Phụ lục 4: Các yêu cầu cho Hạ tầng kỹ thuật, tiêu chuẩn CNTT áp dụng và nguyên tắc triển khai

1. Các tiêu chuẩn CNTT áp dụng cho Kiến trúc Chính quyền điện tử cấp Tỉnh

Sau đây là các tiêu chuẩn CNTT áp dụng cho Kiến trúc Chính quyền điện tử tỉnh Vĩnh Phúc.

1.1. Các tiêu chuẩn quy trình

Tiêu chuẩn số 1: WS-BPEL
WS-BPEL là ngôn ngữ thi hành nhằm mô tả hành vi của các qui trình nghiệp vụ trong môi trường tiêu chuẩn. Các qui trình này có thể sử dụng dịch vụ Web để gọi thực hiện chức năng nghiệp vụ và đưa lên thành các dịch vụ Web.
Tiêu chuẩn số 2: WS-BPEL 2.0 / BPEL4People
Tiêu chuẩn WS-BPEL 2.0 không giải quyết các vấn đề nghiệp vụ về việc con người tham gia vào qui trình nghiệp vụ như thế nào. Tuy nhiên, tiêu chuẩn mở rộng của WS-BPEL là BPEL4People xác định phương thức để mở rộng tiêu chuẩn WS-BPEL nhằm hỗ trợ kịch bản con người tham gia vào qui trình nghiệp vụ. Một thể khác của tiêu chuẩn BPEL4People là WS-HumanTask. Nó xác định phương thức nhiệm vụ của một người có thể được gọi thực hiện như một dịch vụ Web.
Tiêu chuẩn số 3: BPELJ
Trong tiêu chuẩn WS-BPEL 2.0, toàn bộ các bước trong qui trình nghiệp vụ là các viện dẫn thực hiện dịch vụ Web. Có nhiều lúc một chương trình nhỏ cũng được coi như là một phần của qui trình. Thay vì phải xây dựng một chương trình và đưa lên thành dịch vụ Web, tiêu chuẩn mở rộng của WS-BPEL là BPELJ cho phép một qui trình thực thi mã Java™ bên trong qui trình. Điều này cho phép cả BPEL và Java thể hiện được những gì tốt nhất của nó trong cùng một qui trình.
Tiêu chuẩn số 4: WS-Business Activity
Một tiêu chuẩn liên quan là WS-Business Activity 1.1. Nếu một qui trình nghiệp vụ dài gọi thực hiện một qui trình khác như là một bước, các hành động chu trình như

việc huỷ qui trình đầu tiên cần được tiểu qui trình thực hiện. Ví dụ: nếu qui trình đầu tiên bị huỷ, tiểu qui trình có thể thay thế hoặc hoàn tác mọi hoạt động đã thực hiện trước đó. Thông số này cung cấp các kiểu phối hợp hoạt động nghiệp vụ mà có thể sử dụng trong khung WS-Coordination cùng với hai giao thức phối hợp hoạt động nghiệp vụ. Nhà phát triển có thể sử dụng các loại và giao thức phối hợp này khi cần một sự thống nhất về kết quả của các qui trình phân tán dài.

Tiêu chuẩn số 5: BPMN

Một qui trình có thể được minh hoạ thông qua một lược đồ cung cấp một hệ thống ký hiệu tiêu chuẩn cho lược đồ qui trình. Sử dụng một hệ thống ký hiệu để bảo đảm tính nhất quán do vậy dù bất kỳ ai tạo ra biểu đồ thì các biểu tượng giống nhau cũng được sử dụng để biểu diễn cùng một đối tượng. Ví dụ: quyết định luôn là hình thoi (còn được gọi là *cổng kết nối*). Điều này làm cho lược đồ trở nên dễ hiểu hơn, bất kể người sử dụng là nhà phân tích nghiệp vụ không liên quan đến kỹ thuật, lập trình viên hoặc kiến trúc sư hệ thống.

Tiêu chuẩn số 6: XPDL

Mục đích của XPDL là có được định dạng XML cho việc lưu trữ các lược đồ BPMN. Nếu các nhà cung cấp sử dụng XPDL làm định dạng tập tin, họ có thể dễ dàng trao đổi các mô hình qui trình. Ví dụ, nhà thầu A có thể sử dụng cho việc mô hình hoá qui trình ban đầu, nhà thầu B là phân tích qui trình, và nhà thầu C triển khai qui trình. XPDL được coi là bổ sung cho WS-BPEL chứ không phải là một chuẩn cạnh tranh. Trong khi WS-BPEL là ngôn ngữ thi hành, XPDL là định dạng tập tin để tăng tính tương thích của các công cụ. Một vài ứng dụng vẽ lược đồ qui trình sử dụng mô hình XPDL, sử dụng các mô-đun mở rộng để bổ sung chi tiết cần thiết cho một môi trường thực thi.

Tiêu chuẩn số 7: Công cụ mô hình hóa biểu đồ

Khó có thể mô tả một qui trình nếu chỉ dùng từ ngữ để diễn đạt. Sẽ hiệu quả hơn nếu sử dụng lược đồ để mô tả cấu trúc tổng thể của một qui trình nghiệp vụ. Cần một thể hiện trực quan cùng với dữ liệu mô tả để diễn tả các hoạt động trong qui trình cùng

với các qui tắc nghiệp vụ cho các quyết định bên trong qui trình.

Tiêu chuẩn số 8: Cơ chế chạy chương trình

Mô hình chỉ là một thể hiện của một qui trình cụ thể. Nó có thể được sử dụng bởi cơ chế chạy chương trình như một khuôn mẫu để minh hoạ qui trình nghiệp vụ. Cơ chế chạy chương trình duy trì trạng thái của qui trình nghiệp vụ thông thường bằng cách sử dụng cơ sở dữ liệu. Cơ chế chạy chương trình quản lý các qui trình đang chạy và sắp đặt các hoạt động, và một số các hoạt động này là tự động. Hầu hết các cơ chế chạy chương trình có một vài kiểu kết nối hoặc bộ điều hợp nhằm thúc đẩy các hệ thống nghiệp vụ. Các hoạt động khác có thể cần con người can thiệp. Cơ chế chạy chương trình có một số cách khác nhau để phân việc cho người dùng, quản lý danh mục công việc (đôi khi còn được đề cập như là hàng đợi tác vụ hoặc đơn giản chỉ là hàng đợi), và đưa con người tham gia vào qui trình nghiệp vụ.

1.2. Các tiêu chuẩn dữ liệu

Tiêu chuẩn số 1: Các cơ sở dữ liệu mới phải sử dụng hệ quản trị cơ sở dữ liệu quan hệ có hỗ trợ ANSI-Standard SQL.

- Cơ sở dữ liệu quan hệ mang lại sự tin cậy, sự linh hoạt và tính tương thích cho các nhu cầu dữ liệu trong tương lai.
- Dữ liệu có thể được duy trì và truy cập nhanh chóng thông qua các câu lệnh SQL tiêu chuẩn. Ngôn ngữ hỏi đáp có cấu trúc (SQL) là tiêu chuẩn kỹ nghệ cho tầng truy cập dữ liệu của ứng dụng và cho các công cụ truy cập dữ liệu.
- Sử dụng trật tự ưu tiên mở rộng để gắn trách nhiệm với nhà thầu.
- Các sản phẩm cơ sở dữ liệu chạy trên máy desktop thường được coi là các công cụ tra cứu cơ sở dữ liệu của người dùng cuối và không thể dùng cho việc triển khai trên toàn tổ chức.
- Công nghệ phi quan hệ như các tập tin phẳng có thể được sử dụng cho việc lưu trữ dữ liệu tạm thời và dữ liệu phi cấu trúc như dữ liệu văn bản. Việc sử dụng các công nghệ phi cấu trúc trên qui mô lớn cần được loại bỏ.

Tiêu chuẩn số 2: Các hệ thống tự xây dựng phải tuân thủ với các định nghĩa phần tử dữ liệu tiêu chuẩn CMR hiện hành.

- Các cơ sở dữ liệu mới thuộc về các hệ thống tự xây dựng phải tuân thủ các định nghĩa phần tử CMR. Nhóm rà soát phần tử dữ liệu mô tả sẽ rà soát các phần tử dữ liệu để xác định liệu các phần tử này có tuân thủ các tiêu chuẩn hiện hành hay không.
- Bất kỳ một tiêu chuẩn phần tử dữ liệu mới nào đều phải được đề xuất và rà soát để phê chuẩn như là một tiêu chuẩn quốc gia.
- Nếu một định nghĩa phần tử dữ liệu không thể được tùy biến nhằm tuân thủ các tiêu chuẩn hiện hành thì phải được loại bỏ.

Tiêu chuẩn số 3: Các hệ thống thương mại sử dụng các định nghĩa phần tử dữ liệu do phần mềm máy khách kiểm soát phải tuân thủ các định nghĩa phần tử dữ liệu tiêu chuẩn CMR. Nếu không, nhà thầu phải cung cấp một thủ tục chuyển đổi để phù hợp với các tiêu chuẩn trao đổi dữ liệu mô tả nhằm chia sẻ dữ liệu.

- Nếu một hệ thống thương mại có các định dạng dữ liệu mà có thể chỉnh sửa, các phần tử dữ liệu cần phải được chỉnh sửa để phù hợp với các yêu cầu dữ liệu tiêu chuẩn.
- Nếu định nghĩa phần tử dữ liệu không thể được tuỳ biến để phù hợp với các tiêu chuẩn hiện hành, nhà thầu phải cung cấp các thủ tục chuyển đổi nhằm phù hợp với các tiêu chuẩn trao đổi dữ liệu mô tả CMR.

Tiêu chuẩn số 4: Sử dụng các tiêu chuẩn trao đổi dữ liệu mô tả tập trung khi trao đổi dữ liệu giữa các cơ quan.

- Nếu cần phải trao đổi dữ liệu giữa các cơ quan và dữ liệu được lưu ở nhiều nơi khác nhau thì dữ liệu cần phải được trao đổi thông qua tiêu chuẩn trao đổi đã được qui định trong CMR.

1.3. Các tiêu chuẩn ứng dụng

Tiêu chuẩn số 1: Xây dựng các ứng dụng 3 tầng hoặc nhiều tầng

- Tất cả các ứng dụng tầm cơ quan mới phải được xây dựng theo kiến trúc 3 tầng hoặc nhiều tầng để tối ưu hoá tính linh hoạt và khả chuyển.
- Các dự án lớn và phức tạp mà được sử dụng nhiều và/hoặc được sử dụng lâu dài sẽ tốt hơn nếu được xây dựng theo kiến trúc hướng dịch vụ nhiều tầng.

- Việc phân chia các tầng về mặt lôgic cho các phần giao diện người dùng, qui tắc nghiệp vụ và mã truy xuất dữ liệu cho phép các bổ sung đơn giản và dễ dàng đối với mỗi tầng mà không làm ảnh hưởng tới các tầng còn lại.
- Việc phân chia các tầng về mặt lôgic cũng cho phép thay đổi các hệ thống nền tảng của các tầng, mang lại tính khả chuyển cao. Vì các xử lý giao dịch, thời gian đáp ứng hoặc thay đổi thông lượng, một tầng có thể được chuyển từ hệ thống nền tảng mà nó đang được thi hành tới tầng khác mạnh hơn hoặc có thể được chia đều ra nhiều máy mà không làm ảnh hưởng tới các tầng còn lại.
- Trong khi nhiều vấn đề còn tồn tại trong các ứng dụng đơn tầng hoặc 2 tầng hiện hành có thể được khắc phục bằng việc triển khai các ứng dụng với kiến trúc 3 tầng, mục tiêu cuối cùng luôn luôn là triển khai các ứng dụng nhiều tầng.
- Lợi ích tối đa của kiến trúc nhiều tầng được thể hiện khi nhiều ứng dụng nhiều tầng được triển khai khắp Thành phố, chia sẻ các dịch vụ ứng dụng dùng chung và đưa ra nhiều giao diện người dùng.
- Các dự án lớn và phức tạp mà được sử dụng nhiều và/hoặc được sử dụng lâu dài sẽ tốt hơn nếu được xây dựng theo kiến trúc 3 tầng có khả năng truy cập ứng dụng kiến trúc hướng dịch vụ nhiều tầng.
- Với các ứng dụng mô hình khách / chủ 3 tầng, có ít rủi ro hơn trong việc chỉnh sửa mã triển khai qui tắc nghiệp vụ.
- Các ứng dụng mô hình khách / chủ 3 tầng có thể hỗ trợ nhiều giao diện người dùng: ký tự, đồ hoạ, trình duyệt, điện thoại và các giao diện khác.

Tiêu chuẩn số 2: Cô lập phần tuỳ biến với ứng dụng được mua

- Cô lập các phần tuỳ biến trong các mô-đun riêng biệt khỏi ứng dụng được mua để nâng cao khả năng nâng cấp và chuyển sang các phiên bản mới khi cần. Đối với các ứng dụng chuyên ngành được mua cần tích hợp lỏng các mô-đun tự xây dựng với ứng dụng phần mềm tiêu chuẩn..

Tiêu chuẩn số 3: Tránh sử dụng giao diện cổng kết nối chung (CGI) cho lô-gic nghiệp vụ hoặc xuất bản thông tin trên web.

- CGI không khả chuyển, không có khả năng đóng gói và di chuyển và không dễ dàng tích hợp với các máy chủ ứng dụng. Tránh sử dụng CGI để xuất bản thông tin, các ứng dụng xử lý nội bộ hoặc truy xuất dữ liệu.

- Sử dụng HTML hoặc XML thông qua các java servlets để xuất bản thông tin trên web nhằm giảm các phí tổn hoặc công việc trong việc kết nối với các thành phần dựa trên EJB.
- Việc sử dụng ASP hoặc công nghệ xuất bản HTML khác là chấp nhận được với việc xuất bản thông tin (không xử lý nghiệp vụ) tuy nhiên JSP và servlets thường được ưa chuộng hơn.

1.4. Các tiêu chuẩn tích hợp ứng dụng

Tiêu chuẩn số 1: Xác định rõ giao diện ứng dụng

- Để tích hợp các ứng dụng mà Chính quyền tỉnh không có quyền sở hữu mã nguồn các giao diện ứng dụng cần phải được xác định rõ nhằm cho phép trao đổi thông tin một cách tin cậy giữa các ứng dụng.
- Để thúc đẩy việc mua phần mềm tốt nhất trong khi đơn giản hoá việc tích hợp ứng dụng, các giao diện ứng dụng cần phải được xác định một cách rõ ràng.

Tiêu chuẩn số 2: Phải lập tài liệu cấu trúc thông điệp

- Thông điệp hoặc giao dịch là cơ chế để trích xuất dữ liệu từ ứng dụng hoặc gửi dữ liệu tới ứng dụng khác.
- Lập trình viên tích hợp ứng dụng cần phải biết độ dài và kiểu của mẫu tin (tức là liệu mẫu tin có độ dài cố định hay thay đổi, và nếu thay đổi thì ký tự dùng để phân cách các trường là gì), và cần phải biết trường nào là tuỳ chọn và ngược lại trường nào là bắt buộc (có giá trị).
- Cần có mô tả dữ liệu đối với mỗi trường.
- Giải thích và ví dụ về định dạng mẫu tin và mô tả trường thông tin là rất hữu ích và cần phải có.

Tiêu chuẩn số 3: Ứng dụng phải có khả năng truyền và nhận thông điệp sử dụng mô hình khách / chủ

- Ứng dụng máy khách là tiến trình gửi hoặc tạo ra thông điệp. Ứng dụng máy chủ là tiến trình nhận thông điệp.
- Ứng dụng máy khách và ứng dụng máy chủ có thể giao tiếp bằng cách sử dụng TCP/IP và socket, hoặc những giao thức giao tiếp khác như serial và ftp, miễn là

chúng thực hiện cùng một chức năng truyền và nhận.

- Cần phải cung cấp các ký tự đóng gói, dùng để xác định điểm đầu và kết thúc của chuỗi ký tự và định dạng chấp nhận thông điệp.

Tiêu chuẩn số 4: Mua ứng dụng chuyên ngành hơn là tự xây dựng nếu có thể

- Mua ứng dụng chuyên ngành có thể cho phép Chính quyền tỉnh đáp ứng được các nhu cầu nghiệp vụ một cách nhanh chóng hơn là tự xây dựng phần mềm.
- Các giao diện chương trình ứng dụng được công bố có thể không đủ bởi vì sử dụng chúng đòi hỏi phải tự xây dựng ứng dụng và có thể không thể thực hiện giao tiếp giữa hai ứng dụng được mua. Sử dụng máy giao tiếp sẽ mang lại sự linh hoạt hơn nhiều.

1.5. Tiêu chuẩn mạng

Tiêu chuẩn số 1: Tiêu chuẩn mạng LAN nối bằng cáp

- Tiêu chuẩn dây mạng nội bộ là dây xoắn đôi không có vỏ bọc chống nhiễu loại 5, 6, hoặc 7 (Cat 5 UTP, Cat 6 UTP, hoặc Cat 7 UTP). Trừ trường hợp có những nhu cầu cụ thể như EMI cao hoặc khoảng cách xa, UTP có thể được bố trí chạy nằm ngang trong sơ đồ mạng.
  - Dây mạng CAT 5/6/7 UTP có thể được chứng thực là truyền tải được dữ liệu với tốc độ 10/100/1000 MB trên giây.
  - Dây mạng CAT 5/6/7 UTP được coi là tiêu chuẩn kỹ nghệ trong việc nối dây và được Viện các kỹ sư điện và điện tử (IEEE) hỗ trợ.
  - Việc đi dây, dây mạng, đầu nối, và các nhà thầu cung cấp thiết bị đã được tiêu chuẩn hoá với loại dây mạng này.

Tiêu chuẩn số 2: Tiêu chuẩn kết nối đến tầng truy cập

- Tiêu chuẩn cho giao thức truy cập tầng liên kết tiêu chuẩn là phương thức truy cập dựa trên Ethernet và IEEE 802.3 CSMA/CD.
  - Định dạng được chấp nhận phổ biến.
  - Tin cậy, giao thức được sử dụng trong nhiều năm và rất ổn định.
  - Các phiên bản có khả năng mở rộng và nhanh hơn đang xuất hiện giúp việc quản lý sự gia tăng của luồng dữ liệu.

- 1000BaseT Gigabit Ethernet có băng thông đủ để hỗ trợ nhu cầu về thoại và hình ảnh trong tương lai.

1.6. Các tiêu chuẩn an toàn, bảo mật

Tiêu chuẩn số 1: Secure sockets layer (SSL) - Lớp đế an toàn

- SSL là giao thức được hỗ trợ phổ biến nhất đối với việc truyền thông giữa máy chủ web và trình duyệt.
- Giao thức này xác thực máy chủ web và có thể xác thực trình duyệt của người dùng nếu được chỉ định.
- Các phiên bản hiện tại cho phép hỗ trợ xác thực người dùng bằng cách sử dụng các dịch vụ do các cơ quan chứng thực cung cấp.

Tiêu chuẩn số 2: Mở rộng an toàn giao thức IP (IPSec)

- IPSec là một mở rộng của giao thức truyền thông IP, được xây dựng nhằm cung cấp đường truyền an toàn từ điểm đầu đến điểm cuối đối với các gói tin truyền qua mạng Internet.
- IPSec có hai dạng: xác thực người gửi và bảo đảm tính toàn vẹn thông tin nhưng không bảo mật thông qua việc sử dụng bản ghi nhãn xác thực (AH), và xác thực người gửi và bảo đảm tính toàn vẹn thông tin có bảo mật thông qua việc sử dụng gói tin được đóng gói (ESP).

Tiêu chuẩn số 3: Mã hoá phải dựa trên các tiêu chuẩn mở

- Các dịch vụ mã hoá đề cập trong tài liệu này phải dựa trên các tiêu chuẩn mở và được chấp nhận trong ngành.

Tiêu chuẩn số 4: Sử dụng S/MIME để gửi thư điện tử bảo mật

- S/MIME cung cấp phương pháp nhất quán để gửi và nhận thư điện tử bảo mật bao gồm dữ liệu MIME.
- S/MIME xác định một giao thức dùng cho các dịch vụ mã hóa và chữ ký số.
- Phần mềm gửi/nhận thư điện tử cần được đánh giá để hỗ trợ tiêu chuẩn hoặc khả năng tương hợp.

2. Nguyên tắc và minh họa triển khai các ứng dụng Chính quyền điện tử trên nền tảng Chính quyền điện tử cấp Tỉnh

2.1. Các nguyên tắc về kiến trúc công nghệ

Các nguyên tắc Công nghệ của tỉnh Vĩnh Phúc là nền tảng cho Kiến trúc Công nghệ của tỉnh Vĩnh Phúc. Các nguyên tắc này cung cấp một khung hiệu quả bên trong tổ chức CNTT của tỉnh Vĩnh Phúc, trên cơ sở đó có thể đưa ra những quyết định về các phương thức đề xuất dịch vụ CNTT, về khung quản lý được yêu cầu hỗ trợ và bàn giao các dịch vụ này, và về chiến lược phát triển liên quan đến việc sử dụng và triển khai công nghệ.

Nguyên tắc Kiến trúc Công nghệ 01	▪ Kiến trúc Công nghệ cho phép các ứng dụng được tích hợp một cách dễ dàng ▪ Thông tin được quản lý tập trung ▪ Đầu tư vào CNTT phải theo chiến lược lâu dài
Tỉnh Vĩnh Phúc được xét như một tổ chức độc lập và thống nhất.	**Nguyên tắc:** Tất cả các quá trình triển khai công nghệ trong tỉnh Vĩnh Phúc phải được tích hợp chặt chẽ cho phép quá trình xử lý thông tin như một hệ thống duy nhất trong toàn tổ chức, hệ thống này được quản lý tại trung tâm và sử dụng các khung công nghệ đã chọn cho sự phát triển của các khung công nghệ này. **Các thuộc tính:** o Có khả năng truy cập – Thông tin cho người dùng có quyền truy cập phải dễ tìm và dễ truy cập. o Tính đơn giản – Hệ thống phải được thiết kế đơn giản nhất có thể đứng từ góc độ của người dùng. o Khả năng thích ứng trong tương lai (Future - Proof) – Kiến trúc hệ thống phải được thiết kế đơn giản để thích ứng cao với những thay đổi tương lai theo các yêu cầu nghiệp vụ cũng như các giải pháp kỹ thuật. o Tính nhất quán – Cách thức trình bày dịch vụ đăng nhập (log-in), dịch vụ điều hướng (navigation) và dịch vụ đích (target) cho người dùng phải nhất quán giữa các thời điểm, không gian và các kênh truy cập khác nhau.

