

QUYẾT ĐỊNH

**Ban hành Quy chế quản lý, vận hành và sử dụng
Phòng máy chủ Bệnh viện Đa khoa Khánh Hòa**

GIÁM ĐỐC BỆNH VIỆN ĐA KHOA KHÁNH HÒA

Căn cứ Quyết định 578/QĐ-UBND ngày 04/8/2025 của UBND tỉnh Khánh Hòa về việc kiện toàn chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bệnh viện Đa khoa Khánh Hòa;

Căn cứ Luật khám bệnh, chữa bệnh số 15/2023/QH15 ngày 09/01/2023 của Quốc hội;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015 của Quốc hội;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 của Quốc hội;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

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

Căn cứ Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế về Quy định điều kiện hoạt động y tế trên môi trường mạng;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Quyết định số 326/QĐ-BYT ngày 07/02/2024 của Bộ Y tế ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng;

Căn cứ Thông tư số 54/2017/TT-BYT ngày 29/12/2017 của Bộ Y tế Ban hành bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh;

Căn cứ Thông tư số 13/2025/TT-BYT ngày 06/06/2025 của Bộ Y tế về Hướng dẫn triển khai hồ sơ bệnh án điện tử;

Xét đề nghị của Lãnh đạo Phòng Kế hoạch Tổng hợp Bệnh viện Đa khoa Khánh Hòa.

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế quản lý, vận hành và sử dụng Phòng máy chủ Bệnh viện Đa khoa Khánh Hòa (đính kèm).

Điều 2. Quyết định này có hiệu lực kể từ ngày ký ban hành./.

Điều 3. Lãnh đạo các khoa, phòng, trung tâm và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận: (VBĐT)

- Như điều 3;
- Lưu: VT, KHTH.

GIÁM ĐỐC

Phan Hữu Chính

QUY CHẾ QUẢN LÝ, VẬN HÀNH VÀ SỬ DỤNG
PHÒNG MÁY CHỦ BỆNH VIỆN ĐA KHOA KHÁNH HÒA
(Kèm theo Quyết định số 1100/QĐ-BVĐKKH ngày 23/9/2025
của Bệnh viện Đa khoa Khánh Hòa)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

- Phạm vi điều chỉnh: Quy chế này quy định việc quản lý, vận hành và sử dụng Phòng máy chủ Bệnh viện Đa khoa Khánh Hòa.
- Đối tượng áp dụng: Các tổ chức, cá nhân tại Bệnh viện có liên quan tham gia quản lý, vận hành, sử dụng Phòng máy chủ.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *Mạng diện rộng của tỉnh (mạng WAN)*: là mạng tin học được thiết lập để kết nối giữa Phòng máy chủ và mạng nội bộ của cơ quan, địa phương trên địa bàn tỉnh thông qua kết nối mạng cáp quang trực tiếp và cho phép kết nối tới hệ thống mạng chuyên dùng của Chính phủ khi có yêu cầu.

2. *Hạ tầng kỹ thuật công nghệ thông tin*: là tập hợp thiết bị tính toán (máy chủ, máy trạm) thiết bị tường lửa, thiết bị cân bằng tải, thiết bị lưu trữ, thiết bị mạng, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng.

3. *Hệ thống thông tin*: là tập hợp của hạ tầng kỹ thuật, giải pháp, sản phẩm công nghệ thông tin và cơ sở dữ liệu được xây dựng, duy trì, vận hành, nâng cấp và mở rộng bảo đảm kết nối thông suốt, đồng bộ và khả năng chia sẻ, trao đổi thông tin an toàn, thuận tiện giữa các cơ quan nhà nước và giữa cơ quan nhà nước với tổ chức, cá nhân.

4. *An toàn thông tin*: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin trước các nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, thiết bị mạng, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn, an ninh thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

5. *Đơn vị chủ sở hữu Phòng máy chủ*: Bệnh viện Đa khoa Khánh Hòa.

6. *Đơn vị quản lý Phòng máy chủ (sau đây gọi tắt là đơn vị quản lý)*: Phòng Kế hoạch Tổng hợp.

7. *Đơn vị vận hành Phòng máy chủ (sau đây gọi tắt là đơn vị vận hành):* Tổ Công nghệ thông tin – Phòng Kế hoạch Tổng hợp.

8. *Người sử dụng:* Các tổ chức, cá nhân tại Bệnh viện tham gia sử dụng hạ tầng, phần mềm, dịch vụ của Phòng máy chủ.

Điều 3. Vị trí, chức năng của Phòng máy chủ

- Vị trí: Phòng máy chủ là công trình hạ tầng kỹ thuật công nghệ thông tin được Bệnh viện đầu tư thiết kế, xây dựng, duy trì, nâng cấp và mở rộng tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật áp dụng đối với Phòng máy chủ, bảo đảm Phòng máy chủ được hoạt động trong môi trường tiêu chuẩn, quy chuẩn với khả năng dự phòng cao.

- Chức năng: Phòng máy chủ là nơi tập trung các thiết bị công nghệ thông tin và viễn thông chuyên dụng với khả năng lưu trữ, dữ liệu lớn, hệ thống bảo mật an toàn dữ liệu, hệ thống phụ trợ, mạng diện rộng, mạng chuyên dùng và toàn bộ các hệ thống phần mềm ứng dụng công nghệ thông tin Bệnh viện.

