ỦY BAN NHÂN DÂN TỈNH QUẢNG NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 26 /2018/QĐ-UBND	*Quảng Ninh, ngày 20 tháng 9 năm 2018*

QUYẾT ĐỊNH

Ban hành Quy chế quản lý, khai thác và vận hành Trung tâm Tích hợp dữ liệu tỉnh Quảng Ninh

ỦY BAN NHÂN DÂN TỈNH QUẢNG NINH

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19/06/2015;

Căn cứ Luật Giao dịch điện tử ngày 29/11/2005;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật ban hành Văn bản quy phạm pháp luật ngày 22/06/2015;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

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

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

Căn cứ Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông về việc ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Xét đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 472/TTr-STTTT ngày 07/9/2018,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế Quản lý, khai thác và vận hành Trung tâm Tích hợp dữ liệu tỉnh Quảng Ninh".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 01/10/2018 và thay thế Quyết định số 1365/QĐ-UBND ngày 28/5/2013 của UBND tỉnh về quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Điều 3. Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở, ban, ngành trong tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố; Thủ trưởng các cơ quan, đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- TT Tỉnh ủy, HĐND tỉnh (b/c);
- CT, các PCT UBND tỉnh (b/c);
- Như Điều 3 (thực hiện);
- V0, V3, TM3, VX4, TTTT;
- Lưu: VT, XD6;

N.20 – QĐ.056

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đặng Huy Hậu

ỦY BAN NHÂN DÂN TỈNH QUẢNG NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Quản lý, khai thác và vận hành
Trung tâm Tích hợp dữ liệu tỉnh Quảng Ninh
(Ban hành kèm theo Quyết định số 26 /2018/QĐ-UBND ngày 20 /9/2018 của UBND tỉnh Quảng Ninh)

CHƯƠNG I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định việc quản lý, khai thác và vận hành Trung tâm Tích hợp dữ liệu tỉnh Quảng Ninh (sau đây gọi tắt là Trung tâm THDL).

2. Quy chế này áp dụng đối với cơ quan hành chính, đơn vị sự nghiệp trên địa bàn tỉnh Quảng Ninh; Các tổ chức, cá nhân có liên quan tham gia quản lý, khai thác và vận hành Trung tâm THDL.

Điều 2. Giải thích từ ngữ

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

1. Địa chỉ IP (*Internet Protocol - giao thức Internet*) là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

2.VLAN (*virtual local area network)* là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách lô gic trên cùng một kiến trúc hạ tầng vật lý. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ giúp giảm thiểu miền quảng bá (*broadcast domain*) cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. VLAN tương đương như mạng con.

3. Hệ thống tường lửa (Firewall): Là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn các truy cập thông tin không mong muốn từ ngoài vào hệ thống mạng nội bộ cũng như ngăn chặn các thông tin bảo mật nằm trong mạng nội bộ xuất ra ngoài internet mà không được cho phép.

4. Mạng diện rộng (sau đây gọi tắt là mạng WAN) là mạng tin học được thiết lập bằng cách kết nối giữa Trung tâm THDL với mạng nội bộ của các cơ quan, đơn vị trên địa bàn tỉnh thông qua hạ tầng mạng của Nhà cung cấp dịch vụ và cho phép kết nối tới mạng của Chính phủ khi có yêu cầu.

5. Mạng truyền số liệu chuyên dùng trong các cơ quan nhà nước trên địa bàn tỉnh Quảng Ninh là mạng truyền dẫn tốc độ cao, sử dụng đường truyền số liệu

chuyên dùng của các cơ quan Đảng và Nhà nước do Tập đoàn Bưu chính Viễn thông Việt Nam xây dựng để kết nối mạng nội bộ của các cơ quan nhà nước trong tỉnh thành một hệ thống mạng thống nhất trên phạm vi toàn tỉnh (sau đây gọi tắt là mạng truyền số liệu chuyên dùng).

6. Cơ sở dữ liệu (Database) là kho dữ liệu của các hệ thống phần mềm dùng chung, phần mềm chuyên ngành của các đơn vị được lưu trữ trên hệ thống lưu trữ đặt tại Trung tâm THDL.

7. Cổng console là loại cổng quản lý, cung cấp đường kết nối riêng vào router. Cổng này được sử dụng để thiết lập cấu hình cho router, theo dõi hoạt động mạng và khôi phục router khi gặp sự cố nghiêm trọng.

8. Remote access là truy cập từ xa qua mạng.

9. Cơ quan chủ sở hữu Trung tâm THDL tỉnh là Ủy ban nhân dân tỉnh Quảng Ninh.

10. Cơ quan quản lý Trung tâm THDL là Sở Thông tin và Truyền thông tỉnh Quảng Ninh.

11. Đơn vị trực tiếp vận hành Trung tâm THDL là Trung tâm Công nghệ thông tin và Truyền thông - Sở Thông tin và Truyền thông tỉnh Quảng Ninh (Sau đây gọi tắt là Đơn vị vận hành).

Điều 3. Thông tin chung về Trung tâm THDL

Trung tâm THDL là nơi tập trung các máy chủ, thiết bị kỹ thuật công nghệ thông tin chuyên dụng với khả năng lưu trữ, xử lý dữ liệu lớn, hệ thống bảo mật an toàn dữ liệu, hệ thống phụ trợ, mạng diện rộng, các hệ thống phần mềm ứng dụng công nghệ thông tin, cơ sở dữ liệu dùng chung và các hệ thống phần mềm ứng dụng công nghệ thông tin, cơ sở dữ liệu chuyên ngành của tỉnh, được triển khai theo mô hình điện toán đám mây; tuân theo tiêu chuẩn TCVN 9250:2012, TCVN 11930:2017 và tiêu chuẩn quốc tế về Trung tâm dữ liệu (TIA 942 - TIER 3) bảo đảm các thiết bị, phần mềm dùng chung được hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

Điều 4. Hạ tầng kỹ thuật và dịch vụ của Trung tâm THDL

1. Hạ tầng kỹ thuật:

a) Đường truyền: Trung tâm THDL sử dụng đường truyền số liệu chuyên dùng để kết nối hệ thống WAN triển khai cơ sở dữ liệu dùng chung cho các cơ quan, đơn vị, địa phương trên địa bàn toàn tỉnh, đường truyền số liệu chuyên dùng được lựa chọn tốc độ truyền dẫn đảm bảo quá trình giao dịch hành chính trên hệ thống WAN và đường truyền dự phòng khi đường truyền số liệu chuyên dùng bị sự cố. Trung tâm THDL sử dụng đường truyền leased line để cung cấp dịch vụ truy cập qua internet.

b) Mạng và bảo mật: Mạng được chia làm nhiều vùng khác nhau, mỗi vùng được áp đặt các chính sách an ninh và truy cập riêng để phục vụ cho các mục đích khác nhau. Hệ thống tường lửa (Firewall) có bản quyền được thiết kế kết nối đảm

bảo an toàn cho toàn bộ hệ thống mạng từ Trung THDL kết nối vào và ra hệ thống khác. Các máy chủ và máy chủ ảo được cài phần mềm diệt vi rút bản quyền hàng năm, các thiết bị khi kết nối với hệ thống máy chủ tại Trung tâm THDL được quét và kiểm tra đảm bảo an toàn trước khi kết nối với hệ thống. Mỗi thiết bị được thiết kế có tính dự phòng và bổ sung hỗ trợ lẫn nhau.

c) Hệ thống máy chủ: bao gồm hệ thống máy chủ đã được đầu tư phục vụ cho Chính quyền điện tử, thành phố thông minh và các ứng dụng chuyên ngành với khả năng sẵn sàng cho việc mở rộng số lượng máy chủ trong tương lai. Hệ thống máy chủ có khả năng cung cấp năng lực tính toán cho nhiều nền tảng với nhiều mục đích khác nhau như ứng dụng chuyên ngành, trang thông tin điện tử, cơ sở dữ liệu chuyên ngành,… của Tỉnh.

d) Hệ thống lưu trữ: hệ thống quản trị với năng lực xử lý lưu trữ tập trung ở mức cao, khả năng lưu trữ lớn trên hệ thống SAN, DAS kèm theo đó là hệ thống băng từ để bảo đảm cho mục đích sao lưu, phục hồi dữ liệu cho toàn bộ hệ thống. Hệ thống được thiết kế bảo đảm khả năng mở rộng trong tương lai.

