ỦY BAN NHÂN DÂN XÃ LẠC PHƯỢNG

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 2
HỆ THỐNG THÔNG TIN ỦY BAN NHÂN DÂN XÃ LẠC PHƯỢNG

Thành phố Hải Phòng – 2026

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1	DMZ	Vùng phi quân sự (ra internet)
2	CNTT	Công nghệ thông tin
3	CSDL	Cơ sở dữ liệu
4	LAN	Mạng nội bộ
5	VPN	Vitural Private Network
6	TSLCD	Mạng Truyền số liệu chuyên dùng
8	DNS	Domain Name Server
9	THDL	Tích hợp dữ liệu
10	ATTT	An toàn thông tin
11	Nghị định số 85/2016/NĐ-CP	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.
12	Thông tư số 12/2022/TT-BTTTT	Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng 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 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

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: Ủy ban Nhân dân thành phố Hải Phòng

- **Quy định chức năng, nhiệm vụ và quyền hạn**: Luật số 72/2025/QH15 Tổ chức chính quyền địa phương đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XV, Kỳ họp thứ 9 thông qua ngày 16/6/2025

- **Người đại diện**: Ông Đỗ Thành Trung Chức vụ: Chủ tịch UBND thành phố

- **Địa chỉ**: Trung tâm Chính trị - Hành chính thành phố, phường Thủy Nguyên, thành phố Hải Phòng

- **Số điện thoại**: **0225.3821.055**

- Email: congthongtindientu@haiphong.gov.vn

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Uỷ ban nhân dân xã Lạc Phượng.

- **Người đại diện**: Vũ Duy Sỹ Chức vụ: Chủ tịch

- **Quy định chức năng, nhiệm vụ và quyền hạn**: Trên cơ sở Đề án số 381/ĐA-CP ngày 09 tháng 5 năm 2025 của Chính phủ về sắp xếp đơn vị hành chính cấp xã của thành phố Hải Phòng (mới) năm 2025.

- **Địa chỉ**: Thôn Hàm Hy, xã Lạc Phượng, thành phố Hải Phòng.

- **Số điện thoại**: 0912746803

- Email: xalacphuong@haiphong.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống:

Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô: Hệ thống thông tin UBND xã Lạc Phượng được thiết lập để phục vụ truy cập mạng cho cán bộ, công chức của Xã. Quy mô của hệ thống cung cấp dịch vụ cho hơn 100 người sử dụng.

- Đối tượng phục vụ hệ thống:

+ Dùng cho cán bộ, công chức và người lao động tại UBND và Trung tâm phục vụ Hành chính công xã Lạc Phượng.

+ Dùng cho tổ chức, cá nhân đến liên hệ công tác và thực hiện thủ tục hành chính tại Trung tâm phục vụ hành chính công xã.

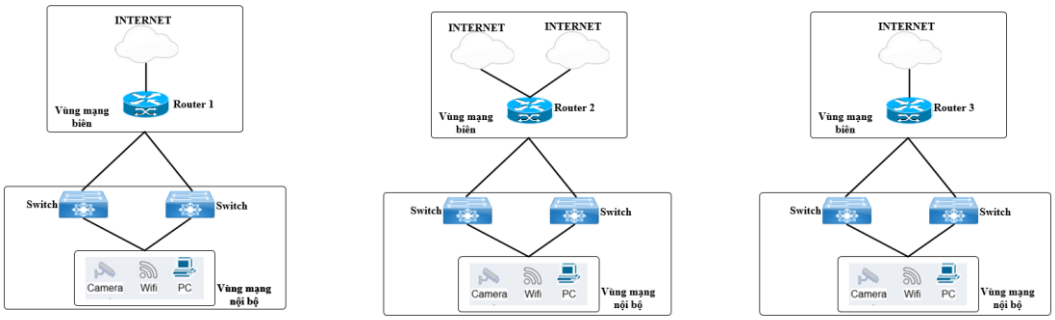
- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi hệ thống:

+ Hệ thống thông tin Trung tâm phục vụ hành chính công UBND xã Lạc Phượng.

+ Hệ thống thông tin UBND xã Lạc Phượng.

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể



Hình 1. Cấu trúc logic của hệ thống

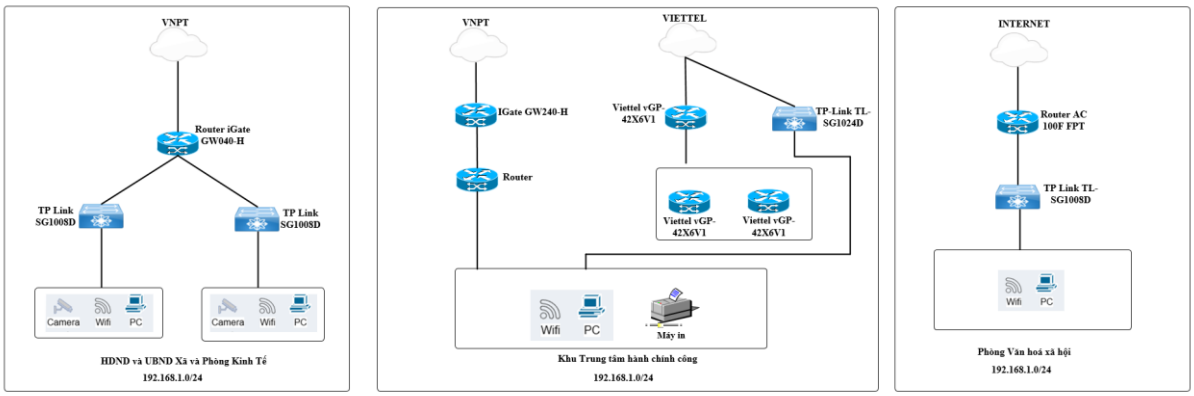
Hệ thống mạng nội bộ tại Trụ sở UBND xã Lạc Phượng do đơn vị trang bị thực hiện nhằm mục đích phục vụ công chức, viên chức, người lao động kết nối hệ thống mạng nội bộ.

Hệ thống hạ tầng mạng nội bộ trụ sở UBND xã Lạc Phượng được xây dựng theo các vùng mạng như sau:

- Vùng mạng biên: Kết nối hệ thống ra các mạng bên ngoài và mạng internet

- Vùng mạng nội bộ: Phục vụ kết nối tới người dùng.