	○ Tính hỗ trợ – Hệ thống phải có khả năng hỗ trợ cho người dùng cũng như cán bộ vận hành, từ đó mọi vấn đề và khó khăn tác nghiệp đều có thể được giải quyết. ○ Có thể mở rộng quy mô – Hệ thống phải có khả năng mở rộng quy mô theo quy mô của cộng đồng người dùng, các yêu cầu lưu trữ dữ liệu, công suất xử lý...có thể phát sinh trong khoảng thời gian vận hành hệ thống. ○ Có thể chuyển đổi – Cần phải có phương án chuyển đổi khả thi và có thể quản lý mà chấp nhận được đối với người dùng. ○ Có khả năng hoạt động tương tác – Hệ thống phải tương tác với các hệ thống tương tự khác ngay ở thời điểm hiện tại và trong tương lai, vì việc trao đổi thông tin giữa các hệ thống ngày càng trở thành một yêu cầu cấp thiết. **Ý nghĩa thực tiễn:** ○ Mỗi trạm làm việc phải có khả năng truy cập vào các dịch vụ chung thông qua một kết nối mạng từ bất cứ một điểm nút nào. ○ Việc đánh giá công nghệ và quy trình chọn lựa cần phải phản ánh được các tiêu chuẩn tích hợp. ○ Có thể hạn chế sự chọn lựa công nghệ và thực thi việc sử dụng các tiêu chuẩn.
Nguyên tắc Kiến trúc Công nghệ 02	▪ Các dịch vụ ứng dụng phải được công bố công khai ▪ Thông tin cần được đưa vào sử dụng tối đa ▪ Siêu dữ liệu thống kê cần phải được sử dụng
Tỉnh Vĩnh Phúc hợp tác với các cơ quan chính phủ khác và người dân	**Nguyên tắc:** Việc triển khai công nghệ phải cho phép các tổ chức bên ngoài truy cập vào tất cả các ứng dụng điện tử dịch vụ công cộng của tỉnh Vĩnh Phúc, cung cấp các thông tin thống kê dưới các định dạng đã

	được phổ biến rộng rãi. **Các thuộc tính:** o Đảm bảo tính nghiệp vụ – Việc đảm bảo tính nghiệp vụ và thực hiện các mục tiêu nghiệp vụ phải là nguyên tắc cơ bản khi thiết kế hệ thống. o Tính nhất quán - Giao diện của dịch vụ đăng nhập (log-in), dịch vụ điều hướng (navigation) và dịch vụ đích (target) cho người dùng phải nhất quán giữa các thời điểm, không gian và các kênh truy cập khác nhau. o Tính hữu hiệu – Hệ thống và các dịch vụ của hệ thống phải được vận hành để duy trì và nâng cao hiệu suất cho người dùng đối với các quy trình nghiệp vụ mà họ đang tham gia. o Không lỗi – Trong suốt quá trình vận hành sản xuất, hệ thống không được gặp bất cứ lỗi nào. o Tính sẵn sàng phục vụ – Các thông tin và dịch vụ mà hệ thống cung cấp phải luôn sẵn sàng theo các yêu cầu quy định trong Bản cam kết mức chất lượng (SLA) o Có khả năng hoạt động tương tác – Hệ thống phải tương tác với các hệ thống tương tự khác ngay ở thời điểm hiện tại và trong tương lai, vì việc trao đổi thông tin giữa các hệ thống ngày càng trở thành một yêu cầu cấp thiết. **Ý nghĩa thực tiễn:** o Giao diện của các ứng dụng phải nhất quán. o Xác định các tiêu chuẩn về khả năng tương tác hoạt động với các Bộ ngành khác yêu cầu phải có sự phối hợp chặt chẽ và có hoạch định lâu dài. o Việc công bố các dịch vụ ứng dụng phải

	yêu cầu một khung Quản lý Dịch vụ CNTT toàn diện đặc biệt khi có bất cứ một sự thay đổi về cấu hình, phát hành, quản lý sự cố cũng như hỗ trợ tiếp nhận phản hồi từ phía người sử dụng. o Việc tương tác với người dân yêu cầu cần có bộ phận hỗ trợ chuyên môn. o Cung cấp các dịch vụ thông tin tới người dân thông qua các kênh điện tử yêu cầu các hệ thống có hiệu suất và mức độ ổn định cao về dịch vụ.
Nguyên tắc Kiến trúc Công nghệ 03	▪ Thông tin phải được quản lý tập trung ▪ Thông tin cần được đưa vào sử dụng tối đa ▪ Siêu dữ liệu thống kê cần phải được sử dụng ▪ Đầu tư vào CNTT phải theo chiến lược lâu dài
Thông tin là tài sản của tỉnh Vĩnh Phúc.	**Nguyên tắc:** Giải pháp công nghệ được triển khai phải đảm bảo tính hữu dụng và tính bảo vệ lâu dài cho tài sản thông tin của tỉnh Vĩnh Phúc. **Các thuộc tính:** o Có khả năng truy cập – Thông tin cho người dùng có quyền truy cập phải dễ tìm và dễ truy cập. o Tính chính xác – Thông tin cung cấp tới người dùng phải chính xác, nằm trong phạm vi đã thỏa thuận để áp dụng đối với dịch vụ được chuyển giao. o Có khả năng bảo vệ – Thông tin và quyền truy cập của người dùng phải được bảo vệ khỏi sự truy xuất không hợp lệ của những người sử dụng hoặc những kẻ xâm nhập khác. o Không lỗi – Trong suốt quá trình vận hành sản xuất, hệ thống không được gặp bất cứ lỗi nào.

	○ Có khả năng quản lý thay đổi – Những thay đổi đối với hệ thống phải được quản lý phù hợp từ đó các tác động của mọi sự thay đổi sẽ được đánh giá và các thay đổi này phải được phê duyệt trước khi đưa vào triển khai. ○ Có thể kiểm định – Các hoạt động của mọi đối tượng có quyền truy cập vào hệ thống, và chuỗi các sự kiện cũng như các kết quả từ các hoạt động này phải được lưu lại để sau này có thể xem xét. Các báo cáo ghi nhận khai thác hệ thống phải cung cấp mức độ chi tiết thích đáng phù hợp với các nhu cầu nghiệp vụ. Việc cấu hình hệ thống phần cứng (Hard system) cũng cần phải được kiểm định để so sánh với cấu hình đích thể hiện quá trình triển khai chính sách bảo mật chi phối toàn hệ thống. **Ý nghĩa thực tiễn:** ○ Quản lý các danh mục, định nghĩa, thư viện thông tin (dữ liệu) phải được thực hiện nhất quán trong mọi đơn vị thuộc tỉnh Vĩnh Phúc. ○ Chính sách bảo vệ nguồn lực thông tin, đặc biệt để đảm bảo tính sẵn sàng của dữ liệu trong các kịch bản dài hạn phải là một phần của mọi quyết định/ hoạch định chiến lược.
Nguyên tắc Kiến trúc Công nghệ04	▪ Kiến Trúc Ứng Dụng mở, hướng dịch vụ ▪ Các dịch vụ ứng dụng phải được công bố công khai ▪ Kiến Trúc Ứng Dụng phải đảm bảo các ứng dụng được tích hợp một cách dễ dàng. ▪ Đầu tư vào CNTT phải theo chiến lược lâu dài
Kiến trúc CNTT của tỉnh Vĩnh Phúc làm đơn giản hóa việc vận	**Nguyên tắc:** Quá trình triển khai công nghệ phải đảm bảo tỉnh Vĩnh Phúc hoạt động có hiệu quả hơn, cung cấp nền tảng xử lý thông

hành tỉnh Vĩnh Phúc.	tin tích hợp cho phép hầu hết các quy trình được hoàn thành trực tuyến. **Các thuộc tính:** o Tính nhất quán - Giao diện của dịch vụ đăng nhập (log-in), dịch vụ điều hướng (navigation) và dịch vụ đích (target) cho người dùng phải nhất quán giữa các thời điểm, không gian và các kênh truy cập khác nhau. o Tính hữu hiệu – Hệ thống và các dịch vụ của hệ thống phải vận hành để duy trì và nâng cao hiệu suất cho người dùng đối với các quy trình nghiệp vụ mà họ đang tham gia. o Đảm bảo tính nghiệp vụ – Việc đảm bảo tính nghiệp vụ và thực hiện các mục tiêu nghiệp vụ phải là nguyên tắc cơ bản khi thiết kế hệ thống. o Không lỗi – Trong suốt quá trình vận hành sản xuất, hệ thống không được gặp bất cứ lỗi nào. o Tính sẵn sàng phục vụ – Các thông tin và dịch vụ mà hệ thống cung cấp phải luôn sẵn sàng theo các yêu cầu quy định trong Bản cam kết mức chất lượng (SLA) o Có thể phục hồi – Hệ thống phải có khả năng phục hồi tình trạng hoạt động trọn vẹn sau một sự cố hoặc hỏng hóc, theo quy định của SLA. o Tính liên tục – Hệ thống phải cung cấp "dịch vụ liên tục". Định nghĩa chính xác về thuộc tính này luôn được quy định rõ trong SLA. o Tính hiệu quả – Hệ thống cần tập trung vào cung cấp các dịch vụ đích với hiệu quả tối ưu, tránh lãng phí các nguồn lực o Tính tự động – Bất cứ khi nào có thể (thiết kế độc lập phụ thuộc vào các yếu tố rà soát

	chi phí/lợi ích) việc quản lý và vận hành của hệ thống phải được tự động hóa. **Ý nghĩa Thực tiễn:** o Các hệ thống ứng dụng phải được thiết kế nhằm phản ánh cơ chế vận hành của tỉnh Vĩnh Phúc từ Trụ sở chính đến các Cục thống kê (PSOs). o Các quy trình mới phải được bổ sung bằng các chỉ số đánh giá hiệu suất, nhằm đảm bảo "tính đơn giản" đã đề ra (Tính hiệu quả và/ hoặc năng suất đạt được).
Nguyên tắc Kiến trúc Công nghệ 05	▪ Kiến Trúc Ứng Dụng mở, hướng dịch vụ. ▪ Các dịch vụ ứng dụng phải được công bố công khai. ▪ Kiến Trúc Ứng Dụng phải đảm bảo các ứng dụng được tích hợp một cách dễ dàng. ▪ Thông tin phải được quản lý tập trung. ▪ Siêu dữ liệu thống kê cần phải được sử dụng. ▪ Đầu tư vào CNTT phải theo chiến lược lâu dài.
Kiến trúc CNTT của tỉnh Vĩnh Phúc là kiến trúc linh hoạt, phù hợp với nghiệp vụ thống kê.	**Nguyên tắc:** Việc triển khai công nghệ có thể được thiết kế nhằm đảm bảo những thay đổi sau này trong các quy trình thống kê có thể được triển khai một cách nhanh chóng và cho phép mở rộng và tương tác trong tương lai với các hệ thống mới và bên ngoài. **Các thuộc tính:** o Đảm bảo tính nghiệp vụ – Việc đảm bảo tính nghiệp vụ và thực hiện các mục tiêu nghiệp vụ phải là nguyên tắc cơ bản khi thiết kế hệ thống. o Tính liên tục – Hệ thống phải cung cấp "dịch vụ liên tục". Định nghĩa chính xác về thuộc tính này luôn được quy định rõ trong SLA. o Luôn được giám sát – Hiệu suất hoạt động

	của hệ thống phải được giám sát liên tục để đảm bảo các đặc tả thuộc tính khác được đáp ứng. Bất cứ sai lệch nào ở mức chấp nhận được phải thông báo với bộ phận quản lý hệ thống. o Linh hoạt/ thích ứng – Hệ thống phải linh hoạt và thích ứng tốt, đáp ứng các yêu cầu nghiệp vụ mới khi chúng phát sinh. o Được đo lường – Hiệu suất của hệ thống phải được đo lường dựa trên một số mục tiêu hiệu suất mong muốn từ đó cung cấp thông tin phản hồi nhằm hỗ trợ quy trình quản lý và kiểm soát. o Được kiểm soát – Hệ thống phải luôn nằm trong tầm kiểm soát của các nhà quản lý. Có nghĩa là việc quản lý sẽ giám sát quá trình vận hành và hoạt động của hệ thống, và sẽ đưa ra các quyết định về cách thức kiểm soát hệ thống dựa trên sự giám sát này, đồng thời sẽ thực hiện các hoạt động để phát huy sự kiểm soát đó. **Ý nghĩa thực tiễn:** o Các quy trình chi tiết phải được xác định để từ đó có thể thực hiện nhanh chóng các yêu cầu vận hành mới của tỉnh Vĩnh Phúc và các hệ thống ứng dụng liên quan được đưa vào cùng với những thay đổi. o Các quá trình thay đổi và cấu hình phải được quản lý thông qua chức năng/đơn vị chuyên môn.
Nguyên tắc Kiến trúc Công nghệ 06	▪ Thông tin cần được đưa vào sử dụng tối đa. ▪ Siêu dữ liệu thống kê cần phải được sử dụng.
Dữ liệu của tỉnh Vĩnh Phúc phải sẵn sàng để đáp ứng cho người dùng tại mọi thời điểm.	**Nguyên tắc:** Việc triển khai công nghệ phải cung cấp các dịch vụ thông tin có tính linh hoạt cao, cho phép người dùng truy cập liên

	tục vào các dữ liệu sẵn sàng để sử dụng. **Các thuộc tính:** o Có khả năng truy cập – Thông tin cho người dùng có quyền truy cập phải dễ tìm và dễ truy cập. o Tính chính xác – Thông tin cung cấp tới người dùng phải chính xác, nằm trong phạm vi đã thỏa thuận để áp dụng đối với dịch vụ được chuyển giao. o Tính thông dụng – Thông tin cung cấp tới người dùng phải thông dụng và cập nhật, nằm trong phạm vi đã được thỏa thuận trước như áp dụng đối với các dịch vụ chuyển giao. o Tính tin cậy – Các dịch vụ cung cấp cho người dùng phải được chuyển giao đảm bảo chất lượng đáng tin cậy. o Phản hồi nhanh – Người dùng nhận được sự phản hồi trong khoảng thời gian thỏa đáng đáp ứng những mong đợi của họ. o Tính kịp thời – Những thông tin được cung cấp hoặc giao quyền truy cập cho người dùng tại thời điểm thích hợp hoặc trong khoảng thời gian thích hợp. o Tính tiện lợi – Hệ thống cần cung cấp các giao diện dễ sử dụng để bất cứ một người sử dụng bình thường nào cũng có thể sử dụng được hệ thống này. Đánh giá của người sử dụng đối với các thao tác trên trong trường hợp tốt nhất là hài lòng và trong trường hợp xấu nhất là chấp nhận được. o Tính sẵn sàng phục vụ – Các thông tin và dịch vụ mà hệ thống cung cấp phải luôn sẵn sàng theo các yêu cầu quy định trong Bản cam kết mức chất lượng (SLA). o Tính liên tục – Hệ thống phải cung cấp "dịch vụ liên tục". Định nghĩa chính xác về

	thuộc tính này luôn được quy định rõ trong SLA. **Ý nghĩa thực tiễn:** o Khung giám quản dữ liệu phải được thực hiện như một phần trong quy trình quản lý của tỉnh Vĩnh Phúc. o Tính sẵn sàng của hệ thống phải được đảm bảo xuyên suốt quá trình sử dụng cấu hình hệ thống có tính sẵn sàng cao (dự phòng). o Tình trạng của dữ liệu (phiên bản, ngày phát hành, quy trình cập nhật) phải được công khai với người dùng.
Nguyên tắc Kiến trúc Công nghệ 07	▪ Thông tin phải được quản lý tập trung. ▪ Luôn luôn đảm bảo tính bảo mật. ▪ Đầu tư vào CNTT phải theo chiến lược lâu dài
Hạ tầng CNTT của tỉnh Vĩnh Phúc phải được chia sẻ, bảo mật và có thể thay đổi.	**Nguyên tắc:** Quá trình triển khai công nghệ phải được thiết kế cho khung dịch vụ chia sẻ, cho phép truy cập an toàn tới thông tin và có thể phát triển cùng với trách nhiệm của tỉnh Vĩnh Phúc trong tương lai. **Các thuộc tính:** o Có khả năng truy cập – Thông tin cho người dùng có quyền truy cập phải dễ tìm và dễ truy cập. o Được kiểm soát – Hệ thống phải luôn nằm trong tầm kiểm soát của các nhà quản lý. Có nghĩa là việc quản lý sẽ giám sát quá trình vận hành và hoạt động của hệ thống, và sẽ đưa ra các quyết định về cách thức kiểm soát hệ thống dựa trên sự giám sát này, đồng thời sẽ thực hiện các hoạt động để phát huy sự kiểm soát đó. o Luôn được giám sát – Hiệu suất hoạt động của hệ thống phải được giám sát liên tục để đảm bảo các đặc tả thuộc tính khác được đáp ứng. Bất cứ sai lệch nào ở mức chấp

	nhận được phải thông báo với bộ phận chức năng quản lý hệ thống. o Bảo mật linh hoạt – Có thể cung cấp tính bảo mật ở các mức độ khác nhau tùy theo nhu cầu nghiệp vụ. Hệ thống phải cung cấp các phương tiện bảo mật thông tin theo các nhu cầu này và có thể đưa ra các mức bảo mật khác nhau cho các loại thông tin khác nhau (theo danh mục bảo mật). o Bảo mật độc lập – An ninh của một hệ thống không nên phụ thuộc vào sự an toàn của bất kỳ hệ thống nào khác mà không nằm trong vùng kiểm soát trực tiếp của hệ thống đó. o Đảm bảo tính toàn vẹn – Tính toàn vẹn của thông tin cần được bảo vệ để đảm bảo rằng thông tin không bị sửa đổi, sao chép hoặc xóa bỏ trái phép. o Có thể mở rộng quy mô – Hệ thống phải có khả năng mở rộng quy mô theo quy mô của cộng đồng người dùng, các yêu cầu lưu trữ dữ liệu, công suất xử lý...có thể phát sinh trong khoảng thời gian vận hành hệ thống. o Có tính hỗ trợ - Hệ thống phải có khả năng hỗ trợ cho người dùng cũng như cán bộ vận hành, từ đó mọi vấn đề và khó khăn tác nghiệp đều có thể được giải quyết. **Ý nghĩa thực tiễn:** o Các dịch vụ CNTT-TT được chia sẻ cần phải được triển khai trong toàn tỉnh Vĩnh Phúc – Việc này yêu cầu một chương trình nâng cao nhận thức toàn diện cho người dùng, cùng với việc nghiêm chỉnh thi hành các chính sách CNTT. o Hiệu suất của hệ thống phải được giám sát chặt chẽ đảm bảo sự hài lòng cho người dùng.

Nguyên tắc Kiến trúc Công nghệ 08	▪ Luôn luôn đảm bảo tính bảo mật. ▪ Đầu tư vào CNTT phải theo chiến lược lâu dài.
Hệ thống CNTT của tỉnh Vĩnh Phúc phải có những khả năng như: có thể thay đổi, sẵn sàng phục vụ, nhất quán, được bảo trì, có hiệu năng và an toàn	**Nguyên tắc:** Quá trình triển khai công nghệ đòi hỏi chỉ ra các khía cạnh bảo mật như một yêu cầu cơ bản mà không có một ngoại lệ nào. **Các thuộc tính:** o Tính sẵn sàng phục vụ – Các thông tin và dịch vụ mà hệ thống cung cấp phải luôn sẵn sàng theo các yêu cầu quy định trong Bản cam kết mức chất lượng (SLA). o Kiểm soát truy cập – Truy cập đến thông tin và chức năng trong hệ thống cần phải được kiểm soát phù hợp với các quyền được cho phép của đối tượng yêu cầu truy cập. Truy cập trái phép sẽ bị ngăn chặn. o Bảo mật linh hoạt – Có thể cung cấp tính bảo mật ở các mức độ khác nhau tùy theo nhu cầu nghiệp vụ. Hệ thống phải cung cấp các phương tiện bảo mật thông tin theo các nhu cầu này và có thể đưa ra các mức bảo mật khác nhau cho các loại thông tin khác nhau (theo danh mục bảo mật). o Bảo mật độc lập – An ninh của một hệ thống không phụ thuộc vào sự an toàn của bất kỳ hệ thống nào khác không nằm trong vùng kiểm soát trực tiếp của hệ thống đó. o Đảm bảo tính toàn vẹn – Tính toàn vẹn của thông tin cần được bảo vệ để đảm bảo rằng thông tin không bị sửa đổi, sao chép hoặc xóa bỏ trái phép. o Được kiểm soát – Hệ thống phải luôn nằm trong tầm kiểm soát của các nhà quản lý. Có nghĩa là việc quản lý sẽ giám sát quá trình vận hành và hoạt động của hệ thống, và sẽ đưa ra các quyết định về cách thức kiểm soát hệ thống dựa trên sự giám sát này, đồng thời sẽ thực hiện các hoạt động

	để phát huy sự kiểm soát đó. o Luôn được giám sát – Hiệu suất hoạt động của hệ thống phải được giám sát liên tục để đảm bảo các đặc tả thuộc tính khác được đáp ứng. **Ý nghĩa thực tiễn:** o Bảo mật phải được triển khai từ khâu thiết kế và được quản lý tại trung tâm bởi các chức năng chuyên môn. o Các yêu cầu Bảo mật/ Riêng tư phải được xác định với tất cả các bên liên quan. o Các yêu cầu bảo mật được điều khiển bởi nghiệp vụ hỗ trợ phải dựa trên các nhu cầu luật pháp, chính sách và nghiệp vụ. o Mô hình bảo mật nhất quán, tin cậy và hiệu quả phải được phát triển cho mục đích sử dụng đối với tất cả các ứng dụng, dữ liệu, hệ thống, và cơ sở hạ tầng.

2.2. Các nguyên tắc ứng dụng CNTT của tỉnh Vĩnh Phúc

Trong quá trình xây dựng kiến trúc Chính quyền điện tử cấp Tỉnh cũng như trong quá trình áp dụng, tuân thủ kiến trúc luôn luôn cần bám sát, tuân thủ các nguyên tắc ứng dụng CNTT. Các nguyên tắc CNTT được xác định theo phương pháp chuyên gia và có mức độ ưu tiên khác nhau:

STT	Nguyên tắc	Cơ sở	Ảnh hưởng
	Nhóm nguyên tắc cho kiến trúc hệ thống thông tin		
1	Để phù hợp với các yêu cầu về sử dụng lại, linh hoạt nhưng không phụ thuộc vào công nghệ cụ thể, hệ thống thông tin phải được thiết kế trên nền tảng hướng dịch vụ	Kiến trúc hướng dịch vụ (SOA) cho phép: hướng sự tập trung vào xây dựng các tính năng nghiệp vụ trong quá trình phát triển phần mềm giảm thiểu	Những hệ thống sẵn có chưa hướng dịch vụ cần phải kết nối thông qua các adapter. Các hệ thống nhỏ viết theo SOA có thể ảnh hưởng đến

		chi phí trong quá trình phát triển; giảm thiểu yêu cầu về đào tạo và kỹ năng; chi phí bảo trì thấp; chu trình phát triển phần mềm nhanh chóng hơn.	hiệu năng.
2	Ứng dụng CNTT cần được thiết kế đáp ứng linh hoạt theo thay đổi theo nghiệp vụ, thúc đẩy tải cấu trúc nghiệp vụ hướng đến đơn giản hóa, thống nhất và tường minh quy trình nghiệp vụ..	Công nghệ thông tin phải phục vụ yêu cầu nghiệp vụ chứ không phải ngược lại vì nghiệp vụ là cốt lõi của bất cứ tổ chức nào, và nghiệp vụ thường thay đổi	Các ứng dụng mới cần phân tách phần mô hình quy trình nghiệp vụ ra khỏi mã nguồn, cho phép điều chỉnh các mô hình này. Cơ sở dữ liệu cũng cần được thiết kế phù hợp. Các ứng dụng cũ có thể phải viết lại nếu nghiệp vụ thường xuyên thay đổi.
	Nhóm nguyên tắc cho ứng dụng		
3	Các ứng dụng cần được xây dựng hướng đến hệ thống dùng chung, có tính sử dụng lại cao hướng đến có thể tích hợp chung trên một nền tảng;	Nguyên tắc này giúp tăng hiệu quả đầu tư và tăng cường khả năng liên thông kết nối và tích hợp giữa các hệ thống thông tin.	Các ứng dụng cũ cần được tích hợp các hệ thống dùng chung, sử dụng lại các thành phần cơ bản. Các thành phần dùng chung nếu chạy như các dịch vụ sẽ đòi hỏi hạ tầng và bảo mật tốt hơn.

