BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 708 /BTTTT-CATTT V/v sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH	*Hà Nội, ngày 02 tháng 03 năm 2024*

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

Căn cứ Nghị định số 48/2022/NĐ-CP ngày 26/7/2022 của Chính phủ về việc Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

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

Căn cứ Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ quy định về Quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;

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

Căn cứ Quyết định số 749/QĐ-TTg ngày 03/6/2020 của Thủ tướng Chính phủ phê duyệt Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030;

Căn cứ Quyết định số 942/QĐ-TTg ngày 15/6/2021 của Thủ tướng Chính phủ phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021-2025, định hướng đến năm 2030;

Căn cứ Quyết định số 06/QĐ-TTg ngày 06/01/2022 của Thủ tướng Chính phủ phê duyệt Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030;

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

Căn cứ Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc Quy định chi tiết và hướng dẫn một số điều của Nghị

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

Căn cứ Thông tư số 19/2023/TT-BTTTT ngày 25/12/2023 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Căn cứ Công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0).

Nhằm đồng bộ, thống nhất nội dung về hướng dẫn về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH với các văn bản quy phạm pháp luật hiện hành, tạo điều kiện thuận lợi cho các bộ, ngành, địa phương triển khai công tác bảo đảm an toàn, an ninh mạng, Bộ Thông tin và Truyền thông sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Mục 7 Công văn số 1552/BTTTT-THH và được hướng dẫn cụ thể tại Công văn này.

Trong quá trình tổ chức thực hiện, nếu có vướng mắc, đề nghị Quý Cơ quan phản ánh về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn giải quyết.

Đầu mối liên hệ: Ông Phạm Tuấn An, Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông, số điện thoại: 0888133359, thư điện tử: anpt@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thủ tướng Chính phủ (để b/c);
- Phó Thủ tướng Chính phủ Trần Hồng Hà (để b/c);
- Phó Thủ tướng Chính phủ Trần Lưu Quang (để b/c);
- Đại tướng, Bộ trưởng Bộ Công an Tô Lâm;
- Bộ trưởng Nguyễn Mạnh Hùng (để b/c);
- Thượng tướng, Thứ trưởng Bộ Công an Nguyễn Duy Ngọc;
- Thứ trưởng Phạm Đức Long;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở TTTT các tỉnh, TP trực thuộc TW;
- Lưu: VT, CATTT. PQM.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Phạm Đức Long

Phụ lục
HƯỚNG DẪN YÊU CẦU VỀ BẢO ĐẢM AN TOÀN, AN NINH MẠNG PHỤC VỤ TRIỂN KHAI ĐỀ ÁN 06
(Kèm theo Công văn số /BTTTT-CATTT Ngày tháng năm 2024 của Bộ Thông tin và Truyền thông)

1. Yêu cầu chung

Các hệ thống thông tin thuộc đối tượng áp dụng theo Công văn số 1552/BTTTT-THH ngày 26/4/2022 về việc hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0) cần đáp ứng các yêu cầu an toàn, an ninh mạng trước khi thực hiện kết nối, bao gồm:

a) Hồ sơ đề xuất cấp độ (HSĐXCĐ) của hệ thống thông tin được phê duyệt theo quy định.

b) Phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đã phê duyệt được triển khai đầy đủ và đáp ứng các yêu cầu an toàn cấp độ 3 trở lên, theo quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP, Điều 9, Điều 10 Thông tư số 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

c) Được kiểm tra, đánh giá an toàn, an ninh mạng bởi các cơ quan, đơn vị chức năng của Bộ Công an, Bộ Quốc phòng và Bộ Thông tin và Truyền thông trước khi kết nối, chia sẻ dữ liệu hoặc khi có thay đổi về thiết kế hệ thống; trường hợp các hệ thống thông tin có yêu cầu kết nối với Cơ sở dữ liệu quốc gia về dân cư đã được kết nối với nền tảng định danh và xác thực điện tử mà không có thay đổi về thiết kế hệ thống thì không phải kiểm tra, đánh giá an toàn, an ninh mạng. Nội dung kiểm tra, đánh giá tối thiểu bao gồm:

- Kiểm tra, đánh giá việc thiết lập cấu hình bảo mật trên thiết bị hệ thống, máy chủ, ứng dụng và cơ sở dữ liệu đáp ứng các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ;

- Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống đối với thiết bị hệ thống, máy chủ và ứng dụng;

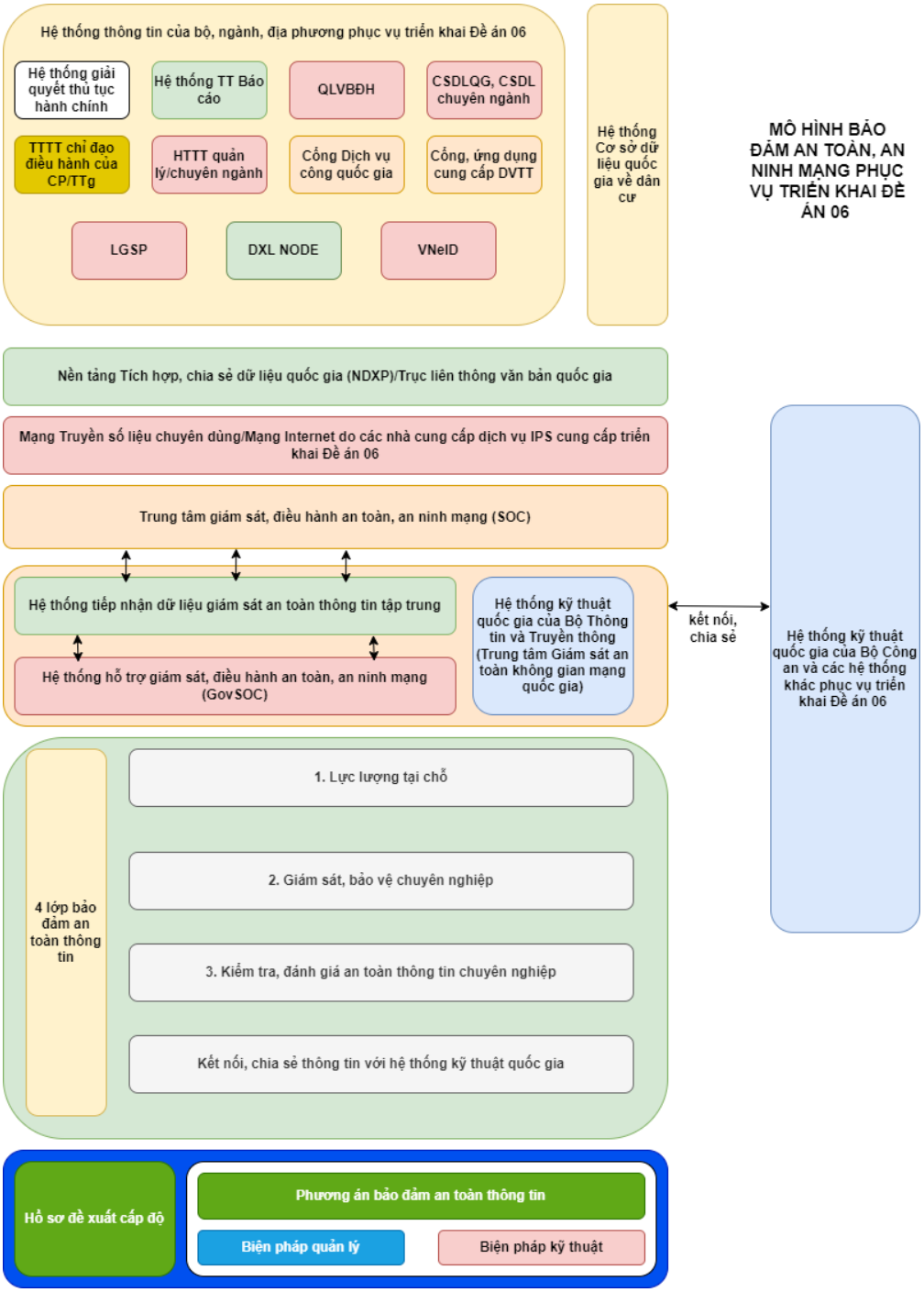
- Kiểm tra, đánh giá an toàn mã nguồn đối với phần mềm nội bộ;