Điều 4. Kiến trúc và dịch vụ của Phòng máy chủ

1. Kiến trúc của Phòng máy chủ được chia thành các thành phần sau:

a) Hệ thống máy chủ: bao gồm các máy chủ được đầu tư phục vụ cho ứng dụng trong hoạt động của đơn vị với khả năng sẵn sàng nâng cấp, mở rộng số lượng máy chủ trong tương lai đảm bảo năng lực cung cấp các dịch vụ ứng dụng với nhiều mục đích khác nhau như: ứng dụng dùng chung, ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành.

b) Hệ thống phần mềm: bao gồm hệ thống ứng dụng dùng chung, ứng dụng chuyên ngành và các hệ thống phần mềm khác được triển khai tại Phòng máy chủ phục vụ công tác chỉ đạo, điều hành, tác nghiệp của đơn vị theo thiết kế được phê duyệt.

c) Hệ thống lưu trữ: bao gồm các thiết bị lưu trữ chuyên dụng với năng lực quản lý tập trung và lưu trữ dữ liệu lớn đảm bảo cho mục đích sao lưu, khôi phục dữ liệu nếu có xảy ra sự cố. Hệ thống lưu trữ có khả năng mở rộng dung lượng lưu trữ dữ liệu trong tương lai.

d) Hệ thống an toàn thông tin: bao gồm các thiết bị tường lửa cho lớp mạng và lớp ứng dụng, các thiết bị ngăn chặn xâm nhập trái phép, thiết bị cân bằng tải, hệ thống kiểm soát ra vào, camera giám sát và các ứng dụng an ninh hệ thống thông tin. Mỗi thành phần trong hệ thống an toàn thông tin đều được thiết kế bảo đảm tính dự phòng và bổ sung hỗ trợ lẫn nhau trong toàn hệ thống thông tin.

đ) Hệ thống cơ sở dữ liệu: bao gồm các phân hệ cơ sở dữ liệu dùng chung hoặc chuyên ngành được xây dựng nhằm liên kết, tích hợp các ứng dụng dùng chung và chuyên ngành phục vụ ứng dụng công nghệ thông tin trong đơn vị.

e) Hệ thống mạng: bao gồm nhiều vùng mạng khác nhau (mạng diện rộng - WAN, vùng mạng riêng - DMZ, vùng mạng nội bộ - LAN...), mỗi vùng mạng được thiết lập các chính sách an ninh và truy cập riêng cho một hoặc nhiều mục đích sử

dụng khác nhau. Hệ thống mạng sử dụng đường truyền băng thông rộng và đường truyền số liệu chuyên dùng để phục vụ kết nối mạng WAN của tỉnh, kết nối các ứng dụng dùng chung, ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành phục vụ các cơ quan, địa phương khai thác, sử dụng và giao dịch hành chính trên môi trường mạng.

g) Các hệ thống phụ trợ: bao gồm hệ thống nguồn điện, hệ thống điều hòa, thiết bị lưu điện, máy phát điện, sàn nâng, hệ thống phòng cháy và chữa cháy, và các hệ thống phụ trợ có liên quan khác.

2. Các giải pháp, phần mềm được cài đặt, cung cấp dịch vụ công nghệ thông tin tại Phòng máy chủ, bao gồm:

a) Các phần mềm dùng chung phục vụ cho việc triển khai các ứng dụng khám, chữa bệnh bao gồm: Hệ thống phần mềm Quản lý bệnh viện (HIS), phần mềm Quản lý xét nghiệm (LIS), phần mềm Lưu trữ và Truyền tải hình ảnh (PACS), phần mềm Bệnh án điện tử (EMR).

b) Hệ thống lưu trữ dữ liệu.

c) Các dịch vụ khác trong phạm vi chức năng và khả năng cung cấp của Phòng máy chủ.

Điều 5. Nguyên tắc quản lý, vận hành và sử dụng Phòng máy chủ

1. Tuân thủ các nguyên tắc, biện pháp bảo đảm cơ sở hạ tầng thông tin phục vụ ứng dụng và phát triển công nghệ thông tin theo Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006.

2. Tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật quy định áp dụng đối với Phòng máy chủ theo Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ trưởng Bộ Thông tin và Truyền thông và các văn bản pháp luật khác có liên quan.

3. Bảo đảm các yêu cầu về an toàn thông tin theo Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa được ban hành tại Quyết định số 38/2015/QĐ-UBND ngày 24/12/2015 của Ủy ban nhân dân tỉnh Khánh Hòa.

4. Tuân thủ nguyên tắc xây dựng, quản lý, bảo vệ và duy trì cơ sở dữ liệu được quy định tại Điều 13 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

5. Đảm bảo các yêu cầu theo tiêu chí của Thông tư 54/2017/TT-BYT ngày 29/12/2017 ban hành Bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh.

6. Tuân thủ tiêu chuẩn theo thông tư 13/2025/TT-BYT ngày 06/6/2025 Hướng dẫn triển khai hồ sơ bệnh án điện tử.

7. Cơ quan quản lý và đơn vị vận hành có trách nhiệm tổ chức quản lý, sử dụng tài sản theo quy định của pháp luật về quản lý, sử dụng tài sản công. Phòng máy chủ không được phép triển khai cung cấp các dịch vụ gia tăng cho các tổ chức, cá nhân khác dưới bất kỳ hình thức nào.

