



Ký bởi: Sở Công thương (M)
Thời gian ký: 11/09/2026 21:12:40

ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN
SỞ CÔNG THƯƠNG

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 2
PHẦN MỀM QUẢN LÝ AN TOÀN THỰC PHẨM
NGÀNH CÔNG THƯƠNG TỈNH HƯNG YÊN

MỤC LỤC

CĂN CỨ LẬP HỒ SƠ.....	3
THUẬT NGỮ, TỪ VIẾT TẮT.....	4
DANH MỤC HÌNH VẼ, BẢNG BIỂU	4
PHẦN I. THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN	5
1. Thông tin chủ quản hệ thống thông tin	5
2. Thông tin đơn vị vận hành hệ thống thông tin	5
3. Mô tả phạm vi, quy mô của hệ thống.....	5
4. Mô tả hiện trạng kiến trúc hệ thống	7
PHẦN II. THUYẾT MINH VỀ VIỆC ĐỀ XUẤT CẤP ĐỘ.....	11
1. Danh mục hệ thống thông tin và cấp độ đề xuất	11
2. Thuyết minh chi tiết	11
3. Nhận diện sơ bộ nguy cơ, rủi ro an ninh mạng	12
PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN NINH MẠNG	14
1. Các nội dung của phương án bảo đảm an ninh mạng	14
2. Phương án đáp ứng yêu cầu cơ bản về quản lý	14
3. Phương án đáp ứng yêu cầu cơ bản về kỹ thuật.....	14
4. Đối với các yêu cầu chưa đáp ứng	15
PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU CƠ BẢN VỀ QUẢN LÝ ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2.....	16
I. THIẾT LẬP CHÍNH SÁCH AN NINH MẠNG	16
II. TỔ CHỨC BẢO ĐẢM AN NINH MẠNG.....	16
III. BẢO ĐẢM NGUỒN NHÂN LỰC.....	18
IV. QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG	19
V. QUẢN LÝ VẬN HÀNH HỆ THỐNG	21
VI. PHƯƠNG ÁN QUẢN LÝ RỦI RO AN NINH MẠNG.....	28
VII. PHƯƠNG ÁN KẾT THÚC VẬN HÀNH, KHAI THÁC, THANH LÝ, HỦY BỎ HỆ THỐNG THÔNG TIN	28
PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU CƠ BẢN VỀ KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2	30
1. BẢO ĐẢM AN TOÀN MẠNG	30
2. BẢO ĐẢM AN TOÀN MÁY CHỦ	34
3. BẢO ĐẢM AN TOÀN ỨNG DỤNG.....	37
4. BẢO ĐẢM AN TOÀN DỮ LIỆU	38
PHẦN IV. CAM KẾT CỦA ĐƠN VỊ VẬN HÀNH.....	40

CĂN CỨ LẬP HỒ SƠ

- Luật An ninh mạng số 116/2025/QH15 ngày 10 tháng 12 năm 2025;
- Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;
- Tiêu chuẩn quốc gia TCVN 14423:2026 An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản;
- Quyết định số 10/2025/QĐ-UBND ngày 01 tháng 7 năm 2025 của Ủy ban nhân dân tỉnh Hưng Yên ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Công Thương tỉnh Hưng Yên;
- Tài liệu thiết kế chi tiết chức năng hệ thống thông tin quản lý an toàn thực phẩm ngành Công Thương tỉnh Hưng Yên (gửi kèm Hồ sơ);
- Quyết định số 209/QĐ-SCT ngày 11/9/2026 của Giám đốc Sở Công Thương tỉnh Hưng Yên ban hành Quy chế bảo đảm an ninh mạng đối với các hệ thống thông tin cấp độ 2 do Sở Công Thương tỉnh Hưng Yên quản lý, vận hành (sau đây gọi tắt là Quy chế bảo đảm an ninh mạng).

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1	ANM	An ninh mạng
2	ATTP	An toàn thực phẩm
3	CSDL	Cơ sở dữ liệu
4	HTTT	Hệ thống thông tin
5	HSĐXCĐ	Hồ sơ đề xuất cấp độ
6	DMZ	Vùng mạng trung gian giữa mạng nội bộ và mạng ngoài
7	WAF	Tường lửa ứng dụng web
8	MFA	Xác thực đa yếu tố
9	NĐ 331	Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ
10	TCVN 14423:2026	Tiêu chuẩn quốc gia TCVN 14423:2026 An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản
11	Trung tâm ĐMST và CDS	Trung tâm Đổi mới sáng tạo và Chuyển đổi số
12	Quy chế bảo đảm ANM	Quy chế bảo đảm an ninh mạng đối với các hệ thống thông tin cấp độ 2 do Sở Công Thương tỉnh Hưng Yên quản lý, vận hành, ban hành kèm theo Quyết định số 209/QĐ-SCT ngày 11/9/2026

DANH MỤC HÌNH VẼ, BẢNG BIỂU

Hình 1. Cấu trúc lô-gic của hệ thống

Hình 2. Kết nối vật lý của hệ thống

Bảng 1. Danh mục thiết bị mạng sử dụng trong hệ thống

Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

Bảng 4. Danh mục hệ thống thông tin và cấp độ đề xuất

Bảng 5. Nhận diện sơ bộ nguy cơ, rủi ro an ninh mạng

PHẦN I. THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

(Theo khoản 3 Điều 22 ND 331)

1. Thông tin chủ quản hệ thống thông tin

- Tên chủ quản: Ủy ban nhân dân tỉnh Hưng Yên.
- Quy định chức năng, nhiệm vụ, quyền hạn: Luật Tổ chức chính quyền địa phương số 72/2025/QH15 ngày 16/6/2025.
- Người đại diện: Ông Nguyễn Mạnh Quyền; chức vụ: Chủ tịch Ủy ban nhân dân tỉnh Hưng Yên.
- Địa chỉ: Số 10, đường Chùa Chuông, phường Phố Hiến, tỉnh Hưng Yên.
- Thông tin liên hệ: Điện thoại 0221.3863823; thư điện tử hungyen@chinhphu.vn.

2. Thông tin đơn vị vận hành hệ thống thông tin

- Tên đơn vị vận hành: Sở Công Thương tỉnh Hưng Yên.
- Quy định chức năng, nhiệm vụ, quyền hạn: Quyết định số 10/2025/QĐ-UBND ngày 01/7/2025 của Ủy ban nhân dân tỉnh Hưng Yên.
- Người đại diện: Ông Vũ Thanh Vân; chức vụ: Giám đốc Sở
- Địa chỉ: Đường Quảng Trường, phường Phố Hiến, tỉnh Hưng Yên.
- Thông tin liên hệ: Điện thoại 02213 862.779; thư điện tử soct@hungyen.gov.vn.
- Đầu mối an ninh mạng của Sở Công Thương: Văn phòng Sở Công Thương. Đầu mối: Ông Nguyễn Xuân Tuấn, Chánh Văn phòng Sở; điện thoại 0982.193.006; thư điện tử nxtuan@hungyen.gov.vn.
- Bộ phận trực tiếp quản trị, vận hành: Phòng Quản lý Công nghiệp, Sở Công Thương tỉnh Hưng Yên (Quyết định số 35/QĐ-UBND ngày 25/7/2025 quy định chức năng, nhiệm vụ, cơ cấu tổ chức và mối quan hệ công tác của Văn phòng Sở và các phòng chuyên môn thuộc Sở Công Thương tỉnh Hưng Yên). Đầu mối: Ông Trần Minh Đức, Trưởng phòng; điện thoại 0973.130.481; thư điện tử tmduc@hungyen.gov.vn.
- Người lập hồ sơ: Ông Vũ Quang Tùng, Phó Trưởng phòng Quản lý Công nghiệp; điện thoại: 0989.067.717.

3. Mô tả phạm vi, quy mô của hệ thống

- Tên hệ thống thông tin: Phần mềm quản lý an toàn thực phẩm ngành Công Thương tỉnh Hưng Yên; địa chỉ truy cập: <https://attp.hungyen.gov.vn>.
- Phạm vi: Hệ thống phục vụ công tác quản lý, theo dõi nội bộ của cơ quan nhà nước trong lĩnh vực an toàn thực phẩm ngành Công Thương tỉnh Hưng Yên; thu thập thông tin về tình hình sản xuất, kinh doanh thực phẩm thuộc phạm vi quản lý và tạo lập cơ sở dữ liệu phục vụ công tác quản lý của Sở Công Thương. Hệ

thống không thực hiện chức năng tiếp nhận, xử lý, giải quyết và trả kết quả thủ tục hành chính trực tuyến cho tổ chức, cá nhân.

- Quy mô: Hệ thống được triển khai trên các máy chủ ảo đặt tại Trung tâm Đổi mới sáng tạo và Chuyển đổi số, quản lý bằng hệ thống quản lý máy ảo VMware vSphere Client, gồm Web Server tại vùng Application và Database Server tại vùng Database.

- Đối tượng sử dụng: Cán bộ, công chức ngành Công Thương tỉnh Hưng Yên, gồm cán bộ tại Sở Công Thương (vai trò quản trị) và cán bộ phụ trách an toàn thực phẩm tại các xã, phường trên địa bàn tỉnh (vai trò người sử dụng). Hiện có 104 tài khoản người sử dụng và 01 tài khoản quản trị nghiệp vụ trên ứng dụng (quản lý người dùng, đơn vị, vai trò, phân quyền) do Phòng Quản lý Công nghiệp quản lý. Sở Công Thương không được cấp tài khoản quản trị hệ điều hành máy chủ ảo và tài khoản quản trị ứng dụng có quyền thay đổi cấu hình.

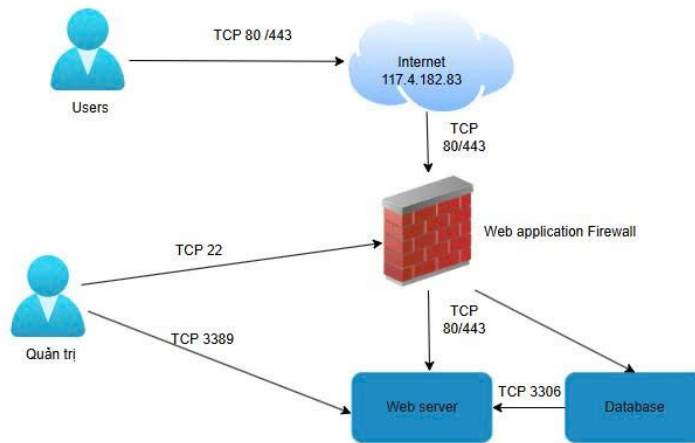
- Các phân hệ nghiệp vụ chính: quản lý cơ sở sản xuất, kinh doanh thực phẩm; theo dõi, thống kê kết quả giải quyết thủ tục hành chính về an toàn thực phẩm; thanh tra, kiểm tra; quản lý văn bản; báo cáo, thống kê; quản trị hệ thống (người dùng, đơn vị, vai trò, phân quyền, nhật ký).