- Kiểm tra, đánh giá an toàn, an ninh đối với thiết bị, phần cứng.

d) Trường hợp hệ thống thông tin kết nối qua Mạng truyền số liệu chuyên dùng cần đáp ứng thêm các yêu cầu về an toàn thông tin được quy định tại Quyết

định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước; Thông tư số 19/2023/TT-BTTTT ngày 25/12/2023 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước.

2. Mô hình tham chiếu bảo đảm an toàn, an ninh mạng



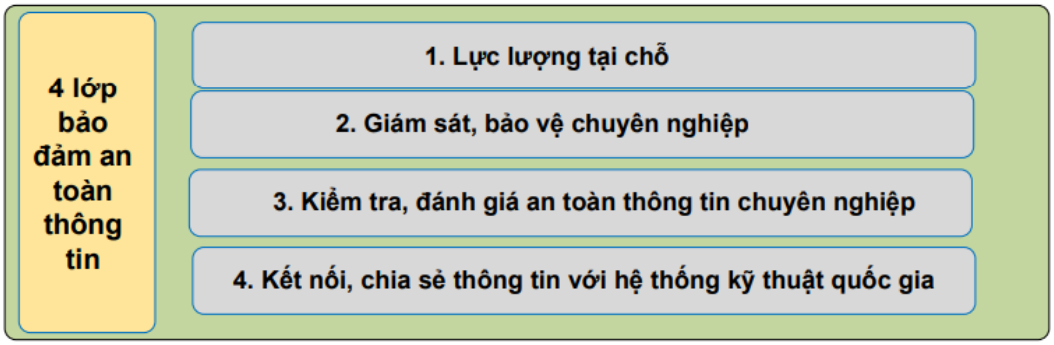
Hình vẽ 1: Mô hình tham chiếu bảo đảm an toàn, an ninh mạng

Mô hình tham chiếu bảo đảm an toàn, an ninh mạng bao gồm các thành phần: (1) Mô hình tổ chức "04 lớp" bảo đảm an toàn thông tin; (2) Mô hình tham chiếu về biện pháp quản lý an toàn thông tin; (3) Mô hình tham chiếu biện pháp kỹ thuật bảo đảm an toàn thông tin; (4) Mô hình tham chiếu về giải pháp, công nghệ; (5) Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng.

Bộ Thông tin và Truyền thông thiết lập hệ thống tiếp nhận dữ liệu giám sát an toàn thông tin tập trung để tiếp nhận dữ liệu chia sẻ từ bộ, ngành, địa phương. Dữ liệu giám sát sẽ được chia sẻ trực tiếp cho hệ thống kỹ thuật quốc gia của Bộ Công an và các hệ thống thông tin khác (theo đề nghị) phục vụ triển khai Đề án 06.

Đối với các hệ thống thông tin quan trọng về an ninh quốc gia, chủ quản hệ thống thông tin thiết lập chia sẻ dữ liệu giám sát an toàn, an ninh mạng về Trung tâm An ninh mạng quốc gia.

3. Mô hình bảo đảm an toàn thông tin theo mô hình 4 lớp



Hình vẽ 2: Mô hình bảo đảm an toàn thông tin theo mô hình 4 lớp

Lớp 1: Lực lượng tại chỗ Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về an toàn thông tin (ATTT) mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng.

Lớp 2: Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp Tự thực hiện giám sát, ứng cứu sự cố ATTT mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn/thuê tổ chức, doanh nghiệp có đủ năng lực để thực hiện cung cấp dịch vụ giám sát, ứng cứu sự cố, bảo vệ ATTT mạng.

Lớp 3: Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ Lựa chọn/thuê tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá ATTT mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật; Đối với các hệ thống thông tin cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền

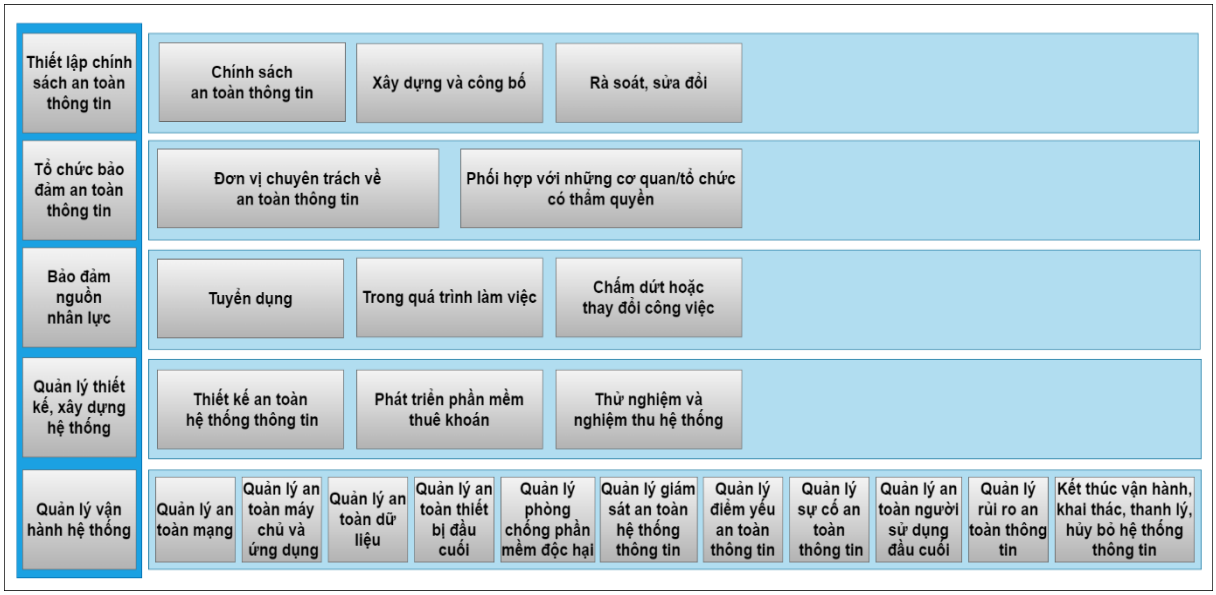
thông để tổng hợp, báo cáo Thủ tướng Chính phủ; Đối với hệ thống thông tin quan trọng quốc gia (cấp độ 5), định kỳ 06 tháng một lần thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông hàng năm để tổng hợp, báo cáo Thủ tướng Chính phủ.

