BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1866/QĐ-BTNMT	*Hà Nội, ngày 23 tháng 7 năm 2019*

QUYẾT ĐỊNH

Phê duyệt đề xuất cấp độ và phương án bảo đảm an toàn thông tin cho hệ thống thông tin

BỘ TRƯỞNG BỘ TÀI NGUYÊN 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 36/2017/NĐ-CP ngày 04 tháng 4 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài nguyên và Môi trường;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 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 3313/QĐ-BTNMT ngày 25/12/2017 của Bộ trưởng Bộ TN&MT Ban hành Kế hoạch triển khai nhiệm vụ bảo đảm an toàn, an ninh thông tin của Bộ Tài nguyên và Môi trường giai đoạn 2018 - 2020;

Căn cứ Quyết định số 3210/QĐ-BTNMT ngày 24/10/2018 của Bộ trưởng Bộ Tài nguyên và Môi trường ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Tài nguyên và Môi trường;

Xét đề nghị của Cục trưởng Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ và phương án bảo đảm an toàn thông tin cho hệ thống thông tin "Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Bộ Tài nguyên và Môi trường", cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin: Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Bộ Tài nguyên và Môi trường.

Bao gồm 02 hệ thống thông tin thành phần:

- Hệ thống cơ sở hạ tầng công nghệ thông tin - Trung tâm dữ liệu tại Trụ sở Bộ Tài nguyên và Môi trường (số 10 Tôn Thất Thuyết, Hà Nội).

- Hệ thống cơ sở hạ tầng công nghệ thông tin - Trung tâm dữ liệu tại Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường (Số 28 Phạm Văn Đồng, Hà Nội).

b) Đơn vị vận hành hệ thống thông tin: Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường.

c) Địa chỉ: Số 28, Phạm Văn Đồng, Phường Dịch Vọng Hậu, Quận Cầu Giấy, TP. 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, quá trình vận hành hệ thống thông tin tương ứng với cấp độ 3 phù hợp với quy định tại Thông tư 03/2017/TT-BTTTT ngày ngày 24 tháng 04 năm 2017 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 và Tiêu chuẩn quốc gia TCVN 11930:2017.

(Thuyết minh hồ sơ đề xuất cấp độ cho Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Bộ Tài nguyên và Môi trường ban hành kèm theo Quyết định này)

Điều 2. Tổ chức thực hiện

1. Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường 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 đơn vị trực thuộc Bộ khi triển khai các hệ thống thông tin trên hạ tầng của Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Bộ Tài nguyên và Môi trường phải tuân thủ các phương án bảo đảm an toàn đã được phê duyệt.

3. Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường có trách nhiệm kiểm tra, giám sát thực hiện Quyết định này và báo cáo Bộ Tài nguyên 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 Công nghệ thông tin và Dữ liệu tài nguyên môi trường và Thủ trưởng các đơn vị trực thuộc Bộ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng, các Thứ trưởng;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, VP, CNTT.

BỘ TRƯỞNG

Ký bởi: Bộ Tài nguyên và Môi trường
Email: btnmt@monre.gov.vn
Cơ quan: Bộ Tài nguyên và Môi trường
Ngày ký: 09:11:25 +07:00

Trần Hồng Hà

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

THUYẾT MINH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ CHO

HỆ THỐNG CƠ SỞ HẠ TẦNG CÔNG NGHỆ THÔNG TIN THUỘC PHẠM VI QUẢN LÝ CỦA BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Hà Nội - 2019

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

THUYẾT MINH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ CHO HỆ THỐNG CƠ SỞ HẠ TẦNG CÔNG NGHỆ THÔNG TIN THUỘC PHẠM VI QUẢN LÝ CỦA BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

(Kèm theo Quyết định số /QĐ-BTNMT ngày tháng năm 2019 của Bộ trưởng Bộ Tài nguyên và Môi trường)

ĐƠN VỊ CHỦ QUẢN BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG BỘ TRƯỞNG	ĐƠN VỊ VẬN HÀNH CỤC CNTT & DỮ LIỆU TNMT KT. CỤC TRƯỞNG PHÓ CỤC TRƯỞNG
Ký bởi: Bộ Tài nguyên và Môi trường Email: hiantt@monre.gov.vn Cơ quan: Bộ Tài nguyên và Môi trường Ngày ký: 23.07.2019 09:11:37 +07:00	
Trần Hồng Hà	**Trần Văn Đoài**

Hà Nội - 2019

MỤC LỤC

PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ

1.1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Bộ Tài nguyên và Môi trường.

- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn: Nghị định số 36/2017/NĐ-CP ngày 04 tháng 04 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của bộ tài nguyên và môi trường.

- Địa chỉ: Số 10 Tôn Thất Thuyết - Hà Nội.

- Thông tin liên hệ: Điện thoại: (0243) 7956868 - Fax: (0243) 8359221 - Email: dinte@monre.gov.vn.

1.2. Thông tin Đơn vị vận hành

STT	Hệ thống thông tin	Đơn vị vận hành
1	Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL của Bộ Tài nguyên và Môi trường tại số 10 Tôn Thất Thuyết, Hà Nội (sau đây gọi tắt là TTDL của Bộ TN&MT đặt tại trụ sở Bộ)	Tên đơn vị: Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường Người đại diện: Lê Phú Hà Chức vụ: Cục Trưởng Địa chỉ: 28 Phạm Văn Đồng, Dịch Vọng Hậu, Cầu Giấy, Hà Nội. Thông tin liên hệ: 02.437548925, cuccntt@monre.gov.vn.
2	Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL của Bộ Tài nguyên và môi trường tại Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường số 28 Phạm Văn Đồng, Hà Nội (sau đây gọi tắt là TTDL của Bộ TN&MT đặt tại Cục CNTT&DL TNMT)	Tên đơn vị: Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường Người đại diện: Lê Phú Hà Chức vụ: Cục Trưởng Địa chỉ: 28 Phạm Văn Đồng, Dịch Vọng Hậu, Cầu Giấy, Hà Nội.

		Thông tin liên hệ: 02.437548925, cuccntt@monre.gov.vn.

1.3. Mô tả phạm vi, quy mô của hệ thống

Hệ thống cơ sở hạ tầng công nghệ thông tin của 02 TTDL được xây dựng qua các dự án của Bộ TN&MT, cụ thể:

STT	Dự án	Mô tả
1	Dự án xây dựng TTDL trụ sở Bộ	- Xây dựng TTDL của Bộ đặt tại trụ sở Bộ TN&MT - Đầu tư các hệ thống môi trường: điện, điều hòa chính xác, lưu điện, phòng chống cháy nổ, phát hiện rò rỉ chất lỏng, ... *(Chi tiết trong Báo cáo Thiết kế dự án "Dự án xây dựng TTDL trụ sở Bộ" kèm theo)*
2	Dự án "Xây dựng hệ thống mạng thông tin ngành Tài nguyên và môi trường"	- Xây dựng TTDL của Bộ đặt tại Cục CNTT&DL TNMT - Đầu tư các hệ thống môi trường: điện, điều hòa chính xác, lưu điện, phòng chống cháy nổ, phát hiện rò rỉ chất lỏng, ... - Đầu tư các hệ thống thiết bị mạng: tường lửa, chuyển mạch lõi, chuyển mạch phân phối, chuyển mạch các phân vùng, định tuyến, ... - Trang bị hệ thống máy chủ ảo hóa *(Chi tiết trong Báo cáo Thiết kế dự án "Xây dựng hệ thống mạng thông tin ngành Tài nguyên và môi trường" kèm theo)*
3	Dự án "Xây dựng hệ thống an toàn thông tin số	- Đầu tư các giải pháp ATTT tại 02 TTDL : tường lửa thế hệ mới, phòng chống tấn

	tài nguyên và môi trường trên mạng”	công mạng (IPS), thu thập phân tích log, sao lưu phục hồi dữ liệu, phòng chống tấn công từ chối dịch vụ, ... *(Chi tiết trong Báo cáo Thiết kế dự án “Xây dựng hệ thống an toàn thông tin số tài nguyên và môi trường trên mạng” kèm theo)*
4	Dự án “Đầu tư mở rộng và nâng cấp hạ tầng công nghệ thông tin phục vụ triển khai ứng dụng công nghệ thông tin ngành tài nguyên và môi trường”	- Mở rộng cơ sở hạ tầng 02 TTDL - Mở năng lực tính toán, lưu trữ, mạng của 02 TTDL *(Chi tiết trong Báo cáo Thiết kế dự án “Đầu tư mở rộng và nâng cấp hạ tầng công nghệ thông tin phục vụ triển khai ứng dụng công nghệ thông tin ngành tài nguyên và môi trường” kèm theo)*

Dưới đây là mô tả quy mô, phạm vi của 02 Hệ thống cơ sở hạ tầng CNTT.