đ) Các hệ thống phụ trợ: Bao gồm hệ thống điện, điều hòa chính xác, thiết bị lưu điện, máy phát điện, sàn nâng, hệ thống phòng cháy chữa cháy, camera an ninh… được thiết kế tuân theo tiêu chuẩn TIA 942 - TIER 3 (tiêu chuẩn quốc tế về Trung tâm THDL), bảo đảm các thiết bị luôn được hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

2. Các dịch vụ của Trung tâm THDL:

- Dịch vụ cho thuê và đặt tủ Rack;

- Dịch vụ cho thuê đặt máy chủ;

- Dịch vụ cho thuê máy chủ, máy chủ ảo;

- Dịch vụ lưu ký (Hosting);

- Dịch vụ cho thuê thiết bị lưu trữ (Storage);

- Các dịch vụ công nghệ thông tin (sau đây viết tắt là CNTT) có giá trị gia tăng khác.

Điều 5. Nguyên tắc quản lý, khai thác, vận hành và nâng cấp Trung tâm THDL

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

2. Xây dựng, nâng cấp Trung tâm THDL phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật quy định áp dụng đối với Trung tâm THDL theo Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông và tiêu chuẩn quốc tế ISO 27001:2013 về quản lý bảo mật thông tin do Tổ chức Chất lượng Quốc tế và Hội đồng Điện tử Quốc tế xuất bản vào ngày 25/9/2013. Đồng thời, tuân thủ theo các quy định hiện hành về bảo đảm an toàn, an ninh thông tin.

3. Trung tâm THDL bảo đảm hoạt động thông suốt, liên tục; bảo đảm khai thác hiệu quả các ứng dụng dùng chung của tỉnh và nâng cao chất lượng ứng dụng

công nghệ thông tin trong hoạt động của các cơ quan, đơn vị, địa phương trên địa bàn tỉnh. Đảm bảo tuân thủ các nguyên tắc xây dựng, quản lý, khai thác, bảo vệ và duy trì cơ sở dữ liệu theo quy định của Pháp luật.

4. Kinh phí ngân sách nhà nước cấp hàng năm đảm bảo cho công tác quản lý, vận hành và bảo trì, bảo dưỡng, thay thế các thiết bị hỏng hóc, bổ sung bản quyền (license) các phần mềm đã đầu tư tại Trung tâm THDL đầy đủ, kịp thời để phục vụ nhiệm vụ chung.

5. Tuân thủ các nguyên tắc, bảo đảm cơ sở hạ tầng và hệ thống công nghệ thông tin phục vụ ứng dụng, phát triển công nghệ thông tin theo Luật Công nghệ thông tin, Luật An toàn thông tin mạng, Luật An ninh mạng và các văn bản pháp lý hiện hành.

6. Các tài liệu, văn bản có nội dung mật được quản lý theo quy định riêng của từng ngành, lĩnh vực và các văn bản quy phạm pháp luật hiện hành. Không đưa các tài liệu, văn bản có nội dung mật lên các hệ thống thông tin, cơ sở dữ liệu, phần mềm dùng chung được cài đặt, khai thác, quản lý, vận hành tại Trung tâm THDL.

7. Các cơ sở hạ tầng, hệ thống thông tin, cơ sở dữ liệu của các cơ quan, đơn vị đặt tại Trung tâm THDL phải tuân thủ theo các quy chuẩn, tiêu chuẩn kỹ thuật do Nhà nước quy định và phù hợp với Kiến trúc Chính quyền điện tử, Kiến trúc thành phố thông minh của tỉnh.

8. Vận hành, triển khai, cung cấp các dịch vụ giá trị gia tăng cho các tổ chức, cá nhân theo quy định của pháp luật và trên cơ sở khai thác hiệu quả hạ tầng Trung tâm THDL.

Điều 6. Các hành vi bị cấm

1. Nghiêm cấm việc sử dụng, phát tán thông tin cá nhân do Trung tâm THDL nắm giữ (các thông tin cá nhân trên được thu thập, xử lý theo Điều 21 của Luật Công nghệ thông tin ngày 29/6/2006) vì mục đích vụ lợi, vi phạm quy định pháp luật hiện hành; trừ các yêu cầu đặc biệt của cơ quan chức năng có thẩm quyền.

2. Nghiêm cấm các hoạt động khai thác, sử dụng cơ sở hạ tầng, dữ liệu, dịch vụ của Trung tâm THDL với mục đích phá hoại, phản động; lưu trữ, truyền tải các nội dung không phù hợp với thuần phong mỹ tục, trái pháp luật, quy định của Nhà nước; Khai thác các dịch vụ trên mạng Internet trái pháp luật (tiền ảo, game online,…) và các hoạt động khác vi phạm quy định của pháp luật.

3. Nghiêm cấm các hành vi đánh cắp, giả mạo tài khoản để truy cập vào các phần mềm, hệ thống thông tin, cơ sở dữ liệu thuộc Trung tâm THDL.

4. Nghiêm cấm sử dụng các công cụ, phần mềm gây mất an toàn hệ thống, ảnh hưởng đến hoạt động chung của Trung tâm THDL.

5. Nghiêm cấm chia sẻ mật khẩu, tài khoản cá nhân cho người khác.

CHƯƠNG II
CÁC QUY ĐỊNH VỀ QUẢN LÝ, KHAI THÁC VÀ VẬN HÀNH TRUNG TÂM TÍCH HỢP DỮ LIỆU TỈNH

Điều 7. Trực vận hành, vào, ra Trung tâm THDL

1. Quy định đối với nhân viên vận hành:

a) Bảo đảm có ít nhất 01 cán bộ (hoặc nhân viên) kỹ thuật trực tại Trung tâm THDL 24 giờ/ngày, 7 ngày/tuần. Thực hiện trực 3 ca, 4 kíp các ngày làm việc.

b) Đi làm đúng thời gian quy định và đảm bảo giờ làm việc; khi làm việc phải đeo thẻ chức danh, mặc trang phục theo quy định.

c) Trong quá trình trực và làm việc tại Trung tâm THDL phải tuân thủ nghiêm ngặt theo các quy trình, quy định và nội quy lao động.

d) Cán bộ, nhân viên vận hành truy cập, khai thác thông tin tại Trung tâm THDL theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; không được tự ý can thiệp vào các phần mềm ứng dụng, dữ liệu do các cơ quan, đơn vị khác triển khai tại Trung tâm THDL.

e) Quá trình làm việc, chuyển giao công nghệ và xử lý nâng cấp, tích hợp, cài đặt các thao tác đối với hệ thống của Trung tâm THDL phải được ghi chép cụ thể vào sổ Nhật ký trực.

