BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 5102 /QĐ-BNNMT	*Hà Nội, ngày 02 tháng 12 năm 2025*

QUYẾT ĐỊNH

Về việc phê duyệt cấp độ và phương án bảo đảm an toàn thông tin cho Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thuỷ văn

BỘ TRƯỞNG BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

Căn cứ Nghị định số 35/2025/NĐ-CP ngày 25 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nông nghiệp và Môi trường;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP;

Căn cứ Quyết định số 1921/QĐ-BNNMT ngày 5 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường;

Xét đề nghị của Cục trưởng Cục Khí tượng Thuỷ văn.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ và phương án bảo đảm an toàn thông tin cho hệ thống thông tin đối với "Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thuỷ văn", cụ thể như sau:

1. Thông tin chung:

a) Tên hệ thống thông tin: Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thuỷ văn.

b) Đơn vị vận hành hệ thống thông tin: Cục Khí tượng Thuỷ văn.

c) Địa chỉ: số 24 Huỳnh Thúc Kháng, phường Láng, Hà Nội.

2. Cấp độ an toàn hệ thống thông tin: cấp độ 3.

3. Phương án bảo đảm an toàn thông tin trong thiết kế và vận hành hệ thống thông tin tương ứng với cấp độ 3 phù hợp với quy định tại Thông tư 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Tiêu chuẩn quốc gia TCVN 11930:2017.

Điều 2. Tổ chức thực hiện

1. Cục Khí tượng Thuỷ văn có trách nhiệm bảo đảm an toàn hệ thống thông tin theo các quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Các cơ quan, tổ chức, cá nhân khi sử dụng Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thuỷ văn phải tuân thủ các quy định có liên quan được nêu trong phương án bảo đảm an toàn cho Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thuỷ văn đã được phê duyệt.

3. Cục Chuyển đổi số có trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này và báo cáo Bộ Nông nghiệp và Môi trường theo quy định của pháp luật.

Điều 3. Hiệu lực và trách nhiệm thi hành

1. Quyết định này có hiệu lực từ ngày ký.

2. Chánh Văn phòng Bộ, Cục trưởng Cục Khí tượng Thuỷ văn, Cục trưởng Cục Chuyển đổi số và Thủ trưởng các đơn vị nêu tại Điều 2 chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng Trần Đức Thắng (để báo cáo);
- Cổng thông tin điện tử Bộ;
- Lưu: VT, VP, KTTV.Linh

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Lê Công Thành

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC KHÍ TƯỢNG THỦY VĂN

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 3
HỆ THỐNG CƠ SỞ HẠ TẦNG THÔNG TIN NGHIỆP VỤ KHÍ TƯỢNG THỦY VĂN

Hà Nội – 2025

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1.	CNTT	Công nghệ thông tin
2.	CSDL	Cơ sở dữ liệu
3.	DVCTT	Dịch vụ công trực tuyến
4.	MCĐT	Một cửa điện tử
5.	WAN	Mạng tin học diện rộng
6.	LAN	Mạng nội bộ
7.	TSLCD	Mạng Truyền số liệu chuyên dùng
8.	VPN	Vitural Private Network
9.	DNS	Domain Name Server

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

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

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Bộ Nông nghiệp và Môi trường.

- Quy định chức năng, nhiệm vụ và quyền hạn: Chủ quản Hệ thống thông tin thực hiện nhiệm vụ, quyền hạn quy định tại Quyết định số 68/2022/NĐ-CP ngày 22 tháng 9 năm 2022 của Phó Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nông nghiệp và Môi trường

- Người đại diện: Trần Đức Thắng, Chức vụ: Bộ trưởng.

- Địa chỉ: 10 Tôn Thất Thuyết, Mỹ Đình, Nam Từ Liêm, Hà Nội

- Thông tin liên hệ:

+ Số điện thoại: 02437956868

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Cục Khí tượng Thủy văn.

- Quy định chức năng, nhiệm vụ và quyền hạn: Chủ quản Hệ thống thông tin thực hiện nhiệm vụ, quyền hạn quy định tại Quyết định số 35 /QĐ-BNNMT ngày 01 tháng 3 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Khí tượng Thủy văn trực thuộc Bộ Nông nghiệp và Môi trường

- Người đại diện: Nguyễn Thượng Hiền, Chức vụ: Cục trưởng.

- Địa chỉ: 24 Huỳnh Thúc Kháng, phường Láng, TP Hà Nội

- Thông tin liên hệ:

+ Số điện thoại: 02432673199 (112)

+ Thư điện tử: tongcuc.kttv@mae.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV: Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV được thiết lập nhằm cung cấp: Môi trường hoạt động cho toàn bộ các thiết bị công nghệ thông tin của các đơn vị tại tòa nhà tác nghiệp KTTV; Hạ tầng đường truyền mạng LAN, mạng Internet cho khối người dùng chuyên môn; Hạ tầng mạng Internet cho các ứng dụng

chuyên môn của các đơn vị trực thuộc Cục KTTV bao gồm các đơn vị làm việc tại tòa nhà tác nghiệp Khí tượng Thủy văn, 3 Đài KTTV khu vực và 31 Đài KTTV tỉnh trên cả nước ; Hạ tầng máy chủ phục vụ công tác chuyên môn, công tác chỉ đạo điều hành trong phạm vi Cục KTTV.

- Đối tượng phục vụ của hệ thống: Cơ quan, đơn vị trực thuộc Cục KTTV.

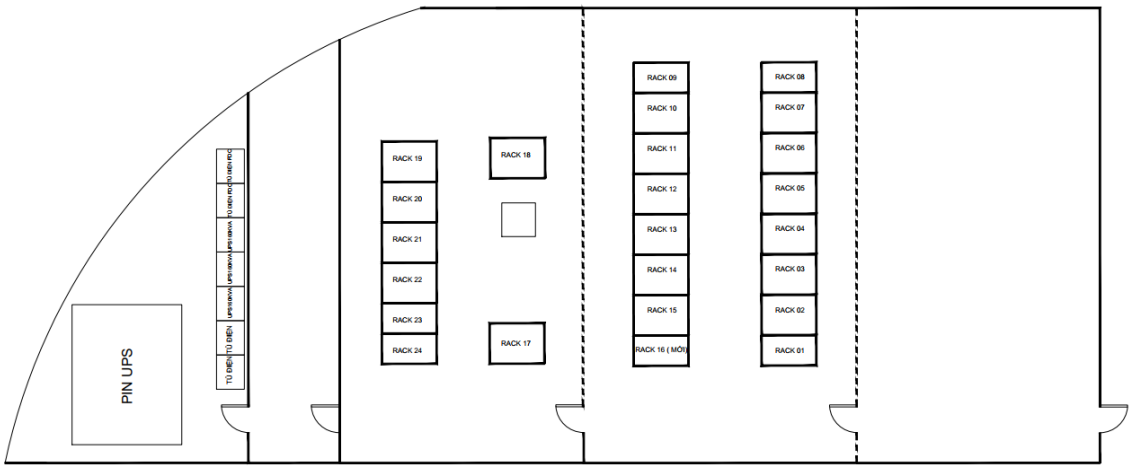
- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi trung tâm dữ liệu:

+ Hệ thống cơ sở hạ tầng công nghệ thông tin;

+ Các máy chủ nghiệp vụ triển khai nền tảng ảo hóa cung cấp hạ tầng máy chủ phục vụ công tác thu nhận, xử lý, chia sẻ, lưu trữ dữ liệu KTTV.

4. Mô tả cấu trúc của hệ thống

4.1. Sơ đồ mặt bằng Trung tâm dữ liệu



MẶT BẰNG TTDL

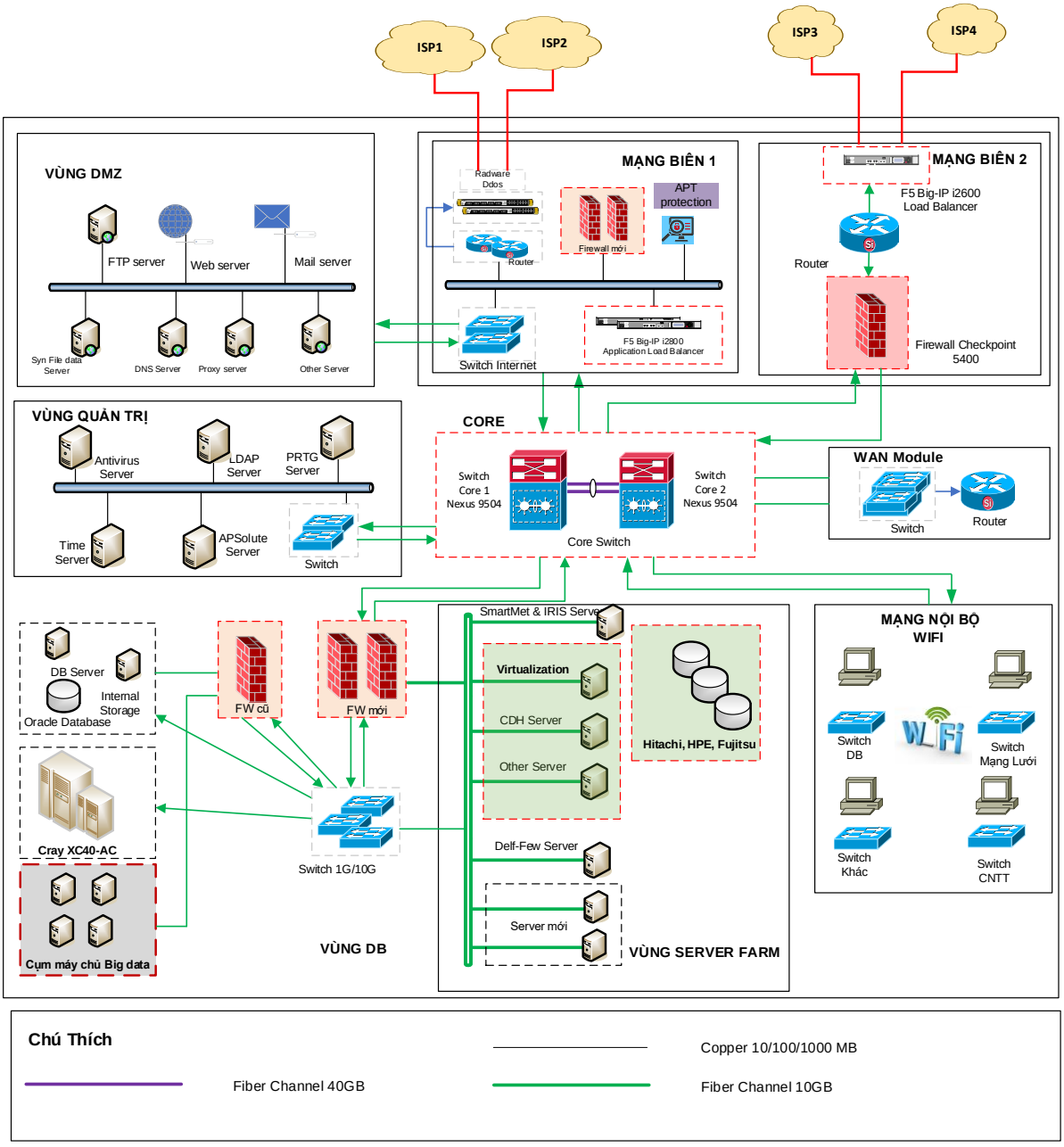
Hiện tại TTDL của Cục Khí tượng Thủy văn đặt tại tầng 3 tòa nhà tác nghiệp KTTV. Tổng diện tích gần 350m2. Đã được trang bị đầy đủ tất cả các hạng mục theo tiêu chuẩn của một TTDL bao gồm: hệ thống Sàn nâng, UPS, báo cháy, báo khói, thang máng cáp, hệ thống điều hòa chính xác, hệ thống tiếp địa, hệ thống chống sét…..

Hệ thống UPS bao gồm 03 UPS với tổng công suất 480KVA cấu hình 2N+1, đảm bảo tính dự phòng. Hiện tại công xuất tiêu thụ hiên tại chỉ chiếm 10-15%.

Hệ thống điều hòa chính xác có 04 thiết bị cấu hình hoạt động phân tải và dự phòng.

Các thiết bị được đầu tư trong khuôn khổ của dự án sẽ được triển khai lắp đặt Trong TTDL. Như vậy toàn bộ các thiết bị và hệ thống sẽ được kế thừa toàn bộ cơ sở vật chất hạ tầng trong Trung tâm Dữ liệu của Cục KTTV.

4.2. Mô hình logic



Hình 4.2.2. Mô hình logic của Trung tâm dữ liệu

Các vùng mạng được thiết kế như sau:

− Vùng mạng biên 1 thiết kế để kết nối hệ thống các máy chủ nghiệp vụ ra các mạng bên ngoài và mạng Internet; bảo vệ các máy chủ nghiệp vụ từ bên ngoài Internet. Vùng mạng này triển khai hệ thống phòng chống tấn công DdoS; hệ thống Firewall thế hệ mới tích hợp tính năng IPS; thiết bị phòng chống tấn công có chủ đích (ATP);

- Vùng mạng biên 2 thiết kế kết nối hệ thống mạng người dùng ra mạng Internet. Vùng mạng này triển khai hệ thống Firewall;

− Vùng Server DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet như: DNS, FTP, Email, NTP, Sync file data…;

- Vùng Core module, đây là vùng xử lý dữ liệu liên vùng;

− Vùng Quản trị, đây là vùng mạng quản trị đặt các máy chủ quản trị hệ thống.

