

Số : 1551/QĐ-DHĐN

Đồng Nai, ngày 14 tháng 9 năm 2023

QUYẾT ĐỊNH

V/v Ban hành Quy trình Quản lý Hệ thống Công nghệ Thông tin

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC ĐỒNG NAI

Căn cứ Quyết định số 1572/QĐ-TTg ngày 20 tháng 8 năm 2010 của Thủ tướng chính phủ về việc thành lập Trường Đại học Đồng Nai trên cơ sở nâng cấp Trường Cao đẳng Sư phạm Đồng Nai;

Căn cứ Nghị quyết 1077/NQ-HĐT Ngày 30 tháng 8 năm 2021 của Hội đồng Trường Đại học Đồng Nai về việc ban hành Quy trình tổ chức và hoạt động của Trường Đại học Đồng Nai;

Căn cứ Chiến lược Phát triển Trường Đại học Đồng Nai giai đoạn đến năm 2025 và tầm nhìn đến 2030;

Xét đề nghị của Phó Giám đốc, phụ trách Trung tâm Thông tin – Thư viện,

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy trình Quản lý Hệ thống Công nghệ Thông tin.

Điều 2. Các ông (bà) Trưởng các Phòng, Trung tâm, Khoa, Lãnh đạo các đơn vị trực thuộc Trường Đại học Đồng Nai chịu trách nhiệm thi hành Quyết định này.

Quyết định này có hiệu lực kể từ ngày ký./.

Nơi nhận:

- Như Điều 2;
- Website của Trường;
- Lưu: VT, TTTV.



TS. Lê Anh Đức

MỤC LỤC

	Trang
CHƯƠNG I. QUY ĐỊNH CHUNG	1
Điều 1. Mục đích	1
Điều 2. Phạm vi điều chỉnh và đối tượng áp dụng.....	1
Điều 3. Giải thích từ ngữ	1
CHƯƠNG II. NGUYÊN TẮC QUẢN LÝ HỆ THỐNG CĐHĐN	3
Điều 4. Quản lý nguồn nhân lực CĐHĐN.....	3
Điều 5. Hệ thống báo cáo của IT	3
Điều 6. Quản lý hệ thống CĐHĐN.....	4
Điều 7. Đảm bảo an toàn hệ thống CĐHĐN	4
Điều 8. Nguyên tắc về bảo quản thông tin điện tử.....	5
Điều 9. Nguyên tắc bảo mật hệ thống thông tin	5
Điều 10. Tuân thủ bản quyền phần mềm	6
CHƯƠNG III. TRÁCH NHIỆM CỦA CÁC ĐƠN VỊ.....	7
Điều 11. Đơn vị phụ trách Hệ Thống Cơ Sở Hạ Tầng	7
Điều 12. Đơn vị phụ trách Phát triển ứng dụng	8
Điều 13. Đơn vị phụ trách Nhân sự	8
Điều 14. Đơn vị phụ trách Thiết bị.....	8
CHƯƠNG IV. THỰC HIỆN QUẢN LÝ HỆ THỐNG CĐHĐN.....	8
Điều 15. Tiêu chuẩn cơ sở hạ tầng hệ thống CĐHĐN tại ĐHĐN	8
Điều 16. Quản lý thông tin truy cập hệ thống.....	11
Điều 17. Quản lý vận hành hệ thống ứng dụng	12
Điều 18. Sao lưu và phục hồi dữ liệu.....	13
Điều 19. Hỗ trợ người dùng hệ thống CĐHĐN.....	15
Điều 20. Bảo trì thiết bị CĐHĐN	15
Điều 21. Quản lý các sự cố về CĐHĐN	15
Điều 22. Quản lý phòng máy chủ	16
CHƯƠNG V. ĐIỀU KHOẢN THI HÀNH.....	16
Điều 23. Trách nhiệm thi hành	16
Điều 24. Thẩm quyền sửa đổi, bổ sung, thay thế, hủy bỏ.....	16
Danh mục Phụ lục, Biểu mẫu liên quan	18

QUY TRÌNH QUẢN LÝ HỆ THỐNG CÔNG NGHỆ THÔNG TIN

CHƯƠNG I. QUY ĐỊNH CHUNG

Điều 1. Mục đích

Quy trình quản lý hệ thống Công nghệ thông tin nhằm đảm bảo chuẩn mực, đồng bộ, quản lý vận hành xuyên suốt hệ thống Công nghệ thông tin trường Đại học Đồng Nai

Điều 2. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy trình này quy định các nguyên tắc và phương thức thực hiện quản lý hệ thống Công nghệ thông tin để đảm bảo an toàn, bảo mật, phòng ngừa các rủi ro cho hệ thống Công nghệ thông tin, trách nhiệm của các Đơn vị có liên quan.

2. Đối tượng áp dụng

Quy trình này áp dụng cho các Hội đồng, các Phòng Ban, các Khoa và các Trung tâm thuộc trường Đại học Đồng Nai.

Điều 3. Giải thích từ ngữ

1. ĐHĐN: là trường Đại học Đồng Nai
2. TCHC & QT: Phòng Tổ chức - Hành chính & Quản trị
3. Đơn vị: là các Đơn vị thực hiện chức năng chuyên môn theo quy định tại quy trình này.
4. Đơn vị PTCSHT: là viết tắt của Đơn vị phụ trách cơ sở hạ tầng. Đơn vị PTCSHT quản lý và vận hành Hệ thống cơ sở hạ tầng công nghệ thông tin ĐHĐN là Phòng Tổ chức - Hành chính & Quản trị.
5. Đơn vị phụ trách Phát triển ứng dụng: là Phòng Tổ chức - Hành chính & Quản trị, phụ trách phát triển các ứng dụng CĐHĐN cho nhà trường.
6. Hệ thống công nghệ thông tin: là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ.
7. CĐHĐN: là viết tắt của Công nghệ thông tin.
8. Tài sản CĐHĐN: là các trang thiết bị, thông tin thuộc hệ thống CĐHĐN của Đơn vị. Bao gồm:
 - a/ Tài sản vật lý: là các thiết bị CĐHĐN, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống CĐHĐN;
 - b/ Tài sản thông tin: là các dữ liệu, tài liệu liên quan đến hệ thống CĐHĐN. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử;

c/ Tài sản phần mềm: bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

9. Rủi ro CDHĐN: là khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến hệ thống CDHĐN. Rủi ro CDHĐN liên quan đến quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người.

10. Quản lý rủi ro CDHĐN: là các hoạt động phối hợp nhằm xác định và kiểm soát các rủi ro CDHĐN có thể xảy ra.

11. Bên thứ ba: là các tổ chức, cá nhân có chuyên môn được ĐHĐN thuê hoặc hợp tác với nhà trường nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống CDHĐN.

12. Hệ thống an ninh mạng: là tập hợp các thiết bị tường lửa; thiết bị kiểm soát, phát hiện truy cập bất hợp pháp; phần mềm quản trị, theo dõi, ghi nhật ký trạng thái an ninh mạng và các trang thiết bị khác có chức năng đảm bảo an toàn hoạt động của mạng, tất cả cùng hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm kiểm soát chặt chẽ tất cả các hoạt động trên mạng.

13. Tường lửa: là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

14. Virus: là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

15. Phần mềm ứng dụng cơ bản: là các phần mềm phục vụ nhu cầu công việc như Microsoft office (word, excel, Powerpoint), phần mềm diệt virus, phần mềm đọc file pdf, phần mềm gõ tiếng việt, phần mềm giải nén....

16. Phần mềm đặc thù: là các phần mềm cần trang bị bản quyền phục vụ nhu cầu công việc như phần mềm quản lý đào tạo/kế toán/nhân sự/kế hoạch/xử lý đồ họa, từ điển...

17. Phần mềm độc hại (mã độc): là các phần mềm có tính năng gây hại như malware, phần mềm do thám (spyware), phần mềm quảng cáo (adware) hoặc các dạng tương tự khác.

18. Email: là hệ thống trao đổi thư điện tử thông qua mạng Internet, phục vụ nhu cầu trao đổi công việc trong nhà trường và đối tác bên ngoài.

19. Active Directory' (AD): là hệ thống quản lý tài khoản và thiết lập các luật lệ chung toàn trường.

20. Video Conference: là hệ thống dùng để kết nối hội họp truyền hình trực tuyến thông qua mạng Internet hoặc kênh truyền số liệu nội bộ.

21. Server File: là hệ thống máy chủ mạng dùng để quản lý tập trung dữ liệu làm việc của CBNV thuộc ĐHĐN.

22. Website: là hệ thống các trang web của trường, dùng để công bố thông tin trường và tương tác với người dùng bên ngoài.

23. Phần mềm Quản lý Đào tạo: là hệ thống quản lý các hoạt động nghiệp vụ Quản lý Đào tạo ĐHĐN.

24. Phần mềm Kế toán: là hệ thống quản lý các hoạt động nghiệp vụ Kế toán ĐHĐN.

25. Phần mềm Quản lý Tài sản: là hệ thống quản lý các hoạt động nghiệp vụ Tài sản ĐHĐN.

26. Phần mềm Quản lý Nhân sự: là hệ thống quản lý các hoạt động nghiệp vụ Nhân sự ĐHĐN.

27. Phần mềm Quản lý Thư viện: là hệ thống quản lý các hoạt động nghiệp vụ Thư viện ĐHĐN.

28. EGov: là hệ thống hỗ trợ các nghiệp vụ văn thư, tin nhắn nội bộ, thông báo của ĐHĐN.

29. E-Office: là hệ thống hỗ trợ các nghiệp vụ ngoài các hệ thống nghiệp vụ (Quản lý đào tạo, Thư viện, Tài sản, Nhân sự, Kế toán) cho CBNV và GV ĐHĐN.

30. E-learning: là hệ thống hỗ trợ, cung cấp công cụ học tập/giảng dạy trực tuyến.

31. Server Backup: là hệ thống máy chủ mạng dùng để sao lưu và phục hồi dữ liệu khi sự cố xảy ra. Tape Backup: là hệ thống lưu trữ dữ liệu backup.

32. Hệ thống giám sát (Monitor): là việc thu thập các thông tin trên các thành phần của hệ thống, phân tích các thông tin, dấu hiệu nhằm đánh giá và đưa ra các cảnh báo cho người quản trị hệ thống.

33. Điểm yếu kỹ thuật: là vị trí trong hệ thống CĐHĐN dễ bị tổn thương khi bị tấn công hoặc xâm nhập bất hợp pháp.

CHƯƠNG II. NGUYÊN TẮC QUẢN LÝ HỆ THỐNG CĐHĐN

Điều 4. Quản lý nguồn nhân lực CĐHĐN

1. TCHC & QT phụ trách theo hàng dọc tất cả các vấn đề chuyên môn hệ thống CĐHĐN tại các cơ sở, chi nhánh thuộc ĐHĐN.

2. IT chịu trách nhiệm quản lý hệ thống CĐHĐN theo sự phân quyền của TCHC & QT.

3. Bất cứ khoản mục đầu tư nào liên quan đến hệ thống CĐHĐN cần phải được TCHC & QT thẩm định và phê duyệt.

Điều 5. Hệ thống báo cáo của IT

IT phải thực hiện việc kiểm tra báo cáo hệ thống CĐHĐN theo định kỳ và quy định sau:

1. Báo cáo hàng ngày: thiết lập chế độ kiểm tra hệ thống CĐHĐN ít nhất 15 phút trước khi bắt đầu giờ làm việc chính thức của mỗi ngày làm việc. Gửi báo cáo cho TCHC & QT theo biểu mẫu CĐHĐN/QC-01/M01.

2. Báo cáo hàng tuần: thực hiện việc báo cáo sao lưu hệ thống CĐHĐN của tuần làm việc ít nhất trước khi kết thúc ngày làm việc cuối cùng của tuần báo cáo. Báo cáo các công tác tuần theo kế hoạch và lập kế hoạch cho tuần kế tiếp. Gửi báo cáo cho TCHC & QT theo biểu mẫu CĐHĐN/QC-01/M02.

3. Báo cáo quý: trong vòng ba (3) ngày kể từ ngày kết thúc quý, phải hoàn tất việc rà soát đánh giá lại tất cả các hoạt động của hệ thống CĐHĐN và đề xuất giải pháp và kế hoạch thực hiện cho quý tiếp theo. Gửi báo cáo cho TCHC & QT.