4.2. Mô hình kết nối vật lý:



Hình 2. Kết nối vật lý của hệ thống

Hệ thống thông tin UBND xã Lạc Phượng hiện tại được triển khai hiện nay theo mô hình như sau:

- **Khu Văn phòng HĐND và UBND xã và Dãy nhà phòng Kinh tế:** hiện có 01 đường truyền Internet của VNPT thông qua modem iGate GW040-H. Khu vực này sử dụng 02 switch TP-Link TL-SG1008D để phân phối kết nối tới các thiết bị đầu cuối và điểm truy cập không dây.
- **Khu Trung tâm hành chính công và Hội trường:** Sử dụng 01 đường truyền VNPT thông qua modem iGate GW240-H tích hợp WiFi, 01 router VNPT được sử dụng như thiết bị phát WiFi khi đấu nối qua cổng LAN, 01 đường truyền Viettel phục vụ riêng cho hạ tầng WiFi, 03 thiết bị Mesh Viettel vGP-42X6V1 và 01 switch TP-Link TL-SG1024D (24 cổng). Thiết bị mạng được bố trí tập trung trong một tủ mạng nhỏ tại góc phòng. Hệ thống phục vụ trực tiếp cho 12 máy tính và 02 kiosk.
- **Khu phòng Văn hóa- Xã hội**: sử dụng các switch TP-Link TL-SG1008D, modem FPT kiêm WiFi và điểm phát WiFi hành lang để cung cấp truy cập cho các máy tính tại từng phòng.

4.3. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router iGate GW040-H	Vùng mạng biên	Thiết bị định tuyến và kết nối ra Internet
2	Router iGate GW240-H	Vùng mạng biên	Thiết bị định tuyến và kết nối ra Internet
3	AC1000F FPT	Vùng mạng biên	Thiết bị định tuyến và kết nối ra Internet
4	TP-Link TL-SG1024D	Vùng mạng nội bộ	Gom lưu lượng từ các thiết bị cuối (máy tính, điện thoại, AP) đồng thời cân bằng tải
5	Switch TL-SG1008D	Vùng mạng nội bộ	Gom lưu lượng từ các thiết bị cuối (máy tính, điện thoại, AP) đồng thời cân bằng tải
6	Mesh Viettel vGP-42X6V1	Vùng mạng nội bộ	Cung cấp kết nối không dây tới người dùng
7	Wifi/Tplink	Vùng mạng nội bộ	Cung cấp kết nối không dây tới người dùng

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

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng

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

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH	Mục đích sử dụng

Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

STT	Vùng mạng	IP Private	IP Public
1	Vùng mạng biên		IP động
2	Vùng mạng nội bộ	192.168.1.0/24	
3	Vùng mạng không giây		

Bảng 2. 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

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống thông tin Trung tâm phục vụ Hành chính công UBND xã Lạc Phượng	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP
2	Hệ thống thông tin mạng nội bộ UBND xã Lạc Phượng	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP

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

2.1. Hệ thống thông tin Trung tâm phục vụ Hành chính công UBND xã Lạc Phượng

Căn cứ phạm vi, quy mô và đối tượng phục vụ của hệ thống, Hệ thống thông tin Trung tâm phục vụ Hành chính công UBND xã Lạc Phượng phục vụ công tác truy cập mạng nội bộ, truy cập internet của cán bộ, công chức xã, đồng thời phục vụ kết nối internet công cộng cho tổ chức, cá nhân đến liên hệ công tác và giao dịch thủ tục hành chính. Do đó, theo quy định tại điểm Khoản 1 Điều 8 Nghị định số 85/2016/NĐ-CP, Hệ thống thông tin Trung tâm phục vụ Hành chính công UBND xã Gia Lộc là hệ thống phục vụ hoạt động nội bộ, chỉ xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước.

Vì vậy, căn cứ theo khoản 1 điều 8 Nghị định số 85/2016/NĐ-CP, đề xuất Hệ thống thông tin Trung tâm phục vụ Hành chính công UBND xã Lạc Phượng là **hệ thống thông tin cấp độ 2.**

2.2. Hệ thống thông tin mạng nội bộ UBND xã Lạc Phượng

Căn cứ phạm vi, quy mô và đối tượng phục vụ của hệ thống, Hệ thống thông tin mạng nội bộ UBND xã Lạc Phượng phục vụ công tác truy cập mạng nội bộ, truy cập internet của cán bộ, công chức xã, đồng thời phục vụ kết nối internet công cộng cho tổ chức, cá nhân đến liên hệ công tác và giao dịch thủ tục hành chính. Do đó, theo quy định tại điểm Khoản 1 Điều 8 Nghị định số 85/2016/NĐ-CP, Hệ thống thông tin mạng nội bộ UBND xã Lạc Phượng là hệ thống phục vụ hoạt động nội bộ, chỉ xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước.

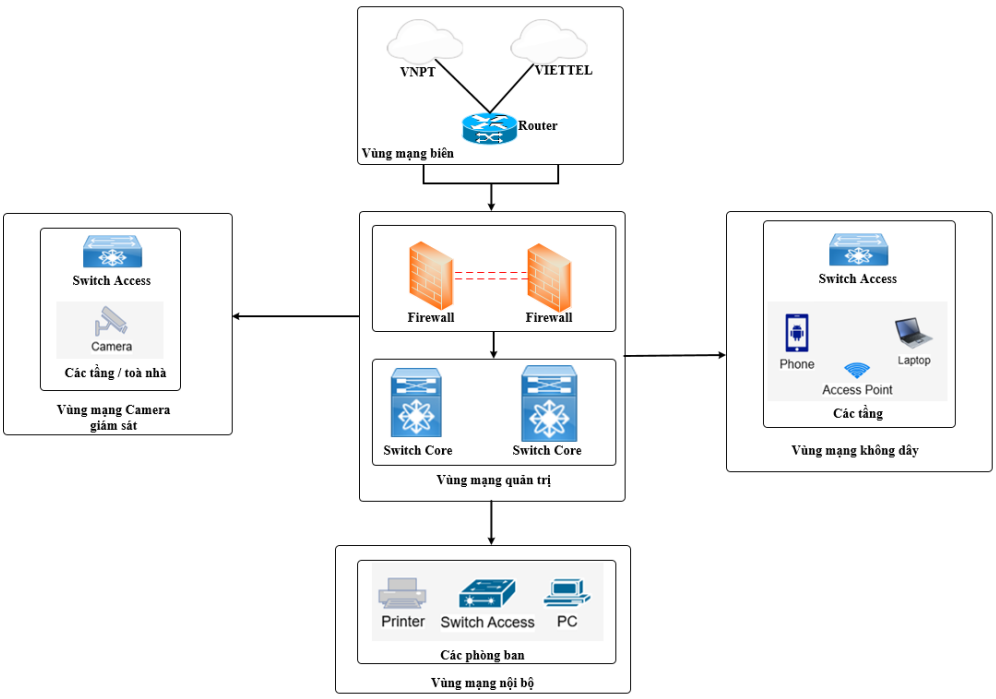
Vì vậy, căn cứ theo khoản 1 điều 8 Nghị định số 85/2016/NĐ-CP, đề xuất Hệ thống thông tin mạng nội bộ UBND xã Lạc Phượng là **hệ thống thông tin cấp độ 2.**

Kết luận:

Dựa trên việc đề xuất cấp độ cho từng hệ thống thành phần như trên, Căn cứ theo Khoản 2 Điều 5 Nghị định 85/2016/NĐ-CP, cấp độ hệ thống thông tin được xác định là cấp độ cao nhất trong các cấp độ của các hệ thống thành phần cấu thành. Vì vậy, đề xuất Hệ thống thông tin của Ủy ban nhân dân xã Lạc Phượng là **hệ thống thông tin cấp độ 2**.