STT	Hệ thống thông tin	Quy mô, phạm vi hệ thống
1	Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL trụ sở Bộ	TTDL của Bộ Tài nguyên và Môi trường cung cấp cơ sở hạ tầng công nghệ thông tin phục vụ chung cho hoạt động của Bộ. TTDL được đặt tại trụ sở Bộ, số 10 Tôn Thất Thuyết, Hà Nội. TTDL bao gồm các thành phần: - Hệ thống điện - Hệ thống UPS - Hệ thống điều hòa chính xác - Hệ thống phòng cháy chữa cháy - Hệ thống phát hiện cảnh báo rò rỉ chất lỏng - Hệ thống mạng: thiết bị chuyển mạch lõi, các thiết bị chuyển mạch khác, router - Các hệ thống đảm bảo an ninh thông tin + Hệ thống tường lửa thế hệ mới (hoạt động tại mức ứng dụng, tích hợp phòng chống tấn

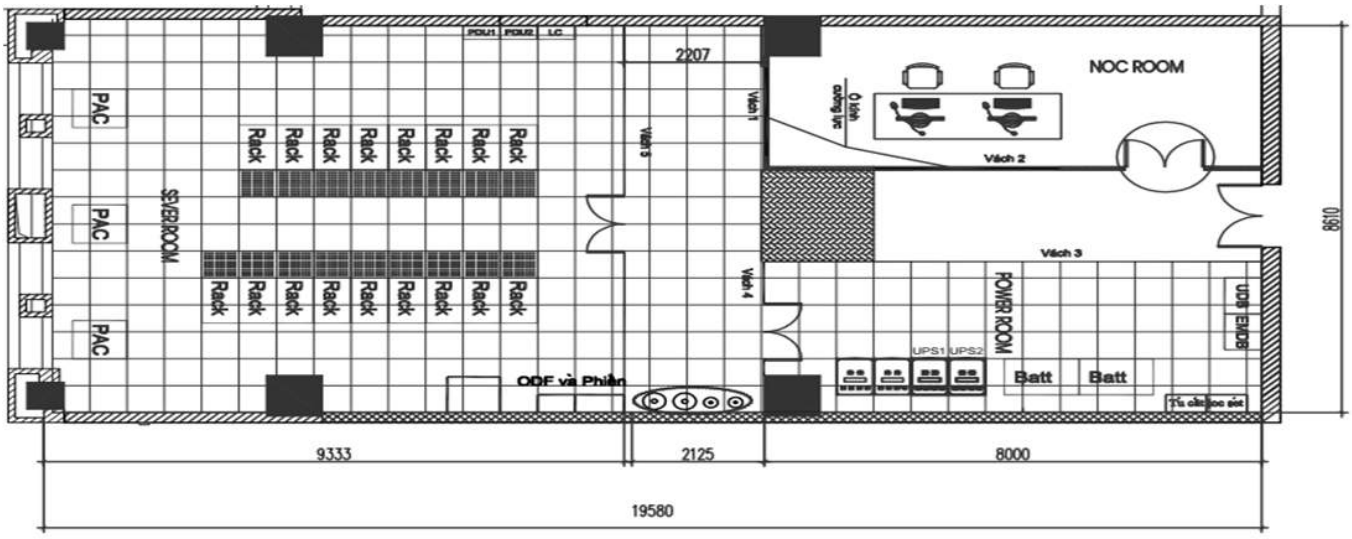
		công mạng IPS, quét virus, phòng chống tấn công có chủ đích) + Hệ thống giảm thiểu tấn công từ chối dịch vụ (DDoS) + Hệ thống thu thập và phân tích log + Hệ thống phòng chống thư rác + Hệ thống cân bằng tải + Hệ thống sao lưu và phục hồi dữ liệu + Hệ thống giám sát mạng, dịch vụ - Dịch vụ quản lý, xác thực người dùng - Dịch vụ mạng riêng ảo - Dịch vụ đồng bộ thời gian - Các hệ thống thông tin đang được đặt tại TTDL: + Cổng thông tin Bộ TN&MT + Dịch vụ công trực tuyến ngành TNMT + Quản lý văn bản điều hành + Tiếp nhận và trả lời ý kiến công dân + Thư điện tử + Quản lý khoa học công nghệ
2	Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL Cục CNTT&DL TNMT	TTDL Cục CNTT&DL TNMT cung cấp cơ sở hạ tầng công nghệ thông tin phục vụ chung cho hoạt động của Cục và dự phòng cho các dịch vụ CNTT tại TTDL trụ sở Bộ. TTDL bao gồm các thành phần: - Hệ thống điện - Hệ thống phát điện dự phòng - Hệ thống UPS - Hệ thống điều hòa chính xác - Hệ thống phòng cháy chữa cháy - Hệ thống phát hiện cảnh báo rò rỉ chất lỏng - Hệ thống mạng: thiết bị chuyển mạch lõi, các thiết bị chuyển mạch khác, router

		- Các hệ thống đảm bảo an ninh thông tin + Hệ thống tường lửa thế hệ mới (hoạt động tại mức ứng dụng, tích hợp phòng chống tấn công mạng IPS, quét virus, phòng chống tấn công có chủ đích, phòng chống thư rác) + Hệ thống thu thập và phân tích log (dùng chung với hệ thống tại TTDL trụ sở Bộ) + Hệ thống sao lưu và phục hồi dữ liệu + Hệ thống giám sát mạng, dịch vụ (dùng chung với hệ thống tại TTDL trụ sở Bộ) - Dịch vụ quản lý, xác thực người dùng (dùng chung với hệ thống tại TTDL trụ sở Bộ) - Dịch vụ mạng riêng ảo - Dịch vụ đồng bộ thời gian (dùng chung với hệ thống tại TTDL trụ sở Bộ) - Các hệ thống thông tin đang được đặt tại TTDL: + Cơ sở dữ liệu quốc gia TNMT + Thư viện điện tử + Thanh tra + Quản lý nhân sự

1.4. Mô tả cấu trúc của hệ thống

1.4.1. Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL trụ sở Bộ

a) Sơ đồ mặt bằng



Hình 1 Mặt bằng TTDL tại trụ sở Bộ

Diện tích hiện tại của TTDL trụ sở Bộ với tổng diện tích là 162 m^2 bao gồm:

+ Phòng điều hành (NOC ROOM) với diện tích là 23m^2.

+ Phòng nguồn có diện tích 24m^2: trong đó có 2 tủ nguồn đầu vào, 2 UPS 60KVA và tủ Acquy.

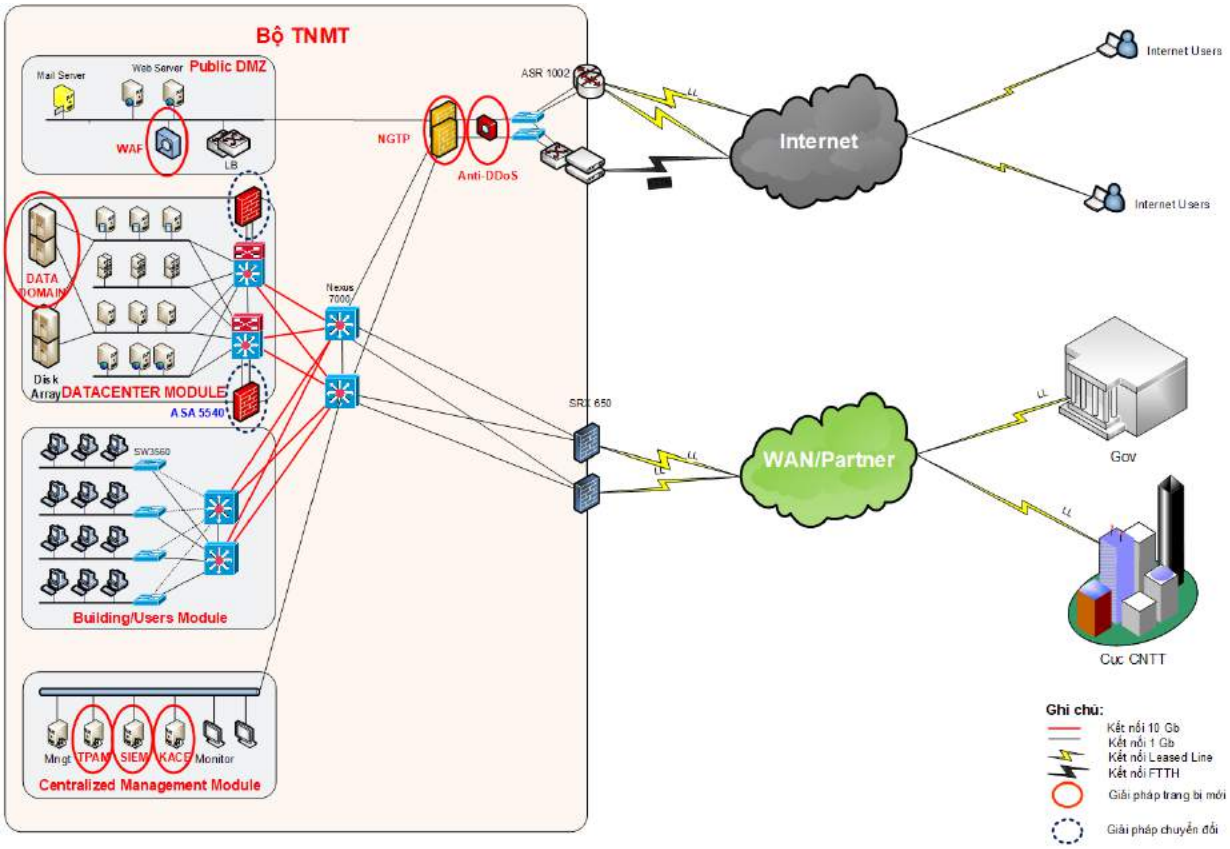
+ Phòng máy chủ có diện tích là 80 m^2: trong đó có 11 tủ rack chạy các máy chủ chạy các dịch vụ của Bộ, 3 tủ rack của Tổng cục môi trường, 3 tủ rack của dự án Hàn Quốc, 2 rack tổng đài điện thoai, 1 rack phân phối cáp quang, 2 tủ PDU phân phối nguồn cho 11 tủ rack của bộ và 3 tủ rack Tổng Cục môi trường.

