữ liệu sau khi xóa, hủy không thể khôi phục.

3.16.3.2.7. Phương án kỹ thuật sử dụng để hủy bỏ (ví dụ: ghi đé đa lần, khử từ, tiêu hủy khóa mã hóa hoặc phá hủy vật lý) đã tuân thủ theo các quy định của pháp luật về lưu trữ, an ninh mạng.

3.16.3.2.8. Hệ thống ghi nhật ký phải ghi lại toàn bộ các hoạt động tác động đến dịch vụ như: truy cập, tải lên, tải xuống, chia sẻ, xóa...

3.16.3.2.9. Các nhật ký sự kiện vá tài liệu điện tử đã áp dụng các biện pháp bảo vệ tính toàn vẹn như: sử dụng hàm băm, cơ chế WORM và sao lưu trong suốt vòng đời lưu trữ.

3.16.3.3. Kết luận

3.16.3.3.1. Đáp ứng: Khi nhà cung cấp dịch vụ đáp ứng đầy đủ các nội dung được liệt kê tại mục 3.16.3.2 và cung cấp được bằng chứng chứng minh.

3.16.3.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên hoặc phát hiện vi phạm cam kết về vị trí lưu trữ, quy trình hủy bỏ không an toàn.

3.16.4. Nhóm đánh giá 2.2.16.4

3.16.4.1. Mục đích đánh giá

Đảm bảo mọi kết nối truy cập từ xa của nhà cung cấp dịch vụ hoặc nhà sản xuất vào hệ thống đều được kiểm soát chặt chẽ, giảm thiểu rủi ro lộ lọt dữ liệu nhạy cám, ngăn chặn việc cài đặt phần mềm không qua kiểm duyệt và đảm bảo tính minh bạch thông qua việc giám sát vá cấp quyền cho từng phiên làm việc.

3.16.4.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy trình vận hành, nhật ký hệ thống, cấu hình thiết bị và quan sát thực tế để xác minh các nội dung sau:

3.16.4.2.1. Đã tuân thủ yêu cầu 2.2.7 Quản lý tài khoản và quyền truy cập tái khoản của người dùng.

3.16.4.2.2. Hệ thống quản lý có cơ chế bắt buộc nhà cung cấp phải gửi yêu cầu và chờ phê duyệt trước mỗi phiên kết nối.

3.16.4.2.3. Quyền truy cập đã được giới hạn, chỉ cho phép kết nối đến các thiết bị hoặc máy chủ trung gian được chỉ định thay vì truy cập trực tiếp vào toàn bộ mạng nội bộ.

3.16.4.2.4. Rà soát cấu hình DLP hoặc bộ lọc gói tin nhằm xác minh các gói dữ liệu chẩn đoán gửi ra ngoài được kiểm tra và loại bỏ thông tin nhạy cảm.

3.16.4.2.5. Hệ thống đã giới hạn chỉ cho phép gửi dữ liệu đến các dải IP đã được xác thực là thuộc sở hữu của nhà cung cấp.

3.16.4.2.6. Trên hệ thống đã vô hiệu hóa các kênh cho phép tải xuống và tự động cài đặt bản cập nhật phần mềm thông qua liên kết hỗ trợ từ xa. Quy trình cập nhật đã bắt buộc phải thực hiện nội bộ hoặc qua kênh được kiểm duyệt riêng.

3.16.4.2.7. Các tính năng tự động gửi dữ liệu chẩn đoán hoặc tự động mở kết nối "gọi về máy chủ" đã bị vô hiệu hóa (trừ trường hợp thiết yếu đã được phê duyệt).

3.16.4.2.8. Các kết nối hỗ trợ từ xa phát sinh đã bắt buộc áp dụng MFA.

3.16.4.2.9. Hệ thống đã ghi lại nhật ký hoặc ghi lại toàn bộ phiên làm việc từ xa của nhà cung cấp.

3.16.4.3. Kết luận

3.16.4.3.1. Đáp ứng: Khi hệ thống và quy trình vận hành đáp ứng đầy đủ các nội dung được liệt kê tại mục 3.16.4.2.

3.16.4.3.2. Không đáp ứng:

Nếu thiếu một trong các yêu cầu trên.