2. Quy định đối với người sử dụng dịch vụ, cung cấp dịch vụ tại Trung tâm THDL:

a) Yêu cầu:

- Tuân thủ nghiêm ngặt theo các quy trình, quy định về an toàn lao động khi làm việc tại Trung tâm THDL.

- Quá trình làm việc, chuyển giao công nghệ và xử lý nâng cấp, tích hợp, cài đặt các thao tác đối với hệ thống của Trung tâm THDL phải được ghi chép cụ thể vào sổ Nhật ký trực.

- Không được mang, sử dụng các thiết bị điện thoại, máy tính xách tay, máy tính bảng hoặc các thiết bị điện tử cá nhân khác (máy chụp hình, máy quay phim, thiết bị lưu trữ,…) khi vào bên trong Trung tâm THDL, trừ trường hợp có sự đồng ý của lãnh đạo đơn vị trực tiếp quản lý, vận hành Trung tâm THDL.

b) Thủ tục: Người sử dụng đăng ký làm việc tại Trung tâm THDL cần có các giấy tờ sau:

- Văn bản đề nghị làm việc tại Trung tâm THDL.

- Các thiết bị đưa vào/ra Trung tâm THDL phải đăng ký (theo Mẫu số 05), lập biên bản đưa thiết bị vào/ra Trung tâm THDL (theo Mẫu số 06).

3. Quy định đối với tổ chức, cá nhân đăng ký tham quan Trung tâm THDL:

a) Yêu cầu: Không được mang các thiết bị điện tử cá nhân (điện thoại, máy chụp hình, máy quay phim, thiết bị lưu trữ,…) khi tham quan.

b) Thủ tục: Tổ chức, cá nhân đến đăng ký tham quan cần có các giấy tờ sau:

- Văn bản đề nghị tham quan Trung tâm THDL (theo Mẫu số 01) phải được sự đồng ý của Thủ trưởng cơ quan quản lý Trung tâm THDL (trước đó, Sở Thông tin và Truyền thông phải tổng hợp, báo cáo xin ý kiến của UBND tỉnh);

- Giấy giới thiệu của cơ quan, đơn vị;

- Danh sách những người tham quan (có thông tin về số CMND, số căn cước công dân hoặc số Hộ chiếu kèm theo).

Điều 8. Quy định về an toàn hoạt động

1. Trung tâm THDL phải có nội quy sử dụng đối với các cơ quan, đơn vị, tổ chức, khách hàng, cán bộ và nhân viên trực tại đây bám sát theo Quy chế này. Trung tâm THDL được giám sát thường xuyên thông qua hệ thống kiểm soát vào ra và chỉ được đặt các thiết bị đang hoạt động phục vụ vận hành hệ thống. Trung tâm THDL tuyệt đối không đặt các thiết bị hỏng, thiết bị chờ thanh lý, các thiết bị của cá nhân, các vật dụng dễ cháy nổ…

2. Trung tâm THDL phải đảm bảo vệ sinh: Môi trường khô ráo, sạch sẽ, không dột, không thấm nước, không bị ánh nắng chiếu rọi trực tiếp. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị CNTT.

3. Hệ thống điện phải được trang bị máy phát điện dự phòng để đảm bảo cho hệ thống hoạt động trong thời gian nguồn điện lưới gặp sự cố.

4. Hệ thống điều hoà phải bảo đảm nhiệt độ cho phòng máy chủ theo tiêu chuẩn quy định đối với Trung tâm THDL.

5. Hệ thống đường truyền Internet cho Trung tâm THDL phải từ 02 nhà cung cấp dịch vụ khác nhau, có giải pháp chia tải, cân bằng tải đường truyền để đảm bảo độ dự phòng cao và tính sẵn sàng kết nối cho toàn hệ thống.

6. Hệ thống camera giám sát phải bảo đảm giám sát toàn bộ Trung tâm THDL liên tục trong 24 giờ/7 ngày; bảo đảm dữ liệu hình ảnh phải được lưu trữ ít nhất trong thời gian 30 ngày.

7. Thực hiện nghiêm túc công tác phòng cháy, chữa cháy theo quy định.

8. Quản lý an toàn hạ tầng mạng bao gồm:

- Quản lý, vận hành hoạt động bình thường của hệ thống;

- Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố;

- Truy cập và quản lý cấu hình hệ thống;

- Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

9. Quản lý an toàn máy chủ và ứng dụng bao gồm:

- Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

- Truy cập mạng của máy chủ;

- Truy cập và quản trị máy chủ, ứng dụng;

- Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

- Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;

- Kết nối và gỡ bỏ hệ thống máy chủ, dịch vụ khỏi hệ thống;

- Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

10. Quản lý an toàn dữ liệu bao gồm:

- Yêu cầu an toàn đối với phương pháp mã hóa;

- Phân loại, quản lý và sử dụng khóa bí mật, dữ liệu mã hóa;

- Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu;

- Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ;

- Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện, thời gian lưu trữ, nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ);

- Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng và hệ thống phụ;

- Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

11. Quản lý an toàn thiết bị đầu cuối bao gồm:

- Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

- Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;

- Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống;

- Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng;

- Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi đưa vào sử dụng.

12. Quản lý phòng chống phần mềm độc hại bao gồm:

- Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

- Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

- Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;

- Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

13. Quản lý giám sát an toàn hệ thống thông tin bao gồm:

- Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;

- Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có);

- Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;

- Truy cập và quản trị hệ thống giám sát;

- Loại thông tin cần được giám sát;

- Lưu trữ và bảo vệ thông tin giám sát (Nhật ký hệ thống);

- Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;

- Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;

- Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin 24/7.

14. Quản lý điểm yếu an toàn thông tin bao gồm:

- Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có);

- Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định;

- Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin;

- Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng;

- Phương án xử lý tạm thời khi điểm yếu an toàn thông tin không/chưa có khả năng xử lý;

- Quy trình khôi phục lại hệ thống sau khi xử lý điểm yếu an toàn thông tin thất bại;

- Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin với thành phần cụ thể trong hệ thống.

15. Quản lý sự cố an toàn người sử dụng đầu cuối bao gồm:

- Quản lý truy cập, sử dụng tài nguyên nội bộ;

- Quản lý truy cập mạng và tài nguyên trên Internet;

- Cài đặt và sử dụng máy tính an toàn.

Điều 9. Quy định về xử lý sự cố

1. Khi phát hiện có sự cố, đơn vị vận hành thực hiện các biện pháp cô lập và xác định nguyên nhân xảy ra sự cố theo nguyên tắc hạn chế tối đa ảnh hưởng tới hoạt động của hệ thống; đồng thời phải thông báo cho bộ phận sử dụng và các cơ quan, đơn vị có liên quan về tình hình sự cố.

2. Tùy thuộc vào mức độ ảnh hưởng của sự cố, đánh giá và phân loại theo 03 mức: sự cố thông thường, sự cố nghiêm trọng và sự cố đặc biệt nghiêm trọng.

a) Đối với các sự cố thông thường (không gây ảnh hưởng đến hoạt động của Trung tâm THDL), đơn vị vận hành nhanh chóng xử lý sự cố. Trường hợp không xử lý được, thông báo cơ quan quản lý để phối hợp giải quyết.

b) Đối với các sự cố nghiêm trọng (các sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố liên quan đến an ninh thông tin, mất mát dữ liệu, gây ảnh hưởng trực tiếp đến hoạt động của Trung tâm THDL), ngay sau khi phát hiện sự cố đơn vị vận hành cần đánh giá ảnh hưởng của sự cố và thực hiện báo cáo về cơ quan quản lý để có chỉ đạo xử lý và báo cáo UBND tỉnh.

c) Đối với các sự cố đặc biệt nghiêm trọng (gây ngưng trệ đến toàn bộ hoạt động của Trung tâm THDL), đơn vị vận hành và cơ quan quản lý phải có đánh giá ảnh hưởng của sự cố và thực hiện báo cáo kịp thời UBND Tỉnh để xin ý kiến chỉ đạo xử lý.