8. Các tổ chức, cá nhân tham gia sử dụng các dịch vụ của Phòng máy chủ phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên các hệ thống ứng dụng và dịch vụ.

9. Đảm bảo kinh phí ngân sách nhà nước thường xuyên hàng năm cho công tác quản lý, duy trì, vận hành và bảo trì, bảo dưỡng, thay thế các thiết bị hỏng hóc, bổ sung, duy trì bản quyền (license) các phần mềm đã đầu tư tại Phòng máy chủ phục vụ nhiệm vụ chung theo quy định của pháp luật.

Điều 6. Các hành vi bị nghiêm cấm trong quản lý, vận hành và sử dụng Phòng máy chủ

- Phá hoại hệ thống thông tin, làm gián đoạn hoặc cản trở hoạt động một phần hoặc toàn bộ hoạt động của hệ thống thông tin tại Phòng máy chủ.

- Sử dụng hoặc phát tán các thông tin cá nhân lưu trữ tại Phòng máy chủ theo quy định tại Điều 21 Luật Công nghệ thông tin và Luật Số 91/2025/QH15 Luật Bảo vệ dữ liệu cá nhân vì mục đích vụ lợi, vi phạm quy định pháp luật hiện hành, trừ các yêu cầu đặc biệt của các cơ quan chức năng có thẩm quyền.

- Đánh cắp, giả mạo tài khoản để truy cập trái phép vào hệ thống thông tin tại Phòng máy chủ.

- Sử dụng các công cụ, phần mềm gây mất an toàn hệ thống và ảnh hưởng đến hoạt động của Phòng máy chủ.

Điều 7. Nội quy chung phòng máy chủ

- Đối với cán bộ, viên chức

+ Cán bộ, viên chức không có nhiệm vụ thì không được phép vào Phòng máy chủ.

+ Cấm hút thuốc, mang thức ăn thức uống, các vật dễ cháy, nổ vào Phòng máy chủ.

- Đối với nhân viên quản trị hệ thống

+ Tuân thủ nguyên tắc an toàn phòng cháy chữa cháy, an toàn điện và đảm bảo vệ sinh.

+ Sắp xếp, bố trí các trang thiết bị gọn gàng, ngăn nắp, dễ thao tác.

+ Thường xuyên theo dõi kiểm tra nhiệt độ, ẩm độ đạt tiêu chuẩn quy định của các thiết bị, máy chủ của phòng máy chủ.

+ Thường xuyên theo dõi kiểm tra các trang thiết bị dùng cho các hoạt động chuyên môn được lắp đặt bên ngoài phòng máy chủ phải có biện pháp giám sát, bảo vệ an toàn chống truy cập trái phép.

+ Các công việc bảo trì, sửa chữa thiết bị máy chủ đều phải ghi lại nhật ký, nhân viên đề nghị sửa chữa có trách nhiệm ký xác nhận vào nhật ký sau mỗi lần bảo trì sửa chữa.

+ Cán bộ quản lý hệ thống có nhu cầu làm việc ngoài giờ phải báo cáo với lãnh đạo.

+ Tài sản ở Phòng máy chủ chỉ được phép mang ra khỏi phòng khi có sự đồng ý của lãnh đạo.

Chương II

QUY ĐỊNH VỀ QUẢN LÝ, VẬN HÀNH VÀ SỬ DỤNG PHÒNG MÁY CHỦ

Điều 8. Quy định chung

1. Tổ chức, cá nhân tham gia quản lý, vận hành và sử dụng Phòng máy chủ phải tuân thủ các quy định về quản lý, vận hành và sử dụng Phòng máy chủ.

2. Quy định đối với cán bộ kỹ thuật quản trị, vận hành trực tiếp các hệ thống tại Phòng máy chủ (sau đây gọi tắt là cán bộ kỹ thuật)

a) Trong quá trình làm việc tại Phòng máy chủ phải tuân thủ nghiêm các quy trình, quy định và nội quy đã được phê duyệt.

b) Cán bộ kỹ thuật truy cập, khai thác và sử dụng thông tin tại Phòng máy chủ theo trách nhiệm và phân quyền được quy định; việc khai thác, sử dụng thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

c) Cán bộ kỹ thuật được giao giữ tài khoản, mật khẩu quản trị các hệ thống của Phòng máy chủ phải thực hiện quy trình thay đổi mật khẩu ít nhất 03 tháng/lần; các trường hợp đặc biệt, nghỉ lộ, lọt mật khẩu hoặc không đảm bảo khả năng giữ bí mật thì phải thực hiện quy trình đổi mật khẩu ngay sau khi sử dụng.

3. Chế độ trực vận hành Phòng máy chủ

a) Căn cứ yêu cầu vận hành Phòng máy chủ trong từng giai đoạn và thời điểm, đơn vị vận hành phân bổ nhân lực trực vận hành Phòng máy chủ phù hợp với điều kiện nhân lực và yêu cầu thực tế.

b) Chế độ trực trong trường hợp đặc biệt (có nguy cơ cao về an toàn thông tin, thiên tai, theo yêu cầu của cơ quan chức năng...): thực hiện chế độ trực 24/24 giờ trong ngày, có thể chia thành các ca trực nhưng không quá 08 giờ/ca trực.