Lớp 4: Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia Kết nối, chia sẻ thông tin giám sát an toàn thông tin với Hệ thống kỹ thuật quốc gia của Bộ Thông tin và Truyền thông (Trung tâm Giám sát an toàn không gian mạng quốc gia); và cung cấp các dải địa chỉ IP Public của các hệ thống thông tin trong cơ quan, tổ chức nhà nước thuộc phạm vi quản lý.

Thực hiện bảo đảm an toàn thông tin theo mô hình 4 lớp theo hướng dẫn của Bộ Thông tin và Truyền thông.

4. Mô hình tham chiếu về biện pháp quản lý an toàn thông tin

Mô hình tham chiếu về biện pháp quản lý an toàn thông tin theo cấp độ.



Hình vẽ 3: Mô hình các yêu cầu về quản lý an toàn thông tin

Các yêu cầu cụ thể được xác định dựa vào cấp độ của hệ thống thông tin tương ứng cần bảo vệ và được chia ra làm 05 nhóm: (1) Thiết lập chính sách an toàn thông tin, (2) Tổ chức bảo đảm an toàn thông tin, (3) Bảo đảm nguồn nhân lực, (4) Quản lý thiết kế, xây dựng hệ thống, (5) Quản lý vận hành hệ thống.

5. Mô hình tham chiếu biện pháp kỹ thuật bảo đảm an toàn thông tin

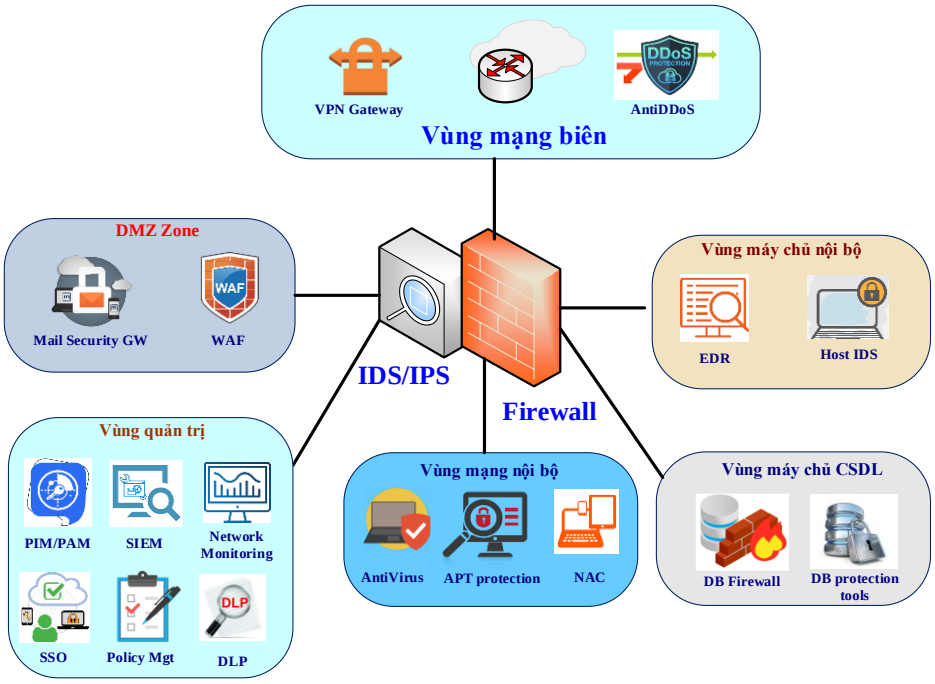
Mô hình tham chiếu biện pháp kỹ thuật bảo đảm an toàn thông tin theo cấp độ.

Hình vẽ 4: Mô hình yêu cầu về kỹ thuật đảm bảo an toàn thông tin

Các yêu cầu cụ thể được xác định dựa vào cấp độ của hệ thống thông tin tương ứng cần bảo vệ và được chia làm 04 nhóm: (1) Bảo đảm an toàn mạng, (2) Bảo đảm an toàn máy chủ, (3) Bảo đảm an toàn ứng dụng, (4) Bảo đảm an toàn dữ liệu.

6. Mô hình tham chiếu về giải pháp, công nghệ

Các Sản phẩm cụ thể được phân chia làm 08 nhóm, bao gồm: (1) Sản phẩm an toàn cho thiết bị đầu cuối; (2) Sản phẩm an toàn lớp mạng; (3) Sản phẩm an toàn lớp ứng dụng; (4) Sản phẩm bảo vệ dữ liệu; (5) Nhóm giải pháp định hướng phát triển theo hình thức cung cấp dịch vụ; (6) Sản phẩm trình duyệt; (7) Sản phẩm nền tảng tích hợp, chia sẻ dữ liệu (8) Sản phẩm nền tảng điện toán đám mây phục vụ chính phủ điện tử.



Hình vẽ 5: Mô hình tham chiếu về giải pháp và công nghệ

7. Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng

Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng (SOC) bao gồm 03 thành phần cơ bản:

Hình vẽ 6: Mô hình Trung tâm điều hành an toàn, an ninh mạng SOC

7.1. Công nghệ

Công nghệ, giải pháp kỹ thuật được sử dụng trong SOC cần phải đáp ứng yêu cầu kỹ thuật theo quy định tại Điều 5, khoản 1 Thông tư số 31/2017/TT-BTTTT (trường hợp văn bản được điều chỉnh, bổ sung hoặc thay thế thì thực hiện theo nội dung được điều chỉnh, bổ sung, hoặc thay thế) đáp ứng bao gồm nhưng không giới hạn các chức năng sau:

a) Chức năng quản trị: Chức năng phân tích tương quan (Correlation); Chức năng lọc (Filters); Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert).

b) Chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng; nhận log trực tiếp qua các giao thức mạng như: Syslog, Netflow, SNMP và các giao thức có chức năng tương đương theo thiết kế của từng hãng cụ thể. Giao thức truyền, nhận log qua môi trường mạng cần hỗ trợ chức năng mã hóa dữ liệu, nén dữ liệu; tải các tệp tin log theo các định dạng khác nhau lên hệ thống để chuẩn hóa và phân tích.

c) Yêu cầu về chức năng giám sát hệ thống: (1) Giám sát lớp mạng là việc thu thập, quản lý và giám sát các sự kiện từ các thiết bị mạng, thiết bị bảo mật như: Router, Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT...; (2) Giám sát lớp máy chủ là việc thu thập, quản lý và giám sát các sự kiện từ các máy chủ hệ thống (cả máy chủ vật lý và ảo hóa) trên các nền tảng khác nhau như: Windows, Linux, Unix…; (3) Giám sát lớp ứng dụng là việc thu thập, quản lý và giám sát các sự kiện từ các ứng dụng như: Ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP,