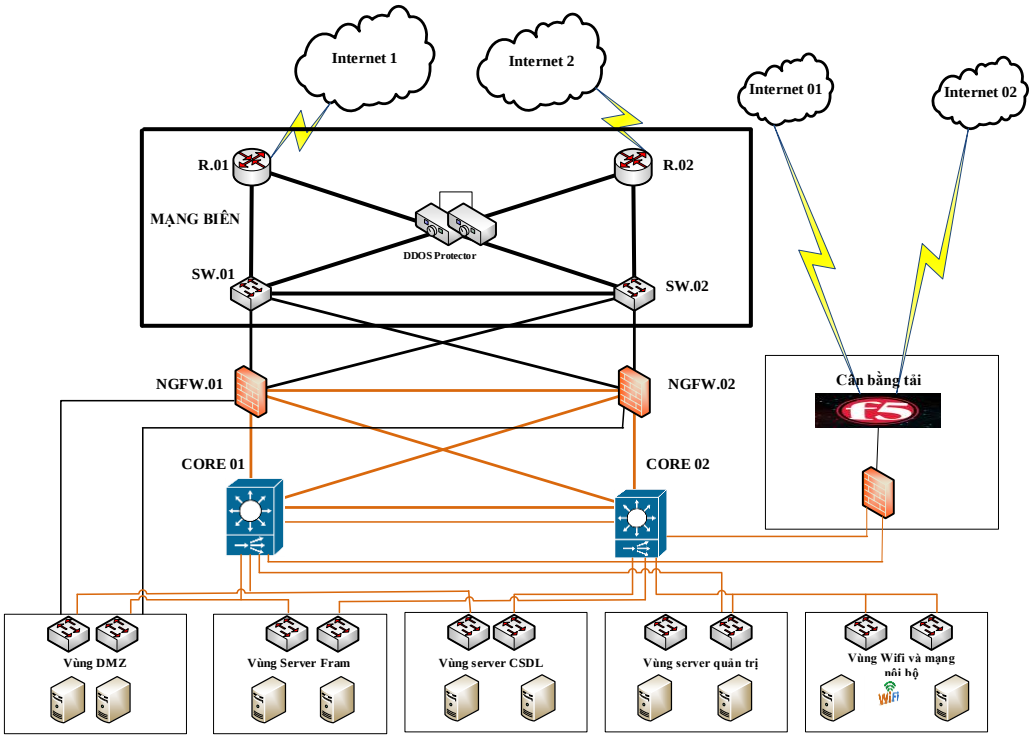
− Vùng máy chủ nội bộ đặt các máy chủ nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị ATP và các máy chủ nghiệp vụ.

− Vùng máy chủ cơ sở dữ liệu (Server DB) đặt các máy chủ cơ sở dữ liệu phục vụ việc lưu trữ và quản lý cơ sở dữ liệu tập trung trên hệ thống. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị DB Firewall CSDL.

- Vùng WAN. Vùng dữ liệu chia sẽ liên ngành; Tích hợp với các các hệ thống khác theo tiêu chuẩn NGSP;

- Vùng mạng nội bộ và Wifi (vùng mạng nội bộ). Vùng máy tính của người dùng các đơn vị chuyên môn tại Cục KTTV và Wifi;

4.3. Mô hình kết nối vật lý



Hình 4.3.2. Mô hình kết nối vật lý

4.4. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	FW01/ Checkpoint 5400	Vùng Server Farm	Quản lý truy cập vào/ra và bảo vệ vùng mạng Server farm.
2	FW02/ Cisco 5520 (Checkpoint 5900 dự phòng)	Vùng DMZ	Quản lý truy cập vào/ra và bảo vệ các vùng mạng DMZ.
3	Ddos 01/Defenpro 1016	Vùng mạng biên	Bảo vệ chống tấn công từ chối dịch vụ kênh truyền VNPT.
4	NGFW01 (Palloalto 5410)	Vùng Server Farm; Vùng DB	Quản lý truy cập vào/ra và bảo vệ vùng mạng Server farm, vùng DB

5	NGFW02 (Palloalto 5410)	Vùng DMZ	Quản lý truy cập vào/ra và bảo vệ các vùng mạng DMZ.
6	APT	Vùng mạng biên	Bảo vệ chống tấn công có chủ đích
7	Ddos 02/Radware	Vùng mạng biên	Bảo vệ chống tấn công từ chối dịch vụ kênh truyền NetNam
8	L2 SW01/ Cisco 2960S	Vùng mạng nội bộ	Thiết bị chuyển mạch vùng mạng nội bộ.
9	SW Core01/ Cisco Nexus 9504	Vùng mạng lõi	Thiết bị chuyển mạch vùng mạng lõi.
10	SW Core02/ Cisco Nexus 9504	Vùng mạng lõi	Thiết bị chuyển mạch vùng mạng lõi.
11	L2 SW02/ Cisco 2960S	Vùng mạng nội bộ	Thiết bị chuyển mạch vùng mạng nội bộ.
12	L2 SW03/ Cisco 2960S	Vùng mạng nội bộ	Thiết bị chuyển mạch vùng mạng nội bộ.
13	L2 SW04/ Cisco 2960S	Vùng mạng nội bộ	Thiết bị chuyển mạch vùng mạng nội bộ.
14	L2 SW05/ Cisco 2960S	Vùng mạng nội bộ	Thiết bị chuyển mạch vùng mạng nội bộ.
15	L3 SW01/ Cisco 3750	Vùng mạng nội bộ	Thiết bị chuyển mạch vùng mạng nội bộ.
16	L3 SW02/ Cisco 3750	Vùng mạng nội bộ	Thiết bị định tuyến vùng mạng chủ nội bộ. Dự phòng nóng 1-1 cho L3 SW01/

17	SAN01/ Hitachi	Vùng Server Farm và vùng DB	Thiết bị lưu trữ SAN Storage (lưu trữ dữ liệu và triển khai DB)
18	SAN02/ Fujitsu	Vùng Server Farm và vùng DB	Thiết bị lưu trữ SAN Storage (lưu trữ dữ liệu và triển khai DB, triển khai ảo hóa)
19	F5	Vùng mạng nội bộ và Wifi	Thiết bị cân bằng tài vùng mạng người dung và Wifi

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

4.5. Danh mục máy chủ

STT	Tên thiết bị/Chủng loại/Hệ điều hành	Địa chỉ IP	Vị trí triển khai	Mục đích sử dụng	Đối tượng được phép truy cập	Cổng dịch vụ
	VM 01 -VM 12/ Máy chủ vật lý cho hệ thống ảo hóa (HP HP DL360 Gen10/ Red Hat 7.0)	10.152.2.10 - 10.152.2.21	Vùng mạng nội bộ	Máy chủ cài đặt nền tảng ảo hóa Ovirt	IP nằm trong vùng quản trị (Admin zone)	iLO: 443
	VM 13 -VM 20/ Máy chủ vật lý cho hệ thống ảo hóa (Fujitsu PRIMERGY RX2540 M5/ Linux (Debian 11)	10.152.2.30 - 10.152.2.37	Vùng mạng nội bộ	Máy chủ cài đặt nền tảng ảo hóa Promox	IP nằm trong vùng quản trị (Admin zone)	iRMC S5: 443

	VM 21 -VM 22/ Máy chủ vật lý cho hệ thống ảo hóa (Dell R750/ Linux (Debian 11)	10.152.2.38 - 10.152.2.39	Vùng mạng nội bộ	Máy chủ cài đặt nền tảng ảo hóa Promox	IP nằm trong vùng quản trị (Admin zone)	iDrac:443
	Máy chủ Dell R 740/Centos 7.0	10.151.2.40	Vùng mạng riêng	Máy chủ cài đặt tổng đài VoIP	IP nằm trong vùng quản trị (Admin zone)	iDrac:443

Bảng 2. Danh mục thiết bị máy chủ sử dụng trong hệ thống

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đặt/Vùng mạng/HĐH	Mục đích sử dụng
1	Ảo hóa (Ovirt)	Server 01-Server 12/, Ret Hat 7.0/ Ftp, Share file, Web / Vùng máy chủ nội bộ, máy chủ DMZ/ Linux (triển khai ảo hóa Promox); port: 20, 21, 135, 137, 139, 445, 1433, 4022, 135, 1434, 80, 443, 53, 22, 4000-5000, 8080, 8000-8022, udp123, tcp 4545, 4546, 8088, 8089, 9443, 9453, 9454, 9773, 9774, 9775	Triển khai các thành phần máy chủ ảo hóa cài đặt các ứng dụng chuyên môn nghiệp vụ
2	Ảo hóa (Promox)	Server 13- Server 20/Debiant 11/ Ftp Socket/Share file/Vùng máy chủ nội bộ, máy chủ vùng DMZ/ Window server 2019; port: 20, 21, 135, 137, 139, 445, 1433, 4022, 135, 1434, 80, 443, 53, 22, 4000-5000, 8080, 8000-8022, udp123, tcp 4545, 4546, 8088, 8089, 9443, 9453, 9454, 9773, 9774, 9775, 6000, 12000	Triển khai các thành phần máy chủ ảo hóa cài đặt các ứng dụng chuyên môn nghiệp vụ (Trung tâm Thông tin và Dữ liệu KTTV)
3	Ảo hóa (Promox)	Server 21- Server 22/Debiant 11/ Ftp Socket/Share file/Vùng máy chủ nội bộ, máy chủ vùng DMZ/ Window server 2019; port: 20, 21, 135, 137, 139, 445, 1433, 4022, 135, 1434, 80, 443, 53, 22, 4000-5000, 8080, 8000-8022, udp123, tcp 4545, 4546, 8088, 8089, 9443, 9453, 9454, 9773, 9774, 9775, 6000, 12000	Triển khai các thành phần máy chủ ảo hóa cài đặt các ứng dụng chuyên môn nghiệp vụ (Trung tâm Dự báo KTTV quốc gia)

4	VoIP	Server 23- Server 24/ Centos 7.0/ SIP, H323, SRTP, RTCP, UDP, SDP	Dịch vụ Thoại qua mạng (LAN, Internet)

Bảng 3. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

STT	Vùng mạng	IP Private	IP Public
1	DMZ	192.168.1.0/24	222.255.xx.xx/26 101.96.xx.xx/27 14.238.xx.xx/29 101.96.xx.xx/29 14.238.xx.xx/32
2	Vùng mạng quản trị	10.152.2.1/25	
3	Vùng máy chủ nội bộ	10.151.2.1/25 10.151.7.1/25 10.151.0.1/23 10.151.4.1/24 10.151.5.1/24 10.151.2.128/25 10.151.3.0/24 10.151.8.1/25	
4	Vùng máy chủ DB	10.151.9.1/25	

Bảng 4. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống thông tin của Đơn vị vận hành bao gồm các hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

STT	Hệ thống thông tin	Mục đích sử dụng	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
	Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thủy văn	Cung cấp môi trường, hạ tầng CNTT, các giải pháp an toàn thông tin cho các máy chủ, thiết bị, dịch vụ đặt tại Trung tâm dữ liệu Cục KTTV	Thông tin riêng	Hệ thống cơ sở hạ tầng thông tin	3	Khoản 3/Điều 9 trong 85/2016/NĐ-CP

2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin

Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thủy văn xử lý thông tin riêng căn cứ theo Điểm b Khoản 1 Điều 6 Nghị định 85/2016/NĐ-CP, và thuộc loại hình Hệ thống cơ sở hạ tầng thông tin căn cứ theo Điểm b, Khoản 2, Điều 6 Nghị định 85/2016/NĐ-CP. Do đó, Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thủy văn thuộc phạm vi quản lý của Bộ Nông nghiệp và Môi trường được đề xuất cấp độ 3 theo Khoản 3, Điều 9 trong Nghị định 85/2016/NĐ-CP.

PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

3.1. Căn cứ pháp lý

- 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

- Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 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

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

- Căn cứ Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế đảm bảo an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường;

- Quyết định số 335/QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh thông tin mạng Cục Khí tượng Thủy văn.

3.2. Thuyết minh phương án về quản lý bao gồm các nội dung sau:

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

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

- Quản lý an toàn thiết bị đầu cuối

- Quản lý phòng chống phần mềm độc hại

- Quản lý giám sát an toàn hệ thống thông tin

- Quản lý điểm yếu an toàn thông tin

- Quản lý sự cố an toàn thông tin

- Quản lý an toàn người sử dụng đầu cuối.

Đối với những yêu cầu quản lý chưa đáp ứng các yêu cầu an toàn trong Thuyết minh này, Đơn vị vận hành sẽ cập nhật, bổ sung trình Chủ quản hệ thống thông tin ban hành trong tháng 12 năm 2024.

3.3. Thuyết minh phương án về kỹ thuật bao gồm các nội dung:

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

1.2. Kiểm soát truy cập từ bên ngoài mạng

1.3. Kiểm soát truy cập từ bên trong mạng

1.4. Nhật ký hệ thống

1.5. Phòng chống xâm nhập

1.6. Phòng chống phần mềm độc hại trên môi trường mạng

1.7. Bảo vệ thiết bị hệ thống

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

2.6. Xử lý máy chủ khi chuyển giao

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

3.4. Bảo mật thông tin liên lạc

3.5. Chống chối bỏ

4. Bảo đảm an toàn dữ liệu

4.1. Nguyên vẹn dữ liệu

4.2. Bảo mật dữ liệu

4.3. Sao lưu dự phòng

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong các năm tiếp theo.

Thuyết minh phương án bảo đảm an toàn thông tin về quản lý đưa ra các quy định liên quan đến con người và quy trình. Các yêu cầu quản lý ở cấp độ cao hơn khi được đáp ứng thì cũng đáp ứng các yêu cầu ở cấp độ thấp hơn. Do đó, thuyết minh phương án bảo đảm an toàn thông tin về quản lý được thuyết minh chung tại Phụ lục I.

Đối với hạ tầng, thiết bị hệ thống, máy chủ dùng chung để bảo vệ nhiều hệ thống thành phần khác nhau, thì hạ tầng, thiết bị hệ thống, máy chủ đó phải được thiết kế, thiết lập để đáp ứng yêu cầu của hệ thống thành phần có cấp độ cao nhất để bảo đảm an toàn thông tin cho cả hệ thống. Do đó, phải thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật theo cấp độ 3.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống cơ sở hạ tầng thông tin nghiệp vụ khí tượng thủy văn của Cục sẽ bao gồm các nội dung sau:

STT	Phương án	Cấp độ đề xuất	Nội dung thuyết minh
1	Thuyết minh phương án đáp ứng yêu cầu quản lý	3	Phụ lục I
2	Thuyết minh phương án đáp ứng yêu cầu kỹ thuật	3	Phụ lục II

PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 3

7.1.1. Thiết lập chính sách an toàn thông tin

7.1.1.1. Chính sách an toàn thông tin

Yêu cầu 7.1.1.1. a	Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng. Quy định tại Điều 3, Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Nguyên tắc (Tham chiếu Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn 1. Đảm bảo an toàn thông tin về vật lý đối với trung tâm dữ liệu, phòng máy chủ theo Điều 9. 2. Chính sách Quản lý an toàn, an ninh thông tin đối với hạ tầng mạng, hệ thống máy chủ và thiết bị đầu cuối, thiết bị số Điều 10. 3. Quản lý an toàn, an ninh thông tin đối với ứng dụng, phần mềm, dịch vụ cài đặt trên máy chủ theo Điều 12. 4. Chính sách Quản lý an toàn thông tin dữ liệu thực hiện theo Điều 13. 5. Chính sách Quản lý trang thiết bị đầu cuối theo Điều 10. 6. Chính sách quản lý tài khoản truy cập theo Điều 11.
Yêu cầu 7.1.1.1. b	Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.
Hiện trạng	Đáp ứng.