3. Yêu cầu đối với việc xử lý sự cố cần tuân thủ các nguyên tắc:

a) Phải tuân thủ Quy trình xử lý sự cố do cơ quan quản lý, vận hành Trung tâm THDL phê duyệt và ban hành.

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

c) Các dữ liệu quan trọng phải được sao lưu trước khi xử lý sự cố.

d) Ghi nhật ký sự cố kỹ thuật phát sinh tại chỗ (theo Mẫu số 02).

đ) Thông báo cho các bên liên quan về thời gian khắc phục xong sự cố.

e) Lập báo cáo sự cố gửi cơ quan quản lý đối với các sự cố nghiêm trọng và đặc biệt nghiêm trọng trong vòng 24 giờ kể từ khi phát hiện sự cố.

Điều 10. Quản lý truy cập

1. Chính sách truy cập thông tin nghiệp vụ

- Phân loại các ứng dụng, hệ thống mạng theo các mức độ an ninh: thông tin bí mật, nhạy cảm, thông tin nội bộ, thông tin dùng chung.

- Phân quyền quản lý truy cập theo người dùng, nhóm người dùng.

2. Chính sách quản lý truy cập mạng

- Phân tách các dịch vụ khác nhau nằm trong các vùng mạng khác nhau. Đặc biệt, các ứng dụng nhạy cảm phải được tách riêng và kiểm soát chặt chẽ.

- Yêu cầu ràng buộc đối với người dùng khi truy cập dịch vụ:

+ Nhập đúng tên người dùng;

+ Đăng nhập đúng phạm vi sử dụng;

+ Thay đổi mật khẩu mặc định;

+ Chấp nhận cơ chế mã hóa dữ liệu của hệ thống;

+ Máy trạm cài đầy đủ các phần mềm bảo mật;

+ Địa chỉ máy trạm được phép truy cập.

- Lập hồ sơ ghi lại cách sử dụng các dịch vụ mạng: Lớp mạng và dịch vụ mạng nào được phép truy cập, ai là người được truy cập, quy trình kiểm soát truy cập như thế nào.

3. Chính sách quản lý kết nối từ xa

- Phải sử dụng những hệ thống, phương thức mã hóa trên đường truyền như OpenSSL, HTTPS, SSH…

- Sử dụng phương thức kết nối an toàn, đảm bảo khả năng bảo mật thông tin như VPN.

- Kiểm soát và hạn chế các kết nối hoặc truy cập đến các cổng điều khiển, quản lý: Cổng console, cổng cho phép remote access trên thiết bị mạng (telnet, ssh). Các cổng kết nối từ xa đến các máy chủ.

- Đặt mật khẩu bảo vệ, đóng các cổng không sử dụng trên thiết bị.

Điều 11. Quy định về an toàn, bảo mật thông tin

1. Chính sách làm việc tại vùng an toàn thông tin

- Người được phân công trực, làm việc tại vùng an toàn thông tin phải có trách nhiệm giữ chìa khóa, vân tay ra vào phòng máy, giám sát những cá nhân khác khi họ vào phòng máy chủ làm việc.

- Những thiết bị xử lý thông tin không được dùng phải được khóa và cất vào kho lưu trữ.

- Các cá nhân tuyệt đối không chụp ảnh, quay phim, ghi âm các cuộc trao đổi thông tin nơi làm việc, trừ trường hợp được sự cho phép của Lãnh đạo đơn vị quản lý, vận hành Trung tâm THDL tỉnh.

2. Phân chia trách nhiệm người dùng

- Phân chia nhiệm vụ quản lý, vận hành và sử dụng hệ thống một cách rõ ràng, không chồng chéo và theo nhu cầu công việc.

- Nhân viên hỗ trợ xử lý sự cố hệ thống chỉ được cấp tài khoản truy cập hệ thống trong trường hợp cần thiết và cắt tài khoản đó ngay sau khi công việc hỗ trợ kết thúc. Đồng thời người quản trị phải giám sát chặt chẽ nhân viên hỗ trợ trong thời gian nhân viên đó truy cập hệ thống.

- Chỉ cho phép nhân viên tạm thời, đối tác, người dùng vãng lai sử dụng tối thiểu các trang thiết bị thông dụng như máy tính để bàn, máy in, máy photo và nghiêm cấm việc ra vào tự do các nơi làm việc của nhân viên chính thức, nơi để thiết bị của Trung tâm THDL.

3. Quy định về việc bảo mật hệ thống

a) Quản lý các phần mềm vận hành

- Chỉ những người quản trị hệ thống mới được cập nhật và sử dụng phần mềm hệ thống có liên quan.

- Chỉ triển khai các phần mềm vận hành khi máy chủ đã được kiểm tra an ninh và sẵn sàng đáp ứng cho việc cài đặt ứng dụng.

- Sao lưu các phần mềm trước khi thay đổi để đề phòng trường hợp phải sử dụng lại những phiên bản cũ.

- Cập nhật thường xuyên các bản vá lỗi bảo mật đối với các phần mềm hệ thống.

- Kiểm soát chặt chẽ hoạt động hỗ trợ của nhà cung cấp đối với các phần mềm hệ thống.

- Ghi nhật ký việc cập nhật các phần mềm vận hành.

b) Bảo vệ dữ liệu kiểm thử hệ thống

- Yêu cầu bảo vệ và kiểm soát các dữ liệu dùng làm kiểm thử như là với dữ liệu thật của hệ thống.

- Áp dụng các chức năng quản lý truy cập đối với cả hệ thống ứng dụng kiểm thử.

- Hạn chế và phân quyền sao chép thông tin vận hành tới hệ thống kiểm thử.

- Xóa thông tin vận hành khỏi hệ thống ứng dụng kiểm thử ngay sau khi việc kiểm thử hoàn tất.

- Ghi nhật ký việc sao chép và sử dụng thông tin vận hành vào mục đích kiểm thử.

Điều 12. Chính sách thiết lập và quản lý mật khẩu

1. Chính sách thiết lập và quản lý mật khẩu áp dụng cho các thiết bị, hệ thống thông tin, cơ sở dữ liệu được lắp đặt, triển khai tại Trung tâm THDL tỉnh.

2. Lãnh đạo đơn vị vận hành Trung tâm THDL có trách nhiệm tiếp nhận mật khẩu quản trị hệ thống sau khi hệ thống được bàn giao và đưa vào sử dụng; sau đó tiến hành bàn giao cho cán bộ quản lý hệ thống có biên bản kèm theo, lưu vào nơi an toàn (cho vào phong bì, để vào tủ có khóa).

3. Nhân viên vận hành được giao mật khẩu quản trị hệ thống từ cán bộ quản lý hệ thống phải thực hiện đổi mật khẩu sau khi tiếp nhận trong vòng 01 ngày. Việc đổi mật khẩu quản trị hệ thống phải tuân thủ theo đúng quy định hướng dẫn về mật khẩu do cơ quan quản lý ban hành.