- Hạ tầng triển khai: Hạ tầng mạng, thiết bị bảo mật, nền tảng ảo hóa, hệ thống lưu trữ và an ninh vật lý do Trung tâm Đổi mới sáng tạo và Chuyển đổi số đầu tư, quản lý, vận hành và được hệ thống sử dụng chung theo khoản 2 Điều 6 NĐ 331.

- Phân định trách nhiệm: Sở Công Thương chịu trách nhiệm tổ chức bảo đảm an ninh mạng đối với hệ thống trong phạm vi quản lý, vận hành của Sở, gồm phần mềm ứng dụng, dữ liệu nghiệp vụ, tài khoản và phân quyền người sử dụng. Đối với các thành phần hạ tầng dùng chung, máy chủ ảo và các thành phần thuộc phạm vi quản lý của Trung tâm Đổi mới sáng tạo và Chuyển đổi số, Sở Công Thương phối hợp thực hiện theo phạm vi trách nhiệm đã được phân công, thống nhất. Đối với thiết bị đầu cuối, Sở Công Thương quy định, hướng dẫn các yêu cầu bảo đảm an toàn khi truy cập hệ thống; người sử dụng và đơn vị quản lý thiết bị có trách nhiệm thực hiện.

4. Mô tả hiện trạng kiến trúc hệ thống

4.1. Mô hình lô-gic



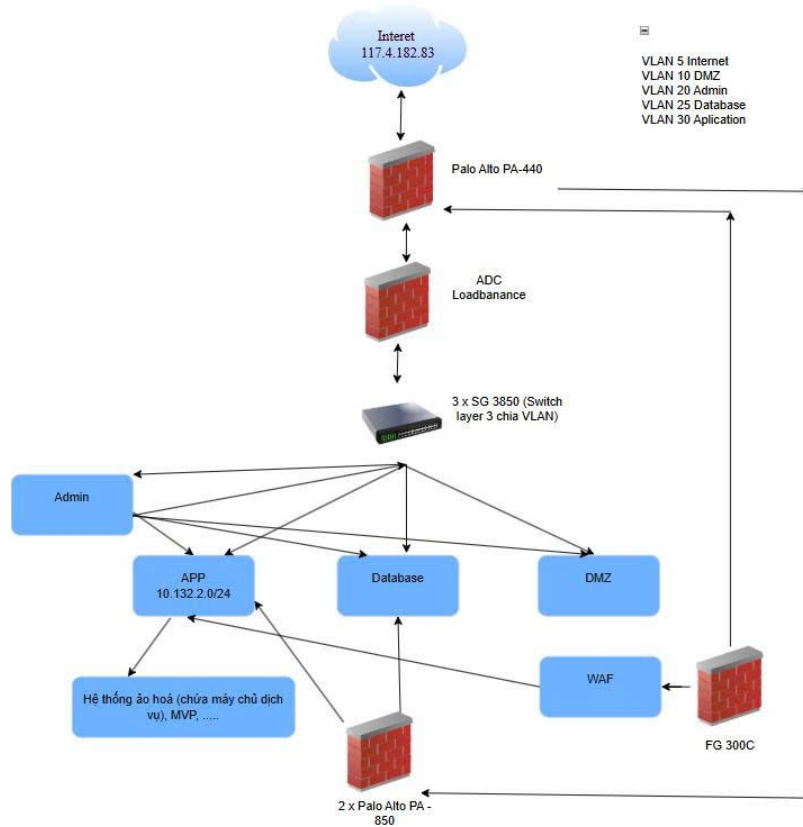
Hình 1. Cấu trúc lô-gic của hệ thống

Các vùng mạng được thiết kế như sau:

- Tường lửa (Firewall) để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.
- Vùng máy chủ Web Server: là các máy chủ triển khai hệ thống website.
- Vùng Database: là các máy chủ cơ sở dữ liệu của hệ thống, lưu trữ dữ liệu của hệ thống.

Người sử dụng truy cập hệ thống từ Internet (địa chỉ IP công khai 117.4.182.83) qua cổng TCP 80/443, đi qua tường lửa ứng dụng web (Web application Firewall) trước khi tới máy chủ Web server. Máy chủ Web server kết nối tới máy chủ cơ sở dữ liệu qua cổng TCP 3306. Người quản trị truy cập hệ thống qua các cổng quản trị TCP 22 và TCP 3389. Các cổng dịch vụ nêu trên theo Hình 1 do Trung tâm Đổi mới sáng tạo và Chuyển đổi số cung cấp.

4.2. Mô hình kết nối vật lý



Hình 2. Kết nối vật lý của hệ thống

Mô tả kết nối vật lý của hệ thống:

- Người dùng, người quản trị kết nối từ ngoài vào qua tường lửa đi vào máy chủ dịch vụ web bằng giao thức HTTP/HTTPS.
- Các máy chủ web khi truy nhập dữ liệu sẽ thông qua tường lửa truy xuất dữ liệu trên cụm Database Cluster.
- Kết nối từ Internet (117.4.182.83) đi qua tường lửa Palo Alto PA-440, thiết bị ADC Loadbalance và cụm 03 thiết bị chuyển mạch lớp 3 SG 3850 thực hiện chia VLAN.
- Hệ thống được phân tách thành các VLAN: VLAN 5 (Internet), VLAN 10 (DMZ), VLAN 20 (Admin), VLAN 25 (Database), VLAN 30 (Application).
- Vùng Application (10.132.2.0/24) chứa hệ thống ảo hóa triển khai các máy chủ dịch vụ của hệ thống.
- Truy cập giữa vùng Application và vùng Database được kiểm soát qua 02 thiết bị tường lửa Palo Alto PA-850.
- Tường lửa ứng dụng web (WAF) và thiết bị FG 300C bảo vệ, kiểm soát truy cập tại vùng DMZ.

4.3. Danh mục thiết bị sử dụng trong hệ thống

TT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Firewall Palo Alto PA-440	Vùng mạng nội bộ	Kiểm soát dữ liệu ra vào, ngăn chặn xâm nhập
2	Firewall ADC	Vùng mạng nội bộ	Bảo mật phòng ngừa tấn công, quản lý truy cập
3	FortiGate FG300	Vùng mạng nội bộ	Kiểm soát ứng dụng và nhận diện người dùng, ngăn chặn các mối đe dọa toàn diện
4	Palo Alto PA-850	Vùng mạng nội bộ	Bảo mật, kiểm soát truy cập vùng Application và Database
5	Switch SG 3850	Vùng mạng nội bộ	Chia VLAN, cấu hình đường truyền
6	WAF	Vùng mạng biên	Phòng chống lỗ hổng web, cấu hình SSL

Bảng 1. Danh mục thiết bị mạng sử dụng trong hệ thống

Các thiết bị nêu trên do Trung tâm Đổi mới sáng tạo và Chuyển đổi số đầu tư, quản lý, vận hành và cung cấp thông tin.

4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

TT	Tên dịch vụ	Máy chủ/Ứng dụng cài đặt/Vùng mạng/Hệ điều hành	Mục đích sử dụng
1	Phần mềm quản lý an toàn thực phẩm ngành Công Thương	Hệ thống quản lý máy ảo VMware vSphere Client. Web Server (máy ảo)/Cài đặt Web-App/Vùng Application/Windows Server 2019. Database Server (máy ảo)/Cài đặt SQL Server 2019/Vùng Database/Windows Server 2019	Cấu hình, quản lý phần mềm và cơ sở dữ liệu

Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

TT	Vùng mạng	IP Private	IP Public
1	Vùng DMZ	10.132.193.0/24	Không
2	Vùng máy chủ nội bộ (Application)	10.132.2.0/24	Không

TT	Vùng mạng	IP Private	IP Public
3	Vùng dữ liệu Database	10.132.195.0/24	Không
4	Vùng mạng biên	10.132.196.1	117.4.182.83

Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

PHẦN II. THUYẾT MINH VỀ VIỆC ĐỀ XUẤT CẤP ĐỘ

(Theo khoản 4 Điều 22 NĐ 331)

1. Danh mục hệ thống thông tin và cấp độ đề xuất

TT	Tên hệ thống thông tin	Loại hình hệ thống thông tin	Cấp độ đề xuất	Căn cứ đề xuất
1	Phần mềm quản lý an toàn thực phẩm ngành Công Thương tỉnh Hưng Yên	Hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức, có xử lý thông tin riêng, thông tin cá nhân của người sử dụng, không xử lý thông tin bí mật nhà nước	Cấp độ 2	Khoản 1 Điều 12 NĐ 331

Bảng 4. Danh mục hệ thống thông tin và cấp độ đề xuất

2. Thuyết minh chi tiết

2.1. Loại thông tin được xử lý

Theo khoản 1 Điều 9 NĐ 331, hệ thống xử lý các loại thông tin sau:

- Thông tin riêng: dữ liệu về tình hình sản xuất, kinh doanh thực phẩm của các cơ sở thuộc phạm vi quản lý, chỉ công khai cho nhóm đối tượng đã được xác định danh tính là cán bộ, công chức được cấp tài khoản.
- Thông tin cá nhân: họ tên, chức vụ, đơn vị công tác, số điện thoại, thư điện tử, tài khoản đăng nhập của người sử dụng; họ tên, số điện thoại của chủ cơ sở, người đại diện cơ sở sản xuất, kinh doanh thực phẩm.
- Hệ thống không xử lý thông tin công cộng và không xử lý thông tin bí mật nhà nước.

2.2. Loại hình hệ thống thông tin

Hệ thống được triển khai trên hạ tầng mạng có kết nối Internet nhằm tạo điều kiện cho cán bộ quản lý các cấp truy cập phục vụ công tác. Tính chất phục vụ nội bộ của hệ thống được thể hiện như sau:

- a) Đối tượng sử dụng: toàn bộ người sử dụng là cán bộ, công chức nhà nước được giao nhiệm vụ quản lý an toàn thực phẩm, thuộc Sở Công Thương và các xã, phường trên địa bàn tỉnh. Hệ thống không cấp tài khoản cho tổ chức, cá nhân ngoài cơ quan nhà nước.
- b) Phương thức truy cập: người dùng đăng nhập bằng tài khoản do Sở Công Thương cấp và quản lý; không có chức năng tự đăng ký tài khoản công khai.
- c) Mục đích: thu thập thông tin, tạo lập cơ sở dữ liệu phục vụ công tác quản lý nhà nước về an toàn thực phẩm của ngành Công Thương.

d) Phạm vi cung cấp: hệ thống không cung cấp dịch vụ trực tuyến cho tổ chức, cá nhân theo khoản 5 Điều 3 NĐ 331; không thực hiện chức năng tiếp nhận, xử lý, giải quyết và trả kết quả thủ tục hành chính trực tuyến cho tổ chức, cá nhân. Việc hệ thống được truy cập qua Internet là phương thức kỹ thuật để cán bộ các cấp truy cập từ xa, không làm thay đổi tính chất phục vụ nội bộ của hệ thống.