	(Tham chiếu Quyết định số số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn)
Phương án	1) Đối tượng, phạm vi điều chỉnh: Điều 1 1. Phạm vi điều chỉnh: Phạm vi điều chỉnh: Quy chế này quy định về công tác bảo đảm an toàn thông tin mạng, an ninh mạng trong các hoạt động của Cục Khí tượng Thuỷ văn và các đơn vị trực thuộc Cục. 2. Đối tượng áp dụng a) Các đơn vị trực thuộc Cục Khí tượng Thuỷ văn và cán bộ, công chức, viên chức và người lao động thuộc các đơn vị trực thuộc Cục; b) Cơ quan, tổ chức, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng của Cục Khí tượng Thuỷ văn; c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng, an ninh mạng cho các đơn vị trực thuộc Cục Khí tượng Thuỷ văn. 2) Đơn vị chuyên trách: Khoản 3, Điều 5 1. Trung tâm Thông tin và Dữ liệu khí tượng thủy văn là đơn vị chuyên trách về an toàn thông tin của Cục Khí tượng Thuỷ văn; 2. Bộ phận chuyên trách về công nghệ thông tin tại các đơn vị trực thuộc Cục thực hiện chuyên trách về an toàn thông tin của đơn vị đó..
Yêu cầu **7.1.1.1.c**	Xác định phạm vi chính sách an toàn thông tin 1. Phạm vi quản lý về vật lý và logic của tổ chức. 2. Các ứng dụng, dịch vụ hệ thống cung cấp. 3. Nguồn nhân lực đảm bảo an toàn thông tin.
Hiện trạng	Đáp ứng. Đã quy định tại Điều 1 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn .

Phương án	**Điều 1.** 1. Phạm vi điều chỉnh Quy chế này quy định về bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động của Cục Khí tượng Thủy văn và các đơn vị trực thuộc Cục. 2. Đối tượng áp dụng a) Các đơn vị trực thuộc Cục Khí tượng Thủy văn (sau đây gọi là đơn vị trực thuộc Cục) và cán bộ, công chức, viên chức và người lao động thuộc các đơn vị trực thuộc Cục Khí tượng Thủy văn. b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Cục Khí tượng Thủy văn. c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị trực thuộc Cục Khí tượng Thủy văn.
Yêu cầu **7.1.1.1.d**	Xây dựng chính sách an toàn thông tin bao gồm: - Quản lý an toàn mạng; - Quản lý an toàn máy chủ và ứng dụng; - Quản lý an toàn dữ liệu; - Quản lý an toàn thiết bị đầu cuối; - Quản lý phòng chống phần mềm độc hại; - Quản lý điểm yếu an toàn thông tin; - Quản lý giám sát an toàn hệ thống thông tin; - Quản lý an toàn người sử dụng đầu cuối
Hiện trạng	Đáp ứng. Đã quy định từ Điều 7 đến Điều 11 và Điều 14 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn .

Phương án	Tuân thủ các quy định trong Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn , cụ thể như sau: 1. Hệ thống mạng nội bộ của Cục Đã được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị, vùng Wifi, cụ thể theo mục 4.1.2 (mô hình logic), mục 4.2.1 (mô hình kết nối vật lý); 2. Dữ liệu trao đổi giữa các vùng mạng được kiểm soát bởi tường lửa giữa các phân vùng mạng (được mô tả tại 4.1.2 mô hình logic, mục 4.2.1 mô hình kết nối vật lý) đồng thời được kiểm tra, giám sát bởi bộ phận bộ phận trực giám sát dữ liệu; 3. Hệ thống Firewall được triển khai ở 02 phân vùng cơ bản: phân vùng DMZ và phân vùng server Farm. Thiết bị Firewall của 2 phân vùng sử dụng hai hãng khác nhau. Tùy từng chức năng và yêu cầu nghiệp vụ của từng hệ thống, mỗi hệ thống được thiết kế các chính sách riêng nhằm đảm bảo việc truy xuất giữa các phân vùng được tối ưu và đảm bảo an toàn. 4. Các máy chủ được triển khai tại các phân vùng server farm và DMZ trước khi đưa vào vận hành đều được cài đặt phần mềm diệt virus có bản quyền, đồng thời phân quyền quản trị theo nhu cầu và chức năng nhiệm vụ của từng bộ phận. Ngoài ra các máy chủ được kiểm soát chặt chẽ trong việc truy cập giữa máy chủ các phân vùng, truy cập Internet các máy chủ (mở các cổng, dịch vụ cần thiết ví dụ như ftp, web, ssh…). 5. Các thiết bị mạng được sao lưu thường xuyên. Ngoài ra khi có thay đổi về mặt cấu trúc, chính sách cụ thể các thông tin cấu hình này đều được sao lưu lại. 6. Kết nối mạng Internet của người dùng và các máy chủ Public

	được kiểm soát bởi thiết bị Firewall. Ngoài ra các đơn vị đều phải tuân thủ các quy định và chính sách về ATTT được quy định tại các văn bản liên quan.

7.1.1.2. Xây dựng và công bố

Yêu cầu 7.1.1.2.a	Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng
Hiện trạng	Đáp ứng. Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn
Phương án	Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: 1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng 2. Quy chế được Đơn vị vận hành xây dựng trình Chủ quản Hệ thống thông tin ban hành.
Yêu cầu 7.1.1.2.b	Chính sách được công bố trước khi áp dụng
Hiện trạng	Đáp ứng: Quy định tại Điều 27 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn .
Phương án	**Điều 21. Trách nhiệm thi hành** 1. Quy định này có hiệu lực thi hành kể từ ngày ký ban hành. 2. Thủ trưởng các đơn vị trực thuộc Cục Khí tượng Thủy văn có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, nhân viên trong đơn vị thực hiện các quy định của Quy chế này 3. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ảnh về Trung tâm Thông tin và Dữ liệu khí tượng thủy văn để tổng hợp, trình Cục Khí tượng Thủy

	văn (qua Vụ Quản lý dự báo khí tượng thủy văn) xem xét, sửa đổi, bổ sung Quy chế)

7.1.1.3. Rà soát, sửa đổi

Yêu cầu 7.1.1.3	Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
Hiện trạng	Đáp ứng. Đã quy định tại Khoản 2 Điều 27 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn
Phương án	Điều 27. Trách nhiệm thi hành 2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ảnh về Trung tâm Thông tin và Dữ liệu khí tượng thủy văn để tổng hợp, trình Cục Khí tượng Thủy văn (qua Vụ Quản lý dự báo khí tượng thủy văn) xem xét, sửa đổi, bổ sung Quy chế

7.1.2. Tổ chức bảo đảm an toàn thông tin

7.1.2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức
Hiện trạng	Đáp ứng. Quy định tại Khoản 3 Điều 5 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Khoản 3 Điều 5 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn. 3. Đơn vị, bộ phận chuyên trách về an toàn thông tin a) Cục giao Trung tâm Thông tin và Dữ liệu khí tượng thủy văn là đơn vị chuyên trách về an toàn thông tin của Cục Khí tượng Thủy văn.

	b) Bộ phận chuyên trách về công nghệ thông tin tại các đơn vị trực thuộc Cục thực hiện chuyên trách về an toàn thông tin của đơn vị đó.
Yêu cầu	Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin.
Hiện trạng	Đáp ứng. Đã quy định tại Khoản 2, Khoản 3 Điều 5 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điều 5. Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn. 2. Đơn vị vận hành hệ thống thông tin a) Giao Trung tâm Thông tin và Dữ liệu khí tượng thủy văn vận hành các hệ thông thông tin và cơ sở dữ liệu dùng chung đặt tại Cục Khí tượng Thủy văn. b) Các đơn vị trực thuộc Cục vận hành hệ thống thông tin và cơ sở dữ liệu thuộc trách nhiệm quản lý của đơn vị mình. Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành. 3. Đơn vị, bộ phận chuyên trách về an toàn thông tin a) Giao Trung tâm Thông tin và Dữ liệu khí tượng thủy văn là đơn vị chuyên trách về an toàn thông tin của Cục Khí tượng Thủy văn. b) Bộ phận chuyên trách về công nghệ thông tin tại các đơn vị trực thuộc Cục thực hiện chuyên trách về an toàn thông tin của đơn vị đó.

7.1.2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin.

7.1.2.2.a	
Hiện trạng	Đáp ứng. Đã quy định tại tại Khoản 5 Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn
Phương án	Cục giao Trung tâm Thông tin và Dữ liệu KTTV làm đầu mối phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin, danh sách thành viên bao gồm: 1. Ông Hoàng Đức Cường; Chức vụ: Phó Cục trưởng; Điện thoại: 0912347504; Email: hdcuong@nchmf.gov.vn 2. Ông Ngô Văn Mạnh; Chức vụ: Phó giám đốc; Điện thoại: 0975594713; Email: Manh.ngovan@gmail.com 3. Ông Phạm Đức Thắng; Chức vụ: Phó trưởng phòng; Điện thoại: 0965578688; Email: pdthang@monre.gov.vn 4. Ông Nguyễn Trọng Nghĩa; Chức vụ: Cán bộ kỹ thuật. Điện thoại: 0983412185; Email: nghia121@gmail.com
Yêu cầu 7.1.2.2.b	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin
Hiện trạng	Đáp ứng. Điều 17. Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Theo đó Cục KTTV giao Trung tâm Thông tin và Dữ liệu làm đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin, danh sách thành viên bao gồm: 1. Ông Hoàng Đức Cường; Chức vụ: Phó Cục trưởng; Điện thoại: 0912347504; Email: hdcuong@nchmf.gov.vn 2. Ông Ngô Văn Mạnh; Chức vụ: Phó giám đốc; Điện thoại: 0975594713; Email: Manh.ngovan@gmail.com

	3. Ông Phạm Đức Thắng; Chức vụ: Phó trưởng phòng; Điện thoại: 0965578688; Email: pdthang@monre.gov.vn 4. Ông Nguyễn Trọng Nghĩa; Chức vụ: Cán bộ kỹ thuật. Điện thoại: 0983412185; Email: nghia121@gmail.com
Yêu cầu 7.1.2.2.c	Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền
Hiện trạng	Đáp ứng. Đã quy định tại tại Điểm b, c khoản 1 Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	b. Cử cán bộ chuyên trách tham gia Đội ứng cứu sự cố an toàn thông tin mạng của Bộ theo đề nghị của Cục Chuyển đổi số. c. Chủ trì liên hệ với Đội ứng cứu sự cố an toàn thông tin mạng của Bộ để nhận hỗ trợ ứng cứu an toàn thông tin mạng của Cục.

7.1.3. Tổ chức bảo đảm an toàn thông tin

7.1.3.1. Tuyển dụng

Yêu cầu 7.1.3.1.a	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng
Hiện trạng	**Đáp ứng.** Đã quy định tại Khoản 1, Điều 14 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	1. Điều kiện, yêu cầu của nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an toàn, an ninh mạng a) Có phẩm chất đạo đức tốt, có đủ tiêu chuẩn chính trị, có kiến thức pháp luật và chuyên môn, nghiệp vụ về bảo vệ thông tin bí mật, nghiêm chỉnh chấp hành đường lối, chủ trương, chính sách của Đảng, pháp luật của Nhà nước.

	b) Có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng. Hiện tại đơn vị chuyên trách về công nghệ thông tin là Trung tâm Thông tin và Dữ liệu KTTV. Có 10 cán bộ chuyên trách về công nghệ thông tin có bằng cử nhân hoặc kỹ sư công nghệ thông tin.
Yêu cầu 7.1.3.1.b	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ
Hiện trạng	**Đáp ứng.** Đã xây dựng và ban hành quy trình nội bộ đối với các nội dung liên quan đến tuyển dụng, ký và chấm dứt hợp đồng lao động. Ngoài ra quy định về việc tuyển dụng cán bộ Đã quy định tại Khoản 1, Điều 14 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	1. Điều kiện, yêu cầu của nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an toàn, an ninh mạng a) Có phẩm chất đạo đức tốt, có đủ tiêu chuẩn chính trị, có kiến thức pháp luật và chuyên môn, nghiệp vụ về bảo vệ thông tin bí mật, nghiêm chỉnh chấp hành đường lối, chủ trương, chính sách của Đảng, pháp luật của Nhà nước. b) Có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng. Hiện tại đơn vị chuyên trách về công nghệ thông tin là Trung tâm Thông tin và Dữ liệu KTTV. Có 10 cán bộ chuyên trách về công nghệ thông tin có bằng cử nhân hoặc kỹ sư công nghệ thông tin.

7.1.3.2. Trong quá trình làm việc

Yêu cầu 7.1.3.2.a	Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống

Hiện trạng	Đáp ứng Đã quy định tại Khoản 2, Điều 14, Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	2. Quy định trách nhiệm bảo đảm an toàn, an ninh thông tin trong quản lý và sử dụng nhân sự Các đơn vị trực thuộc Cục Khí tượng Thủy văn có trách nhiệm: a) Xác định các yêu cầu và trách nhiệm cụ thể của bộ phận, cán bộ, nhân viên trong việc bảo đảm an toàn, an ninh thông tin cho từng vị trí phân công. b) Phổ biến cho nhân sự mới tuyển dụng các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị. Định kỳ tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong đơn vị. c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị. d) Có biện pháp quản lý tài khoản người dùng của cán bộ, công chức, viên chức và người lao động trên các hệ thống thông tin quan trọng. đ) Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý. Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

Yêu cầu 7.1.3.2.b	Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.
Hiện trạng	Đáp ứng. Đã quy định tại Điều 18 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Việc phổ biến tuyên truyền nâng cao nhận thức về ATTT được Cục KTTV thực hiện thường xuyên và liên tục thông qua các cuộc họp, đường công văn. Ngoài ra đơn vị vận hành hệ thống thông tin đã đề xuất bổ sung nhiệm vụ có lồng ghép nội dung phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.
Yêu cầu 7.1.3.2.c	Định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.
Hiện trạng	Đáp ứng. Đã quy định tại Điều 18 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Căn cứ nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin của các đơn vị trực thuộc Cục Khí tượng Thủy văn xây dựng trình Cục xem xét, báo cáo Bộ Nông nghiệp và Môi trường tổng hợp, phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Cục và phối hợp tổ chức thực hiện đào tạo theo kế hoạch đã phê duyệt.