4. Quy định đối với các tổ chức, cá nhân liên quan đến làm việc, đăng ký tham quan tại Phòng máy chủ

a) Các tổ chức, cá nhân đến làm việc, đăng ký tham quan phải tuân thủ theo các quy định của cơ quan quản lý Phòng máy chủ.

b) Tổ chức, cá nhân đến làm việc, đăng ký tham quan không được mang, sử dụng các thiết bị điện thoại, máy tính xách tay, máy tính bảng hoặc các thiết bị điện tử cá nhân khác (máy chụp hình, máy quay phim, thiết bị lưu trữ...) khi vào bên trong Phòng máy chủ.

c) Tổ chức, cá nhân đến làm việc, đăng ký tham quan cung cấp giấy giới thiệu của cơ quan, đơn vị hoặc giấy đề nghị làm việc, tham quan tại Phòng máy chủ.

d) Các thiết bị đưa vào, ra Phòng máy chủ phải được lập danh sách và biên bản giao nhận để quản lý.

Điều 9. Quy định về hệ thống mạng, bảo mật mạng

1. Hệ thống mạng phải bảo đảm:

a) Hệ thống mạng hoạt động liên tục 24/24 giờ, ổn định, an toàn và đáp ứng được yêu cầu về băng thông cho các ứng dụng trong hệ thống.

b) Áp dụng các giải pháp kiểm soát việc truy cập mạng để đảm bảo các quy định về an ninh, các chính sách bảo mật.

c) Tuân theo các tiêu chuẩn của Phòng máy chủ về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức đi dây, đầu nối, phân bổ nút mạng.

d) Đối với các kết nối Internet phải có các giải pháp, chính sách bảo mật đảm bảo hệ thống không bị tấn công xâm nhập, lây lan virus, phần mềm độc hại từ bên ngoài; cũng như ngăn chặn, không để phát tán virus, phần mềm độc hại từ các thiết bị ngoại vi khác. Đường truyền Internet cho Phòng máy chủ tối thiểu phải từ 02 (hai) nhà cung cấp dịch vụ khác nhau.

đ) Cán bộ kỹ thuật không được sử dụng trình duyệt hoặc các phần mềm để truy cập Internet từ các máy tính có địa chỉ IP chung hệ thống máy chủ thuộc Phòng máy chủ, trừ những trường hợp truy cập để phục vụ trực tiếp nghiệp vụ kiểm tra hệ thống.

2. Đơn vị vận hành chịu trách nhiệm giám sát, kiểm tra nội dung và băng thông truy cập, ngăn chặn và đề xuất các biện pháp xử lý các hành vi vi phạm.

Điều 10. Quy định về quản lý thiết bị

1. Thiết bị đặt tại Phòng máy chủ phải được đặt tên và dán nhãn tài sản nhà nước theo đúng tiêu chuẩn quy định.

2. Đơn vị vận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị tại Phòng máy chủ hàng quý, năm và báo cáo về đơn vị quản lý theo quy định.

3. Trường hợp thiết bị hỏng là thiết bị quan trọng (gây ảnh hưởng đến hoạt động của Phòng máy chủ), đơn vị vận hành phải báo cáo ngay về đơn vị quản lý để có biện pháp khắc phục kịp thời.

4. Ghi nhật ký, quy định thời gian lưu trữ các thông tin về hoạt động của các thiết bị, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra giám sát về sau.

Điều 11. Quy định về sao lưu, phục hồi dữ liệu

1. Thực hiện lưu trữ đầy đủ các dữ liệu của người dùng, ứng dụng và hệ thống. Tùy theo từng loại dữ liệu, thực hiện lưu trữ đúng và đủ thời hạn, đảm bảo phục hồi nguyên trạng khi có sự cố xảy ra.

2. Đơn vị vận hành có trách nhiệm xây dựng và triển khai thực hiện Quy trình sao lưu, phục hồi dữ liệu cho toàn bộ Phòng máy chủ.

3. Dữ liệu phải được phân loại để lưu trữ theo thứ tự ưu tiên về mức độ quan trọng, sao lưu theo thời gian, loại thông tin, nơi lưu trữ. Đối với các dữ liệu quan trọng phải được lưu trữ tối thiểu tại hai địa điểm cách biệt nhau.

4. Tần suất sao lưu tùy thuộc vào mức độ quan trọng dữ liệu và phải được kiểm soát và đối chiếu sau khi sao lưu.

Điều 12. Quy định về bảo mật hệ thống

1. Duy trì, cập nhật, theo dõi thường xuyên đối với hệ thống bảo mật (thiết bị tường lửa, phần mềm phòng chống mã độc tập trung, thiết bị giám sát phát hiện và ngăn chặn xâm nhập trái phép và các thiết bị chuyên dụng có liên quan khác) để bảo đảm an toàn, bảo mật cho Phòng máy chủ.

2. Tất cả các máy chủ tại Phòng máy chủ phải được cài đặt phần mềm phòng chống mã độc tập trung và luôn được cập nhật kịp thời các bản sửa lỗi, cơ sở dữ liệu các mẫu virus mới đồng thời được đặt ở chế độ quét thường xuyên, kiểm tra, rà quét trước khi có kết nối với các thiết bị ngoại vi như: ổ cứng di động, USB, ổ cứng gắn ngoài và các thiết bị lưu trữ khác. Những máy chủ được phát hiện có virus phải được cách ly ngay khỏi hệ thống để tránh lây nhiễm sang các máy chủ khác trong cùng hệ thống.