Do đó, hệ thống thuộc loại hình "Hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức" quy định tại điểm a khoản 2 Điều 9 NĐ 331.

2.3. Căn cứ đề xuất cấp độ

Khoản 1 Điều 12 NĐ 331 quy định: hệ thống thông tin cấp độ 2 là hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức và có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước. Hệ thống đáp ứng đồng thời các dấu hiệu nêu trên: phục vụ hoạt động nội bộ của cơ quan nhà nước (mục 2.2); có xử lý thông tin riêng và thông tin cá nhân của người sử dụng; không xử lý thông tin bí mật nhà nước (mục 2.1).

Kết luận: Hệ thống được đề xuất là hệ thống thông tin cấp độ 2 theo khoản 1 Điều 12 NĐ 331.

3. Nhận diện sơ bộ nguy cơ, rủi ro an ninh mạng

(Điểm c khoản 4 Điều 22 NĐ 331)

TT	Nguy cơ, rủi ro an ninh mạng chính	Mức độ	Ảnh hưởng dự kiến
1	Tấn công, khai thác lỗ hổng ứng dụng web	Cao	Lộ lọt, sửa đổi trái phép thông tin riêng và thông tin cá nhân
2	Chiếm đoạt tài khoản người sử dụng, tài khoản quản trị	Cao	Truy cập, khai thác trái phép dữ liệu; thao tác sai lệch dữ liệu nghiệp vụ
3	Lây nhiễm mã độc từ máy trạm, thiết bị đầu cuối	Trung bình	Mã hóa, phá hủy dữ liệu; gián đoạn hoạt động nghiệp vụ
4	Mất dữ liệu khi xảy ra sự cố	Trung bình	Mất dữ liệu nghiệp vụ, không bảo đảm tính liên tục
5	Gián đoạn hoạt động do sự cố hạ tầng dùng chung	Trung bình	Gián đoạn truy cập của cán bộ, công chức
6	Truy cập trái phép của cán bộ đã nghỉ việc, chuyển công tác	Thấp	Truy cập, khai thác trái phép dữ liệu sau khi chấm dứt nhiệm vụ

Bảng 5. Nhận diện sơ bộ nguy cơ, rủi ro an ninh mạng

Khi bị tấn công mạng hoặc gián đoạn hoạt động, hệ thống có thể làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân và gián đoạn công tác quản lý nhà

nước về an toàn thực phẩm trên địa bàn tỉnh, chưa gây hậu quả tới quốc phòng, an ninh quốc gia. Kết quả nhận diện phù hợp với cấp độ 2 được đề xuất.

PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN NINH MẠNG

(Theo khoản 6 Điều 22, Điều 29 và Điều 30 NĐ 331)

Phương án bảo đảm an ninh mạng đối với hệ thống thông tin cấp độ 2 được xây dựng đáp ứng các yêu cầu cơ bản quy định tại Điều 30 NĐ 331 và Mục 4 Tiêu chuẩn quốc gia TCVN 14423:2026. Theo khoản 2 Điều 30 NĐ 331, đây là các yêu cầu tối thiểu và không bao gồm các yêu cầu bảo đảm an ninh vật lý.

1. Các nội dung của phương án bảo đảm an ninh mạng

(Khoản 2 Điều 29 NĐ 331)

TT	Nội dung	Vị trí thuyết minh
a	Bảo đảm an ninh mạng trong thiết kế, xây dựng	Mục 4 Phần I; mục IV Phụ lục I; mục 1.1 Phụ lục II
b	Bảo đảm an ninh mạng trong quá trình vận hành	Mục V Phụ lục I; Phụ lục II
c	Kiểm tra, đánh giá an ninh mạng	Mục V.10 Phụ lục I
d	Quản lý rủi ro an ninh mạng	Mục VI Phụ lục I
đ	Giám sát an ninh mạng	Mục V.10 Phụ lục I
e	Dự phòng, ứng phó sự cố an ninh mạng, khôi phục sau thảm họa	Mục V.7, V.8 Phụ lục I
g	Kết thúc vận hành, khai thác, thanh lý, hủy bỏ	Mục VII Phụ lục I

2. Phương án đáp ứng yêu cầu cơ bản về quản lý

Theo khoản 3 Điều 30 NĐ 331, yêu cầu cơ bản về quản lý gồm 07 nhóm: a) thiết lập chính sách an ninh mạng; b) tổ chức bảo đảm an ninh mạng; c) bảo đảm nguồn nhân lực; d) quản lý thiết kế, xây dựng hệ thống; đ) quản lý vận hành hệ thống; e) phương án quản lý rủi ro an ninh mạng; g) phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

Thuyết minh chi tiết tại **Phụ lục I**. Các nội dung quản lý được cụ thể hóa tại Quy chế bảo đảm an ninh mạng ban hành kèm theo Quyết định số 209/QĐ-SCT ngày 11/9/2026 của Giám đốc Sở Công Thương tỉnh Hưng Yên, gửi kèm Hồ sơ theo khoản 7 Điều 30 NĐ 331.

3. Phương án đáp ứng yêu cầu cơ bản về kỹ thuật

Theo khoản 4 Điều 30 NĐ 331, yêu cầu cơ bản về kỹ thuật gồm 04 nhóm: a) bảo đảm an toàn mạng; b) bảo đảm an toàn máy chủ; c) bảo đảm an toàn ứng dụng; d) bảo đảm an toàn dữ liệu.

Thuyết minh chi tiết tại **Phụ lục II**. Phương án kỹ thuật được xây dựng trên cơ sở xem xét khả năng dùng chung các giải pháp bảo vệ đã được trang bị tại Trung tâm Đổi mới sáng tạo và Chuyển đổi số theo điểm a khoản 5 Điều 30 NĐ 331.

4. Đối với các yêu cầu chưa đáp ứng

Sở Công Thương xây dựng lộ trình khắc phục nội bộ đối với các nội dung còn chưa đáp ứng nêu tại Phụ lục I và Phụ lục II theo điều kiện thực tế của đơn vị, dự kiến hoàn thành trong thời hạn 06 tháng đối với các nội dung quản lý và 12 tháng đối với các nội dung kỹ thuật. Đây là lộ trình khắc phục nội bộ của đơn vị vận hành, không phải thời hạn gia hạn theo quy định.

Tiến độ và kết quả thực hiện được tổng hợp trong báo cáo định kỳ hằng năm theo Điều 35, Điều 36 NĐ 331.

PHỤ LỤC I
THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU CƠ BẢN VỀ QUẢN
LÝ ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2
(Khoản 3 Điều 30 NĐ 33/2017 và Mục 4 TCVN 14423:2026)

I. THIẾT LẬP CHÍNH SÁCH AN NINH MẠNG

I.1. Chính sách an ninh mạng

Yêu cầu	Xây dựng chính sách an ninh mạng bao gồm quản lý an toàn mạng, máy chủ, ứng dụng, dữ liệu và thiết bị đầu cuối; chính sách được người có thẩm quyền thông qua trước khi công bố áp dụng.
Hiện trạng	Đáp ứng. Quy chế bảo đảm an ninh mạng ban hành kèm theo Quyết định số 209/QĐ-SCT ngày 11/9/2026 của Giám đốc Sở Công Thương tỉnh Hưng Yên, áp dụng chung cho các hệ thống thông tin cấp độ 2 do Sở quản lý, vận hành; gửi kèm Hồ sơ.
Phương án	Quy chế bảo đảm an ninh mạng do Văn phòng Sở tham mưu, đã được Giám đốc Sở Công Thương ký ban hành và phổ biến tới công chức, người lao động của Sở và người sử dụng hệ thống.

I.2. Rà soát, sửa đổi chính sách

Yêu cầu	Định kỳ hoặc khi có thay đổi, chính sách an ninh mạng phải được kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật.
Hiện trạng	Đáp ứng về quy định. Khoản 2 Điều 24 Quy chế bảo đảm an ninh mạng quy định rà soát, cập nhật Quy chế tối thiểu 01 lần/năm hoặc khi có thay đổi. Việc thực hiện theo phân công tại Quy chế.
Phương án	Định kỳ tối thiểu 01 lần/năm hoặc khi có thay đổi về quy định pháp luật, chức năng, phạm vi, công nghệ triển khai hệ thống, Quy chế bảo đảm an ninh mạng được rà soát, cập nhật. Trong quá trình thực hiện, vướng mắc phát sinh được phản ánh về Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở xem xét sửa đổi, bổ sung.

II. TỔ CHỨC BẢO ĐẢM AN NINH MẠNG

II.1. Tổ chức đầu mối an ninh mạng

Yêu cầu	Bố trí bộ phận hoặc nhân sự chuyên trách về an ninh mạng phù hợp với cấp độ của hệ thống; bảo đảm tính độc lập phù
----------------	--

	hợp giữa hoạt động quản trị, vận hành và hoạt động bảo vệ an ninh mạng (điểm b khoản 1 Điều 31 NĐ 331; mục 4.13.1 TCVN 14423:2026). Đối với hệ thống cấp độ 2, việc bố trí nhân sự phụ trách đáp ứng yêu cầu này; không bắt buộc thành lập bộ phận chuyên trách riêng.
Hiện trạng	Đáp ứng về quy định. Điều 4 Quy chế bảo đảm an ninh mạng quy định Văn phòng Sở là đầu mối an ninh mạng của Sở; Giám đốc Sở phân công 01 công chức đầu mối và ít nhất 01 công chức dự phòng đối với quy trình ứng phó sự cố; phòng, đơn vị trực tiếp quản lý, vận hành thực hiện nhiệm vụ tác nghiệp, bảo đảm tính độc lập phù hợp giữa vận hành và bảo vệ an ninh mạng. Việc phân công cụ thể thực hiện theo Quy chế.
Phương án	1. Văn phòng Sở là đầu mối an ninh mạng của Sở; Phòng Quản lý Công nghiệp là phòng trực tiếp quản lý, vận hành hệ thống (khoản 2, khoản 4 Điều 4 Quy chế bảo đảm an ninh mạng). 2. Giám đốc Sở phân công 01 công chức đầu mối và ít nhất 01 công chức dự phòng đối với quy trình ứng phó sự cố an ninh mạng theo khoản 5 Điều 4 Quy chế. 3. Việc bố trí bộ phận hoặc nhân sự chuyên trách về an ninh mạng thực hiện theo quyết định của chủ quản hệ thống thông tin (khoản 1 Điều 31 NĐ 331, khoản 3 Điều 4 Quy chế).