4. Báo cáo sơ kết, tổng kết: thực hiện việc đánh giá về các mặt hoạt động CĐHĐN của Đơn vị mình phụ trách, báo cáo trực tiếp về TCHC & QT.

5. Báo cáo dự án: thực hiện các báo cáo cho Người đứng đầu dự án theo phân công.

Điều 6. Quản lý hệ thống CĐHĐN

1. Hệ thống CĐHĐN tại các đơn vị là một bộ phận của hệ thống CĐHĐN của nhà trường và được kết nối với hệ thống CĐHĐN trường.

2. Việc quản lý và vận hành hệ thống CĐHĐN tại các đơn vị phải áp dụng chung chính sách CĐHĐN của nhà trường.

3. IT phải tuân thủ các chính sách đã được thiết lập trên hệ thống CĐHĐN.

4. IT được thao tác các quyền được thiết lập trên hệ thống CĐHĐN.

5. Hệ thống dữ liệu và phần mềm ứng dụng chính tại các đơn vị trong nhà trường phải tập trung tại Datacenter ĐHĐN và do TCHC & QT quản lý và vận hành.

Điều 7. Đảm bảo an toàn hệ thống CĐHĐN

1. Tất cả các hệ thống CĐHĐN phải được bảo vệ bằng mật khẩu và mật khẩu phải được thay đổi định kỳ. Hệ thống CĐHĐN được thiết lập thời gian khóa tự động khi không thực hiện hoạt động nào trong một khoảng thời gian cụ thể, việc đăng nhập và đăng xuất phải được ghi nhật ký lại.

2. Tất cả hệ thống CĐHĐN phải luôn được cập nhật các bản vá lỗi (update) mới nhất đã có sự kiểm tra.

3. Trên tất cả hệ thống CĐHĐN, các dịch vụ và phần mềm không sử dụng phải được gỡ bỏ khỏi hệ thống hoặc vô hiệu hóa.

4. IT định kỳ hàng quý cập nhật và duy trì danh mục tất cả các máy tính và phần mềm điện tử sử dụng trên hệ thống CĐHĐN.

5. Phần mềm diệt virus quản lý tập trung được tự động cập nhật chữ ký virus mới nhất phải được sử dụng.

6. Tường lửa trên máy tính luôn được cập nhật bản vá lỗi mới nhất phải được duy trì đặc biệt nếu sử dụng truy cập Internet khi CBNV làm việc tại trường hay tại địa điểm bên ngoài trường.

7. Hệ thống mạng của nhà trường nên được thiết lập tường lửa 2 lớp cũng như các hệ thống ngăn chặn xâm nhập hoặc tấn công như IDS, IPS...

8. Các công truy cập mạng nội bộ của CDHĐN được kiểm soát bằng các phương pháp như an ninh cổng (port security)... nhằm chống người lạ tiếp cận vào hệ thống CDHĐN.

9. Các mạng không dây (wireless) trong ĐHĐN phải được kiểm soát bằng mật khẩu. Đối với mạng không dây dành cho sinh viên/khách (Guest), thì phải được cô lập với mạng nội bộ.

10. Tất cả hệ thống mạng trong ĐHĐN (kể cả mạng không dây) được phân loại và được thiết lập một chuẩn an ninh tương ứng tùy theo nhu cầu mức độ an ninh của mỗi loại.

11. Các ứng dụng thông tin sử dụng trên trình duyệt của Internet, hoặc các việc truy cập từ xa như remote desktop, truy cập từ bên ngoài trường... phải được mã hóa bằng các phương pháp như https, VPN...

Điều 8. Nguyên tắc về bảo quản thông tin điện tử

1. Thông tin do cá nhân chịu trách nhiệm lưu trữ là thông tin hoặc do cá nhân tạo ra trong quá trình làm việc, hoặc được giao trách nhiệm lưu trữ.

2. Thông tin do đơn vị chịu trách nhiệm lưu trữ là dạng thông tin cơ sở dữ liệu, bao gồm nhiều dữ liệu của nhiều cá nhân thuộc một Đơn vị hoặc của nhiều Đơn vị.

3. Cá nhân hoặc Đơn vị có trách nhiệm lưu trữ theo cây thư mục hoặc quy ước ký hiệu, các văn bản có nhiều phiên bản hoặc thời gian ban hành khác nhau thì tên thư mục phải kèm ngày tháng năm thực hiện.

4. Đơn vị PTCST có trách nhiệm quản lý, lưu trữ hệ thống mạng, mã nguồn, đảm bảo an toàn cơ sở dữ liệu.

Điều 9. Nguyên tắc bảo mật hệ thống thông tin

1. Đối với thông tin thể hiện bằng tập tin mỗi đơn vị, cá nhân được cung cấp nơi lưu trữ thông tin trên hệ thống máy chủ;

a/ Các cá nhân, Đơn vị không được sao chép, phát tán dữ liệu thông tin ra ngoài không phải mục đích phục vụ công việc của Đơn vị, công việc của nhà trường;

b/ Các cá nhân lưu trữ tập tin quan trọng (liên quan đến bí mật, bí quyết nhà trường, dữ liệu sinh viên,...) phải cài đặt mật mã. Mật mã phải thông báo cho Trưởng đơn vị ngay sau khi cài đặt. Trừ trường hợp dữ liệu được cấp thẩm quyền tại trường phân công quản lý riêng và phải bàn giao khi nghỉ việc, chuyển công tác;

c/ Nếu dữ liệu nhạy cảm được lưu trữ trên các máy tính, phần mềm tường lửa và các phần mềm phát hiện ngăn chặn xâm nhập khác phải được sử dụng.

2. Đối với thông tin thể hiện bằng thư tín điện tử (email): Cá nhân có trách nhiệm quản lý và bảo mật thông tin thư điện tử của mình (tên truy cập, mật mã, nội dung thư điện tử). Nếu để các cá nhân, tổ chức khác sử dụng email gây thiệt hại cho trường thì phải bồi thường theo mức độ vi phạm.

3/ Đối với thông tin thể hiện bằng cơ sở dữ liệu

a/ Thông tin được tạo ra từ các phần mềm ứng dụng chuyên môn đang được áp dụng tại trường sẽ được quản lý qua các hệ cơ sở dữ liệu;

b/ Các thông tin thể hiện bằng cơ sở dữ liệu phải được lưu trữ tập trung trên hệ thống máy chủ của trường;

c/ Không ai được tự ý can thiệp vào thông tin cơ sở dữ liệu khi không được phép;

d/ Tùy theo chức danh, CBNV được cấp quyền truy cập với các mức độ khác nhau vào các hệ thống cơ sở dữ liệu (xem toàn bộ, một phần, chỉnh sửa...). Việc cấp quyền truy cập được thực hiện dựa vào sự phê duyệt của cấp thẩm quyền tại trường hoặc người được ủy quyền khi thiết lập hệ thống cơ sở dữ liệu hoặc trong quá trình thực hiện công việc;

e/ CBNV chỉ được truy cập vào hệ thống cơ sở dữ liệu khi sử dụng máy tính do trường cấp hoặc chấp nhận sử dụng tại trụ sở và các địa điểm trực thuộc. Các trường hợp khác phải được sự đồng ý của cấp thẩm quyền tại trường;

4. Đối với thông tin thể hiện qua hình ảnh, video, audio, học liệu, nội dung thương hiệu

a/ Thông tin được tạo từ hình ảnh, nội dung, tư liệu... liên quan đến trường được quản lý theo quy định;

b/ Những thông tin thể hiện qua hình ảnh sẽ được lưu trữ và quản lý trên hệ thống máy chủ.

Điều 10. Tuân thủ bản quyền phần mềm

1. Tiêu chuẩn cài đặt phần mềm ứng dụng

1.1 Đối với CBNV thông thường (không sử dụng phần mềm chuyên ngành):

a/ Hệ điều hành window có bản quyền;

b/ Bộ ứng dụng văn phòng có bản quyền (Microsoft office);

c/ Bộ gõ chữ tiếng việt và font chữ miễn phí;

d/ Phần mềm quét virus có bản quyền;

e/ Phần mềm hỗ trợ đọc pdf bản miễn phí;

f/ Phần mềm hỗ trợ in file pdf bản miễn phí (do pdf, foxit reader,...);

g/ Phần mềm nén và giải nén file bản miễn phí;

h/ Các phần mềm hỗ trợ đọc các dạng file bản miễn phí;

i/ Phần mềm hỗ trợ in ấn theo thiết bị.

1.2 Đối với CBNV cần sử dụng phần mềm chuyên ngành:

a/ Ngoài các phần mềm quy định tại điểm a khoản 1 Điều này, được cài đặt thêm các phần mềm chuyên ngành hỗ trợ nghiệp vụ;

b/ Việc cài đặt phần mềm hỗ trợ nghiệp vụ phải được cấp thẩm quyền tại trường phê duyệt về chi phí, mua bản quyền trước khi được cài đặt vào máy tính sử dụng.

1.3 Đối với CBNV cần sử dụng phần mềm nghiệp vụ:

a/ Ngoài các phần mềm quy định tại điểm a khoản 1 Điều này được cài đặt thêm các phần mềm khách (client) nhằm kết nối đến máy chủ ứng dụng theo yêu cầu của ứng dụng nghiệp vụ đó;

b/ Đối với các ứng dụng chạy trên trình duyệt website sẽ phải có sự kiểm tra về an ninh, chứng thực trước khi cho phép kết nối đến máy chủ ứng dụng.

2. Quy định về rà soát và kiểm soát phần mềm bản quyền

a/ Hệ thống máy tính của CBNV phải được kết nối với AD và áp dụng các chính sách và quyền hạn cho từng người dùng cuối.

b/ CBNV không được tự ý cài đặt các phần mềm vào trong máy tính cá nhân của mình. Khi có nhu cầu cài đặt phần mềm khác với các tiêu chuẩn cài đặt quy định tại khoản 1 Điều này, CBNV phải làm phiếu đề xuất nói rõ nhu cầu và chi phí kèm theo và phải được cấp thẩm quyền tại trường phê duyệt thực hiện.

c/ Tất cả các phần mềm không nằm trong các tiêu chuẩn quy định tại khoản 1 Điều này phải được sao lưu dữ liệu (nếu có) và tiến hành xóa bỏ khỏi hệ thống CĐHĐN.

d/ Việc thực hiện rà soát các phần mềm ứng dụng phải được thực hiện mỗi quý 1 lần và gửi kết quả rà soát báo cáo về TCHC & QT.

CHƯƠNG III. TRÁCH NHIỆM CỦA CÁC ĐƠN VỊ

Điều 11. Đơn vị phụ trách Hệ Thống Cơ sở Hạ Tầng

1. Đảm bảo Hệ thống CĐHĐN được vận hành liên tục, trừ những trường hợp dừng hệ thống để bảo trì, sửa chữa, nâng cấp.

2. Hướng dẫn xây dựng hệ thống cơ sở hạ tầng đúng tiêu chuẩn kỹ thuật.

3. Đào tạo hướng dẫn IT trong việc thao tác và sử dụng Hệ thống CĐHĐN theo đúng các quy chuẩn để khai thác tối đa giá trị của hệ thống.

4. Thiết lập cơ chế phân quyền, quản lý việc truy cập hệ thống đảm bảo tính bảo mật, an toàn.

5. Xây dựng các biện pháp hỗ trợ để duy trì tính ổn định về hệ thống, an toàn về dữ liệu trong suốt quá trình hoạt động.

Điều 12. Đơn vị phụ trách Phát triển ứng dụng

1. Xây dựng và phát triển hệ thống ứng dụng theo đúng định hướng chiến lược CĐHĐN của trường.
2. Đảm bảo tính tiện ích, hiệu quả trong việc ứng dụng công nghệ thông tin tại các đơn vị
3. Hướng dẫn người dùng cuối trong việc khai thác và sử dụng hiệu quả ứng dụng
4. Thiết lập cơ chế phân quyền, quản lý trên hệ thống ứng dụng đảm bảo tính bảo mật, an toàn.

Điều 13. Đơn vị phụ trách Nhân sự

Khi tiến hành tuyển dụng nhân sự IT, Đơn vị phụ trách Nhân sự ĐHĐN là phòng TCHC & QT tiến hành phối hợp phỏng vấn tuyển dụng, đánh giá chất lượng nhân sự theo lĩnh vực chuyên môn phụ trách.