7.1.3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu 7.1.3.3.a	Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức

Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ đối với các nội dung liên quan đến tuyển dụng, ký và chấm dứt hoặc thay đổi công việc, đồng thời cũng quy định tại Khoản 3, Điều 14 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	3. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, các đơn vị phải: a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao. b) Lập biên bản bàn giao tài sản công nghệ thông tin với đơn vị chủ quản và các đơn vị liên quan. c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin. d) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin để bảo đảm tài khoản người dùng của cán bộ, công chức, viên chức và người lao động đã nghỉ việc được thu hồi.
Yêu cầu 7.1.3.3.b	Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc
Hiện trạng	Đáp ứng. Đã quy định tại Điểm c, d Khoản 3, Điều 14 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm c, d, Khoản 3, Điều 14 3. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, các đơn vị phải: c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

	d) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin để bảo đảm tài khoản người dùng của cán bộ, công chức, viên chức và người lao động đã nghỉ việc được thu hồi.
Yêu cầu 7.1.3.3.c	Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.
Hiện trạng	Đáp ứng. Đã quy định tại Khoản 2, Mục c, Điều 14 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm c, Khoản 2 Điều 14 c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị.

7.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin

7.1.4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu 7.1.4.1.a	Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin
Hiện trạng	Đáp ứng.
Phương án	Tài liệu thiết kế hệ thống đã được trình các cấp thẩm định và phê duyệt theo quy định. Thông tin tổng thể về hệ thống đã được mô tả chi tiết tại Phần I "Thông tin tổng quan về hệ thống"
Yêu cầu 7.1.4.1.b	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin

Hiện trạng	Đáp ứng
Phương án	Tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin có trong tài liệu thiết kế hệ thống, tài liệu nạy đã được trình các cấp thẩm định và phê duyệt theo quy định. Thông tin tổng thể về hệ thống đã được mô tả chi tiết tại Phần I "Thông tin tổng quan về hệ thống"
Yêu cầu 7.1.4.1.c	Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ
Hiện trạng	Tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ có trong tài liệu thiết kế hệ thống.
Phương án	Tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ. Sơ bộ phương án bảo đảm an toàn thông tin đã được mô tả tại Phần I "Thông tin tổng quan về hệ thống"
Yêu cầu 7.1.4.1.d	Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng: Tài liệu thiết kế hệ thống được xây dựng dựa trên nội dung Thông tư 14/2020 ngày 27 tháng 11 năm 2020 của Bộ Tài nguyên và Môi trường "ban hành quy trình và định mức kinh tế - kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường"
Phương án	Tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin có trong tài liệu thiết kế hệ thống. Cụ thể Mục 4.1.2. Phương án triển khai hệ thống (trang 40 đến trang 45"; Mục 4.2.2. Phương án kết nối giữa các thiết bị (trang 86 đến trang 95); Mục 4.2.5. Phương án tối ưu hóa và cấu hình bảo mật (trang 253 đến trang 255); Mục 4.2.6. Phương án vận hành và quản trị hệ thống (trang 256 đến trang 258).

Yêu cầu 7.1.4.1.đ	Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.
Hiện trạng	Đáp ứng
Phương án	Trong quá trình triển khai nếu phát sinh các vấn đề liên quan đến ATTT, đơn vị sẽ thực hiện quy trình thay đổi thiết kế đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, lấy ý kiến các đơn vị có liên quan và trình đơn vị cấp trên xem xét và phê duyệt.

7.1.4.2. Phát triển phần mềm thuê khoán

Yêu cầu 7.1.4.2.a	Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán
Hiện trạng	Đáp ứng: Các nội dung về biên bản, hộ đồng được hoàn thiện dựa trên Thông tư 14/2020 ngày 27 tháng 11 năm 2020 của Bộ Tài nguyên và Môi trường "ban hành quy trình và định mức kinh tế - kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường.
Phương án	Danh mục các tài liệu trong quá trình phát triển và đưa vào hoạt động nghiệp vụ các phần mềm thuê khoán bao gồm: 1. Hợp đồng; 2. Biên bản nghiệm thu vận hành thử mức hệ thống phần mềm CNTT; 3. Báo cáo kết quả vận hành thử hệ thống; 4. Biên bản nghiệm thu từng hạng mục, nội dung; 5. Biên bản nghiệm thu hoàn thành hệ thống
Yêu cầu 7.1.4.2.b	Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

Hiện trạng	Đáp ứng. Nội dung được quy định tại tại Mục I, Mục II, Mục IV, Chương III. Quy trình kiểm tra, nghiệm thu sản phẩm công nghệ thông tin ngành Tài nguyên và Môi trường, Thông tư 14/2020/TT-MTNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường
Phương án	Các tài liệu nghiệm thu đã được tiến hành theo quy định Thông tư 14/2020 ngày 27 tháng 11 năm 2020 của Bộ Tài nguyên và Môi trường "ban hành quy trình và định mức kinh tế - kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường", tài liệu nghiệm thu bao gồm các thành phần sau: 1. Biên bản nghiệm thu vận hành thử mức hệ thống phần mềm CNTT; 2. Báo cáo kết quả vận hành thử hệ thống; 3. Biên bản nghiệm thu từng hạng mục, nội dung; 4. Biên bản nghiệm thu hoàn thành hệ thống; 5. Mã nguồn hệ thống.
Yêu cầu 7.1.4.2.c	Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng
Hiện trạng	Đáp ứng. Nội dung được quy định tại Thông tư 14/2020/TT-TNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường. Chi tiết tại Chương III, Mục I, Mục II.
Phương án	Các hệ thống CNTT trước khi đưa vào hoạt động nghiệp vụ đều phải qua các bước kiểm thử trước khi đưa vào sử dụng, các tài liệu theo quy định bao gồm: 1. Báo cáo kết quả vận hành thử đơn động; 2. Báo cáo kết quả vận hành thử hệ thống;

	3. Biên bản nghiệm thu vận hành thử mức hệ thống thiết bị, phần mềm công nghệ thông tin; 4. Biên bản nghiệm thu từng hạng mục, nội dung; 5. Biên bản nghiệm thu hoàn thành.
Yêu cầu 7.1.4.2.d	Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.
Hiện trạng	Đáp ứng. Đã quy định tại Khoản 6 Điều 12 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Nội dung kiểm tra đánh giá an toàn thông tin đều được đưa vào các yêu cầu kiểm thử hệ thống bao gồm: 1. Báo cáo kết quả vận hành thử đơn động; 2. Báo cáo kết quả vận hành thử hệ thống; 3. Biên bản nghiệm thu vận hành thử mức hệ thống thiết bị, phần mềm công nghệ thông tin; 4. Biên bản nghiệm thu từng hạng mục, nội dung; 5. Biên bản nghiệm thu hoàn thành.

7.1.4.3. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu 7.1.4.3.a	Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng
Hiện trạng	Đáp ứng. Nội dung được quy định tại Thông tư 14/2020/TT-TNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường. Chi tiết tại Chương III, Mục I, Mục II.
Phương án	Các tài liệu liên quan đến kiểm thử hệ thống trước khi đưa vào vận hành khai thác sử dụng bao gồm:

	1. Báo cáo kết quả vận hành thử đơn động; 2. Báo cáo kết quả vận hành thử hệ thống; 3. Biên bản nghiệm thu vận hành thử mức hệ thống thiết bị, phần mềm công nghệ thông tin; 4. Biên bản nghiệm thu từng hạng mục, nội dung; 5. Biên bản nghiệm thu hoàn thành.
Yêu cầu 7.1.4.3.b	Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng. Nội dung được quy định tại Thông tư 14/2020/TT-MTNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường. Chi tiết tại Chương III, Mục I, Mục II.
Phương án	Đối với các dự án công nghệ thông tin bất kỳ, Cục KTTV đều thành lập Tổ Hỗ trợ kỹ thuật. Vai trò của tổ hỗ trợ kỹ thuật sẽ giúp việc cho Cục KTTV các vấn đề về mặt kỹ thuật trong quá trình thực hiện dự án. Các nội dung liên quan đến yêu cầu về nội dung, kế hoạch và quy trình thử nghiệm, nghiệm thu hệ thống sẽ được Tổ hỗ trợ kỹ thuật sẽ yêu cầu đơn vị triển khai dự án thực hiện. *(Tham chiếu theo các hợp đồng thực hiện dự án đều có yêu cầu kiểm thử hệ thống trước khi bàn giao đưa vào sử dụng).*
Yêu cầu 7.1.4.3.c	Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng. Nội dung được quy định tại Thông tư 14/2020/TT-MTNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường. Chi tiết tại Chương III, Mục I, Mục II.

Phương án	Đối với các dự án công nghệ thông tin bất kỳ, Cục KTTV đều thành lập Tổ hỗ trợ kỹ thuật. Vai trò của tổ hỗ trợ kỹ thuật sẽ giúp việc cho Cục KTTV các vấn đề về mặt kỹ thuật. Các nội dung liên quan đến việc thử nghiệm, nghiệm thu hệ thống sẽ được Tổ hỗ trợ kỹ thuật sẽ yêu cầu đơn vị triển khai dự án thực hiện. Bộ phận thực hiện thử nghiệm và nghiệm thu hệ thống (về mặt kỹ thuật) sẽ do nhà thầu thực hiện dưới sự giám sát của bộ phận phụ trách về CNTT, ATTT tại đơn vị quản lý hệ thống. Các tài liệu liên quan đến kiểm thử hệ thống trước khi đưa vào vận hành khai thác sử dụng bao gồm: 1. Báo cáo kết quả vận hành thử đơn động; 2. Báo cáo kết quả vận hành thử hệ thống; 3. Biên bản nghiệm thu vận hành thử mức hệ thống thiết bị, phần mềm công nghệ thông tin; 4. Biên bản nghiệm thu từng hạng mục, nội dung; 5. Biên bản nghiệm thu hoàn thành.
Yêu cầu 7.1.4.3.d	Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng. Nội dung được quy định tại Chi tiết tại Mục I. Quy trình kiểm tra, nghiệm thu sản phẩm công nghệ thông tin ngành Tài nguyên và Môi trường, Thông tư 14/2020/TT-MTNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Nông nghiệp và Môi trường.
Phương án	Đối với các dự án công nghệ thông tin bất kỳ, Cục KTTV đều thành lập Tổ Hỗ trợ kỹ thuật. Vai trò của tổ hỗ trợ kỹ thuật sẽ giúp việc cho Cục KTTV các vấn đề về mặt kỹ thuật trong quá trình thực hiện dự án. Các nội dung liên quan giám sát quá trình

	thử nghiệm và nghiệm thu hệ thống sẽ được thực hiện dưới sứ giám sát của các thành viên thuộc Tổ hỗ trợ kỹ thuật. *(Tham chiếu theo các hợp đồng thực hiện dự án đều có yêu cầu tư vấn, giám sát thử nghiệm hệ thống trước khi bàn giao đưa vào sử dụng)*
Yêu cầu 7.1.4.3.đ	Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.
Hiện trạng	Đáp ứng. Nội dung được quy định tại Thông tư 14/2020/TT-MTNMT ngày 27 tháng 11 năm 2020 về Ban hành quy trình và Định mức kinh tế kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành Tài nguyên và Môi trường. Chi tiết tại Mục I, Mục II, Mục IV, Chương III.
Phương án	Các tài liệu liên quan đến nghiệm thu hệ thống bao gồm 1. Báo cáo kết quả vận hành thử đơn động; 2. Báo cáo kết quả vận hành thử hệ thống; 3. Biên bản nghiệm thu vận hành thử mức hệ thống thiết bị, phần mềm công nghệ thông tin; 4. Biên bản nghiệm thu từng hạng mục, nội dung; 5. Biên bản nghiệm thu hoàn thành; 6. Hợp đồng; 7. Nhật ký công tác triển khai; 8. Danh mục catalog và hướng dẫn sử dụng hệ thống; 9. Tài liệ về chứng nhận xuất xứ và chất lượng sản phẩm

7.1.5. Quản lý vận hành hệ thống thông tin

7.1.5.1. Quản lý an toàn mạng

Yêu cầu 7.1.5.1.a	Chính sách và quy trình quản lý an toàn mạng bao gồm: Quản lý, vận hành hoạt động bình thường của hệ thống

Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ đối với các nội dung liên quan đến quản lý ATTT mạng, các chính sách về ATTT được quy định từ Điều 8 đến Điều 13, Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Hệ thống mạng của Cục được thiết kế theo mô hình mạng chuẩn, phân chia các vùng mạng theo chức năng nhiệm vụ. Các lớp mạng được được quy hoạch và phân chia rõ ràng về mặt chức năng. Mỗi phân vùng đều được kiểm soát ít nhất thông qua một hệ thống Firewall. Các chính sách trên thiết bị Firewall được tùy biến và cập nhật tùy theo nhu cầu sử dụng và tình hình thực tế. Việc truy cập đến các thiết bị mạng được kiểm soát chặt chẽ. Ngoài ra việc giám sát và vận hành các hệ thống CNTT được tuân thủ theo quy trình trực nghiệp vụ của đơn vị, theo đó các thiết bị được kiểm tra, giám sát 24h/24h.
Yêu cầu 7.1.5.1.b	Chính sách và quy trình quản lý an toàn mạng bao gồm: Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ đối với các nội dung liên quan đến quản lý ATTT mạng.
Phương án	Các thiết bị mạng lõi tại Cục KTTV đều được sử dụng theo cặp nhằm đảm bảo tính dự phòng: Các thiết bị được cấu hình theo chế độ hoạt động active-active (Cặp core switch, cặp Router, Firewall) hoặc active – Standby (Switch Acess). Ngoài ra các thiết bị mạng được cập nhật và sao lưu cấu hình nhằm đảm bảo việc khôi phục hệ thống sau khi gặp sự cố.
Yêu cầu 7.1.5.1.c	Chính sách và quy trình quản lý an toàn mạng bao gồm: Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn mạng đồng thời các quy định kỹ thuật cũng đã được quy định tại

	điểm b, Khoản 2 Điều 9. Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Việc truy cập và quản lý cấu hình hệ thống được tuân thủ theo các quy định như: Phân công cán bộ có thẩm quyền quản trị và vận hành hệ thống; Khi kết nối tới thiết bị chỉ sử dụng các giải pháp kết nối an toàn, có xác thực; Thực hiện sao lưu cấu hình hệ thống trước khi cập nhật hoặc thay đổi cấu hình…
Yêu cầu 7.1.5.1.d	Chính sách và quy trình quản lý an toàn mạng bao gồm: Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác
Hiện trạng	Đáp ứng Đã quy định tại mục c, khoản 1 Điều 10. Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng

7.1.5.2. Quản lý an toàn máy chủ và ứng dụng

Yêu cầu 7.1.5.2.a	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ về quản lý an toàn máy chủ đồng thời cũng được quy định tại Điều 10, Điều 12 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.