Điều 13. Quy định về an toàn hoạt động

1. Không được phép đặt tại Phòng máy chủ: thiết bị hỏng, thiết bị chờ thanh lý, hủy, tài liệu, vật tư, các vật dụng dễ cháy, nổ...

2. Phòng máy chủ phải đảm bảo vệ sinh, sạch sẽ, môi trường khô ráo. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị. Hệ thống máy lạnh, máy hút ẩm phải được kiểm tra, bảo dưỡng định kỳ 06 tháng/lần.

3. Hệ thống phòng cháy và chữa cháy phải đáp ứng theo tiêu chuẩn quy định, được cấp giấy phép của cơ quan có thẩm quyền, vừa đảm bảo an toàn tuyệt đối cho toàn hệ thống thiết bị, vừa đảm bảo an toàn cho người quản trị các hệ thống tại Phòng máy chủ.

4. Đảm bảo hệ thống điện cho Phòng máy chủ

a) Hệ thống điện cấp cho Phòng máy chủ phải có ít nhất 2 nguồn ổn định, liên tục được trang bị hệ thống lưu điện (UPS) và máy phát điện dự phòng để đảm bảo cho hệ thống vẫn hoạt động trong thời gian nguồn điện lưới gặp sự cố.

b) Hệ thống UPS và máy phát điện phải được kiểm tra hàng tuần (kiểm tra tải, pin của UPS, chạy không tải máy phát điện và kiểm tra các thông số kỹ thuật liên quan) và thực hiện bảo dưỡng định kỳ 06 tháng/lần.

5. Hệ thống camera thực hiện giám sát toàn bộ Phòng máy chủ liên tục 24/24 giờ; dữ liệu hình ảnh phải được lưu trữ ít nhất trong thời gian là 30 ngày.

6. Hệ thống kiểm soát ra, vào hoạt động 24/24 giờ và ghi đầy đủ nhật ký nhằm đảm bảo an ninh, chính xác và linh hoạt cho Phòng máy chủ.

7. Quản lý ra, vào Phòng máy chủ

a) Mỗi thành viên đơn vị vận hành được hệ thống kiểm soát ra, vào cấp thẻ từ, khóa vân tay riêng và chỉ sử dụng thẻ từ, khóa vân tay của mình khi ra, vào Phòng máy chủ.

b) Những người đến làm việc hoặc tham quan Phòng máy chủ phải thực hiện đăng ký theo quy định tại khoản 4 Điều 7 Quy chế này và đơn vị vận hành phải cập nhật thông tin vào sổ quản lý để theo dõi.

Điều 14. Quy định về quản lý hệ thống phần mềm

1. Đơn vị vận hành lập danh sách phần mềm đang triển khai tại Phòng máy chủ với các thông tin cơ bản gồm: tên phần mềm, giá trị, mức độ quan trọng, mục đích sử dụng, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, nơi lưu giữ.

2. Đơn vị vận hành phải phân loại và đánh giá mức độ rủi ro dựa trên yêu cầu về tính bảo mật, tính toàn vẹn, tính sẵn sàng cho việc sử dụng của tài sản phần mềm để thực hiện các biện pháp quản lý, bảo vệ phù hợp.

3. Các phần mềm triển khai tại Phòng máy chủ phải có bản quyền sử dụng theo đúng quy định của pháp luật.

4. Cài đặt và sử dụng các hệ thống phần mềm

a) Đối với phần mềm cài đặt mới tại Phòng máy chủ:

- Phần mềm trước khi cài đặt phải đáp ứng được các yêu cầu về mặt kỹ thuật, đúng với hồ sơ thiết kế được Giám đốc Bệnh viện phê duyệt.

- Khi cài đặt phải rà quét (scan) virus, mã độc... và sử dụng máy tính có ghi màn hình tất cả quá trình thao tác tại Phòng máy chủ.

b) Đối với các phần mềm đang triển khai tại Phòng máy chủ:

- Người sử dụng chịu trách nhiệm thường xuyên cập nhật thông tin, nội dung thông tin của các hệ thống thông tin, cơ sở dữ liệu, phần mềm chuyên ngành của mình; khi cung cấp thông tin ra bên ngoài phải đảm bảo các yêu cầu về an toàn, bảo mật, phạm vi cung cấp thông tin, tính đúng đắn, hợp pháp của thông tin.

- Thường xuyên cập nhật các bản vá lỗi đối với hệ điều hành, các phần mềm nền tảng, hệ thống mã nguồn theo khuyến nghị của nhà sản xuất.

5. Không phát tán, chia sẻ các hệ thống phần mềm tại Phòng máy chủ dưới bất kỳ hình thức nào khi chưa được sự đồng ý của Giám đốc Bệnh viện.

Điều 15. Quy định về xử lý sự cố Phòng máy chủ

1. Khi phát hiện có sự cố, người sử dụng hoặc cán bộ vận hành, đơn vị vận hành hệ thống có trách nhiệm báo cáo kịp thời cho lãnh đạo đơn vị vận hành và lãnh đạo cơ quan quản lý để có biện pháp cô lập và xác định nguyên nhân xảy ra sự cố, hạn chế tối đa ảnh hưởng tới hoạt động của hệ thống.