Nếu phát hiện các kết nối từ xa được thiết lập tự động mà không qua phê duyệt, cho phép cập nhật phần mềm trực tiếp qua kênh truy cập từ xa hoặc thiếu cơ chế giám sát, MFA.

3.17. Nhóm đánh giá 2.2.17

3.17.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin thiết lập một vòng đời phát triển phần mềm an toàn từ thiết kế, lập trình, quản lý thành phần bên thứ ba đến kiểm thử và vận hành; kiểm soát chặt chẽ rủi ro từ mã nguồn (bao gồm cả thuê khoán) và duy trì năng lực xử lý lỗ hổng bảo mật liên tục.

3.17.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy trình phát triển phần mềm, thỏa thuận thuê khoán, hồ sơ kiểm thử và hệ thống quản lý lỗi để xác minh các nội dung sau:

3.17.2.1. Chủ quản hệ thống thông tin đã xây dựng và ban hành quy trình phát triển ứng dụng an toàn; quy trình được rà soát, cập nhật tối thiểu 01 lần/năm.

3.17.2.2. Có điều khoản yêu cầu bàn giao mã nguồn để chủ quản hệ thống thông tin có thể kiểm soát và rà quét lỗ hổng.

3.17.2.3. Thử nghiệm thực tế hoặc kiểm tra tài liệu để bảo đảm có cơ chế, phương thức tiếp nhận được công bố để báo cáo lỗ hổng.

3.17.2.4. Kiểm tra danh mục phần mềm:

3.17.2.4.1. Có danh sách thư viện, mô-đun bên thứ ba đang sử dụng.

3.17.2.4.2. Tần suất cập nhật danh sách thư viện đáp ứng tối thiểu 01 lần/tháng.

3.17.2.4.3. Kiểm tra đánh giá rủi ro: có thông tin kèm theo về các lỗ hổng đã biết của từng thư viện trong danh sách.

3.17.2.5. Kiểm tra kiến trúc và mã hóa:

3.17.2.5.1. Tài liệu thiết kế đã thể hiện rõ nguyên tắc bảo mật (đặc biệt là đặc quyền tối thiểu) ngay từ đầu.

3.17.2.5.2. Kiểm tra các thuật toán mã hóa: Đảm bảo ứng dụng sử dụng các thư viện chuẩn thay vì tự viết thuật toán mã hóa riêng nhưng chưa được chứng nhận.

3.17.2.5.3. Kiểm tra tính năng ghi nhật ký: Xác minh ứng dụng có ghi lại các hành vi của người dùng.

3.17.2.6. Kiểm tra việc phân tách môi trường:

3.17.2.6.1. Yêu cầu sơ đồ mạng hoặc cấu hình thực tế chứng minh sự tách biệt vật lý/logic giữa 03 môi trường: Phát triển - Kiểm thử - Vận hành.

3.17.2.6.2. Kiểm tra mã nguồn: Rà quét để đảm bảo không có thông tin xác thực hoặc dữ liệu bí mật trong mã nguồn.

3.17.2.7. Kiểm tra đào tạo:

Rà soát hồ sơ đào tạo: Đảm bảo lập trình viên được đào tạo về phát triển ứng dụng an toàn (ví dụ: OWASP Top 10) tối thiểu 01 lần/năm.

3.17.2.8. Kiểm tra hoạt động kiểm thử:

3.17.2.8.1. Có báo cáo rà quét lỗ hổng mã nguồn đối với các thư viện và đoạn mã tự viết.

3.17.2.8.2. Có báo cáo kiểm thử xâm nhập trên môi trường giả lập/thử nghiệm.

3.17.2.8.3. Xác nhận toàn bộ các lỗ hổng nghiêm trọng đã được khắc phục trước khi ứng dụng được đưa vào môi trường vận hành chính thức.

3.17.3. Kết luận

3.17.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.17.2.

3.17.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.18. Nhóm đánh giá 2.2.18

3.18.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin có sự chuẩn bị sẵn sàng về nhân lực, quy trình gồm: báo cáo, xử lý, phối hợp với cơ quan có thẩm quyền và có kênh liên lạc để phát hiện, tiếp nhận và xử lý kịp thời các sự cố an ninh mạng, giảm thiểu thiệt hại cho hệ thống.