VPN, Proxy Server…; Ứng dụng cung cấp dịch vụ: Web, Mail, FPT, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL ...; (4) Giám sát lớp thiết bị đầu cuối là việc thu thập, quản lý và giám sát các sự kiện từ các thiết bị như: Máy tính người sử dụng, máy in, máy fax, IP Phone, IP Camera…; (5) Giám sát trên đường truyền là việc thu thập, quản lý và giám sát các sự kiện từ: Điểm giám sát biên tại giao diện kết nối của thiết bị định tuyến biên với các mạng bên ngoài; điểm giám sát tại mỗi vùng mạng của hệ thống.

d) Yêu cầu về lưu trữ: Yêu cầu lưu trữ đối với hệ thống quản lý tập trung cần bảo đảm thời gian tối thiểu để lưu trữ nhật ký hệ thống căn cứ vào cấp độ (Điều 10 Thông tư số 12/2022/TT-BTTTT) của hệ thống thông tin được triển khai giám sát, bảo vệ, cụ thể: Hệ thống thông tin cấp độ 1 hoặc cấp độ 2 là 01 tháng; Hệ thống thông tin cấp độ 3 là 03 tháng; Hệ thống thông tin cấp độ 4 là 06 tháng; Hệ thống cấp độ 5 là 12 tháng.

đ) Chức năng mở rộng: Quản lý điểm yếu an toàn thông tin; Quản lý quy trình nghiệp vụ xử lý sự cố an toàn thông tin; Tích hợp, tổng hợp và phân tích thông tin từ hệ thống Threat Intelligence; Tự động tương tác với thiết bị mạng và máy chủ để ngăn chặn tấn công; Hỗ trợ và tích hợp các công nghệ Big data & Machine learning, Kill-chain, Advanced malware analysis, AI.

7.2. Quy trình

Quy trình trong một hệ thống SOC cơ bản bao gồm 02 nhóm quy trình: quy trình quản lý, vận hành hệ thống và quy trình giám sát bảo vệ các hệ thống cần được bảo vệ như dưới đây.

a) Quy trình quản lý, vận hành bảo đảm an toàn thông tin cho hệ thống SOC

Các quy định, quy trình liên quan đến quản lý, vận hành hoạt động bình thường của hệ thống giám sát là các quy định, quy trình nhằm bảo đảm hệ thống giám sát hoạt động ổn định, có tính chịu lỗi cao và sẵn sàng khôi phục lại trạng thái bình thường khi xảy ra sự cố. Các quy định, quy trình cần tối thiểu bao gồm các nội dung: Khởi động và tắt hệ thống giám sát; Thay đổi cấu hình và các thành phần của hệ thống giám sát; Quy trình xử lý các sự cố liên quan đến hoạt động của hệ thống giám sát; Quy trình sao lưu, dự phòng cấu hình hệ thống và log của hệ thống; Quy trình bảo trì, nâng cấp hệ thống giám sát; Quy trình khôi phục hệ thống sau sự cố.

b) Quy trình giám sát, bảo vệ hệ thống thông tin: Giám sát quản lý các sự kiện và cảnh báo an toàn thông tin; Xử lý sự cố an toàn thông tin; Tối ưu cảnh báo: Tối ưu cảnh báo trên hệ thống giám sát để tăng hiệu quả của việc vận hành, giảm thiểu tối đa cảnh báo sai; Điều tra, phân tích các nguy cơ mất an toàn thông tin.

7.3. Con người

Đơn vị vận hành hệ thống SOC cần tổ chức và bố trí nhân sự thực hiện quản lý, vận hành hệ thống và giám sát an toàn thông tin, bao gồm các nhóm sau: Nhóm quản lý vận hành hệ thống giám sát; Nhóm theo dõi và cảnh báo; Nhóm xử lý sự cố; Nhóm điều tra, phân tích.

8. Danh mục phương án, thiết bị tối thiểu phục vụ bảo đảm an toàn, an ninh mạng

STT	Yêu cầu	Phương án đáp ứng
Cấp độ 3		
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng Sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 3 có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP yêu cầu Hệ thống sử dụng Sản phẩm VPN. 2. Các hệ thống thông tin cấp độ 3 có loại hình khác có thể sử dụng chức năng VPN được tích hợp trên tường lửa. 3. Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Minh chứng Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa được cấu hình trên Hệ thống thực.
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng Sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc Sản phẩm Phòng, chống xâm nhập lớp mạng	1. Đối với hệ thống thông tin cấp độ 3 có thể sử dụng Tường lửa tích hợp chức năng phòng, chống xâm nhập hoặc sử dụng Sản phẩm phòng, chống xâm nhập chuyên dụng. 2. Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập

		đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Minh chứng Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSĐXCĐ.
3	Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với các hệ thống thông tin cấp độ 3 được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP Yêu cầu sử dụng Sản phẩm Tường lửa ứng dụng web. Sản phẩm Tường lửa ứng dụng web phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa ứng dụng web đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Tường lửa ứng dụng web được cấu hình để bảo vệ đầy đủ các ứng dụng được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống cấp độ 3 không yêu cầu bắt buộc sử dụng Sản phẩm Tường lửa ứng dụng web thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Không để máy chủ ứng dụng web lộ mặt trực tiếp ngoài Internet mà phải thông qua Máy chủ đại diện (Reverse proxy) và có kiểm soát truy cập và phòng chống xâm nhập giữa máy chủ đại diện và máy chủ ứng dụng web. - Thiết lập cấu hình tăng cường bảo mật cho máy chủ Reverse proxy, cài đặt phần mềm phòng, chống phần mềm độc hại. - Thiết lập cấu hình tường lửa trên máy chủ Reverse proxy. - Kiểm tra, đánh giá an toàn thông tin cho máy chủ Reverse proxy.
4	Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị	1. Đối với hệ thống thông tin cấp độ 3 yêu cầu các thiết bị mạng chính trong hệ thống đều có thiết bị dự phòng nóng và cấu hình để thực hiện chức năng cân bằng tải, dự phòng nóng cho nhau. Các thiết bị mạng chính tối thiểu bao gồm: Thiết bị

	chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có)	chuyển mạch trung tâm hoặc tương đương; Thiết bị tường lửa trung tâm; Tường lửa ứng dụng web; Hệ thống lưu trữ tập trung; Tường lửa cơ sở dữ liệu (nếu có). (Đối với Hệ thống lưu trữ tập trung yêu cầu thiết bị chuyển mạch được trang bị theo cặp. Thiết bị lưu trữ phải được phân tách 02 vùng logic độc lập) 2. Có sơ đồ thiết kế vật lý để minh chứng các thiết bị có thiết bị dự phòng. 3. Có cấu hình của các thiết bị mạng chính để chứng minh chức năng cân bằng tải và dự phòng nóng.
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng Sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 3 là hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu. Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa cơ sở dữ liệu đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Tường lửa cơ sở dữ liệu được cấu hình để bảo vệ đầy đủ các cơ sở dữ liệu được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 3 không yêu cầu bắt buộc sử dụng Sản phẩm Tường lửa cơ sở dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để toàn