II.2. Đầu mối liên hệ, phối hợp

Yêu cầu	Thiết lập và duy trì đầu mối liên hệ, phối hợp với cơ quan có thẩm quyền quản lý nhà nước về an ninh mạng và trong công tác hỗ trợ điều phối, ứng cứu sự cố; xác minh, cập nhật thông tin liên hệ hằng năm.
Hiện trạng	Đáp ứng. Danh sách đầu mối được lập, duy trì theo khoản 6 Điều 4 Quy chế bảo đảm an ninh mạng.
Phương án	1. Đầu mối của Sở Công Thương nêu tại mục 2 Phần I. 2. Đầu mối phối hợp gồm: Công an tỉnh Hưng Yên (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao), Trung tâm Đổi mới sáng tạo và Chuyển đổi số và đơn vị phát triển, bảo trì phần mềm. 3. Danh sách đầu mối được rà soát, cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi nhân sự.

II.3. Chế độ báo cáo

Yêu cầu	Thực hiện chế độ báo cáo định kỳ về công tác bảo đảm an ninh mạng và báo cáo sự cố an ninh mạng theo quy định.
Hiện trạng	Đáp ứng về quy định. Chế độ báo cáo được quy định tại Điều 22 Quy chế bảo đảm an ninh mạng; thực hiện đầy đủ từ kỳ báo cáo năm 2026. Việc thực hiện theo phân công tại Quy chế.
Phương án	1. Báo cáo định kỳ hằng năm theo Điều 35, Điều 36 NĐ 331 và Mẫu số 08 ban hành kèm NĐ 331; chốt số liệu từ ngày 15/12 năm trước đến ngày 14/12 của kỳ báo cáo; gửi chủ quản hệ thống thông tin trước ngày 20/12 hằng năm. 2. Báo cáo sự cố: khi phát hiện sự cố, Sở Công Thương báo cáo ngay chủ quản hệ thống thông tin và đơn vị chuyên trách về an ninh mạng để thực hiện trách nhiệm báo cáo theo điểm d khoản 2 Điều 31 NĐ 331. 3. Báo cáo định kỳ hoặc đột xuất theo yêu cầu của chủ quản hệ thống thông tin hoặc cơ quan có thẩm quyền theo khoản 6 Điều 33 NĐ 331.

III. BẢO ĐẢM NGUỒN NHÂN LỰC

III.1. Nhân sự và cam kết bảo mật

Yêu cầu	Nhân sự phụ trách vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, công nghệ thông tin; có cam kết bảo mật thông tin trong quá trình làm việc và sau khi nghỉ việc.
Hiện trạng	Đáp ứng về quy định. Yêu cầu về trình độ chuyên môn và cam kết bảo mật thông tin được quy định tại khoản 1, khoản 2 Điều 5 Quy chế bảo đảm an ninh mạng. Việc thực hiện theo phân công tại Quy chế.
Phương án	Công chức được phân công (kể cả kiêm nhiệm) vào vị trí làm về an ninh mạng có trình độ, chuyên ngành về công nghệ thông tin, an toàn thông tin phù hợp. Đối với vị trí tiếp xúc, quản lý dữ liệu quan trọng hoặc quản trị hệ thống, yêu cầu nhân sự ký cam kết bảo mật thông tin bằng văn bản, bao gồm cả sau khi nghỉ việc.

III.2. Đào tạo, nâng cao nhận thức

Yêu cầu	Có chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin; tiến hành đào tạo tối thiểu 01 lần/năm.
Hiện trạng	Đáp ứng về quy định. Quy định tại khoản 3 Điều 5 Quy chế

	bảo đảm an ninh mạng. Việc thực hiện theo phân công tại Quy chế.
Phương án	Hàng năm, Sở Công Thương tổ chức hoặc cử công chức tham gia các chương trình đào tạo, tập huấn về an ninh mạng do Công an tỉnh và các cơ quan chức năng tổ chức, tối thiểu 01 lần/năm; tổ chức quán triệt, tuyên truyền nâng cao nhận thức cho toàn thể người sử dụng hệ thống.

III.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin lưu trên các phương tiện lưu trữ, trang thiết bị và tài sản khác thuộc sở hữu của tổ chức; có quy trình và thực hiện vô hiệu hóa tất cả các quyền truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.
Hiện trạng	Đáp ứng về quy định. Việc bàn giao, khóa tài khoản, hủy quyền truy cập khi công chức chấm dứt hoặc thay đổi công việc được quy định tại Điều 6 Quy chế bảo đảm an ninh mạng. Việc thực hiện theo phân công tại Quy chế.
Phương án	Công chức chấm dứt hoặc thay đổi công việc phải bàn giao dữ liệu, tài sản được giao thuộc sở hữu của cơ quan và lập biên bản bàn giao. Phòng, đơn vị trực tiếp quản lý, vận hành khóa tài khoản, hủy quyền truy cập ngay khi công chức thôi việc hoặc chuyển công tác; Văn phòng Sở theo dõi, đôn đốc. Sở Công Thương hướng dẫn các đơn vị sử dụng hệ thống thông báo khi có thay đổi nhân sự để kịp thời vô hiệu hóa tài khoản.

IV. QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

IV.1. Tài liệu thiết kế và phương án bảo đảm an ninh mạng

Yêu cầu	Có tài liệu mô tả quy mô, phạm vi, đối tượng sử dụng; tài liệu mô tả thiết kế và các thành phần của hệ thống; tài liệu mô tả phương án bảo đảm an ninh mạng theo cấp độ. Xem xét, cập nhật sơ đồ mạng tối thiểu 01 lần/năm; khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế.
Hiện trạng	Đáp ứng. Yêu cầu về tài liệu hệ thống và việc cập nhật sơ đồ kiến trúc mạng được quy định tại khoản 1, khoản 2 Điều 8 Quy chế bảo đảm an ninh mạng.
Phương án	1. Tài liệu mô tả quy mô, phạm vi, đối tượng sử dụng: mục 3 Phần I. 2. Tài liệu mô tả thiết kế và các thành phần: mục

	4 Phần I. 3. Tài liệu thiết kế chi tiết chức năng của hệ thống đã được lập, nghiệm thu và gửi kèm Hồ sơ. 4. Phương án bảo đảm an ninh mạng: Phần III, Phụ lục I và Phụ lục II. 5. Sơ đồ kiến trúc mạng được xem xét, cập nhật tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến sơ đồ hệ thống. Khi có thay đổi về thiết kế, chức năng, phạm vi phục vụ, đối tượng sử dụng, loại thông tin xử lý hoặc công nghệ triển khai, Văn phòng Sở phối hợp phòng, đơn vị trực tiếp quản lý, vận hành đánh giá lại tính phù hợp của phương án; trường hợp phải xác định lại cấp độ thì thực hiện theo Điều 25 NĐ 331.
--	---

IV.2. Phát triển phần mềm thuê khoán

Yêu cầu	Có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán; yêu cầu nhà phát triển cung cấp mã nguồn phần mềm (mục 4.3.2.3 TCVN 14423:2026).
Hiện trạng	Đáp ứng. Phần mềm được mua sắm theo hình thức chỉ định thầu rút gọn; có hợp đồng với nhà thầu và Biên bản nghiệm thu, bàn giao. Mã nguồn phần mềm đã được nhà thầu bàn giao cho Sở Công Thương quản lý.
Phương án	1. Nội dung cam kết bảo mật và phạm vi trách nhiệm của các bên trong bảo đảm an ninh mạng, quản trị dữ liệu, kiểm soát truy cập và phối hợp xử lý sự cố được thực hiện theo hợp đồng và khoản 2 Điều 9 Quy chế bảo đảm an ninh mạng. 2. Mã nguồn phần mềm đã bàn giao được lưu giữ, kiểm soát truy cập tại Sở Công Thương theo hợp đồng và Điều 9 Quy chế bảo đảm an ninh mạng. 3. Sau mỗi lần nâng cấp, thay đổi chức năng, Sở Công Thương yêu cầu nhà thầu bàn giao mã nguồn và tài liệu kỹ thuật tương ứng theo khoản 5 Điều 9 Quy chế bảo đảm an ninh mạng.

IV.3. Thử nghiệm, nghiệm thu hệ thống và quản lý nhà cung cấp

Yêu cầu	Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống; thực hiện kiểm thử trước khi đưa vào vận hành; có nhân sự chịu trách nhiệm thực hiện (mục 4.12.2.3). Thiết lập và duy trì bản kiểm kê nhà cung cấp sản phẩm, dịch vụ; thực hiện phân loại nhà cung cấp; xem xét, cập nhật danh sách tối thiểu 01 lần/năm (mục 4.14.2 TCVN 14423:2026).
Hiện trạng	Đáp ứng. Đã thực hiện kiểm thử, nghiệm thu và bàn giao theo hợp đồng (Biên bản nghiệm thu gửi kèm Hồ sơ). Yêu cầu về kiểm thử, nghiệm thu và quản lý nhà cung cấp được

	quy định tại khoản 3 Điều 8 và khoản 6 Điều 9 Quy chế bảo đảm an ninh mạng.
Phương án	1. Nội dung, kế hoạch nghiệm thu và nhân sự chịu trách nhiệm thực hiện theo hợp đồng. Việc kiểm thử tiếp tục được thực hiện sau mỗi lần nâng cấp, thay đổi cấu hình do Phòng Quản lý Công nghiệp phối hợp với đơn vị phát triển, bảo trì phần mềm thực hiện. 2. Bản kiểm kê nhà cung cấp gồm 02 đơn vị: đơn vị phát triển, bảo trì phần mềm và Trung tâm Đổi mới sáng tạo và Chuyển đổi số; xem xét, cập nhật tối thiểu 01 lần/năm.