3. Đề xuất mô hình hệ thống để đáp ứng cấp độ

3.1. Mô hình logic đề xuất để đáp ứng cấp độ



Hình 4. Mô hình logic đề xuất Hệ thống thông tin

Hệ thống thông tin UBND xã Lạc Phượng sẽ được quy hoạch thành một hệ thống mạng duy nhất.

Hệ thống được thiết kế thành các vùng mạng như sau:

- **Vùng mạng biên:** Kết nối hệ thống với mạng Internet và mạng diện rộng
- **Vùng mạng nội bộ:** Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống. Vùng mạng

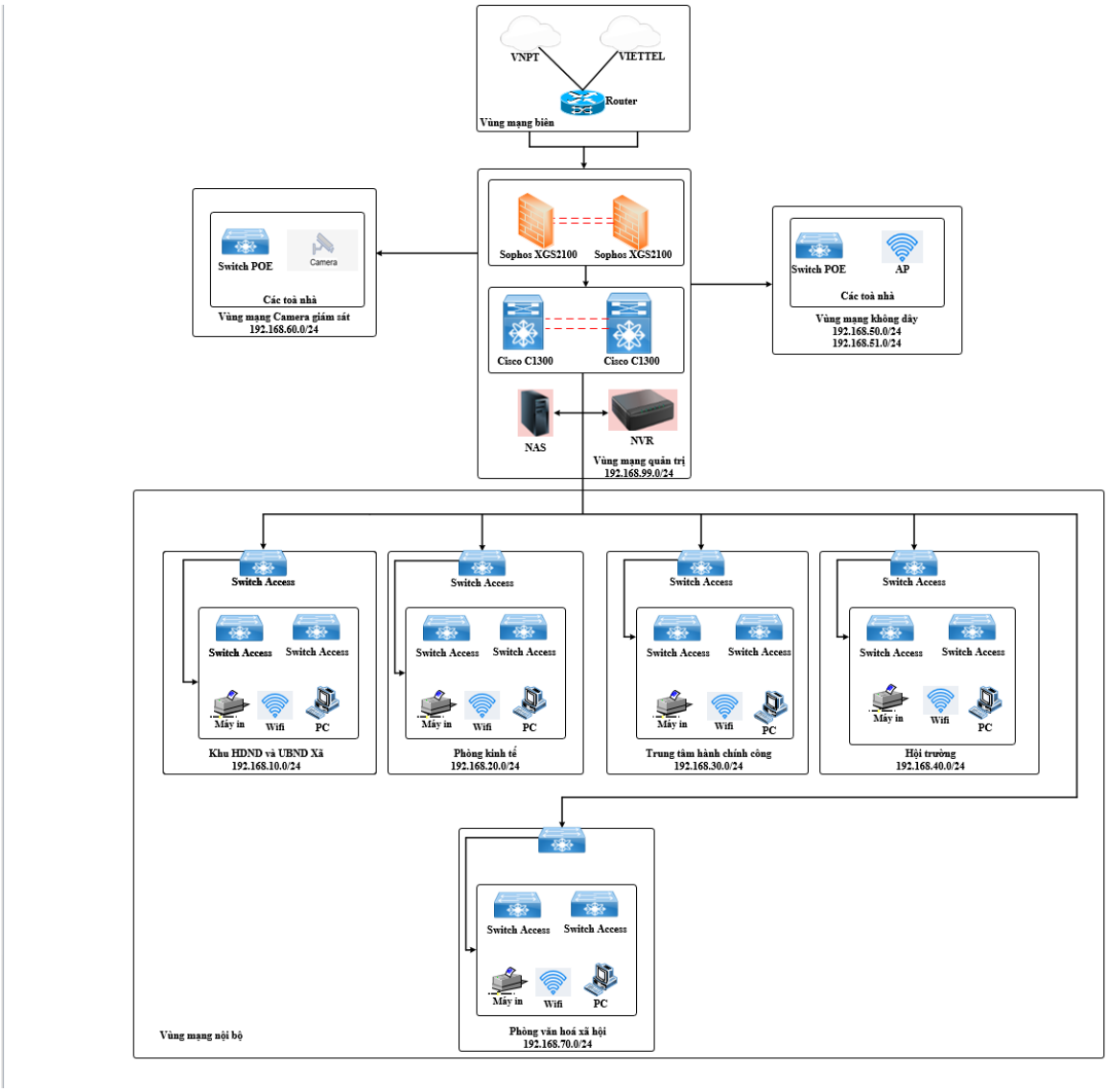
này hiện cũng đang cung cấp mạng không dây cho người dân tới làm việc tại trụ sở.

- **Vùng mạng không dây:** Vùng mạng cung cấp kết nối wifi cho người sử dụng. Tách biệt kết nối cho người dân (khách) sử dụng và cán bộ công chức sử dụng.

- **Vùng mạng Camera giám sát**: là vùng mạng riêng cho hệ thống camera giám sát, được cô lập với các vùng mạng khác nhằm đảm bảo an toàn và kiểm soát truy cập.

- **Vùng mạng quản trị:** Là vùng mạng trung tâm dùng để quản lý, giám sát và cấu hình các thiết bị mạng, thiết bị bảo mật đồng thời kiểm soát kết nối giữa các vùng mạng trong hệ thống.

3.2. Mô hình vật lý đề xuất để đáp ứng cấp độ



Hình 5. Mô hình vật lý đề xuất Hệ thống thông tin

Mô hình mạng đề xuất sử dụng 02 đường truyền Internet từ nhà cung cấp dịch vụ, kết nối tại vùng mạng biên thông qua các thiết bị modem quang của nhà mạng. Lưu lượng Internet được chuyển tiếp về hệ thống tường lửa gồm 02 thiết bị Sophos XGS210 triển khai theo cơ chế dự phòng (HA), thực hiện kiểm soát truy cập, bảo mật và định tuyến giữa mạng nội bộ và mạng bên ngoài.

Tại lớp mạng lõi, hệ thống sử dụng 02 switch Cisco Catalyst C1300 kết nối dự phòng, đóng vai trò tập trung và phân phối lưu lượng đến các vùng mạng trong hệ thống. Các switch truy cập được triển khai tại từng tòa nhà làm việc để kết nối máy tính người dùng và thiết bị mạng nội bộ.