3.18.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quyết định thành lập đội ứng phó sự cố, quy trình ứng phó sự cố, danh sách liên lạc và các biên bản diễn tập/xử lý sự cố để xác minh các nội dung sau:

3.18.2.1. Đối với hệ thống thông tin cấp độ 1, 2:

3.18.2.1.1. Chủ quản hệ thống thông tin đã ban hành quyết định thành lập lực lượng ứng phó sự cố an ninh mạng, trong đó:

3.18.2.1.1.1. Phân công, chỉ định rõ người quản lý chính và người dự phòng để quản lý quy trình ứng phó sự cố.

3.18.2.1.1.2. Chỉ định đầu mối liên lạc để báo cáo sự cố trong hệ thống thông tin.

3.18.2.1.1.3. Quy định trách nhiệm thực hiện rà soát tối thiểu 01 lần/năm đối với danh sáoh các đầu mối liên lạc bên ngoài, bao gồm: cơ quan chức năng, đơn vị hỗ trợ, nhà cung cấp dịch vụ và cô bằng chứng chứng minh việc thực hiện.

3.18.2.1.1.4. Phân công vị trí, vai trô và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.

3.18.2.1.1.5. Quy định trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.

3.18.2.1.2. Chủ quản hệ thống thông tin đã ban hành vá tuân thủ quy trình nội bộ để báo cáo sự cố an ninh mạng; quy trình được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy trình, tối thiểu bao gồm việc thực hiện phân nhóm sự cố an ninh mạng.

3.18.2.1.3. Chủ quản hệ thống thông tin đã ban hành và tuận thủ quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với các cơ quan chứo năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng; quy trình được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy trình.

3.18.2.1.4. Chủ quản hệ thống thông tin đã 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; cơ chế liên lạc được đánh giá và cập nhật tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến cơ chế.

3.18.2.2. Đối với hệ thống thông tin cấp độ 3, 4, 5:

3.18.2.2.1. Tuận thủ các yêu cầu tại 3.18.2.1;

3.18.2.2.2. Yêu cầu cung cấp "Báo cáo tổng kết sau sự cố" của các sự cố đã xảy ra trong oùng kỳ; Báo cáo phải bao gồm: nguyên nhân gốc rễ, mốc thời gian xử lý, hiệu quả của quy trình ứng phó.

3.18.2.2.3. Chủ quản hệ thống thông tin đã thực hiện đề xuất cải tiến từ buổi đánh giá sau sự cố để đưa vào áp dụng thực tế.

3.18.2.2.4. Chủ quản hệ thống thông tin đã thực hiện chia sẻ thông tin, báo cáo sự cố trong vòng 24 giờ kể từ khi phát hiện cho cơ quan có thẩm quyền theo quy định của pháp luật.

3.18.2.2.5. Kiểm tra kế hoạch diễn tập

Có kế hoạch diễn tập hằng năm với tần suất tối thiểu là 01 lần/năm và các kịch bản diễn tập cụ thể.

3.18.2.2.6. Kiểm tra báo cáo kết quả diễn tập:

Thời gian phản ứng của đội ứng cứu, sự phối hợp giữa các bộ phận và các vấn đề tồn tại được ghi nhận sau diễn tập.

3.18.2.2.7. Có tál liệu định nghĩa ngưỡng và quy định về ngưỡng sự cố an ninh mạng:

3.18.2.2.7.1. Cô văn bản quy định các "ngưỡng" để phân biệt giữa một sự kiện bình thường và một sự cố.

3.18.2.2.7.2. Đối chiếu các ngưỡng đã quy định với cấu hình cảnh báo trên các công cụ giám sát, đảm bảo ngưỡng được thiết lập theo quy định để cảnh báo kịp thời và tránh gây nhiễu.

3.18.2.2.7.3. Việc đánh giá và điều chỉnh lại các ngưỡng này tối thiểu 01 lần/năm hoặc khi có thay đổi hạ tầng (để phù hợp với mức độ hoạt động mới của hệ thống).

3.18.3. Kết luận

3.18.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.18.2.