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

a) Độ dài của mật khẩu:

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

- Đối với mật khẩu quản trị hệ thống (sử dụng cho quản trị các hệ thống mạng, bảo mật, máy chủ, thư điện tử, ứng dụng,...): Tối thiểu là 12 ký tự.

b) Nội dung mật khẩu:

- Không bao gồm các từ dễ nhớ như tên, ngày sinh, số điện thoại;

- Không được đặt theo ký tự chữ cái, ký tự chữ số tuần tự hoặc một dãy các ký tự giống nhau, ví dụ: ABCDEFGH, 98765432 hoặc !!!!!!!!...;

- Đối với mật khẩu phải kết hợp các loại ký tự sau: Chữ cái in thường (a, b,…), chữ cái in hoa (A, B,…), ký tự số (1, 2,…) và các ký tự đặc biệt (@, !, #...).

c) Thời gian sử dụng mật khẩu:

- Mật khẩu phải được thay đổi ít nhất 01 tháng 01 lần.

- Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn thông tin thì Thủ trưởng đơn vị vận hành Trung tâm THDL quyết định việc thay đổi toàn bộ mật khẩu quản trị của Trung tâm THDL.

d) Quy định sử dụng và lưu trữ mật khẩu:

- Người sử dụng phải thay đổi mật khẩu ngay từ lần đăng nhập đầu tiên;

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

- Không được chia sẻ mật khẩu cho người khác;

- Phải tiến hành thay đổi mật khẩu ngay khi nghi ngờ bị lộ lọt thông tin mật khẩu;

- Mật khẩu mới thay đổi phải đảm bảo không trùng với những mật khẩu đã từng sử dụng trước đó;

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

Điều 13. Quy định về việc sao lưu dữ liệu

Các đơn vị, cá nhân tham gia vào Trung tâm THDL của tỉnh đều phải tạo lập chế độ lưu giữ thông tin theo quy định, với những yêu cầu sau:

1. Với người sử dụng: Có thể sao lưu lên thiết bị lưu trữ dời như (usb, ổ cứng di động, …) Chỉ thực hiện sao lưu những dữ liệu quan trọng của riêng mình.

2. Với dữ liệu trên máy chủ: Có thể sao lưu lên ổ đĩa cứng khác (trên máy chủ hoặc một máy đơn lẻ), sao lưu ra băng từ hoặc đĩa từ quang.

3. Quy định chu kỳ sao lưu: Cuối một chu kỳ sao lưu, thực hiện sao lưu toàn bộ dữ liệu cần thiết (full backup). Trong một chu kỳ lớn, có thể chia thành các khoảng nhỏ (ví dụ 1 ngày/lần), thực hiện sao lưu những thay đổi kể từ lần sao lưu đầy đủ mới nhất.

4. Dữ liệu của hai lần sao lưu đầy đủ liền nhau phải lưu lên hai băng từ hoặc hai đĩa từ quang khác nhau. Cần quy định số lượng và dung lượng băng từ tối thiểu phải sử dụng (tuỳ theo thông tin cần sao lưu). Dung lượng trống để phục vụ lưu trữ tối thiểu phải gấp ít nhất ba lần tổng dữ liệu cần sao lưu.

5. Đĩa và băng từ sao lưu phải được giữ ở nơi cách xa về vật lý với máy chủ, đề phòng trường hợp hoả hoạn hay bất trắc xảy ra.

6. Thông tin về tất cả các lần sao lưu đều phải ghi rõ trong Nhật ký sao lưu dữ liệu. Các băng, đĩa sử dụng sao lưu phải có đánh số, dán nhãn và ghi chú cẩn thận để có thể tìm lại dễ dàng, tránh nhầm lẫn.

Điều 14. Quy định về quản lý thiết bị

1. Thiết bị CNTT đặt tại Trung tâm THDL phải đặt tên và dán nhãn theo đúng quy định.

2. Đơn vịvận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị tại Trung tâm THDL hàng quý.

3. Đơn vịvận hành đề xuất mua thêm thiết bị CNTT và các thiết bị phụ trợ khác trong trường hợp thiết bị hết bảo hành bị hỏng. Thiết bị được trang bị phải tuân theo các tiêu chuẩn về thiết bị cho Trung tâm THDL.

4. Đối với thiết bị hỏng còn bảo hành, đơn vị khai thác, vận hành yêu cầu đơn vị cung cấp sửa chữa. Thiết bị hỏng đã hết bảo hành, cơ quan vận hành báo cáo cơ quan quản lý về phương án sửa chữa.

5. Trường hợp thiết bị hỏng là thiết bị quan trọng (máy chủ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị tường lửa), đơn vị vận hành phải báo cáo ngay về cơ quan quản lý để có biện pháp khắc phục nhanh.

Điều 15. Quy định về hệ thống mạng và truyền dẫn

1. Hệ thống mạng và truyền dẫn phải đảm bảo hiệu năng cho các ứng dụng, khả năng sẵn sàng và có các giải pháp để đảm bảo an toàn hệ thống.

2. Hệ thống mạng và truyền dẫn phải bảo đảm:

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

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

c) Tuân thủ theo các tiêu chuẩn của Trung tâm THDL về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức đi dây, đấu nối, phân bổ nút mạng.

d) Tuân thủ quy định về các phân vùng chức năng đã được quy hoạch. Mỗi phân vùng trong Trung tâm THDL ứng với dải địa chỉ IP cấp phát riêng và VLAN tương ứng, đồng thời được thiết lập các chính sách an ninh và truy cập khác nhau.

e) Hàng năm, đơn vị vận hành đề xuất cơ quan quản lý về thuê đường truyền Internet đảm bảo tốc độ, băng thông cho hoạt động Trung tâm THDL. Đường truyền Internet cho Trung tâm THDL phải từ tối thiểu 02 nhà cung cấp dịch vụ khác nhau để đảm bảo độ dự phòng cao và tính sẵn sàng cho hệ thống.

Điều 16. Quy định về giám sát an toàn thông tin cho hệ thống

1. Đảm bảo thực hiện thường xuyên, liên tục.

2. Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

3. Đảm bảo ổn định tính bí mật thông tin được cung cấp, trao đổi trong quá trình giám sát.

4. Có sự điều phối, kết hợp chặt chẽ, hiệu quả giữa việc giám sát của Bộ Thông tin và Truyền thông và hoạt động giám sát của chủ quản hệ thống thông tin; Từng bước xây dựng khả năng liên thông giữa hệ thống giám sát của Bộ Thông tin và Truyền thông và hệ thống giám sát của chủ quản hệ thống thông tin trên phạm vi toàn quốc.

Điều 17. Quy định về quản lý bản quyền phần mềm

1. Các phần mềm, chương trình ứng dụng sử dụng cho Trung tâm THDL phải có bản quyền sử dụng và được gia hạn bản quyền định kỳ, đảm bảo cho các hệ thống hoạt động liên tục, ổn định, không gián đoạn.

2. Chỉ được cài đặt và sử dụng các phần mềm đã mua bản quyền. Các phần mềm chưa có bản quyền, phần mềm mã nguồn mở, phần mềm miễn phí phải được cơ quan quản lý về chuyên môn phê duyệt, đồng ý trước khi sử dụng.

3. Đơn vị vận hành quản lý, theo dõi sử dụng các bản quyền phần mềm tại Trung tâm THDL. Lập dự toán và báo cáo các cơ quan liên quan gia hạn bản quyền đảm bảo hoạt động liên tục, ổn định của toàn bộ hệ thống.