V. QUẢN LÝ VẬN HÀNH HỆ THỐNG

V.1. Quản lý tài sản

Yêu cầu	Lập danh sách, theo dõi, cập nhật trạng thái tài sản phần cứng, phần mềm và tài sản thông tin; kiểm kê, rà soát định kỳ tối thiểu 01 lần/năm; có quy trình xử lý tài sản chưa được quản lý và phần mềm trái phép.
Hiện trạng	Đáp ứng. Quy định quản lý tài sản tại Điều 10 Quy chế bảo đảm an ninh mạng. Danh sách tài sản phần mềm, dữ liệu nghiệp vụ và tài khoản thuộc phạm vi quản lý của Sở do Sở Công Thương lập; danh sách tài sản hạ tầng, máy chủ, máy chủ ảo, thiết bị mạng do Trung tâm Đổi mới sáng tạo và Chuyển đổi số lập theo phạm vi quản lý. Danh mục ứng dụng, dịch vụ của hệ thống nêu tại Bảng 2 Phần I.
Phương án	1. Phạm vi tài sản của Sở Công Thương gồm: phần mềm ứng dụng, dữ liệu nghiệp vụ và tài khoản người sử dụng. Máy chủ ảo, hạ tầng và tài nguyên dùng chung thuộc phạm vi quản lý của Trung tâm Đổi mới sáng tạo và Chuyển đổi số; thiết bị đầu cuối thuộc phạm vi quản lý của đơn vị, cá nhân sử dụng. 2. Đơn vị quản lý tài sản nào thì lập, theo dõi, cập nhật danh sách tài sản đó: Sở Công Thương lập danh sách tài sản phần mềm, dữ liệu nghiệp vụ và tài khoản thuộc phạm vi của Sở; Trung tâm Đổi mới sáng tạo và Chuyển đổi số lập danh sách tài sản hạ tầng theo phạm vi quản lý và cung cấp thông tin cần thiết khi Sở Công Thương đề nghị. 3. Danh sách tài sản phần mềm của Sở gồm: tên tài sản, mục đích sử dụng, phạm vi sử dụng, chủ thể quản lý, thông tin bản quyền, phiên bản; chỉ cài đặt phần mềm đã được phê duyệt. 4. Dữ liệu nghiệp vụ của hệ thống được xếp ở mức Hạn chế truy cập. 5. Rà soát, cập nhật danh sách

	tài sản tối thiểu 01 lần/năm.
--	-------------------------------

V.2. Quản lý vận hành và quản lý thay đổi

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống; về truy cập và quản lý cấu hình hệ thống; thực hiện quản lý thay đổi (mục 4.12.2.2 TCVN 14423:2026).
Hiện trạng	Đáp ứng về quy định. Nội dung quản lý vận hành, truy cập từ xa và quản lý thay đổi được quy định tại khoản 6, khoản 7 Điều 11 Quy chế bảo đảm an ninh mạng. Việc thực hiện theo phân công tại Quy chế.
Phương án	1. Việc truy cập, quản trị nghiệp vụ trên ứng dụng từ xa phải sử dụng giao thức có mã hóa và chỉ thực hiện từ dải địa chỉ mạng được phép. 2. Mọi thay đổi về cấu hình, phiên bản, chức năng của hệ thống đều phải được Sở Công Thương đề nghị bằng văn bản, ghi nhận và kiểm tra lại hoạt động của hệ thống sau khi Trung tâm Đổi mới sáng tạo và Chuyển đổi số hoặc đơn vị phát triển phần mềm thực hiện. 3. Việc quản lý, cấu hình hạ tầng mạng và thiết bị bảo mật thuộc phạm vi quản lý của Trung tâm Đổi mới sáng tạo và Chuyển đổi số; Sở Công Thương đề nghị bằng văn bản và phối hợp thực hiện khi có nhu cầu thay đổi.

V.3. Cấu hình an toàn

Yêu cầu	Có quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm; có tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình tăng cường bảo mật; vô hiệu hóa giao thức mạng không an toàn và dịch vụ không sử dụng; cấu hình tự động khóa phiên làm việc; đánh giá, cập nhật tối thiểu 01 lần/năm (mục 4.5 TCVN 14423:2026).
Hiện trạng	Đáp ứng về quy định. Yêu cầu cấu hình an toàn được quy định tại Điều 11 Quy chế bảo đảm an ninh mạng. Việc thiết lập cấu hình an toàn máy chủ ảo, hệ điều hành do Trung tâm Đổi mới sáng tạo và Chuyển đổi số thực hiện; cấu hình an toàn ứng dụng do đơn vị phát triển, bảo trì phần mềm thực hiện; Sở Công Thương quản lý phần thuộc phạm vi của Sở và lưu giữ tài liệu cần thiết.
Phương án	1. Đơn vị quản lý thành phần nào thì thiết lập, duy trì cấu hình an toàn và cung cấp thông tin cấu hình của thành phần đó: Trung tâm Đổi mới sáng tạo và Chuyển đổi số đối với máy chủ ảo, hệ điều hành, thiết bị mạng và thiết bị bảo mật;

	đơn vị phát triển, bảo trì phần mềm đối với ứng dụng, gồm tự động khóa phiên làm việc và khóa tài khoản sau số lần đăng nhập sai liên tiếp. 2. Sở Công Thương quản lý cấu hình phần thuộc phạm vi của Sở, lưu giữ tài liệu cấu hình do các đơn vị cung cấp và đề nghị cung cấp khi cần thiết. 3. Yêu cầu cấu hình an toàn đối với thiết bị đầu cuối truy cập hệ thống được quy định tại Điều 15, Điều 16 Quy chế bảo đảm an ninh mạng; Văn phòng Sở hướng dẫn, kiểm tra việc thực hiện. 4. Rà soát, cập nhật nội dung cấu hình an toàn tối thiểu 01 lần/năm.
--	---

V.4. Quản lý tài khoản và quyền truy cập

Yêu cầu	Lập danh sách tài khoản, phân loại tối thiểu thành tài khoản quản trị, tài khoản tác nghiệp và tài khoản kỹ thuật; rà soát tối thiểu 01 lần/năm; xây dựng và tuân thủ quy định sử dụng mật khẩu, quy định quản lý tài khoản và quy định quản lý truy cập.
Hiện trạng	Đáp ứng một phần. Hệ thống đã phân quyền theo vai trò và theo đơn vị, có chức năng đổi mật khẩu, khóa và mở khóa tài khoản. Chính sách mật khẩu, quản lý tài khoản và quản lý truy cập được quy định tại Điều 12 Quy chế bảo đảm an ninh mạng; trên ứng dụng chưa triển khai xác thực đa yếu tố.
Phương án	1. Danh sách tài khoản gồm: loại tài khoản, tên tài khoản, trạng thái, người quản lý, đơn vị, ngày kích hoạt, ngày vô hiệu hóa; rà soát tối thiểu 01 lần/năm. 2. Chính sách mật khẩu: thay đổi mật khẩu mặc định và trong lần đăng nhập đầu tiên; mật khẩu tối thiểu 08 ký tự nếu có áp dụng xác thực đa yếu tố hoặc tối thiểu 14 ký tự nếu không áp dụng; tài khoản quản trị thay đổi mật khẩu tối thiểu 01 lần/02 tháng. 3. Quản lý tài khoản: vô hiệu hóa tài khoản mặc định; mỗi tài khoản gán cho một người sử dụng; vô hiệu hóa tài khoản không hoạt động sau 45 ngày hoặc khi có thay đổi nhân sự. 4. Quản lý truy cập: cấp quyền tối thiểu theo chức danh; đề nghị áp dụng xác thực đa yếu tố đối với tài khoản quản trị; đề nghị giới hạn dải địa chỉ mạng được phép quản trị từ xa. 5. Nội dung tại khoản 2 và khoản 4 được thực hiện trên ứng dụng thông qua đề nghị đơn vị phát triển phần mềm trong quá trình bảo trì, nâng cấp.

V.5. Quản lý lỗ hổng bảo mật và bản vá

Yêu cầu	Có quy trình quản lý lỗ hổng bảo mật và quy trình quản lý bản vá; rà soát quy trình và rà quét lỗ hổng bảo mật tối thiểu 01 lần/năm; kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng tối thiểu 01 lần/tháng (mục 4.7 TCVN 14423:2026).
Hiện trạng	Đáp ứng về quy định. Quy trình quản lý lỗ hổng bảo mật và quản lý bản vá được quy định tại Điều 13 Quy chế bảo đảm an ninh mạng, trong đó phân định: hạ tầng, máy chủ, máy chủ ảo và thiết bị mạng do Trung tâm Đổi mới sáng tạo và Chuyển đổi số thực hiện; ứng dụng do đơn vị phát triển, bảo trì thực hiện theo hợp đồng; Sở Công Thương tiếp nhận cảnh báo, đề nghị khắc phục, phối hợp và theo dõi kết quả. Việc thực hiện theo phân công tại Quy chế.
Phương án	1. Phân định thực hiện: hạ tầng, máy chủ, máy chủ ảo, thiết bị mạng và thiết bị bảo mật do Trung tâm Đổi mới sáng tạo và Chuyển đổi số thực hiện việc rà quét, khắc phục lỗ hổng và cập nhật bản vá; ứng dụng do đơn vị phát triển, bảo trì phần mềm thực hiện theo phạm vi hợp đồng. 2. Sở Công Thương tiếp nhận cảnh báo lỗ hổng từ cơ quan có thẩm quyền, Trung tâm Đổi mới sáng tạo và Chuyển đổi số và đơn vị phát triển, bảo trì phần mềm; đề nghị khắc phục, phối hợp và theo dõi kết quả. Đối với lỗ hổng có mức độ nghiêm trọng cao, đề nghị khắc phục ngay. 3. Rà quét lỗ hổng bảo mật thực hiện tối thiểu 01 lần/năm; kiểm tra, cập nhật bản vá tối thiểu 01 lần/tháng theo mục 4.7 TCVN 14423:2026; Sở Công Thương đề nghị và tiếp nhận kết quả từ các đơn vị nêu tại khoản 1. 4. Đối với thiết bị đầu cuối, Sở Công Thương hướng dẫn thiết lập chế độ cập nhật bản vá tự động. 5. Rà soát nội dung quản lý lỗ hổng bảo mật và bản vá tối thiểu 01 lần/năm.

V.6. Quản lý nhật ký an ninh mạng

Yêu cầu	Có quy định quản lý nhật ký an ninh mạng; thu thập tối thiểu nhật ký truy cập hệ thống, nhật ký ứng dụng và nhật ký cảnh báo của thiết bị bảo mật; đồng bộ thời gian; duy trì không gian lưu trữ nhật ký tối thiểu 01 tháng; rà soát nhật ký tối thiểu 01 lần/năm.
Hiện trạng	Đáp ứng về quy định. Việc quản lý nhật ký và giám sát an ninh mạng được quy định tại Điều 14 Quy chế bảo đảm an ninh mạng; ứng dụng đã ghi nhật ký thao tác của người sử

	dụng. Thời hạn lưu trữ và việc rà soát nhật ký thực hiện theo Quy chế.
Phương án	1. Thực hiện quản lý nhật ký theo Điều 14 Quy chế bảo đảm an ninh mạng. 2. Thu thập tối thiểu: nhật ký truy cập hệ thống (gồm địa chỉ nguồn, địa chỉ đích, tài khoản đích, thời điểm, thông tin hành vi), nhật ký ứng dụng và nhật ký cảnh báo của thiết bị bảo mật. 3. Các thành phần của hệ thống được đồng bộ thời gian theo máy chủ thời gian do Trung tâm Đối mới sáng tạo và Chuyển đổi số cung cấp. 4. Duy trì không gian lưu trữ nhật ký tối thiểu 01 tháng; rà soát nhật ký tối thiểu 01 lần/năm và rà soát ngay khi có cảnh báo. 5. Nhật ký của tường lửa, tường lửa ứng dụng web, thiết bị chuyển mạch và các thiết bị hạ tầng khác do Trung tâm Đối mới sáng tạo và Chuyển đổi số quản lý; Sở Công Thương đề nghị cung cấp khi cần phục vụ xác minh, xử lý sự cố theo khoản 3 Điều 14 Quy chế bảo đảm an ninh mạng.