4	Ưu tiên áp dụng chuẩn mở	Nguyên tắc này mang lại lợi ích: giá thành sử dụng chuẩn thấp và không có bất cứ khó khăn nào khi tiếp cận; được công bố rộng rãi và duy trì một chính sách truy cập hoàn toàn tự do; không hạn chế về việc tái sử dụng chuẩn.	Các hệ thống sử dụng chuẩn mở sẽ được ưu tiên mua sắm, các hệ thống cũ không dùng chuẩn mở sẽ cần được tích hợp lại
	Nhóm nguyên tắc cho dịch vụ công		
5	Hệ thống phải ưu tiên triển khai dịch vụ công có tính đơn giản, mức độ sử dụng cao	Tính đơn giản cho phép triển khai nhanh, mức độ sử dụng cao đảm bảo hiệu quả đầu tư.	Hệ thống cần được thiết kế hướng đến hiệu năng theo nhu cầu sử dụng và có khả năng triển khai nhanh các dịch vụ công mới
6	Hệ thống ứng dụng CNTT phải cho phép theo dõi kết quả xử lý nghiệp vụ	Hệ thống CNTT cần phục vụ yêu cầu "làm cho hoạt động của cơ quan nhà nước minh bạch hơn" thông qua việc đo lường kiểm soát thực hiện thủ tục hành chính.	Hệ thống cần có khả năng thống kê các chỉ số thực hiện các bước trong thực hiện nghiệp vụ. Với các ứng dụng sẵn có cần phải sửa hoặc thêm các dịch vụ theo dõi. Cần có chuẩn về đo lường cho các hệ thống có thể tích hợp với nhau

7	Hệ thống phải đảm bảo yêu cầu, trình tự, cấu trúc dịch vụ công là thống nhất, xuyên suốt	Hệ thống ứng dụng dịch vụ công cần đáp ứng yêu cầu của Đề án 30, thể hiện sự nhất quán trong giao dịch giữa chính phủ với người dân, lấy người dân làm trung tâm chính trong toàn bộ các nỗ lực cung cấp thông tin, các thông tin trong hệ thống cần được chia sẻ thông suốt giữa các đầu mối thực hiện dịch vụ công, người dân chỉ cần 1 đầu mối tương tác với toàn bộ hệ thống	Các hệ thống cần được tích hợp về đăng nhập, chia sẻ dữ liệu, hồ sơ của người dùng, mô hình nghiệp vụ được tường minh và quản lý. Với các ứng dụng sẵn có cần sửa để tích hợp hoặc nâng cấp
	Về nhóm nguyên tắc cho thông tin, dữ liệu		
8	Thông tin là trọng tâm, mang giá trị cốt lõi của toàn bộ hệ thống, phục vụ mọi hoạt động nghiệp vụ;	Thông tin được sử dụng vào các quá trình ra quyết định và tạo nền tảng để phát triển các chức năng, dịch vụ chất lượng cao. Thông tin cần được quản lý chặt chẽ đảm bảo tính chính xác, nhất quán, tích hợp giúp tiết kiệm việc nhập liệu	Cần thay đổi cách đầu tư, quản lý ứng dụng CNTT chú trọng đến quản lý dữ liệu. Các hệ thống CNTT cần có thiết kế mô hình dữ liệu phù hợp và theo kiến trúc dữ liệu quy định. Các ứng dụng cũ cần được tài liệu hóa lại

			và sử dụng các kỹ thuật ETL
9	Thông tin phải được lưu trữ, thu thập đầy đủ	Các thông tin đầu được thu thập và lưu trữ đầy đủ sẽ cho phép phát huy ứng dụng CNTT, làm giàu hiệu quả đầu tư, nâng cao độ tin cậy và tính hữu ích của thông tin.	Cần có quy định cụ thể về vòng đời của thông tin và nguyên tắc gắn trách nhiệm về thông tin.
10	Thông tin phải được quản lý tập trung, thống nhất	Mặc dù thông tin có thể nằm ở nhiều nơi, khả năng quản lý tập trung thống nhất sẽ cho phép dữ liệu có tính sẵn sàng cao, cập nhật chính xác, kịp thời, dễ dàng hơn để theo dõi vận hành, khắc phục sự cố và bảo đảm an toàn, an ninh thông tin.	Các hệ thống sẵn có cần được tích hợp, cần có chuẩn tích hợp dữ liệu cho dữ liệu. Cần tổ chức các hệ thống quản lý dữ liệu tập trung
11	Thông tin phải được chia sẻ tối đa	Thông tin được chia sẻ sẽ giúp giảm chi phí thu thập, nhập, tổng hợp, kiểm tra, đối chiếu, chuyển đổi thông tin, giúp hệ thống ứng dụng phục vụ người dùng hiệu quả hơn.	Các hệ thống cũ cần có cách chia sẻ dữ liệu có thể thông qua những nền tảng tích hợp. Những ứng dụng mới cần có dịch vụ chia sẻ dữ liệu

	Nhóm nguyên tắc cho công nghệ nền tảng		
12	Ưu tiên công nghệ nền tảng ứng dụng Web	Theo xu hướng phát triển mạng Internet, thiết bị di động và điện toán đám mây.	Những ứng dụng cũ có thể phải viết lại giao diện, hoặc nâng cấp.
13	Ưu tiên các công nghệ cho phép tích hợp chặt chẽ nhiều loại ứng dụng, chạy trên nhiều loại thiết bị đầu cuối và kết nối với các nền tảng khác	Nguyên tắc này tạo điều kiện chủ đầu tư không phụ thuộc vào công nghệ, cho phép đa dạng hóa hệ thống, thiết bị và dễ dàng hơn khi tích hợp và phục vụ nhiều người sử dụng hơn	Hệ thống cần tách phần xử lý và phần giao diện, đảm bảo tính tích hợp và chạy trên đa nền tảng
14	Công nghệ phổ biến, mở, nhiều lựa chọn giải pháp, dễ vận hành, can thiệp	Tránh tình trạng bị phụ thuộc vào nhà cung cấp, giảm tổng chi phí sở hữu	Việc lựa chọn công nghệ có thể khó hơn và có thể tăng chi phí.
	Nhóm nguyên tắc về bảo mật		
15	Bảo mật phải được triển khai đồng bộ tại tất cả các thành phần kiến trúc đồng bộ với quy trình, chính sách, đào tạo và đi kèm với giải pháp cụ thể phòng tránh thảm họa	Tránh tình trạng có các lỗ hổng bảo mật khi quá tập trung vào bảo mật một số thành phần trong khi xem nhẹ bảo mật các thành phần khác	Hệ thống mất mát, sai lệch dữ liệu

2.3. Các nguyên tắc về phát triển phần mềm ứng dụng

TT	Nguyên tắc	Co ư sở	Ảnh hưởng

TT	Nguyên tắc	Co ư sở	Ảnh hưởng
1	Kiến trúc Ứng dụng hướng dịch vụ, mở	Trong những năm tới, Tỉnh sẽ nhận được ngày càng nhiều những yêu cầu từ các bên liên quan về những dịch vụ của Tỉnh. Một số trong đó vẫn chưa được biết đến. Mục tiêu quan trọng là Tỉnh có thể đáp ứng các yêu cầu dịch vụ một cách nhanh chóng, và không bị giới hạn bởi một kiến trúc riêng, cố định.	Phương pháp xây dựng các ứng dụng hướng dịch vụ cần được áp dụng. Tại mọi thời điểm, cần đảm bảo rằng Kiến trúc Ứng dụng đáp ứng những Yêu cầu Nghiệp vụ (thực hiện Kiến trúc Nghiệp vụ). Những ứng dụng phải hỗ trợ những yêu cầu công việc của Tỉnh. Cần nỗ lực để bảo đảm rằng những ứng dụng càng thân thiện với người sử dụng càng tốt, và nhờ vậy bảo đảm rằng công tác nghiệp vụ sẽ đạt được lợi ích tối đa từ các ứng dụng. Các nhân viên của Tỉnh có thể sử dụng tốt các ứng dụng mà không cần phải có kiến thức CNTT chuyên sâu. Những dịch vụ (web) ứng dụng phải được công bố công khai. Những ứng dụng nên dựa trên các tiêu chuẩn mở, ví dụ như tiêu chuẩn bảng mã ký tự Unicode. Yêu cầu những ứng dụng thực hiện những tiêu chuẩn mở cần được đảm bảo là một phần của quy trình dự toán ngân sách. Việc thực hiện những tiêu chuẩn mở

TT	Nguyên tắc	Co ư sở	Ảnh hưởng
			có thể là một khoản đầu tư trong ngắn hạn, nhưng sẽ mang lại lợi ích trong dài hạn. Những ứng dụng phải có thể nâng cấp được. Những ứng dụng có thể chia sẻ mã nguồn, khi cần.
2	Những dịch vụ ứng dụng cần được công bố công khai	Để tăng cường việc sử dụng những ứng dụng và dữ liệu thống kê trong Tỉnh, thì cần phải công bố những dịch vụ ứng dụng. Nhờ vậy, mỗi dịch vụ không bị xây dựng lặp lại nhiều lần, mà được sử dụng lại mỗi khi cần.	Một danh mục các dịch vụ ứng dụng phải được thiết lập. Cuốn danh mục này sẽ bao gồm những định nghĩa mô tả dịch vụ và những thông tin liên quan (người sử dụng, thời gian, mức dịch vụ, …)
3	Kiến trúc Ứng dụng phải đảm bảo rằng những ứng dụng được tích hợp một cách dễ dàng	Tỉnh sẽ cần chức năng tích hợp mạnh đối với không chỉ các ứng dụng nội bộ mà còn đối với các ứng dụng của các bộ khác và của các bên liên quan khác của Tỉnh. Kiến trúc Ứng dụng phải đáp ứng được yêu cầu quan trọng này.	Cho phép khai thác và tích hợp dữ liệu từ nhiều nguồn dữ liệu khác nhau. Do vậy, những nguồn dữ liệu này cần phải được chuẩn hóa.

TT	Nguyên tắc	Co ư sở	Ảnh hưởng
4	Những ứng dụng phải sử dụng phần mềm được cấp phép.	Tỉnh muốn đảm bảo rằng tất cả các phần mềm được sử dụng đều phải là phần mềm được cấp phép chính thức.	Cần thiết lập cơ chế quản lý cấp phép, bao gồm những người chịu trách nhiệm và hệ thống quản lý giấy phép. Chức năng quản lý giấy phép sẽ giúp Tỉnh giám sát và đảm bảo rằng tại mọi thời điểm tất cả các phần mềm đang được sử dụng đều có giấy phép sử dụng, và tránh việc phải trả tiền cho những giấy phép không còn được sử dụng nữa.
5	Thứ tự ưu tiên cân nhắc triển khai ứng dụng: Tái sử dụng; Mua; Xây dựng. Trước tiên, Tỉnh sẽ cố gắng tái sử dụng những giải pháp đã được chấp nhận. Sau đó, Tỉnh mới cân nhắc việc mua và cài đặt các ứng dụng phần mềm thương mại (COTS) hoặc các ứng dụng phần mềm nguồn mở và miễn phí (FOSS) (phiên bản (n-1) – là phiên bản trước phiên bản mới nhất). Cuối cùng, Tỉnh mới cân nhắc việc tự phát triển các sản phẩm mới.	Tỉnh muốn tập trung vào những hoạt động lõi là các công việc thống kê, và đặt mức ưu tiên thấp nhất đối với việc tự xây dựng hệ thống CNTT. Tuy nhiên trước khi mua hệ thống mới, Tỉnh muốn tối thiểu hóa chi phí đầu tư bằng cách tái sử dụng đến mức tối đa có thể những hệ thống sẵn có.	Nhóm CNTT của Tỉnh sẽ phải duy trì sự hiểu biết sâu sắc về Kiến trúc CNTT hiện tại của Tỉnh để biết những thành phần nào có thể sử dụng lại được và những thành phần nào có thể được sử dụng bởi COTS và FOSS. Nhóm CNTT của Tỉnh sẽ phát triển phần mềm mới nếu phần mềm hiện có hoặc phần mềm COTS/FOSS không thích hợp.

TT	Nguyên tắc	Co ư sở	Ảnh hưởng
6	Sự lưu hành của những ứng dụng COTS (phiên bản (n-1)): Tỉnh sẽ hướng đến việc sở hữu những sản phẩm phiên bản (n-1), và tránh không là người sử dụng đầu tiên đối với những phiên bản mới chính thức, nhưng cũng tránh không để bị lạc hậu do sử dụng các phiên bản không còn được hỗ trợ bởi nhà cung cấp của những sản phẩm đó	Khi mua những ứng dụng COTS, Tỉnh muốn đảm bảo những giấy phép sử dụng của những ứng dụng này phải là mới (cập nhật) và hợp lệ. Việc chọn phiên bản (n-1) thông thường là cách phù hợp để đạt được điều này.	Hệ thống CNTT của Tỉnh sẽ thường là không có phiên bản mới nhất của các ứng dụng COTS, nhưng cũng không được để bị lạc hậu. Điều này đòi hỏi nhóm CNTT của Tỉnh phải theo dõi vòng đời của các ứng dụng COTS được sử dụng và biết khi nào cần mua hoặc nâng cấp.
7	Độc lập với hệ điều hành: Tất cả những ứng dụng được sử dụng trong Tỉnh cần hoạt động một cách độc lập (không phụ thuộc) tối đa với cơ sở hạ tầng hoặc hệ điều hành	Những ứng dụng độc lập với hệ điều hành và cơ sở hạ tầng tạo ra lợi nhuận cao hơn trên đầu tư và thông thường giảm chi phí tổng thể cho chủ sở hữu. Điều này cho phép sự linh động trong triển khai CNTT trong Tỉnh.	Việc lựa chọn giới hạn các ứng dụng COTS có thể giúp đạt được điều này. Với các hệ thống sẵn có không độc lập với hệ điều hành, Tỉnh sẽ phải có lộ trình để thay đổi. Các phần mềm trung gian nên được sử dụng để tách riêng những ứng dụng khỏi những giải pháp phần mềm cụ thể.
8	Độc lập kênh: Tất cả những ứng dụng phải được thiết kế và xây dựng để hoạt động độc lập (không phụ thuộc) kênh cung cấp và hỗ trợ đa kênh cung cấp	Ngày nay, người sử dụng dùng nhiều kênh khác nhau để truy cập dữ liệu của Tỉnh, và do vậy tất cả những ứng dụng cần phải đáp ứng được yêu cầu này.	Việc lựa chọn giới hạn các ứng dụng COTS có thể giúp đạt được điều này. Với các hệ thống sẵn có không độc lập kênh, Tỉnh sẽ phải có lộ trình để thay đổi.

TT	Nguyên tắc	Co ư sở	Ảnh hưởng
9	Tách biệt những nguyên tắc nghiệp vụ: Trong mọi trường hợp có thể, thì phải tách biệt và tập trung việc duy trì đặc tả của những nguyên tắc nghiệp vụ, và không được gắn chặt những nguyên tắc đó vào trong các ứng dụng	Những ứng dụng càng kém gắn kết với những nguyên tắc nghiệp vụ thì càng có tính linh động cao hơn. Điều này giúp đáp ứng tốt hơn với những thay đổi về quy trình nghiệp vụ của Tỉnh, và đồng thời nâng cao khả năng tái sử dụng.	Nguyên tắc này ngụ ý những ứng dụng hướng quản lý quy trình nghiệp vụ (BPM), khiến Kiến trúc Ứng dụng phức tạp hơn. Điều đó cũng có nghĩa là cần có một hệ thống quản lý quy trình nghiệp vụ ở trong Kiến trúc Tổng thể của Tỉnh.
10	Định hướng siêu dữ liệu: Trong mọi trường hợp có thể, thì những ứng dụng nên sử dụng siêu dữ liệu để định nghĩa và xử lý dữ liệu. Như vậy, những trường mô tả dữ liệu này không bị gắn cứng bên trong các ứng dụng.	Nghiệp vụ của Tỉnh phụ thuộc vào chất lượng dữ liệu, và điều này chỉ có thể được đảm bảo nhờ việc xử lý dữ liệu một cách nhất quán. Siêu dữ liệu được sử dụng vì mục đích này, và do vậy những ứng dụng phải được định hướng siêu dữ liệu.	Nguyên tắc này hàm ý tới những dịch vụ siêu dữ liệu ở trong Kiến trúc Ứng dụng, trong đó những ứng dụng có thể lấy được thông tin siêu dữ liệu tại thời điểm thiết kế và thời điểm chạy. Điều này cũng có nghĩa là cần có kho siêu dữ liệu và lớp các dịch vụ dữ liệu.
11	Giao diện người dùng nhất quán: Tất cả những ứng dụng của Tỉnh cần phải nhất quán về giao diện người dùng và cách thức tương tác với người dùng	Những ứng dụng của Tỉnh cần phải dễ sử dụng đối với người dùng. Giao diện người dùng nhất quán là mức cơ bản của yêu cầu này.	Nguyên tắc này hàm ý tới những tiêu chuẩn đối với giao diện đồ họa người dùng (GUI). Tỉnh phải xây dựng và duy trì những tiêu chuẩn về giao diện đồ họa người dùng cho tất cả các ứng dụng.

3. Hạ tầng kỹ thuật

Cơ sở hạ tầng CNTT&TT tỉnh Vĩnh Phúc bao gồm thiết bị đầu cuối; mạng MAN/WAN, Internet và Trung tâm dữ liệu. Nhằm quản lý và cung cấp các tài nguyên cơ sở hạ tầng cần thiết cho hoạt động của các dịch vụ và ứng dụng ở các

tầng phía trên của kiến trúc CQĐT tỉnh Vĩnh Phúc. Cơ sở hạ tầng phải được nâng cấp đồng bộ, theo chuẩn để triển khai theo mô hình điện toán đám mây hỗ trợ việc triển khai cơ sở hạ tầng CNTT như là dịch vụ (IaaS). Đây là xu thế mới trong CNTT giúp thúc đẩy việc đầu tư các trung tâm dữ liệu tập trung và được chia sẻ sử dụng trong nhiều cơ quan nhà nước dưới dạng các dịch vụ hạ tầng CNTT.

Các ứng dụng/dịch vụ được sử dụng cho mục đích tạo dựng hạ tầng CNTT được phân loại theo các nhóm sau:

- Hệ điều hành tạo dựng môi trường vận hành quản lý và chạy các phần mềm ứng dụng trên hệ thống máy tính.

- Quản trị lưu trữ cung cấp dịch lưu trữ dữ liệu trên các thiết bị vật lí của hạ tầng CNTT trong đó có các thiết bị chuyên dụng như SAN hoặc NAS. Ứng dụng quản trị lưu trữ cung cấp các tính năng cho phép sao lưu, nhân bản và phục hồi dữ liệu ở cấp độ bộ nhớ vật lý.

- Quản trị mạng cung cấp dịch vụ hỗ trợ kết nối mạng LAN, WAN và Internet cho các thiết bị CNTT. Ứng dụng quản trị mạng cung cấp các tính năng cho phép cấu hình và quản lý các đường truyền số liệu trong cơ sở hạ tầng CNTT.

- Dịch vụ ảo hóa là công nghệ được thiết kế để tạo ra tầng trung gian giữa hệ thống phần cứng máy chủ và phần mềm chạy trên nó. Công nghệ ảo hóa máy chủ cho phép từ một máy vật lí đơn lẻ có thể tạo thành nhiều máy ảo độc lập. Mỗi máy ảo đều có một thiết lập nguồn hệ thống riêng rẽ, hệ điều hành và các ứng dụng riêng.

- Đảm bảo độ sẵn sàng cao bao gồm các hệ thống cân bằng tải, hệ thống phân cụm cho phép tạo dựng môi trường sẵn sàng cao, phân phối khối lượng công việc lớn được thực hiện trên một cụm máy tính làm việc song song từ đó cải thiện năng suất hoạt động và tính sẵn sàng cao của cả hệ thống.

- An ninh thông tin cung cấp các công cụ hỗ trợ bảo mật trên nhiều tầng ứng dụng khác nhau bao gồm hạ tầng mã hóa công khai (PKI) và mã hóa bảo mật dữ liệu trên đường truyền như SSL.

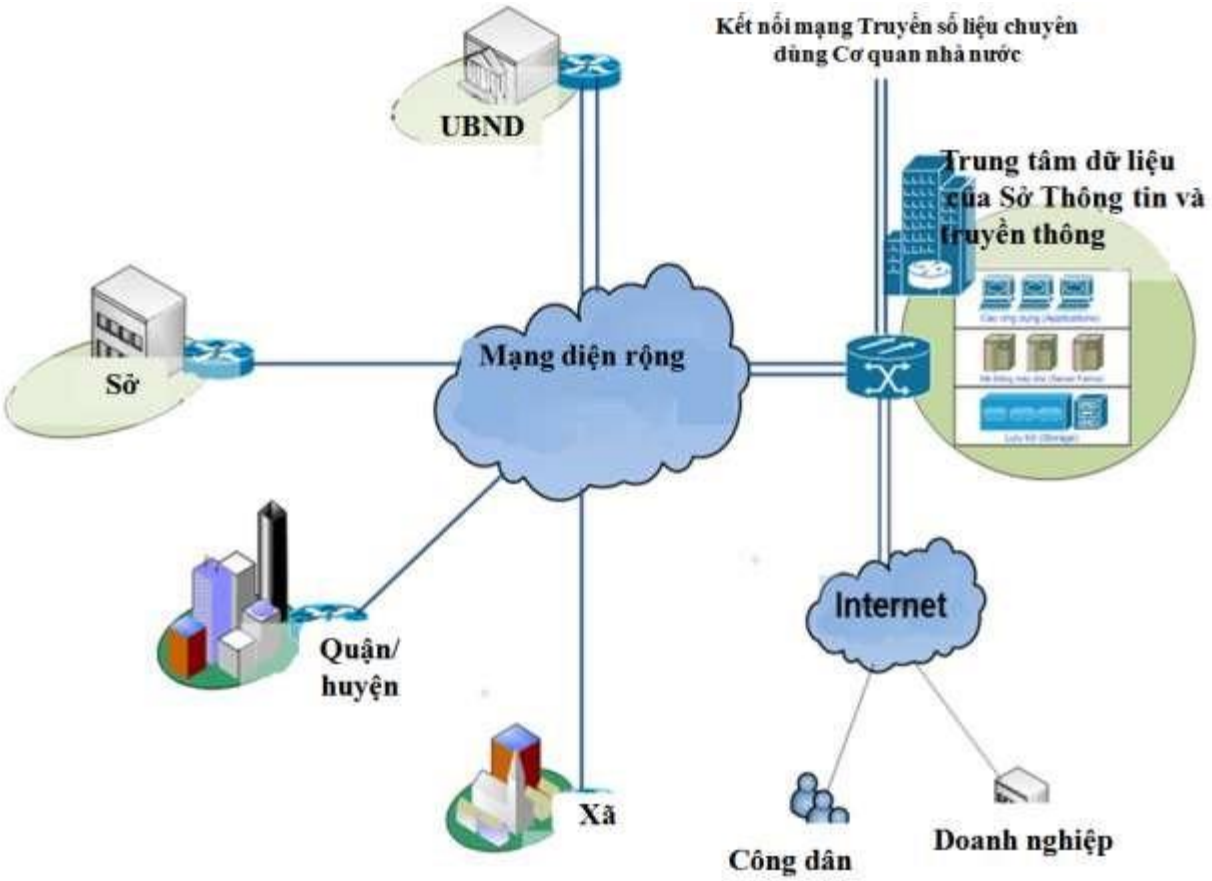
- Kiểm soát truy nhập dịch vụ này giúp kiểm soát việc truy nhập đối với các thành phần và các tài nguyên của hệ thống.