+ Hành lang: 35m^2.

Hiện trạng lắp đặt sàn nâng tại TTDL (tại trụ sở Bộ): Tại TTDL (tại trụ sở Bộ), các khu vực đã được lắp đặt sàn nâng bao gồm Phòng máy chủ, phòng nguồn và 1 phần hành lang với tổng diện tích khoảng 122m^2.

Các hệ thống phòng cháy chữa cháy, cảnh báo rò rỉ chất lỏng và điều hòa chính xác được tại các vị trí theo thiết kế bên trong TTDL.

b) *Bản vẽ và thuyết minh giải pháp an ninh bảo mật tổng thể tại TTDL tại Trụ sở Bộ TN&MT*



Hình 2 Sơ đồ tổng thể hệ thống mạng - TTDL trụ sở Bộ

Thiết kế tổng thể hệ thống an toàn bảo mật tại TTDL Trụ sở Bộ TN&MT bao gồm các hạng mục sau:

- Hệ thống tường lửa thế hệ mới kiểm soát tải cổng Internet: tường lửa tại cổng Internet, được triển khai ở Layer 3, đáp ứng tính sẵn sàng cao. Các thiết bị tường lửa được quản trị thông qua phần mềm quản trị tập trung.

- Hệ thống phòng chống tấn công từ chối dịch vụ DDoS: được triển khai theo mô hình Inline tại cổng Internet. Hệ thống được triển khai chạy đơn và đặt phia trước cặp tường lửa Internet (theo hướng từ ngoài vào). Hệ thống cho phép giảm thiểu và bảo vệ các ứng dụng Public, hệ thống của MONRE trước các tấn công DDoS - tấn công gây ra mất tính sẵn sàng cho hệ thống.

- Hệ thống thu thập và phân tích log: được triển khai theo mô hình tích hợp với các thiết bị CNTT trong hệ thống. Hệ thống cho phép quản lý và phân tích và đưa ra cảnh báo an ninh cho tổ chức; hệ thống cũng cho phép quản lý và phân tích cho hệ thống mạng tại Cục CNTT thông qua đường truyền WAN. Hệ thống được đặt trong vùng mạng quản trị.

- Hệ thống sao lưu, phục hồi dữ liệu (Online và Offline): được triển khai theo mô hình tích hợp với các thiết bị CNTT trong hệ thống. Hệ thống cho phép sao lưu, phục hồi các dữ liệu quan trọng đang lưu trữ tại TTDL Trụ sở Bộ. Ngoài ra hệ thống này cho phép sao lưu, phục hồi các dữ liệu quan trọng đang lưu trữ tại TTDL Cục CNTT thông qua đường WAN. Hệ thống đặt trong vùng datacenter.

- Hệ thống phòng chống thư rác: được triển khai trong phân vùng DMZ. Về mặt logic, luồng mail vào và ra khỏi hệ thống thư điện tử monre.gov.vn được lọc tại hệ thống phòng chống thư rác nhằm: ngăn chặn thư rác, ngăn chặn email có đính kèm virus, ...

- Hệ thống cân bằng tải: cung cấp khả năng cân bằng tải mức lớp 4 (mạng) và lớp 7 (ứng dụng).

c) Danh mục thiết bị sử dụng trong hệ thống

Danh mục thiết bị, dịch vụ

STT	Tên máy chủ/thiết bị	Phân Vùng	Ghi chú
1	**Các thiết bị đảm bảo môi trường hoạt động**		
1.1	Hệ thống điện (02 tủ nguồn, 02 UPS, 02 tủ ắc qui)		
1.2	Hệ thống phòng cháy chữa cháy (bình chứa khí FM200, hệ thống ống dẫn, vòi phun)		
1.3	Hệ thống cảnh báo rò rỉ chất lỏng (thiết bị cảnh báo, hệ thống dây dẫn, sensor)		
1.4	Hệ thống điều hòa chính xác (03 điều hòa)		
2	**Các thiết bị mạng**		
2.1	Thiết bị chuyển mạch lõi (02 thiết bị)	Vùng quản trị	
2.2	Thiết bị chuyển mạch vùng DMZ (02 thiết bị)	DMZ	
2.3	Thiết bị chuyển mạch vùng FARM (02 thiết bị)	FARM	

2.4	Thiết bị định tuyến Internet (02 thiết bị)	Vùng quản trị	
2.5	Thiết bị định tuyến mạng WAN (01 thiết bị)		
3	**Các thiết bị/máy chủ bảo mật**		
3.1	Thiết bị tường lửa thế hệ mới Checkpoint 12000 (02 thiết bị chạy mô hình cluster, 01 thiết bị quản lý)	Vùng quản trị	
3.2	Thiết bị chống tấn công DDoS Checkpoint DP-506 (01 thiết bị)	Vùng quản trị	
3.3	Thiết bị lọc thư rác Fortimail 400c (01 thiết bị)	FARM	
3.4	Thiết bị thu thập và phân tích log HP Arcsight Express	FARM	
3.5	Thiết bị sao lưu và phục hồi dữ liệu EMC Networker, Data Domain (01 thiết bị lưu trữ)	DMZ	
3.6	Máy chủ giám sát mạng, dịch vụ (01 máy chủ)	DMZ	Centos 7
3.7	Thiết bị cân bằng tải Citrix Netscaler 5550	FARM	
3.8	Máy chủ quản lý, xác thực người dùng Microsoft và đồng bộ thời gian (04 máy chủ)	FARM	Windows 2008 R2 Standard, Windows 2012 Standard
3.9	Máy chủ mạng riêng ảo	DMZ	Centos 7