4. Không phát tán, chia sẻ phần mềm có bản quyền của Trung tâm THDL ra bên ngoài.

Điều 18. Quy định về bảo trì, bảo dưỡng

1. Đơn vị vận hành có trách nhiệm:

a) Xây dựng, tham mưu cơ quan quản lý phê duyệt và ban hành quy trình bảo trì, bảo dưỡng hệ thống.

b) Trực tiếp thực hiện hoặc thuê dịch vụ để thực hiện bảo trì, bảo dưỡng các hệ thống.

2. Yêu cầu về bảo trì, bảo dưỡng:

a) Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn và ảnh

hưởng đến tình hình cung cấp dịch vụ của Trung tâm THDL.

b) Quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, quy trình và ghi nhật ký về quá trình bảo trì, bảo dưỡng, tình trạng hoạt động trước và sau khi thực hiện.

3. Hệ thống điện, lưu điện UPS

- Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần.

- Các công việc bảo trì, bảo dưỡng hệ thống:

+ Vệ sinh công nghiệp toàn bộ hệ thống điện, lưu điện UPS;

+ Kiểm tra tình trạng kết nối vật lý của các cấu phần trong hệ thống điện, lưu điện UPS;

+ Kiểm tra, đánh giá tình trạng hoạt động của các cấu phần trên lưu điện UPS: Bảng điện, tụ lọc, bộ chỉnh lưu, bộ nạp điện, quạt, máy biến thế, cuộn cảm, thanh cái, cầu chì, dây cáp nguồn, cáp tín hiệu và các cấu phần khác (nếu cần);

+ Kiểm tra, đánh giá tình trạng sử dụng ắc quy, thời gian hoạt động khi mất nguồn đầu vào;

+ Kiểm tra, đánh giá tải sử dụng trên hệ thống tủ phân phối nguồn; thực hiện cân lại tải nếu cần;

+ Kiểm tra bộ phận chống sét, tiếp đất của toàn bộ hệ thống điện, lưu điện UPS;

+ Xử lý các vấn đề phát hiện được sau khi kiểm tra hệ thống;

+ Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

4. Hệ thống điều hòa, hệ thống thông gió

Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần. Các công việc bảo trì, bảo dưỡng hệ thống tối thiểu gồm:

a) Hệ thống điều hòa:

- Vệ sinh công nghiệp toàn bộ hệ thống điều hòa;

- Kiểm tra trạng thái vật lý của thiết bị (vỏ ngoài, tiếng động lạ);

- Kiểm tra các cảnh báo, log (sự kiện);

- Kiểm tra tình trạng hoạt động các thành phần của dàn nóng: Quạt, bộ điều khiển;

- Kiểm tra tình trạng hoạt động các thành phần của dàn lạnh: Bộ lọc, bảng mạch điều khiển, quạt, dây curoa, dàn ngưng tụ, bộ tạo ẩm, van tiết lưu, khay cấp/thoát nước;

- Kiểm tra tình trạng hoạt động của máy nén, ống dẫn ga: Rơle áp suất, áp suất đường ống ga, tình trạng rò rỉ của đường ống, thông số về dòng điện;

- Kiểm tra tình trạng hoạt động các thành phần điện cấp cho điều hòa: Thiết bị chống quá tải, rơle, dây cáp nguồn, cáp tín hiệu, các điểm đấu nối;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra hệ thống;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

b) Hệ thống phát hiện chất lỏng:

- Kiểm tra trạng thái vật lý của cáp dùng để phát hiện chất lỏng;

- Kiểm tra hoạt động của các bảng mạch điều khiển và nguồn điện cấp cho bảng mạch;

- Thử nghiệm phát hiện chất lỏng, kiểm tra việc cảnh báo khi xuất hiện chất lỏng;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra hệ thống;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

c) Hệ thống giám sát môi trường:

- Vệ sinh các đầu cảm biến;

- Kiểm tra tính chính xác của đầu cảm biến;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

5. Hệ thống kiểm soát an ninh

- Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần.

- Các công việc bảo trì, bảo dưỡng hệ thống:

+ Vệ sinh công nghiệp thiết bị camera, đầu đọc thẻ từ/đầu đọc vân tay các thiết bị phụ trợ cho hệ thống;

+ Kiểm tra bộ kết nối từ camera, đầu đọc thẻ từ/đầu đọc vân tay đến bộ phận điều khiển;

+ Xử lý các vấn đề phát hiện được sau khi kiểm tra;

+ Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

6. Hệ thống phòng cháy chữa cháy

Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần.

Các công việc bảo trì, bảo dưỡng hệ thống:

a) Hệ thống phát hiện khói độ nhạy cao:

- Vệ sinh công nghiệp toàn bộ hệ thống;

- Kiểm tra quạt hút, vệ sinh bộ lọc khí. Kiểm tra kết nối và trạng thái dây tín hiệu và dây nguồn;

- Kiểm tra chức năng báo khói của bảng điều khiển, đèn còi cảnh báo, đầu cảm biến;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

b) Hệ thống chữa cháy:

- Vệ sinh công nghiệp toàn bộ hệ thống;

- Kiểm tra chức năng báo cháy của bảng điều khiển, đèn còi cảnh báo, đầu cảm biến;

- Kiểm tra tình trạng vật lý của các thiết bị. Kiểm tra đầu xả, nút xả/ngắt khí;

- Kiểm tra áp suất bình khí chữa cháy;

- Kiểm thử hoạt động của hệ thống chữa cháy (test không xả);

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

7. Hệ thống giám sát và cảnh báo sớm an toàn thông tin

- Đảm bảo được thực hiện, sử dụng, khai thác thường xuyên, liên tục.

- Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

- Đảm bảo giám sát đầy đủ các điểm thuộc phạm vi giám sát.

- Đảm bảo hoạt động ổn định, bí mật cho thông tin được cung cấp, trao đổi trong quá trình giám sát.

- Thường xuyên tổng hợp báo cáo giám sát hàng tuần (vào thứ hai hàng tuần), tháng và báo cáo giám sát đột xuất theo yêu cầu của cơ quan quản lý để cảnh báo, hướng dẫn các đơn vị liên quan và báo cáo các cơ quan cấp trên có thẩm quyền.

8. Hệ thống mạng

Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần.

Các công việc bảo trì, bảo dưỡng hệ thống:

- Vệ sinh thiết bị mạng, hệ thống mạng 01tháng/1lần;

- Kiểm tra chức năng của giao diện quản trị hệ thống mạng, các phần mềm

quản trị hệ thống mạng;

- Sử dụng các phần mềm chuyên dùng để kiểm tra đánh giá tình trạng vật lý thiết bị mạng;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

9. Hệ thống máy chủ

Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần.

Các công việc bảo trì, bảo dưỡng hệ thống:

- Vệ sinh máy chủ, hệ thống máy chủ 01tháng/1lần;

- Kiểm tra chức năng của giao diện quản trị máy chủ, các phần mềm quản trị hệ thống máy chủ liên quan;

- Sử dụng các phần mềm chuyên dùng để kiểm tra đánh giá tình trạng vật lý máy chủ;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

10. Hệ thống lưu trữ, sao lưu, khôi phục dữ liệu

Tần suất thực hiện bảo trì, bảo dưỡng: Tối thiểu mỗi quý (3 tháng) thực hiện 1 lần.

Các công việc bảo trì, bảo dưỡng hệ thống:

a) Hệ thống lưu trữ

- Vệ sinh công nghiệp toàn bộ hệ thống;

- Kiểm tra kết nối và trạng thái dây tín hiệu và dây nguồn;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

b) Hệ thống sao lưu dữ liệu

- Vệ sinh công nghiệp toàn bộ hệ thống;

- Kiểm tra kết nối và trạng thái dây tín hiệu và dây nguồn;

- Xử lý các vấn đề phát hiện được sau khi kiểm tra;

- Nhận xét, đánh giá hiện trạng của hệ thống và đưa ra những khuyến nghị, dự báo sự cố có thể xảy ra với hệ thống (nếu có).