- An ninh mạng cung cấp các dịch vụ cho phép phòng ngừa ngăn chặn tấn công mạng của tin tặc thông qua hệ thống tường lửa và các phần mềm hỗ trợ phát hiện xâm nhập, phòng chống virus.

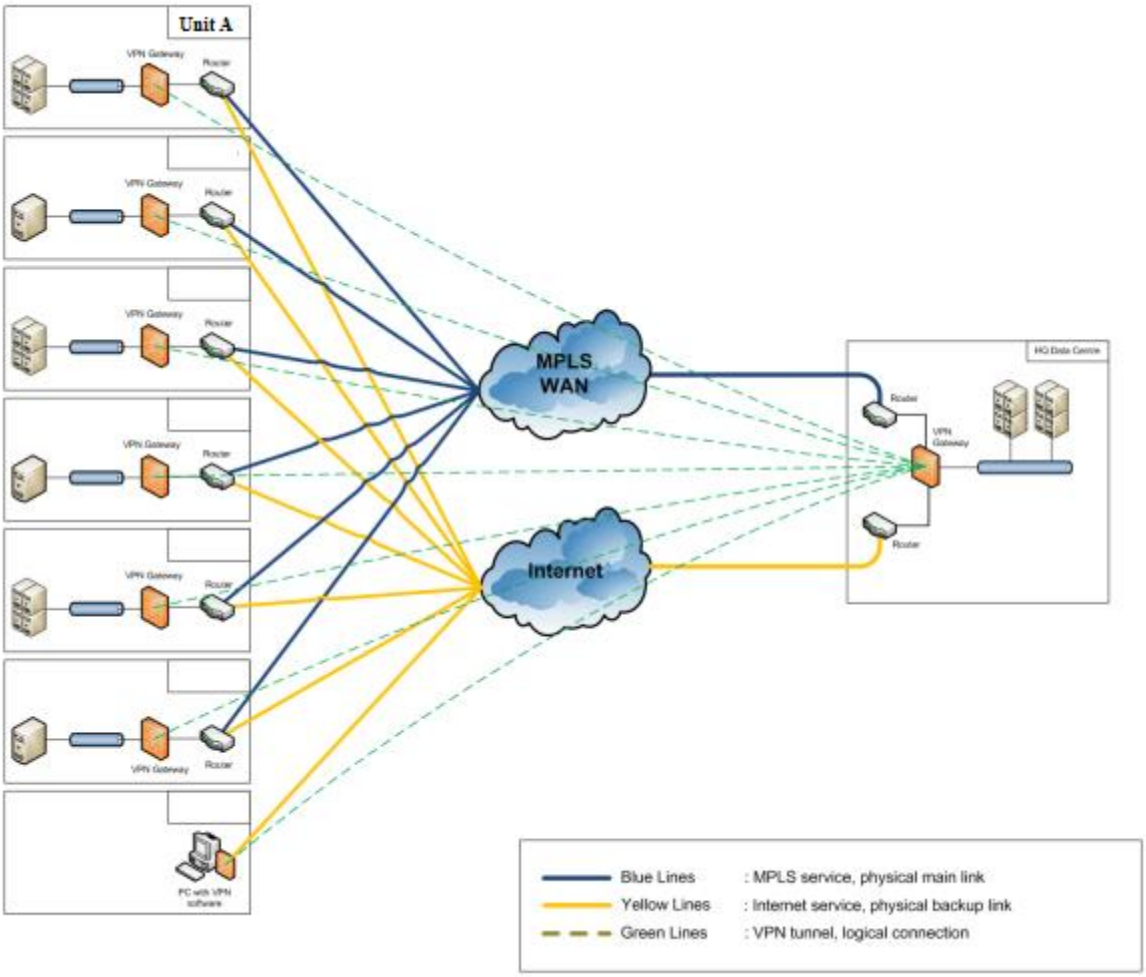
Sau đây là các mô tả cụ thể về hạ tầng kỹ thuật của tỉnh Vĩnh Phúc:

3.1. Xác định các mô hình mạng và nền tảng mạng truyền thông

3.1.1 Xác định mô hình mạng tổng thể, bao gồm trong nội bộ và kết nối ra bên ngoài của tỉnh (MAN, WAN)

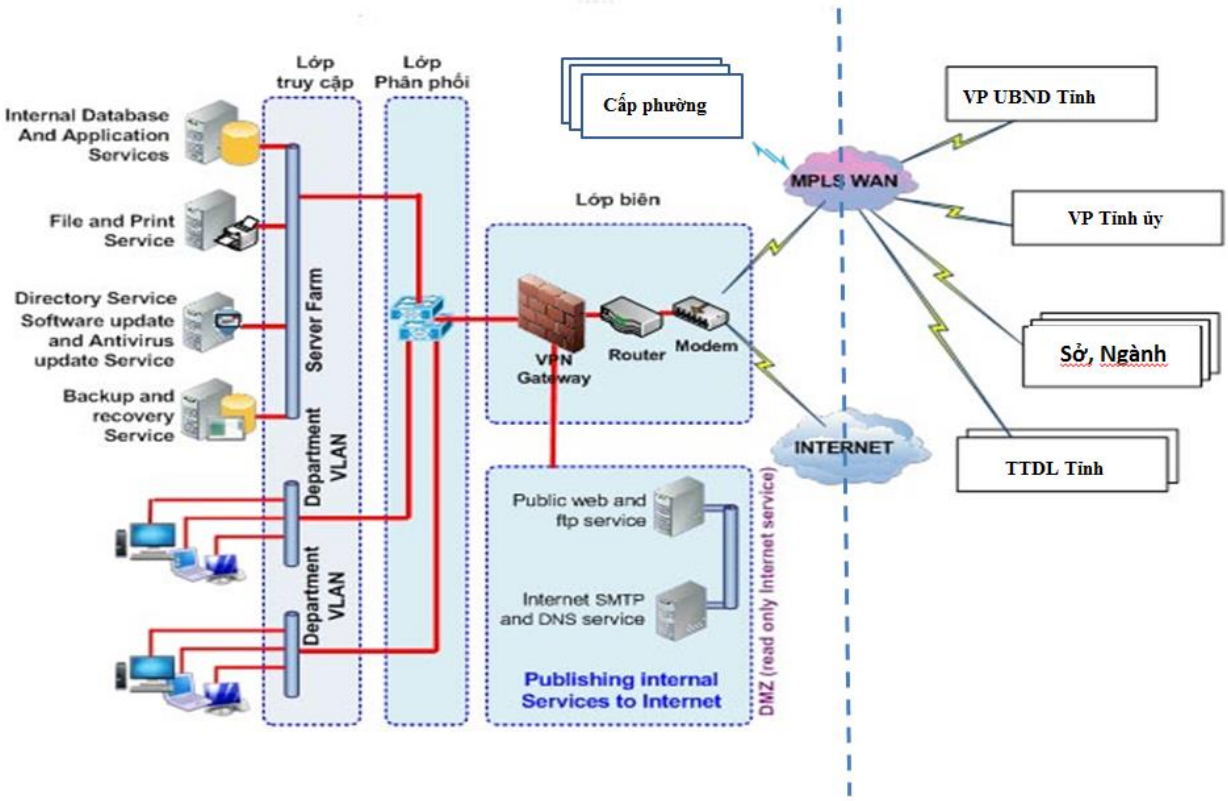


Mô hình kết nối mạng tổng thể

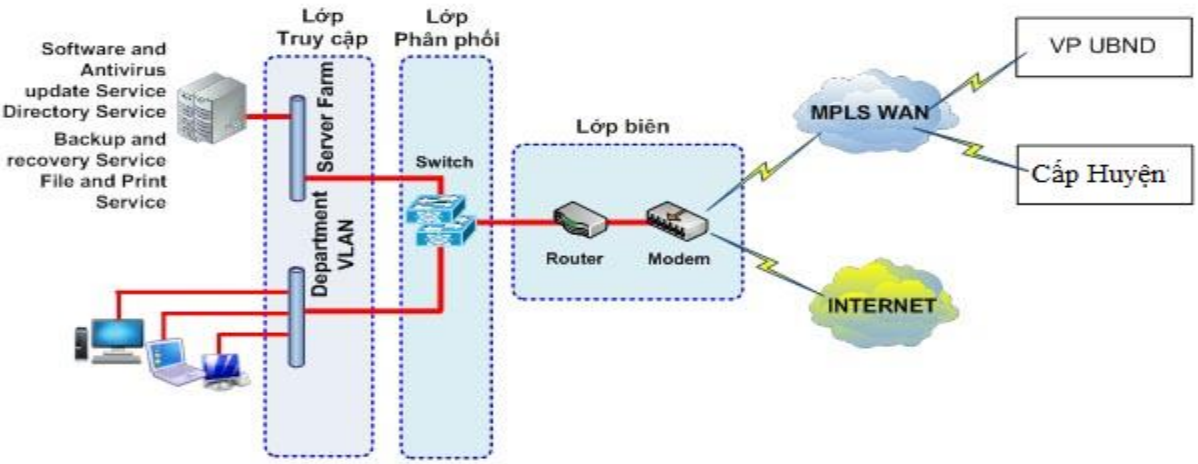


Mạng WAN tương lai sẽ sử dụng thiết kế Trung tâm đầu mối (Hub) và Spoke, nơi tất cả các đơn vị thuộc Tỉnh được kết nối tới một Trung tâm Điều hành mạng ở Trung tâm dữ liệu của tỉnh Vĩnh Phúc, sử dụng các kết nối VPN WAN. Các kết nối WAN có thể hoặc được dành riêng các đường dây mạng WAN, hoặc chạy các VPN tunnel trong kết nối Internet, sử dụng IPsec.

3.1.2 Xác định mô hình mạng điển hình của 1 cơ quan (LAN), sơ đồ kết nối với mạng chung của Tỉnh (MAN, WAN)

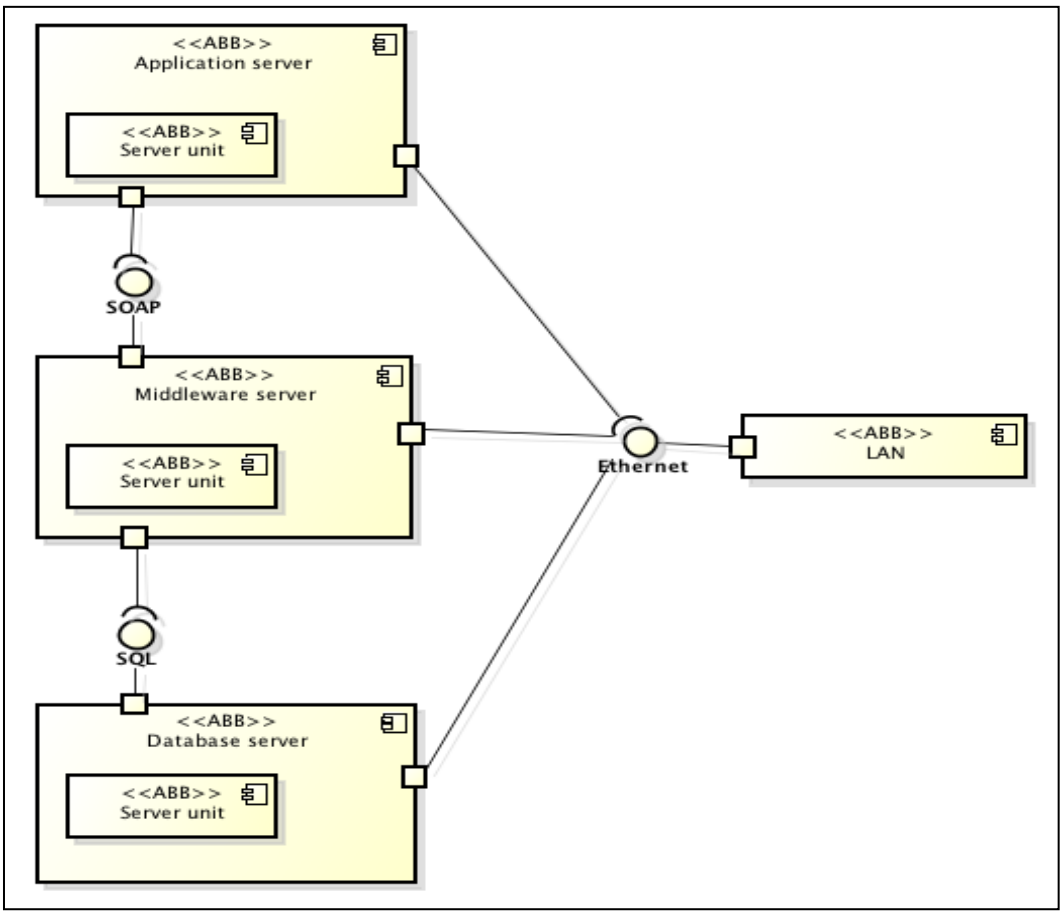


Mô hình điển hình mạng cấp Huyện



Mô hình điển hình mạng cấp Xã

Trong khi các mô hình trên mô tả điển hình của 01 cơ quan cấp Huyện, cấp Xã của tỉnh thì sau đây là minh họa cách thức kết nối các phân hệ kết thành hệ thống điển hình của 01 cơ quan để hình thành một cấu trúc liên kết hệ thống đơn giản trong mạng LAN trong một ứng dụng 3 tầng chung (a generic 3-tier application).



Mô hình điển hình tại 01 cơ quan (LAN)

Hình trên chỉ ra các phân hệ kết thành hệ thống "Máy chủ Ứng dụng", "Máy chủ Middleware" và "Máy chủ CSDL" đều có chứa một phân hệ "Đơn vị máy chủ" như một phần bên trong. Điều này minh họa cho đặc điểm tổng hợp của các phân hệ kết thành hệ thống được mô tả trước đó. Hình trên cũng chỉ ra tất cả các phân hệ đó được kết nối tới các phân hệ "Mạng LAN" thông qua giao diện "Ethernet" được cung cấp. Kết nối này có thể thực hiện được do giao diện "Ethernet" được xác định trong mô tả của tất cả các phân hệ kết thành hệ thống đó (tham khảo mô tả mỗi phân hệ kết thành hệ thống trong phần trước). Tương tự, "Máy chủ CSDL" cung cấp giao diện SQL mà "Máy chủ Middleware" đăng nhập

vào. Kết nối này có thể được thực hiện do mô tả của cả hai phân hệ kết thành hệ thống đều liệt kê SQL như một giao diện trong phần trước. Trường hợp tương tự áp dụng trong giao diện SOAP do "Máy chủ Middleware" cung cấp và "Máy chủ Ứng dụng" truy cập vào.

Tóm lại, một cấu trúc liên kết hệ thống hoặc một kiến trúc mục tiêu cho một hệ thống/ ứng dụng cụ thể có thể được thiết kế bằng việc kết nối các giao diện tương thích của các phân hệ kết thành hệ thống có sẵn. Thiết kế kết quả có thể sau đó được tái sử dụng như ABB trong việc xây dựng hệ thống/ ứng dụng khác thậm chí ở mức trừu tượng hơn, trong khi vẫn đồng thời giữ khả năng truy lại nguồn gốc xuất xứ của tất cả phân hệ theo các tiêu chuẩn công nghệ và các nguyên tắc quản lý của tỉnh.

3.1.3 Các nền tảng mạng

Các nền tảng Mạng là những công nghệ được sử dụng để đơn giản hóa quá trình truyền tải mạng thông tin giữa các thành phần ứng dụng và người dùng.

- Mạng giao dịch (Delivery Network): Mạng giao dịch là loại hình mạng được sử dụng để chuyển giao các ứng dụng và/ hoặc thông tin tới người dùng. Một số mạng giao dịch phổ biến hiện nay gồm có:
    - Internet: là hệ thống mạng máy tính toàn cầu mà người dùng tại bất kỳ máy tính nào, nếu có quyền, đều có thể lấy thông tin từ bất cứ một máy tính khác.
    - Intranet: là hệ thống mạng riêng trong tỉnh, có thể bao gồm nhiều mạng cục bộ (LAN) kết nối với nhau và được dùng để chia sẻ thông tin cũng như tài nguyên của cơ quan, đơn vị, tỉnh giữa các cán bộ.
    - Extranet: là hệ thống mạng riêng sử dụng giao thức Internet và hệ thống viễn thông công cộng để chia sẻ an toàn một phần thông tin trong tỉnh hoặc các hoạt động với các nhà cung cấp, liên doanh, đối tác, khách hàng hoặc các cơ quan, đơn vị khác. Mạng extranet có thể được xem như một phần của mạng intranet trong tỉnh nhưng được mở rộng với người dùng bên ngoài phạm vi quản lý của tỉnh.
    - Mạng riêng Ảo (Virtual Private Network - VPN): VPN tận dụng cơ sở hạ tầng viễn thông công cộng duy trì tính bảo mật thông qua việc sử dụng giao thức tạo đường hầm (tunneling protocol) và các

thủ tục bảo mật (security procedures).

- Chuyển tải mạng: Chuyển tải mạng là các phương tiện chức năng và thủ tục chuyển tải các chuỗi dữ liệu với độ dài biến đổi từ một máy chủ nguồn trên hệ thống mạng này đến một máy chủ đích trên hệ thống mạng khác, nhưng vẫn đảm bảo được chất lượng của dịch vụ. Một số giải pháp chuyển tải mạng phổ biến gồm có:
    - IP (Internet Protocol): là giao thức chính trong Tầng Internet (Internet Layer) của Bộ Giao thức Internet (Internet Protocol Suite) và có nhiệm vụ chuyển giao các gói dữ liệu (datagrams) từ máy chủ nguồn đến máy chủ đích hoàn toàn dựa trên địa chỉ của các gói dữ liệu này. Với mục đích này, IP xác định các phương pháp và cấu trúc ghi địa chỉ để đóng gói các gói dữ liệu.
    - Internetwork Packet Exchange (IPX): là giao thức tầng mạng mô hình OSI (OSI-model Network layer protocol) trong chồng giao thức IPX/SPX. Nhìn chung, việc sử dụng IPX đã giảm do sự bùng nổ của Internet đã làm TCP/IP gần như phổ biến trên toàn cầu. Máy tính và các hệ thống mạng có thể vận hành nhiều giao thức mạng, do đó, hầu như tất cả các điểm IPX sẽ chạy TCP/IP và cho phép kết nối Internet.
- Chuyển tải ứng dụng: Chuyển tải ứng dụng bao gồm tất cả các giao thức và phương thức thuộc lĩnh vực trao đổi thông tin giữa các quy trình (process-to-process communications) trong hệ thống mạng. Các phương thức chuyển tải ứng dụng sử dụng các giao thức tầng chuyển tải cơ sở để thiết lập kết nối giữa các máy chủ (host-to-host connections). Một số giải pháp về chuyển tải ứng dụng:
    - FTP (file transfer protocol - Giao thức truyền tập tin): là một chuẩn giao thức mạng sử dụng để truyền tập tin từ máy chủ này đến một máy chủ khác thông qua một mạng lưới có nền TCP, ví dụ như mạng Internet. FTP được phát triển trên kiến trúc khách-chủ, tận dụng kiểm soát riêng và kết nối dữ liệu giữa máy chủ và máy khách. Người dùng FTP có thể tự xác thực bằng cách sử dụng giao thức đăng nhập ở dạng văn bản thường (clear-text sign-in protocol) nhưng có thể kết nối ẩn danh nếu máy chủ cho phép.
    - SMTP (simple mail transfer protocol - giao thức truyền tải thư tín

đơn giản): là một chuẩn Internet truyền tải thư điện tử (e-mail) qua mạng Giao thức Internet (IP). SMTP bao gồm SMTP mở rộng (ESMTP), và là giao thức được dùng phổ biến hiện nay.

  - HTTP (hypertext transfer protocol - giao thức truyền tải siêu văn bản): là một giao thức mạng cho các hệ thống thông tin phân phối, hợp tác, siêu phương tiện. HTTP là cơ sở trao đổi dữ liệu cho World Wide Web (WWW).

- Các giao diện vật lý và kết nối: Các giao diện vật lý và kết nối là giao thức trao đổi thông tin cung cấp cơ chế kiểm soát ghi địa chỉ và truy cập kênh cho phép các thiết bị đầu cuối và các nút mạng có thể trao đổi thông tin trong một mạng đa điểm. Một số giao diện vật lý và kết nối:
  - Ethernet: tầng vật lý Ethernet đã phát triển qua một khoảng thời gian đáng kể và gồm nhiều giao diện truyền thông vật lý, dung lượng truyền khác nhau. Tốc độ thường dao động từ 1 Mbit/s đến 100 Gbit/s trong khi đó phương tiện vật lý phát triển từ cáp đồng trục, cáp xoắn, tới cáp quang. Nhìn chung, phần mềm chồng giao thức mạng sẽ hoạt động tương tự nhau trong tất cả các tầng vật lý.
  - IEEE 802.11: là tập hợp các chuẩn thực hiện trao đổi thông tin trên máy tính trong mạng cục bộ không dây (WLAN), băng tần tần số 2.4, 3.6, và 5 GHz. Các băng tần tần số này được tạo ra và duy trì bởi IEEE LAN/MAN Standards Committee (IEEE 802). Phiên bản hiện tại của chuẩn này là IEEE 802.11-2007. Các chuẩn này cung cấp cơ sở cho mạng không dây Wi-Fi.
  - Giao diện Dữ liệu Phân bố theo Cáp sợi quang (Fiber Distributed Data Interface-FDDI): cung cấp chuẩn quang truyền tải dữ liệu trong mạng cục bộ với tốc độ 100 Mbit/s và có thể hoạt động trong khu vực 200km (124 dặm). Mặc dù cấu trúc topo lôgíc FDDI là mạng vòng chuyển thẻ bài, nhưng cấu trúc này không sử dụng giao thức vòng chuyển thẻ bài IEEE 802.5 như nền tảng của mình; thay vào đó, giao thức của FDDI bắt nguồn từ giao thức thẻ bài với mạng BUS IEEE 802.4.
- Các dịch vụ mạng hỗ trợ: Các dịch vụ mạng hỗ trợ là các giao thức hỗ trợ được sử dụng để trợ giúp việc quản lý mạng. Một số dịch vụ mạng hỗ trợ:

- DNS (domain name system - Hệ thống tên miền): là hệ thống đặt tên theo thứ tự được phát triển trên cơ sở dữ liệu phân tán cho máy vi tính, dịch vụ, hoặc bất kì nguồn nào kết nối với Internet hoặc một mạng riêng. Quan trọng nhất là, DNS chuyển tên miền có ý nghĩa đối với con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị này khắp thế giới.
- DHCP (dynamic host configuration protocol - Giao thức cấu hình động máy chủ): là giao thức cấu hình tự động được sử dụng trên hệ thống mạng IP. Máy tính kết nối vào mạng IP phải được cấu hình trước khi trao đổi thông tin với các máy tính khác trong hệ thống mạng. DHCP cho phép một máy tính được cấu hình một cách tự động vì thế sẽ giảm việc can thiệp của người quản trị vào hệ thống mạng. DHCP cũng cung cấp một cơ sở dữ liệu trung tâm để theo dõi tất cả các máy tính kết nối vào hệ thống mạng nhằm tránh trường hợp hai máy tính khác nhau lại có cùng địa chỉ IP.