Điều 14. Đơn vị phụ trách Thiết bị

1. Bảo quản tài sản liên quan đến CĐHĐN theo quy định.
2. Khi tiến hành mua sắm các tài sản liên quan đến Hệ thống CĐHĐN, cần thông báo và phối hợp đánh giá trước khi tiến hành mua sắm.
3. Phối hợp với IT gửi thông báo cho TCHC & QT kết quả kiểm kê đánh giá tài sản CĐHĐN theo kế hoạch hoặc trước khi thực hiện thanh lý tài sản CĐHĐN.

CHƯƠNG IV. THỰC HIỆN QUẢN LÝ HỆ THỐNG CĐHĐN

Điều 15. Tiêu chuẩn cơ sở hạ tầng hệ thống CĐHĐN tại ĐHĐN

1. Tiêu chuẩn hạ tầng mạng tại ĐHĐH phải thực hiện theo quy định tại Phụ lục
2. Tiêu chuẩn hạ tầng hệ thống
 - 2.1 Mô hình hệ thống máy chủ và kỹ thuật: ĐHĐN phải thực hiện theo quy định tại Phụ lục 1.
 - 2.2 Tiêu chuẩn thiết bị công nghệ thông tin dùng cho văn phòng:
 - a/ Trang bị máy vi tính xách tay (Laptop):
 - Tính chất:
 - + Cấp cố định theo tính chất công việc thường xuyên công tác ngoài, hoặc theo tính chất đối ngoại;
 - + Cấp tạm thời có thời hạn theo tính chất công việc không thường xuyên công tác ngoài hoặc công tác đột xuất.
 - Kỹ thuật:
 - + Máy vi tính xách tay phải được cài hệ điều hành window có bản quyền đi kèm theo máy;
 - + Máy vi tính xách tay phải được bảo trì định kỳ theo kế hoạch.
 - Đối tượng được trang bị:

+ Các nhân sự đảm nhiệm chức danh quản lý theo hệ thống chức danh của ĐHĐN

+ Cấp theo tính chất đặc thù công việc phải có sự phê duyệt của cấp thẩm quyền tại ĐHĐN

- Tiêu chuẩn:

+ Máy vi tính xách tay có cấu hình phục vụ công việc đặc thù được cấp phát cho các công việc cần tốc độ, khả năng xử lý cao:

Bộ xử lý: trang bị vi xử lý thế hệ mới nhất tương ứng với công nghệ hiện có tại từng thời điểm;

Bộ nhớ tối thiểu: 4GB Ram;

Dung lượng cài đặt hệ điều hành: tối thiểu 100GB;

Dung lượng lưu trữ: đáp ứng nhu cầu lưu trữ công việc, tối thiểu 500GB, trang bị HDD;

Card đồ họa: trang bị Card đồ họa rời thế hệ mới nhất tương ứng với công nghệ hiện có tại từng thời điểm. Chọn Card đồ họa có GPU càng cao thì tốc độ xử lý đồ họa càng tốt.

+ Máy vi tính xách tay có cấu hình phục vụ công việc văn phòng được cấp phát cho các công việc cần tốc độ, khả năng xử lý bình thường:

Bộ xử lý: trang bị vi xử lý thế hệ mới nhất tương ứng với công nghệ hiện có tại từng thời điểm;

Bộ nhớ tối thiểu: 4GB Ram;

Dung lượng cài đặt hệ điều hành: tối thiểu 100GB;

Dung lượng lưu trữ: đáp ứng nhu cầu lưu trữ công việc, tối thiểu 500GB.

+ Tiêu chuẩn khác: được sự phê duyệt của cấp thẩm quyền tại ĐHĐN và sự tham mưu của TCHC & QT.

b/Trang bị máy vi tính để bàn (Desktop):

- Tính chất:

+ Cấp cố định theo tính chất công việc văn phòng;

+ Cấp tạm thời có thời hạn thu hồi theo tính chất công việc theo thời vụ hoặc tạm thời.

- Kỹ thuật:

+ Máy vi tính để bàn tùy theo tính chất công việc sẽ được cài đặt các phần mềm phù hợp công việc;

+ Máy vi tính để bàn do ĐHĐN cấp phát sẽ được bảo trì định kỳ theo quy trình bảo trì, sửa chữa.

- Đối tượng được trang bị:

+ CBNV theo tính chất công việc văn phòng (trừ những vị trí đã cấp máy vi tính xách tay);

+ Các trường hợp khác: căn cứ vào bản mô tả công việc, tính chất công việc hiện hành, cộng tác viên, thực tập... và được sự phê duyệt của Cấp thẩm quyền tại ĐHĐN.

- Tiêu chuẩn:

+ Máy vi tính để bàn có cấu hình phục vụ công việc đặc thù được cấp phát cho các công việc cần tốc độ, khả năng xử lý cao.

Bộ xử lý: trang bị vi xử lý thế hệ mới nhất tương ứng với công nghệ hiện có tại từng thời điểm;

Bộ nhớ tối thiểu: 8GB Ram;

Dung lượng cài đặt hệ điều hành: tối thiểu 100GB, yêu cầu SSD;

Dung lượng lưu trữ: đáp ứng nhu cầu lưu trữ công việc, tối thiểu 500GB;

Card đồ họa: trang bị Card đồ họa rời thế hệ mới nhất tương ứng với công nghệ hiện có tại từng thời điểm. Chọn Card đồ họa có GPU càng cao thì tốc độ xử lý đồ họa càng tốt.

+ Máy vi tính để bàn có cấu hình phục vụ công việc văn phòng được cấp phát cho các công việc cần tốc độ, khả năng xử lý bình thường.

Bộ xử lý: trang bị vi xử lý thế hệ mới nhất tương ứng với công nghệ hiện có tại từng thời điểm;

Bộ nhớ tối thiểu: 4GB Ram;

Dung lượng cài đặt hệ điều hành: tối thiểu 100GB, yêu cầu SSD;

Dung lượng lưu trữ: đáp ứng nhu cầu lưu trữ công việc, tối thiểu 500GB, trang bị HDD.

+ Tiêu chuẩn khác: được sự phê duyệt của cấp thẩm quyền tại ĐHĐH và sự tham mưu của TCHC & QT.

b/ Trang bị các thiết bị khác:

- Máy in màu: đáp ứng khả năng in các kích thước khổ giấy A3 - A4. màu chính xác, không bị nhòe hay sai màu mực in.

- Máy in trắng đen: đáp ứng khả năng in 2 mặt, chất lượng in sạch sẽ và tiết kiệm.

- Ổ cứng di động: đáp ứng khả năng lưu trữ trong công việc, thiết kế gọn và nhẹ. Sử dụng phải tuân thủ quy định bảo mật dữ liệu của ĐHĐN

- Các thiết bị khác: tùy theo tính chất công việc.

- Những trường hợp trang bị ngoài quy định hiện hành phải có ý kiến của TCHC & QT và được sự phê duyệt của cấp thẩm quyền tại ĐHĐN.

- Việc chọn lựa thông số kỹ thuật thiết bị công nghệ thông tin phải được TCHC & QT thực hiện theo quy định hiện hành hoặc phù hợp với tình hình phát triển công nghệ thông tin của ĐHĐN.

- Việc mua sắm thiết bị công nghệ thông tin phải tuân thủ quy định trang bị này, ngoại trừ những thiết bị chưa được mô tả trong quy định và được sự xác nhận phù hợp nền tảng Hệ thống CĐHĐN ĐHĐN.

Điều 16. Quản lý thông tin truy cập hệ thống

1. Yêu cầu nghiệp vụ đối với kiểm soát truy cập

a/ Quản lý truy cập đối với người sử dụng, nhóm người sử dụng, đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn, bảo mật gồm các nội dung cơ bản sau:

b/ Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng;

c/ Giới hạn và kiểm soát các truy cập đặc quyền;

d/ Quản lý, cấp phát mật khẩu;

e/ Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng.

f/ Quản lý mật khẩu phải đáp ứng các yêu cầu sau:

g/ Mật khẩu phải có độ dài sáu ký tự trở lên;

h/ Các mật khẩu mặc định của nhà sản xuất cài đặt sẵn trên các trang thiết bị, phần mềm, cơ sở dữ liệu phải được thay đổi ngay khi đưa vào sử dụng.

i/ Quản lý trách nhiệm người sử dụng gồm: Sử dụng mật khẩu đúng quy định, giữ bí mật mật khẩu, thoát khỏi hệ thống khi không làm việc trên hệ thống hoặc tạm thời không làm việc trên hệ thống.

2. Quản lý truy cập mạng

a/ Quản lý sử dụng mạng và các dịch vụ mạng; các thủ tục cấp phép, xóa bỏ quyền kết nối trên mạng và dịch vụ mạng; những cách thức, phương tiện truy cập mạng, dịch vụ mạng. Bao gồm:

b/ Các mạng và dịch vụ mạng được phép sử dụng;

c/ Các điều kiện để được kết nối mạng.

d/ Sử dụng các biện pháp thích hợp để xác thực người sử dụng kết nối từ bên ngoài vào mạng nội bộ đảm bảo an toàn, bảo mật.

e/ Kiểm soát truy cập các cổng dùng để cấu hình và quản trị thiết bị mạng.

f/ Chia tách hệ thống mạng thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin.

3. Kiểm soát truy cập hệ điều hành

a/ Kiểm soát truy cập hệ điều hành; quy định quản lý mật khẩu truy cập hệ điều hành an toàn, bảo mật.

b/ Mỗi người sử dụng hệ điều hành phải có một định danh duy nhất và được xác thực, nhận dạng, lưu dấu vết khi truy cập hệ điều hành.

c/ Quy định giới hạn và kiểm soát chặt chẽ những tiện ích hệ thống có khả năng ảnh hưởng đến hệ thống và chương trình ứng dụng khác.

d/ Tự động ngắt phiên làm việc sau một thời gian không sử dụng, nhằm ngăn chặn sự truy cập trái phép.

e/ Quy định giới hạn thời gian kết nối với những ứng dụng có độ rủi ro cao.

f/ Kiểm soát truy cập thông tin và ứng dụng

g/ Quản lý và phân quyền truy cập thông tin và ứng dụng phù hợp với chức năng nhiệm vụ của người sử dụng:

h/ Phân quyền truy cập đến từng thư mục, chức năng của chương trình;

i/ Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.

j/ Các hệ thống thông tin quan trọng phải đặt trong môi trường mạng máy tính riêng. Nếu các hệ thống thông tin cùng sử dụng nguồn tài nguyên chung thì phải được người quản trị hệ thống chấp nhận.

Điều 17. Quản lý vận hành hệ thống ứng dụng

1. Mô hình ứng dụng

Ứng dụng được thiết kế theo mô hình phục vụ khách/ chủ (MVC.MVP,MVVM).

a/ Ứng dụng có thể được cài đặt trên một hoặc nhiều máy chủ, tùy theo mô hình thực tế và mức độ yêu cầu của phần mềm.

b/ Ứng dụng nếu có cơ sở dữ liệu, thì từ người dùng không được phép kết nối trực tiếp đến cơ sở dữ liệu mà phải qua lớp ứng dụng người dùng.

c/ Quy hoạch rõ ràng các môi trường hoạt động cho hệ thống ứng dụng: môi trường phát triển môi trường kiểm tra, môi trường vận hành.

d/ Các ứng dụng phải được quy hoạch cài đặt trên các môi trường khác nhau theo các chức năng và phạm vi của từng ứng dụng theo từng giai đoạn.

e/ Tài liệu và phiên bản ứng dụng, phần mềm ứng dụng phải có tài liệu cài đặt, các phiên bản cùng tính năng của mỗi phiên bản.

f/ Tài liệu vận hành phải rõ ràng, chi tiết để người vận hành có thể hiểu rõ trong quá trình hoạt động, tránh xảy ra sai sót.

g/ Tài liệu xử lý các trường hợp hỗ trợ thường gặp cho mỗi phiên bản.

h/ Sau khi ứng dụng hoàn thành triển khai phải được đóng gói và chuyển lên môi trường vận hành để quản lý. Mỗi thay đổi, cập nhật mới khi đưa lên môi trường vận hành sẽ được xem như một phiên bản của ứng dụng đó.

2. Tính sẵn sàng và khả năng chịu lỗi của ứng dụng

a/ Phần mềm ứng dụng phải đảm bảo tính sẵn sàng cao, khả năng chịu lỗi, nhằm giảm thiểu thời gian ngưng phục vụ của ứng dụng.

b/ Phải xây dựng quy trình vận hành cho từng ứng dụng tránh sai sót có thể xảy ra làm ảnh hưởng đến hoạt động của ứng dụng.