		bộ hoạt động liên quan đến CSDL được quản lý trên Hệ thống Quản lý và phân tích sự kiện an toàn thông tin – SIEM. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để định kỳ tự động thực hiện sao lưu dự phòng cơ sở dữ liệu trên hệ thống lưu trữ độc lập. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để kiểm soát truy cập cơ sở dữ liệu được sao lưu dự phòng trên hệ thống lưu trữ độc lập.
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương	1. Đối với hệ thống thông tin cấp độ 3 sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng. Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng phải đáp ứng tối thiểu các yêu cầu sau: Minh chứng chức năng phòng, chống mã độc trên môi trường mạng được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 3 không sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng Sản phẩm phòng, chống xâm nhập có tích hợp chức năng phòng, chống mã độc trên môi trường mạng. - Sử dụng các giải pháp khác (nếu có) cho phép phát hiện kết nối từ các máy trong mạng đến các địa chỉ độc hại, phát hiện truy vấn tên miền độc hại và các dấu hiệu mã độc mà có thể được phát hiện thông qua phân tích gói tin trên mạng.
7	Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống	1. Đối với các hệ thống thông tin cấp độ 3 là hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP

	tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP	Yêu cầu sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ. Dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ phải đáp ứng một trong hai yêu cầu sau: - Trường hợp sử dụng dịch vụ, yêu cầu có hợp đồng cung cấp dịch vụ. - Trường hợp sử dụng Sản phẩm Phòng, chống tấn công từ chối dịch vụ, yêu cầu minh chứng chức năng Phòng, chống tấn công từ chối dịch vụ được cấu hình để bảo vệ hệ thống. 2. Đối với các hệ thống thông tin cấp độ 3 không yêu cầu bắt buộc sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng chức năng phòng, chống tấn công từ chối dịch vụ được tích hợp trên các thiết bị bảo mật. - Có cam kết của tối thiểu 01 nhà cung cấp dịch vụ về việc hỗ trợ xử lý tấn công từ chối dịch vụ khi hệ thống bị tấn công.
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP (Chỉ áp dụng đối với hệ thống thư điện tử trực tiếp kết nối)	1. Đối với hệ thống Thư điện tử cấp độ 3, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử. Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử phải đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. 2. Đối với các Hệ thống thư điện tử cấp độ 3 khác không yêu cầu bắt buộc sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều

		hành máy chủ thư điện tử để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành máy chủ và ứng dụng thư điện tử.
9	Có phương án quản lý truy cập lớp mạng; sử dụng Sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 3 là hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Quản lý truy cập lớp mạng. Sản phẩm Quản lý truy cập lớp mạng phải đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý truy cập lớp mạng đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 3 không yêu cầu bắt buộc sử dụng Sản phẩm Quản lý truy cập lớp mạng thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Thiết lập cấu hình bảo mật trên thiết bị chuyển mạch lớp 2 cho phép phát hiện và quản lý truy cập mạng lớp 2 đối với các thiết bị kết nối vào hệ thống. - Thiết lập cấu hình nhật ký hệ thống trên thiết bị lớp 2 để quản lý được thông tin kết nối của các thiết bị vào hệ thống trên hệ thống Quản lý và phân tích sự kiện an toàn thông tin – SIEM.
10	Có phương án giám sát hệ thống thông tin tập trung	1. Đối với các hệ thống thông tin cấp độ 3, yêu cầu phương án sử dụng giám sát được trạng thái hoạt động của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ. 2. Trạng thái giám sát tối thiểu bao gồm các thông tin hiệu năng của CPU, RAM, Storage và các giao diện mạng.
11	Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng Sản phẩm Quản lý và phân tích sự kiện	1. Đối với các hệ thống thông tin cấp độ 3 sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin.

	an toàn thông tin hoặc Sản phẩm tương đương	Yêu cầu đối với Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng các yêu cầu tối thiểu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Quản lý và phân tích sự kiện an toàn thông tin của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 3 sử dụng Sản phẩm tương đương đáp ứng tối thiểu các yêu cầu sau: - Có chức năng quản trị: Chức năng phân tích tương quan (Correlation); Chức năng lọc (Filters), Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert). - Có chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng.
12	Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và Sản phẩm quản lý lưu trữ tập trung	Đối với các hệ thống thông tin cấp độ 3, yêu cầu hệ thống có hệ thống lưu trữ và Sản phẩm để phục vụ việc quản lý lưu trữ tập trung. Yêu cầu đối với Sản phẩm quản lý lưu trữ tập trung đáp ứng các yêu cầu tối thiểu sau: - Tối thiểu các dữ liệu sau yêu cầu được lưu trữ trên hệ thống quản lý tập trung: Ảnh hệ điều hành của các máy chủ trong hệ thống, tệp tin cấu hình các thiết bị hệ thống, cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có). - Dữ liệu phải được sao lưu, dự phòng tối thiểu trên 02 thiết bị vật lí lưu trữ khác nhau.
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính	1. Đối với các hệ thống thông tin cấp độ 3, yêu cầu hệ thống sử dụng Sản phẩm Phòng, chống mã

	người dùng, sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung	độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối. Yêu cầu đối với Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối phải đáp ứng tối thiểu các yêu cầu sau: - Có chức năng quản lý tập trung. - Minh chứng toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt Sản phẩm và được quản lý trên hệ thống quản lý tập trung.
14	Có phương án phòng, chống thất thoát dữ liệu; sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 3 có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu. Bảo đảm tối thiểu các máy chủ cơ sở dữ liệu, máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu. 2. Đối với các hệ thống thông tin cấp độ 3 không yêu cầu bắt buộc sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng chức năng phòng, chống thất thoát dữ liệu được tích hợp trên thiết bị/sản phẩm bảo mật sử dụng trong hệ thống (nếu có). - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho các máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu.

15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Yêu cầu có kết nối dự phòng, Hệ thống duy trì tối thiểu 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.
16	Có phương án bảo đảm an toàn cho mạng không dây (Yêu cầu này chỉ áp dụng trong trường hợp hệ thống Mạng không dây kết nối trực tiếp với hệ thống Cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử)	Sử dụng giải pháp bảo đảm an toàn cho mạng không dây theo phương án thuyết minh trong HSĐXCĐ.
Cấp độ 4		
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng Sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước	1. Đối với hệ thống thông tin cấp độ 4 có xử lý thông tin bí mật nhà nước yêu cầu Hệ thống sử dụng Sản phẩm VPN. 2. Các hệ thống thông tin cấp độ 4 có loại hình khác có thể sử dụng chức năng VPN được tích hợp trên tường lửa. 3. Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Minh chứng Sản phẩm/chức năng VPN tích hợp trên Thiết bị Tường lửa được cấu hình trên Hệ thống thực.
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng Sản phẩm Tường lửa có tích hợp chức năng	1. Đối với hệ thống thông tin cấp độ 4 có thể sử dụng Tường lửa tích hợp chức năng phòng, chống xâm nhập hoặc sử dụng Sản phẩm phòng, chống xâm nhập chuyên dụng.