3.2. Xác định mô hình triển khai trung tâm dữ liệu

Trong tương lai, tỉnh Vĩnh Phúc cần tiếp tục hoàn thiện Trung tâm dữ liệu hiện đại của Tỉnh, đáp ứng yêu cầu của các hệ thống CNTT, CSDL, trong đó có các hệ thống chính quyền điện tử.

- Có hạ tầng hiện đại theo tiêu chuẩn quốc tế.
- Có kiến trúc mạng và bảo mật đảm bảo phục vụ các kết nối an toàn đến các hệ thống thông tin tại Trung tâm.
- Trung tâm dữ liệu được đặt tại vị trí an toàn, đảm bảo tránh được bão, lụt và các thảm họa thiên nhiên khác.
- Trung tâm được đặt tại địa điểm được bảo vệ an toàn.
- Có diện tích đáp ứng yêu cầu của các hệ thống hiện tại cũng như khả năng mở rộng trong tương lai.
- Có đường giao thông thuận tiện, đáp ứng yêu cầu vận chuyển thiết bị, nhiên liệu phục vụ hoạt động của trung tâm.
- Được cung cấp nguồn điện ổn định từ lưới điện quốc gia.
- Có kết nối đến các nhà cung cấp viễn thông khác nhau, đảm bảo các kết nối WAN và Internet với chất lượng ổn định, băng thông đáp ứng yêu

cầu.

- Trung tâm được thiết kế đáp ứng các tiêu chuẩn quốc tế về Data Center (tiêu chuẩn Tier 3 của Uptime Institute, TIA-942, ASHRAE...).
- Có hệ thống sàn nâng, máng cáp theo tiêu chuẩn. Có hệ thống vách ngăn chống cháy và cửa cường lực đảm bảo an toàn cho trung tâm cũng như cho nhân viên vận hành.
- Có hệ thống máy phát điện riêng đảm bảo hoạt động khi có sự cố về điện lưới. Hệ thống bồn chứa nhiên liệu đảm bảo trung tâm có thể hoạt động tối thiểu 24h khi có sự cố điện lưới.
- Có hệ thống UPS công suất lớn, hoạt động theo chế độ online, được thiết kế theo tiêu chuẩn N+1, đảm bảo hệ thống luôn vận hành liên tục, ổn định không bị ngắt quãng.
- Có hệ thống điều hòa chuyên dụngcho trung tâm dữ liệu, đảm bảo môi trường hoạt động theo tiêu chuẩn cho các hệ thống máy móc, thiết bị CNTT.
- Có hệ thống giám sát hoạt động, hệ thống cảnh báo cháy nổ, rò rỉ nước...
- Có hệ thống phòng chống cháy chuyên dụng cho trung tâm dữ liệu, đảm bảo các yêu cầu về phòng chống cháy nổ.
- Có hệ thống camera giám sát, hệ thống an toàn bảo mật hệ thống.

a) Các phòng chức năng trong TTDL

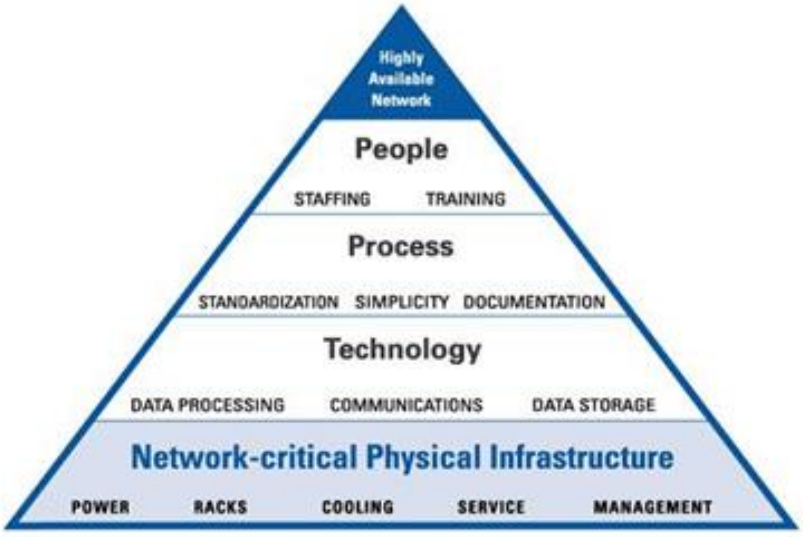
Diện tích mặt bằng Trung tâm dữ liệu phải đủ để bố trí các phòng chức năng sau:

- Phòng máy chủ: Dùng để lắp đặt và cài đặt các hệ thống máy chủ, phần mềm ứng dụng, hệ thống lưu trữ, hệ thống mạng và bảo mật, truyền dẫn
- Phòng PCCC: Dùng để lắp hệ thống bình khí và tủ điều khiển hệ thống phòng cháy chữa cháy.
- Phòng M&E: Dùng để lắp đặt hệ thống phân phối điện chính như tủ điện MSB, UPS, Battery UPS
- Phòng NOC: Phòng giám sát và vận hành các hệ thống trong TTDL
- Phòng Staging: Dùng để kiểm tra, cài đặt thiết bị trước khi đưa và lắp đặt trong TTDL, bảo trì các thiết bị trong TTDL

- Phòng Warehouse: Dùng để chứa các thiết bị dự phòng phục vụ vận hành TTDL

Ngoài ra, Trung tâm dữ liệu cũng phải đảm bảo bố trí không gian hành lang: dùng để đi lại và vận chuyển thiết bị phục vụ TTDL.

Để đảm bảo đầu tư, vận hành, khai thác hiệu quả tất cả các yêu cầu như sự gia tăng của công suất nguồn, công suất làm lạnh do sự gia tăng của các thiết bị lưu trữ dữ liệu, cáp truyền dẫn, … thì trung tâm dữ liệu cần đảm bảo cơ sở vật lý hạ tầng thiết yếu-NCPI (Network- Critical Physical Infrastructure). Phương pháp xây dựng TTDL dựa trên việc chuẩn hóa các thành phần của TTDL thành các khối chuẩn, mở và có khả năng mở rộng. Mô hình của NCPI như sau:



Mô hình của Mạng hạ tầng vật lý thiết yếu

Mô hình NCPI bao gồm:

- Hệ thống nguồn điện;
- Hệ thống UPS;
- Hệ thống phân phối nguồn;
- Hệ thống máy phát điện;
- Tủ Rack;
- Hệ thống làm mát;
- Hệ thống cáp mạng;
- Hệ thống truyền thông;

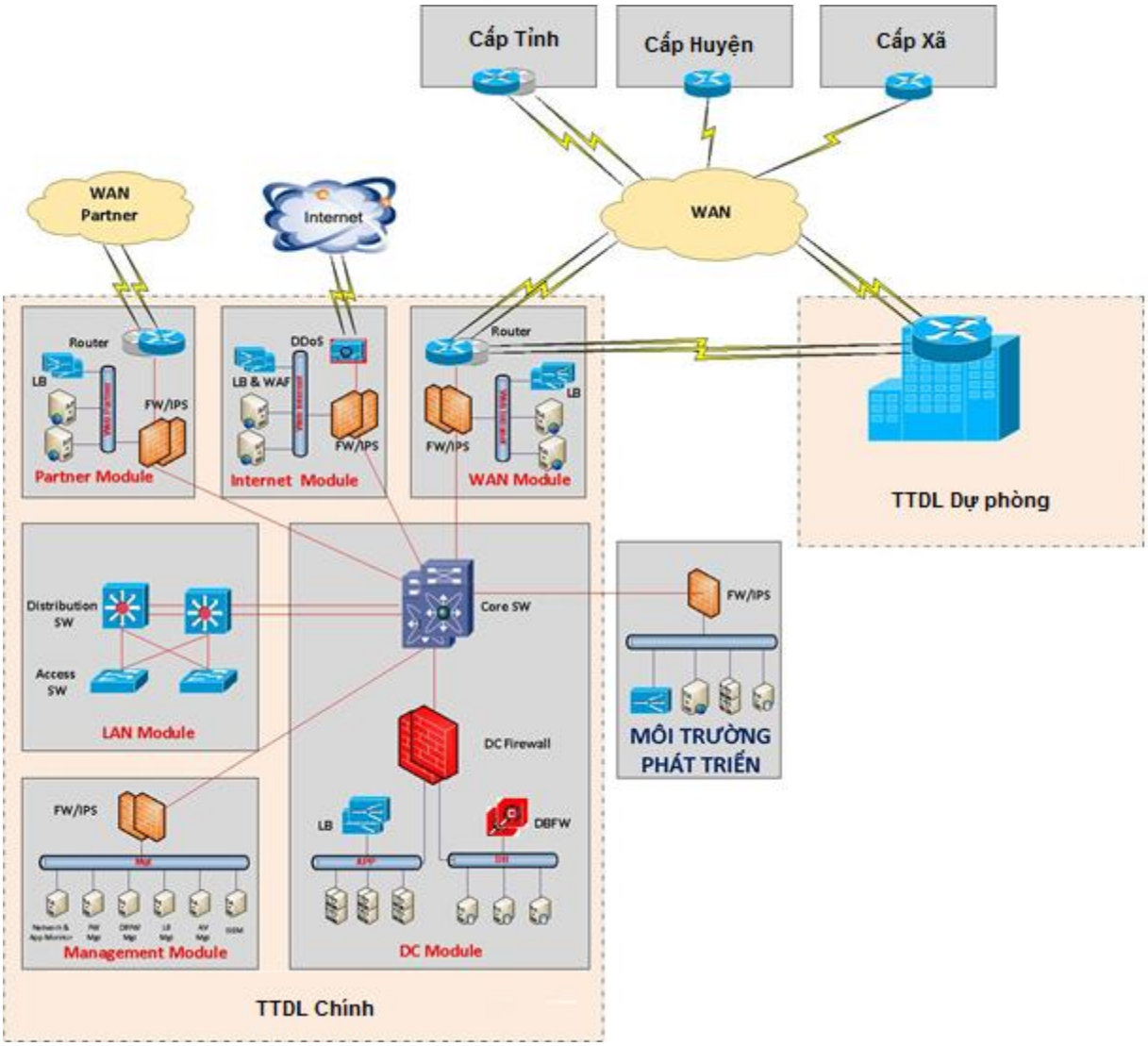
- Hệ thống quản trị;

- Hệ thống báo động, đo nhiệt độ môi trường và báo cháy báo nổ, phòng cháy, chữa cháy;

- Hệ thống dịch vụ…

b) Sơ đồ kiến trúc tổng thể Trung tâm dữ liệu của Tỉnh

Sơ đồ thiết kế tổng thể Trung tâm dữ liệu tỉnh Vĩnh Phúc được thể hiện trên hình sau:



TTDL của tỉnh Vĩnh Phúc cần phải được thiết kế để đảm bảo tính sẵn sàng cao nhất và năng lực thực thi phục vụ các hệ thống ứng dụng nghiệp vụ và CSDL của tỉnh sẽ bao gồm: TTDL Chính và TTDL Dự phòng. Thiết kế sơ bộ cho DC (DR có mô hình tương tự DC nhưng công suất có thể sẽ được tính toán với năng

lực tương đương khoảng 70% DC) được dựa trên phương pháp thiết kế phân lớp (Hierarchical) và và mô-đun (Modular). Dựa trên phương pháp thiết kế phân lớp và module, TTDL của tỉnh sẽ bao gồm các thành phần:

- **Data Center:** Là thành phần quan trọng nhất trong TTDL quốc gia về dân cư, nơi đặt toàn bộ các hệ thống máy chủ ứng dụng và database của hệ thống CSDL của toàn tỉnh. Thành phần bao gồm các thiết bị Core Switch giữ vai trò định tuyến và chuyển tiếp lưu thông giữa các phân hệ, Switch cung cấp kết nốivới tốc độ 10 Gbps cho các Server, các thiết bị chuyên dụng như Firewall, thiết bị cân bằng , tường lửa CSDL. Mô hình mạng trong TTDL được thiết kế theo mô hình Leaf-spine với Core switch đóng vai trò Spine và các switch/blade switch đóng vai trò Leaf. Hệ thống bảo vệ bao gồm 1 cặp firewallcó cấu hình cao, chạy chế độ HA, đảm bảo tính sẵn sàng cao và đảm bảo cho lưu lượng vào các máy chủ không bị tắc nghẽn. Một cặp thiết bị database firewall được đặt trước các máy chủ database, kiểm soát tất cả các hành động có tác động đến hệ thống cơ sở dữ liệu trong máy chủ, thiết bị này có khả năng bypass khi gặp sự cố, không ảnh hưởng đến hệ thống. Trên mỗi máy chủ cơ sở dữ liệu đều được triển khai thành phần agent database firewall nhằm tăng cường tính bảo mật cho dữ liệu;

- **WAN**: Là thành phần hội tụ các kết nối mạng đến từ các đơn vị cấp Tỉnh, Huyện, Xã trên địa bàn tỉnh; ngoài ra còn có đường truyền kết nối giữa TTDL chính và TTDL dự phòng để đồng bộ và trao đổi dữ liệu giữa hai TTDL. Thành phần WAN bao gồm các WAN Router, WAN Firewall tích hợp IPS. Các WAN router có nhiều vụ tạo các tunnel qua mạng MPLS VPN và định tuyến đến các đơn vị. Hệ thống bảo mật cho phân hệ WAN gồm 1 cặp firewall tích hợp IPS đều chạy chế độ HA, cung cấp tính sẵn sàng cao cho hệ thống. Module này kết nối giữa 2 TTDL và kết nối từ TTDL đến các đơn vị cấp Tỉnh/Huyện/Xã. Các đơn vị kết nối đến phân hệ WAN đều là các hệ thống trực thuộc. Vì vậy, thiết bị firewall chỉ cần trang bị các tính năng chính như firewall, IPS... Kết nối, truy cập từ các đơn vị đến TTDL sẽ được kiểm soát bởi hệ thống policy trên firewall, chỉ các kết nối được cho phép mới có thể đi vào trong TTDL. Các truy cập được cho phép đi qua firewall sẽ được kiểm soát bởi cặp IPS để phát hiện và ngăn chặn kịp thời các nguy cơ tấn công. Trong phân hệ WAN còn có một cặp thiết bị cân bằng tải để giảm tải cho DC tại lúc cao điểm hoặc khôi phục hệ thống từ DR. Cặp thiết bị này có thể hoạt động ở chế độ Active-Active hoặc Active-Standby;

- **Internet:** Thành phần cho phép quảng bá các những dịch vụ phục vụ tra cứu

thông tin chung cho người dùng trên Internet, cung cấp dịch vụ Internet cho người dung trong trung tâm. Thành phần bao gồm các Thiết bị giảm thiểu DDoS , Internet Firewall tích hợp IPS, thiết bị cân bằng tải và tường lửa ứng dụng Web. Hệ thống bảo mật bao gồm 1 cặp firewall tích hợp IPS chạy chế độ HA, cung cấp tính sẵn sàng cao cho hệ thống. Môi trường internet ẩn chứa rất nhiều mối nguy: Tấn công từ chối truy cập (DDoS), malware, hacker... Vì thế, thiết bị firewall cần được trang bị nhiều tính năng hơn như antivirus, antispam, URL Filtering, anti-bot, application control, IPS …Tường lửa chuyên dụng cho ứng dụng Web (WAF) đóng vai trò lọc toàn bộ kết nối nguy hiểm đến các máy chủ web, bảo vệ trước những nguy cơ như ăn cắp hoặc sửa đổi dữ liệu. Thiết bị cân bằng tải thực hiện cân bằng tải cho nhiều đường Internet theo cả chiều Inbound va Outbound, cân bằng tải cho ứng dụng Web, chuyển người dùng giữa DC và DR để giảm tải cho DC cũng như khôi phục thảm họa.

- Extranet (Partner Module): Thành phần này cung cấp các cổng kết nối cho các đơn vị bên ngoài địa bàn tỉnh có thể truy cập vào những ứng dụng, dữ liệu để trao đổi thông tin, liên thông nghiệp vụ hoặc thao tác các ứng dụng theo ngành dọc. Thành phần bao gồm các Extranet Router, Extranet Firewall tích hợp IPS, thiết bị cân bằng tải. Hệ thống bảo mật bao gồm 1 cặp firewall tích hợp IPS chạy chế độ HA, cung cấp tính sẵn sàng cao cho hệ thống. Module này kết nối giữa TTDL tạiTp. Hà Nội và các bộ, ban, ngành, đều là các hệ thống có tính an toàn cao hơn so với kết nối Internet, vì vậy thiết bị firewall chỉ cần trang bị các tính năng chính như firewall, IPS.. Kết nối, truy cập từ các sở đến TTDL sẽ được kiểm soát bởi hệ thống policy trên firewall, chỉ các kết nối được cho phép mới có thể đi vào trong TTDL. Thiết bị cân bằng tải thực hiện cân bằng tải cho nhiều đường WAN theo cả chiều Inbound va Outbound, cân bằng tải cho ứng dụng Web, chuyển người dùng giữa DC và DR để giảm tải cho DC cũng như khôi phục thảm họa.

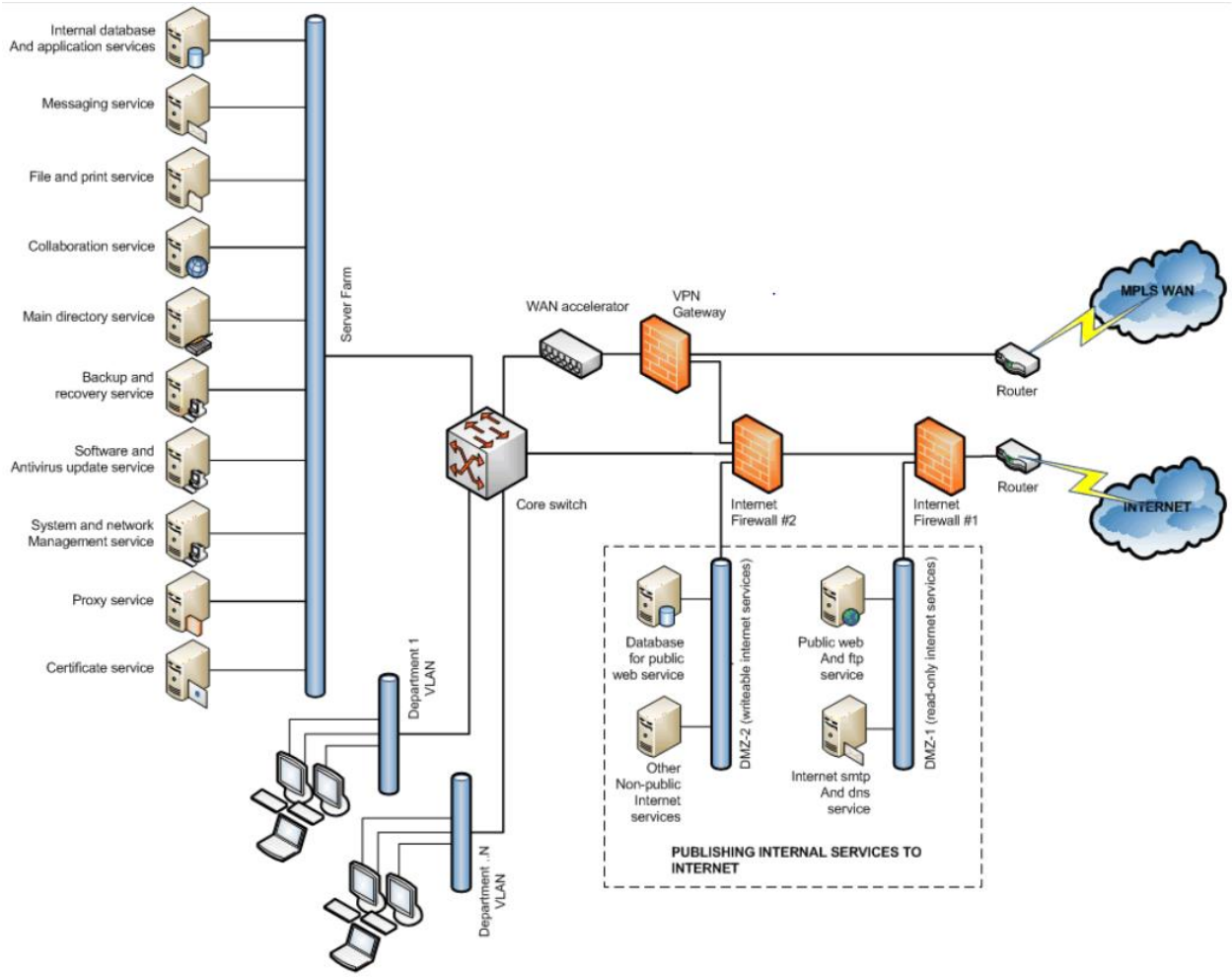
- LAN: Thành phần cung cấp truy cập cho người dùng làm việc trong TTDL. Thành phần bao gồm các Distribution Switch và Access Switch;

- Quản trị: Thành phần cung cấp các dịch vụ quản trị mạng, quản trị an ninh, quản trị hệ thống server và storage, và hệ thống anti-virus. Thành phần bao gồm các phần mềm quản trị và thiết bị quản trị chuyên dụng. Các kết nối quản trị thông qua giao diện riêng độc lập với các kết nối truyền dữ liệu (OOB - Out of Band Management)

Ngoài ra, TTDL còn có thể mở rộng một môi trường mới là Môi trường phát

triển, kiểm thử, đào tạo, được xây dựng với mục đích giúp các cán bộ kỹ thuật tỉnh Vĩnh Phúc có khả năng làm chủ các hệ thống CNTT trong tương lai.

c) Mô hình mạng TTDL trong tương lai



Mô hình mạng Trung tâm dữ liệu tương lai

- Thiết kế mạng cần đáp ứng các mục tiêu:
  - Tuân theo kiến trúc thiết kế phân tầng Hierarchical và Modular
  - Hiệu năng mạng: Hệ thống mạng cần phải có một hiệu năng tốt để phục vụ truyền tải thông tin và các ứng dụng bên trong mạng, tránh xảy ra bất cứ hiện tượng nghẽn trên mạng, thời gian phản hồi chậm, hoặc mức độ sử dụng tài nguyên thiết bị mạng.
  - Tính Module hóa: Thiết kế mạng trên cơ sở module hoá các thành phần trong mạng sẽ đảm bảo việc phân tách một hệ thống mạng

phức tạp thành các cấu phần nhỏ hơn, đảm bảo dễ dàng, thuận lợi trong vận hành, quản lý và bảo trì cũng như khả năng cô lập các sự cố.