Hệ thống được phân tách thành các vùng mạng độc lập nhằm đảm bảo an toàn và tối ưu vận hành, bao gồm: mạng nội bộ phục vụ công việc chuyên môn tại các phòng ban, mạng không dây dành cho cán bộ (192.168.50.0/24), mạng không dây dành cho khách (192.168.51.0/24), mạng camera giám sát (192.168.60.0/24) và mạng quản trị (192.168.99.0/24) để quản lý cấu hình chính sách cho các thiết bị mạng và thiết bị bảo mật trong hệ thống. Việc truy cập giữa các vùng mạng được kiểm soát tập trung thông qua hệ thống tường lửa, đảm bảo an toàn thông tin và quản lý truy cập theo chính sách.

Các thiết bị mạng chính được bố trí phương án dự phòng thay thế. Mô hình đáp ứng yêu cầu phân vùng mạng và duy trì khả năng hoạt động liên tục của hệ thống.

Toàn bộ máy tính trong hệ thống được cài đặt Bkav hoặc Kaspersky để ngăn chặn malware, ransomware và các cuộc tấn công mạng tại điểm cuối.

Trang bị thiết bị NAS chuyên dụng để lưu trữ các thông tin quan trọng. Việc này giúp quản lý dữ liệu tập trung, hỗ trợ phân quyền truy cập và thuận tiện cho công tác sao lưu (backup).

Sử dụng công nghệ VPN thiết lập trực tiếp trên tường lửa. Cho phép cán bộ truy cập vào mạng nội bộ từ xa một cách an toàn, dữ liệu được mã hóa để tránh bị đánh cắp trên môi trường Internet. Tất cả các thiết bị mạng được đặt trong tủ rack được khóa bảo vệ và dán niêm phong trong phòng máy chủ.

3.3. Bảng đề xuất thiết bị để đáp ứng cấp độ

STT	Tên thiết bị	Số lượng	Đơn vị tính	Chức năng

1	Firewall Sophos XGS210	02	Thiết bị	Thiết bị tường lửa trung tâm, thực hiện chức năng định tuyến, NAT, VPN, kiểm soát truy cập, phát hiện và ngăn chặn xâm nhập; triển khai chế độ HA đảm bảo dự phòng hệ thống
2	License firewall Sophos XGS210	02	License	Bản quyền kích hoạt các tính năng bảo mật nâng cao của tường lửa: IPS, Antivirus, Web filtering, Application control, cập nhật signatures …
3	Switch Core Catalyst C1300	02	Thiết bị	Switch lõi mạng nội bộ, hỗ trợ VLAN, trunk, phân chia vùng mạng nội bộ, wifi, camera; kết nối dự phòng song song đảm bảo tính sẵn sàng hệ thống
4	Switch Access (24/48 port)	Tùy thực tế	Thiết bị	Kết nối các thiết bị đầu cuối tại các phòng ban/toà nhà, uplink về switch core, cấu hình access VLAN theo từng vùng mạng
5	Switch PoE cấp nguồn camera/wifi	Tùy thực tế	Thiết bị	Cấp nguồn PoE cho camera IP và thiết bị phát wifi, đồng thời truyền dữ liệu về hệ thống mạng nội bộ
6	Bộ phát Wifi/Access Point	Tùy thực tế	Thiết bị	Cung cấp mạng không dây cho cán bộ và khách; cấu hình SSID tách biệt và ánh xạ VLAN tương ứng
7	Phần mềm diệt virus Bkav hoặc Kaspersky	64	Phần mềm	Cài đặt cho các máy tính cán bộ

Bảng 5. Danh mục thiết bị đề xuất trong hệ thống

3.4. Bảng quy hoạch địa chỉ IP

STT	Vùng mạng	IP	Mô tả	Ghi chú
1	Vùng mạng biên	//	Kết nối hệ thống với mạng Internet và mạng diện rộng	Sử dụng IP động
2	Vùng mạng nội bộ	192.168.10.0/24 192.168.20.0/24 192.168.30.0/24 192.168.40.0/24 192.168.70.0/24	Sử dụng để kết nối có dây tới các thiết bị tại các tòa nhà của trụ sở	Không giới hạn băng thông
3	Vùng mạng không dây (dành cho cán bộ)	192.168.50.0/24	Sử dụng để các cán bộ công chức tại trụ sở sử dụng	Không giới hạn băng thông
4	Vùng mạng không dây (dành cho khách)	192.168.51.0/24	Sử dụng để công dân tới sử dụng	Giới hạn băng thông. Chặn kết nối tới tất cả các vùng mạng còn lại
5	Vùng mạng Camera giám sát	192.168.60.0/24	Sử dụng để thiết lập cho các thiết bị Camera giám sát	Không giới hạn băng thông
6	Vùng mạng quản trị	192.168.99.0/24	Sử dụng để thiết lập cho các thiết bị mạng, thiết bị quản trị	Không giới hạn băng thông Chỉ cho phép truy cập từ các máy quản trị được phân quyền

				Chặn truy cập từ các vùng mạng người dùng và mạng khách

Bảng 6. Quy hoạch địa chỉ IP đề xuất cho các vùng mạng trong hệ thống

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

I. 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 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 vòng 06 tháng, kể từ khi HSĐXCĐ được phê duyệt.

II. 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. 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. An toàn ứng dụng và mã nguồn

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

4.2. 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 vòng 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống ... sẽ bao gồm các thuyết minh thành phần sau:

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

PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 2

6.1.1. Thiết lập chính sách an toàn thông tin

6.1.1.1. Chính sách an toàn thông tin

Yêu cầu	Xây dựng chính sách an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	Việc quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác được thực hiện trên cơ sở QĐ số 60/QĐ-UBND về quản lý vận hành hệ thống trung tâm dữ liệu tính. Triển khai với mạng Lan như sau: - Áp dụng Khoản 1, 2, 3 **Điều 11 về Quản lý an toàn mạng** quyết định số 60/QĐ-UBND: 1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. 2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. 3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

6.1.1.2. Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng. Tham chiếu Điều 31. Tổ chức thực hiện
Phương án	Áp dụng khoản 3 Điều 31. Tổ chức thực hiện 3. Định kỳ 02 năm hoặc khi có thay đổi về chính sách ATTT, Phòng Văn hóa - xã hội kiểm tra tính phù hợp của Quy chế này

	và thực hiện rà soát, cập nhật bổ sung đảm bảo đúng với quy định của pháp luật.

6.1.1.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng. Tham chiếu Điều 31. Tổ chức thực hiện
Phương án	3. Định kỳ 02 năm hoặc khi có thay đổi về chính sách ATTT, Phòng Văn hóa - xã hội kiểm tra tính phù hợp của Quy chế này và thực hiện rà soát, cập nhật bổ sung đảm bảo đúng với quy định của pháp luật.