	phòng, chống xâm nhập hoặc Sản phẩm Phòng, chống xâm nhập lớp mạng	2. Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Minh chứng Sản phẩm/Tường lửa tích hợp chức năng phòng, chống xâm nhập được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSĐXCĐ.
3	Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2 Điều 10 Nghị định 85/2016/NĐ-CP hoặc Hệ thống Trung tâm dữ liệu, điện toán đám mây, Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, Kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP	1. Đối với các hệ thống thông tin cấp độ 4 được quy định tại khoản 2 Điều 10 Nghị định 85/2016/NĐ-CP hoặc Hệ thống Trung tâm dữ liệu, điện toán đám mây, Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, Kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Tường lửa ứng dụng web. Sản phẩm Tường lửa ứng dụng web phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa ứng dụng web đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Tường lửa ứng dụng web được cấu hình để bảo vệ đầy đủ các ứng dụng được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 4 không yêu cầu bắt buộc sử dụng Sản phẩm Tường lửa ứng dụng web thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Không để máy chủ ứng dụng web lộ mặt trực tiếp ngoài Internet mà phải thông qua Máy chủ đại diện (Reverse proxy) và có kiểm soát truy cập và phòng chống xâm nhập giữa máy chủ đại diện và máy chủ ứng dụng web. - Thiết lập cấu hình tăng cường bảo mật cho máy chủ Reverse proxy, cài đặt phần mềm phòng, chống phần mềm độc hại.

		- Thiết lập cấu hình tường lửa trên máy chủ Reverse proxy. - Kiểm tra, đánh giá an toàn thông tin cho máy chủ Reverse proxy.
4	Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có)	1. Đối với hệ thống thông tin cấp độ 4 yêu cầu các thiết bị mạng chính trong hệ thống đều có thiết bị dự phòng nóng và cấu hình để thực hiện chức năng cân bằng tải, dự phòng nóng cho nhau. Các thiết bị mạng chính tối thiểu bao gồm: Thiết bị chuyển mạch trung tâm hoặc tương đương; Thiết bị tường lửa trung tâm; Tường lửa ứng dụng web; Hệ thống lưu trữ tập trung; Tường lửa cơ sở dữ liệu (nếu có). (Đối với Hệ thống lưu trữ tập trung yêu cầu thiết bị chuyển mạch được trang bị theo cặp. Thiết bị lưu trữ phải được phân tách 02 vùng logic độc lập) 2. Có sơ đồ thiết kế vật lý để minh chứng các thiết bị có thiết bị dự phòng. 3. Có cấu hình của các thiết bị mạng chính để chứng minh chức năng cân bằng tải và dự phòng nóng.
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng Sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống Cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 4 là hệ thống Cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu. Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa cơ sở dữ liệu đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Tường lửa cơ sở dữ liệu được cấu hình để bảo vệ đầy đủ các cơ sở dữ liệu được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 4 không yêu cầu bắt buộc sử dụng Sản phẩm Tường lửa cơ

		sở dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để toàn bộ hoạt động liên quan đến CSDL được quản lý trên Hệ thống Quản lý và phân tích sự kiện an toàn thông tin – SIEM. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để định kỳ tự động thực hiện sao lưu dự phòng cơ sở dữ liệu trên hệ thống lưu trữ độc lập. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để kiểm soát truy cập cơ sở dữ liệu được sao lưu dự phòng trên hệ thống lưu trữ độc lập.
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Sản phẩm Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương	1. Đối với hệ thống thông tin cấp độ 4 sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng. Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng phải đáp ứng tối thiểu yêu cầu sau: Minh chứng chức năng phòng, chống mã độc trên môi trường mạng được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 4 không sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng Sản phẩm phòng, chống xâm nhập có tích hợp chức năng phòng, chống mã độc trên môi trường mạng.

		- Sử dụng các giải pháp khác (nếu có) cho phép phát hiện kết nối từ các máy trong mạng đến các địa chỉ độc hại, phát hiện truy vấn tên miền độc hại và các dấu hiệu mã độc mà có thể được phát hiện thông qua phân tích gói tin trên mạng.
7	Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống thông tin được quy định tại khoản 2 Điều 10 Nghị định 85/2016/NĐ-CP hoặc Hệ thống Trung tâm dữ liệu, điện toán đám mây, Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, Kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP	1. Đối với các hệ thống thông tin cấp độ 4 được quy định tại khoản 2 Điều 10 Nghị định 85/2016/NĐ-CP hoặc Hệ thống Trung tâm dữ liệu, điện toán đám mây, Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, Kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ. Dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ phải đáp ứng một trong hai yêu cầu sau: - Trường hợp sử dụng dịch vụ, yêu cầu có hợp đồng cung cấp dịch vụ. - Trường hợp sử dụng Sản phẩm Phòng, chống tấn công từ chối dịch vụ, yêu cầu minh chứng chức năng Phòng, chống tấn công từ chối dịch vụ được cấu hình để bảo vệ hệ thống 2. Đối với các hệ thống thông tin cấp độ 4 không yêu cầu bắt buộc sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng chức năng phòng, chống tấn công từ chối dịch vụ được tích hợp trên các thiết bị bảo mật. - Có cam kết của tối thiểu 01 nhà cung cấp dịch vụ về việc hỗ trợ xử lý tấn công từ chối dịch vụ khi hệ thống bị tấn công.
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng Sản phẩm Bảo đảm an toàn	Đối với Hệ thống thông tin cấp độ 4 là Hệ thống thư điện tử yêu cầu sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử. Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử phải đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Bảo đảm an

	thông tin cho hệ thống thư điện tử (Chỉ áp dụng đối với hệ thống thư điện tử trực tiếp kết nối)	toàn thông tin cho hệ thống thư điện tử đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ.
9	Có phương án quản lý truy cập lớp mạng; sử dụng Sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 4 là hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Quản lý truy cập lớp mạng. Sản phẩm Quản lý truy cập lớp mạng phải đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý truy cập lớp mạng đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 4 không yêu cầu bắt buộc sử dụng Sản phẩm Quản lý truy cập lớp mạng thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Thiết lập cấu hình bảo mật trên thiết bị chuyển mạch lớp 2 cho phép phát hiện và quản lý truy cập mạng lớp 2 đối với các thiết bị kết nối vào hệ thống. - Thiết lập cấu hình nhật ký hệ thống trên thiết bị lớp 2 để quản lý được thông tin kết nối của các thiết bị vào hệ thống trên hệ thống Quản lý và phân tích sự kiện an toàn thông tin – SIEM.
10	Có phương án giám sát hệ thống thông tin tập trung sử dụng Sản phẩm Giám sát hệ thống thông tin tập trung	Đối với hệ thống thông tin cấp độ 4, yêu cầu sử dụng Sản phẩm Giám sát hệ thống thông tin tập trung. Sản phẩm Giám sát hệ thống thông tin tập trung phải đáp ứng các yêu cầu tối thiểu sau: - Sản phẩm sử dụng giám sát được trạng thái hoạt động của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ. - Trạng thái giám sát tối thiểu bao gồm các thông tin hiệu năng của CPU, RAM, Storage và các giao diện mạng.