V.7. Sao lưu và khôi phục dữ liệu

Yêu cầu	Có quy định sao lưu và khôi phục dữ liệu, xác định loại dữ liệu cần sao lưu, tần suất, phương pháp, quản lý vùng lưu trữ và việc định kỳ khôi phục thử; bản sao lưu được bảo vệ, quản lý phiên bản và lưu trữ ở hạ tầng tách biệt với môi trường vận hành.
Hiện trạng	Đáp ứng. Quy định sao lưu và khôi phục dữ liệu tại Điều 17 Quy chế bảo đảm an ninh mạng. Việc sao lưu dữ liệu của hệ thống do Trung tâm Đối mới sáng tạo và Chuyển đổi số thực hiện trên hạ tầng lưu trữ của Trung tâm; Trung tâm đã thực hiện khôi phục thử để kiểm tra khả năng khôi phục của bản sao lưu.
Phương án	1. Các loại dữ liệu cần sao lưu: tập tin cấu hình hệ thống, cơ sở dữ liệu, dữ liệu và thông tin nghiệp vụ. Việc sao lưu, quản lý hạ tầng lưu trữ bản sao lưu do Trung tâm Đối mới sáng tạo và Chuyển đổi số thực hiện; Sở Công Thương đề nghị, phối hợp và theo dõi kết quả theo khoản 2 Điều 17 Quy chế bảo đảm an ninh mạng. 2. Tần suất: sao lưu toàn phần theo tuần và sao lưu gia tăng theo ngày đối với cơ sở dữ liệu; sao lưu cấu hình hệ thống theo tháng hoặc khi có thay đổi. 3. Bản sao lưu được định danh, quản lý theo phiên bản, có kiểm soát truy cập và lưu trữ trên hệ thống lưu trữ

	do Trung tâm Đổi mới sáng tạo và Chuyển đổi số cung cấp, tách biệt với môi trường vận hành. 4. Việc khôi phục thử để kiểm tra khả năng khôi phục do Trung tâm Đổi mới sáng tạo và Chuyển đổi số thực hiện, có sự phối hợp của Sở Công Thương theo phân công; kết quả được ghi nhận và cung cấp cho Sở Công Thương; định kỳ thực hiện lại theo mục 4.11.2.1 TCVN 14423:2026. 5. Rà soát, cập nhật quy định sao lưu, khôi phục dữ liệu tối thiểu 01 lần/năm.
--	--

V.8. Quản lý sự cố an ninh mạng

Yêu cầu	Có chính sách, quy trình xử lý sự cố an ninh mạng gồm: phân nhóm sự cố; phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu; kế hoạch ứng phó; quy trình ứng cứu sự cố thông thường và nghiêm trọng; cơ chế phối hợp với cơ quan chức năng, bên cung cấp dịch vụ.
Hiện trạng	Đáp ứng. Quy trình ứng phó và xử lý sự cố an ninh mạng được quy định tại Điều 19 Quy chế bảo đảm an ninh mạng.
Phương án	1. Phân nhóm sự cố theo mức độ nghiêm trọng, tối thiểu gồm sự cố thông thường và sự cố nghiêm trọng. 2. Người sử dụng khi phát hiện nguy cơ hoặc sự cố phải báo cáo ngay cấp trên trực tiếp và Văn phòng Sở. Văn phòng Sở tiếp nhận, xác minh, phân loại và triển khai biện pháp ngăn chặn ban đầu. 3. Quy trình ứng cứu theo các bước: phát hiện - phân loại - ngăn chặn - khắc phục - phục hồi - báo cáo - rút kinh nghiệm; báo cáo thực hiện theo mục II.3 Phụ lục này. 4. Trường hợp sự cố thuộc lớp hạ tầng, phối hợp với Trung tâm Đổi mới sáng tạo và Chuyển đổi số xử lý. Trường hợp sự cố nghiêm trọng vượt quá khả năng khắc phục, phối hợp với Công an tỉnh Hưng Yên để được hướng dẫn, hỗ trợ và thực hiện theo đúng hướng dẫn (khoản 5 Điều 33 NĐ 331).

V.9. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu	Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ và truy cập tài nguyên trên Internet đối với người sử dụng đầu cuối; triển khai giải pháp phòng chống mã độc và kiểm soát phương tiện lưu trữ di động.
Hiện trạng	Đáp ứng về quy định. Quy định quản lý trình duyệt web, truy cập Internet và phòng, chống phần mềm độc hại tại Điều 15, Điều 16 Quy chế bảo đảm an ninh mạng. Việc thực hiện đối với thiết bị đầu cuối theo hướng dẫn của Sở Công Thương.

Phương án	1. Sở Công Thương quy định, hướng dẫn các yêu cầu bảo đảm an toàn đối với thiết bị đầu cuối khi truy cập hệ thống: cấu hình bảo mật trước khi kết nối; thiết lập chế độ cập nhật bản vá tự động; cài đặt phần mềm phòng chống mã độc có bảo vệ thời gian thực, tự động cập nhật mẫu nhận diện. Người sử dụng và đơn vị quản lý thiết bị có trách nhiệm thực hiện các yêu cầu này. 2. Người sử dụng tự quản lý, bảo quản thiết bị và tài khoản được giao; đặt mật khẩu theo chính sách tại mục V.4 Phụ lục này; không chia sẻ mật khẩu; không sử dụng tính năng lưu mật khẩu hoặc đăng nhập tự động; khóa máy tính khi rời khỏi vị trí. 3. Người sử dụng chỉ truy nhập các trang thông tin điện tử, ứng dụng tin cậy, phù hợp với chức năng, nhiệm vụ; không mở tệp tin, thư điện tử không rõ nguồn gốc. 4. Sở Công Thương hướng dẫn người sử dụng kiểm tra, rà quét phần mềm độc hại khi sao chép, mở tệp tin, trước khi kết nối phương tiện lưu trữ di động và vô hiệu hóa tính năng tự động thực thi theo khoản 3 Điều 15 Quy chế bảo đảm an ninh mạng.
------------------	--

V.10. Kiểm tra, đánh giá và giám sát an ninh mạng

Yêu cầu	Tổ chức kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin theo quy định tại Điều 27 NBĐ 331; có phương án giám sát an ninh mạng và bảo đảm các điều kiện cần thiết phục vụ hoạt động giám sát của lực lượng chuyên trách bảo vệ an ninh mạng.
Hiện trạng	Đáp ứng một phần. Quy định kiểm tra, đánh giá và kiểm thử an ninh mạng tại Điều 20 Quy chế bảo đảm an ninh mạng; chưa tổ chức kiểm tra, đánh giá an ninh mạng đối với hệ thống.
Phương án	1. Sở Công Thương tổ chức kiểm tra, đánh giá an ninh mạng đối với hệ thống trong phạm vi quản lý, vận hành của Sở theo Điều 20 Quy chế bảo đảm an ninh mạng; kết quả được sử dụng để khắc phục các tồn tại, điểm yếu và cập nhật phương án bảo đảm an ninh mạng. Đối với thành phần thuộc phạm vi quản lý của Trung tâm Đối mới sáng tạo và Chuyển đổi số và đơn vị phát triển, bảo trì phần mềm, Sở Công Thương đề nghị, phối hợp và tiếp nhận kết quả. 2. Sở Công Thương giám sát ở lớp ứng dụng, cơ sở dữ liệu và tài khoản thông qua theo dõi, rà soát nhật ký theo mục V.6 Phụ lục này; đầu mối tiếp nhận, xử lý cảnh báo là Văn phòng Sở. 3. Sở Công Thương phối hợp, cung cấp thông tin, dữ

	liệu và đáp ứng các điều kiện cần thiết phục vụ hoạt động giám sát an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng theo khoản 5 Điều 33 NĐ 331.
--	---

VI. PHƯƠNG ÁN QUẢN LÝ RỦI RO AN NINH MẠNG

Yêu cầu	Có quy định, quy trình quản lý rủi ro an ninh mạng, thực hiện tối thiểu các bước: xác định, phân tích, đánh giá và xử lý rủi ro; đánh giá, cập nhật quy định, quy trình tối thiểu 01 lần/năm.
Hiện trạng	Đáp ứng. Quy định quản lý rủi ro an ninh mạng tại Điều 18 Quy chế bảo đảm an ninh mạng.
Phương án	1. Nguyên tắc: quản lý rủi ro được thực hiện thường xuyên, liên tục trong suốt vòng đời của hệ thống, bảo đảm rủi ro được duy trì trong ngưỡng chấp nhận được. 2. Các trường hợp phải đánh giá rủi ro theo khoản 2 Điều 10 NĐ 331: khi xác định cấp độ lần đầu; khi có thay đổi về chức năng, phạm vi phục vụ, đối tượng sử dụng, loại thông tin xử lý hoặc công nghệ triển khai; khi hệ thống mở rộng quy mô, tích hợp, kết nối liên thông hoặc chia sẻ dữ liệu; khi xảy ra sự cố nghiêm trọng; khi có yêu cầu của cơ quan có thẩm quyền. Ngoài ra, rà soát tình trạng rủi ro tối thiểu 01 lần/năm. 3. Nội dung đánh giá rủi ro thực hiện theo khoản 3 Điều 10 NĐ 331. 4. Xử lý rủi ro: lựa chọn một hoặc nhiều biện pháp gồm giảm thiểu, tránh, chuyển giao rủi ro hoặc chấp nhận rủi ro khi nằm trong ngưỡng chấp nhận; việc chấp nhận rủi ro phải được người có thẩm quyền phê duyệt và lập thành hồ sơ. 5. Theo khoản 2 Điều 10 NĐ 331, việc đánh giá rủi ro an ninh mạng thuộc trách nhiệm của chủ quản hệ thống thông tin. Văn phòng Sở tham mưu, phối hợp thực hiện trong phạm vi hệ thống do Sở vận hành và báo cáo kết quả về chủ quản hệ thống thông tin.