6.1.2. Tổ chức bảo đảm an toàn thông tin

6.1.2.1. 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. Tham chiếu Điều 5. Phối hợp với những cơ quan/ tổ chức có thẩm quyền
Phương án	Áp dụng Khoản 1, Điều 5 Phối hợp với những cơ quan/ tổ chức có thẩm quyền 1. Phân công bộ phận chuyên trách về an toàn thông tin UBND xã giao bộ phận chuyên trách về công nghệ thông tin của UBND thuộc Phòng Văn hóa - xã hội là bộ phận chuyên trách về an toàn thông tin.

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

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

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
Hiện trạng	Đáp ứng. Tham chiếu Điều 5. Phối hợp với những cơ quan/ tổ chức có thẩm quyền

Phương án	Áp dụng Khoản 2, Điều 5. Phối hợp với những cơ quan/ tổ chức có thẩm quyền a) Là đầu mối liên hệ, tiếp nhận, phối hợp với các cơ quan, tổ chức (có thẩm quyền quản lý về an toàn thông tin) trong công tác đảm bảo an toàn thông tin, hỗ trợ điều phối xử lý sự cố an toàn thông tin b) Là đầu mối liên hệ, phối hợp với Sở Khoa học và công nghệ và các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho các Hệ thống thông tin do UBND xã triển khai. c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền. d) Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ UBND. đ) Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả e) Phối hợp chặt chẽ với Công an thành phố, Sở Khoa học và công nghệ và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng. g) Định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Khoa học và công nghệ (theo hướng dẫn của Sở Khoa học và công nghệ).

6.1.2.2.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

Yêu cầu	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. Tham chiếu Điều 5. Phối hợp với những cơ quan/ tổ chức có thẩm quyền
Phương án	Áp dụng mục e, g Khoản 2, Điều 5. Phối hợp với những cơ quan/ tổ chức có thẩm quyền e) Phối hợp chặt chẽ với Công an thành phố, Sở Khoa học và

	công nghệ và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng. g) Định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Khoa học và công nghệ (theo hướng dẫn của Sở Khoa học và công nghệ).

6.1.2.2.c. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền

Yêu cầu	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
Phương án	Áp dụng mục c Khoản 2, Điều 5. Phối hợp với những cơ quan/ tổ chức có thẩm quyền c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

6.1.3. Bảo đảm nguồn nhân lực

6.1.3.1. Tuyển dụng

Yêu cầu	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ
Hiện trạng	Đáp ứng. Tham chiếu Điều 6. Bảo đảm nguồn nhân lực
Phương án	Theo quy định khoản 1 tại Điều 6. Bảo đảm nguồn nhân lực: 1. Tuyển dụng a. Cán bộ được tuyển dụng vào vị trí việc 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; b. Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ c. Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng. 2. Trong quá trình làm việc 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. 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. c) Có kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: Cán bộ kỹ thuật, cán bộ quản lý và người sử dụng hệ thống.

6.1.3.2. Trong quá trình làm việc

6.1.3.2.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

Yêu cầu	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. Tham chiếu Điều 6. Bảo đảm nguồn nhân lực
Phương án	Theo quy định mục a khoản 2 tại Điều 6. Bảo đảm nguồn nhân lực: 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.

6.1.3.2.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

Yêu cầu	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. Tham chiếu Điều 6. Bảo đảm nguồn nhân lực
Phương án	Theo quy định mục b khoản 2 tại Điều 6. Bảo đảm nguồn nhân lực: 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.

6.1.3.3. Chấm dứt hoặc thay đổi công việc

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.

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc
Hiện trạng	Đáp ứng. Tham chiếu Điều 6. Bảo đảm nguồn nhân lực
Phương án	Áp dụng muc a Khoản 3 Điều 6. Bảo đảm nguồn nhân lực 3. Chấm dứt thay đổi công việc 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 UBND hữu của tổ chức;

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.

Yêu cầu	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. Tham chiếu Điều 6. Bảo đảm nguồn nhân lực
Phương án	Áp dụng mục b, c Khoản 3 Điều 6. Bảo đảm nguồn nhân lực 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;

	c. Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc

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

6.1.4.1. Thiết kế an toàn hệ thống thông tin

6.1.4.1.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

Yêu cầu	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. Tham chiếu Điều 7. Thiết kế an toàn hệ thống thông tin
Phương án	Áp dụng khoản 1 Điều 7. Thiết kế an toàn hệ thống thông tin 1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

6.1.4.1.b. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin

Yêu cầu	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin
Hiện trạng	Đáp ứng. Tham chiếu Điều 7. Thiết kế an toàn hệ thống thông tin
Phương án	Áp dụng khoản 2 Điều 7. Thiết kế an toàn hệ thống thông tin 2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

6.1.4.1.c. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ

Yêu cầu	Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ
Hiện trạng	Đáp ứng. Tham chiếu Điều 7. Thiết kế an toàn hệ thống thông tin
Phương án	Áp dụng khoản 3 Điều 7. Thiết kế an toàn hệ thống thông tin 3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

6.1.4.1.d. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin

Yêu cầu	Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng. Tham chiếu Điều 7. Thiết kế an toàn hệ thống thông tin
Phương án	Áp dụng khoản 4 Điều 7. Thiết kế an toàn hệ thống thông tin 4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

6.1.4.1.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

Yêu cầu	Có quy định 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. Tham chiếu Điều 7. Thiết kế an toàn hệ thống thông tin
Phương án	Áp dụng khoản 5 Điều 7. Thiết kế an toàn hệ thống thông tin 5. 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.

6.1.4.2. Phát triển phần mềm thuê khoán

6.1.4.2.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

Yêu cầu	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. Tham chiếu Điều 9. Phát triển phần mềm thuê khoán
Phương án	Áp dụng khoản 1 Điều 9. Phát triển phần mềm thuê khoán 1. 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.