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

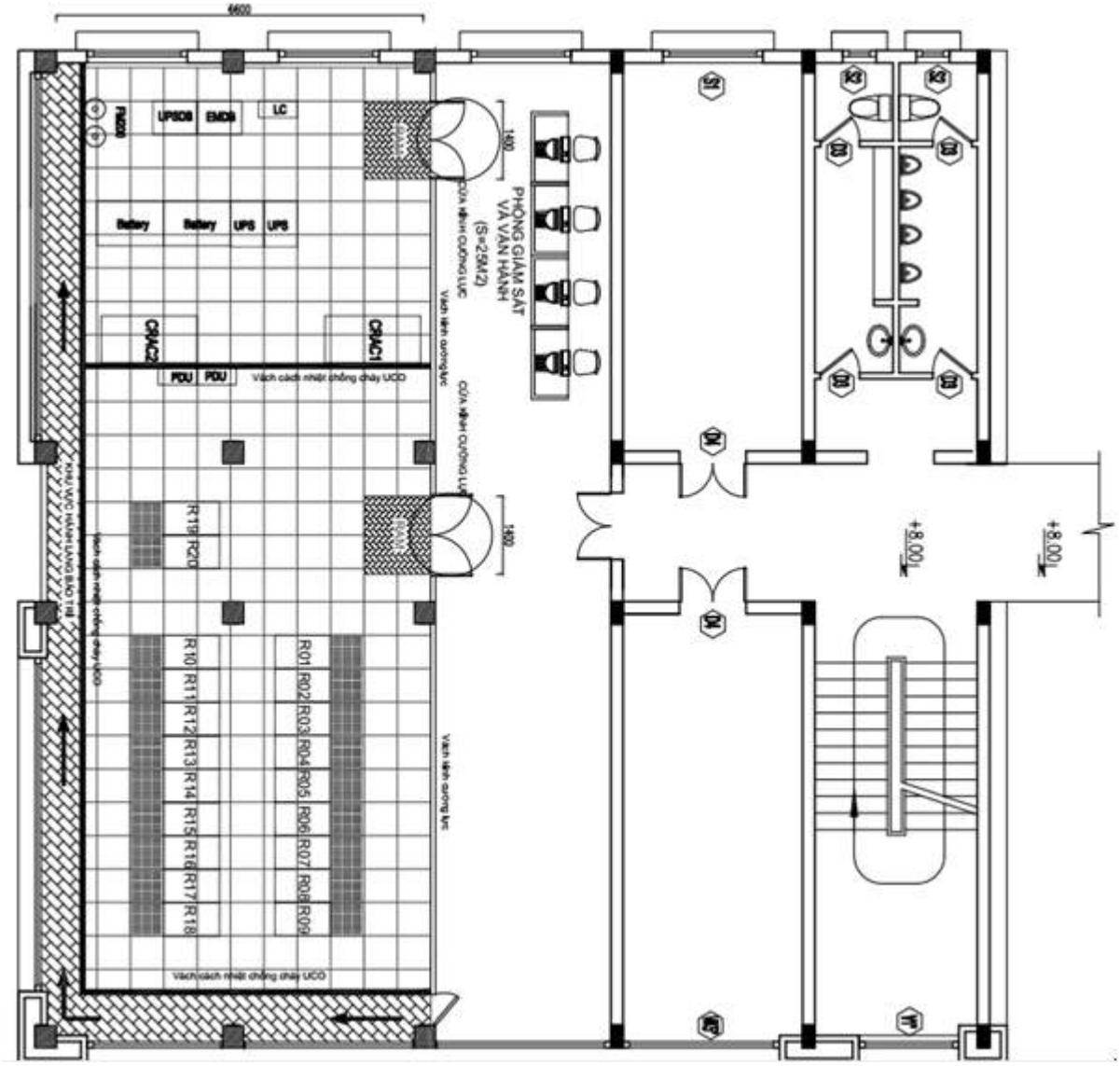
STT	Tên ứng dụng	Máy chủ triển khai	Mục đích sử dụng

1	Dịch vụ tường lửa internet	Thiết bị mục 3.1	- Tạo lập các chính sách truy cập internet, giữa các phân vùng mạng. - Phòng chống tấn công mạng (IPS) - Quét virus, phát hiện kết nối tới mạng botnet - QoS
2	Dịch vụ chống tấn công DDoS	Thiết bị mục 3.2	- Chống tấn công DdoS - Thông lượng 500 Mbps
3	Dịch vụ lọc thư rác	Thiết bị mục 3.3	- Lọc thư rác cho hệ thống email - Dò quét virus, mã độc trong các email, file đính kèm
4	Dịch vụ thu thập và phân tích log	Thiết bị mục 3.4	- Thu thập log thiết bị, ứng dụng - Phân tích log để cảnh báo nguy cơ bảo mật - Dung lượng lưu trữ 500 GB - Khả năng thu thập 250 sự kiện trên giây
5	Dịch vụ sao lưu và phục hồi dữ liệu	Thiết bị mục 3.5	- Sao lưu dữ liệu (hỗ trợ nén, mã hóa, chống trùng lặp, lập lịch) - Dung lượng sao lưu dữ liệu trên Data Domain 10 TB
6	Dịch vụ giám sát mạng, dịch vụ	Thiết bị mục 3.6	- Giám sát trạng thái thiết bị, dịch vụ

			- Giám sát băng thông mạng - Giám sát hiệu năng thiết bị, dịch vụ
7	Dịch vụ cân bằng tải	Thiết bị mục 3.7	- Cân bằng tải lớp mạng và ứng dụng
8	Dịch vụ quản lý, xác thực người dùng	Thiết bị mục 3.8	- Dịch vụ quản lý, xác thực người dùng (Microsoft Active Directory)
9	Dịch vụ mạng riêng ảo (VPN)	Thiết bị mục 3.9	- Phục vụ truy cập, quản trị các thiết bị mạng, máy chủ từ mạng Internet
10	Dịch vụ đồng bộ thời gian	Thiết bị mục 3.8	- Dịch vụ đồng bộ thời gian

1.4.2. Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL Cục CNTT&DL TNMT

a) Sơ đồ mặt bằng



Hình 3 Mặt bằng TTDL tại Cục CNTT sở Bộ

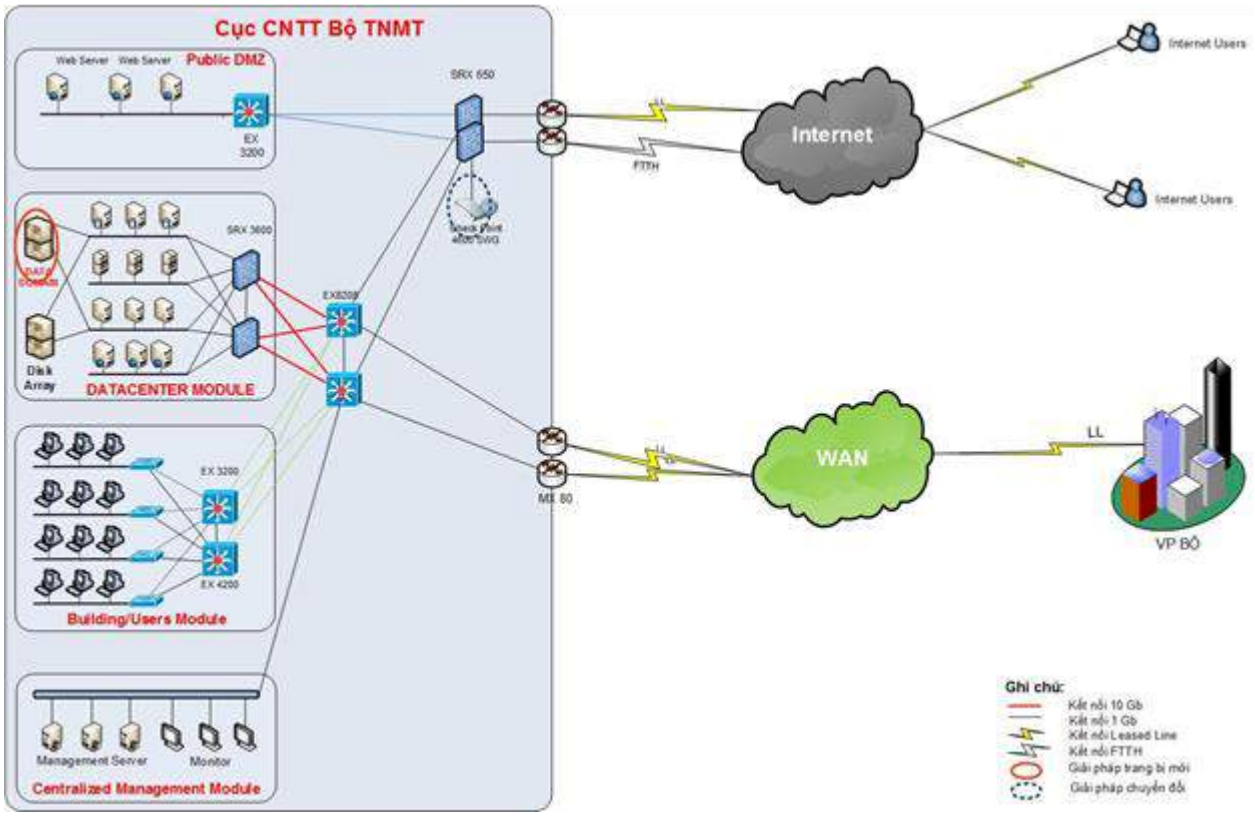
Với tổng diện tích là 152 m2, TTDL được chia thành các phòng chức năng và các hệ thống như sau:

+ Phòng điều hành với diện tích là 52m2

+ Phòng nguồn có diện tích 32m2: trong đó có 2 tủ nguồn đầu vào, 2 UPS 60KVA và 02 tủ Acquy.

+ Phòng máy chủ có diện tích là 68 m2: trong đó có 17 tủ rack chạy các máy chủ chạy các dịch vụ của Bộ và các đơn vị khác và 3 tủ rack chứa các thiết bị switch phân tầng và thiết bị thoại voice IP.

b) Bản vẽ và thuyết minh giải pháp an ninh bảo mật tổng thể tại TTDL Cục CNTT&DL TNMT



Hình 4 Sơ đồ tổng thể hệ thống mạng - TTDL Cục CNTT&DL TNMT

Thiết kế tổng thể hệ thống an toàn bảo mật tại Cục CNTT&DL TNMT bao gồm các hạng mục sau:

- Thiết bị tường lửa này sẽ thực hiện kiểm soát và đảm bảo an ninh cho người dùng trước các mối đe dọa từ Internet như: phòng chống bị tấn công mạng (IPS), phòng chống virus, kiểm soát ứng dụng, lọc và kiểm soát truy cập URL, phòng chống Botnet.