Phương án	Các máy chủ được đặt trong các vùng mạng dành riêng cho máy chủ tách biệt giữa máy chủ vùng DMZ, máy chủ CSDL, và máy chủ Server Farm. Các máy chủ vùng DMZ, Server Farm được kiểm soát chặt chẽ thông qua thiết bị Firewall DMZ và Firewall Server Farm. Trước khi đưa vào vận hành các máy chủ đều được cập nhật các bản vá cài đặt các giải pháp phòng chống mã độc, đặc biệt các máy chủ chỉ được cài đặt các phần mềm có bản quyền, không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết Các phần mềm, ứng dụng trước khi cài đặt đưa vào sử dụng đều được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin. Định kỳ thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ.
Yêu cầu 7.1.5.2.b	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Truy cập mạng của máy chủ
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn máy chủ, đồng thời các quy định kỹ thuật cũng được quy định tại Khoản 2 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Các máy chủ được đặt trong các vùng riêng biệt tùy theo chức năng. Việc truy cập máy chủ được phân quyền chặt chẽ, tài khoản quản trị tách biệt với tài khoản người sử dụng thông thường.
Yêu cầu 7.1.5.2.c	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Truy cập và quản trị máy chủ và ứng dụng
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn máy chủ, đồng thời các quy định kỹ thuật cũng được quy định tại Khoản 2 Điều 10; Khoản 2, khoản 3, Điều 12 Quyết định số 335

	/QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Việc truy cập, quản trị máy chủ ứng dụng được phân quyền theo chức năng nghiệp vụ. Các máy chủ được thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng. Việc truy cập máy chủ sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý
Yêu cầu 7.1.5.2.d	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn máy chủ, đồng thời các quy định kỹ thuật cũng được quy định tại điểm e, Khoản 2, Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm e, Khoản 2 Điều 10. 1. Hệ thống máy chủ e) Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố.
Yêu cầu 7.1.5.2.đ	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

	Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn máy chủ, đồng thời các quy định kỹ thuật cũng được quy định tại điểm d, đ Khoản 2, Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm d, đ Khoản 2 Điều 10 1. Hệ thống máy chủ d) Chỉ cài đặt và sử dụng các phần mềm đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết; đ) Cài đặt các giải pháp phòng chống mã độc tập trung và phòng chống tấn công xâm nhập mạng phù hợp với yêu cầu theo từng cấp độ.
Yêu cầu 7.1.5.2.e	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn máy chủ, đồng thời các quy định kỹ thuật cũng được quy định tại Khoản 2, Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm a, b, c Khoản 2 Điều 10 2. Hệ thống máy chủ a) Phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ và vùng mạng máy chủ quản trị.

	b) Chỉ cho phép kết nối đến những dịch vụ cần thiết trên Internet. c) Chỉ mở và cung cấp các dịch vụ cần thiết ra Internet.
Yêu cầu 7.1.5.2. g	Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành Quy trình quản lý an toàn máy chủ đồng thời các quy định kỹ thuật cũng dã được quy định tại Khoản 2 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Để bảo đảm an toàn cho hệ thống máy chủ và ứng dụng trước khi đưa vào vận hành, đơn vị triển khai các biện pháp kỹ thuật và quản lý như sau: 1. Cấu hình tối ưu và tăng cường bảo mật cho toàn bộ máy chủ: Thực hiện vô hiệu hóa các dịch vụ, cổng kết nối, và tài khoản mặc định không cần thiết.; Thiết lập cơ chế kiểm soát truy cập chặt chẽ, sử dụng xác thực đa yếu tố (MFA) cho tài khoản quản trị.; Cập nhật và vá lỗi hệ điều hành, phần mềm, middleware theo định kỳ và ngay khi có cảnh báo bảo mật mới 2. Triển khai quy trình kiểm tra an toàn trước khi vận hành**:** Kiểm thử lỗ hổng bảo mật, quét cấu hình sai, đánh giá rủi ro trước khi máy chủ được đưa vào hoạt động; Ghi nhận kết quả đánh giá và biên bản nghiệm thu bảo mật trước khi bàn giao hệ thống cho vận hành chính thức.

7.1.5.3. Quản lý an toàn dữ liệu

Yêu cầu	Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

7.1.5.3.a	Xây dựng và thực thi chính sách, quy trình dự phòng và khôi phục dữ liệu
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn dữ liệu đồng thời các quy định kỹ thuật cũng đã được quy định tại Điều 13 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Điều 13. Quản lý an toàn, an ninh thông tin dữ liệu** 1. Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu. 2. Đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. 3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó. 4. Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ

	liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu). Khi thanh lý thiết bị phải xóa nội dung dữ liệu lưu trữ bằng phần mềm, thiết bị hủy dữ liệu chuyên dụng hoặc phá hủy vật lý. 5. Bố trí máy tính riêng không kết nối mạng, đặt mật khẩu và các biện pháp bảo mật phù hợp để soạn thảo, lưu trữ thông tin, tài liệu mật. Đối với các thiết bị chứa thông tin mật bắt buộc phải kết nối mạng thì phải áp dụng các giải pháp bảo mật an toàn, an ninh thông tin được Ban Cơ yếu Chính phủ đánh giá và cho phép. 6. Các đơn vị trực thuộc Cục phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.
Yêu cầu 7.1.5.3.b	Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn dữ liệu đồng thời các quy định kỹ thuật cũng đã được quy định tại Khoản 2, Điều 13 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Khoản 2 Điều 13** 2. Đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng

	loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

7.1.5.4. Quản lý an toàn thiết bị đầu cuối

Yêu cầu 7.1.6.4.a	Chính sách quy trình quản lý an toàn người sử dụng đầu cuối bao gồm: Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn thiết bị đầu cuối, đồng thời các quy định kỹ thuật cũng được quy định tại Điểm đ, Điểm g, Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm đ, Điểm g, Khoản 3 Điều 10 3. Thiết bị đầu cuối và thiết bị số đ) Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của Lãnh đạo đơn vị; thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị lưu trữ di động như mã hóa dữ liệu, quét mã độc định kỳ. g) Đối với thiết bị số phục vụ quản trị hệ thống: Chỉ được sử dụng cho mục đích quản trị hệ thống; chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết; không được kết nối trực tiếp đến máy chủ để thực hiện quản trị cấu hình mà phải kết nối với máy chủ quản trị qua các đường truyền có mã hóa bảo mật theo quy định
Yêu cầu 7.1.6.4.b	Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn thiết bị đầu cuối, đồng thời các quy định kỹ thuật cũng đã được

	quy định tại Điểm c Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Các thiết bị CNTT được thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng. Ngoài ra cán bộ quản trị chỉ sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; Không cho phép truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.
Yêu cầu 7.1.6.4.c	Chính sách quy trình quản lý an toàn người sử dụng đầu cuối bao gồm: Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn thiết bị đầu cuối, đồng thời các quy định kỹ thuật cũng đã được quy định tại Điểm a, điểm b, điểm c Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Điểm a, b, c Khoản 3 Điều 10** 3. Thiết bị đầu cuối và thiết bị số a) Người sử dụng chỉ cài đặt phần mềm có hỗ trợ cập nhật các bản vá, tính năng mới, bản vá lỗ hổng bảo mật; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật bản vá cho các phần mềm ứng dụng,

	hệ điều hành và các phần mềm phục vụ công việc; b) Cài đặt phần mềm phòng, chống mã độc và phải thiết lập chế độ tự động cập nhật tính năng mới cho phần mềm khi có thông báo từ hãng khuyến nghị; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời; c) Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác;

7.1.5.5. Quản lý phòng chống phần mềm độc hại

Yêu cầu 7.1.5.5.a	Chính sách quy trình quản lý phòng chống phần mềm độc hại bao gồm: Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình phòng chống phần mềm độc hại, đồng thời các quy định kỹ thuật cũng đã được quy định tại Điểm a, Điểm b Khoản 3, Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Điểm a, Điểm b Khoản 3 Điều 10** a) Người sử dụng chỉ cài đặt phần mềm có hỗ trợ cập nhật các bản vá, tính năng mới, bản vá lỗ hổng bảo mật; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật bản vá cho các phần mềm ứng dụng, hệ điều hành và các phần mềm phục vụ công việc;

	b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.
Yêu cầu 7.1.5.5.b	Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình phòng chống phần mềm độc hại, đồng thời các quy định kỹ thuật cũng đã được quy định tại Đã quy định tại Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Điểm a, Điểm b, Điểm c Khoản 3 Điều 10** a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan, đơn vị có thẩm quyền ban hành trên máy tính được cơ quan, đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềmkhi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời. c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

Yêu cầu 7.1.5.5.c	Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn dữ liệu. Ngoài ra các quy định kỹ thuật cũng đã được quy định tại Khoản 1,6,7 Điều 13 và điểm đ Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Khoản 1, 6,7 Điều 13** 1. Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu. 6. Các đơn vị trực thuộc Cục phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin. 7. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.
Yêu cầu 7.1.5.5.d	Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại

	khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ đối với việc quản lý phòng chống phần mềm độc hại.
Phương án	Để đảm bảo an toàn cho hệ thống trước nguy cơ phần mềm độc hại, đơn vị triển khai quy trình phòng chống và xử lý mã độc như sau: 1. Thiết lập hệ thống kiểm tra và giám sát phần mềm độc hại định kỳ: Thực hiện quét toàn bộ hệ thống máy chủ, máy trạm, thiết bị lưu trữ bằng công cụ chống mã độc được cập nhật thường xuyên (Kaspersky); Đặt lịch quét tự động định kỳ và kiểm tra lại sau mỗi lần cập nhật hệ điều hành hoặc phần mềm quan trọng 2. Phát hiện và xử lý sự cố phần mềm độc hại: Khi phát hiện dấu hiệu nghi ngờ (hoạt động bất thường, cảnh báo từ hệ thống giám sát, truy cập trái phép...), tiến hành cách ly thiết bị bị nhiễm, phân tích mẫu và xác định nguồn gốc tấn công; Thực hiện khôi phục hệ thống từ bản sao lưu sạch, cập nhật bản vá bảo mật, và ghi nhận sự cố theo quy trình nội bộ.

7.1.5.6. Quản lý giám sát an toàn hệ thống thông tin

Yêu cầu 7.1.5.6.a	Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm: Quản lý, vận hành hoạt động bình thường của hệ thống giám sát
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ thực hiện quản lý giám sát an toàn thông tin đồng thời cũng quy định tại Khoản 1, 2 Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.

Phương án	Khoản 1, 2 Điều 15 1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin. 2. Chủ quản hệ thống thông tin chỉ đạo việc giám sát an toàn, an ninh thông tin mạng đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Trung tâm Thông tin và Dữ liệu khí tượng thủy văn, các đơn vị quản lý về công tác thông tin dữ liệu của Cục Khí tượng Thủy văn, Bộ Nông nghiệp và Môi trường và các đơn vị chức năng của Bộ Thông tin và Truyền thông giám sát theo quy định.
Yêu cầu 7.1.5.6.b	Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có)
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ thực hiện quản lý giám sát an toàn thông tin.
Phương án	Để bảo đảm công tác giám sát an toàn thông tin được triển khai toàn diện và hiệu quả, đơn vị thực hiện như sau: 1. Xác định phạm vi và đối tượng giám sát: Đưa vào danh mục giám sát toàn bộ thiết bị trong hệ thống bao gồm máy chủ, thiết bị mạng, ứng dụng, dịch vụ và các thành phần liên quan (CSDL, tường lửa, thiết bị lưu trữ…); Cập nhật định kỳ danh mục giám sát khi có thay đổi về hạ tầng hoặc hệ thống ứng dụng mới. 2. Thiết lập cơ chế giám sát tập trung: Kết nối các đối tượng giám sát về hệ thống quản lý giám sát an toàn thông tin (SIEM); Thu thập log, sự kiện an ninh, và cảnh báo theo thời gian thực để phát hiện sớm các hành vi bất thường. 3. Đảm bảo duy trì liên tục

	Định kỳ đánh giá hiệu quả giám sát, bổ sung đối tượng mới khi mở rộng hạ tầng CNTT
Yêu cầu 7.1.5.6.c	Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ thực hiện quản lý giám sát an toàn thông tin.
Phương án	Thiết lập hệ thống giám sát tập trung thu thập, truyền và lưu trữ log tự động từ các thiết bị đồng thời định kỳ kiểm tra, đánh giá và cập nhật quy trình quản lý giám sát ATTT
Yêu cầu 7.1.5.6.d	Truy cập và quản trị hệ thống giám sát
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ thực hiện quản lý giám sát an toàn thông tin, đồng thời cũng quy định tại Khoản 4 Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Khoản 4 Điều 15 4. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.
Yêu cầu 7.1.5.6.đ	Loại thông tin cần được giám sát
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình nội bộ thực hiện quản lý giám sát an toàn thông tin, đồng thời cũng quy định tại Khoản 4 Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.