VII. PHƯƠNG ÁN KẾT THÚC VẬN HÀNH, KHAI THÁC, THANH LÝ, HỦY BỎ HỆ THỐNG THÔNG TIN

Yêu cầu	Có quy định, quy trình về kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin; có phương án xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.
Hiện trạng	Đáp ứng. Quy định kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin tại Điều 21 Quy chế bảo đảm an

	ninh mạng.
Phương án	1. Thiết bị có chứa dữ liệu khi bị hỏng phải được kiểm tra, sửa chữa, có biện pháp giám sát bảo đảm không để lộ lọt thông tin. 2. Trước khi thanh lý hoặc loại bỏ thiết bị, phải áp dụng biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu, bảo đảm không thể phục hồi; máy tính, thiết bị mạng, phương tiện lưu trữ phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng. 3. Đối với máy chủ ảo, khi kết thúc vận hành, Sở Công Thương phối hợp với Trung tâm Đổi mới sáng tạo và Chuyển đổi số thực hiện xóa an toàn dữ liệu và thu hồi tài nguyên. 4. Khi kết thúc vận hành, khai thác hệ thống: lập biên bản kết thúc vận hành; xử lý dữ liệu theo quy định của pháp luật về lưu trữ và bảo vệ dữ liệu cá nhân; thu hồi, vô hiệu hóa toàn bộ tài khoản và quyền truy cập; thu hồi tên miền, địa chỉ IP; gỡ bỏ ứng dụng và dữ liệu; thông báo cho chủ quản hệ thống thông tin và đơn vị chuyên trách về an ninh mạng.

PHỤ LỤC II

THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU CƠ BẢN VỀ KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2

(Khoản 4 Điều 30 NĐ 331 và Mục 4 TCVN 14423:2026)

Các biện pháp thuộc lớp hạ tầng mạng do Trung tâm Đổi mới sáng tạo và Chuyển đổi số đầu tư, quản lý, vận hành và được hệ thống sử dụng chung theo điểm a khoản 5 Điều 30 NĐ 331. Thông tin về thiết bị, vùng mạng, địa chỉ IP và hiện trạng cấu hình nêu tại mục 1 Phụ lục này do Trung tâm Đổi mới sáng tạo và Chuyển đổi số cung cấp.

1. BẢO ĐẢM AN TOÀN MẠNG

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Có	Vùng mạng nội bộ của Trung tâm Đổi mới sáng tạo và Chuyển đổi số, nơi triển khai các thiết bị mạng, thiết bị bảo mật nêu tại Bảng 1 Phần I; bao gồm vùng quản trị hệ thống (VLAN 20)
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet (VLAN 5; 10.132.196.1; IP Public 117.4.182.83); triển khai WAF theo Bảng 1 Phần I
3	Vùng DMZ	Có	Vùng mạng trung gian giữa mạng nội bộ và mạng ngoài (VLAN 10; 10.132.193.0/24)
4	Vùng máy chủ nội bộ (Application)	Có	Triển khai Web Server (ứng dụng ATTP) trên hệ thống ảo hóa tại vùng Application (VLAN 30; 10.132.2.0/24)
5	Vùng dữ liệu Database	Có	Triển khai Database Server (SQL Server 2019) tại vùng Database riêng biệt (VLAN 25; 10.132.195.0/24); truy cập từ vùng Application được kiểm soát qua 02 thiết bị Palo Alto PA-850
6	Vùng mạng không dây	Không áp dụng	Hệ thống không sử dụng kết nối mạng không dây

b) Phương án bảo đảm an ninh mạng:

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Sử dụng Firewall Palo Alto PA-440 để kiểm soát dữ liệu ra vào, ngăn chặn xâm nhập; việc quản trị hệ thống từ xa chỉ thực hiện qua các cổng quản trị được kiểm soát (TCP 22, TCP 3389) và giới hạn theo dải địa chỉ mạng được phép
2	Kiến trúc an toàn	Có	Phân tách các vùng mạng thành các vùng riêng biệt về lô-gic bằng VLAN trên cụm 03 thiết bị chuyển mạch lớp 3 SG 3850; lập và cập nhật sơ đồ mạng tối thiểu 01 lần/năm
3	Phương án quản lý truy cập giữa các vùng mạng và phòng, chống xâm nhập bằng tường lửa tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương	Có	Sử dụng FortiGate FG300 (kiểm soát ứng dụng, nhận diện người dùng, ngăn chặn các mối đe dọa) và Palo Alto PA-850 (kiểm soát truy cập vùng Application và Database) theo Bảng 1 Phần I
4	Phương án phòng, chống mã độc cho máy chủ và máy trạm	Có	Máy chủ ảo thuộc phạm vi quản lý của Trung tâm Đổi mới sáng tạo và Chuyển đổi số được thực hiện các biện pháp phòng, chống mã độc theo phạm vi quản lý của Trung tâm; đối với thiết bị đầu cuối, thực hiện theo hướng dẫn của Sở Công Thương
5	Phương án phòng, chống tấn công mạng cho ứng dụng web	Có	Sử dụng tường lửa ứng dụng web (WAF) tại vùng mạng biên
6	Phương án bảo đảm an ninh mạng cho hệ thống thư điện tử	Không áp dụng	Hệ thống không được trang bị hệ thống thư điện tử riêng
7	Phương án dự phòng cho các thiết bị mạng chính	Có	Thiết bị tường lửa và thiết bị chuyển mạch có phương án dự phòng: 02 thiết bị Palo Alto PA-850, cụm 03 thiết bị chuyển mạch SG 3850
8	Phương án giám sát	Có	Triển khai giải pháp kiểm tra hiệu năng

TT	Yêu cầu	P/A	Ghi chú/Mô tả
	hiệu năng hạ tầng mạng		(RAM, CPU...), bảo đảm hoạt động bình thường của hệ thống
9	Phương án bảo vệ duyệt web và lọc tên miền	Có	Triển khai sử dụng dịch vụ lọc tên miền để ngăn chặn các tên miền giả mạo và độc hại
10	Thực hiện quản lý thay đổi	Có	Mọi thay đổi cấu hình trong phạm vi Sở quản lý phải được phê duyệt, ghi nhận và kiểm tra lại sau khi thay đổi theo mục V.2 Phụ lục I

1.2. Kiểm soát truy cập từ bên ngoài mạng

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép kết nối an toàn khi truy cập từ bên ngoài	Có	Ứng dụng chỉ cung cấp qua HTTPS; việc quản trị từ xa sử dụng giao thức có mã hóa qua các cổng quản trị được kiểm soát
2	Kiểm soát truy cập theo từng dịch vụ; chặn dịch vụ không cung cấp	Có	Palo Alto PA-440 thiết lập chính sách kiểm soát truy cập từ bên ngoài theo từng dịch vụ, ứng dụng; chặn tất cả truy cập không được phép
3	Giới hạn dải địa chỉ mạng được phép quản trị từ xa	Có	Chỉ cho phép quản trị máy chủ ảo, ứng dụng từ các dải địa chỉ mạng được phép
4	Thiết lập giới hạn thời gian chờ để đóng phiên kết nối	Có	Thiết lập giới hạn thời gian chờ trên Firewall Palo Alto PA-440; tự động đóng phiên kết nối khi không có thao tác
5	Yêu cầu xác thực bổ sung trước khi truy cập vào hệ thống	Chưa đáp ứng	Phương án triển khai xác thực đa yếu tố đối với tài khoản quản trị tại mục V.4 Phụ lục I

1.3. Kiểm soát truy cập từ bên trong mạng

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập dịch vụ bên ngoài theo yêu cầu nghiệp vụ	Có	Chính sách kiểm soát truy cập chiều ra được thiết lập trên các thiết bị tường lửa nêu tại Bảng 1 Phần I
2	Kiểm soát truy cập giữa các vùng mạng	Có	Palo Alto PA-850 chỉ cho phép kết nối từ Web Server tại vùng Application tới

TT	Yêu cầu	P/A	Ghi chú/Mô tả
	trong hệ thống		Database Server tại vùng Database; chặn các kết nối khác

1.4. Nhật ký hệ thống mạng

Thiết bị	Ghi và lưu trữ nhật ký trên thiết bị	Đồng bộ thời gian với máy chủ thời gian	Lưu trữ nhật ký tối thiểu 01 tháng
Firewall Palo Alto PA-440	Có	Có	Có
Firewall ADC	Có	Có	Có
FortiGate FG300	Có	Có	Có
Palo Alto PA-850	Có	Có	Có
Switch SG 3850	Có	Có	Có
WAF	Có	Có	Có

Các thiết bị nêu trên thuộc phạm vi quản lý, vận hành của Trung tâm Đổi mới sáng tạo và Chuyển đổi số; Sở Công Thương đề nghị cung cấp nhật ký khi cần phục vụ điều tra, xác minh sự cố.

1.5. Phòng, chống xâm nhập

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng, chống xâm nhập bảo vệ các vùng mạng trong hệ thống	Có	Firewall Palo Alto PA-440 ngăn chặn xâm nhập tại vùng mạng biên; FortiGate FG300 và Palo Alto PA-850 kiểm soát truy cập giữa các vùng mạng; WAF phòng chống lỗ hổng ứng dụng web
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Có	Cập nhật định kỳ cơ sở dữ liệu dấu hiệu tấn công trên các thiết bị tường lửa và bộ quy tắc phòng chống lỗ hổng web trên WAF

1.6. Bảo vệ thiết bị hệ thống

Thiết bị	Cấu hình chức năng xác thực trên thiết bị	Chỉ cho phép kết nối mạng an toàn khi quản trị từ xa	Hạn chế địa chỉ mạng được kết nối, quản trị từ xa	Tự động khóa phiên quản trị sau không quá 05 phút
Firewall Palo Alto	Có	Có	Có	Có

Thiết bị	Cấu hình chức năng xác thực trên thiết bị	Chỉ cho phép kết nối mạng an toàn khi quản trị từ xa	Hạn chế địa chỉ mạng được kết nối, quản trị từ xa	Tự động khóa phiên quản trị sau không quá 05 phút
PA-440				
Firewall ADC	Có	Có	Có	Có
FortiGate FG300	Có	Có	Có	Có
Palo Alto PA-850	Có	Có	Có	Có
Switch SG 3850	Có	Có	Có	Có
WAF	Có	Có	Có	Có

1.7. Bảo vệ duyệt web, dịch vụ thư điện tử

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có danh sách trình duyệt web, dịch vụ thư điện tử được phép sử dụng	Chưa đáp ứng	Chưa có danh sách. Phương án: Sở Công Thương ban hành, hướng dẫn danh sách trình duyệt web được phép sử dụng để truy cập hệ thống và yêu cầu sử dụng phiên bản còn được nhà cung cấp hỗ trợ. Hệ thống không được trang bị dịch vụ thư điện tử riêng
2	Bảo đảm trình duyệt web trong danh sách đang trong thời gian hỗ trợ của nhà cung cấp	Đáp ứng một phần	Rà soát, đối chiếu phiên bản trình duyệt trên máy trạm tối thiểu 01 lần/năm
3	Rà soát, cập nhật bản vá lỗ hổng bảo mật cho trình duyệt web	Có	Máy trạm thiết lập chế độ cập nhật bản vá tự động; kiểm tra tối thiểu 01 lần/tháng
4	Triển khai dịch vụ lọc tên miền	Có	Xem điểm b mục 1.1 Phụ lục này

2. BẢO ĐẢM AN TOÀN MÁY CHỦ

Hệ thống được triển khai trên các máy chủ ảo quản lý bằng VMware vSphere Client, gồm Web Server tại vùng Application và Database Server tại vùng Database. Các nội dung liên quan đến thiết bị đầu cuối (máy trạm) được nêu tại các mục dưới đây là yêu cầu do Sở Công Thương quy định, hướng dẫn khi truy cập hệ thống; người sử dụng và đơn vị quản lý thiết bị có trách nhiệm thực hiện.