11	Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc Sản phẩm tương đương	1. Đối với các hệ thống thông tin cấp độ 4 sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin. Yêu cầu đối với Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng các yêu cầu tối thiểu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Quản lý và phân tích sự kiện an toàn thông tin của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 4 sử dụng Sản phẩm tương đương đáp ứng tối thiểu các yêu cầu sau: - Có bản quyền hoặc giấy phép sử dụng, văn bản/tài liệu minh chứng quyền sử dụng hợp pháp đối với phần mềm còn thời hạn sử dụng trong vòng tối thiểu 03 tháng tại thời điểm đánh giá. - Có chức năng quản trị: Chức năng phân tích tương quan (Correlation); Chức năng lọc (Filters); Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert). - Có chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng.
12	Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và Sản phẩm quản lý lưu trữ tập trung	Đối với các hệ thống thông tin cấp độ 4, yêu cầu hệ thống có hệ thống lưu trữ và Sản phẩm để phục vụ việc quản lý lưu trữ tập trung. Yêu cầu đối với Sản phẩm quản lý lưu trữ tập trung đáp ứng các yêu cầu tối thiểu sau: - Tối thiểu các dữ liệu sau yêu cầu được lưu trữ trên hệ thống quản lý tập trung: Ảnh hệ điều hành của các máy chủ trong hệ thống, tệp tin cấu hình

		các thiết bị hệ thống, cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có). - Dữ liệu phải được sao lưu, dự phòng tối thiểu trên 02 thiết bị vật lí lưu trữ khác nhau.
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung	Đối với các hệ thống thông tin cấp độ 4, yêu cầu hệ thống sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối. Yêu cầu đối với Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối phải đáp ứng tối thiểu các yêu cầu sau: - Có chức năng quản lý tập trung. - Minh chứng toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt Sản phẩm và được quản lý trên hệ thống quản lý tập trung.
14	Có phương án phòng, chống thất thoát dữ liệu; sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống Cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 4 có xử lý thông tin bí mật nhà nước hoặc hệ thống Cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu. Bảo đảm tối thiểu các máy chủ cơ sở dữ liệu, máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu. 2. Đối với các hệ thống cấp độ 4 không yêu cầu bắt buộc sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng chức năng phòng, chống thất thoát dữ liệu được tích hợp trên thiết bị/sản phẩm bảo mật sử dụng trong hệ thống (nếu có). - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng.

		- Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho các máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu.
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Yêu cầu có kết nối dự phòng, Hệ thống duy trì tối thiểu 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.
16	Có phương án bảo đảm an toàn cho mạng không dây. Yêu cầu này chỉ áp dụng trong trường hợp hệ thống Mạng không dây là đối tượng kết nối vào hệ thống Cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	Sử dụng giải pháp bảo đảm an toàn cho mạng không dây theo phương án thuyết minh trong HSĐXCĐ.
17	Có phương án quản lý tài khoản đặc quyền, sử dụng Sản phẩm Quản lý tài khoản đặc quyền	Đối với các hệ thống thông tin cấp độ 4, yêu cầu sử dụng Sản phẩm Quản lý tài khoản đặc quyền và minh chứng Sản phẩm Quản lý tài khoản đặc quyền được cấu hình trên Hệ thống thực.
Cấp độ 5		
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng Sản phẩm Mạng riêng ảo	Đối với Hệ thống thông tin cấp độ 5, yêu cầu Hệ thống sử dụng Sản phẩm VPN. Sản phẩm VPN phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm VPN đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Minh chứng Sản phẩm được cấu hình trên Hệ thống thực.

2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng Sản phẩm Phòng, chống xâm nhập lớp mạng	Đối với hệ thống thông tin cấp độ 5, yêu cầu Hệ thống sử dụng Sản phẩm phòng, chống xâm nhập lớp mạng. Sản phẩm phòng, chống xâm nhập lớp mạng phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm phòng, chống xâm nhập lớp mạng đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Minh chứng Sản phẩm phòng, chống xâm nhập lớp mạng được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSĐXCĐ.
3	Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng Sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 5 theo quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Tường lửa ứng dụng web. Sản phẩm Tường lửa ứng dụng web phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa ứng dụng web đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Tường lửa ứng dụng web được cấu hình để bảo vệ đầy đủ các ứng dụng được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 5 không yêu cầu bắt buộc sử dụng Sản phẩm Tường lửa ứng dụng web thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Không để máy chủ ứng dụng web lộ mặt trực tiếp ngoài Internet mà phải thông qua Máy chủ đại diện (Reverse proxy) và có kiểm soát truy cập và phòng chống xâm nhập giữa máy chủ đại diện và máy chủ ứng dụng web. - Thiết lập cấu hình tăng cường bảo mật cho máy chủ Reverse proxy, cài đặt phần mềm phòng, chống phần mềm độc hại.

		- Thiết lập cấu hình tường lửa trên máy chủ Reverse proxy. - Kiểm tra, đánh giá an toàn thông tin cho máy chủ Reverse proxy.
4	Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng	1. Đối với hệ thống thông tin cấp độ 5 yêu cầu các thiết bị mạng trong hệ thống đều có thiết bị dự phòng nóng và cấu hình để thực hiện chức năng cân bằng tải, dự phòng nóng cho nhau. 2. Yêu cầu thiết bị chuyển mạch được trang bị theo cặp. Thiết bị lưu trữ phải được phân tách 02 vùng logic độc lập. 3. Có sơ đồ thiết kế vật lý để minh chứng các thiết bị có thiết bị dự phòng. 4. Có cấu hình của các thiết bị mạng để chứng minh chức năng cân bằng tải và dự phòng nóng.
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng Sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống thông tin được quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 5 được quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu. Sản phẩm Tường lửa cơ sở dữ liệu hoặc Sản phẩm bảo vệ cơ sở dữ liệu phải đáp ứng tối thiểu các yêu cầu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Tường lửa cơ sở dữ liệu đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Tường lửa cơ sở dữ liệu được cấu hình để bảo vệ đầy đủ các cơ sở dữ liệu được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 5 không yêu cầu bắt buộc sử dụng Sản phẩm Tường lửa cơ sở dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng.

		- Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để toàn bộ hoạt động liên quan đến CSDL được quản lý trên Hệ thống Quản lý và phân tích sự kiện an toàn thông tin – SIEM. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để định kỳ tự động thực hiện sao lưu dự phòng cơ sở dữ liệu trên hệ thống lưu trữ độc lập. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình hệ thống để kiểm soát truy cập cơ sở dữ liệu được sao lưu dự phòng trên hệ thống lưu trữ độc lập.
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Sản phẩm Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương	1. Đối với hệ thống thông tin cấp độ 5 sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng. Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng phải minh chứng chức năng phòng, chống mã độc trên môi trường mạng được cấu hình để giám sát, bảo vệ đầy đủ các vùng mạng trong hệ thống được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 5 không sử dụng Sản phẩm Tường lửa lớp mạng có tích hợp chức năng phòng, chống mã độc trên môi trường mạng thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng Sản phẩm phòng, chống xâm nhập có tích hợp chức năng phòng, chống mã độc trên môi trường mạng. - Sử dụng các giải pháp khác (nếu có) cho phép phát hiện kết nối từ các máy trong mạng đến các địa chỉ độc hại, phát hiện truy vấn tên miền độc hại và các dấu hiệu mã độc mà có thể được phát hiện thông qua phân tích gói tin trên mạng.