3. Bảo mật

a/ Xây dựng các cơ chế chứng thực người dùng trên từng ứng dụng.

b/Dữ liệu đến người dùng phải đảm bảo được mã hóa từ lớp cơ sở dữ liệu.

4. Bảo trì ứng dụng

c/ Các ứng dụng khi có nhu cầu bảo trì hoặc xử lý lỗi trong quá trình vận hành, cần tuân thủ quy định vận hành ứng dụng.

d/Nhật ký bảo trì, xử lý lỗi phải được cập nhật nhật ký hệ thống.

5. Sao lưu phục hồi ứng dụng

a/ Phần mềm ứng dụng phải được sao lưu thường xuyên, và định kỳ phục hồi trên hệ thống giả lập để kiểm tra tính khả dụng của dữ liệu sao lưu.

b/ Dữ liệu sao lưu bao gồm: cơ sở dữ liệu, cấu hình ứng dụng, hệ điều hành máy chủ ứng dụng.

c/ Tham khảo thêm quy định sao lưu/phục hồi dữ liệu.

6. Kiểm tra đánh giá

Các ứng dụng cần phải kiểm tra đánh giá, xác nhận trước khi chuyển lên môi trường vận hành chính thức.

Điều 18. Sao lưu và phục hồi dữ liệu

1. Hệ thống máy chủ dữ liệu

a/ Hệ thống máy chủ dữ liệu được truy cập tại địa chỉ:

b/ Ổ đĩa mạng chung ĐHĐN (lưu trữ dữ liệu chung của ĐHĐN):

WTen may chu\datacenter\DU LIEU CHUNG;

c/ Ổ đĩa mạng chung Đơn vị (lưu trữ dữ liệu của Đơn vị):

WTen may chu\datacenter\Ten Don vi;

d/Ổ đĩa mạng chung Khối (lưu trữ dữ liệu của Khối): \\Ten_may_chu\datacenter\Ten_khoi;

e/Ổ đĩa mạng cá nhân (lưu trữ dữ liệu của riêng từng cá nhân):

\\Ten_may_chu\userdriver\Ten_dang_nhap (sẽ giống phần tên đăng nhập vào mạng).

Hạng mục này sẽ mở theo nhu cầu chứ mặc định sẽ không cung cấp.

f/ Quyền truy cập:

g/Tại thư mục [Dữ liệu chung]: phạm vi truy cập thư mục này là toàn thể CBNV có tài khoản truy cập hệ thống, nên dữ liệu lưu trữ tại đây là những dữ liệu mang tính chất phổ biến rộng rãi;

h/ Tại thư mục [Tên Khối]: phạm vi truy cập thư mục này là toàn thể CBNV thuộc Khối, dữ liệu lưu trữ tại đây là những dữ liệu mang tính chất phổ biến trong phạm vi Khối;

i/ Tại thư mục [Tên Đơn vị]: phạm vi truy cập thư mục này là các CBNV trong cùng Đơn vị, nên dữ liệu lưu trữ tại đây mang tính chất bảo mật cấp Đơn vị;

j/ Tại thư mục [Cá nhân]: phạm vi truy cập thư mục này là tương ứng với mỗi CBNV, nên dữ liệu lưu trữ tại đây mang tính chất bảo mật cấp cá nhân từng CBNV;

k/ CBNV có nhu cầu truy cập vào dữ liệu của Khối/Đơn vị khác thì phải được sự phê duyệt của cấp thẩm quyền tại ĐHĐN.

2. Lưu trữ dữ liệu trên hệ thống máy chủ

a. Toàn bộ dữ liệu công việc, dữ liệu hệ thống phải được lưu trữ tập trung trên ổ đĩa mạng, không được lưu trữ trên máy tính làm việc hoặc máy tính cá nhân.

b. Mỗi đơn vị được cung cấp một thư mục chung, với tên trùng tên Đơn vị, trên hệ thống máy chủ dữ liệu. Chỉ có các thành viên thuộc Đơn vị đó mới có thể truy cập dữ liệu.được lưu trữ trong thư mục chung này. Dữ liệu của CBNV nào trong Đơn vị lưu trữ trên thư mục chung này thì chỉ có CBNV đó mới được quyền xóa hoặc đổi tên (rename).

c. Trong trường hợp các Đơn vị được tổ chức trong một Khối thì được lập thư mục dùng chung cho Khối. Các CBNV của Khối được quyền truy cập và lưu trữ dữ liệu tương tự như thư mục dùng chung cho Đơn vị.

d. Mỗi CBNV được cung cấp một thư mục riêng, với tên tương ứng tên đăng nhập hệ thống mạng, trên hệ thống máy chủ dữ liệu. Chỉ có CBNV đó mới có quyền truy cập và lưu trữ dữ liệu trên thư mục của mình.

e. Đối với máy vi tính đã tham gia hệ thống mạng nội bộ, khi đăng nhập máy vi tính, hệ thống sẽ tự động tạo các ổ đĩa mạng tương ứng với quyền truy cập của từng CBNV. Đối với máy vi tính chưa tham gia hệ thống mạng, CBNV truy cập theo địa chỉ hệ thống máy chủ dữ liệu bằng tài khoản truy cập hệ thống của mình.

f. Tổng dung lượng lưu trữ: bao gồm toàn bộ dung lượng mà CBNV sử dụng trên máy chủ. Định mức được quy định như sau nhưng có thể thay đổi theo tính chất công việc và phê duyệt của cấp thẩm quyền tại ĐHĐN:

- i. Ban Giám Hiệu được quyền lưu trữ dữ liệu với tổng dung lượng là 10 GB;
- ii. Trưởng Đơn vị được quyền lưu trữ dữ liệu với tổng dung lượng là 03 GB;
- iii. Mỗi CBNV được quyền lưu trữ dữ liệu với tổng dung lượng là 02 GB.

1. Quy định về bảo mật dữ liệu sao lưu

- a. Dữ liệu công việc: dữ liệu trên máy chủ chia sẻ tập tin, do Đơn vị hoặc cá nhân trong ĐHĐN tạo ra. Quyền tiếp cận dữ liệu này sẽ do Đơn vị, cá nhân đó quyết định. Trường hợp nhân sự nghỉ việc phải tuân thủ quy định quản lý thông tin truy cập hệ thống.
- b. Dữ liệu hệ thống: chỉ IT ĐHĐN được Trưởng phòng QTTT cấp quyền mới có quyền tiếp cận dữ liệu sao lưu trên các phương tiện lưu trữ. Đơn vị khác chỉ có quyền tiếp cận khi Cấp thẩm quyền tại ĐHĐN phê duyệt.

2. Lưu giữ, bảo mật các bản sao lưu dữ liệu

- a. Yêu cầu chung:
 - i. Mỗi phương tiện lưu trữ phải được dán nhãn, mã số ghi thông tin rõ ràng thuận tiện cho việc quản lý;
 - ii. Các bản sao lưu sẽ được lưu giữ tập trung do Đơn vị quản lý công nghệ thông tin quản lý theo cách phù hợp. Tùy theo mức độ quan trọng, các bản sao lưu phải được làm thành nhiều bản giống nhau và lưu giữ ít nhất là hai nơi có địa điểm vật lý cách nhau, trong khu vực có điều kiện nhiệt độ thích hợp và trong các thiết bị an toàn đảm bảo tính toàn vẹn của các bản sao lưu;
 - iii. Quy trình lưu giữ và ghi nhận các bản sao lưu do nhóm phụ trách sao lưu dữ liệu thuộc Đơn vị quản lý công nghệ thông tin lập và cập nhật;
 - iv. Dữ liệu hệ thống sao lưu được tập hợp lưu trữ theo từng năm.
- b. Sử dụng khu vực và thiết bị an toàn khẩn cấp: cấp thẩm quyền sẽ chỉ định khu vực và thiết bị dữ liệu khẩn cấp để lưu giữ các bản sao lưu. Những nơi này phải đáp ứng được các tiêu chuẩn về bảo mật và an toàn theo quy định.
- c. Kiểm tra và loại bỏ các phương tiện lưu trữ

- i. Đơn vị quản lý công nghệ thông tin cần kiểm tra định kỳ sự thành công của việc phục hồi dữ liệu từ các bản sao lưu được lưu giữ lâu dài và có biên bản ghi nhận việc kiểm tra dựa trên quy định phục hồi dữ liệu;
- ii. Việc kiểm tra phục hồi này được thực hiện trên một môi trường thử nghiệm;
- iii. Sau khi hết thời hạn lưu giữ bản sao lưu, phương tiện lưu trữ (băng từ (magnetic tape), USB, DVD...) có thể được sử dụng lại hoặc hủy bỏ theo phê duyệt của cấp thẩm quyền.

Điều 19. Hỗ trợ người dùng hệ thống CDHĐN

1. Người dùng có quyền yêu cầu hỗ trợ các vấn đề hệ thống CDHĐN.
2. Việc yêu cầu hỗ trợ thông qua một trong ba hình thức sau:
 - a. Gửi email qua địa chỉ hotro@ĐHĐN.edu.vn;
 - b. Gọi điện thoại cho Đơn vị phụ trách Hỗ trợ CDHĐN;
 - c. Gặp trực tiếp cán bộ hỗ trợ để đặt ra các yêu cầu.
3. Các trường hợp yêu cầu hỗ trợ phải được đánh mã số và ghi nhận trên hệ thống hỗ trợ CDHĐN.
4. Đơn vị phụ trách Hỗ trợ CDHĐN có quyền từ chối các yêu cầu hỗ trợ không liên quan đến nghiệp vụ chuyên môn. các yêu cầu hỗ trợ mang tính chất cá nhân không phục vụ cho công việc.
5. Các yêu cầu hỗ trợ có tính chất ảnh hưởng đến hoạt động chung, cần phải lập Phiếu/ email và phải được cấp thẩm quyền tại ĐHĐN phê duyệt.

Điều 20. Bảo trì thiết bị CDHĐN

1. Việc bảo trì thiết bị Công nghệ thông tin được thực hiện định kỳ 2 lần/năm vào Quý II và Quý IV hàng năm.
2. Trước khi tiến hành bảo trì thiết bị Công nghệ thông tin cần tổ chức đánh giá tình trạng thiết bị CDHĐN và lập kế hoạch bảo trì cụ thể.
3. Biễn bản đánh giá tình trạng thiết bị cần có sự xác nhận của Đơn vị/ cá nhân sử dụng thiết bị đó.
4. Sau khi tiến hành bảo trì thiết bị cần lập bảng đánh giá tình trạng thiết bị sau bảo trì có xác nhận giữa các bên. Tiến hành cập nhật và lưu lại hồ sơ theo dõi tình thiết bị CDHĐN theo quy định.

Điều 21. Quản lý các sự cố về CDHĐN

I. Báo cáo sự cố

- a. Xây dựng quy trình báo cáo, các mẫu báo cáo và xác định rõ người nhận báo cáo về các sự cố CDHĐN.
- b. Quy định rõ trách nhiệm báo cáo của CBNV và bên thứ ba về các sự cố CDHĐN.
 1. Các sự cố mất an toàn phải được lập tức báo cáo đến cấp thẩm quyền và những người có liên quan để có biện pháp khắc phục trong thời gian sớm nhất. Kiểm soát và khắc phục sự cố

- a. Ban hành quy trình, trách nhiệm khắc phục và phòng ngừa sự cố CDHĐN, đảm bảo sự cố được xử lý trong thời gian ngắn nhất và giảm thiểu khả năng sự cố lặp lại.
- b. Quá trình xử lý sự cố phải được ghi chép và lưu trữ.
- c. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố về CNTT có liên quan đến các vi phạm pháp luật, ĐHĐN có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

Điều 22. Quản lý phòng máy chủ

1. Quy định chung về cơ sở hạ tầng
 - a. Phòng máy chủ phải luôn được đảm bảo cung cấp liên tục các nguồn điện cho tất cả các thiết bị thuộc phạm vi của nó.
 - b. Nhiệt độ phòng máy chủ phải được đảm bảo thích hợp cho các máy chủ hoạt động hiệu quả, an toàn.
 - c. Phòng máy chủ phải được cung cấp ánh sáng thích hợp và luôn được giữ vệ sinh sạch sẽ. Các đồ đạc, dụng cụ phải được sắp xếp ngăn nắp gọn gàng.
 - d. Phải luôn đảm bảo an toàn về cháy nổ cho phòng máy chủ.
 - e. Phải có thiết bị chống sét trực tiếp và chống sét lan truyền cho các thiết bị trong phòng máy chủ
 - f. Các thiết bị và các dây kết nối trong phòng máy chủ phải luôn được dán nhãn in chữ rõ ràng và phải được bố trí gọn gàng.
2. Quy định chung về an ninh
 - a. Phòng máy chủ phải được quản lý kiểm soát an ninh tiếp cận ra vào.
 - b. Cá nhân tiếp cận phòng máy chủ phải được phân quyền hạn, trách nhiệm rõ ràng.
 - c. Phải có nhật ký theo dõi vào ra phòng máy chủ.
 - d. Phải quản lý danh sách những người được quyền tiếp cận phòng máy chủ.