3.18.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.19. Nhóm đánh giá 2.2.19

3.19.1. Mục đích đánh giá

Đảm bảo chủ quản hệ thống thông tin chủ động phát hiện lỗ hổng bảo mật thông qua việc mô phỏng các cuộc tấn công thực tế từ bên trong và bên ngoài; đảm bảo các lỗ hổng tìm thấy được khắc phục triệt để; định kỳ rà soát để tìm kiếm các dấu hiệu tấn công mạng hoặc mã độc đang tồn tại trong hệ thống.

3.19.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên chương trình/kế hoạch kiểm thử, thỏa thuận cung cấp dịch vụ, các báo cáo kết quả kiểm thử và báo cáo khắc phục để xác minh các nội dung sau:

3.19.2.1. Chủ quản hệ thống thông tin đã thiết lập và triển khai chương trình, kế hoạch tổng thể về kiểm thử xâm nhập, trong kế hoạch cần chỉ rõ:

3.19.2.1.1. Quy định rõ các hành vi bị cấm khi thực hiện kiểm thử.

3.19.2.1.2. Quy định rõ đội giám sát có được báo trước hay phải tự phát hiện cuộc tấn công giả lập.

3.19.2.2. Đối với kiểm thử từ bên ngoài: Có báo cáo kiểm thử đối với các địa chỉ IP công cộng, trang web, ứng dụng di động công khai; tần suất thực hiện tối thiểu 01 lần/năm.

3.19.2.3. Đối với kiểm thử từ bên trong: Có báo cáo kiểm thử đối với mạng nội bộ, máy chủ nội bộ; tần suất thực hiện tối thiểu 01 lần/năm.

3.19.2.4. Có báo cáo khắc phục lỗ hổng bảo mật được phát hiện trong quá trình kiểm thử và thể hiện rõ kết quả khắc phục ở thời điểm hiện tại; có xác nhận các lỗ hổng đã được khắc phục thành công.

3.19.2.5. Kiểm tra rà soát biện pháp bảo vệ:

Sau đợt kiểm thử, đã điều chỉnh lại cấu hình tường lửa, IPS/IDS, WAF để chặn các kỹ thuật tấn công vừa được phát hiện.

3.19.2.6. Có báo cáo thực hiện rà soát các dấu hiệu tấn công trên toàn hệ thống, nội dung tối thiểu gồm: rà quét mã độc trên máy trạm/máy chủ, phân tích nhật ký hệ thống để tìm hành vi bất thường, rà soát các kết nối tới máy chủ điều khiển và ra lệnh từ xa; tần suất thực hiện tối thiểu 01 lần/năm.

3.19.3. Kết luận

3.19.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.19.2.

3.19.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.20. Nhóm đánh giá 2.2.20

3.20.1. Mục đích đánh giá

Đảm bảo hoạt động của hệ thống thông tin lưu trữ tài liệu điện tử và được duy trì ổn định, liên tục thông qua các hoạt động bảo trì phòng ngừa và khắc phục được quy định rõ ràng; ngăn chặn rủi ro mất mát hoặc sai lệch dữ liệu trong quá trình kiểm tra, sửa chữa và đảm bảo tính truy vết của mọi can thiệp kỹ thuật vào hệ thống.

3.20.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên quy trình bảo trì, nhật ký hệ thống, tài liệu khuyến nghị của nhà sản xuất và biên bản nghiệm thu bảo trì để xác minh các nội dung sau:

3.20.2.1. Chủ quản hệ thống thông tin đã ban hành và tuân thủ quy định về bảo trì hệ thống; nội dung quy định phải bao gồm cả hai loại hình: bảo trì phòng ngừa và bảo trì khắc phục.

3.20.2.2. Kiểm tra nhật ký hệ thống:

3.20.2.2.1. Chủ quản hệ thống thông tin đã thực hiện ghi nhật ký hoặc có sổ theo dõi bảo trì trong 12 tháng gần nhất.

3.20.2.2.2. Mọi hoạt động can thiệp (bao gồm thay thế ổ cứng, cập nhật phần mềm, bảo trì thiết bị, vá lỗi...) phải được ghi nhận đầy đủ, bao gồm thông tin về thời gian, người thực hiện, nội dung công việc và kết quả thực hiện.