- Tính sẵn sàng và tin cậy: Việc đảm bảo tính ổn định và tin cậy cũng là một mục tiêu rất cần thiết trong thiết kế mạng. Thiết kế mạng Data Center cần phải đảm bảo tính sẵn sàng cao nhất, tránh điểm lỗi đơn trên mạng với:
  - Khả năng dự phòng đối với các thiết bị quan trọng như Core Switch, Core Router…, các thành phần của thiết bị như bộ xử lý trung tâm, các module giao tiếp, các module dịch vụ…
  - Khả năng dự phòng cho các đường kết nối vật lý giữa các thiết bị
  - Khả năng sẵn sàng và tin cậy thông qua các giao thức OSPF, HSRP, STP…
- Khả năng mở rộng: Thiết kế mạng Data Center phải có khả năng mở rộng về qui mô và nâng cấp các dịch vụ mới một cách dễ dàng mà không làm thay đổi kiến trúc.
- Khả năng quản trị: Thiết kế mạng Data Center cần đảm bảo khả năng quản trị tập trung, đơn giản và dễ dàng, hỗ trợ một cách nhanh chóng việc xác định, cô lập và khắc phục sự cố.
- Thỏa mãn nhu cầu của ứng dụng và dịch vụ.

d) Hệ thống bảo mật cho TTDL

Quan điểm để xây dựng chính sách bảo mật: An ninh mạng là một tiến trình lặp đi lặp lại, bao gồm các bước xoay vòng như sau:

- Xác định các đối tượng cần được bảo vệ (máy chủ, các tài nguyên, các ứng dụng, các thiết bị mạng, máy trạm, người dùng…);

- Xác định các hiểm họa có thể gây nên cho mạng và hệ thống;

- Thiết lập chính sách an ninh cho mạng, bao gồm các nhà lãnh đạo, quản lý và tin học, quản trị mạng và người dùng;

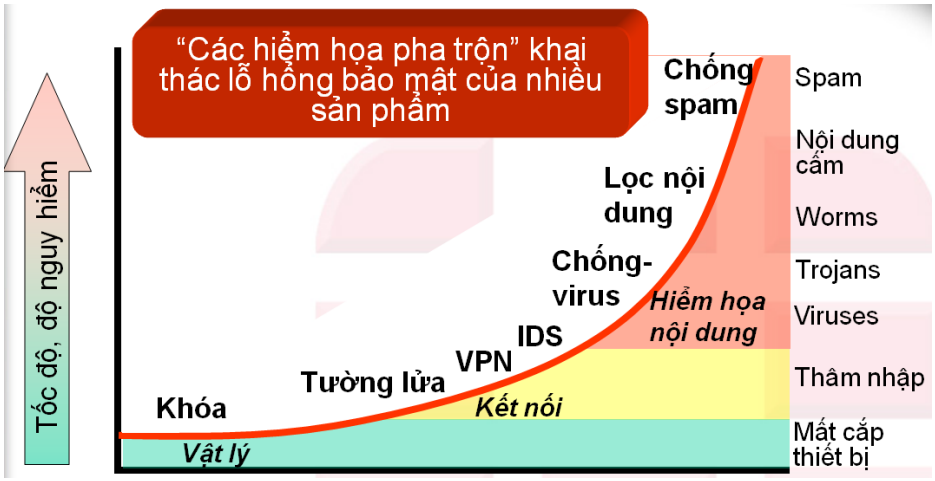
- Thiết lập các chính sách an ninh mạng bằng các phương pháp điện tử và hành chính. Các phương pháp điện tử bao gồm: Thiết kế quy hoạch lại mạng, Firewall, VPN, IDS, ACS và quản trị an ninh mạng;

- Theo dõi an ninh mạng và phản ứng lại các biểu hiện bất thường;

- Kiểm tra chính sách an ninh và các thiết bị an ninh mạng để đáp ứng các thay đổi;

- Tiếp tục theo dõi và quản lý an ninh mạng, thay đổi chính sách an ninh và cấu hình các thiết bị an ninh mạng để phù hợp với ngữ cảnh an ninh mới.

Xu hướng phát triển các hiểm họa bảo mật như sau:



Có rất nhiều giải pháp bảo mật, mỗi giải pháp tập trung vào bảo vệ một đối tượng cụ thể:

- Firewall

Là thiết bị tường lửa thế hệ mới. Với các tường lửa thế hệ mới này hệ thống có thể được bảo vệ từ lớp mạng đến lớp ứng dụng do Firewall thế hệ mới ngoài các tính năng quản lý truy cập dựa trên thông tin lớp mạng (IP) và lớp truyền dẫn (port), Firewall này còn có khả năng quản lý các ứng dụng (hiểu được ứng dụng và can thiệp vào các tác vụ trong ứng dụng), người dùng. Firewall cũng cung cấp các tính năng quản lý băng thông để hệ thống mạng tối ưu hóa hiệu năng sử dụng. Ngoài ra trên Firewall thế hệ mới cũng có thêm các lựa chọn Anti-virus, Antispam, chống tấn công DoS… trong đó tính năng Anti-virus cũng có thể được dùng để cung cấp thêm một lựa chọn bảo vệ nữa cho hệ thống.

- IPS (Intrusion prevention systems)

Là thiết bị phát hiện và ngăn chặn tấn công. Thiết bị này giám sát luồng dữ liệu đi qua nó phát hiện những mẫu tấn công, các luồng dữ liệu bất thường, và dựa trên hành vi của các luồng dữ liệu mà chủ động ngăn chặn các tấn công. Thiết bị này có thể chống tấn công Malware, tấn công nhằm giảm hiệu năng thiết bị. Trong hệ

thống có 2 lớp IPS, lớp thứ nhất để bảo vệ các Web Server và bảo vệ tấn công từ mạng bên ngoài, lớp thứ 2 bảo vệ các máy chủ ứng dụng và CSDL trong vùng Server Farm.

- **WAF**: Tường lửa ứng dụng web (Web Application Firewall - WAF)

Là một thiết bị phần cứng hoặc phần mềm được cài lên máy chủ có chức năng theo dõi các thông tin được truyền qua giao thức http/https giữa trình duyệt của người dùng và máy chủ web tại lớp 7. Một WAF có khả năng thực thi các chính sách bảo mật dựa trên các dấu hiệu tấn công, các giao thức tiêu chuẩn và các lưu lượng truy cập ứng dụng web bất thường. Đây là điều mà các tường lửa mạng khác không làm được. Một số tính năng của thiết bị tường lửa ứng dụng Web (WAF):

- Cho phép nhận diện và xử lý các dạng tấn công phổ biến như XSS, CSRF, các loại tấn công Injection...
- Tự động xây dựng một mô hình bảo mật bảo vệ ứng dụng bằng cách liên tục theo dõi hoạt động của người dùng theo thời gian thực.
- Bảo vệ tấn công thay đổi giao diện web: Tự động phục hồi lại ứng dụng bằng các bản đã lưu khi phát hiện có tấn công thay đổi giao diện web.

- Giải pháp chống **DDoS** dựa trên DDoSAppliance: Ngày nay các cuộc tấn công từ chối dịch vụ DDoS là thách thức lớn nhất của các tổ chức cung cấp dịch vụ ra Internet như dịch vụ Cổng thông tin điện tử về dân cư. Các tiếp cận truyền thống như Firewall, IPS, WAF sử dụng cơ chế Stateful không ngăn chặn DDoS hiệu quả, nhiều khi còn chính là đối tường để các hacker thực hiện tấn công DDoS. Các tổ chức cần phải có một giải pháp hoàn toàn mới theo hướng Stateless. Giải pháp này thức hiện theo 4 bước:

1. Cài đặt DDoS Appliance ở vùng biên
2. Pháp hiện tấn công DDoS dựa trên stateless
3. Ngăn chặn
4. Cảnh báo

- **SIEM (Security information and event management):** Giải pháp hệ thống quản trị, phân tích log tập trung và quản lý sự kiện an ninh; thực hiện thu thập log từ nhiều nguồn khác nhau, phân tích và đánh giá mức độ an ninh và rủi ro của các sự kiện an toàn thông tin, nhanh chóng nhận diện, đánh giá mức độ và đáp trả các chính sách sai phạm, các tấn công từ bên ngoài và các mối đe dọa từ bên trong. Hỗ trợ xử lý sự cố: thông qua các công cụ phân tích điều tra, tạo luồng phối hợp công việc xử lý sự cố, tạo lập cơ sở dữ liệu về các sự cố để tiện tra cứu sau này. Bên

cạnh đó còn có các giải pháp quét virus trên các máy chủ, máy trạm và tại cổng kết nối với mạng bên ngoài mà điển hình là Internet. Ngoài ra là các giải pháp mạng riêng ảo (VPN) mã hóa các dữ liệu trên đường truyền, kiểm soát truy cập web (Web Filtering, URL Filtering) giảm thiểu các nguy cơ mất an toàn cho các máy trạm khi truy cập web, ngăn chặn thư rác (Spam Mail), ...

Mỗi sản phẩm bảo mật của mỗi nhà cung cấp có một thế mạnh riêng. Tuy nhiên mỗi hệ thống CNTT cần trang bị tối thiểu 3 giải pháp sau:

1. Giải pháp an ninh tích hợp: Tích hợp các tính năng như tường lửa (firewall), mạng riêng ảo (VPN), ngăn chặn xâm nhập (Intrusion Prevention - IPS), quét virus tại cổng kết nối mạng(anti-virus), kiểm soát truy cập web của các nhân viên (Web Filtering, URL Filtering)...;
2. Giải pháp phòng ngừa virus: Ngoài giải pháp an ninh tích hợp, cần vẫn thêm giải pháp phòng ngừa virus cho các máy chủ và các máy trạm.
3. Giải pháp quản trị phân tích log tập trung và quản lý sự kiện An ninh (SIEM)

Xu hướng của nhiều hãng bảo mật với các sản phẩm bảo mật đơn lẻ hiện nay là mở rộng, tích hợp thêm nhiều chức năng bảo mật khác thành một sản phẩm. Điển hình là nhiều sản phẩm firewall trước kia giờ đây được gọi là giải pháp tường lửa thế hệ mới (Next Generation Firewall - NGFW) với việc tích hợp các chức năng Firewall dựa trên công nghệ kiểm soát sâu vào gói tin (DPI - Deep Packet Inspection), IPS, URL filtering, Antivirus, Anti-spam, Anti-botnet,kiểm soát ứng dụng (Application Control), chống thất thoát dữ liệu (Data Loss Prevention)... trên cùng một thiết bị.

Ngoài ra, để đảm bảo an toàn của hệ thống đối với các lỗi logic trong dữ liệu của CSDL như tính toàn vẹn, hợp lý, đồng bộ dữ liệu, thay đổi cố ý về nội dung thông tin gây sai lệch đến tính đúng đắn của dữ liệu…, có thể áp dụng các giải pháp sau:

- Thiết lập tầng CSDL trung gian: Trong mô hình này, một CSDL trung gian (proxy) được xây dựng giữa ứng dụng và CSDL gốc. CSDL trung gian này có vai trò mã hóa dữ liệu trước khi cập nhật vào CSDL gốc, đồng thời giải mã dữ liệu trước khi cung cấp cho ứng dụng. CSDL trung gian đồng thời cung cấp thêm các chức năng quản lý khóa, xác thực người dùng và cấp phép truy cập;

- Sử dụng giải pháp tường lửa chuyên dụng cho cơ sở dữ liệu. Giải pháp chuyên dụng cần có các tính năng:

+ Quản lý rủi ro: Tìm và phân loại dữ liệu nhạy cảm bên trong CSDL, quét và phát hiện điểm yếu, cấu hình chưa tốt trên CSDL. Lập báo cáo phân tích rủi ro dựa theo quan hệ giữa điểm yếu và dữ liệu cũng như mức độ nhạy cảm của dữ liệu, trên cơ sở này lập chính sách bảo vệ và đưa ra biện pháp giảm nhẹ rủi ro.Với các điểm yếu được phát hiện, hệ thống cung cấp bản vá ảo (Virtual Patching) trên thiết bị cho phép bảo vệ các điểm yếu một cách nhanh chóng và trong suốt trong khi chưa thể thực hiện việc sửa chữa và cài đặt bản vá vào hệ thống CSDL;

+ Giám sát các truy cập tới dữ liệu nhạy cảm: Các giao dịch trên CSDL, đặc biệt các truy cập, tác động tới dữ liệu nhạy cảm được audit (ghi log) liên tục. Các thông tin Audit cung cấp đầy đủ chi tiết cho mỗi phiên giao dịch với CSDL như ai, thao tác lên đối tượng, dữ liệu nhạy cảm gì, sử dụng công cụ, câu lệnh gì, thao tác như thế nào, khi nào và tại đâu,…Chức năng Audit hoạt động một cách độc lập với hệ quản trị CSDL, người quản trị CSDL không can thiệp được, không làm ảnh hưởng tới hiệu năng của máy chủ CSDL. Các thông tin Audit độc lập với CSDL và được lưu trữ bảo mật, cung cấp báo cáo, chứng cứ tin cậy khi xem xét các sự cố an ninh;

+ Kiểm soát truy cập CSDL: Giải pháp có thể nhìn sâu vào mọi hành động trên CSDL như các login, các truy vấn (SELECT), các thao tác của user cũng như của DBA (DML, DDL, DCL), các thay đổi liên quan đến dữ liệu, thủ tục, cấu trúc CSDL để giúp ngăn chặn các thao tác trái quyền.Chính sách bảo vệ dữ liệu được thiết lập để kiểm soát người dùng, ứng dụng và thao tác CSDL. Chính sách có thể quy định từ người dùng nào (user, DBA), sử dụng công cụ gì, được phép tác động tới đối tượng/dữ liệu gì, và được tác động dữ liệu như thế nào. Những thao tác trái quyền tới dữ liệu nhạy cảm có thể bị ngăn chặn hoặc cảnh báo vi phạm. Giải pháp có thể phân tích dữ liệu trả ra từ CSDL từ các câu lệnh truy vấn, kết quả trả ra chứa dữ liệu nhạy cảm có thể được cảnh báo hoặc ngăn chặn.Cơ chế tự học các giao dịch CSDL (Dynamic Profiling) cho phép hiểu các hoạt động bình thường, ngăn chặn các hành vi bất thường trái với quy luật thông thường. Dynamic Profiling sẽ học một (nhóm) người dùng, thường hay sử dụng công cụ gì, thường có những thao tác gì với những đối tượng dữ liệu nào và mức độ ra sao. Ví dụ việc truy vấn, hoặc sửa đổi số lượng bản ghi lớn vượt quá ngưỡng bình thường sẽ bị cảnh báo/ngăn chặn. Cung cấp chức năng IPS - phát hiện và ngăn chặn các tấn công trong thời gian thực tại mức hệ điều hành, mức giao thức cũng như mức các thao tác SQL, chống tấn công SQL Injection;

+ Quản lý thông tin phân quyền: Chức năng quản lý thông tin tài khoản - User Right Management (tùy chọn, cần mua thêm license), cho phép phân tích quyền được cấp cho tài khoản và đối tượng dữ liệu mà quyền tác động.

- Sử dụng cơ chế sẵn có trong CSDL:

+ Các hàm Stored Procedure trong CSDL cho chức năng mã hóa và giải mã;

+ Sử dụng cơ chế View trong CSDL tạo các bảng ảo, thay thế các bảng thật đã được mã hóa;

+ Cơ chế "instead of" trigger được sử dụng nhằm tự động hóa quá trình mã hóa từ View đến bảng gốc.

- Phân quyền truy cập dữ liệu theo vai trò của người dùng;

- Sử dụng cơ chế log của hệ quản trị CSDL để theo dõi, giám sát quá trình cập nhật dữ liệu;

- Thiết lập cơ chế backup định kỳ hoặc đột xuất dữ liệu cho hệ thống;

- Thiết lập các quy tắc cảnh báo trên hệ quản trị CSDL, cho phép thông báo tới quản trị hệ thống và ngăn chặn kịp thời các truy xuất bất thường đến hệ thống dữ liệu.

Mô hình tham chiếu hệ thống bảo mật TTDL

e) Hệ thống máy chủ

Hệ thống máy chủ và lưu trữ của Trung tâm dữ liệu được thiết kế để đáp ứng các tiêu chí quan trọng như sau:

Chức năng

- Tiêu chí đầu tiên và quan trọng khi thiết kế hệ thống là các khối chức năng trong hê thống trong TTDLS. Các chức năng chính của các cấu phần trong hệ thống bao gồm:
- Chức năng xử lý trong phân hệ ứng dụng được thiết kế cho các máy chủ ứng dụng Web/App
- Chức năng xử lý và quản trị Cơ sở dữ liệu tập trung, xây dựng trên các cặp máy chủ CSDL hoạt động ở chế độ song hành (clustering), cho phép xử lý và quản trị toàn bộ CSDL tập trung của Tỉnh.
- Chức năng quản trị thiết bị và hệ thống; được xây dựng phục vụ công tác

quản trị thiết bị trong hệ thống, quản trị công tác sao lưu và khôi phục dữ liệu trong hệ thống

- Chức năng lưu trữ tập trung được phục vụ trên hê thống lưu trư tập trung, với công nghệ hiện đại, đảm bảo tính sẵn sang và ổn định của toàn bộ dữ liệu của TTDL Tỉnh.
- Chức năng sao lưu và khôi phục dữ liệu: được quan tâm như là giải pháp đảm bảo sự an toàn của dữ liệu tập trung, trên cơ sở sử dụng những công nghệ sao lưu và khôi phục mới nhất, cùng phần mềm quản trị sao lưu tập trung.

Năng lực xử lý

- Tiêu chí năng lực xử lý của hệ thống được sử dụng nhằm xây dựng một hệ thống hạ tầng máy chủ, lưu trữ, sao lưu và khôi phục dữ liệu cho các hệ thống ứng dụng của Tỉnh, đáp ứng yêu cầu hiện tại và khả năng mở rộng trong tương lai.
- Tiêu chí năng lực xử lý được quan tâm đến khi lựa chọn công nghệ và thiết bị cho từng cấu phần trong hê thống, cụ thể như sau:
- Hệ thống máy chủ CSDL sử dụng máy chủ có năng lức xử lý đáp ứng yêu cầu của ứng dụng nghiệp vụ và khả năng mở rộng trong tương lai
- Hê thống máy chủ ứng dụng sử dụng máy chủ x86 có khả năng xử lý mạnh, với bộ xử lý Intel Xeon với tốc độ cao, nhiều nhân xử lý
- Hệ thống lưu trữ tập trung sử dụng thiết bị lưu trữ tầm trung, với tính sẵn sàng và độ ổn định cao nhất cho dữ liệu tập trung.
- Hệ thống SAN Switch sử dụng công nghệ xử lý và chuyển mạch tốc 10Gb FC, cho phép kết nối hệ thống máy chủ, hệ thống lưu trữ và sao lưu trong toàn bộ hệ thống với tốc độ cao.

Năng lực mở rộng

- Năng lực mở rộng của các thiết bị cũng là một tiêu chí được quan tâm khi thiết kế hệ thống. Các thiết bị chính được thiết kế cho phép mở rộng trong tương lai (trong nội bộ các thiết bị) và khả năng mở rộng về thiết kế.
- Khả năng mở rộng về thiết kế được thể hiện ở những điểm sau:
- Phân hệ ứng dụng (App Zone) được thiết kế cho phép mở rộng bằng các

thêm các máy chủ vào Phân hệ ứng dụng

- Phân hệ CSDL được thiết kế với khả năng hoạt động song hành của cụm cluster với sự hỗ trợ xử lý song song
- Phân hệ lưu trữ được thiết kế với các SAN Switch kết nối dự phòng cao, khả năng mở rộng thông qua việc mở rộng cổng trên SAN Switch hoặc sử dụng công nghệ cascade các SAN Switch với nhau.

Khả năng quản lý

- Tiêu chí về khả năng quản lý được đặt ra đảm bảo dễ dàng trong quá trình vận hành, khai thác hệ thống và khắc phục khi có sự cố xảy ra. Khả năng quản lý được xem xét khi lựa chọn các thiết bị trong hệ thống. Khả năng quản lý được đánh giá ở một số điểm sau:
- Khả năng quản lý thiết bị (Hardware)
- Khả năng quản lý môi trường (Hệ điều hành/cluster)
- Khả năng quản trị môi trường ảo hóa trên nền tảng VMWare
- Khả năng quản lý sao lưu và khôi phục dữ liệu

Tiết kiệm chi phí

- Tiêu chí tiết kiệm chi phí được xem xét khi lựa chọn thiết bị và giải pháp đảm bảo tiết kiệm trong đầu tư ban đầu, cũng như bảo vệ đầu tư trong tương lai.

Khả năng kết nối

- Thiết kế đáp ứng các yêu cầu chính đặt ra khi kết nối hệ thống các thiết bị trong hệ thống bao gồm:
- Đảm bảo kết nối giữa các thành phần hệ thống với nhau:
    - Các hệ thống máy chủ được kết nối với hạ thống mạng Ethernet, tốc độ 10Gb/s thông qua các cổng 10Gb trên các máy chủ
    - Các máy chủ ứng dụng Web/App đảm bảo kết nối với người dùng và kết nối với phân hệ dữ liệu (các máy chủ CSDL)
    - Các máy chủ CSDL kết nối với các máy chủ ứng dụng, các máy chủ quản trị sao lưu và khôi phục dữ liệu
    - Các hệ thống máy chủ cần kết nối với hệ thống lưu trữ được trang bị các HBA cung cấp các giao diện 10Gb Fibre Channel, để kết nối với

mạng SAN tập trung

- Các hệ thống lưu trữ tập trung, các hệ thống thư viện băng từ và máy chủ quản trị sao lưu và khôi phục dữ liệu được kết nối với nhau qua mạng SAN tốc độ cao, phục vụ công việc lưu trữ dữ liệu, sao lưu và khôi phục dữ liệu khi cần

- Đảm bảo băng thông:
  - Băng thông kết nối mạng Ethernet giữa các thiết bị trong hệ thống được đảm bảo tốc độ 10Gb/s.
  - Băng thông kết nối các máy chủ với hệ thống SAN được thiết kế với tốc độ 8Gb/s thông quan mạng cáp quang SAN chuẩn FC. Hệ thống SAN switch với khả năng chuyển mạch cao sẽ đáp ứng yêu cầu hiện tại và mở rộng trong tương lai của hệ thống.
- Các hệ thống lưu trữ tập trung, hệ thống thư viện băng từ được kết nối với hệ thống SAN switch tốc độ cao, đảm bảo không tắc nghẽn khi phục vụ các ứng dụng.
- Đảm bảo tính sẵn sàng
- Mỗi máy chủ trong hệ thống: từ máy chủ ứng dụng, máy chủ CSDL đến các máy chủ quản trị, đều được trang bị ít nhất 2 card mạng tốc độ 10Gb/s, với 2 cổng trên 1 card, đảm bảo tính sẵn sàng cao nhất về kết nối từ các máy chủ đến hệ thống mạng Etnernet trung tâm
- Tương tự đối với các kết nối FC, các hệ thống máy chủ được trang bị HBA với 2 cổng FC, đảm bảo kết nối dự phòng đến hệ thống mạng SAN và đến các hệ thống lưu trữ và sao lưu tập trung.
- Hệ thống SAN switch được thiết kế dự phòng, bao gồm 02 SAN Switch, đảm bảo tính sẵn sàng cao từ các máy chủ đến hệ thống mạng SAN. Trong trường hợp 1 SAN Switch có sự cố, hệ thống vẫn hoạt động bình thường.

f) Hệ thống điều hành, giám sát an ninh mạng

Hệ thống điều hành, giám sát an ninh mạng phải đáp ứng các yêu cầu sau:

- Giám sát mạng:
  - Tình trạng hoạt động các thiết bị
  - Băng thông, đường truyền.