CHƯƠNG V. ĐIỀU KHOẢN THI HÀNH

Điều 23. Trách nhiệm thi hành

1. P. TCHC & QT làm đầu mối triển khai, hướng dẫn thực hiện và tuân thủ quy trình này.
2. Giao Ban Giám Hiệu ban hành các quy định, quy trình mẫu để hướng dẫn ĐHĐN thực hiện Quy trình này.

Điều 24. Thẩm quyền sửa đổi, bổ sung, thay thế, hủy bỏ

Việc sửa đổi, bổ sung, thay thế, hủy bỏ Quy trình này thuộc thẩm quyền của Ban Giám Hiệu.

Danh mục Phụ lục, Biểu mẫu liên quan

STT	TÊN	MÃ SỐ
1.	Phụ lục 01: Tiêu chuẩn cơ sở hạ tầng hệ thống CĐHĐN tại ĐHĐN	CĐHĐN/QC-01/PL01
2.	Báo cáo kiểm tra	CĐHĐN/QC-01/M01
3.	Biên bản sao lưu dữ liệu	CĐHĐN/QC-01/M02

PHỤ LỤC 1

TIÊU CHUẨN CƠ SỞ Hạ Tầng Hệ Thống CĐHĐN TẠI ĐHĐN

I. TIÊU CHUẨN Hạ Tầng Mạng

I. Phân loại mô hình hệ thống CĐHĐN

Xem xét đồng thời cả 2 điều kiện:

- a. Theo phân cấp tổ chức:
 - i. Lớp A: chủ thể cơ sở chính được xác định là gốc, giữ cấp cao nhất trong phân cấp quan hệ phụ thuộc dựa theo sơ đồ tổ chức.
 - ii. Lớp B: các Đơn vị, chi nhánh được xác định là nhánh, chịu sự quản lý bởi các cấp bên trên dựa theo sơ đồ tổ chức.
- b. Theo quy mô tổ chức:
 - i. Nhóm 1 - Quy mô lớn: các chi nhánh, văn phòng, cơ sở có số lượng CBNV sử dụng máy tính thường xuyên từ 200 người dùng trở lên.
 - ii. Nhóm 2 - Quy mô vừa và nhỏ: các chi nhánh, văn phòng, cơ sở có số lượng CBNV sử dụng máy tính thường xuyên dưới 200 người dùng.

Ma trận tham chiếu phân cấp mô hình hệ thống CĐHĐN

Quy mô Phân cấp	Nhóm 1	Nhóm 2
Lớp A	A1 - Quy mô lớn	A2 - Quy mô vừa & nhỏ
Lớp B	BI - Quy mô lớn	B2 - Quy mô vừa & nhỏ

2. Yêu cầu về đường truyền

- a. Đường truyền Internet: áp dụng cho tất cả mô hình toàn trường - yêu cầu tối thiểu phải có hai đường kết nối riêng biệt từ hai nhà cung cấp dịch vụ khác nhau với thước đo tổng băng thông các đường truyền không thấp hơn một nửa số lượng CBNV/SV sử dụng Internet thường xuyên tại Đơn vị.
- b. Đường truyền số liệu:
 - i. Nhóm 1: yêu cầu tối thiểu phải có một đường truyền số liệu từ một nhà cung cấp dịch vụ lớn tại Việt Nam, băng thông đường truyền phải đảm bảo đáp ứng đồng thời 100% nhu cầu sử dụng các dịch vụ như Video Conference, phần mềm QLĐT, nhập liệu từ xa & các ứng dụng khác (dựa trên số liệu tham chiếu cụ thể từ IT - ĐHĐN/Đơn vị PTCSHT).
 - ii. Nhóm 2: yêu cầu tối thiểu phải có một đường truyền số liệu từ một nhà cung cấp dịch vụ lớn tại Việt Nam, băng thông đường truyền phải đảm bảo đáp ứng đồng thời 60% nhu cầu sử dụng các dịch vụ như Video Conference, phần mềm QLĐT, nhập liệu từ xa & các ứng dụng khác (dựa trên số liệu tham chiếu cụ thể từ IT - ĐHĐN/Đơn vị PTCSHT).
- c. Các nhu cầu phát sinh băng thông đường truyền:
 - i. Đối với đường truyền Internet: yêu cầu nâng cấp băng thông đường truyền Internet phải dựa trên cơ sở số lượng CBNV/SV có nhu cầu sử

dụng Internet thường xuyên tại cơ sở, IT ĐHDN phải đánh giá và lập báo cáo hiện trạng làm cơ sở đề xuất.

- ii. Đối với đường truyền số liệu: ĐHDN khi có nhu cầu như triển khai ứng dụng mới cần chạy nội bộ, phát sinh điểm kết nối Video Conference, ... IT ĐHDN liệt kê chi tiết, yêu cầu kỹ thuật và lập báo cáo bằng thông hiện trạng, bằng thông phát sinh khi thử nghiệm ứng dụng mới để làm cơ sở đề xuất nâng băng thông.

3. Yêu cầu về thiết bị

a. Theo tiêu chí phân cấp:

- i. Lớp A: đảm bảo dự phòng 1-1 cho tất cả các hạng mục thiết bị mạng.
- ii. Lớp B: đáp ứng tối thiểu một Đơn vị thiết bị cho từng hạng mục.

- b. Theo tiêu chí quy mô: thiết bị hạ tầng mạng phải đáp ứng yêu cầu kỹ thuật về hiệu suất, tính năng và độ bền tương ứng quy mô cơ sở dựa theo phân nhóm quy định tại khoản 2 Mục A.I Phụ lục này. Cụ thể:

Nhóm 1:

Danh mục thiết bị	Cấu hình	Khả năng mở rộng
Router - Bộ định tuyến	Tối thiểu 03 cổng kết nối vật lý cho: mạng nội bộ; đường truyền và dự phòng.	Khả năng cho phép mở rộng thêm tối đa 04 cổng vật lý trong tương lai.
	Bộ nhớ RAM: tối thiểu 04 GB phục vụ cho xử lý định tuyến lưu lượng lớn.	Khả năng cho phép mở rộng tối đa 16 GB.
	Phần cứng chuyên dụng tăng hiệu suất xử lý mã hóa: DES, 3DES, AES.	
	Khe mở rộng: tối thiểu 02 khe.	Khả năng gắn mở rộng card tích hợp tính năng tổng đài thoại. Khả năng gắn card mở rộng cổng kết nối vật lý.
Core Switch - Bộ chuyển mạch lõi	24 hoặc 48 cổng vật lý kết nối.	Khả năng stacking – hợp nhất luân lý với các switch khác.
	Tối thiểu 04 slot chuyên biệt cho mục đích uplink dữ liệu.	Khả năng cho phép linh hoạt gắn nhiều loại module vật lý thay đổi tốc độ cổng uplink.
		Khả năng mở rộng: đóng vai trò Wireless Controller cho các Access Point cùng hãng.
		Khả năng mở rộng: xử lý dữ liệu NetFlow.
Access Switch - Bộ chuyên	24 hoặc 48 cổng vật lý kết nối.	Khả năng stacking - hợp nhất luân lý với các switch

mạch đầu cuối		khác.
	Tối thiểu 04 slot chuyên biệt cho mục đích uplink dữ liệu.	
Firewall - Tường lửa	Tối thiểu 24 cổng LAN vật lý.	Khả năng mở rộng lên tối đa 40 cổng LAN vật lý.
	Tối thiểu 02 cổng DMZ vật lý.	
	Tối thiểu 02 cổng WAN vật lý.	
	Ổ cứng lưu trữ dạng SSD.	
	Tối thiểu 01 nguồn.	Khả năng gắn nguồn mở rộng.
		APT, IPS, Thead prevention, Anti-virus
Link Load Balancing - Cân bằng tải	Tối thiểu 03 cổng LAN.	
	Tối thiểu 03 cổng WAN.	Khả năng gắn USB 3G mở rộng WAN.
Wifi	Đáp ứng chuẩn 802.11 a/b/g/n/ac.	
	Hoạt động ở chế độ Standalone	Khả năng mở rộng: chuyển đổi hoạt động ở chế độ Controller-based.
	Được quản lý qua controller	Áp dụng được tính năng captive portal

Nhóm 2:

Danh mục thiết bị	Cấu hình	Khả năng mở rộng
Router - Bộ định tuyến	Tối thiểu 02 cổng kết nối vật lý cho: mạng nội bộ; đường truyền và dự phòng.	Khả năng cho phép mở rộng thêm tối đa 04 cổng vật lý trong tương lai.
	Bộ nhớ RAM: tối thiểu 04 GB phục vụ cho xử lý định tuyến lưu lượng lớn.	Khả năng cho phép mở rộng tối đa 08 GB.
Router - Bộ định tuyến	Phần cứng chuyên dụng tăng hiệu suất xử lý mã hóa: DES, 3DES AES.	
	Khe mở rộng: tối thiểu 02 khe.	Khả năng gắn mở rộng card tích hợp tính năng tổng đài thoại. Khả năng gắn card mở rộng cổng kết nối vật lý.
Core Switch - Bộ chuyển mạch lõi	24 hoặc 48 cổng vật lý kết nối.	Khả năng stacking - hợp nhất luận lý với các switch khác.
	Tối thiểu 04 slot chuyên biệt cho mục đích uplink dữ liệu.	Khả năng cho phép linh hoạt gắn nhiều loại module vật lý thay đổi tốc độ cổng uplink.
		Khả năng mở rộng: đóng vai trò Wireless Controller cho các Access Point cùng hãng.
		Khả năng mở rộng: xử lý dữ liệu NetFlow.

Access Switch - Bộ chuyên mạch đầu cuối	24 hoặc 48 cổng vật lý kết nối.	Khả năng stacking - hợp nhất luận lý với các switch khác.
	Tối thiểu 04 slot chuyên biệt cho mục đích uplink dữ liệu.	
Firewall - Tường lửa	Tối thiểu 16 cổng LAN vật lý.	Khả năng mở rộng lên tối đa 40 cổng LAN vật lý.
	Tối thiểu 02 cổng DMZ vật lý.	
	Tối thiểu 02 cổng WAN vật lý.	
	Ổ cứng lưu trữ dạng SSD.	
	Tối thiểu 01 nguồn.	Khả năng gắn nguồn mở rộng.
		APT, IPS, Thead prevention, Anti-virus
Link Load Balancing - Cân bằng tải	Tối thiểu 07 cổng LAN.	Khả năng mở rộng cho phép chuyển đổi 01 cổng LAN thành cổng WAN.
	Tối thiểu 02 cổng WAN.	Khả năng gắn USB 3G mở rộng WAN.
Wifi	Đáp ứng chuẩn 802.11 a/b/g/n/ac.	
	Hoạt động ở chế độ Standalone.	Khả năng mở rộng: chuyển đổi hoạt động ở chế độ Controller-based.
	Controller	Triển khai được captive portal

c. Yêu cầu kỹ thuật thiết bị:

- i. Thiết bị định tuyến: phải đảm bảo đáp ứng hiệu suất định tuyến, khả năng mở rộng và triển khai tốt các công nghệ định tuyến phổ biến hiện nay bao gồm: OSPF, EIGRP, BGP, RIPv2; khả năng triển khai linh hoạt các công nghệ IPSec VPN phổ biến: DMVPN, MPLS VPN, GET VPN, FlexVPN, đồng thời phải tương thích ngược với các công nghệ truyền thống.
- ii. Thiết bị chuyên mạch: phải đảm bảo đáp ứng hiệu suất chuyên mạch, khả năng chia VLAN, công nghệ stacking đồng nhất khối, công nghệ trunking dựa trên chuẩn mã hóa Dot1Q và 1SL.
- iii. Thiết bị tường lửa: phải đảm bảo đáp ứng hiệu suất, khả năng nhận dạng và quản lý ứng dụng để phát hiện, phòng ngừa và ngăn chặn các mối rủi ro tiềm tàng gây nguy hại đến hệ thống mạng của Tập đoàn và của các Công ty.

iv. Thiết bị cân bằng tải: phải đảm bảo đáp ứng hiệu suất & khả năng cân bằng tải

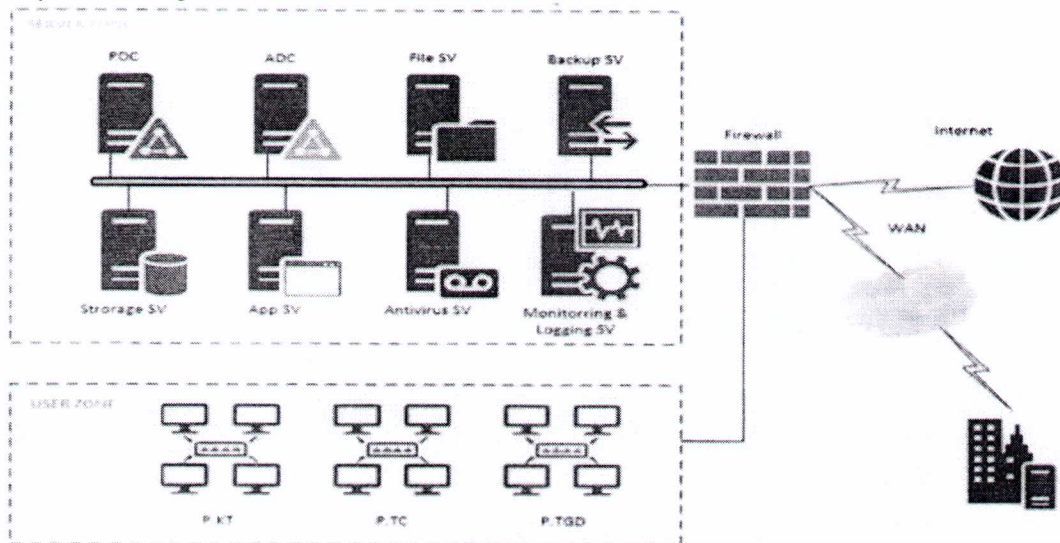
Đường truyền Internet cũng như đường truyền số liệu, tăng tính hiệu quả trong việc kết nối hạ tầng CĐHĐN tại Tập đoàn và các Công ty.

v. Thiết bị mạng không dây: đảm bảo đáp ứng hiệu suất, nhu cầu kết nối số đông người dùng, quản lý tập trung và khả năng chứng thực người dùng không dây qua các hệ thống chứng thực phổ biến như: AD, RADIUS, LDAP, Kerberos.

II. TIÊU CHUẨN HẠ TẦNG HỆ THỐNG

1. Mô hình hệ thống máy chủ

Hệ thống máy chủ được phân bổ tuân thủ mô hình sau:



Giải thích mô hình:

- Hệ thống phải được chứng thực tập trung qua Active Directory (PDC và ADC).
- Hệ thống chia sẻ tập tin nội bộ phải chứng thực qua Active Directory (File Sv).
- Hệ thống được sao lưu dự phòng qua chương trình sao lưu chuyên dụng (Backup Sv).
- Hệ thống được giám sát thường xuyên qua chương trình giám sát chuyên dụng (Monitoring & Logging Sv).
- Hệ thống được bảo vệ bởi hệ thống quản lý anti-virus tập trung, Antivirus Sv.
- Đối với các ứng dụng, sẽ tùy vào loại ứng dụng, mô hình và cách tổ chức sẽ khác nhau.

Trên đây là mô hình luận lý, về mặt vật lý, có thể gom một số tính năng chạy cùng một máy chủ.

2. Kỹ thuật

- Phân vùng: hệ thống được phân hoạch theo các phân vùng riêng biệt: phân vùng chứa máy chủ, phân vùng publish dịch vụ, phân vùng kiểm thử, phân vùng phát triển sản phẩm, phân vùng làm việc các phòng ban. phân vùng dành cho đối tượng khách/sinh viên.
- Máy chủ: trang bị những dòng máy chủ chuyên dụng, đầy đủ chứng nhận xuất xứ chứng nhận chất lượng sản phẩm. không dùng dạng lắp ráp. Đồng thời sản phẩm phải còn được hỗ trợ/sản xuất tính tại thời điểm nâng cấp/đầu tư mới. Có hỗ trợ các chuẩn RAID 1-5-6, tối thiểu 2 nguồn, 2 card mạng. Còn khe mở rộng.
- Thiết bị lưu trữ: lưu trữ qua Tape, ổ cứng USB, Server lưu trữ hoặc SAN.
- Bản quyền hệ điều hành máy chủ phải được trang bị cùng với máy, sử dụng phần mềm sao lưu phục hồi hệ thống chuyên dụng, và phải thực hiện được lúc hệ thống đang vận hành.
- Các chương trình đều được trang bị bản quyền đầy đủ.

- f. Thiết bị kết sắt chống cháy nổ, chứa dữ liệu sao lưu phải được trang bị.
- g. Bảo trì: được tổ chức định kỳ hàng năm để ghi nhận, đánh giá về tình trạng hệ thống nhằm có kế hoạch nâng cấp, thay thế.

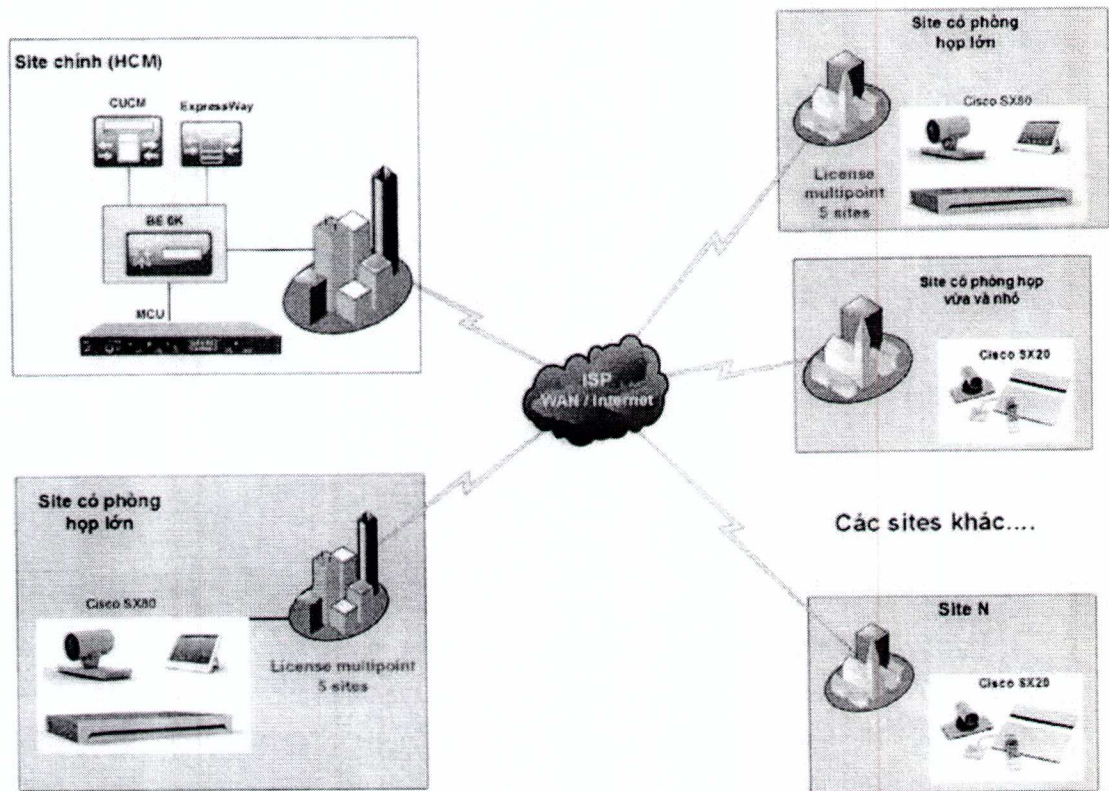
III. TIÊU CHUẨN HỆ THỐNG THIẾT BỊ HỘI NGHỊ TRUYỀN HÌNH

1. Tiêu chuẩn hạ tầng mạng

Công ty phải thực hiện theo quy định tại Phần I của Phụ lục.

2. Tiêu chuẩn hạ tầng hệ thống:

a. Mô hình kết nối



b. Tiêu chí:

i. Thiết bị:

- Thiết bị phải tương thích được với hệ thống hiện có của ĐHQG.
- Thiết bị thực hiện được cuộc gọi đa điểm (thực hiện 4 site cùng lúc).

ii. Phòng họp:

- Vị trí đặt thiết bị trên kệ đặt điểm giữa và đầu bàn họp, độ cao sao cho camera thấy được hình toàn bộ người tham dự.
- Nguồn điện 110-220 VAC.
- Màn hình LCD độ phân giải HD hoặc máy chiếu chuyên dùng.
- Nếu dùng n.323 phải cung cấp địa chỉ IP tĩnh trong mạng LAN cho thiết bị hội nghị, IP này không bị hệ thống Firewall ngăn chặn.
- Mạng LAN liên kết được với các điểm hội nghị khác thông qua mạng WAN khi sử dụng thông qua Leased Line hay VPN-MPLS.
- Yêu cầu phải có màn hình hiển thị (máy chiếu hay tivi) có giao tiếp ngõ vào hình ảnh là HDMI.

- Đầu ra âm thanh kết nối với hệ thống loa để tái tạo âm thanh trong phòng lớn và rõ ràng.
- Ánh sáng trong phòng phải đủ để camera có thể thu rõ mặt người tham dự.

c. Tiêu chuẩn:

h. Thiết bị dùng cho phòng họp có sức chứa từ 20 người trở xuống.

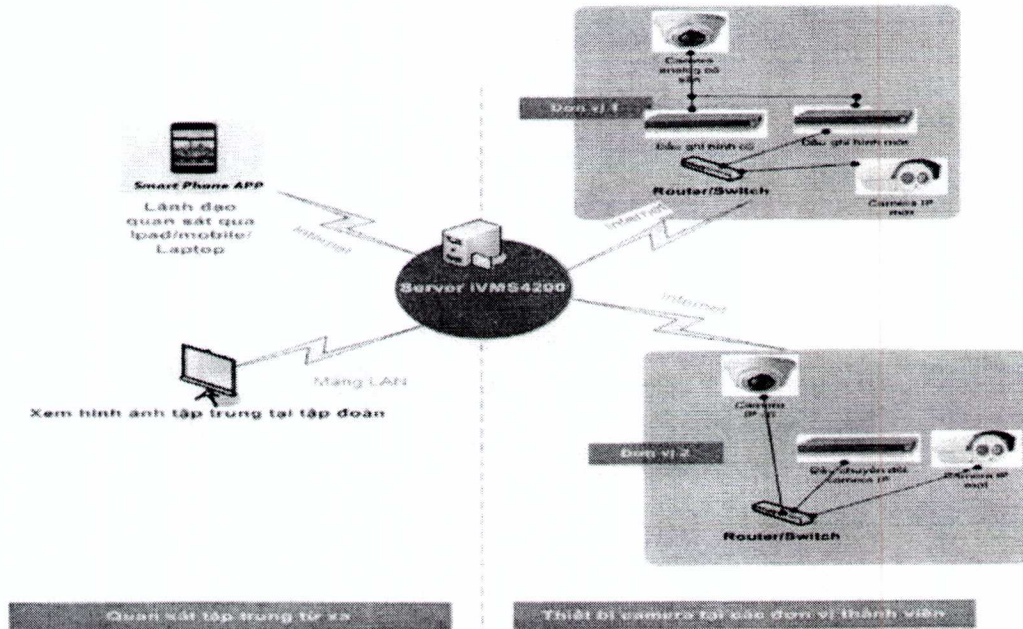
ĐẶC ĐIỂM	MÔ TẢ
Thiết kế	Giao tiếp chuẩn video HD thế hệ mới. Độ phân giải chuẩn 1080p.
Ứng dụng	Phối hợp với 4 đầu vào video đồng thời. Chuẩn H323/SIP cho cuộc gọi lên tới 10Mbs.
Băng thông	720p30 from 768 kbps. 720p60 from 1152 kbps. 1080p30 from 1472 kbps. 1080p60 from 2560 kbps.
Chuẩn Video	H.261, H.263, H.263+, H.264 and H.265.
Các chuẩn Audio	G.711, G.722, G.722.1, G.729AB. 64 kbps and 128 kbps. MPEG4 AAC-LD mono and stereo.
Giao diện mạng	One LAN/Ethernet (RJ-45) 10/100/1000 Mbit.
Camera	1 Camera thu nhận tín hiệu hình ảnh.
Micro	1 Micro thu nhận tín hiệu âm thanh.