6.1.4.2.b. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

Yêu cầu	Có quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

Hiện trạng	Đáp ứng. Tham chiếu Điều 9. Phát triển phần mềm thuê khoán
Phương án	Áp dụng khoản 2 Điều 9. Phát triển phần mềm thuê khoán 2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

6.1.4.3. Thử nghiệm và nghiệm thu hệ thống

6.1.4.3.a. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng

Yêu cầu	Có quy định về việc thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng
Hiện trạng	Đáp ứng. Tham chiếu Điều 9. Phát triển phần mềm thuê khoán
Phương án	Áp dụng khoản 3 Điều 9. Phát triển phần mềm thuê khoán 3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng

6.1.4.3.b. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có yêu cầu về nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng. Tham chiếu Điều 10. Thử nghiệm và Nghiệm thu hệ thống
Phương án	Áp dụng khoản 1, 2 Điều 10. Thử nghiệm và Nghiệm thu hệ thống 1. Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng. 2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống

6.1.4.3.c. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng. Tham chiếu Điều 10. Thử nghiệm và Nghiệm thu hệ thống

Phương án	Áp dụng khoản 3 Điều 10. Thử nghiệm và Nghiệm thu hệ thống 3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

6.1.5. Quản lý vận hành hệ thống thông tin

6.1.5.1. Quản lý an toàn mạng

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn mạng. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

6.1.5.1.a. Quản lý, vận hành hoạt động bình thường của hệ thống

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống
Hiện trạng	Đáp ứng. Tham chiếu Điều 11. Quản lý an toàn mạng
Phương án	Áp dụng khoản 4 Điều 11. Quản lý an toàn mạng a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có. c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm nhà cung cấp. đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn. g) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng. h) Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng i) Triển khai phương án cảnh báo thời gian thực trực tiếp đến

	người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng k) Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

6.1.5.1.b. Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố
Hiện trạng	Đáp ứng. Tham chiếu Điều 11. Quản lý an toàn mạng
Phương án	- Áp dụng muc a, b, c khoản 5 Điều 11. Quản lý an toàn mạng 5) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: a) 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. b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống. c) Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

6.1.5.1.c. Truy cập và quản lý cấu hình hệ thống

Yêu cầu	Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng. Tham chiếu Điều 11. Quản lý an toàn mạng
Phương án	- Áp dụng khoản 6 Điều 11. Quản lý an toàn mạng 6. Truy cập và quản lý cấu hình hệ thống:

	a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài. b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm. c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác. d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

6.1.5.2. Quản lý an toàn máy chủ và ứng dụng

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn máy chủ và ứng dụng. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

6.1.5.2.a. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ
Hiện trạng	Đáp ứng. Tham chiếu Điều 12. Quản lý an toàn máy chủ và ứng dụng
Phương án	Áp dụng khoản 2 Điều 12. Quản lý an toàn máy chủ và ứng dụng 2) Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

	a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có. c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp. đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

6.1.5.2.b. Truy cập mạng của máy chủ

Yêu cầu	Có quy định quản lý truy cập mạng của máy chủ.
Hiện trạng	Đáp ứng. Tham chiếu Điều 12. Quản lý an toàn máy chủ và ứng dụng
Phương án	Áp dụng khoản 3 Điều 12. Quản lý an toàn máy chủ và ứng dụng 3. Truy cập mạng của máy chủ: Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

6.1.5.2.c. Truy cập và quản trị máy chủ và ứng dụng

Yêu cầu	Có quy định quản lý truy cập và quản trị máy chủ và ứng dụng
Hiện trạng	Đáp ứng. Tham chiếu Điều 12. Quản lý an toàn máy chủ và ứng dụng
Phương án	Áp dụng khoản 4 Điều 12. Quản lý an toàn máy chủ và ứng dụng 4) Truy cập và quản trị máy chủ và ứng dụng:

	a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng. b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành. c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet. d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ. đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống. e) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng. g) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

6.1.5.2.d. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

Yêu cầu	Có quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
Hiện trạng	Đáp ứng. Tham chiếu Điều 12. Quản lý an toàn máy chủ và ứng dụng
Phương án	Áp dụng khoản 5 Điều 12. Quản lý an toàn máy chủ và ứng dụng 5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: a. 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. b. Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống. c. Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng. d. Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

6.1.5.3. Quản lý an toàn dữ liệu

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn dữ liệu. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

6.1.5.3.a. Chính sách, quy trình dự phòng và khôi phục dữ liệu

Yêu cầu	Có chính sách, quy trình dự phòng và khôi phục dữ liệu
Hiện trạng	Đáp ứng. Tham chiếu Điều 16 Quản lý an toàn dữ liệu
Phương án	- Áp dụng khoản 7 Điều 16 Quản lý an toàn dữ liệu: 7. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

6.1.5.3.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

Yêu cầu	Có quy định 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. Tham chiếu Điều 16 Quản lý an toàn dữ liệu
Phương án	- Áp dụng khoản 8 Điều 16 Quản lý an toàn dữ liệu: 8. 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 và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

6.1.5.4. Quản lý sự cố an toàn thông tin

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý sự cố an toàn thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

6.1.5.4.a. Phân nhóm sự cố an toàn thông tin mạng

Yêu cầu	Có quy định về phân nhóm sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng. Tham chiếu Điều 18. Quản lý sự cố an toàn thông tin.
Phương án	Áp dụng Khoản 1 Điều 18. Quản lý sự cố an toàn thông tin 1. Phân nhóm sự cố an toàn thông tin, bao gồm: a. Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị như: máy tính trạm bị nhiễm phần mềm độc hại, phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi. b. Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 (một) phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban. c. Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như: hệ thống quản lý văn bản và điều hành, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch

	trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng. d. Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung ...

6.1.5.4.b. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

Yêu cầu	Có phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng. Tham chiếu Điều 18. Quản lý sự cố an toàn thông tin
Phương án	Áp dụng Khoản 2 Điều 18. Quản lý sự cố an toàn thông tin 2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau: a. Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Khoa học và công nghệ quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu thành phố) thì thực hiện tiếp Bước 3. b. Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3. c. Bước 3: Báo sự cố đến Sở Khoa học và công nghệ theo mẫu tại Phụ lục 1 kèm Quy chế và thực hiện tiếp Bước 4.

	d. Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Khoa học và công nghệ và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5. đ. Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu tại Phụ lục 2 kèm Quy chế, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Khoa học và công nghệ. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Khoa học và công nghệ để được hướng dẫn, hỗ trợ.

6.1.5.4.c. Kế hoạch ứng phó sự cố an toàn thông tin mạng

Yêu cầu	Xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng. Tham chiếu Điều 18. Quản lý sự cố an toàn thông tin
Phương án	Áp dụng Khoản 3 Điều 18. Quản lý sự cố an toàn thông tin 3. Bộ phận chuyên trách về an toàn thông tin có trách nhiệm: a. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia (Quyết định số 05); xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng. b. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg. c. Phối hợp với các đơn vị chức năng xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg. d. Có phương án và điều động nhân lực có kinh nghiệm thực

	hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống. e. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg. f. 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; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống. g. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo. h. 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; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

6.1.5.4.d. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý giám sát, phát hiện và cảnh báo sự cố an toàn thông tin
Hiện trạng	Đáp ứng. Điều 18. Quản lý sự cố an toàn thông tin
Phương án	Áp dụng mục d Khoản 3 Điều 18. Quản lý sự cố an toàn thông tin d. Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối

	hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống

6.1.5.4.đ. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng thông thường
Hiện trạng	Đáp ứng. Điều 18. Quản lý sự cố an toàn thông tin
Phương án	Áp dụng mục b, c Khoản 3 Điều 18. Quản lý sự cố an toàn thông tin b. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg. c. Phối hợp với các đơn vị chức năng xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