Điều 19. Quy định về quản lý hồ sơ

1. Danh sách các loại hồ sơ lưu trữ

a) Các quy trình vận hành kỹ thuật, bảo trì, bảo dưỡng các hệ thống.

b) Hồ sơ thiết kế, thuyết minh kỹ thuật, hoàn công.

c) Hồ sơ quản trị các hệ thống thông tin (báo cáo định kỳ, báo cáo sự cố, nhật ký vận hành).

d) Hồ sơ lưu các dịch vụ cung cấp cho các tổ chức, cơ quan, đơn vị, khách hàng.

đ) Bảng thống kê danh sách thiết bị; Danh sách các thiết bị hỏng, hết khấu hao sử dụng chờ thanh lý, thanh hủy; Biên bản bàn giao thiết bị.

e) Tài liệu, biên bản kiểm tra, đánh giá của Trung tâm THDL.

g) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ phải được lưu bằng văn bản, tập tin bản mềm trên máy tính và phải được cập nhật khi có sự thay đổi theo quy định.

Điều 20. Quy định về kiểm tra, báo cáo định kỳ

1. Hằng tháng, cán bộ quản lý Trung tâm THDL phải thực hiện báo cáo tình hình hoạt động của Trung tâm THDL lên Lãnh đạo đơn vị vận hành và tổng hợp báo cáo Cơ quan quản lý.

2. Cơ quan quản lý, đơn vị vận hành tổ chức kiểm tra việc tuân thủ các quy định về quản lý, triển khai, vận hành và khai thác sử dụng Trung tâm THDL theo các quy định tại Quy chế này định kỳ hàng năm, hoặc kiểm tra đột xuất khi có các vấn đề phát sinh cần làm rõ.

3. Các nội dung kiểm tra:

a) Việc bảo đảm các điều kiện về vệ sinh, môi trường cho hoạt động của Trung tâm THDL.

b) Tình hình sử dụng thiết bị, sử dụng ứng dụng của hệ thống.

c) Hoạt động của hệ thống máy chủ, máy trạm, các dịch vụ (cập nhật các bản vá, bản sửa lỗi, dung lượng ổ cứng, hiệu năng sử dụng…).

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

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

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

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

4. Hàng quý, cơ quan vận hành tiến hành kiểm tra định kỳ, đánh giá phân tích hiệu quả hoạt động của Trung tâm THDL và tổng hợp báo cáo (theo Mẫu số 03) với cơ quan quản lý. Trong trường hợp phát hiện các bất cập, lỗi liên quan đến các hệ thống, cần thực hiện báo cáo nhanh và xây dựng kế hoạch khắc phục.

CHƯƠNG III
TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN CÓ LIÊN QUAN

Điều 21. Trách nhiệm của cơ quan, đơn vị có hệ thống đặt tại Trung tâm THDL, đơn vị và cá nhân khai thác, sử dụng các hệ thống thông tin tại Trung tâm THDL tỉnh

1. Sử dụng dịch vụ Trung tâm THDL trong phạm vi cho phép.

2. Tuân thủ Quyết định số 708/QĐ-UBND ngày 14/4/2014 của UBND tỉnh về ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước tỉnh Quảng Ninh, các quy định về an toàn bảo mật thông tin, quản lý, khai thác và vận hành Trung tâm THDL.

3. Mỗi cơ quan nhà nước, tổ chức có kết nối về Trung tâm THDL cử ít nhất một cán bộ có trình độ về công nghệ thông tin hoặc am hiểu về công nghệ thông tin, quản trị mạng giúp lãnh đạo cơ quan, tổ chức thực hiện công tác quản trị mạng (gọi tắt là Quản trị mạng cơ sở). Cán bộ này có nhiệm vụ triển khai công tác kỹ thuật quản trị mạng đối với hệ thống mạng cục bộ tại đơn vị tuân thủ theo các quy định của Trung tâm THDL để thống nhất về cấu trúc hạ tầng và cấu trúc vật lý của toàn bộ Hệ thống mạng truyền số liệu chuyên dùng, kịp thời báo cáo các sự cố kỹ thuật để cơ quan vận hành Trung tâm THDL tỉnh xử lý.

4. Trường hợp bàn giao tài khoản quản trị, vận hành hệ thống đặt tại Trung tâm tích hợp dữ liệu tỉnh (theo Mẫu số 07).

5. Trường hợp phát hiện sự cố, thông báo cho Đơn vị vận hành (theo Mẫu số 08), cán bộ kỹ thuật của Đơn vị vận hành để được hướng dẫn và hỗ trợ khắc phục. Phối hợp với cán bộ kỹ thuật của Đơn vị vận hành trong việc xử lý sự cố và xác nhận kết quả xử lý.

6. Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật về đảm bảo an toàn thông tin cho toàn bộ hệ thống thông tin của đơn vị theo các Quy định được áp dụng tại Trung tâm THDL.

7. Thực hiện quy định quản lý về tài khoản các phần mềm, hệ thống thông tin, địa chỉ IP (Internet Protocol) và các giao thức kết nối hệ thống mạng WAN của tỉnh và có trách nhiệm tuân thủ các hướng dẫn, quy trình vận hành mạng cục bộ của Quản trị mạng cơ sở, các quy định về an toàn an ninh thông tin đối với hệ thống thiết bị mạng cục bộ của đơn vị.

8. Chịu trách nhiệm về nội dung, thông tin lưu trữ của đơn vị mình tại Trung tâm THDL theo đúng quy định pháp luật và có trách nhiệm sao lưu định kỳ dữ liệu của đơn vị, theo sự hướng dẫn của Đơn vị vận hành.

9. Thực hiện các hướng dẫn, quy trình vận hành trong hệ thống mạng truyền số liệu chuyên dùng của tỉnh. Khi có thay đổi kết nối, cấu trúc mạng cục bộ của đơn vị phải thông báo với Đơn vị vận hành để phối hợp triển khai đảm bảo an toàn và ổn định của hệ thống mạng.

10. Các cán bộ, công chức, viên chức ở các đơn vị chịu trách nhiệm về thông tin tài khoản, mật mã đăng nhập vào hệ thống; đồng thời, có trách nhiệm thay đổi ngay mật mã sau khi được Đơn vị vận hành cung cấp. Ngoài ra, không được sử dụng bất cứ hình thức nào để truy nhập trái phép vào hệ thống mạng, ứng dụng của tổ chức, cá nhân khác (trừ các yêu cầu của cơ quan chức năng có thẩm quyền). Phối hợp với cán bộ kỹ thuật của cơ quan, đơn vị mình trong việc xử lý sự cố và xác nhận kết quả xử lý.

11. Khi có nhu cầu về các dịch vụ, hệ thống phần mềm của Trung tâm THDL phục vụ hoạt động ứng dụng công nghệ thông tin thì cơ quan, tổ chức phải gửi Đăng ký sử dụng các dịch vụ của Trung tâm THDL (theo Mẫu số 04) về Sở Thông tin và Truyền thông, Trung tâm Công nghệ thông tin và Truyền thông xem xét, cấp phát tài nguyên phù hợp với quy hoạch hạ tầng kỹ thuật chung của tỉnh và phù hợp với công năng toàn hệ thống THDL.