iii. Thiết bị dùng cho phòng họp có sức chứa từ 50 người trở lên:

ĐẶC ĐIỂM	MÔ TẢ
Màn hình hiển thị	Tivi / Projector.
Thiết kế	Giao tiếp chuẩn video HD thế hệ mới. Độ phân giải chuẩn 1080p.
Ứng dụng	Phối hợp với 4 đầu vào video đồng thời. Chuẩn H323/SIP cho cuộc gọi điểm điểm lên tới 10Mbs.
Băng thông	720p30 from 768 kbps. 720p60 from 1152 kbps. 1080p30 from 1472 kbps. 1080p60 from 2560 kbps.
Chuẩn Video	H.261, H.263, H.263+, H.264 and H.265.
Các chuẩn Audio	G.711. G.722, G.722.1, G.729AB. 64 kbps and 128 kbps. MPEG4 AAC-LD mono and stereo.
Giao diện mạng	One LAN/Ethernet (RJ-45) 10/100/1000 Mbit.
Camera	2 hoặc 3 Camera thu nhận tín hiệu hình ảnh.
Micro	4 Micro thu nhận tín hiệu âm thanh.
Màn hình hiển thị	Tivi / Projector.
Loa	Phát tín hiệu âm thanh của các phòng họp từ xa.

IV. TIÊU CHUẨN HỆ THỐNG CAMERA

1. Tiêu chuẩn hạ tầng mạng:
ĐHĐN phải thực hiện theo quy định tại khoản A Phụ lục 01.
2. Tiêu chuẩn hạ tầng hệ thống:
 - a. Mô hình kết nối:



1. Phạm vi áp dụng:
Dựa theo phân loại chi nhánh/cơ sở mà có thiết bị tương thích.
2. Tiêu chí
 - a. Tích hợp được với hệ thống camera hiện tại và tích hợp hệ thống camera của cơ sở chính 300A.
 - b. Hệ thống camera giám sát được xây dựng, thiết kế phải là một hệ thống CCTV có cấu trúc mở, có khả năng đáp ứng yêu cầu mở rộng hệ thống như tăng cường thêm các điểm camera và thiết bị xử lý trung tâm mà không cần can thiệp và thay đổi các thiết bị đang hoạt động.
 - c. Hệ thống camera giám sát có khả năng nâng cấp mở rộng kết nối, tích hợp với các hệ thống camera cũ, các hệ thống camera giám sát thành một hệ thống thống nhất sau này.
 - d. Hệ thống có khả năng phân quyền, cho phép người sử dụng có thể quan sát và điều khiển các camera theo ý kiến chỉ đạo của cấp có thẩm quyền tại ĐHQĐN
 - e. Hình ảnh thu được từ hiện trường có thể được xử lý ngay hoặc được biên tập, chỉnh lý, lưu trữ phục vụ yêu cầu công tác chỉ đạo chỉ huy, nghiên cứu, đối chứng và thống kê phân tích số liệu khi cần.
 - f. Điều khiển toàn bộ hệ thống dễ dàng và nhanh chóng thông qua bàn điều khiển có cần xoay linh hoạt.
 - g. Khả năng quay ngang 3600 và nghiêng lên 2100.
 - h. Có khả năng tự động điều chỉnh độ tương phản.
 - i. Công nghệ giảm nhiễu XDNR.
 - j. Chế độ day/nigh.
 - k. Vỏ thiết bị đạt chuẩn IP66.

- l. Giải pháp hiện đại, và hiệu quả đáp ứng cho bài toán giám sát từ xa từ nhiều địa điểm trên diện rộng của ĐHĐN. Đồng thời, cho phép mở rộng các nhu cầu quản trị khác sau này mà vẫn sử dụng lại bộ thiết bị này.
- m. Giải pháp cho phép tích hợp, sử dụng lại các camera sẵn có tại các Đơn vị, quản lý tập trung.
3. Tiêu chuẩn kỹ thuật
- a. Đối với Camera dùng quan sát trong khu làm việc văn phòng.
- i. Tích hợp được với hệ thống camera hiện có của ĐHĐN.
- ii. Sử dụng các dòng camera indoor: đặt trong khu vực văn phòng không cần bảo vệ như các camera lắp tại khu xưởng/nhà kho.
- iii. Đối với Camera: dạng tròn dùng lắp đặt trên trần nhà, lắp đặt tại khu văn phòng với góc quay 360 độ, và cận cảnh khi cần thiết ở nhiều vị trí khác nhau.
- iv. Speed – Đối với Camera: cao cấp hơn, tốc độ điều khiển nhanh, lấy cận cảnh với tầm hoạt động chính xác theo từng góc. Sử dụng ở các khu vực rộng theo dõi được nhiều điểm cho từng trường hợp đối tượng và có thể nhớ nhiều vị trí góc quay thiết lập sẵn mà không cần điều khiển nhiều.
- v. IR camera: Camera hồng ngoại. Tia hồng ngoại - Infrared rays: Đối với những khu vực cần quan sát 24/24 giờ thì cần trang bị camera hồng ngoại để có thể quan sát vào ban đêm. Cần quan tâm đến những thông số sau:
- v' IR LED: Số lượng đèn LED hồng ngoại.
- s VISIBLE DISTANCE AT: Khoảng cách quan sát.
- J Nguồn điện cấp cho camera.
- vi. Resolution: Độ phân giải càng lớn thì chất lượng hình ảnh càng nét. Thường thì trong các ứng dụng không cần thiết phải quan sát thật rõ nét thì độ phân giải 480 TV Lines là hoàn toàn có thể chấp nhận được.
- vii. Góc quan sát: Trong tài liệu kỹ thuật thường không ghi góc mở, mà ghi thông số thay cho góc mở. Có thể sử dụng bảng quy đổi sau:

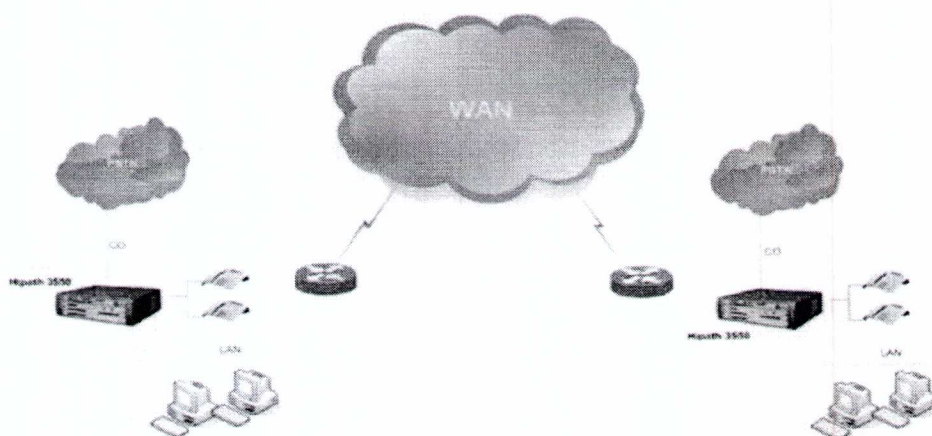
Tiêu cự	Góc mở
2.8mm	1050
3.6mm	900
4mm	850
6mm	700
8mm	550

- viii. Tùy vào ứng dụng mà nên chọn loại Camera có góc quan sát là bao nhiêu độ. Nếu cần quan sát rộng, có thể chọn loại Camera có góc mở lớn (thường là 900). Nếu quan sát trong một phạm vi rất hẹp thì chọn loại Camera có góc mở nhỏ.
- b. Đối với Camera dùng quan sát khu vực nhà máy, resort, khu vực khác có diện tích rộng/cần quan sát xa
- i. Sử dụng camera outdoor: chịu đựng được các tác động bên ngoài như độ ẩm, thời tiết, nước, bụi, hay các tác nhân phá hoại khác.
- ii. Có zoom lớn.

V. TIÊU CHUẨN HỆ THỐNG TỔNG ĐÀI

- Tiêu chuẩn hạ tầng mạng:
ĐHĐN phải thực hiện theo quy định tại khoản A Phụ lục 01.
- Tiêu chuẩn hạ tầng hệ thống:

- a. Mô hình kết nối:
- b. Phạm vi áp dụng: Dựa theo phân loại cơ sở/chi nhánh mà có thiết bị tương thích



3. Tiêu chí

- a. Có khả năng tích hợp với hệ thống tổng đài giữa các chi nhánh/cơ sở và tích hợp với hệ thống tổng đài hiện có của cơ sở chính ĐHĐN.
- b. Độ sẵn sàng, độ tin cậy cao, đảm bảo khả năng phục vụ 24/24 giờ.
- c. Có khả năng nâng cấp, mở rộng về quy mô và dịch vụ, đảm bảo khả năng khai thác lâu dài.
- d. Có khả năng tương thích và tích hợp với cơ sở hạ tầng công nghệ thông tin truyền thông
- e. Quản lý, khai thác, bảo dưỡng, bảo trì đơn giản, chi phí thấp.
- f. Chi phí đầu tư ban đầu hợp lý và được bảo toàn trong tương lai.

4. Tiêu chuẩn kỹ thuật

- a. Có thể mở rộng kết nối với các Đơn vị trực thuộc, đơn vị liên kết, với nhiều hãng khác nhau và có thể kết nối về cơ sở chính.
- b. Tùy theo nhu cầu thực tế sử dụng số lượng máy nhánh analog, số máy nhánh số, số line trung kế mà chọn dòng thiết bị phù hợp.
- c. Các hệ thống có thể kết nối với nhau và với các hệ thống truyền thông khác tạo thành một mạng đồng nhất với số người dùng không hạn chế dựa trên các đường kết nối riêng hay qua các mạng PSTN/ISDN, IP, ATM, Frame Relay, MegaWan cung cấp cho người dùng các tính năng dịch vụ có thể được truy cập tại bất kỳ vị trí nào trong mạng như từ một hệ thống duy nhất.
- d. Khả năng đánh số mềm dẻo: Kế hoạch đánh số nội bộ cho phép các số máy nội bộ có thể được đánh số từ 1 đến 6 chữ số, số chữ số của các máy lẻ có thể không đồng đều. Kế hoạch đánh số gọi ra cho phép 6 chữ số để định nghĩa mã chiếm trung kế. Kế hoạch đánh số gọi vào cho phép các số DID (Direct Inward Dialling) có tối đa 6 chữ số.
- e. Nhạc chờ và thông báo: Thuê bao có thể đưa đối phương vào trạng thái chờ (hold) để thực hiện thảo luận hay làm việc gì khác trước khi quay trở lại cuộc thoại. Đối phương bị chờ sẽ có thể được nghe các bản nhạc chờ (Music on Hold).
- f. Gọi vào nhờ sự hỗ trợ của điện thoại viên: Hệ thống cho phép lập trình hướng các cuộc gọi từ các trung kế nhất định đến bàn điện thoại viên (hay một thuê bao bất kỳ) và điện thoại viên (hay thuê bao được định nghĩa) sẽ thực hiện chuyển tiếp cuộc gọi đến thuê bao nội bộ theo yêu cầu.
- g. Người gọi từ bên ngoài có thể được nghe một lời chào và hướng dẫn quay số ghi âm được. Các trường hợp quay sai số, không quay số, thuê bao đang bận hoặc không nhắc máy có thể lập trình để đổ chuông vào điện thoại viên hay trượt sang thuê bao khác hoặc hệ thống trả lời tự động, hộp thư thoại.