6.1.5.4.e. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng
Hiện trạng	Đáp ứng. Điều 18. Quản lý sự cố an toàn thông tin
Phương án	Áp dụng mục e Khoản 3 Điều 18. Quản lý sự cố an toàn thông tin e. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

6.1.5.4.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

Yêu cầu	Có quy định về 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. Điều 18. Quản lý sự cố an toàn thông tin
Phương án	Áp dụng mục f, g, h Khoản 3 Điều 18. Quản lý sự cố an toàn thông tin

	f. 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; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống. g. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo. h. 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; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

6.1.5.5. Quản lý an toàn người sử dụng đầu cuối

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn người sử dụng đầu cuối. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

6.1.5.5.a. Quản lý truy cập, sử dụng tài nguyên nội bộ

Yêu cầu	Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ
Hiện trạng	Đáp ứng. Tham chiếu Điều 17. Quản lý an toàn người sử dụng đầu cuối
Phương án	Áp dụng khoản 7 Điều 17. Quản lý an toàn người sử dụng đầu cuối 7. Quản lý truy cập, sử dụng tài nguyên nội bộ a. Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

	b. Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin. c. Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trýớc khi kết nối vào hệ thống. Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống

6.1.5.5.b. Quản lý truy cập mạng và tài nguyên trên Internet

Yêu cầu	Có quy định về quản lý truy cập mạng và tài nguyên trên Internet
Hiện trạng	Đáp ứng. Tham chiếu Điều 17. Quản lý an toàn người sử dụng đầu cuối
Phương án	Áp dụng khoản 8 Điều 17. Quản lý an toàn người sử dụng đầu cuối 8. Quản lý truy cập mạng và tài nguyên trên Internet: a. Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; b. Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; c. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; d. Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

6.1.5.6. Phương án Quản lý rủi ro an toàn thông tin

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình Quản lý rủi ro an toàn thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

Yêu cầu	Có chính sách, quy trình quản lý quản lý rủi ro an toàn thông tin
Hiện trạng	Đáp ứng. Tham chiếu Điều 21 Quản lý rủi ro an toàn thông tin
Phương án	Áp dụng Điều 21 Quản lý rủi ro an toàn thông tin 1. Xác định tài sản: a) Lập danh mục thiết bị, máy chủ, phần mềm, dịch vụ, ứng dụng thuộc hệ thống. b) Kịp thời cập nhật danh mục, nội dung hồ sơ đề xuất cấp độ an toàn thong tin của hệ thống khi có thay đổi. 2. Đánh giá rủi ro: a) Xác định rủi ro: Định kỳ hàng tháng, Phòng Văn hóa - xã hội tiến hành rà soát, xác định các mối đe dọa, điểm yếu, lỗ hổng bảo mật có thể ảnh hưởng, gây mất an toàn thông tin (ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn sàng) đối với các thành phần của hệ thống theo danh mục tài sản đã được xác định hoặc các yêu cầu về chính sách về quản lý, kỹ thuật được khuyến nghị thực hiện để bảo đảm an toàn thông tin nhưng chưa thể thực hiện được. b) Phân tích tác động của rủi ro: Làm rõ mức độ tác động, ảnh hưởng của từng rủi ro được xác định và đề xuất phương án xử lý. c) Phân loại rủi ro theo mức độ ảnh hưởng: - Mức thấp: Rủi ro mất an toàn thông tin có thể xử lý thông qua cập nhật miễn phí bản vá của hệ điều hành, phần mềm, ứng dụng, dịch vụ. - Mức cao: Rủi ro mất an toàn thông tin không thể xử lý thông qua cập nhật hoặc phải trả phí để được cập nhật bản vá của hệ điều hành, phần mềm, ứng dụng, dịch vụ. 3. Xử lý rủi ro: a) Phòng Văn hóa - xã hội chủ động, kịp thời xử lý các rủi ro ở mức độ thấp. b) Báo cáo Lãnh đạo đơn vị quyết định phương án xử lý đối với

	các rủi ro ở mức cao. 4. Chấp nhận rủi ro: Việc xử lý sớm toàn bộ các rủi ro là khó khả thi. Đối với các rủi ro ở mức thấp hoặc rủi ro ở mức cao được phát hiện nhưng được đánh giá không làm tổn hại đến hoạt động bình thường của hệ thống hoặc đã có các biện pháp khác hạn chế rủi ro thì có thể chấp nhận sự tồn tại của rủi ro trên hệ thống. Tuy nhiên, cần từng bước có biện pháp xử lý triệt để các rủi ro. 5. Trường hợp sự cố mất an toàn thông tin xảy ra: a) Phòng Văn hóa - xã hội chủ động thực hiện các biện pháp nghiệp vụ cần thiết để kịp thời xử lý. b) Trong trường hợp sự cố mất an toàn thông tin vượt quá khả năng xử lý, Phòng Văn hóa - xã hội kịp thời báo cáo Lãnh đạo đơn vị để xử lý.

6.1.5.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

Yêu cầu	Có quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ
Hiện trạng	Đáp ứng. Tham chiếu Điều 22 Kết thúc vận hành, khai thác, thanh lý, hủy bỏ
Phương án	Áp dụng Điều 22. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ 1. Trường hợp hệ thống phải kết thúc vận hành, khai thác, thanh lý, hủy bỏ, Phòng Văn hóa - xã hội tham mưu Lãnh đạo đơn vị báo cáo UBND thành phố phương án thực hiện, trong đó làm rõ: a) Lý do kết thúc vận hành, khai thác, thanh lý, hủy bỏ và phương án thay thế (nếu có). b) Phương án xử lý xóa bỏ các thông tin, dữ liệu: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối, phương tiện lưu trữ chứa thông tin, dữ liệu cần xóa. Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung cần đề xuất xử lý, các thư mục

	chứa dữ liệu sao lưu cần xóa dữ liệu …, phương thức xóa bỏ thông tin, dữ liệu, bảo đảm thông tin, dữ liệu được xóa hoàn toàn, không thể khôi phục trên các máy chủ, thiết bị, phương tiện lưu trữ. c) Phương án gỡ bỏ các phần mềm, ứng dụng hoặc dịch vụ có liên quan: Liệt kê đầy đủ danh mục máy chủ, thiết bị mạng, thiết bị đầu cuối có cài đặt phần mềm, ứng dụng hoặc dịch vụ có liên quan đến hệ thống cần thực hiện gỡ bỏ. Ứng với mỗi máy chủ, thiết bị cần làm rõ các nội dung đề xuất xử lý, phương thức xử lý bảo đảm phần mềm, ứng dụng, dịch vụ được xóa hoàn toàn, không thể phục hồi trên các máy chủ, thiết bị mạng, thiết bị đầu cuối có liên quan. d) Danh mục các máy chủ, thiết bị mạng, thiết bị đầu cuối, thiết bị lưu trữ cần thanh lý (nếu có), làm rõ phương án thanh lý. Các máy chủ, thiết bị mang, thiết bị đầu cuối, thiết bị lưu trữ cần được xử lý xóa bỏ thông tin, dữ liệu, gỡ bỏ phần mềm, ứng dụng, dịch vụ trước khi tiến hành thanh lý. 2. Trình tự, thủ tục thực hiện: Sau khi được sự đồng ý bằng văn bản của UBND thành phố Hải Phòng, Phòng Văn hóa - xã hội tham mưu Lãnh đạo đơn vị thực hiện thanh lý, hủy bỏ hệ thống theo đúng các quy định tại Điều 29, Điều 30 Nghị định số 151/2017/NĐ-CP ngày 26/12/2017 của Chính phủ Quy định chi tiết một số điều của Luật Quản lý, sử dụng tài sản công1.].

PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2

Hệ thống thông tin: Mạng LAN được đề xuất là cấp độ 2. Do đó, các máy chủ được sử dụng để triển khai hệ thống và các thành phần khác trong hệ thống như hạ tầng mạng, hệ thống lưu trữ…được thuyết minh phương án đáp ứng yêu cầu cấp độ 2 như sau:

6.2.1. Bảo đảm an toàn mạng

6.2.1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet và mạng diện rộng
2	Vùng mạng nội bộ	Có	Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống
3	Vùng mạng không dây	Có	Đơn vị sẽ triển khai vùng mạng này để cung cấp kết nối mạng không dây cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống
4	Vùng DMZ	Không có	Hiện tại đơn vị không cung cấp dịch vụ ra ngoài internet nên không sử dụng vùng mạng DMZ
5	Vùng mạng quản trị	Có	Đơn vị sẽ triển khai vùng mạng này để thiết lập, quản lý và giám sát các thiết bị mạng, thiết bị quản trị trong hệ thống

6	Vùng mạng Camera giám sát	Có	Đơn vị sẽ triển khai vùng mạng này để thiết lập kết nối cho các camera giám sát và đẩy dữ liệu về đầu ghi camera tập trung
7	Vùng máy chủ nội bộ	Không có	Hiện tại đơn vị không sử dụng máy chủ nên không sử dụng vùng mạng máy chủ nội bộ

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	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, tích hợp VPN để hỗ trợ quản lý từ xa an toàn qua internet Dự kiến đầu tư: Firewall Sophos XGS210
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, tích hợp IPS/IDS để quản lý xâm nhập các vùng mạng Dự kiến đầu tư: Firewall Sophos XGS210
3	Phương án phòng chống mã độc cho máy chủ và máy trạm	Có	Đơn vị sẽ thực hiện bổ sung phần mềm diệt virus Bkav hoặc Kaspersky trong thời gian 6-12 tháng tới, có tính năng nhận diện và phòng chống mã độc

4	Phương án dự phòng cho các thiết bị mạng chính	Có	Đơn vị sẽ thực hiện đầu tư, mua sắm các thiết bị mạng dự phòng cho các thiết bị mạng chính trong thời gian tới Dự kiến đầu tư: firewall, router, switch

6.2.1.2. 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	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, cấu hình quản lý 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 Dự kiến đầu tư: Firewall Sophos XGS210
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	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, sẽ cấu hình 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 Dự kiến đầu tư: Firewall Sophos XGS210
3	Thiết lập giới hạn thời gian chờ (timeout) để	Có	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới,

	đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.		cấu hình kiểm soát truy cập từ bên ngoài mạng Thời gian timeout 15 phút Dự kiến đầu tư: Firewall Sophos XGS210

6.2.1.3 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	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, cấu hình quản lý 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 Dự kiến đầu tư: Firewall Sophos XGS210

6.2.1.4. 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
Firewall Sophos XGS210	+	+
Switch Cisco C1300	+	+

6.2.1.5. 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	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, có tính năng phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống Dự kiến đầu tư: Firewall Sophos XGS210
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Có	Đơn vị sẽ thực hiện bổ sung thiết bị firewall trong thời gian 6-12 tháng tới, sẽ định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng Dự kiến đầu tư: Firewall Sophos XGS210

6.2.1.6. Bảo vệ thiết bị hệ thống

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa
Firewall Sophos XGS210	+	+	+
Switch Cisco C1300	+	+	+

6.2.2. Bảo đảm an toàn máy chủ

6.2.2.1. Xác thực

Yêu cầu	Thiết lập chính sách xác thực	Thay đổi các tài khoản mặc định trên hệ	Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự;

Máy chủ	trên máy chủ	thống hoặc vô hiệu hóa	Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ
-	-	-	

6.2.2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)
Máy chủ		
-	-	-

6.2.2.3. 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	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng
Máy chủ			
-	-	-	-

6.2.2.4. Phòng chống xâm nhập

Yêu cầu	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
Máy chủ				
-	-	-	-	-

6.2.2.5. Phòng chống phần mềm độc hại

Yêu cầu	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
Máy chủ		
-	-	-

6.2.2.6. 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	Hiện tại chưa có phương án chuyển giao cho đơn vị sử dụng. Sẽ có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

6.2.3. Bảo đảm an toàn ứng dụng

6.2.3.1. 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
Ứng dụng				
-	-	-	-	-

6.2.3.2. 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	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa

Ứng dụng		nhận được yêu cầu từ người dùng	
-	-	-	-

6.2.3.3. 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 (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
-	-	-

6.2.3.4. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
-	-

6.2.4. Bảo đảm an toàn dữ liệu

6.2.4.1 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	Hệ thống thông tin của đơn vị hiện chủ yếu hoạt động trong phạm vi mạng nội bộ, không cung cấp dịch vụ ra môi trường Internet. Dữ liệu phát sinh trong quá trình xử lý công việc được lưu trữ trên các máy trạm và thiết bị nội bộ, được quản lý thông qua cơ chế phân quyền người dùng,

			mật khẩu truy cập và các thiết lập bảo mật của hệ điều hành. Việc truy cập và khai thác dữ liệu được kiểm soát trong phạm vi mạng nội bộ nhằm hạn chế rủi ro mất an toàn thông tin.

6.2.4.2 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	Đơn vị thực hiện sao lưu dự phòng đối với các dữ liệu quan trọng phục vụ công tác chuyên môn nhằm đảm bảo khả năng khôi phục khi xảy ra sự cố. Dữ liệu hiện được sao lưu định kỳ trên các thiết bị lưu trữ nội bộ. Trong thời gian tới, đơn vị dự kiến đầu tư bổ sung thiết bị lưu trữ mạng (NAS) để thực hiện sao lưu tập trung, nâng cao khả năng bảo vệ và khôi phục dữ liệu khi cần thiết.