- Lập sơ đồ logic hoạt động toàn hệ thống
- Lập báo cáo chi tiết về hiệu năng toàn hệ thống
- Giám sát các ứng dụng như cơ sở dữ liệu, hệ thống email...
- Giám sát hệ thống ảo hóa
- Giám sát hệ điều hành
- Giám sát hệ thống Server
- Cảnh báo các yếu tố bất lợi đối với hệ thống qua hệ thống thư điện tử, SMS, RSS, WEB.

g) Hệ thống lưu trữ, sao lưu

Hệ thống lưu trữ đóng một vai trò hạt nhân vô cùng quan trọng trong một hệ thống. Với vai trò là thành phần trực tiếp lưu trữ dữ liệu tích hợp của tổ chức, thiết kế của hệ thống lưu trữ sẽ ảnh hưởng trực tiếp đến hiệu suất hoạt động, mức độ an toàn dữ liệu cũng như khả năng đáp ứng dịch vụ dữ liệu một cách liên tục của toàn bộ hệ thống. Giải pháp sao lưu, lưu trữ đảm bảo tuân thủ mô hình lưu trữ tập trung dựa trên công nghệ lưu trữ mạng tiên tiến nhất, đáp ứng các yêu cầu sau:

- Khả năng đáp ứng uyển chuyển (Scalability): Hệ thống phải có khả năng mở rộng dung lượng dễ dàng, nhanh chóng theo yêu cầu. Hệ thống lưu phải cho phép nâng cấp từ một volume (phục vụ một máy chủ) lên tới hàng nghìn volumes (phục vụ hàng nghìn máy chủ khác nhau) với chức năng nhiều truy cập đồng thời tới mỗi volume.
- Tính ổn định (Stability): Hệ thống lưu trữ phải được thiết kế để đảm bảo tối đa sự an toàn của dữ liệu, cũng như khả năng sẵn sàng phục vụ liên tục của dữ liệu. Hệ thống cũng cho phép triển khai các chức năng Disaster Recovery cho phép lưu trữ và phục hồi lại dữ liệu từ các thảm hoạ tồi tệ nhất (như cháy nổ, động đất ...)
- Tốc độ (Speed): Hệ thống lưu trữ phải có khả năng đáp ứng tốc độ kết nối cao, giảm thiểu thời gian truy cập cho người sử dụng và các ứng dụng.
- Khả năng chia sẻ, dùng chung dữ liệu (Shareability): Hệ thống cần được thiết kế cho phép hợp nhất dữ liệu trùng lặp, sao cho số lượng các bản sao vật lý của dữ liệu là tối thiểu, cùng với khả năng cho phép nhiều ứng dụng hay nhiều máy chủ với hệ điều hành khác nhau (Windows, Linux, Solaris,

HP-UX, AIX…) có thể truy cập đồng thời vào các dữ liệu này.

- Tính đơn giản (Simplicity): Hệ thống lưu trữ phải được thiết để đơn giản hoá tối đa các thao tác quản trị, tích hợp và cấu hình cho phép triển khai hay nâng cấp nhanh chóng, sử dụng dễ dàng, nâng cao độ tin cậy và giảm các chi phí vận hành bảo trì sau này.

Hệ thống lưu trữ cung cấp khả năng quản lý lưu trữ tập trung, đảm bảo an toàn và cung cấp không gian lưu trữ cho các máy chủ trong toàn hệ thống như: máy chủ Database, máy chủ Mailbox Database và các máy chủ ảo hoá … có khả năng cung cấp mở rộng dung lượng lưu trữ khi cần thiết. Các yêu cầu đối với hệ thống lưu trữ tại TTDL:

- Tài nguyên phải được dự phòng với một mức độ nhất định để đảm bảo đáp ứng được các biến đổi bất thường về nhu cầu sử dụng tài nguyên tại một vài thời điểm nhất định.
- Các thiết bị máy chủ và lưu trữ phải đảm bảo dự phòng cho tất cả các thành phần và các kết nối. Nhằm giúp cho các ứng dụng có đủ tài nguyên để hoạt động một cách liên tục.
- Đảm bảo khả năng quản trị đơn giản, dễ dàng và tập trung. Đồng thời phải có khả năng backup và phục hồi nhanh nhất khi xảy ra sự cố.

Đối với hệ thống sao lưu thì hiện nay có hai loại công nghệ sao lưu đang được sử dụng phổ biến là:

- Công nghệ sao lưu ra băng từ (công nghệ truyền thống) hay còn được gọi là Disk to Disk to Tape.

- Công nghệ sao lưu ra tủ đĩa hay còn được gọi là Disk to Disk.

Công nghệ sao lưu băng từ gồm các giải pháp sau:

- **Tape drive** (thay băng tape bằng tay khi băng tape đầy dữ liệu):

+ DAT Drives: Là công nghệ tầm thấp thường dùng cho các doanh nghiệp nhỏ với độ tin cậy và chi phí thấp;

+ LTO (LTO1-200GB, LTO2-400GB, LTO3-800GB, LTO4-1.6TB, LTO5-3TB) Ultrium Drives: có dạng half- and full-height là loại cao cấp hơn DAT với băng tape dung lượng lớn hơn và hiệu suất cao hơn.

- **Tape Autoloader** được thiết kết theo kiểu nạp băng tape tự động (cho các

băng tape trắng vào khe ổ tape sau đó băng nào đầy được tự động thay băng mới vào để backup tiếp dữ liệu) Tape Autoloader thường cho các công ty với các đặc điểm sau:

+ Ngăn chặn việc thay băng tape bằng tay mất thời gian và bị động, phải có người theo dõi khi băng tape đầy để thay băng mới;

+ Có dữ liệu nhiều hơn băng tape;

+ Hiệu suất cao, hiệu quả cao.

- Tape Library: Là thiết bị sao lưu dạng tự động, với dung lượng lớn (nguồn dữ liệu ở nhiều nơi), thời gian nhanh, hiệu suất cao. Đây là giải pháp hoàn hảo, quản trị đơn giản, để dàng thao tác, vừa khít với nhiều môi trường của khách hàng, làm việc trên LAN, SAN, được trang bị những công cụ thông minh.

Phương thức sao lưu disk-to-disk được phát triển để khắc phục thời gian truy nhập dữ liệu trong quá trình phục hồi. Sao lưu theo phương thức disk-to-disk (gọi ngắn gọn là d2d, hay còn được nhắc đến với thuật ngữ kỹ thuật disk-to-disk-to-tape hoặc tape-cache backup) về mặt vật lý là khi dữ liệu trước hết được sao lưu từ đĩa cứng sang đĩa cứng, thay vì sang băng từ như trong phương thức thông thường. Dữ liệu từ đĩa cứng sao lưu, sau khi được lưu trữ một thời gian dài cần thiết, mới được chuyển tiếp (sao chép, hoặc tạo bản clone) sang băng từ vật lý tại thời điểm được kích hoạt tùy theo nhu cầu của người quản trị. Như vậy quá trình phục hồi dữ liệu phần lớn sẽ là chuyển dữ liệu ngược lại từ đĩa cứng sang đĩa cứng, giảm thiểu được thời gian truy cập vào dữ liệu cần được phục hồi, và theo đó là giảm thời gian phục hồi dữ liệu.

3.3. Xác định các ứng dụng quản lý cơ sở hạ tầng và mô tả các yêu cầu cơ bản đối với các ứng dụng này

Các ứng dụng quản lý cơ sở hạ tầng là các dịch vụ mạng chia sẻ được sử dụng để quản lý hoặc tích hợp cơ sở hạ tầng khác.

- Quản lý cơ sở hạ tầng: Quản lý cơ sở hạ tầng là nền tảng phần mềm được sử dụng để thực hiện quản lý hệ thống, quản lý mạng và quản lý lưu trữ. Một số ví dụ về quản lý cơ sở hạ tầng. Dịch vụ này cho phép giám sát tổng thể toàn bộ các thành phần hạ tầng, đảm bảo nâng cao tầm nhìn hệ thống mạng, tìm ra những hỏng hóc trong hệ thống mạng, cải thiện tính sẵn sàng và hiệu năng của hệ thống mạng giữa các máy tính và các thiết bị nhằm đơn giản hóa việc trao đổi thông tin, chia sẻ nguồn lực và thông

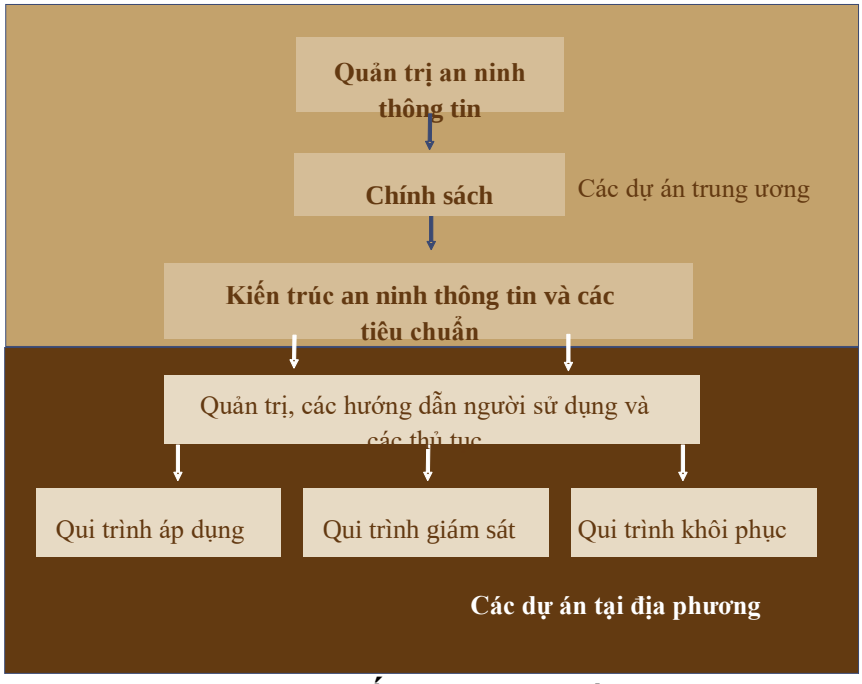
tin giữa các thiết bị được kết nối với nhau.

- Trao đổi thông tin và cộng tác: Trao đổi thông tin và cộng tác là các nền tảng phần mềm cho phép phân phối các kênh trực tuyến khác nhau, gồm trao đổi thông tin trên cơ sở thông điệp (message-based), thư điện tử (e-mail) và âm thanh (voice) hoặc hình ảnh (video). Một số ví dụ về Trao đổi thông tin và cộng tác. Các dịch vụ trao đổi thông tin và công tác bao gồm dịch vụ thư điện tử, lịch (calendar), địa chỉ liên lạc (contacts), và công việc (tasks); hỗ trợ truy cập thông tin trên thiết bị di động và trên nền web; hỗ trợ lưu trữ dữ liệu. Ngoài ra, còn có hệ thống quản lý cuộc gọi, đảm bảo có khả năng theo dõi tất cả các thành phần đang hoạt động trong hệ thống tổng đài điện thoại nội bộ truyền thống hoặc mạng VoIP; những thành phần này gồm có điện thoại, cổng nối (gateway), cầu hội nghị (conference bridges), nguồn chuyển mã (transcoding resources), và hộp thư thoại (voicemail)...
- Các dịch vụ thư mục: Dịch vụ thư mục là hệ thống phần mềm lưu trữ, tổ chức và truy cập thông tin trong một thư mục. Trong kỹ thuật phần mềm, một thư mục là một sơ đồ giữa các tên và các giá trị. Nó cho phép tra cứu các giá trị được gán vào một tên, tương tự như một cuốn từ điển. Giống như một từ trong từ điển có thể có nhiều định nghĩa, trong một thư mục một tên cũng có thể liên quan đến nhiều mảng thông tin khác nhau. Tương tự như vậy, một từ có thể có các dạng từ loại khác nhau và các định nghĩa khác nhau, do đó, một tên trong thư mục cũng có thể có nhiều loại dữ liệu khác nhau.
- Quản lý cấu hình: Quản lý cấu hình là các nền tảng phần mềm cho phép kiểm soát tập trung dựa trên các cơ sở hạ tầng khác nhau sẵn có trên mạng như quản lý các máy tính/nhóm máy tính lớn trong hệ thống cũng như cung cấp chức năng quản lý từ xa, vá lỗi, phân phối phần mềm, triển khai hệ điều hành, bảo vệ truy cập hệ thống mạng, và kho lưu trữ phần cứng, phần mềm.
- Quản lý đám mây riêng” Quản lý đám mây riêng là một bộ nền tảng phần mềm mở rộng nền tảng ảo hóa cơ bản cho phép cung cấp mô hình điện toán đám mây “cơ sở hạ tầng như một dịch vụ” trong tỉnh. Giải pháp quản lý đám mây riêng cần có khả năng trừu tượng hóa các nguồn lực ảo hóa để cho phép người dùng tự truy cập vào các nguồn lực này thông qua

một danh mục dịch vụ.

3.4. Xác định mô hình triển khai đảm bảo An toàn thông tin tổng thể của Tỉnh; xác định các thành phần then chốt và mô tả yêu cầu căn bản đối với các thành phần

Cũng giống như mọi lĩnh vực khác, công nghệ cũng có những rủi ro và thách thức riêng. Những rủi ro về thông tin cũng đã tăng lên gấp nhiều lần do việc ứng dụng những công nghệ mới. An toàn không chỉ là việc giữ bí mật dữ liệu mà còn phải bảo vệ tính toàn vẹn, cách thức truy nhập và tính sẵn có của dữ liệu. An toàn là cần thiết để thiết lập và giữ vững uy tín giữa các cơ quan chính quyền và người dân, những người đang sinh sống tại địa phương và các doanh nghiệp. Thông tin kịp thời và tin cậy là cần thiết để xử lý giao dịch và hỗ trợ hoạt động của từng cơ quan. Với các dự án CPĐT thì mức độ phụ thuộc vào thông tin lại càng cao, và bất kì sự rò rỉ thông tin hoặc không bảo đảm tính toàn vẹn của thông tin cũng sẽ ảnh hưởng trực tiếp đến lợi ích của tỉnh Vĩnh Phúc.



Kiến trúc bảo mật

Rủi ro an toàn thông tin

Mức độ rủi ro về an toàn thông tin đang tiếp tục tăng lên và cao hơn bao giờ hết. Để giải quyết được vấn đề này không chỉ cần có công cụ kiểm soát an toàn là

đủ. Bảo vệ an toàn là một quá trình liên tục, trong đó các công cụ kiểm soát chỉ là một yếu tố của cả hệ thống. Các yếu tố khác bao gồm năng lực của nhân viên CNTT trong việc thường xuyên tự đánh giá khả năng của mình và đối phó kịp thời với các nguy cơ mới trong môi trường công nghệ và nghiệp vụ thường xuyên thay đổi. Để thiết lập và duy trì hệ thống an toàn thông tin một cách hiệu quả thì chính quyền tỉnh Vĩnh Phúc cần phải thống nhất các quy trình, con người và công nghệ để giảm bớt rủi ro, phù hợp với chính sách quản lý rủi ro và giữ mức độ rủi ro ở giới hạn cho phép. Điều này có thể được thực hiện bằng cách xây dựng một quy trình xác định rủi ro và đưa ra chiến lược phù hợp để thực thi. Chiến lược này cần được thử nghiệm một cách có cấu trúc và được giám sát thường xuyên. Để bảo đảm tính hiệu quả của hệ thống an toàn thông tin của tỉnh Vĩnh Phúc, cần có khung an toàn thông tin đa cấp. Hình trên đây đề xuất kiến trúc an toàn thông tin cho các sở, ban, ngành ở tỉnh Vĩnh Phúc và đề xuất này cũng là một phần của CPĐT.

a) Chính sách quản trị an toàn trung tâm

Tất cả các ứng dụng và cơ sở hạ tầng được sử dụng và quản lý trong các dự án CPĐT là các hệ thống có tầm quan trọng quốc gia và đòi hỏi phải có hệ thống an toàn đầy đủ. Để bảo đảm hệ thống an toàn được xây dựng một cách nhất quán và đầy đủ, cán bộ lãnh đạo CNTT cần tập trung thực hiện một số công việc sau:

- Thành lập một hội đồng quản trị an toàn.
- Xây dựng chính sách an toàn cho tỉnh Vĩnh Phúc
- Xây dựng các kiến trúc và tiêu chuẩn an toàn.

Những công việc dù được thực hiện ở cấp Tỉnh vẫn cần phải được áp dụng cho tất cả các cơ quan, đơn vị.

Hội đồng quản trị an toàn

Nhằm quản lý hiệu quả hệ thống an toàn cho các đơn vị trên toàn tỉnh, cần thành lập một hội đồng quản trị an toàn tập trung. Ngoài việc giám sát và nâng cấp các chương trình bảo mật, hội đồng này có trách nhiệm xây dựng và phê duyệt các chính sách bảo vệ an toàn. Trách nhiệm của hội đồng quản trị an toàn là:

- Xác định và điều hành các mục đích, chiến lược, chính sách và nâng cao

nhận thức về an toàn thông tin trong toàn Tỉnh.

- Phê duyệt tất cả các vấn đề chính sách có liên quan đến an toàn thông tin và thay đổi nếu có.
- Phê duyệt từng trường hợp ngoại lệ cụ thể nếu như yêu cầu về chính sách an toàn không được đáp ứng, đưa ra khung thời gian cho các trường hợp ngoại lệ và theo dõi các trường hợp này cho tới khi nào đáp ứng được những yêu cầu của chính sách an toàn.
- Tổ chức thảo luận các vấn đề liên quan đến an toàn thông tin và các vấn đề nảy sinh từ các cơ quan, đơn vị để bảo đảm rằng những đơn vị này sẽ nhận được sự tham mưu hữu ích và triển khai các thủ tục bảo vệ an toàn hiệu quả.
- Chỉ đạo và tham mưu cho các đơn vị chịu trách nhiệm xây dựng các hệ thống bảo vệ an toàn.

Chính sách an toàn

Chính sách bảo vệ an toàn chính là bản tuyên ngôn về mục đích quản lý. Cần phải xây dựng một chính sách bảo vệ an toàn toàn diện để làm nền tảng cho việc triển khai các phương án bảo vệ an toàn tại toàn bộ các đơn vị. Chính sách an toàn phải bao trùm toàn bộ các lĩnh vực an toàn thông tin và phải cung cấp các nguyên tắc hướng dẫn cho các đơn vị triển khai các phương án bảo vệ an toàn tại đơn vị của mình.

Dựa trên các tiêu chuẩn an toàn quốc tế, dưới đây là khung đề xuất cho việc xây dựng chính sách an toàn thông tin.

Kiến trúc và các tiêu chuẩn an toàn kỹ thuật

Kiến trúc an toàn kỹ thuật xác định các phương thức bảo vệ an toàn cho nhiều ứng dụng và hợp phần cơ sở hạ tầng. Kiến trúc an toàn thông tin sẽ bao gồm các thông tin đầu vào để xây dựng kiến trúc mạng và ứng dụng bảo đảm tính tương tác về an toàn. Kiến trúc kỹ thuật sẽ đưa ra hướng dẫn về những khía cạnh sau:

Kiến trúc mạng an toàn - Kiến trúc này bao gồm một mạng được thiết kế để bảo đảm cung cấp độ an toàn hợp lý cho từng hợp phần thông qua việc phân chia mạng. Kiến trúc mạng an toàn cũng tính đến các quy định bảo mật khi đưa các dịch vụ lên mạng Internet và sự phân chia mạng giữa các cơ quan và dịch vụ khác

nhau. Bên cạnh đó kiến trúc mạng an toàn sẽ bảo đảm các dịch vụ dùng chung như DNS, thư mục và mạng tin cậy được cung cấp một cách an toàn cho tất cả các cơ quan.

Kiến trúc mạng an toàn cũng xác định các thiết bị an toàn và kịch bản triển khai những thiết bị này nhằm bảo vệ cơ sở hạ tầng quan trọng. Các thiết bị an toàn bao gồm thiết bị lọc gói tin, tường lửa, hệ thống phát hiện và ngăn ngừa thâm nhập và hệ thống giám sát và cảnh báo.