7	Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống thông tin được quy định tại khoản 2, khoản 3 Điều 11 Nghị định 85/2016/NĐ-CP	1. Đối với các hệ thống thông tin cấp độ 5 được quy định tại khoản 2, khoản 3 Điều 11 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ. Dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ phải đáp ứng một trong hai yêu cầu sau: - Trường hợp sử dụng dịch vụ, yêu cầu có hợp đồng cung cấp dịch vụ. - Trường hợp sử dụng Sản phẩm Phòng, chống tấn công từ chối dịch vụ, yêu cầu minh chứng chức năng phòng, chống tấn công từ chối dịch vụ được cấu hình để bảo vệ hệ thống. 2. Đối với các hệ thống thông tin cấp độ 5 không yêu cầu bắt buộc sử dụng dịch vụ của doanh nghiệp hoặc Sản phẩm Phòng, chống tấn công từ chối dịch vụ thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng chức năng phòng, chống tấn công từ chối dịch vụ được tích hợp trên các thiết bị bảo mật. - Có cam kết của tối thiểu 01 nhà cung cấp dịch vụ về việc hỗ trợ xử lý tấn công từ chối dịch vụ khi hệ thống bị tấn công.
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử, sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử. (Chỉ áp dụng đối với hệ thống thư điện tử trực tiếp kết nối)	Đối với Hệ thống thư điện tử cấp độ 5 yêu cầu sử dụng Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử. Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử phải đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ.
9	Có phương án quản lý truy cập lớp mạng, sử dụng Sản phẩm Quản lý truy cập lớp mạng	Đối với hệ thống thông tin cấp độ 5, yêu cầu sử dụng Sản phẩm Quản lý truy cập lớp mạng. Sản phẩm Quản lý truy cập lớp mạng đáp ứng tối thiểu yêu cầu sau: Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý truy cập lớp mạng đáp ứng đầy đủ

		các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ.
10	Có phương án giám sát hệ thống thông tin tập trung sử dụng Sản phẩm Giám sát hệ thống thông tin tập trung	Đối với hệ thống thông tin cấp độ 5, yêu cầu sử dụng Sản phẩm Giám sát hệ thống thông tin tập trung. Sản phẩm Giám sát hệ thống thông tin tập trung phải đáp ứng các yêu cầu tối thiểu sau: - Sản phẩm sử dụng giám sát được trạng thái hoạt động của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ. - Trạng thái giám sát tối thiểu bao gồm các thông tin hiệu năng của CPU, RAM, Storage và các giao diện mạng.
11	Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc Sản phẩm tương đương	1. Đối với các hệ thống thông tin cấp độ 5 sử dụng Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin. Yêu cầu đối với Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng các yêu cầu tối thiểu sau: - Thiết lập cấu hình bảo mật cho Sản phẩm Quản lý và phân tích sự kiện an toàn thông tin đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ. - Quản lý và phân tích sự kiện an toàn thông tin của toàn bộ thiết bị, máy chủ và ứng dụng được thuyết minh trong HSĐXCĐ. 2. Đối với các hệ thống thông tin cấp độ 5 sử dụng Sản phẩm tương đương đáp ứng tối thiểu các yêu cầu sau: - Có chức năng quản trị: Chức năng phân tích tương quan (Correlation); Chức năng lọc (Filters); Tạo các luật (Rules), Chức năng hiển thị (Dashboards), Chức năng cảnh báo và báo cáo (Alerts and Reports), Chức năng cảnh báo thời gian thực (Real Time Alert). - Có chức năng nhận log: Cho phép nhận log từ các nguồn với nhiều định dạng khác nhau từ các thiết bị mạng, máy chủ và ứng dụng; định dạng, chuẩn hóa log nhận được theo các trường thông tin tùy biến theo nhu cầu sử dụng.

12	Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và Sản phẩm quản lý lưu trữ tập trung	Đối với các hệ thống thông tin cấp độ 5, yêu cầu hệ thống có hệ thống lưu trữ và Sản phẩm để phục vụ việc quản lý lưu trữ tập trung. Yêu cầu đối với Sản phẩm quản lý lưu trữ tập trung đáp ứng các yêu cầu tối thiểu sau: - Tối thiểu các dữ liệu sau yêu cầu được lưu trữ trên hệ thống quản lý tập trung: Ảnh hệ điều hành của các máy chủ trong hệ thống, tệp tin cấu hình các thiết bị hệ thống, cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có). - Dữ liệu phải được sao lưu, dự phòng tối thiểu trên 02 thiết bị vật lí lưu trữ khác nhau.
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung	Đối với các hệ thống thông tin cấp độ 5, yêu cầu hệ thống sử dụng Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối. Yêu cầu đối với Sản phẩm Phòng, chống mã độc và/hoặc Sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối phải đáp ứng tối thiểu các yêu cầu sau: - Có chức năng quản lý tập trung. - Minh chứng toàn bộ các máy chủ, máy trạm trong hệ thống được cài đặt Sản phẩm và được quản lý trên hệ thống quản lý tập trung.
14	Có phương án phòng, chống thất thoát dữ liệu; sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP	1. Đối với hệ thống thông tin cấp độ 5 có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu. Sản phẩm Phòng, chống thất thoát dữ liệu phải Bảo đảm tối thiểu các máy chủ cơ sở dữ liệu, máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu. 2. Đối với các hệ thống thông tin cấp độ 5 không yêu cầu bắt buộc sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau:

		- Sử dụng chức năng phòng, chống thất thoát dữ liệu được tích hợp trên thiết bị/sản phẩm bảo mật sử dụng trong hệ thống (nếu có). - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho các máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu.
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Yêu cầu có kết nối dự phòng, Hệ thống duy trì tối thiểu 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.
16	Có phương án bảo đảm an toàn cho mạng không dây. Yêu cầu này chỉ áp dụng trong trường hợp hệ thống Mạng không dây là đối tượng kết nối vào hệ thống Cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	Sử dụng giải pháp bảo đảm an toàn cho mạng không dây theo phương án thuyết minh trong HSĐXCĐ.
17	Có phương án quản lý tài khoản đặc quyền, sử dụng Sản phẩm Quản lý tài khoản đặc quyền	Đối với các hệ thống thông tin cấp độ 5, yêu cầu sử dụng Sản phẩm Quản lý tài khoản đặc quyền và minh chứng Sản phẩm Quản lý tài khoản đặc quyền được cấu hình trên Hệ thống thực.
18	Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30 km	Đối với hệ thống thông tin cấp độ 5 yêu cầu phải có hệ thống dự phòng. Hệ thống dự phòng cách hệ thống chính tối thiểu 30km và ở 02 vị trí khác nhau

19	Có phương án dự phòng cho kết nối mạng giữa các hệ thống chính và dự phòng	Yêu cầu có kết nối vật lý cho kết nối mạng theo hai hướng khác nhau giữa hệ thống chính và hệ thống dự phòng.