3.20.2.3. Chủ quản hệ thống thông tin đã xây dựng và tuân thủ quy trình thử nghiệm thiết bị lưu trữ trước khi đưa vào vận hành hoặc sau khi sửa chữa.

3.20.2.4. Kiểm tra vật mang tin chuyên dụng và xác minh các ổ cứng/thiết bị dự phòng hoặc môi trường thử nghiệm riêng được sử dụng để chạy thử nghiệm.

3.20.2.5. Đối với các thiết bị gắn liền không thể tháo rời: Yêu cầu nhân sự mô tả hoặc chứng minh phương pháp thử nghiệm đảm bảo dữ liệu không bị ghi đè, bị xóa và không làm thay đổi dữ liệu gốc đang lưu trữ.

3.20.2.6. Đối chiếu tài liệu hãng sản xuất:

3.20.2.6.1. Có tài liệu hướng dẫn vận hành/bảo trì của nhà sản xuất thiết bị.

3.20.2.6.2. So sánh lịch bảo trì thực tế của đơn vị với khuyến nghị về chu kỳ bảo trì của hãng, đảm bảo việc bảo trì phòng ngừa được thực hiện theo khuyến nghị và đúng định kỳ.

3.20.3. Kết luận

3.20.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.20.2.

3.20.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trện.

3.21. Nhóm đánh giá 2.2.21

3.21.1. Mục đích đánh giá

Đảm bảo các hệ thống thông tin quan trọng từ cấp độ 3 trở lên có sẵn kịch bản và năng lực kỹ thuật để khôi phục hoạt động sau thảm họa; đảm bảo tính toàn vẹn của dữ liệu sau khi khôi phục; quá trình thực hiện phải được giám sát tự động.

3.21.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên hồ sơ đề xuất cấp độ hệ thống, kế hoạch khôi phục sau thảm họa, nhật ký hệ thống và biên bản diễn tập để xác minh các nội dung sau:

3.21.2.1. Chủ quản hệ thống thông tin đã xây dựng, ban hành và tuân thủ quy trình ứng cứu sự cố và khôi phục sau thảm họa. Nội dung quy trình mô tả các bước để khôi phục hệ thống từ bản sao lưu hoặo kích hoạt hệ thống dự phòng.

3.21.2.2. Kiểm tra giải pháp kỹ thuật:

Rà soát thiết kế hệ thống để đánh giá khả năng đáp ứng mục tiêu khôi phục; hệ thống có cơ chế sao chép đồng bộ hoặc các biện pháp bảo vệ dữ liệu tức thời để không bị mất dữ liệu.

3.21.2.3. Kiểm tra đối tượng khôi phục:

3.21.2.3.1. Có biên bản thử nghiệm khôi phục dữ liệu hoặc nhật ký hệ thống ghi nhận kết quả khôi phục, trong đó, trạng thái khôi phục được ghi nhận là "Thành công" và nằm trong khoảng thời gian quy định.

3.21.2.3.2. Dữ liệu chính: Tệp tin sau khi khôi phục có thể mở, đọc bình thường và có giá trị băm trùng khớp hoàn toàn với giá trị băm của tệp tin gốc.

3.21.2.3.3. Siêu dữ liệu: Các thuộc tính gắn liền với tài liệu như: người tạo, thời gian tạo, mức độ mật, loại tài liệu, từ khóa... đã khôi phục đầy đủ và chính xác, không bị mất hoặc sai lệch về định dạng.

3.21.2.3.4. Nhật ký hoạt động: Lịch sử truy vết của tài liệu được khôi phục kèm theo tài liệu.

3.21.2.4. Kiểm tra tính năng ghi nhật ký tự động, đáp ứng các yêu cầu:

3.21.2.4.1. Khi thực hiện một lệnh khôi phục, hệ thống tự động sinh ra nhật ký.

3.21.2.4.2. Nội dung nhật ký phải ghi rõ người thực hiện, thời gian bắt đầu, kết thúc, danh sách tệp được khôi phục và trạng thái.

3.21.2.5. Chủ quản hệ thống thông tin đã định kỳ phục hồi thử để kiểm tra khả năng khôi phục của bản sao lưu; thực hiện đánh giá lại hiệu quả của quy trình ứng cứu sự cố sau mỗi lần diễn tập.