Kiến trúc ứng dụng an toàn - Kiến trúc ứng dụng an toàn xác định các tiêu chuẩn an toàn phải được áp dụng khi xây dựng và kết nối ứng dụng. Kiến trúc này bao gồm các tiêu chuẩn an toàn kết nối, quy định mã hóa giữa các ứng dụng (ví dụ như lớp cổng bảo mật SSL), kênh an toàn, hồ sơ xác thực và cấp quyền trong ứng dụng. Các tiêu chuẩn an toàn xuất phát từ chính sách an toàn và đưa ra cái nhìn toàn cảnh về những hành động cần thiết nhằm đạt được các mục tiêu đã đề ra trong chính sách an toàn. Tỉnh Vĩnh Phúc cần tập trung xác định các tiêu chuẩn an toàn trong đó cung cấp các hướng dẫn trong việc thực thi chính sách an toàn. Những tiêu chuẩn này bao gồm các quy trình và tiêu chuẩn cụ thể được thiết lập tại toàn bộ các cơ quan nhằm tuân thủ chính sách an toàn. Các tiêu chuẩn cho việc lập cấu hình bảo vệ an toàn của hệ điều hành, các thiết bị mạng và các hợp phần được mua bên ngoài cũng sẽ được xác định một cách tập trung.

b) Các hợp phần của chính sách bảo vệ an toàn

Phần	Lĩnh vực
1	**Phân loại và kiểm soát thông tin**
1.1	Chủ sở hữu dữ liệu
1.2	Phân loại thông tin
2	**Bảo mật vật lý và môi trường hệ thống**
2.1	An toàn vật lý
2.2	An toàn môi trường hệ thống
2.3	Cấp điện

Phần	Lĩnh vực
2.4	An toàn hệ thống dây mạng
2.5	An toàn máy tính xách tay
2.6	Chính sách dọn bàn làm việc và khoá màn hình
3	**Bảo mật nguồn nhân lực**
3.1	An toàn trong việc tuyển dụng, luân chuyển và chấm dứt hợp đồng lao động
3.2	Trách nhiệm của người sử dụng
3.3	Các khoá học định hướng và nâng cao nhận thức về An toàn
4	**Kiểm soát truy cập lôgic**
4.1	Quản lý truy nhập của người dùng
4.2	Trách nhiệm của người dùng
4.3	Bảo mật lôgic máy tính cá nhân, máy xách tay
4.4	Quy định sử dụng các tiện ích hệ thống nhạy cảm
5	**Quản trị môi trường máy tính**
5.1	Xác định thiết bị phần cứng
5.2	Xử lý và bảo vệ an toàn thông tin
5.3	Các thủ tục trong tình huống khẩn cấp, các tài khoản ưu tiên
5.4	Thủ tục xử lý tai nạn
5.5	Phân chia trách nhiệm
5.6	Bảo vệ an toàn tài liệu hệ thống
5.7	Kiểm soát virus máy tính
5.8	Thủ tục loại bỏ phương tiện lưu trữ
5.9	Mã hoá và quản lý khoá
6	**An toàn hệ thống mạng**
6.1	Kiểm soát quản lý mạng
6.2	Các thiết bị mạng

Phần	Lĩnh vực
6.3	Các công cụ chẩn đoán mạng
7	**An toàn Internet**
7.1	Sử dụng Internet
7.2	An toàn e-mail
7.3	An toàn tường lửa
8	**Xây dựng và duy trì hệ thống**
8.1	Kiểm soát môi trường hệ thống
8.2	Yêu cầu thay đổi
8.3	Quản lý mã nguồn
8.4	Kiểm soát phiên bản
8.5	Kiểm thử
8.6	Yêu cầu duy trì
8.7	Kỹ thuật dịch ngược
9	**Kế hoạch tiếp tục hoạt động sau thảm hoạ**[1]
9.1	Kế hoạch phục hồi sau thảm hoạ
9.2	Thủ tục sao lưu và phục hồi
10	**Tuân thủ**
10.1	Việc sử dụng phần mềm không được phép
10.2	Mua sắm và quy định sử dụng phần mềm
11	**Bên thứ ba và dịch vụ gia công**
11.1	Đánh giá rủi ro
11.2	Kiểm soát truy cập
11.3	Các điều kiện bảo mật trong hợp đồng với bên thứ ba

[1] Kế hoạch tiếp tục hoạt động sau thảm hoạ cần phải được triển khai cho chương trình CPĐT nhằm bảo đảm khả năng sẵn sàng 24X7 của cơ sở hạ tầng và dịch vụ CPĐT.

Phần	Lĩnh vực
11.4	Các điều kiện bảo mật trong các hợp đồng gia công
11.5	Cam kết chất lượng dịch vụ

Các hợp phần của chính sách bảo mật

Các dịch vụ bảo mật như được minh họa trong hình dưới đây, là tập hợp các công nghệ cung cấp khung kiểm soát bảo mật cho tất cả các công nghệ trong các vùng dịch vụ khác.

- Kiểm soát danh tính và truy cập: Kiểm soát danh tính và truy cập là một vùng quản trị rộng có chức năng xác định các cá nhân trong một hệ thống

(ví dụ quốc gia, hệ thống mạng, tổ chức của cá nhân đó) và kiểm soát truy cập vào các nguồn lực trong hệ thống này bằng cách đặt ra những giới hạn về danh tính đã thiết lập cho các cá nhân đó.

- Quản lý danh tính: Quản lý danh tính là một nền tảng phần mềm quản lý phương thức người dùng được xác định và ủy quyền thông qua các hệ thống mạng máy tính. Quản lý danh tính bao gồm các vấn đề như cách thức người dùng được gán một danh tính, bảo vệ danh tính đó và các công nghệ hỗ trợ việc bảo vệ đó.
- Xác thực: Xác thực là giao thức bảo mật được sử dụng để xác nhận danh tính của một thực thể trước khi đưa thực thể đó đến kiểm tra ủy quyền trong một hệ thống kiểm soát truy cập.
    - Kerberos: Là giao thức xác thực mạng máy tính hoạt động trên cơ sở "vé" để cho phép các nút mạng trao đổi thông tin thông qua một đường truyền không an toàn nhằm chứng minh danh tính của các nút mạng đó với các nút mạng khác theo phương thức an toàn. Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình khách - chủ và đảm bảo xác thực cho cả hai chiều – cả người dùng và máy chủ đều xác nhận được danh tính của nhau. Thông điệp của giao thức Kerberos được bảo vệ chống lại việc nghe lén và gửi lại các gói tin cũ. Kerberos xây dựng dựa trên mật mã hóa khóa đối xứng và cần đến một bên thứ ba được tin tưởng, và tùy ý có thể sử dụng mật mã hóa khóa công khai bằng cách tận dụng mật mã hóa khóa không đối xứng trong các giai đoạn chứng thực nhất định.
    - Remote Authentication Dial In User Service (RADIUS): Là giao thức mạng cung cấp quản lý AAA (Xác thực, Phân quyền và Tính cước) tập trung cho máy tính để kết nối và sử dụng dịch vụ mạng. RADIUS được phát triển bởi Tập đoàn Livingston Enterprises vào năm 1991 như một giao thức xác thực và tính cước cho máy chủ truy cập và sau đó được đưa vào tiêu chuẩn Internet Engineering Task Force (IETF).
- Kiểm soát truy cập: Kiểm soát truy cập là một hệ thống cho phép xác thực để kiểm soát truy cập trong các khu vực và nguồn lực của

một cơ sở vật lý hoặc một hệ thống thông tin dựa trên máy tính. Một số ví dụ về kiểm soát truy cập:

- Firewall: Thiết bị được thiết kế để cho phép hoặc từ chối truyền mạng dựa trên một số nguyên tắc và thường được sử dụng để bảo vệ hệ thống mạng khỏi các truy cập trái phép trong khi đó những trao đổi thông tin hợp pháp vẫn được thông qua.
- Network Access Control (NAC): phương thức bảo mật mạng lưới máy tính hợp nhất các công nghệ bảo mật điểm đầu nút (ví dụ như antivirus, ngăn chặn xâm nhập và lỗ hổng máy chủ), xác thực người dùng hoặc hệ thống và thực hiện bảo mật đường truyền.

- Kiểm định: Kiểm định chỉ một bản ghi các hoạt động trong hệ thống theo thứ tự thời gian cho phép kiểm tra và tái thiết lập trình tự các sự kiện và/ hoặc các thay đổi trong một sự kiện; thu thập, chuẩn hóa và phân tích các nhật ký từ các thiết bị trên toàn hệ thống mạng, ví dụ như các nhật ký từ tường lửa, các hệ thống phát hiện và ngăn chặn xâm nhập và các giải pháp chống mất dữ liệu cũng như lưu lượng truy cập mạng, các nhật ký ứng dụng và hoạt động của người dùng.
- Kiểm soát đe dọa và xâm nhập: Kiểm soát đe dọa và xâm nhập là nền tảng được sử dụng để ngăn chặn sự xuất hiện của những sự cố bảo mật bằng cách kiểm soát sự đe dọa cũng như các xâm nhập đến bảo mật.
    - Quản lý xâm nhập: Quản lý xâm nhập là nền tảng phần mềm được sử dụng để phát hiện và hạn chế những xâm nhập/lỗ hổng phát hiện trong hệ thống mạng máy tính, đảm bảo khả năng quét lỗ hổng và bản vá xác thực, công cụ này xác định các chương trình đã cài đặt và các bản vá (patches) bảo mật còn thiếu.
    - Quản lý đe dọa: Quản lý đe dọa là nền tảng phần mềm được sử dụng để phát hiện và ngăn chặn các đe dọa bảo mật ví dụ như sự tấn công chủ động đến các hệ thống được bảo vệ.
        - Hệ thống Antivirus: là gói phần mềm được sử dụng để ngăn chặn, phát hiện và hủy phần mềm độc hại (malware), bao gồm nhưng không giới hạn virus máy tính, sâu máy tính,

trojan horses, spyware và adware.

- Hệ thống ngăn chặn xâm nhập: thường là các thiết bị bảo mật đường truyền có chức năng giám sát mạng và/ hoặc các hoạt động trong hệ thống để xác định các hoạt động nguy hiểm. Chức năng chính của hệ thống ngăn chặn xâm nhập là xác định các hoạt động nguy hiểm, thông tin đăng nhập của các hoạt động đó, cố gắng ngăn chặn/ dừng hoạt động và đưa ra cảnh báo về các hoạt động đó.
- Hệ thống quản lý sự kiện và thông tin bảo mật (Security event and information manager - SIEM): là một công cụ máy tính được sử dụng trên các đường truyền dữ liệu để tập trung kho lưu trữ và giải thích các bản ghi hoặc sự kiện bảo mật được tạo ra bởi các phần mềm khác chạy trong hệ thống mạng. SIEM thường thực hiện sự tương quan và giải thích về các bản ghi đã thu thập, và chỉ định nguy cơ và/hoặc mức tin cậy nhằm giúp giảm các cảnh báo sai tích cực (false-positive).

- Kiểm soát tính bảo mật và tính toàn vẹn: Kiểm soát tính bảo mật và tính toàn vẹn đề cập đến các nền tảng và công nghệ được sử dụng để bảo vệ tính bảo mật và xác thực của thông tin.
    - Nền tảng PKI: Nền tảng PKI (Cơ sở hạ tầng khóa công khai) là nền tảng phần mềm cho phép tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi chứng thực số. Trong mật mã, PKI là sự sắp xếp các khóa công khai liên kết với người dùng tương ứng bằng các phương tiện của nhà cung cấp chứng thực (CA).
    - Mã hóa mạng: Mã hóa mạng là phương pháp duy trì tính bảo mật và tính toàn vẹn của thông tin được trao đổi trên hệ thống mạng hoặc tại tầng giao vận. Một số ví dụ về mã hóa mạng:
        - Internet Protocol Security (IPsec): bộ giao thức bảo đảm trao đổi thông tin trên Giao thức Internet bằng cách xác thực và mã hóa mỗi gói IP của một kỳ trao đổi thông tin. IPsec cũng bao gồm các giao thức thiết lập xác thực hai chiều giữa các tác nhân tại đầu kỳ trao đổi và thương thảo khóa mật mã được sử dụng trong suốt kỳ trao đổi đó.

- OpenVPN: là ứng dụng phần mềm mã nguồn mở miễn phí thực hiện kỹ thuật mạng riêng ảo (VPN) để tạo kết nối điểm-tới-điểm hoặc site-to-site trong các cấu hình định tuyến hoặc bắc cầu và các phương tiện truy cập từ xa. OpenVNP sử dụng phương pháp bảo mật SSL/TLS để mã hóa và có khả năng vượt qua công nghệ chuyển dịch địa chỉ mạng (NATs) và tường lửa.

- Mã hóa kho lưu trữ: Mã hóa kho lưu trữ là phương pháp duy trì tính bảo mật và tính toàn vẹn của thông tin được lưu trữ, ví dụ như tập tin và/ hoặc cơ sở dữ liệu. Một số ví dụ về mã hóa kho lưu trữ:
  - Mã hóa ổ đĩa cứng sử dụng phần mềm hoặc phần cứng mã hóa ổ đĩa để mã hóa mọi bit dữ liệu ghi trên đĩa, hoặc khối lượng đĩa. Mã hóa ổ đĩa ngăn chặn truy cập trái phép vào kho lưu trữ dữ liệu. Thuật ngữ "mã hóa toàn bộ ổ đĩa cứng" (full disk encryption hoặc whole disk encryption) thường được sử dụng để nhấn mạnh rằng mọi dữ liệu trên đĩa đã được mã hóa, bao gồm cả các chương trình mã hóa phân vùng hệ điều hành khởi động.
  - Mã hóa hệ thống tệp tin, thường được gọi là mã hóa tệp tin hoặc thư mục, là một hình thức mã hóa ổ đĩa cứng mà trong đó các tệp tin hoặc thư mục riêng biệt được mã hóa bởi chính hệ thống tệp tin của riêng mình. Điều này đối lập với mã hóa toàn bộ ổ đĩa cứng khi mà toàn bộ phân vùng hoặc ổ đĩa cứng chứa hệ thống tệp tin được mã hóa.
- Kiểm chuẩn tính toàn vẹn: Kiểm chuẩn tính toàn vẹn là phương pháp chứng thực tính toàn vẹn của hệ thống thông tin và dữ liệu. Kiểm chuẩn tính toàn vẹn của tệp tin là quá trình sử dụng một thuật toán để xác minh tính toàn vẹn hoặc tính xác thực của một tập tin máy tính. Điều này thường được thực hiện bằng cách so sánh hàm băm mật mã học (cryptographic hash function) của các tập tin so với một tài liệu tham chiếu đã biết. Một số phương pháp kiểm chuẩn tính toàn vẹn:
  - SHA-1: là một hàm băm mật mã học được xây dựng bởi Cơ quan An ninh Quốc gia (National Security Agency) và được

phát hành bởi NIST theo Tiêu chuẩn Xử lý Thông tin của Liên Bang Hoa Kỳ (U.S. Federal Information Processing Standard). SHA là viết tắt của Thuật toán giải Băm An toàn (Secure Hash Algorithm). Ba thuật toán SHA được kết cấu khác nhau và được phân biệt bằng các tên gọi SHA-0, SHA-1, và SHA-2. SHA-1 rất giống với SHA-0 nhưng SHA-1 sửa một lỗi trong đặc điểm kỹ thuật băm SHA gốc, mà lỗi này là nguồn gốc dẫn đến những điểm yếu đáng kể. Nhiều ứng dụng không chấp nhận thuật toán SHA-0.

- MD5 (Message-Digest algorithm 5): một hàm băm mật mã học được sử dụng phổ biến với giá trị băm dài 128-bit (16-byte). Là một chuẩn Internet (RFC1321), MD5 đã được dùng trong nhiều ứng dụng bảo mật, và cũng được dùng phổ biến để kiểm tra tính toàn vẹn của dữ liệu. Tuy nhiên, người ta đã chứng minh rằng MD5 không có khả năng chịu va chạm, như vậy, MD5 là không phù hợp cho các ứng dụng như giấy chứng nhận SSL (SSL certificates) hoặc chữ ký số (digital signatures) dựa trên thuộc tính này. Một bảng băm MD5 thường được diễn tả bằng một số hệ thập lục phân 32 ký tự.

3.5. Xác định nội dung ưu tiên triển khai giai đoạn 2016-2020

1. Giai đoạn 2016-2017

a) Xây dựng và ban hành các văn bản:

- Xây dựng và ban hành Quy hoạch phát triển CNTT tỉnh Vĩnh Phúc giai đoạn 2016-2025, định hướng đến 2035.

- Xây dựng và ban hành Kiến trúc Chính quyền điện tử tỉnh Vĩnh Phúc.

- Đưa hiệu quả và mức độ ứng dụng CNTT thành tiêu chí đánh giá thi đua khen thưởng đối với các cơ quan nhà nước của tỉnh.

b) Hoàn thiện hệ thống hạ tầng CNTT:

- Tiến hành nâng cấp hệ thống mạng nội bộ tại các cơ quan, đơn vị cấp tỉnh và huyện đảm bảo an toàn thông tin mạng, tạo điều kiện để triển khai kết nối mạng diện rộng giữa các cơ quan nhà nước từ cấp tỉnh đến huyện.

- Nâng cấp Trung tâm tích hợp dữ liệu số của tỉnh.

- Triển khai hệ thống mạng diện rộng của tỉnh trên cơ sở Mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước.

c) Đẩy mạnh ứng dụng CNTT trong các cơ quan nhà nước:

- Triển khai Phần mềm quản lý văn bản và điều hành đến 100% các sở, ban, ngành, UBND các huyện, thành, thị; kết nối liên thông đến UBND các xã phục vụ hoạt động gửi nhận văn bản điện tử.

- Tiếp tục triển khai, nhân rộng sử dụng thư điện tử công vụ để trao đổi thông tin giữa CBCC và các cơ quan nhà nước của tỉnh.

- Triển khai xây dựng các hệ thống cơ sở dữ liệu về dân cư và đất đai.

- Triển khai các ứng dụng chuyên ngành theo Kế hoạch hành động số 638/HK-UBND ngày 29/02/2016 của UBND tỉnh Vĩnh Phúc Thực hiện Nghị quyết 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử.

d) Ứng dụng CNTT phục vụ người dân và doanh nghiệp:

- Tiếp tục triển khai Hệ thống một cửa điện tử, tích hợp dịch vụ công trực tuyến tại các cơ quan nhà nước cấp tỉnh và huyện, chú trọng tập trung triển khai trước tại các cơ quan, đơn vị có số lượng lớn các giao dịch và hiệu quả mang lại cao. Đảm bảo kết nối liên thông hệ thống cung cấp dịch vụ công trực tuyến của tỉnh với hệ thống cung cấp dịch vụ công của trung ương theo lộ trình.

- Nâng cấp Cổng thông tin điện tử của tỉnh; Nâng cấp trang tin điện tử của của các cơ quan, đơn vị đáp ứng yêu cầu tại Nghị định số 43/2011/NĐ-CP của Chính phủ.

e) Đào tạo, tập huấn CNTT:

- Đào tạo nâng cao khả năng quản lý nhà nước về CNTT cho các đối tượng là lãnh đạo các cơ quan đơn vị.

- Đào tạo kỹ năng quản lý, vận hành, đảm bảo an toàn thông tin mạng đối với hệ thống thông tin cho đối tượng là cán bộ chuyên trách, phụ trách CNTT.

- Đào tạo nâng cao khả năng sử dụng máy tính, khai thác các ứng dụng, đảm bảo an toàn thông tin mạng cho các đối tượng là CBCC các cấp đáp ứng yêu cầu của công việc.

f) Đảm bảo an toàn thông tin mạng:

- Tuyên truyền, phổ cập, nâng cao nhận thức về an toàn thông tin mạng trên

các phương tiện thông tin đại chúng đến rộng rãi mọi tầng lớp trong xã hội trên địa bàn tỉnh; tăng cường công tác đảm bảo an toàn thông tin đối với hệ thống hạ tầng thông tin, hệ thống điều khiển công nghiệp và các hệ thống thông tin quan trọng khác do doanh nghiệp quản lý, khai thác, vận hành.

- Rà soát ban hành các quy định, quy chế về đảm bảo an toàn thông tin mạng đối với hệ thống thông tin dùng chung của tỉnh và các hệ thống tại các cơ quan quản lý nhà nước.

- Triển khai nhân rộng việc sử dụng Chữ ký số trong các các cơ quan nhà nước phục vụ công tác gửi nhận văn bản điện tử.

- Triển khai các giải pháp đảm bảo an toàn thông tin mạng đối với hệ thống thông tin dùng chung của tỉnh và hệ thống thông tin tại các cơ quan, đơn vị.

- Đào tạo, bồi dưỡng nâng cao trình độ cho cán bộ chuyên trách về CNTT tại các cơ quan đơn vị có đủ năng lực thực hiện nhiệm vụ đảm bảo an toàn thông tin mạng tại đơn vị.

- Phối hợp với các địa phương, tổ chức và chuyên gia trong lĩnh vực đảm bảo an toàn thông tin mạng thực hiện các nhiệm vụ đảm bảo an toàn thông tin mạng.

2. Giai đoạn 2018-2020

a) Xây dựng và ban hành các văn bản:

Tiếp tục nghiên cứu, xây dựng và ban hành các văn bản nhằm quản lý, hỗ trợ và thúc đẩy hoạt động ứng dụng và phát triển CNTT.

b) Hoàn thiện hệ thống hạ tầng CNTT:

- Hoàn thành nâng cấp Trung tâm tích hợp dữ liệu số của tỉnh.

- Hoàn thiện mạng diện rộng của tỉnh trên cơ sở Mạng truyền số liệu chuyên dùng trong các cơ quan Đảng và Nhà nước, kết nối các cơ quan nhà nước từ cấp tỉnh đến huyện và một số UBND cấp xã.

- Triển khai nhân rộng Chữ ký số phục vụ các nhiệm vụ đảm bảo an toàn thông tin mạng, tạo nền tảng thúc đẩy các giao dịch điện tử với trọng tâm là gửi nhận văn bản điện tử trong các cơ quan nhà nước.

- Xây dựng nền tảng triển khai Chính quyền điện tử cấp tỉnh: Xây dựng và từng bước hoàn thiện nền tảng kết nối, chia sẻ cấp tỉnh. Xây dựng và đưa vào vận hành các phần mềm vận hành nền tảng kết nối, chia sẻ cấp tỉnh. Xây dựng hệ thống nền tảng ứng dụng chính quyền điện tử cấp tỉnh.

c) Đẩy mạnh ứng dụng CNTT trong các cơ quan nhà nước:

- Tiếp tục sử dụng hiệu quả các phần mềm dung chung, các phần mềm chuyên ngành đã triển khai. Tăng cường xây dựng và đưa vào sử dụng các phần mềm chuyên ngành tại các cơ quan, đơn vị.

- Triển khai các chức năng phù hợp của Phần mềm quản lý văn bản và điều hành đến UBND các xã.

- Xây dựng, hoàn chỉnh các phần mềm dung chung đảm bảo tuân thủ kiến trúc chính quyền điện tử cấp tỉnh.

d) Ứng dụng CNTT phục vụ người dân và doanh nghiệp:

Tiếp tục triển khai Hệ thống một cửa điện tử, tích hợp dịch vụ công trực tuyến tại các cơ quan nhà nước cấp tỉnh và huyện; triển khai thí điểm hệ thống tại UBND cấp xã, căn cứ kết quả thu được, từng bước nhân rộng đến các đơn vị khác.

e) Đào tạo, tập huấn CNTT:

- Tiếp tục đào tạo nâng cao khả năng quản lý nhà nước về CNTT cho các đối tượng là lãnh đạo các cơ quan đơn vị; Đào tạo kỹ năng quản lý, vận hành, đảm bảo an toàn thông tin mạng đối với hệ thống thông tin cho đối tượng là cán bộ chuyên trách, phụ trách CNTT; Đào tạo nâng cao khả năng sử dụng máy tính, khai thác các ứng dụng, đảm bảo an toàn thông tin mạng cho các đối tượng là CBCC các cấp đáp ứng yêu cầu của công việc.

- Đào tạo cho người dân và doanh nghiệp về sử dụng và khai thác hiệu quả các dịch vụ công trực tuyến của tỉnh.

f) Đảm bảo an toàn thông tin mạng:

- Tiếp tục tổ chức thực hiện các giải pháp, nhiệm vụ đảm bảo an toàn thông tin mạng đối với hệ thống thông tin dùng chung của tỉnh và các hệ thống thông tin tại các cơ quan đơn vị.

- Triển khai các hoạt động giám sát, cảnh báo, đầu tư công cụ dò quét lỗ hổng, mã độc và hướng dẫn biện pháp đảm bảo an toàn thông tin mạng trong các cơ quan, tổ chức, doanh nghiệp trên địa bàn tỉnh; Triển khai thí điểm các tiêu chuẩn quản lý an toàn thông tin mạng tại một số cơ quan nhà nước nhằm giảm thiểu nguy

cơ xảy ra sự cố, khắc phục và truy vết trong trường hợp sự cố xảy ra.

Thành lập Nhóm ứng cứu sự cố máy tính trên địa bàn tỉnh nhằm hỗ trợ và giải quyết các sự cố máy tính.