Phương án	Khoản 4 Điều 15 4. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.
Yêu cầu 7.1.5.6.e	Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống)
Hiện trạng	Đáp ứng. Điểm a Khoản 1 Điều 10, Khoản 5 Điều 12, Khoản 3 Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm a Khoản 1 Điều 10 a) Định kỳ sao lưu cấu hình thiết bị kết nối mạng nội bộ. Lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam. Khoản 5 Điều 12 5. Ghi và lưu giữ bản ghi nhật ký hệ thống (log files) của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy cập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị. Khoản 3 Điều 15 3. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

Yêu cầu 7.1.5.6.g	Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát
Hiện trạng	Đáp ứng. Quy định tại Điểm a, Khoản 1 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm a, Khoản 1 Điều 10 a) Định kỳ sao lưu cấu hình thiết bị kết nối mạng nội bộ. Lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam; Ngoài ra Cục KTTV triển khai 02 máy chủ time server, 02 máy chủ này được cấu hình HA. Toàn bộ thiết bị CNTT và máy chủ được cấu hình đồng bộ thời gian thông qua cặp máy chủ này.
Yêu cầu 7.1.5.6.h	Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin
Hiện trạng	Đáp ứng. Quy định tại Khoản 4 Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Khoản 4 Điều 15 4. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

7.1.5.7. Quản lý điểm yếu an toàn thông tin

Yêu cầu 7.1.5.7.a	Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm:

	Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có)
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý điểm yếu ATTT đồng thời cũng được Quy định tại khoản 6 Điều 12 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Để bảo đảm việc quản lý và khắc phục điểm yếu an toàn thông tin được thực hiện đồng bộ, đơn vị triển khai các biện pháp sau: 1, Thiết lập và thực hiện quy trình quản lý điểm yếu ATTT: Xây dựng quy trình nhận diện, đánh giá, phân loại và xử lý điểm yếu cho toàn bộ thành phần trong hệ thống (thiết bị hạ tầng, hệ điều hành, ứng dụng, dịch vụ…); Đề xuất các nhiệm liên vụ liên quan đến nội dung rà quét lỗ hổng, kiểm thử xâm nhập; Cập nhật quy trình quản lý điểm yếu khi có thay đổi công nghệ, hạ tầng hoặc yêu cầu pháp lý mới.; Phối hợp với nhóm chuyên gia và đơn vị an toàn thông tin bên ngoài để hỗ trợ phân tích, đánh giá chuyên sâu khi cần thiết. 2. Cơ chế phản ứng và khắc phục: Khi phát hiện điểm yếu, thực hiện đánh giá mức độ rủi ro, lên kế hoạch khắc phục và xác minh sau xử lý; Lưu trữ biên bản khắc phục, kết quả đánh giá lại và báo cáo định kỳ theo quy định quản lý an toàn thông tin nội bộ.
Yêu cầu 7.1.5.7.b	Chính sách quy trình quản lý điểm yếu an toàn thông tin bao gồm: Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;

Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý điểm yếu ATTT
Phương án	Đơn vị đã ban hành quy trình quản lý điểm yếu ATTT quy định rõ các bước phát hiện, đánh giá, xử lý và theo dõi. Thường xuyên cập nhật thông tin điểm yếu từ các nguồn tin chính thống của Chính phủ. Tiến hành triển khai biện pháp khắc phục, kiểm thử lại sau xử lý và báo cáo định kỳ.
Yêu cầu 7.1.7.7.c	Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm: Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin
Hiện trạng	Đáp ứng. Đơn vị đã xây dựng và ban hành quy trình quản lý điểm yếu ATTT.
Phương án	Thiết lập cơ chế phối hợp với đơn vị chuyên trách và nhà cung cấp dịch vụ an toàn thông tin để kịp thời phát hiện, xử lý và khắc phục điểm yếu bảo mật đồng thời thực hiện rà quét, đánh giá định kỳ và lưu hồ sơ phối hợp, đảm bảo tuân thủ quy chế an toàn thông tin mạng. Xây dựng các đề án, nhiệm vụ chuyên môn liên quan đến ATTT
Yêu cầu 7.1.5.7. d	Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng
Hiện trạng	Đáp ứng. Đơn vị đã xây dựng và ban hành quy trình quản lý điểm yếu ATTT đồng thời cũng quy định tại Khoản1, 2, 3 Điều 8 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Khoản 1, Khoản 2, Khoản 3 Điều 8** 1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ

	thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết. 2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện. 3. Các hệ thống thông tin được triển khai, cài đặt tại Trung tâm dữ liệu của Cục cần đáp ứng các yêu cầu: a) Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm; b) Áp dụng các giải pháp bảo đảm an toàn, an ninh thông tin; c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng; d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin; đ) Áp dụng các biện pháp bảo đảm tính toàn vẹn dữ liệu; e) Mọi thao tác trên hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.
Yêu cầu 7.1.5.7. đ	Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm: Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống
Hiện trạng	Đáp ứng. Đơn vị đã xây dựng và ban hành quy trình quản lý điểm yếu ATTT đồng thời cũng quy định tại Khoản 6 Điều 12, Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.

Phương án	Để bảo đảm việc phát hiện và xử lý điểm yếu an toàn thông tin được thực hiện liên tục, đơn vị triển khai như sau: 1. Thực hiện kiểm tra, đánh giá định kỳ: Tổ chức quét lỗ hổng, đánh giá điểm yếu bảo mật trên toàn bộ hệ thống (máy chủ, thiết bị mạng, ứng dụng, cơ sở dữ liệu) theo hướng dẫn của cơ quan quản lý (Cục Chuyển đổi số); Lập danh mục điểm yếu, đánh giá mức độ rủi ro và phân loại theo mức nghiêm trọng. 2. Xử lý và theo dõi khắc phục: Xây dựng kế hoạch xử lý cụ thể cho từng điểm yếu Sau khi khắc phục, tiến hành kiểm tra lại và xác nhận tình trạng an toàn trước khi đưa hệ thống trở lại hoạt động bình thường. 3. Cập nhật quy trình và thông tin cảnh báo về ATTT Theo dõi cảnh báo điểm yếu mới từ các tổ chức bảo mật uy tín, cập nhật cơ sở dữ liệu lỗ hổng bảo mật; Rà soát, cập nhật quy trình kiểm tra và khắc phục để đảm bảo tuân thủ quy định về an toàn thông tin mạng của Cục Khí tượng Thủy văn.

7.1.5.8. Quản lý sự cố an toàn thông tin

Yêu cầu 7.1.5.8.a	Chính sách quy trình quản lý sự cố an toàn thông tin bao gồm: Phân nhóm sự cố an toàn thông tin
Hiện trạng	Đáp ứng. Đơn vị đã xây dựng và ban hành quy trình quản lý sự cố ATTT đồng thời cũng quy định Quy định tại Điểm b Khoản 3 Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm b Khoản 3 Điều 17

	b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TTBTTT, đồng thời thông báo Trung tâm Thông tin và Dữ liệu khí tượng thủy văn trường để tổng hợp, báo cáo các đơn vị có thẩm quyền. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.
Yêu cầu 7.1.5.8.b	Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin
Hiện trạng	Đáp ứng. Đơn vị đã xây dựng và ban hành quy trình quản lý sự cố ATTT đồng thời cũng quy định tại Khoản 3 Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Khoản 3 Điều 17 a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin liên quan và Trung tâm Thông tin và Dữ liệu khí tượng thủy văn. Trung tâm Thông tin và Dữ liệu khí tượng thủy văn có trách nhiệm thông báo thông tin liên lạc, đường dây nóng của các đơn vị/bộ phận tiếp nhận thông tin sự cố của Cục Khí tượng Thủy văn lên Trang thông tin điện tử của Cục. b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TT-BTTT, đồng thời thông báo Trung tâm Thông tin và Dữ liệu khí tượng thủy

	văn trường để tổng hợp, báo cáo các đơn vị có thẩm quyền. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT. c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.
Yêu cầu 7.1.5.8.c	Kế hoạch ứng phó sự cố an toàn thông tin
Hiện trạng	Đáp ứng. Quy định tại Khoản 2 Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Khoản 2 Điều 17** 2. Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng a) Chủ quản hệ thống thông tin trực thuộc Cục tổ chức xây dựng, trình Cục xem xét phê duyệt kế hoạch ứng phó sự cố cho các hệ thống thông tin do Cục quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. b) Trung tâm Thông tin và Dữ liệu khí tượng thủy văn có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Cục Khí tượng Thủy văn, trình Cục xem xét, phê duyệt. c) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn thông tin năm tiếp theo.
Yêu cầu 7.1.5.8.d	Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

Hiện trạng	Đáp ứng. Quy định tại Điều 15 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điều 15 1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin 2. Chủ quản hệ thống thông tin chỉ đạo việc giám sát an toàn, an ninh thông tin mạng đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Trung tâm Thông tin và Dữ liệu khí tượng thủy văn, các đơn vị quản lý về công tác thông tin dữ liệu của Cục Khí tượng Thủy văn, Bộ Nông nghiệp và Môi trường và các đơn vị chức năng của Bộ Khoa học và Công nghệ giám sát theo quy định; 3. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép. 4. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin. 5. Đơn vị chuyên trách về an toàn thông tin của các đơn vị trực thuộc Cục cử 01 lãnh đạo đơn vị và 01 cán bộ (hoặc 01 đơn vị trực thuộc) làm đầu mối giám sát an toàn, an ninh thông tin để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Trung tâm Thông tin và Dữ liệu khí tượng thủy văn trong các hoạt động giám sát an toàn, an ninh thông tin tại đơn vị và tại Cục Khí tượng Thủy văn.
Yêu cầu	Quy trình ứng cứu sự cố an toàn thông tin thông thường

7.1.5.8.đ	
Hiện trạng	Đáp ứng. Quy định tại Điểm a Khoản 3 Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm a Khoản 3 Điều 17 a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin liên quan và Trung tâm Thông tin và Dữ liệu khí tượng thủy văn. Trung tâm Thông tin và Dữ liệu khí tượng thủy văn có trách nhiệm thông báo thông tin liên lạc, đường dây nóng của các đơn vị/bộ phận tiếp nhận thông tin sự cố của Cục Khí tượng Thuỷ văn lên Trang thông tin điện tử của Cục.
Yêu cầu 7.1.5.8.e	Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng
Hiện trạng	Đáp ứng. Quy định tại Điểm b, c Khoản 3 Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm b,c Khoản 3 Điều 17 b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại điểm a khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TTBTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, đồng thời thông báo Trung tâm Thông tin và Dữ liệu khí tượng thủy văn trường để tổng hợp, báo cáo các đơn vị có thẩm quyền. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng

	theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT; c) Quy trình ứng cứu sự cố an toàn thông tin mạng quy định tại Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT
Yêu cầu 7.1.5.8.g	Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin
Hiện trạng	Đáp ứng. Xây dựng và đề xuất các nhiệm vụ chuyên môn liên quan đến ATTT Hợp tác với các đơn vị, tổ chức chuyên về ATTT đồng thời xây dựng và đề xuất các nhiệm vụ chuyên môn liên quan đến ATTT
Phương án	Để bảo đảm việc xử lý và khắc phục sự cố an toàn thông tin được thực hiện nhanh chóng, chính xác và tuân thủ quy định, đơn vị triển khai như sau: 1. Thiết lập cơ chế phối hợp chính thức với các bên liên quan: Xây dựng đầu mối liên lạc và quy trình phối hợp giữa đơn vị với cơ quan quản lý nhà nước (Cục CĐS, VNCS), các nhóm chuyên gia và nhà cung cấp dịch vụ ATTT 2. Tổ chức tiếp nhận, xử lý và khắc phục sự cố: Khi phát hiện sự cố hoặc dấu hiệu tấn công mạng, đơn vị nhanh chóng kích hoạt quy trình ứng cứu, ghi nhận log, cô lập hệ thống bị ảnh hưởng và thông báo cho cơ quan chức năng theo quy định; Phối hợp với chuyên gia và nhà cung cấp để phân tích nguyên nhân, khôi phục hệ thống, đồng thời cập nhật biện pháp phòng ngừa tái diễn.
Yêu cầu 7.1.5.8.h	Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin

Hiện trạng	Đáp ứng. Quy định tại điểm a, Khoản 4, Điều 17 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Khoản 4, Điều 17 Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt

7.1.5.9. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu 7.1.5.9.a	Chính sách quy trình quản lý an toàn người sử dụng đầu cuối bao gồm: Quản lý truy cập, sử dụng tài nguyên nội bộ
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý an toàn thiết bị đầu cuối, đồng thời cũng quy định tại Điểm d, đ, g Khoản 3 Điều 10; Khoản 3,4 Điều 12 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Điểm d, đ, g Khoản 3 Điều 10 d) Khóa màn hình máy tính khi rời khỏi bàn làm việc. Đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng. Tắt máy an toàn sau mỗi buổi làm việc; đ) Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của Lãnh đạo đơn vị; thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị lưu trữ di động như mã hóa dữ liệu, quét mã độc định kỳ; g) Đối với thiết bị số phục vụ quản trị hệ thống: Chỉ được sử dụng cho mục đích quản trị hệ thống; chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết; không được kết nối trực tiếp đến máy chủ để thực hiện quản trị cấu hình mà phải kết nối với máy chủ quản trị qua các đường truyền có mã hóa bảo mật theo quy định.

	Khoản 3, 4 Điều 12 3. Thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng; 4. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy cập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.
Yêu cầu 7.1.5.9.b	Quản lý truy cập mạng và tài nguyên trên Internet
Hiện trạng	Đáp ứng. Quy định tại điểm c, Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Điểm c, Khoản 3 Điều 10** c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.
Yêu cầu 7.1.5.9.c	Cài đặt và sử dụng máy tính an toàn
Hiện trạng	Đáp ứng. Đã Quy định tại Khoản 3 Điều 10 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Khoản 3 Điều 10**

	a) Người sử dụng chỉ cài đặt phần mềm có hỗ trợ cập nhật các bản vá, tính năng mới, bản vá lỗ hổng bảo mật; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật bản vá cho các phần mềm ứng dụng, hệ điều hành và các phần mềm phục vụ công việc; b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời. c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

7.1.5.10. Quản lý rủi ro an toàn thông tin

Yêu cầu	Có chính sách, quy trình quản lý quản lý rủi ro an toàn thông tin
Hiện trạng	Đáp ứng. Đã xây dựng và ban hành quy trình quản lý rủi ro ATTT đồng thời cũng quy định tại Khoản 2 Điều 8 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	**Khoản 2 Điều 8** 2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

7.1.5.11. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Yêu cầu	Có quy định về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Hiện trạng	Đáp ứng. Đã Quy định tại Khoản 3, Khoản 4 Điều 13 Quyết định số 335 /QĐ-KTTV ngày 30 tháng 6 năm 2025 về Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Khí tượng Thủy văn.
Phương án	Khoản 3, Khoản 4 Điều 13 3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó. 4. Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu). Khi thanh lý thiết bị phải xóa nội dung dữ liệu lưu trữ bằng phần mềm, thiết bị hủy dữ liệu chuyên dụng hoặc phá hủy vật lý.

PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT CẤP ĐỘ 3

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Có	Vùng mạng nội bộ độc tập, tách riêng mạng người dùng thông thường phục vụ nghiệp vụ
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet
3	Vùng DMZ	Có	Vùng máy chủ dịch vụ, cung cấp dịch vụ trực tiếp ra bên ngoài Internet
4	Vùng máy chủ nội bộ	Có	Vùng máy chủ nội bộ, cung cấp các dịch vụ nội bộ
5	Vùng mạng máy chủ cơ sở dữ liệu	Có	Lưu trữ và quản lý cơ sở dữ liệu tập trung của các hệ thống thành phần
6	Vùng mạng không dây	Có	Vùng mạng không dây quản trị tập trung
7	Vùng quản trị	Có	Server Management (Quản lý hạ tầng) cài đặt một tập hợp các công cụ quản trị và giám sát toàn bộ các thiết bị mạng, bảo mật, máy chủ và lưu trữ.

b) Phương án bảo đảm an toàn thông tin

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Hệ thống quản trị từ xa bắt buộc đi qua VPN/SSL-VPN/IPsec với mã hóa mạnh, xác thực tài khoản. Chỉ cho phép quản trị qua jump server/bastion; chặn toàn bộ truy cập

			trực tiếp từ Internet. Policy "least privilege", ghi log đầy đủ về SIEM.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Kiến trúc phân vùng Server Farm/DMZ/User chạy trên cụm NGFW. Áp dụng nguyên tắc default-deny/allow-list, kiểm soát L3–L7, IPS/Anti-Malware/URL filtering/SSL inspection trong phạm vi thiết kế. Lưu lượng giữa các vùng đều qua NGFW và được giám sát 24/7.
3	Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính	Có	Các thiết bị mạng chính được thiết kế và cấu hình hoạt động ở chế độ A-A. Cụ thể: - Firewall: NGFW01 và NGFW02 được đầu tư trong dự án "Xây dựng, hoàn thiện hệ thống thông tin, cơ sở dữ liệu Nông nghiệp và Môi trường (Giai đoạn 1)"; - DB Firewall: DB NGFW01 và DB NGFW02 được đầu tư trong dự án "Xây dựng, hoàn thiện hệ thống thông tin, cơ sở dữ liệu Nông nghiệp và Môi trường (Giai đoạn 1)"; - Switch Core: Core SW01/ Cisco serial 9000; Core SW02/ Cisco serial 9000 (Dự phòng nóng 1-1 cho Core SW01) - Ddos: Ddos01 Radware; Ddos01 DefensePro 1016/ - Router: Router01 Cisco ASR1001-X; Router 02 Cisco ASR1001-X - Balancing: Balancing 01 F5 Big-IP i2600; Balancing 02 F5 Big-IP i2800
4	Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Có	Quản lý truy cập CSDL qua NGFW; không cho phép kết nối Internet trực tiếp tới máy chủ DB. Bật HIPS/EDR trên server,

			Cài đặt Phần mềm virus và cập nhật định kỳ cho máy chủ CSDL.
5	Phương án chặn lọc phần mềm độc hại trên môi trường mạng	Có	Đã triển khai đồng bộ: NGFW với IPS/Anti-Malware, Web Gateway lọc URL/Attachment và triển khai giải pháp phòng chống tấn công có chủ đích (APT) trong hệ thống mạng của đơn vị quản lý vận hành.
6	Phương án phòng chống tấn công từ chối dịch vụ	Có	Hệ thống sử dụng giải pháp phòng chống tấn công từ chối dịch vụ được triển khai ở vùng mạng biên để thực hiện phát hiện và phòng chống tấn công Ddos: Ddos01 Radware; Ddos01 DefensePro 1016/.
7	Phương án phòng, chống tấn công mạng cho ứng dụng web	Có	Hệ thống đã triển khai WAF/Reverse Proxy trước các ứng dụng Web, bật đầy đủ chính sách OWASP Top-10 (SQLi, XSS, XXE, CSRF…), kiểm tra tệp/URL độc hại, bot/DoS mitigation **và** rate-limit (tính năng trên thiết bị F5 i2800). Lưu lượng qua biên được kiểm soát bởi NGFW (IPS/Anti-Malware/SSL inspection trong phạm vi thiết kế)
8	Phương án quản lý truy cập lớp mạng	Có	Truy cập giữa các lớp chỉ qua NGFW với nguyên tắc default-deny/allow-list, đăng ký & kiểm soát IP/MAC, cách ly thiết bị lạ/quarantined VLAN. Trên switch/router cấu hình ACL**,** port-security**,** DHCP snooping**,** IP Source Guard.
9	Phương án giám sát hệ thống thông tin tập trung	Có	Sử dụng phần mềm Zabbix để giám sát hiệu năng, trạng thái các thiết bị trong hệ thống.

10	Phương án giám sát an toàn hệ thống thông tin tập trung	Có	Sử dụng giải pháp Spluk Enterprice Security
11	Phương án quản lý sao lưu dự phòng tập trung	Có	Hệ thống backup tập trung lưu trữ trên SAN dung lượng hữu dụng ~200 TB**.** Áp dụng quy tắc 3–2–1 (bản sao tại chỗ, bản sao khác phương tiện, bản sao ngoại vi/DR). Lịch sao lưu tự động theo (hằng ngày/tuần/tháng); kiểm tra khôi phục định kỳ.
12	Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	Có	Sử dụng giải pháp AntiVirus có chức năng quản lý tập trung (kaspersky)
13	Có phương án phòng, chống thất thoát dữ liệu	Có	Trung tâm thực hiện trực giám sát 24/24h kiểm soát toàn thời gian khu vực Trung tâm dữ liệu (DC) thực hiện đăng ký ra vào, ra, khu vực tiếp cận và làm việc trong DC… Ngoài ra đơn vị vận hành đang sử dụng giải pháp phòng chống thất thoát dữ liệu (DLP) của fortra.
14	Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau	Có	Sử dụng đồng thời hai kết nối Internet của hai nhà cung cấp dịch vụ khác nhau để đảm bảo kết nối không bị gián đoạn (sử dụng dịch vụ của VNPT và NetNam)
15	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	N/A	

1.2. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	Cặp NGFW01–NGFW02 và VPN Gateway đã triển khai: bắt buộc VPN/SSL-VPN/IPSec với mã hóa mạnh, xác thực tài khoản/đa yếu tố (nếu bật), giới hạn nguồn theo địa chỉ IP và chính sách truy cập theo hệ. Tất cả truy cập quản trị từ Internet chỉ qua VPN; lưu nhật ký về SIEM 24/7
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài	Có	Triển khai chính sách tường lửa theo nguyên tắc default-deny/allow-list áp dụng trên NGFW ở biên và DMZ. Mỗi ứng dụng công bố ra ngoài có policy riêng (đích, cổng, giao thức, NAT, IPS/AV/URL). Tất cả dịch vụ khác bị chặn
3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Có	Đã cấu hình idle-timeout cho VPN, phiên quản trị và dịch vụ công bố (theo khuyến nghị nhà sản xuất và yêu cầu ATTT). Phiên rỗi tự động hủy
4	Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý.	Có	Thực hiện chính sách trên thiết bị VPN Gateway tại vùng mạng biên. Mỗi người sử dụng sẽ có tài khoản khác nhau, khi kết nối VPN sẽ nhận được địa chỉ IP và chính sách truy cập vào hệ thống khác nhau.

5	Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống	Có	NGFW đã cấu hình connection/session limit, rate-limit/DoS profile cho từng dịch vụ công bố; áp dụng ngưỡng theo năng lực thực tế của cụm NGFW01–NGFW02. Có cảnh báo sớm khi tiệm cận ngưỡng; tự động drop/throttle khi vượt ngưỡng

1.3 Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức	Có	Cặp NGFW đã áp dụng nguyên tắc default-deny/allow-list tại biên và DMZ. Mỗi dịch vụ công bố ra Internet có policy riêng (nguồn/đích/cổng/giao thức, NAT, IPS/AV/URL, SSL inspection trong phạm vi thiết kế). Tất cả dịch vụ ngoài danh mục nghiệp vụ bị chặn. Nhật ký được tập trung về SIEM và giám sát 24/7.
2	Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian	Có	Đã cấu hình time-based policy trên NGFW/Reverse Proxy cho từng dịch vụ: chỉ cho phép trong khung giờ làm việc hoặc lịch đã phê duyệt; ngoài thời gian này tự động từ chối. Phiên rỗi bị hủy bằng idle-timeout; có lịch bật/tắt tạm khi bảo trì.
3	Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy	Có	Đã triển khai RBAC trên VPN/NGFW: người dùng đăng nhập bằng tài khoản cá nhân được gán nhóm/quyền theo chức năng; chính sách tường lửa User-ID/group-based

	chủ nội bộ theo chức năng và chính sách của tổ chức		map đến phân đoạn đích (server, DB, ứng dụng). Bổ sung Network Access Control/Endpoint kiểm tra thiết bị trước khi cấp quyền.

1.4. Nhật ký hệ thống

Yêu cầu **Thiết bị**	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống	Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian	Lưu trữ và quản lý tập trung nhật ký hệ thống	Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng
Danh mục thiết bị được được mô tả chi tiết tại mục 4.4	+ (Thiết lập chức năng tự động lưu log trên các thiết bị mạng)	+ (Hệ thống có cài đặt 02 máy chủ time server, các thiết bị mạng được đồng bộ thời gian qua 02 server này)	+ (Phân bổ phân vùng trên máy chủ để lưu log)	+ (Thực hiện lưu trữ log thủ công trên hệ thống lưu trữ của đơn vị)

1.5. Phòng chống xâm nhập

STT	**Yêu cầu**	**P/A**	**Ghi chú/Mô tả**
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Có	Cặp NGFW đã triển khai đầy đủ IPS/Anti-Malware cho tất cả phân vùng (Server Farm/DMZ/User). Chính sách "default-deny/allow-list", nhật ký tập trung về SIEM và giám sát 24/7.

2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Có	Cặp NGFW + hệ APT đã cấu hình cập nhật tự động signature/engine đồng thời áp dụng áp dụng cập nhật khẩn khi có CVE/zero-day.
3	Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp	Có	Hệ thống mạng lõi, tường lửa chạy HA bật các profile bảo mật trong phạm vi hiệu năng

1.6. Phòng chống phần mềm độc hại trên môi trường mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống phần mềm độc hại trên môi trường mạng	Có	Hệ thống đã triển khai đồng bộ cặp Firewall NGFW bật IPS/Anti-Malware/URL Filtering.
2	Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại	Có	Tất cả thành phần (NGFW, AV) cập nhật tự động signature/engine/IOC theo lịch của hãng đồng thời Áp dụng cập nhật khẩn khi có CVE/zero-day
3	Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp	Có	Cặp NGFW chạy HA; năng lực throughput/sessions đáp ứng yêu cầu kỹ thuật ngay cả khi bật toàn bộ các tính năng bảo mật

1.7. Bảo vệ thiết bị hệ thống

Yêu cầu	Cấu hình chức năng xác	Chỉ cho phép sử dụng các kết nối	Hạn chế các địa chỉ mạng có thể	Hạn chế được số	Phân quyền truy cập,	Nâng cấp, xử lý điểm yếu an	Xóa bỏ thông tin cấu hình, dữ liệu

Thiết bị	thực trên các thiết bị.	mạng an toàn khi truy cập, quản trị thiết bị từ xa	kết nối, quản trị thiết bị từ xa	lần đăng nhập sai	quản trị thiết bị	toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng	trên thiết bị hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ khỏi hệ thống
Danh mục thiết bị mạng tại mục 4.4	+ (Cấu hình xác thực trên các thiết bị: các thiết bị mạng được cấu hình xác thực qua tài khoản được tạo trên thiết bị)	+ (Chỉ sử dụng các kết nối an toàn và được mã hóa hoặc sử dụng phần mềm chia sẻ màn hình từ xa an toàn có bản quyền trong quá trình quản trị)	+ Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa: thực hiện trên các thiết bị tường lửa của TTDL (đã trình bày tại các phần trước)	+ Hạn chế được số lần đăng nhập sai: được thực hiện trên thiết bị mạng 5 lần login sai trong 3 phút sẽ bị tạm khóa tài khoản 15 phút)	+ Phân quyền truy cập, quản trị thiết bị: được thực hiện trên thiết bị mạng	+ (Các thiết bị được cập nhật OS hoặc các bản vá mới nhất trước khi đưa vào sử dụng)	+ (Luôn luôn Thực hiện xóa bỏ cấu hình thiết bị khi thay đổi hệ thống hoặc gỡ bỏ thiết bị khỏi hệ thống có kiểm tra và giám sát quá trình này)

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

Yêu cầu **Máy chủ**	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn	Hạn chế số lần đăng nhập sai	vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định
Danh sách máy chủ, hệ điều hành, ứng dụng đi kèm tại mục 4.5	+ (Thiết lập chính sách xác thực trên máy chủ: Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, xác thực trên các máy chủ thông qua kết nối SSH hoặc truy cập từ xa qua kết nối VPN)	+ (Sau khi cài đặt thực hiện xóa bỏ các tài khoản mặc định)	+ (Thiết lập mật khẩu bao gồm đầy đủ các yếu tố theo quy định và định kỳ thay đổi mật khẩu đăng nhập)	+ Có giao diện cho phép thiết lập thiết lập chính sách về số lần đăng nhập sai trong khoảng thời gian nhất định	+ Cho phép vô hiệu hóa tài khoản khi tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định

2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối		Thay đổi cổng quản trị	Giới hạn địa chỉ mạng

Máy chủ	mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)	mặc định của máy chủ	được phép truy cập, quản trị máy chủ từ xa
Danh sách máy chủ, hệ điều hành, ứng dụng đi kèm tại mục 4.5	+ Đối với máy chủ Window. Thiết lập một máy chủ quản trị sử dụng giải pháp kết nối VPN, từ máy chủ quản trị này cho phép kết nối đến các máy chủ, thiết bị mạng trong hệ thống. Đối với máy chủ linux sử dụng giải pháp kết nối có mã hóa (SSH)	+ Cấu hình thời gian chờ sau 10s nếu không có thao tác tự động kết thúc phiên kết nôi	+ Thực hiện thay đổi cổng quản trị mặc định của máy chủ, thông thường thay đổi cổng RDP	+ Thực hiện cấu hình các máy chủ chỉ cho phép kết nối tới các máy trong bảng danh sách acess list (thực hiện cấu hình trên firewall)

2.3. Nhật ký hệ thống

Yêu cầu	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống	Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng
Máy chủ					

Danh sách máy chủ, hệ điều hành, ứng dụng đi kèm tại mục 4.4	+ (Thiết lập chức năng tự động lưu log trên các máy chủ nghiệp vụ)	+ (Hệ thống có cài đặt 02 máy chỉ time server, các máy chủ nghiệp vụ được đồng bộ thời gian qua 02 server này)	+ (Phân bổ phân vùng trên máy chủ để lưu log)	+ (Thực hiện lưu trữ log thủ công trên hệ thống lưu trữ của đơn vị, đồng thời cũng đề xuất giải pháp quản lý lưu trữ log tập trung)	+ (Định kỳ Back up dữ liệu log trên hệ thống SAN)

2.4. Phòng chống xâm nhập

Yêu cầu / **Máy chủ**	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Danh sách máy chủ, hệ điều hành, ứng dụng đi kèm tại mục 4.4	+ (Xóa bỏ hoặc vô hiệu hóa các tài khoản mặc định. Đồng thời chỉ tạo lập các tài khoản theo	+ (Thiết lập chính sách dựa trên nghiệp vụ của từng máy chủ, tạo danh	+ (Chỉ mở các cổng cần thiết tương ứng với yêu cầu của PM, ứng dụng	+ (Các máy chủ trước khi đưa vào hoạt động nghiệp vụ phải được rà quét các lỗ

	nhu cầu của bộ phận chuyên môn)	sách access list chi tiết (In, Out) cho từng máy chủ trên Firewall	hoặc dịch vụ, đồng thời khi phát hiện nguy cơ an toàn mạng cần thiết có thể định nghĩa và đổi lại các cổng cho phù hợp. Các cổng này phải được định nghĩa trên phần mềm và cấu hình trên FW)	hổng bảo mật và kiểm tra nâng cấp OS phiên bản mới nhất)