- Hệ thống sao lưu, phục hồi dữ liệu (Online và Offline): được triển khai theo mô hình tích hợp với các thiết bị CNTT trong hệ thống. Hệ thống cho phép sao lưu, phục hồi các dữ liệu quan trọng đang lưu trữ tại TTDL Cục CNTT. Ngoài ra hệ thống này cho phép sao lưu, phục hồi các dữ liệu quan trọng đang lưu trữ tại TTDL Trụ sở Bộ thông qua đường WAN. Hệ thống đặt trong vùng datacenter.

- Hệ thống thu thập và phân tích log: dùng chung hệ thống thu thập và phân tích log tại TTDL trụ sở Bộ.

c) Danh mục thiết bị sử dụng trong hệ thống

Danh mục thiết bị, dịch vụ

STT	Tên máy chủ/thiết bị	Phân Vùng	Ghi chú
1	**Các thiết bị đảm bảo môi trường hoạt động**		
1.1	Hệ thống điện (02 tủ nguồn, 02 UPS, 02 tủ ắc qui)	DMZ	
1.2	Hệ thống phòng cháy chữa cháy (bình chứa khí FM200, hệ thống ống dẫn, vòi phun)		
1.3	Hệ thống cảnh báo rò rỉ chất lỏng (thiết bị cảnh báo, hệ thống dây dẫn, sensor)		
1.4	Hệ thống điều hòa chính xác (02 điều hòa)	DMZ	
2	**Các thiết bị mạng**		
2.1	Thiết bị chuyển mạch lõi (02 thiết bị)		
2.2	Thiết bị chuyển mạch vùng DMZ, FARM (02 thiết bị chạy mô hình cluster)		
2.4	Thiết bị định tuyến Internet (02 thiết bị chạy mô hình cluster)		
2.5	Thiết bị định tuyến mạng WAN (02 thiết bị)		
3	**Các thiết bị/máy chủ bảo mật**		
3.1	Thiết bị tường lửa thế hệ mới Checkpoint 4600 (01 thiết bị)		
3.2	Thiết bị tường lửa Juniper SRX650: tường lửa DMZ, phân vùng mạng các lĩnh vực đặt máy chủ (02 thiết bị chạy mô hình cluster)		

3.3	Thiết bị tường lửa SRX3600: vùng người dùng và FARM (02 thiết chạy mô hình cluster)		
3.4	Thiết bị sao lưu và phục hồi dữ liệu EMC Networker, Datadomain (01 máy chủ quản lý sao lưu, 01 thiết bị lưu trữ)	DMZ	
3.5	Máy chủ mạng riêng ảo	DMZ	Centos 7

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

STT	Tên ứng dụng	Máy chủ triển khai	Mục đích sử dụng
1	Dịch vụ tường lửa internet	Thiết bị mục 3.1	- Tạo lập các chính sách truy cập internet, giữa các phân vùng mạng. - Phòng chống tấn công mạng (IPS) - Quét virus, phát hiện kết nối tới mạng botnet - QoS
3	Dịch vụ chặn thư rác	Thiết bị mục 3.1	- Lọc thư rác cho hệ thống email - Dò quét virus, mã độc trong các email, file đính kèm
4	Dịch vụ thu thập và phân tích log	Dùng chung thiết bị và giải pháp tại TTDL trụ sở Bộ mục 3.4	- Thu thập log thiết bị, ứng dụng - Phân tích log để cảnh báo nguy cơ bảo mật
5	Dịch vụ sao lưu và phục hồi dữ liệu	Thiết bị mục 3.5	- Sao lưu dữ liệu (hỗ trợ nén, mã hóa, chống trùng lặp, lập lịch)

6	Dịch vụ giám sát mạng, dịch vụ	Dùng chung thiết bị và giải pháp tại TTDL trụ sở Bộ mục 3.6	- Giám sát trạng thái thiết bị, dịch vụ - Giám sát băng thông mạng - Giám sát hiệu năng thiết bị, dịch vụ
7	Dịch vụ quản lý, xác thực người dùng	Dùng chung thiết bị và giải pháp tại TTDL trụ sở Bộ mục 3.7	- Dịch vụ quản lý, xác thực người dùng (Microsoft Active Directory)
8	Dịch vụ mạng riêng ảo (VPN)	Thiết bị mục 3.5	- Phục vụ truy cập, quản trị các thiết bị mạng, máy chủ từ mạng Internet

PHẦN II. THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

2.1. Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng

Hệ thống thông tin thuộc phạm vi quản lý của Bộ Tài nguyên và Môi trường, bao gồm các hệ thống thông tin với cấp độ đề xuất tương ứng

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
1	**Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL trụ sở Bộ**	Cung cấp hạ tầng TTDL, các giải pháp an toàn thông tin cho các máy chủ, thiết bị, dịch vụ đặt tại TTDL trụ sở Bộ	Cung cấp dịch vụ hạ tầng, ATTT cho các HTTT khác	Hệ thống cơ sở hạ tầng công nghệ thông tin	3	Khoản 3/Điều 9 trong 85/2016 /NĐ-CP
2	**Hệ thống cơ sở hạ tầng công nghệ thông tin - TTDL Cục CNTT&DL TNMT**	Cung cấp hạ tầng TTDL, các giải pháp an toàn thông tin cho các máy chủ, thiết bị, dịch vụ đặt tại TTDL Cục CNTT&DL TNMT	Cung cấp dịch vụ hạ tầng, ATTT cho các HTTT khác	Hệ thống cơ sở hạ tầng công nghệ thông tin	3	Khoản 3/Điều 9 trong 85/2016 /NĐ-CP

2.2. Tổng hợp đề xuất cấp độ hệ thống thông tin

Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của bộ tài nguyên và môi trường, bao gồm:

- Hệ thống cơ sở hạ tầng công nghệ thông tin - Trung tâm dữ liệu tại Trụ sở Bộ Tài nguyên và Môi trường (số 10 Tôn Thất Thuyết, Hà Nội)

- Hệ thống cơ sở hạ tầng công nghệ thông tin - Trung tâm dữ liệu tại Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường (Số 28 Phạm Văn Đồng, Hà Nội)

Theo thuyết minh trong mục 2.1, hai hệ thống thông tin thành phần đều đề xuất là cấp độ 3. Do vậy, Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của bộ tài nguyên và môi trường đề xuất **cấp độ 3**.

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

3.1. Thuyết minh phương án quản lý an toàn thông tin

Các quy định liên quan đến đảm bảo an toàn thông tin

- Bộ Tài nguyên và Môi trường ban hành Quyết định số 3313/QĐ-BTNMT ngày 25/12/2017 của Bộ trưởng Bộ TN&MT Ban hành Kế hoạch triển khai nhiệm vụ bảo đảm an toàn, an ninh thông tin của Bộ TNMT giai đoạn 2018 - 2020;

- Bộ Tài nguyên và Môi trường ban hành Quyết định 3210/QĐ-BTNMT ngày 24 tháng 10 năm 2018 "Ban hành Quy chế đảm bảo an toàn, an ninh thông tin mạng Bộ Tài nguyên và Môi trường" nhằm quy định về bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động của Bộ Tài nguyên và Môi trường và các đơn vị trực thuộc Bộ.

- Bộ Tài nguyên và Môi trường ban hành Quyết định 2019/QĐ-BTNMT ngày 01 tháng 9 năm 2016 "Ban hành Quy chế quản lý, sử dụng hệ thống thư điện tử của Bộ Tài nguyên và Môi trường" nhằm quy định việc quản lý, vận hành và sử dụng hệ thống thư điện tử công vụ của Bộ Tài nguyên và Môi trường đảm bảo phục vụ công tác quản lý, điều hành của Bộ Tài nguyên và Môi trường.

- Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường là đơn vị chuyên trách về Công nghệ thông tin của Bộ ban hành Quyết định 87/QĐ-CNTT ngày 20 tháng 5 năm 2019 "Ban hành Quy chế quản lý, vận hành, khai thác Trung tâm dữ liệu" nhằm quy định về việc quản lý, vận hành, khai thác Trung tâm dữ liệu phục vụ hiệu quả các chương trình ứng dụng, phát triển công nghệ thông tin, hiện đại hóa ngành Tài nguyên và môi trường.