2. Tùy thuộc vào mức độ ảnh hưởng của sự cố, đánh giá và phân loại theo 03 mức:

a) Các sự cố thông thường (không gây ảnh hưởng hoặc ít ảnh hưởng đến hoạt động của Phòng máy chủ): đơn vị vận hành nhanh chóng xử lý sự cố.

b) Các sự cố nghiêm trọng (sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố liên quan đến an ninh thông tin, mất dữ liệu, gây ảnh hưởng trực tiếp đến hoạt động của Phòng máy chủ): ngay sau khi phát hiện sự cố, đơn vị vận hành cần thực hiện theo quy trình quản lý sự cố, đánh giá ảnh hưởng của sự cố và thực hiện báo cáo về cơ quan quản lý để phối hợp với các đơn vị chuyên trách hướng dẫn xử lý.

c) Các sự cố đặc biệt nghiêm trọng (gây ngưng trệ đến toàn bộ hoạt động của Phòng máy chủ): đơn vị vận hành phải thực hiện theo quy trình quản lý sự cố đánh giá ảnh hưởng của sự cố, phối hợp với các cơ quan Bộ, ngành liên quan, đồng thời thực hiện báo cáo nhanh về cơ quan quản lý để có chỉ đạo xử lý.

3. Nguyên tắc thực hiện khắc phục sự cố

a) Thực hiện sao lưu dữ liệu trước khi khắc phục sự cố (ưu tiên dữ liệu quan trọng).

b) Đảm bảo an toàn cho người và thiết bị hệ thống.

c) Ghi nhật ký diễn biến sự cố, phương án khắc phục.

4. Đối với các sự cố vượt khả năng xử lý (nếu có), Lãnh đạo đơn vị vận hành báo cáo Lãnh đạo đơn vị, cơ quan chủ quản để đề nghị đơn vị tư vấn, đơn vị cung cấp, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), và các đơn vị liên quan hỗ trợ ứng phó và khắc phục sự cố.

Điều 16. Quy định về bảo trì, bảo dưỡng Phòng máy chủ

1. Đơn vị vận hành có trách nhiệm thực hiện bảo trì, bảo dưỡng hệ thống theo quy trình và kế hoạch được duyệt.

2. Việc thực hiện bảo trì, bảo dưỡng các hệ thống do đơn vị vận hành thực hiện hoặc thuê dịch vụ.

3. Thời gian bảo trì, bảo dưỡng từng thiết bị, phần mềm thực hiện theo yêu cầu thực tiễn và khuyến nghị của nhà cung cấp. Bảo trì, bảo dưỡng tổng thể toàn bộ hệ thống ít nhất 01 lần/năm.

4. Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến hoạt động của Phòng máy chủ; quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, quy trình và ghi nhật ký về tình trạng hoạt động trước và sau khi thực hiện.

Điều 17. Quy định về quản lý mật khẩu quản trị hệ thống Phòng máy chủ

1. Người đứng đầu đơn vị vận hành có trách nhiệm quản lý hệ thống mật khẩu quản trị của Phòng máy chủ và lập 01 (một) bản in hệ thống mật khẩu quản trị hiện

hành cho vào phong bì, niêm phong, dán kín, quản lý, lưu trữ theo chế độ “Mật” tại trụ sở của đơn vị vận hành.

2. Mật khẩu phải bảo đảm độ phức tạp về độ dài, nội dung, thời gian sử dụng:

a) Độ dài của mật khẩu:

- Đối với mật khẩu của nhân viên và người sử dụng (dùng để đăng nhập thư điện tử, ứng dụng nghiệp vụ, máy tính cá nhân và các ứng dụng khác): tối thiểu là 08 ký tự.

- Đối với mật khẩu quản trị hệ thống (sử dụng cho quản trị các hệ thống mạng, bảo mật, máy chủ, thư điện tử, ứng dụng dùng chung): tối thiểu là 11 ký tự.

b) Nội dung mật khẩu:

- Không bao gồm các từ dễ nhớ như: tên, ngày tháng năm sinh, số điện thoại.

- Đối với mật khẩu quản trị hệ thống phải bao gồm các loại ký tự sau: chữ cái in thường, chữ cái in hoa, ký tự đặc biệt, số.

c) Thời gian sử dụng mật khẩu:

Đối với mật khẩu của nhân viên vận hành, của người quản trị hệ thống (không phải quản trị cấp cao nhất) định kỳ phải được thay đổi ít nhất 03 tháng một lần. Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn an ninh thông tin thì Thủ trưởng đơn vị vận hành quyết định việc thay đổi toàn bộ mật khẩu quản trị của Phòng máy chủ.

d) Quy định lưu trữ mật khẩu:

- Không lưu trữ mật khẩu trên máy tính cá nhân, các thiết bị điện tử.

- Các tài liệu liên quan đến mật khẩu được xem là tài liệu mật, không soạn thảo trên máy tính có nối mạng Internet.

Điều 18. Quy định về cài đặt phần mềm, tiếp nhận thiết bị, phần mềm triển khai tại Phòng máy chủ

1. Việc triển khai các dự án, nhiệm vụ ứng dụng công nghệ thông tin trên hạ tầng Phòng máy chủ phải được quy định cụ thể trong thiết kế kỹ thuật được cơ quan có thẩm quyền phê duyệt.