2.1. Xác thực

Đối tượng	Thiết lập chính sách xác thực, vô hiệu hóa tài khoản mặc định	Quản lý tách biệt tài khoản quản trị, tác nghiệp, kỹ thuật	Thiết lập chính sách mật khẩu an toàn
Web Server (máy ảo)/Web-App/Vùng Application/Windows Server 2019	Có	Có	Đáp ứng một phần - phương án tại mục V.4 Phụ lục I
Database Server (máy ảo)/SQL Server 2019/Vùng Database/Windows Server 2019	Có	Có	Đáp ứng một phần - như trên
Máy trạm người sử dụng	Có	Có	Đáp ứng một phần - như trên

2.2. Kiểm soát truy cập

Đối tượng	Chỉ cho phép kết nối mạng an toàn khi truy cập, quản trị từ xa	Thiết lập giới hạn thời gian chờ	Tự động khóa phiên làm việc
Web Server và Database Server	Có	Có	Có - khóa phiên quản trị sau không quá 05 phút không sử dụng
Máy trạm người sử dụng	Có	Có	Có - khóa màn hình sau không quá 15 phút không sử dụng

2.3. Nhật ký hệ thống

Đối tượng	Ghi nhật ký hệ thống	Đồng bộ thời gian với máy chủ thời gian	Lưu trữ nhật ký tối thiểu 01 tháng
Web Server (máy ảo)/Web-App/Vùng Application/Windows Server 2019	Có	Có	Có
Database Server (máy	Có	Có	Có

Đối tượng	Ghi nhật ký hệ thống	Đồng bộ thời gian với máy chủ thời gian	Lưu trữ nhật ký tối thiểu 01 tháng
ảo)/SQL Server 2019/Vùng Database/Windows Server 2019			
Máy trạm người sử dụng	Có	Có	Có

2.4. Phòng, chống xâm nhập

Đối tượng	Loại bỏ tài khoản không sử dụng, không còn hợp lệ	Sử dụng tường lửa của hệ điều hành	Vô hiệu hóa giao thức mạng không an toàn, dịch vụ không sử dụng	Xử lý điểm yếu trước khi đưa vào sử dụng
Web Server (máy ảo)	Có	Có	Có	Có
Database Server (máy ảo)	Có	Có	Có	Có
Máy trạm người sử dụng	Có	Có	Có	Có

2.5. Phòng, chống phần mềm độc hại

Đối tượng	Cài đặt phần mềm phòng, chống mã độc, tự động cập nhật mẫu nhận diện	Rà quét mã độc và vô hiệu hóa tính năng tự động thực thi đối với phương tiện lưu trữ di động
Web Server và Database Server	Có	Không áp dụng - không kết nối phương tiện lưu trữ di động
Máy trạm người sử dụng	Có	Có

2.6. Cấu hình an toàn, cứng hóa

Đối tượng	Thiết lập cấu hình an toàn, phòng chống đăng nhập tự động đối với tài sản xử lý dữ liệu quan trọng	Áp dụng tài liệu cấu hình tiêu chuẩn, cấu hình tăng cường bảo mật
------------------	---	--

Đối tượng	Thiết lập cấu hình an toàn, phòng chống đăng nhập tự động đối với tài sản xử lý dữ liệu quan trọng	Áp dụng tài liệu cấu hình tiêu chuẩn, cấu hình tăng cường bảo mật
Web Server (máy ảo)	Có	Do Trung tâm Đổi mới sáng tạo và Chuyển đổi số thiết lập, quản lý
Database Server (máy ảo)	Có	Do Trung tâm Đổi mới sáng tạo và Chuyển đổi số thiết lập, quản lý
Máy trạm người sử dụng	Có	Theo yêu cầu tại Điều 15 Quy chế bảo đảm an ninh mạng; Sở Công Thương hướng dẫn, kiểm tra việc thực hiện

2.7. Xử lý máy chủ, máy trạm khi chuyển giao

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng	Có	Áp dụng biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu. Đối với máy chủ ảo, Sở Công Thương phối hợp với Trung tâm Đổi mới sáng tạo và Chuyển đổi số thực hiện xóa an toàn dữ liệu và thu hồi tài nguyên. Chi tiết tại mục VII Phụ lục I

3. BẢO ĐẢM AN TOÀN ỨNG DỤNG

3.1. Xác thực

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Có	Toàn bộ chức năng của ứng dụng yêu cầu đăng nhập
2	Lưu trữ có mã hóa thông tin xác thực	Có	Thông tin xác thực được lưu trữ dưới dạng mã hóa
3	Cấu hình ứng dụng bảo đảm an toàn mật khẩu người sử dụng	Đáp ứng một phần	Phương án triển khai xác thực đa yếu tố đối với tài khoản quản trị tại mục V.4 Phụ lục I
4	Hạn chế số lần đăng nhập	Có	Khóa tài khoản sau tối đa 05 lần

TT	Yêu cầu	P/A	Ghi chú/Mô tả
	sai và giới hạn thời gian mở khóa		đăng nhập sai liên tiếp

3.2. Kiểm soát truy cập

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa; giới hạn địa chỉ mạng quản trị	Có	Ứng dụng chỉ cung cấp qua HTTPS; quản trị ứng dụng chỉ từ dải địa chỉ được phép
2	Thiết lập giới hạn thời gian chờ để đóng phiên kết nối	Có	Ứng dụng thiết lập thời gian chờ phiên làm việc
3	Tự động khóa phiên làm việc không quá 15 phút không sử dụng	Có	Áp dụng đối với phiên làm việc của người sử dụng trên ứng dụng

3.3. Nhật ký hệ thống

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Ghi nhật ký: truy cập ứng dụng; đăng nhập quản trị; lỗi phát sinh; thay đổi cấu hình ứng dụng	Có	Ứng dụng ghi nhận đầy đủ 04 loại nhật ký nêu trên, có đồng bộ thời gian
2	Nhật ký được lưu trữ tối thiểu 01 tháng	Có	Đáp ứng yêu cầu đối với hệ thống thông tin cấp độ 2

3.4. An toàn ứng dụng và mã nguồn

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	Có	Ứng dụng thực hiện kiểm tra, chuẩn hóa dữ liệu đầu vào trước khi xử lý và lưu trữ
2	Bảo đảm an toàn mã nguồn phần mềm thuê khoán	Có	Mã nguồn phần mềm đã được nhà thầu bàn giao, do Sở Công Thương lưu giữ và kiểm soát truy cập (mục IV.2 Phụ lục I)

4. BẢO ĐẢM AN TOÀN DỮ LIỆU

4.1. Bảo mật dữ liệu

TT	Yêu cầu	P/A	Ghi chú/Mô tả
----	---------	-----	---------------

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Mã hóa thông tin xác thực và dữ liệu không phải là dữ liệu công khai khi lưu trữ	Có	Thông tin xác thực và dữ liệu không phải là dữ liệu công khai được lưu trữ dưới dạng mã hóa
2	Bảo đảm an toàn dữ liệu trên đường truyền	Có	Dữ liệu truyền tải được bảo vệ bằng giao thức TLS

4.2. Sao lưu dự phòng

TT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu và thông tin nghiệp vụ	Có	Sao lưu trên hệ thống lưu trữ do Trung tâm Đổi mới sáng tạo và Chuyển đổi số cung cấp
2	Xác định danh sách dữ liệu cần sao lưu và tần suất sao lưu	Có	Sao lưu toàn phần theo tuần, sao lưu gia tăng theo ngày đối với cơ sở dữ liệu; sao lưu cấu hình hệ thống theo tháng hoặc khi có thay đổi
3	Bảo vệ bản sao lưu, bảo đảm tính toàn vẹn, tính sẵn sàng và khả năng khôi phục	Có	Bản sao lưu được kiểm soát truy cập trên hệ thống lưu trữ của Trung tâm Đổi mới sáng tạo và Chuyển đổi số
4	Bản sao lưu được định danh, quản lý phiên bản và lưu trữ tách biệt với môi trường vận hành	Có	Lưu trữ trên hệ thống lưu trữ tách biệt với môi trường vận hành
5	Có quy định sao lưu, khôi phục dữ liệu; định kỳ khôi phục thử	Có	Quy định tại Điều 17 Quy chế bảo đảm an ninh mạng; Trung tâm Đổi mới sáng tạo và Chuyển đổi số đã thực hiện khôi phục thử (mục V.7 Phụ lục I)

PHẦN IV. CAM KẾT CỦA ĐƠN VỊ VẬN HÀNH

Sở Công Thương tỉnh Hưng Yên - đơn vị vận hành hệ thống thông tin "Phần mềm quản lý an toàn thực phẩm ngành Công Thương tỉnh Hưng Yên" - cam kết:

1. Các nội dung thuyết minh trong Hồ sơ đề xuất cấp độ này là trung thực, đầy đủ và phản ánh đúng hiện trạng hệ thống thông tin.
2. Thực hiện các biện pháp bảo vệ an ninh mạng theo phương án đã được phê duyệt và theo quy định của pháp luật, tiêu chuẩn kỹ thuật về an ninh mạng.
3. Định kỳ đánh giá hiệu quả của các biện pháp bảo vệ an ninh mạng, báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết.
4. Phối hợp với đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin và Trung tâm Đổi mới sáng tạo và Chuyển đổi số trong việc xử lý, khắc phục điểm yếu, lỗ hổng bảo mật và ứng phó sự cố an ninh mạng.
5. Phối hợp thực hiện theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng và đáp ứng các điều kiện cần thiết phục vụ giám sát an ninh mạng.
6. Thực hiện chế độ báo cáo định kỳ và báo cáo sự cố an ninh mạng theo Điều 33, Điều 35, Điều 36 NĐ 331.
7. Hoàn thiện các yêu cầu chưa đáp ứng theo đúng thời hạn nêu tại mục 4 Phần III.
8. Trường hợp có thay đổi về chức năng, phạm vi phục vụ, đối tượng sử dụng, loại thông tin xử lý hoặc công nghệ triển khai, kịp thời thực hiện đánh giá lại rủi ro an ninh mạng và xác định lại cấp độ theo Điều 25 NĐ 331./.

ĐẠI DIỆN ĐƠN VỊ VẬN HÀNH