TT	Yêu cầu quản lý	Mô tả khả năng đáp ứng
1	**Chính sách chung**	

1.1	Định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin	Đáp ứng. Cụ thể: - Đã ban hành quy chế bảo đảm an toàn, an ninh thông tin mạng theo Quyết định 3210/QĐ-BTNMT ngày 24 tháng 10 năm 2018, giao cục cntt rà soát cập nhật theo định kỳ.
1.2	Có chính sách an toàn thông tin cho người sử dụng bao gồm các nội dung: chính sách truy cập và sử dụng mạng và tài nguyên trên Internet; truy cập và sử dụng ứng dụng.	Đáp ứng. Cụ thể: - Quy định tại Điều 7, Quyết định 3210/QĐ-BTNMT.
1.3	Có chính sách an toàn thông tin cho đối tượng quản trị, vận hành hệ thống	Đáp ứng. Cụ thể: - Quy định tại Điều 17, 18 Quyết định 87/QĐ-CNTT.
2	**Tổ chức, nhân sự**	
2.1	Có kế hoạch và định kỳ tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan	Chưa đáp ứng. Cụ thể: ☐Có kế hoạch và định kỳ tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan. Ghi chú: Trên thực tế, đơn vị đã có những quy định về mặt chính sách và có những hoạt động đào tạo, bồi dưỡng, tuyên truyền như sau: - Quy định tại Điều 13, Quyết định 3210/QĐ-BTNMT.

		- Đơn vị vận hành cử cán bộ tham gia đầy đủ các khóa đào tạo về ATTT thuộc đề án 99 "Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020". - Định kỳ tổ chức lớp bồi dưỡng kiến thức, kỹ năng về ATTT cho cán bộ kỹ thuật quản lý, vận hành các hệ thống thông tin và người sử dụng theo yêu cầu công việc thực tế. - Là thành viên Ban Điều hành Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia. Tham gia đầy đủ các hoạt động hợp tác, chia sẻ, phối hợp trong việc đảm bảo ATTT mạng. Cục Công nghệ thông tin và Dữ liệu TNMT đang trình phê duyệt nhiệm vụ đặc thù "Ứng cứu sự cố, bảo đảm an toàn thông tin mạng tại Bộ Tài nguyên và Môi trường", trong đó hàng năm sẽ tổ chức đào tạo 03 khóa về ATTT, do đó yêu cầu 2.1 sẽ được đáp ứng vào năm 2020.
2.2	Có chính sách yêu cầu cán bộ liên quan khi thôi việc cần cam kết giữ bí mật thông tin liên quan đến dữ liệu trên hệ thống, thông tin riêng của tổ chức hoặc thông tin nhạy cảm khác;	Đáp ứng. Cụ thể: - Quy định tại Điều 6, Quyết định 3210/QĐ-BTNMT. - Quy định tại Điều 6, Quyết định 2019/QĐ-BTNMT (Quy trình cấp mới, thay đổi, hủy bỏ hộp thư điện tử). - Quy định tại Điều 3, Thông tư 11/2017/TT-BTNMT

		- Các điều khoản về cam kết giữ bí mật thông tin liên quan đến dữ liệu trên hệ thống được đưa vào trong hợp đồng lao động và cam kết riêng theo mẫu Thông tư 11.
2.3	Có quy trình, thủ tục để cấp phát, loại bỏ tài khoản, quyền truy cập của cán bộ mới tham gia sử dụng hệ thống, cán bộ thay đổi nhiệm vụ hoặc cán bộ ngừng sử dụng hệ thống	Đáp ứng. Cụ thể: - Quy định tại Khoản 4, Điều 7, Quyết định 3210/QĐ-BTNMT.
2.4	Có đầu mối liên hệ để thông báo, trao đổi, xử lý vấn đề phát sinh hoặc sự cố mất an toàn thông tin xảy ra với hệ thống thông tin.	Đáp ứng. Cụ thể: - Quyết định 87/QĐ-CNTT. Cụ thể: Đơn vị đơn vị quản lý vận hành hạ tầng TTDL: Trung tâm Cơ sở hạ tầng Công nghệ thông tin; SĐT: 024.37956868 (ext: 1005)
3	**Thiết kế xây dựng hệ thống**	
3.1	Có hồ sơ đề xuất cấp độ được thẩm định bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin	Đáp ứng. Tài liệu này là Hồ sơ đề xuất cấp độ lần đầu của Hệ thống thông tin cơ sở hạ tầng tại 02 TTDL.
3.2	Có tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin	Đáp ứng. Cụ thể: - Mô tả các phương án, giải pháp kỹ thuật đảm bảo an toàn hệ thống thông tin được trình bày trong tài liệu thiết kế thi công Dự án "Xây dựng hệ thống an toàn thông tin số tài nguyên và môi trường trên mạng".

3.3	Có phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu, bàn giao	Đáp ứng. Cụ thể: - Hệ thống cơ sở hạ tầng công nghệ thông tin (tại 02 TTDL) được xây dựng, bàn giao, nghiệm thu thông qua các dự án: 1. "Xây dựng hệ thống mạng thông tin ngành Tài nguyên và môi trường" ; 2. "Xây dựng hệ thống an toàn thông tin số tài nguyên và môi trường trên mạng"; 3. "Đầu tư mở rộng và nâng cấp hạ tầng công nghệ thông tin phục vụ triển khai ứng dụng công nghệ thông tin ngành Tài nguyên và môi trường"
4	**Quản lý vận hành**	
4.1	Có phương án giám sát an toàn thông tin cho hệ thống trong quá trình vận hành theo quy định của pháp luật	Đáp ứng. Cụ thể: - Quy định tại Điều 10, Quyết định 3210/QĐ-BTNMT. - Đơn vị thực hiện việc giám sát dựa trên các giải pháp kỹ thuật: tưởng lửa, IPS, hệ thống giám sát mạng, giải pháp dò quét lỗ hổng ứng dụng web, ...
4.2	Có kế hoạch và định kỳ tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống; cử cán bộ tham gia vào các cuộc diễn tập quốc gia hoặc quốc tế do cơ quan chức năng triệu tập	Chưa đáp ứng. ☐ Có kế hoạch. ☐ Định kỳ tổ chức Hai yêu cầu trên hiện chưa đáp ứng, nguyên nhân:

		- Bộ đã ban hành Quyết định số 3313/QĐ-BTNMT ngày 25/12/2017 của Bộ trưởng Bộ TN&MT Ban hành Kế hoạch triển khai nhiệm vụ bảo đảm an toàn, an ninh thông tin của Bộ TNMT giai đoạn 2018 - 2020, trong đó có kế hoạch xây dựng kế hoạch và tổ chức diễn tập. - Cục Công nghệ thông tin và Dữ liệu TNMT đang trình phê duyệt nhiệm vụ đặc thù "Ứng cứu sự cố, bảo đảm an toàn thông tin mạng tại Bộ Tài nguyên và Môi trường" (2020), trong đó có nội dung xây dựng kế hoạch và tổ chức diễn tập định kỳ hàng năm. Do đó 02 yêu cầu này sẽ được đáp ứng vào năm 2020. ☑ Cử cán bộ tham gia vào các cuộc diễn tập quốc gia hoặc quốc tế do cơ quan chức năng triệu tập. Đơn vị vận hành cử cán bộ tham gia đầy đủ cuộc diễn tập ứng cứu sự cố an ninh mạng do Bộ Thông tin truyền thông tổ chức với qui mô trong và ngoài nước.
4.3	Có kế hoạch khôi phục hoạt động bình thường của hệ thống trong trường hợp xảy ra sự cố hoặc thảm họa	Chưa đáp ứng. Cụ thể: Việc lập và phê duyệt kế hoạch khôi phục hoạt động của hệ thống trong trường hợp xảy ra sự cố hoặc thảm họa sẽ được Cục CNTT&DL TNMT xây dựng và phê duyệt trong nhiệm vụ đặc thù "Ứng cứu sự cố, bảo đảm an toàn thông tin mạng

		tại Bộ Tài nguyên và Môi trường" (hiện Cục đang trình Bộ phê duyệt và thực hiện năm 2020).
4.4	Có quy trình quản lý, vận hành hệ thống phù hợp yêu cầu kỹ thuật cơ bản; quản lý sự thay đổi, di chuyển hệ thống; kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống	Chưa đáp ứng. Cụ thể: ☑Có quy trình quản lý, vận hành hệ thống phù hợp yêu cầu kỹ thuật cơ bản. Quy định chính sách và quy trình tại Quyết định 87/QĐ-CNTT. ☐ Quản lý sự thay đổi, di chuyển hệ thống; kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống. Nội dung yêu cầu "Quản lý sự thay đổi, di chuyển hệ thống; kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống" sẽ được nghiên cứu, bổ sung vào Quyết định thay thế, chỉnh sửa Quyết định 87/QĐ-CNTT (năm 2020).
5	**Kiểm tra, đánh giá và quản lý rủi ro**	
5.1	Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật.	Đáp ứng. Đơn vị thực hiện hằng năm kiểm tra đánh giá an toàn thông tin.
5.2	Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.	Đáp ứng. Cục CNTT&DL TNMT là đơn vị được giao chức năng kiểm tra, đánh giá ATTT và đánh giá rủi ro (theo Điều 9 Quyết định 1168/QĐ-BTNMT về "Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường"