2.5. Phòng chống phần mềm độc hại

Yêu cầu **Máy chủ**	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt	Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ
Danh sách máy chủ, hệ điều hành, ứng dụng đi kèm tại mục 4.4	+ (Trước khi đưa vào hoạt động nghiệp vụ các máy chủ phải được cài đặt phần mềm diệt	+ (Các máy chủ trước khi đưa vào hoạt động nghiệp vụ phải được kiểm tra dò quét xử lý các phần mềm độc hại)	+ (Chỉ sử dụng giải pháp quản lý tập trung phần mềm phòng chống virus, mã độc)

	virus có bản quyền)		

2.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Có	Sử dụng giải pháp đi kèm HĐH
2	Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành	Có	Sử dụng các giải pháp sao lưu trên các hệ thống máy chủ, SAN để thực hiện sao lưu dữ liệu trên máy chủ,
3	Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa	Có	Format cấp thấp hệ thiết bị. Hủy thiết bị cũ/hỏng

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

Yêu cầu	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định	Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng	Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng
Ứng dụng						

Danh sách ứng dụng/dịch vụ hạ tầng đi kèm tại mục 4.6	+ (Sử dụng các ứng dụng quản trị kèm theo thiết bị do hãng cung cấp)	+ (Các thông tin xác thực hệ thống được tuân thủ theo tiêu chuẩn của hãng)	+ (Sử dụng các ứng dụng quản trị kèm theo thiết bị do đó thông tin xác thực được mã hóa theo tiêu chuẩn của nhà sản xuất)	+ (Sử dụng các ứng dụng quản trị kèm theo thiết bị do hãng cung cấp có tính năng hạn chế số lần đăng nhập sai)	+ (Sử dụng các ứng dụng quản trị kèm theo thiết bị do đó thông tin xác thực được mã hóa theo tiêu chuẩn của hãng)	+ (Sử dụng các ứng dụng quản trị kèm theo thiết bị do hãng cung cấp)

3.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa	Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với từng người/nhóm sử dụng	Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng
Ứng dụng					

Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV	+ (Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa: truy cập quản trị các thiết bị qua kết nối SSH; truy cập từ xa qua kết nối VPN (đã trình bày tại các phần trước)	+ (Thiết bị có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng)	+ (Thực hiện trên các thiết bị tường lửa của TTDL (đã trình bày tại các phần trước)	+ (Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng người/nhóm sử dụng. Có chức năng thực thi chính sách phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau)	+ (Sử dụng phần mềm quản trị đi kèm của hãng. Phần mềm có chức năng Giới hạn số lượng các kết nối đồng thời)

3.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động	Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng
Ứng dụng			

Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV	+ (Thực hiện theo quy trình nghiệp vụ)	+ Đã triển khai Hệ thống log tập trung/SIEM (collector–indexer–dashboard).	+ (Thực hiện lưu trữ log thủ công trên hệ thống lưu trữ của đơn vị, đồng thời cũng đề xuất giải pháp quản lý lưu trữ log tập trung hoặc nghiên cứu triển khai hệ thống lưu trữ log tập trung mã nguồn mở)

3.4. Bảo mật thông tin liên lạc

Yêu cầu	Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật.	Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền
Ứng dụng		
Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV	+ (Sử dụng phần mềm quản trị do hãng cung cấp do đó các thông tin, dữ liệu đã được mã hóa theo tiêu chuẩn của nhà sản xuất)	+ (Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền: Sử dụng giao thức Https để đảm bảo các thông tin trao đổi trên môi trường mạng đã được mã hóa an toàn)

3.5. Chống chối bỏ

Yêu cầu	

Ứng dụng	Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu
Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV	+ Các ứng dụng dùng để quản trị và vận hành Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV đều là các giải pháp thương mại hoặc mã nguồn mở. Hệ thống không có các ứng dụng tự phát triển.

3.6. An toàn ứng dụng và mã nguồn

Yêu cầu **Ứng dụng**	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa	Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS Command injection, RFI, LFI, Xpath injection, XSS, CSRF
Hệ thống cơ sở hạ tầng thông tin nghiệp vụ KTTV	+ (Sử dụng phần mềm quản trị do hãng cung cấp do đó chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý được tuân thủ theo tiêu chuẩn của nhà sản xuất)	+ (Sử dụng phần mềm quản trị do hãng cung cấp do đó chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy được tuân thủ theo tiêu chuẩn của nhà sản xuất)	+ Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa: thực hiện trên các thiết bị tường lửa của TTDL (đã trình bày tại các phần trước)	+ (Sử dụng phần mềm quản trị do hãng cung cấp do đó thiết bị có tính năng chống lại những dạng tấn công phổ biến: SQL Injection, OS Command injection, RFI, LFI, Xpath injection, XSS, CSRF.)

4. Bảo đảm an toàn dữ liệu

4.1. Nguyên vẹn dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.	Có	Các tệp cấu hình của thiết bị hạ tầng được tạo mã HASH trước khi sao lưu định kỳ. Bản sao lưu và mã HASH được lưu tại 2 nơi khác nhau.

4.2. Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có	Các thông tin cấu hình, mật khẩu truy cập… được quản lý trong phần mềm mã hóa trước khi lưu trữ trên hệ thống lưu trữ và sao lưu. Ngoài ra đơn vị cũng sử dụng phần mềm mã nguồn mở (KeePass) để quản lý mật khẩu

4.3. Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ	Có	Sao lưu các tập tin cấu hình hệ thống, cấu hình phần mềm, cơ sở dữ liệu, thông tin thư mục, đường dẫn. Các bản sao lưu được lưu giữ trên 02 thiết bị khác nhau (SAN và thiết bị lưu trữ di động).

			Trong trường hợp khôi phục cán bộ kỹ thuật sẽ thực hiện các kỹ thuật kiểm tra các file cấu hình và các mã kiểm tra để đánh giá tính toàn vẹn của thông tin sao lưu.
2	Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau	Có	Thông tin dữ liệu được phân theo từng nhóm: Nhóm CSDL; Máy chủ hạ tầng; Thiết bị mạng, Thiết bị ATTT…
3	Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng	Có	Hệ thống SAN được phân vùng lưu trữ riêng để phục vụ việc lưu trữ thông tin, dữ liệu.

PHẦN IV. YÊU CẦU CƠ BẢN VỀ AN TOÀN VẬT LÝ CHO HỆ THỐNG THÔNG TIN CẤP ĐỘ 3

A.3. Yêu cầu vật lý cho hệ thống thông tin cấp độ 3

A.3.1. Lựa chọn vị trí vật lý

Yêu cầu A.3.1	Lựa chọn vị trí vật lý Vị trí phòng máy chủ không được nằm ở các tầng cao của tòa nhà; không đặt dưới tầng hầm hoặc dưới các nơi chứa, đựng nước
Hiện trạng	Đáp ứng.
Phương án	Trung tâm dữ liệu của Cục KTTV đặt tại tầng 3 tòa nhà tác nghiệp KTTV

A.3.2. Kiểm soát truy cập vật lý

Yêu cầu A.3.2 a	Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ
Hiện trạng	Đáp ứng.
Phương án	Trung tâm Dữ liệu của Cục KTTV được chia thành các phòng riêng biệt. Các phòng đều được bố trí hệ thống kiểm soát ra vào (nhận dạng vân tay hoặc mật khẩu riêng của từng cá nhân, việc ra vào DC được đăng ký và giám sát bởi cán bộ kỹ thuật trực tại phòng NOC)
Yêu cầu A.3.2 b	Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ. Dữ liệu nhật ký Camera phải được lưu trữ tối thiểu 03 tháng
Hiện trạng	Đáp ứng
Phương án	Trung tâm Dữ liệu của Cục KTTV có hệ thống Camera giám sát. Dữ liệu hình ảnh được truyền về thiết bị chuyên dụng cho phép cán bộ quản trị giám sát online đồng thời lưu trữ dữ liệu phục vụ việc trích xuất dữ liệu hình ảnh khi cần thiết.

Yêu cầu A.3.2 c	Có phương án kiểm soát các thiết bị, vật dụng được mang ra vào phòng máy chủ
Hiện trạng	Đáp ứng
Phương án	Thiết kế Trung tâm Dữ liệu của Cục có phòng NOC. Đơn vị vận hành hệ thống thực hiện thực hiện giám sát 24h/24h. Việc ra vào phòng máy chủ phải được sự đồng ý của cán bộ giám sát.

A.3.3. Chống trộm, chống phá hoại

Yêu cầu A.3.3 a	Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định và gắn nhãn mô tả
Hiện trạng	Đáp ứng.
Phương án	Toàn bộ máy chủ, thiết bị mạng đều được đặt trong các tủ Rack và được gắn nhãn mô tả
Yêu cầu A.3.3 b	Kết nối vật lý (cáp mạng, điện thoại…) trong phòng phải được đi ngầm và có đường ống bảo vệ
Hiện trạng	Đáp ứng
Phương án	Trong Trung tâm Dữ liệu của Cục, cáp mạng được đi trên hệ thống thang máng cáp riêng biệt
Yêu cầu A.3.3 c	Thiết lập hệ thống báo động chống trộm tự động
Hiện trạng	Đáp ứng
Phương án	Trung tâm dữ liệu đã triển khai hệ thống camera giám sát an ninh 24/7**,** được kết nối tập trung về phòng NOC nhằm bảo đảm kiểm soát, phát hiện và cảnh báo kịp thời các hành vi xâm nhập trái phép.

A.3.4. Chống sét

Yêu cầu A.3.4 a	Tòa nhà đặt trong phòng máy chủ phải được thiết lập hệ thống chống sét và được nghiệm thu, kiểm tra kỹ thuật của ban quản lý tòa nhà
Hiện trạng	Đáp ứng.
Phương án	Trung tâm dữ liệu của Cục KTTV được thiết kế bao gồm hệ thống chống sét trực tiếp và hệ thống chống sét lan truyền đường nguồn. Trước khi đưa vào vận hành, hệ thống chống sét đã được kiểm tra kỹ thuật của ban quản lý tòa nhà.
Yêu cầu A.3.4 b	Các thiết bị, tủ kỹ thuật trong phòng máy chủ phải được nối đất
Hiện trạng	Đáp ứng
Phương án	Toàn bộ các Rack trong Trung tâm dữ liệu đã được thực hiện nối đất. Hệ thống tiếp địa được được đo kiểm bằng thiết bị chuyên dụng.

A.3.5. Chống cháy

Yêu cầu A.3.5 a	Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động
Hiện trạng	Đáp ứng.
Phương án	Trung tâm Dữ liệu của Cục được trang bị hệ thống tự động cảnh báo và tự động chữa cháy sử dụng khí FM200.
Yêu cầu A.3.5 b	Phòng máy chủ phải được xây dựng xử dụng các vật liệu chịu lửa
Hiện trạng	Đáp ứng

Phương án	Thiết kế vách ngăn giữa các phòng trong Trung tâm dữ liệu được sử dụng vật liệu thạch cao chống cháy

A.3.6. Chống ẩm và chống thấm

Yêu cầu A.3.6 a	Tường và sàn nhà của phòng máy chủ có các đường ống thoát nước không được đi qua trần, sàn phòng máy chủ
Hiện trạng	Đáp ứng.
Phương án	Trong Trung tâm dữ liệu của Cục không có các đường ống thoát nước
Yêu cầu A.3.6 b	Trần và các cửa, cửa sổ phòng máy chủ phải được thiết kế đảm bảo không bị nước mưa hắt vào
Hiện trạng	Đáp ứng
Phương án	
Yêu cầu A.3.6 c	Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy
Hiện trạng	Đáp ứng
Phương án	

A.3.7. Chống tĩnh điện

Yêu cầu A.3.2 a	Có biện pháp chống tĩnh điện đối với các thiết bị mạng chính
Hiện trạng	Đáp ứng
Phương án	Các thiết bị mạng, tủ rack đều được nối đất
Yêu cầu	Sàn phòng máy chủ cần phải được lắp đặt sàn chống tĩnh điện

A.3.2 b	
Hiện trạng	Đáp ứng
Phương án	Vật liệu thi công sàn nâng trong Trung tâm dữ liệu của Cục là sàn nâng chống được tĩnh điện, chống ẩm ướt và chống cháy.

A.3.8. Kiểm soát nhiệt độ và độ ẩm

Yêu cầu A.3.2	Có điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ
Hiện trạng	Đáp ứng.
Phương án	Trung tâm dữ liệu của Cục được đầu tư 04 hệ thống điều hòa chính xác đảm bảo về nhiệt độ, độ ẩm trong phòng máy chủ

A.3.9. Nguồn cung cấp

Yêu cầu A.3.9 a	Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định có ổn áp, chống quá tải
Hiện trạng	Đáp ứng.
Phương án	Nguồn điện cung cấp cho các máy chủ được đấu nối với UPS. UPS có tính năng ổn áp và chống quá tải
Yêu cầu A.3.9 b	Có nguồn cung cấp điện dự phòng, có thể thay thế nguồn cung cấp điện chính
Hiện trạng	Đáp ứng
Phương án	Trung tâm dữ liệu sử dụng nguồn điện dự phòng bằng máy phát điện của tòa nhà tác nghiệp KTTV
Yêu cầu A.3.9 c	Có hệ thống UPS đảm bảo hoạt động liên tục của các thiết bị hệ thống và máy chủ
Hiện trạng	Đáp ứng

Phương án	Trung tâm dữ liệu của Cục được đầu tư 03 UPS với tổng công suất 480KVA và được cấu hình 2N+1

A.3.10. Bảo vệ điện từ

Yêu cầu A.3.10 a	Đường điện và cáp tín hiệu (cáp mạng, thoại…) phải được cách ly để tránh nhiễu điện từ trường sang cáp tín hiệu
Hiện trạng	Đáp ứng.
Phương án	Đường điện trong Trung tâm dữ liệu dược triển khai dưới sàn nâng, đường cáp mạng được triển khai trên các hệ thống thang máng cáp (trên trần).
Yêu cầu A.3.10 b	Có phương án che chắn, cách ly các nguồn nhiễu điện từ như: các máy biến áp, các động cơ và máy phát điện, thiết bị X quang, các máy phát rada hoặc vô tuyến, thiết bị hàn nhiệt
Hiện trạng	Đáp ứng
Phương án	Trung tâm dữ liệu của Cục KTTV được chia thành các phòng chức năng riêng biệt (Phòng mạng, phòng máy chủ, phòng nguồn, phòng điều hòa, phòng chữa cháy). Các phòng được phân chia và ngăn cách bởi các vách ngăn bằng thạch cao. Các tấm thạch cao này là thạch cao chuyên dụng có khả năng chống lại bức xạ điện từ bên ngoài hoặc nhiễu điện từ.