3.21.3. Kết luận

3.21.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.21.2.

3.21.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

3.22. Nhóm đánh giá 2.2.22

3.22.1. Mục đích đánh giá

Đảm bảo hệ thống sử dụng nguồn thời gian chuẩn, chính xác và thống nhất trên toàn bộ các thành phần để phục vụ công tác ghi nhật ký, truy vết sự kiện và đảm bảo tính pháp lý cho tài liệu điện tử.

3.22.2. Phương pháp đánh giá

Người thực hiện đánh giá dựa trên hồ sơ thiết kế kỹ thuật, cấu hình hệ thống thực tế và kiểm tra dữ liệu nhật ký hệ thống để xác minh các nội dung sau:

3.22.2.1. Nguồn cấp thời gian phải là nguồn được cung cấp bởi tổ chức có thẩm quyền hoặc các nguồn quốc tế được công nhận tại Việt Nam, tuân thủ quy định pháp luật hiện hành. Thiết bị đã được đồng bộ trực tiếp với nguồn tin cậy đã công bố trong hồ sơ.

3.22.2.2. Hệ thống đã sử dụng chuẩn UTC làm gốc hoặc có cơ chế tự động quy đổi chính xác từ giờ địa phương sang UTC khi ghi nhận sự kiện.

3.22.2.3. Có định dạng trường thời gian trong cơ sở dữ liệu và nhật ký hệ thống.

3.22.2.4. Rà soát hồ sơ thiết kế kỹ thuật: Hệ thống có mô tả chi tiết về nguồn thời gian, giao thức đồng bộ (NTP, PTP) và chu kỳ cập nhật.

3.22.2.5. Hệ thống đã ghi lại trạng thái đồng bộ thành công/thất bại và độ lệch thời gian định kỳ. Đảm bảo độ lệch thời gian nằm trong ngưỡng cho phép của hệ thống và quy định hiện hành.

3.22.3. Kết luận

3.22.3.1. Đáp ứng: Khi có đầy đủ các nội dung tối thiểu được liệt kê tại mục 3.22.2.

3.22.3.2. Không đáp ứng: Nếu thiếu một trong các yêu cầu trên.

4. QUY ĐỊNH QUẢN LÝ

Việc quản lý, vận hành và công tác bảo đảm an ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử thuộc phạm vi điều chỉnh phải tuân thủ các yêu cầu tại Quy chuẩn này và các quy định của pháp luật về an ninh mạng, lưu trữ.

5. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

5.1. Cơ quan, tổ chức, cá nhân liên quan có trách nhiệm thực hiện các quy định của Quy chuẩn này và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định hiện hành.

5.2. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an các tỉnh, thành phố có trách nhiệm tổ chức triển khai, hướng dẫn cho các hệ thống thông tin lưu trữ tài liệu điện tử theo Quy chuẩn này.

5.3. Cục Khoa học, chiến lược và lịch sử Công an chịu trách nhiệm tổ chức phổ biến Quy chuẩn này cho tổ chức, cá nhân có liên quan theo quy định của pháp luật.

6. TỔ CHỨC THỰC HIỆN

6.1. Quy chuẩn kỹ thuật này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2026.

6.2. Hệ thống thông tin lưu trữ tài liệu điện tử đã được xây dựng đáp ứng các quy định pháp luật khác trước khi Quy chuẩn này được ban hành vẫn được phép hoạt động bình thường; kể từ khi Quy chuẩn có hiệu lực, đối với hệ thống cấp độ 3, 4, 5 phải đáp ứng các quy định tại Quy chuẩn này trong 12 tháng, đối với hệ thống cấp độ 1, 2 phải đáp ứng các quy định tại Quy chuẩn này trong 18 tháng.

6.3. Trong trường hợp các văn bản quy phạm pháp luật quy định tại Quy chuẩn này có sự thay đổi, bổ sung hoặc được thay thế thì thực hiện theo các văn bản mới.

6.4. Trong quá trình triển khai thực hiện Quy chuẩn này, nếu có vấn đề phát sinh, vướng mắc, các tổ chức và cá nhân có liên quan phản ánh bằng văn bản về Bộ Công an (qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để được hướng dẫn, giải quyết.