2. Khi có nhu cầu cài đặt phần mềm trên máy chủ Phòng máy chủ hoặc đặt máy chủ để triển khai ứng dụng trên nền hạ tầng Phòng máy chủ, các tổ chức, cá nhân gửi văn bản đề nghị về cơ quan quản lý xem xét, quyết định. Đối với phần mềm, phải có cam kết và tài liệu chứng minh phần mềm đã được thực hiện kiểm thử, kiểm tra về an toàn, bảo mật trước khi cài đặt tại Phòng máy chủ. Đơn vị vận hành ban hành thủ tục tiếp nhận yêu cầu cài đặt phần mềm, đặt máy chủ và quản lý tài sản đặt tại Phòng máy chủ.

3. Các tổ chức, cá nhân có thiết bị hoặc ứng dụng đặt tại Phòng máy chủ chịu trách nhiệm quản trị nội dung, phần mềm tuân thủ các nguyên tắc đảm bảo an toàn, an ninh hệ thống. Bên cạnh đó, hàng năm bố trí kinh phí để thực hiện bảo trì, bảo

dưỡng thiết bị, cập nhật, nâng cấp phần mềm và duy trì bản quyền các phần mềm thương mại có liên quan đến thiết bị, ứng dụng triển khai tại Phòng máy chủ.

Điều 19. Quy định về quản lý hồ sơ liên quan đến Phòng máy chủ

1. Danh sách các hồ sơ lưu trữ
 - a) Các quy định về quản lý, triển khai, vận hành các hệ thống.
 - b) Các quy trình vận hành kỹ thuật, bảo trì, bảo dưỡng hệ thống; quy trình xử lý, khắc phục sự cố; quy trình sao lưu, phục hồi dữ liệu lưu trữ tại Phòng máy chủ.
 - c) Hồ sơ thiết kế, thuyết minh kỹ thuật.
 - d) Hồ sơ quản trị các hệ thống thông tin (báo cáo định kỳ, báo cáo sự cố, nhật ký vận hành...).
 - đ) Bảng thống kê danh sách thiết bị, phần mềm; danh sách các thiết bị hỏng, hết khấu hao chờ thanh lý; biên bản bàn giao thiết bị cho người quản trị, người sử dụng (nếu có).
 - e) Tài liệu, biên bản kiểm tra, đánh giá của Phòng máy chủ.
 - g) Sổ quản lý ra, vào; lịch phân công trực Phòng máy chủ.
 - h) Các hồ sơ, tài liệu kỹ thuật khác.
2. Hồ sơ phải được lưu bằng văn bản, tập tin bản mềm trên máy tính và phải được cập nhật khi có sự thay đổi theo quy định.
3. Danh mục hồ sơ tài liệu của Phòng máy chủ được quản lý theo chế độ “Mật”:
 - a) Sơ đồ thiết kế mạng và lắp đặt thiết bị tại Phòng máy chủ.
 - b) Bảng phân bổ địa chỉ IP cho các vùng mạng tại Phòng máy chủ.
 - c) Thông số cấu hình các thiết bị trọng yếu: tường lửa (firewall), bộ định tuyến (router), bộ chuyển mạch trung tâm (core switch), thiết bị phòng chống xâm nhập IPS...
 - d) Bảng quản lý tài khoản và mật khẩu tại Phòng máy chủ.
 - đ) Các thông tin tài liệu khác theo quy định của đơn vị chủ sở hữu và đơn vị quản lý.

Điều 20. Kiểm tra của đơn vị quản lý đối với công tác quản lý, vận hành Phòng máy chủ

1. Đơn vị quản lý tổ chức kiểm tra việc tuân thủ các quy định về quản lý kỹ thuật, triển khai, vận hành và sử dụng Phòng máy chủ theo các quy định tại Quy chế này định kỳ tối thiểu 01 năm một lần hoặc kiểm tra đột xuất khi cần thiết.
2. Nội dung kiểm tra:
 - a) Việc bảo đảm các điều kiện về môi trường cho hoạt động của Phòng máy chủ.
 - b) Tình hình sử dụng thiết bị, ứng dụng của hệ thống.

c) Hoạt động của hệ thống máy chủ, các phần mềm, dịch vụ (cập nhật các bản sửa lỗi, dung lượng ổ cứng, hiệu năng sử dụng và các hoạt động có liên quan).

d) Tình hình an ninh bảo mật hệ thống, đánh giá hiệu quả (khả năng phát hiện và ngăn chặn) của hệ thống bảo mật.

đ) Kiểm tra công tác sao lưu, lưu trữ, phục hồi dữ liệu.

e) Quản lý hồ sơ: Ghi nhật ký, cập nhật, tổng hợp thiết bị, báo cáo...

g) Việc tuân thủ các quy định khác nêu tại Quy chế này.

3. Các vấn đề phát hiện sau khi kiểm tra phải được tổng hợp, đánh giá phân tích mức độ ảnh hưởng với hoạt động của Phòng máy chủ, giao đơn vị vận hành lập kế hoạch khắc phục xử lý và báo cáo đơn vị quản lý để theo dõi, chỉ đạo.