3.2. Thuyết minh phương án kỹ thuật

TT	Yêu cầu kỹ thuật	Mô tả khả năng, phương án kỹ thuật đáp ứng
1	**An toàn hạ tầng mạng**	
1.1	Có thiết kế vùng mạng dành riêng bao gồm vùng mạng riêng cho máy chủ nội bộ, vùng mạng riêng cho các máy chủ cung cấp các dịch vụ hệ thống cần thiết, vùng mạng riêng cho máy chủ cơ sở dữ liệu và các vùng mạng riêng khác theo yêu cầu của tổ chức	Đáp ứng. Hệ thống mạng tại 02 TTDL được phân vùng thành các vùng mạng khác nhau. Cụ thể như sau: - Vùng quản trị: dành cho cán bộ quản trị TTDL. - Vùng máy chủ: DMZ (public dịch vụ ra internet, ...), FARM (các dịch vụ không public, dịch vụ cơ sở dữ liệu, ...) - Các vùng mạng khác: vùng mạng không dây, vùng mạng cho các đơn vị đặt nhờ máy chủ, thiết bị.
1.2	Có thiết kế vùng mạng nội bộ thành các mạng chức năng riêng theo yêu cầu nghiệp vụ; phân vùng mạng riêng cho mạng không dây tách biệt với các vùng mạng chức năng; phân vùng mạng riêng cho các máy chủ cung cấp dịch vụ ra ngoài mạng Internet;	
1.3	Có phương án cân bằng tải và giảm thiểu tấn công từ chối dịch vụ	- Đáp ứng. Giải pháp cân bằng tải và giảm thiểu tấn công từ chối dịch vụ tại TTDL trụ sở Bộ (Phần 1 - Mục 4.1 - c - 3.7)
1.4	Có thiết kế hệ thống quản lý lưu trữ tập trung và giám sát an toàn thông tin	- Đáp ứng. Giám sát an toàn thông tin thông qua hệ thống tường lửa thế hệ mới và hệ thống giám sát mạng tai 02 TTDL.

1.5	Có phương án sử dụng thiết bị có chức năng tường lửa giữa các vùng mạng quan trọng	- Đáp ứng. Thiết bị tường lửa có tính năng chống xâm nhập, chặn lọc phần mềm độc hại được sử dụng giữa các phân vùng quan trọng: Internet, FARM, DMZ, người dùng, wifi, ... (thiết bị tường lửa xem tại Phần 1 - 4.1 - c và Phần 1 - 4.2 - c).
1.6	Có phương án phát hiện, phòng chống xâm nhập và chặn lọc phần mềm độc hại giữa mạng Internet và các mạng bên trong	
1.7	Có lưu trữ nhật ký các thiết bị mạng và quản lý tập trung trong vùng mạng quản trị đối với các thiết bị mạng có hỗ trợ tính năng này hoặc thiết bị mạng quan trọng	Đáp ứng. Nhật ký (log) của các thiết bị mạng được thu thập thông qua hệ thống thu thập và phân tích log (xem Phần 1 - 4.1 - c - 3.4).
1.8	Có 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	Đáp ứng. Nhật ký các thiết bị mạng (log) được lưu trữ tập trung thông qua hệ thống lưu trữ và phân tích log, tạo lập chính sách lưu trữ trong 03 tháng.
1.9	Có thiết kế dự phòng cho các thiết bị mạng chính trong hệ thống bảo đảm duy trì hoạt động bình thường của hệ thống khi một thiết bị mạng gặp sự cố	Đáp ứng. Hệ thống mạng tại 02 TTDL được thiết kế dự phòng 1+1: các thiết bị chuyển mạch cho vùng FARM, DMZ, Internet đều có dự phòng (xem Phần 1 - 4.1- c và Phần 1 - 4.2- c).
1.10	Có phương án cập nhật phần mềm, xử lý điểm yếu an toàn thông tin và cấu hình tối ưu thiết bị mạng trước khi đưa vào sử dụng trong mạng	Đáp ứng. Các thiết bị mạng đều được cập nhật phiên bản ổn định mới nhất và cấu hình tối ưu trước khi đưa vào hoạt động trong TTDL.

1.11	Có phương án xác thực tài khoản quản trị trên tất cả các thiết bị mạng trong đó bảo đảm yêu cầu về mật khẩu có độ phức tạp cần thiết, phòng chống dò quét mật khẩu	Đáp ứng. Tài khoản quản trị trên các thiết bị mạng lấy từ tài khoản dịch vụ quản lý người dùng (Active Directory) chung, đảm bảo độ phức tạp của mật khẩu, có thiết lập khóa tài khoản nếu đăng nhập sai mật khẩu 20 lần. Mật khẩu yêu cầu độ phức tạp (trên 10 ký tự; chứa 3 trong số 4 yếu tố sau: chữ hoa, chữ thường, số và ký tự đặc biệt; không chứa tên tài khoản trong mật khẩu).
1.12	Có phương án giới hạn các nguồn truy cập, quản trị các thiết bị mạng	Đáp ứng. Nguồn địa chỉ IP được truy cập, quản trị thiết bị mạng được giới hạn trong dải mạng dành riêng cho quản trị.
1.13	Có phương án chỉ cho phép quản trị các thiết bị mạng thông qua mạng Internet bằng mạng riêng ảo hoặc các phương pháp khác tương đương	Đáp ứng. Thông qua giải pháp mạng riêng ảo (xem Phần 1 - 4.1 - c - 3.9 và Phần 1 - 4.2 - c - 3.5).
1.14	Có ghi nhật ký đối với các hoạt động trên thiết bị mạng nội bộ và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian	Đáp ứng. Nhật ký (log) của các thiết bị mạng được thu thập thông qua hệ thống thu thập và phân tích log (xem Phần 1 - 4.1 - c - 3.4).
1.15	Có mã hóa thông tin xác thực lưu trên thiết bị mạng	Đáp ứng. Mật khẩu được cấu hình ở chế độ mã hóa trên các thiết bị.
1.16	Có cơ chế xác thực và mã hóa khi sử dụng mạng không dây	Đáp ứng. Mạng không dây tại 02 TTDL sử dụng cơ chế xác thực và mã hóa như sau:

		- Cơ chế xác thực WPA2, mã hóa AES cho mạng khách. - Cơ chế xác thực WPA2 Enterprise cho mạng người dùng, với tài khoản người dùng lấy từ hệ thống quản lý và xác thực người dùng của Bộ.
2	**An toàn máy chủ**	
2.1	Có phương án quản lý xác thực tập trung; chống đăng nhập tự động và tự động hủy phiên đăng nhập sau một khoảng thời gian chờ phù hợp với chính sách của tổ chức	Đáp ứng, cụ thể: - Các máy chủ sử dụng xác thực tập trung của hệ thống quản lý và xác thực người dùng. - Truy cập quản trị máy chủ theo giao thức RDP (đối với máy chủ Windows) và SSH (đối với máy chủ Linux); việc truy cập được giới hạn theo tài khoản truy cập, vùng mạng.
2.2	Có thiết lập quyền truy cập, quản trị, sử dụng tài nguyên của từng tài khoản trên hệ thống phù hợp với nhiệm vụ, yêu cầu nghiệp vụ khác nhau	Đáp ứng. Thực hiện việc phân quyền truy cập, sử dụng tài nguyên theo tài khoản dựa trên nhiệm vụ thực hiện.
2.3	Có phương án quản lý bản vá, nâng cấp phần mềm hệ thống tập trung	Đáp ứng. Phát hiện có bản vá được thực hiện bằng giải pháp giám sát tự động (dịch vụ giám sát mạng) và thủ công (kiểm tra định kỳ hằng ngày trên máy chủ, trên website hãng). - Việc theo dõi các bản nâng cấp phần mềm được thực hiện định kỳ.