- h. Tính cước : Hệ thống có khả năng tính cước cho từng thuê bao. Thông tin cước có thể được hiển thị tại chỗ trên máy điện thoại có màn hình và tập trung toàn hệ thống được ghi lại vào vùng nhớ đệm và được đưa ra liên tục trên các công V.24. Các bản ghi chi tiết cuộc gọi sẽ được xử lý bởi máy tính cài đặt phần mềm CAS 4.0. Máy tính tính cước được nối với một công V.24 của tổng đài tổng đài thông qua công COM và một cáp số liệu.

vi. **TIÊU CHUẨN HỆ THỐNG PHẦN MỀM**

1. Tiêu chuẩn hạ tầng mạng:

ĐHĐN phải thực hiện theo quy định tại khoản A Phụ lục 01.

2. Tiêu chuẩn hạ tầng hệ thống:

b. Mô hình kết nối:

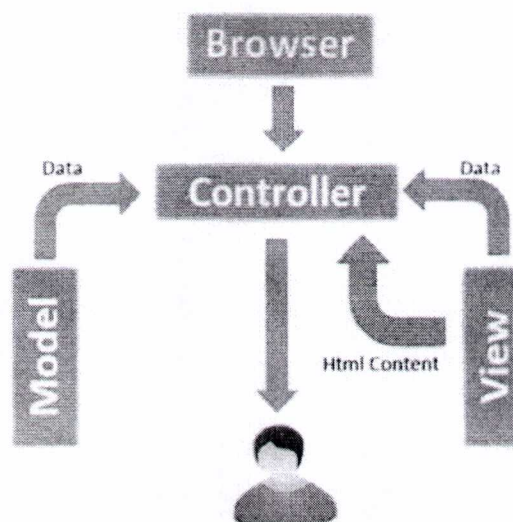
3. Phạm vi áp dụng: tất cả các phần mềm được sử dụng tại ĐHĐN Tiêu chí:

- Đáp ứng đầy đủ các nhu cầu nghiệp vụ.
- Hỗ trợ các loại báo cáo cho quản lý, điều hành.
- Tài liệu phát triển (đối với phần mềm ĐHĐN tự phát triển) đầy đủ, rõ ràng, clear code - complete code.
- Tài liệu vận hành, tài liệu sử dụng cho người dùng cuối đầy đủ, cập nhật thường xuyên.
- Nhật ký hệ thống, kịch bản xử lý sự cố được kiểm tra, cập nhật tức thời khi phát sinh.
- Bộ tài liệu blue print (bao gồm các tài liệu trên) phải được cập nhật đúng thực tế và bảo quản tại đơn vị vận hành chức năng/vận hành kỹ thuật.
- Đảm bảo độ ổn định - sẵn sàng, thông tin đầy đủ - kịp thời - chính xác của ứng dụng cung cấp tới người dùng.
- Phân quyền chi tiết tới từng user/group.
- Hỗ trợ cơ chế giám sát, ghi log phục vụ sửa lỗi và giám sát hệ thống.
- Đáp ứng cơ chế bảo mật ở mức application và mức database.

4. Tiêu chuẩn kỹ thuật:

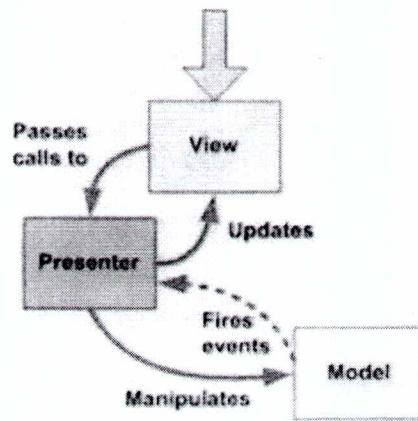
a. Mô hình thiết kế:

Mô hình MVC



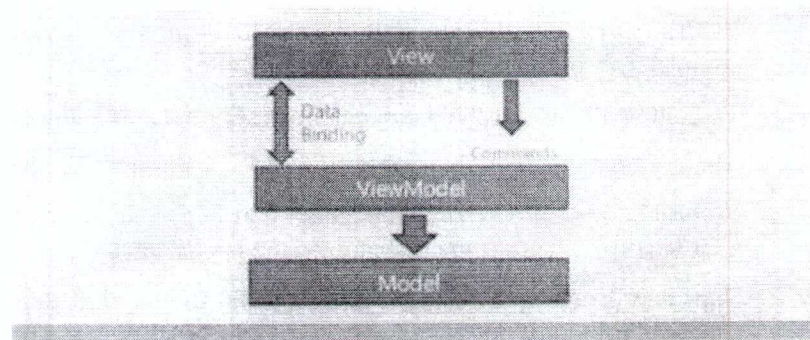
Mô hình MVM

user Interaction



MVVM

Model View -ViewModel



b. Công nghệ:

- i. Application: .NET framework, ASP.NET, HTML5 (load balancer cho application, đảm bảo cơ chế dự phòng mức application).
- ii. Database: SQL Server hoặc Oracle database (cluster hoặc always on, đảm bảo cơ chế dự phòng mức database).
- iii. UI: web browser hoặc dạng hy-brid (vừa web form và window form).
- iv. Mobile App: IOS & Android.

V. Security: đáp ứng các tiêu chuẩn bảo mật hiện hành, theo ngành nghề, chức năng.

ĐHĐN	BIÊN BẢN SAO LƯU DỮ LIỆU	Mã số: CĐHĐN/QC-01/M02 Hiệu lực: .../.../2018
------	---------------------------------	--

TT	SERVER BACKUP	LOẠI BACKUP		KẾT QUẢ		NGÀY/GIỜ BACKUP	GHI CHÚ
		FULL	DIFF	Thành Công	Thất bại		
		<u>1 1</u>	<u>1 1</u>	<u>1 1</u>	<u>1 1</u>		
			<u>1 1</u>	<u>1 1</u>	<u>1 1</u>		
		<u>1 1</u>	<u>1 1</u>	<u>1 1</u>	<u>1 1</u>		
		□	<u>1 1</u>	<u>1 1</u>	<u>1 1</u>		
		<u>1 1</u>	□	<u>1 1</u>	<u>1 1</u>		
		<u>r 1</u>	<u>1 1</u>	<u>1 1</u>	<u>1 1</u>		
		<u>1 1</u>	<u>1 1</u>	<u>1 1</u>	<u>1 1</u>		

Lưu ý :

- **Server Backup:** nhập đầy đủ thông tin tên server backup
- **Loại Backup:** bao gồm loại backup đầy đủ hoặc backup từng phần trên một server.

Trưởng Đơn vị P.TCHC & QT

Nhân sự thực hiện

ĐH ĐHĐN		BÁO CÁO KIỂM TRA ngày		Mã số: CĐHĐN/QC-01/M02 Hiệu lực: .../.../2018	
A. HỆ THỐNG					
stt	Danh Mục Kiểm Tra	Hạng mục kiểm tra	Kết Quả		Ghi Chú
			Đạt(Pass)	KĐ (Fail)	
	Kiểm Tra kết nối	Kiểm tra kết nối Internet			
		• Ping <IP public address > kiểm tra connection			
		• Ping <Domain name > Kiểm tra DNS			
		• Tracert <IP address> Kiểm tra routing			
	Kiểm tra kết nối MegaWAN	• Kiểm tra kết nối MegaWAN			
		• Log on Webmail Google app			
		■ Send mail to internal			
		• Send mail to External (send mail to Gmail.Yahoo,Hotmail,etc...)			
	Kiểm tra send & Receive mail	■ Receive mail from Internet (receive mail from Gmail, Yahoo,Hotmail,etc...)			
		Check Physiscal Device: HDD, Raid, Power, Interface, etc...			
		• Log on to : tất cả Server			
		• Check Connection Status			
	Kiểm Tra Blade Chassic & Blade Host Server	• Check Physiscal Device			
		Raid.Power.Interface.etc...			
	Kiểm Tra SAN system	Log on to Thinksystem, SAN Storage System, Controller port			
		• Check Connection Status			
	Kiểm tra database	• MS SQL			
		• MySQL: các website			
		SQL Server: các ứng dụng			
	Kiểm tra backup	OS: tat cả các server			
		• Database			
		• File source code web			
		• Tape			
	Kiểm Tra reverse IP Address Domain name	• Check Reverse IP			
	Kiểm Tra Reverse Domain và IP Address	Check Reverse Domain: mail.DHĐN.edu.vn			
	Kiểm Tra Website	■ Website ĐHĐN			

Stt	Danh Mục Kiểm Tra	Hạng mục kiểmTra	Kết Quả		Ghi Chú
			Đạt (Pass)	KĐ (Fail)	
10	Kiểm Tra Application	• Tất cả các ứng dụng			
11	Kiểm Tra Server VMs	• Tất cả server			
A.r	4. MẠNG				
1	Kiểm tra Access Control phòng Datacenter	Nguồn điện cung cấp.			
		Data synchronization Access Control and PC.			
2	Kiểm tra hệ thống điện phòng Datacenter	Kiểm tra tín hiệu tủ điện, CB			
		Kiểm tra máy phát điện (tầng hầm)			
3	Kiểm tra UPS	Kiểm tra nguồn điện UPS APC, Emersion			
4	Kiểm tra hệ thống lạnh phòng Datacenter và phòng nguồn	Nguồn điện cung cấp.			
		Nhiệt độ phòng			
		Nguồn và trình trạng máy bơm			
5	Kiểm tra thiết bị báo cháy phòng Datacenter và phòng nguồn	Nguồn điện thiết bị.			
		Trình trạng thiết bị (đèn cảnh báo,...).			
6	Kiểm Tra Camera phòng Server	Nguồn điện thiết bị.			
		Data synchronization Camera and PC.			
7	Kiểm tra hệ thống cắt lọc sét.	Nguồn điện thiết bị			
		Tình trạng thiết bị.			
8	Kiểm Tra Camera	Kiểm tra hệ thống cắt lọc sét đường nguồn			
		Kiểm tra hệ thống cắt lọc sét lan truyền mạng			
		Nguồn điện server, client.			
		Dữ liệu hình ảnh			
		Kiểm Tra Modem - Draytek sử dụng cho Camera			
		Kiểm tra máy chủ Camera			
9	Kiểm Tra tổng đài điện thoại	Check Physiscal Device :Power,Slot Interface,etc...			
		Call to Internal (Local,All Other Site)			
		Call to External			
		Check Connection Status (Voice IP)			
		Kiểm tra máy tính cước và PC-Management			
10	Kiểm tra mạng nội bộ	Kiểm tra các Access Switch tầng			
		Kiểm tra kết nối về Server Farm			
		Kiểm tra kết nối về DMZ			
		Kiểm tra kết nối về Core Switch			

stt	Danh Mục Kiểm Tra	Hạng mục kiểm tra	Kết Quả		Ghi chú
			Đạt (Pass)	KĐ (Fail)	
11	Kiểm tra mạng WAN	Ping <IP public address > kiểm tra connection			
		Ping <Domain name > Kiểm tra DNS			
		Tracert <IP address> Kiểm tra routing			
		Kiểm tra kết nối MPLS			
12	Kiểm tra mạng Internet	Kiểm tra kết nối Internet Lease Line Viettel, VDC, VNPT, CMC			
13	Kiểm tra kết nối mạng không dây Wireless	Kiểm Tra VPN Site to Site, Client to Site			
		Kiểm tra các AP tầng			
		Kiểm tra controller			
		Kiểm tra kết nối về Radius Server			
14	Kiểm Tra Access Switch 2960	Kiểm tra Access Switch tầng			
		Kiểm tra Trunking về Core			
		Check Physiscal Device : Led,Power,Interface,etc...			
		Login SW2960G			
		Check Connection Status			
		Check IOS,NVRAM,Startup config,Running Config,etc...			
15	Core Switch - 01	Nguồn điện thiết bị			
		Tình trạng thiết bị.			
		Kiểm tra performance, Traffic, vss			
16	Core Switch - 02	Nguồn điện thiết bị			
		Tình trạng thiết bị.			
		Kiểm tra performance, Traffic, vss			
17	Paloalto PA-3220 - Internal FW	Nguồn điện thiết bị			
		Tình trạng thiết bị.			
		Kiểm tra performance, Traffic, Rule,...			
18	Watchguard 400 - Internal FW	Nguồn điện thiết bị			
		Tình trạng thiết bị.			
		Kiểm tra performance, Traffic, Rule, Nat,...			
		Kiểm tra kết nối Internet to Draytek			