Chương III

QUY ĐỊNH TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN TRONG VIỆC QUẢN LÝ, VẬN HÀNH VÀ SỬ DỤNG PHÒNG MÁY CHỦ

Điều 21. Trách nhiệm của đơn vị quản lý

- Tham mưu đơn vị chủ sở hữu nâng cấp và mở rộng Phòng máy chủ đáp ứng nhu cầu triển khai ứng dụng công nghệ thông tin của đơn vị.

- Tham mưu đơn vị chủ sở hữu nâng cấp tái cấu trúc mô hình và hạ tầng theo công nghệ mới (cloud, big-data...) đảm bảo chuẩn hóa, thống nhất hệ thống hạ tầng, ứng dụng công nghệ thông tin và cơ sở dữ liệu được triển khai tại Phòng máy chủ.

- Phê duyệt Quy trình tiếp nhận yêu cầu cài đặt phần mềm, chuyển giao thiết bị và quản lý tài sản đối với các thiết bị triển khai tại Phòng máy chủ.

- Kiểm tra và giám sát việc quản lý, vận hành và sử dụng Phòng máy chủ của đơn vị vận hành theo quy định tại Điều 19 của Quy chế này và các quy định của pháp luật khác có liên quan.

- Định kỳ hàng năm hoặc đột xuất, thực hiện báo cáo đơn vị chủ sở hữu về tình hình hoạt động của Phòng máy chủ.

Điều 22. Trách nhiệm của đơn vị vận hành

- Xây dựng và tham mưu đơn vị quản lý ban hành quy định tiếp nhận yêu cầu cài đặt phần mềm, chuyển giao thiết bị và quản lý tài sản đối với các thiết bị của triển khai tại Phòng máy chủ và tổ chức triển khai thực hiện sau khi được phê duyệt.

- Ban hành quy trình về vận hành, bảo trì, bảo dưỡng; quy trình xử lý, khắc phục sự cố; quy trình sao lưu, phục hồi dữ liệu lưu trữ tại Phòng máy chủ và tổ chức triển khai thực hiện sau khi ban hành.

- Ban hành nội quy làm việc tại Phòng máy chủ.

- Xây dựng hồ sơ đề xuất cấp độ an toàn thông tin cho hệ thống thông tin tại Phòng máy chủ theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7

năm 2016 của Chính phủ gửi cơ quan quản lý thẩm định, trình cấp có thẩm quyền xem xét phê duyệt.

- Xây dựng và tổ chức thực hiện kế hoạch bảo dưỡng, bảo trì, sửa chữa và thay thế trang thiết bị tại Phòng máy chủ; xây dựng kế hoạch, bố trí cán bộ quản lý, vận hành trực và theo dõi các hệ thống tại Phòng máy chủ.

- Quy hoạch tài nguyên hệ thống, xây dựng các giải pháp, phương án kỹ thuật, các tài liệu hướng dẫn sử dụng các dịch vụ triển khai tại Phòng máy chủ và các kế hoạch phát triển Phòng máy chủ.

- Ban hành và tổ chức thực hiện kế hoạch đào tạo cán bộ quản lý, vận hành có chuyên môn đáp ứng yêu cầu, được trang bị các kiến thức liên quan tới hoạt động của Phòng máy chủ.

- Nghiên cứu, đề xuất nâng cấp và mở rộng Phòng máy chủ đáp ứng nhu cầu cho các ứng dụng công nghệ thông tin đảm bảo chuẩn hóa, thống nhất hệ thống hạ tầng, ứng dụng và cơ sở dữ liệu được triển khai tại Phòng máy chủ.

- Hàng năm, xây dựng dự toán kinh phí đảm bảo công tác duy trì hoạt động, vận hành, bảo dưỡng, sửa chữa, thay thế trang thiết bị Phòng máy chủ, xây dựng hoặc nâng cấp phần mềm quản lý triển khai tại Phòng máy chủ trình đơn vị quản lý và triển khai sau khi được phê duyệt.

- Thực hiện báo cáo định kỳ hàng quý hoặc đột xuất theo yêu cầu cho cơ quan quản lý về tình hình hoạt động của Phòng máy chủ.

Điều 23. Trách nhiệm của tổ chức, cá nhân sử dụng khai thác sử dụng các dịch vụ tại Phòng máy chủ

- Sử dụng các dịch vụ của Phòng máy chủ theo quy chế này và các hướng dẫn khác của cơ quan quản lý và đơn vị vận hành.

- Phối hợp với đơn vị vận hành trong công tác bảo đảm an toàn thông tin

Đối với người sử dụng thực hiện khai thác, sử dụng các dịch vụ tại Phòng máy chủ tỉnh: Tuân thủ các quy định về an toàn bảo mật thông tin, quản lý, vận hành và sử dụng Phòng máy chủ. Không được thực hiện các hành vi đánh cắp, giả mạo tài khoản, truy cập trái phép, sử dụng các công cụ, phần mềm làm tổn hại đến hoạt động của Phòng máy chủ.

- Trường hợp phát sinh sự cố, phải thông báo ngay cho cán bộ kỹ thuật của đơn vị vận hành để phối hợp trong việc xử lý sự cố và xác nhận kết quả xử lý.

Chương IV TỔ CHỨC THỰC HIỆN

Điều 24. Điều khoản thi hành

Trong quá trình thực hiện nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung, các cá nhân phản ánh trực tiếp về Tổ Công nghệ thông tin - Phòng Kế hoạch Tổng hợp để được hướng dẫn cụ thể./.