		- Việc thực hiện nâng cấp phần mềm dựa trên phân tích nhu cầu thực tế, các rủi ro đi kèm.
2.4	Có phương án lưu trữ và quản lý tập trung nhật ký máy chủ. Nhật ký được lưu tối thiểu 03 tháng	Đáp ứng. Nhật ký máy chủ được phân loại, các nhật ký liên quan đến an ninh thông tin (ví dụ: đăng nhập) được thu thập bằng hệ thống thu thập và phân tích log; có khả năng lưu được 03 tháng.
2.5	Có phương án đồng bộ nhật ký máy chủ với hệ thống giám sát an toàn thông tin	Đáp ứng. Nhật ký máy chủ được đồng bộ với hệ thống thu thập và phân tích log.
2.6	Có phương án giới hạn các nguồn cho phép truy cập, quản trị máy chủ; việc quản trị máy chủ thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương	Đáp ứng. Truy cập tới máy chủ qua xác thực hệ thống quản lý và xác thực người dùng. Truy cập quản trị máy chủ theo giao thức RDP và SSH; việc truy cập được giới hạn theo tài khoản truy cập, vùng mạng. Truy cập từ Internet sử dụng dịch vụ mạng riêng ảo.
2.7	Có phương án sử dụng tường lửa trên từng máy chủ nhằm thiết lập chỉ cho phép các kết nối hợp pháp theo các dịch vụ được máy chủ cung cấp	Đáp ứng. Tường lửa trên từng máy chủ được sử dụng để hạn chế truy cập đến máy chủ theo các dịch vụ máy chủ cung cấp (ví dụ: dịch vụ RDP, SSH, mạng riêng ảo, quản lý và xác thực người dùng, ...).
2.8	Có phương án sao lưu dự phòng hệ điều hành máy chủ, cấu hình máy chủ phù hợp với yêu cầu của tổ chức	Đáp ứng. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu. Chính sách sao lưu dựa theo yêu cầu

		của người quản trị dịch vụ và phù hợp với quy định chung của tổ chức.
2.9	Có ghi nhật ký đối với các hoạt động truy cập, quản trị, phát sinh lỗi	Đáp ứng. Nhật ký truy cập, quản trị, phát sinh lỗi được gửi tới hệ thống thu thập và phân tích log.
2.10	Có sử dụng phần mềm phòng, chống mã độc trên máy chủ và có cơ chế tự động cập nhật phiên bản mới hoặc dấu hiệu nhận dạng mã độc mới cho phần mềm này	Đáp ứng. Cụ thể: - Các máy chủ được cài đặt phần mềm chống antivirus và được duy trì bản quyền, cập nhật thường xuyên.
2.11	Có cơ chế xác thực bằng mật khẩu bảo đảm độ phức tạp cần thiết, yêu cầu thay đổi mật khẩu định kỳ theo quy định của tổ chức và có cơ chế phòng chống dò quét mật khẩu; Các thông tin xác thực phải được lưu trữ trên hệ thống dưới dạng mã hóa	Đáp ứng. Cụ thể: - Các máy chủ được join vào hệ thống quản lý và xác thực người dùng. Độ phức tạp của mật khẩu được đảm bảo theo yêu cầu (trên 10 ký tự; chứa 3 trong số 4 yếu tố sau: chữ hoa, chữ thường, số và ký tự đặc biệt; không chứa tên tài khoản trong mật khẩu). Thông tin xác thực đều được mã hóa. - Việc phòng chống dò tìm mật khẩu và hạn chế IP truy cập quản trị máy chủ được thực hiện qua tính năng tường lửa của phần mềm antivirus cài đặt trên máy chủ và trên các thiết bị tường lửa giữa các phân vùng.

2.12	Có phương án vô hiệu hóa các tài khoản mặc định hoặc không hoạt động trên hệ thống; vô hiệu hóa các dịch vụ, phần mềm không sử dụng trên máy chủ	Đáp ứng. Cụ thể: - Trên máy chủ chỉ kích hoạt các tài khoản cần sử dụng. - Trên máy chủ chỉ cài đặt, kích hoạt các phần mềm, dịch vụ được phù hợp với mục đích sử dụng của máy chủ.
2.13	Có ghi nhật ký hệ thống đối với hoạt động truy cập, quản trị máy chủ	Đáp ứng. Nhật ký truy cập, quản trị máy chủ được kích hoạt trên máy chủ.
2.14	Có thiết lập cơ chế cập nhật bản vá điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ	Đáp ứng. Việc giám sát bản vá điểm yếu an toàn thông tin được thực hiện bằng giải pháp giám sát tự động và bằng phương pháp kiểm tra thủ công. Việc thực hiện nâng cấp phần mềm dựa trên phân tích nhu cầu thực tế, các rủi ro đi kèm.
3	**An toàn ứng dụng**	
3.1	Có thiết lập yêu cầu thay đổi mật khẩu định kỳ đối với tài khoản quản trị ứng dụng; giới hạn thời gian chờ để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Đáp ứng. Cụ thể: - Việc thiết lập thời gian đổi mật khẩu định kỳ đối với tài khoản quản trị ứng dụng được thực hiện trên hệ thống quản lý người dùng tập trung hoặc trên ứng dụng (nếu sử dụng tài khoản riêng của ứng dụng). - Việc thiết lập thời gian chờ để đóng phiên kết nối được thực hiện trên ứng dụng.

3.2	Có thiết lập tách biệt ứng dụng quản trị với ứng dụng cung cấp dịch vụ cho người sử dụng và bảo đảm ứng dụng hoạt động với quyền tối thiểu trên hệ thống	Đáp ứng. Các dịch vụ tách biệt giao diện quản trị và giao diện cung cấp dịch vụ người dùng. Ứng dụng được cấp quyền phù hợp và tối thiểu trên hệ thống.
3.3	Có phương án giới hạn các nguồn cho phép truy cập, quản trị ứng dụng; việc quản trị ứng dụng thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương	Đáp ứng. Cụ thể: - Giới hạn nguồn truy cập và quản trị ứng dụng (tài khoản, địa chỉ IP) thông qua cấu hình phân quyền của ứng dụng, cấu hình tường lửa trên máy chủ ứng dụng, tường lửa của hệ thống mạng. - Truy cập quản trị ứng dụng từ Internet qua dịch vụ mạng riêng ảo.
3.4	Có phương án kiểm tra, lọc các dữ liệu đầu vào từ phía người sử dụng, bảo đảm các dữ liệu này không ảnh hưởng đến an toàn thông tin của ứng dụng.	Đây là hệ thống thông tin cơ sở hạ tầng. Các dịch vụ cung cấp không tương tác với dữ liệu nhập từ người dùng.
3.5	Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp cần thiết để hạn chế tấn công dò quét mật khẩu; các thông tin xác thực phải được lưu trữ dưới dạng mã hóa	Đáp ứng. Cụ thể: - Mật khẩu được thiết lập đảm bảo độ phức tạp (trên 10 ký tự; chứa 3 trong số 4 yếu tố sau: chữ hoa, chữ thường, số và ký tự đặc biệt; không chứa tên tài khoản trong mật khẩu).

3.6	Có thiết lập yêu cầu ghi nhật ký truy cập, lỗi phát sinh	Đáp ứng. Ứng dụng được thiết lập lưu nhật ký truy cập, lỗi phát sinh.
3.7	Không sử dụng kết nối mạng không mã hóa trong việc quản trị ứng dụng từ xa	Đáp ứng. Kết nối quản trị ứng dụng qua môi trường mạng được mã hóa.
3.8	Có xác thực bằng cơ chế mật khẩu và ghi nhật ký đối với hoạt động truy cập ứng dụng và đăng nhập chức năng quản trị	Đáp ứng. Ứng dụng được thiết lập xác thực và ghi nhật ký đối với hoạt động truy cập ứng dụng, đăng nhập chức năng quản trị.
4	**An toàn dữ liệu**	
4.1	Có phương án mã hóa dữ liệu lưu trữ (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.	Các dịch vụ cung cấp của hệ thống cơ sở hạ tầng công nghệ thông tin không lưu trữ xử lý dữ liệu của người dùng.
4.2	Có phương án tự động sao lưu dự phòng đối với thông tin/dữ liệu phù hợp với tần suất thay đổi của dữ liệu	Đáp ứng. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu. Chính sách sao lưu dựa theo yêu cầu của người quản trị dịch vụ và phù hợp với quy định chung của tổ chức.
4.3	Có phương án sử dụng hệ thống hoặc phương tiện lưu trữ độc lập để sao lưu dự phòng các dữ liệu quan trọng trên máy chủ. Việc sao lưu được thực hiện định kỳ theo quy định của tổ chức	Đáp ứng. Dữ liệu quan trọng (chủ yếu là dữ liệu cấu hình của các ứng dụng) được sao lưu thông qua hệ thống sao lưu dữ liệu. Chính sách sao lưu dựa theo yêu cầu của người quản trị dịch vụ và phù hợp với quy định chung của tổ chức..

4.4	Có sao lưu dự phòng định kỳ dữ liệu trên hệ thống tùy theo yêu cầu, mục đích sử dụng	Đáp ứng. Dữ liệu (chủ yếu là dữ liệu cấu hình của các ứng dụng) được sao lưu thông qua hệ thống sao lưu dữ liệu. Chính sách sao lưu dựa theo yêu cầu của người quản trị dịch vụ và phù hợp với quy định chung của tổ chức..