12. Trường hợp phát hiện sự cố, thông báo cho cán bộ kỹ thuật của đơn vị vận hành để được hướng dẫn và hỗ trợ khắc phục. Phối hợp với cán bộ kỹ thuật của Đơn vị vận hành trong việc xử lý sự cố và xác nhận kết quả xử lý.

13. Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật về đảm bảo an toàn thông tin cho toàn bộ hệ thống thông tin của đơn vị theo các Quy định được áp dụng tại Trung tâm THDL.

Điều 22. Trách nhiệm của cơ quan quản lý Trung tâm THDL

1. Tham mưu UBND tỉnh quản lý, đảm bảo vận hành, nâng cấp và mở rộng Trung tâm THDL của tỉnh, đáp ứng nhu cầu ứng dụng công nghệ thông tin, xây dựng chính quyền điện tử, thành phố thông minh.

2. Phê duyệt các quy trình về vận hành, bảo trì, bảo dưỡng và khắc phục sự cố; quy trình cung cấp dịch vụ Trung tâm THDL.

3. Hướng dẫn các cơ quan, cán bộ, công chức, viên chức và doanh nghiệp, người dân sử dụng dịch vụ Trung tâm THDL.

4. Hướng dẫn triển khai các giải pháp bảo đảm an toàn, an ninh đối với các hệ thống thông tin điện tử thuộc Trung tâm THDL.

5. Quy hoạch tài nguyên hệ thống, các giải pháp, phương án kỹ thuật, các kế hoạch nâng cấp, phát triển Trung tâm THDL.

6. Chỉ đạo mở hoặc dừng đột xuất một số dịch vụ Trung tâm THDL trong các trường hợp có sự cố an toàn thông tin mạng hoặc để đảm bảo hoạt động ổn định của Trung tâm THDL.

7. Kiểm tra và giám sát việc quản trị, vận hành, khai thác dịch vụ, hệ thống phần mềm tại Trung tâm THDL.

8. Định kỳ hằng năm hoặc đột xuất, thực hiện báo cáo UBND tỉnh về tình hình hoạt động và cung cấp dịch vụ, đảm bảo an toàn thông tin của Trung tâm THDL.

Điều 23. Trách nhiệm của Sở Tài chính

Chủ trì thẩm định, tham mưu và bố trí kinh phí để duy trì hoạt động của Trung tâm THDL theo đề xuất của Sở Thông tin và Truyền thông để trình UBND tỉnh phê duyệt kinh phí hằng năm đối với công tác quản lý, vận hành, bảo trì, bảo dưỡng Trung tâm tích hợp dữ liệu.

Điều 24. Trách nhiệm của đơn vị trực tiếp vận hành Trung tâm THDL

1. Chịu trách nhiệm toàn diện về việc vận hành có hiệu quả, bảo vệ, bảo trì, bảo dưỡng và khắc phục sự cố bảo đảm các yêu cầu về hạ tầng kỹ thuật, chất lượng dịch vụ, an toàn thông tin và hoạt động thông suốt của Trung tâm THDL theo quy chế này.

2. Có trách nhiệm lập dự toán, chấp hành dự toán, thực hiện chế độ kế toán, chịu trách nhiệm quản lý và sử dụng các nguồn tài chính, tài sản và cơ sở vật chất được giao theo quy định của pháp luật để vận hành Trung tâm THDL.

3. Đào tạo cán bộ quản lý, vận hành có chuyên môn đáp ứng yêu cầu, được trang bị các kiến thức liên quan đến hoạt động của Trung tâm THDL.

4. Triển khai các nhiệm vụ được UBND tỉnh, Sở Thông tin và Truyền thông giao; Xây dựng kế hoạch hợp tác, khai thác Trung tâm THDL với các tổ chức có liên quan trình Cơ quan quản lý Trung tâm THDL xem xét, phê duyệt để triển khai thực hiện.

5. Tiếp nhận yêu cầu cung cấp dịch vụ của các tổ chức, cá nhân trong phạm vi quy định và triển khai cung cấp dịch vụ theo đúng với tiêu chuẩn chất lượng, quy trình và trên cơ sở khai thác hiệu quả hạ tầng Trung tâm THDL khi được sự phê duyệt của Cơ quan quản lý Trung tâm THDL.

6. Trực tiếp thực hiện hoặc thuê dịch vụ để thực hiện bảo trì, bảo dưỡng các hệ thống.

7. Xây dựng phương án đề xuất nâng cấp, mở rộng Trung tâm THDL tỉnh.

8. Thực hiện báo cáo định kỳ hàng quý cho cơ quan quản lý về tình hình hoạt động và cung cấp dịch vụ của Trung tâm THDLvà báo cáo đột xuất khi có yêu cầu.

9. Tuân thủ và thực hiện đúng các quy định của nhà nước, quy định của ngành và các quy định nêu trong văn bản này.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 25. Xử lý vi phạm

Đơn vị, tổ chức, cá nhân vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm mà bị xử lý theo trách nhiệm, xử phạt hành chính, bồi thường thiệt hại hoặc bị truy cứu trách nhiệm hình sự theo quy định hiện hành.

Điều 26. Điều khoản thi hành

1. Giao Sở Thông tin và Truyền thông chịu trách nhiệm giám sát, theo dõi, đôn đốc, triển khai thực hiện Quy chế này; định kỳ hàng năm tổng hợp báo cáo UBND tỉnh.

2. Thủ trưởng các cơ quan, đơn vị, cá nhân có liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này. Trong quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị, địa phương kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đặng Huy Hậu

DANH MỤC CÁC MẪU VĂN BẢN

(Ban hành kèm theo Quyết định số 26 /2018/QĐ-UBND ngày 20 /9/2018 của UBND tỉnh)

STT	Danh mục	Ký hiệu
1	Đề nghị tham quan Trung tâm Tích hợp dữ liệu tỉnh Quảng Ninh	Mẫu số 01
2	Nhật ký sự cố kỹ thuật Trung tâm Tích hợp dữ liệu	Mẫu số 02
3	Báo cáo về tình hình hoạt động của Trung tâm Tích hợp dữ liệu	Mẫu số 03
4	Đề nghị cung cấp dịch vụ Trung tâm Tích hợp dữ liệu	Mẫu số 04
5	Phiếu yêu cầu về việc đưa thiết bị vào/ra Trung tâm Tích hợp dữ liệu	Mẫu số 05
6	Biên bản đưa thiết bị vào/ra Trung tâm Tích hợp dữ liệu	Mẫu số 06
7	Biên bản bàn giao	Mẫu số 07
8	Đề nghị về việc khắc phục sự cố	Mẫu số 08

Mẫu số 01

Tên cơ quan:
.....

Số: .....
V/v Đề nghị tham quan Trung tâm Tích hợp dữ liệu tỉnh Quảng Ninh

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

....., ngày ..... tháng ..... năm 20....

Kính gửi: Sở Thông tin và Truyền thông.

A. Thông tin chung

Tên cơ quan: . .....

Địa chỉ: .....

Điện thoại: ..... Email: .....

Đầu mối liên hệ (Tên cán bộ, địa chỉ email, số điện thoại): .....

.....

B. Phần đề nghị

Chúng tôi đề nghị được tham quan Trung tâm tích hợp dữ liệu tỉnh:

1. Mục đích:

.....

2. Thời gian đến tham quan:

.....

3. Thành phần đoàn tham quan: *(kèm theo danh sách chi tiết)*

.....

4. Các đề nghị khác: *(nếu có)*

.....

.....

Chúng tôi cam kết tuân thủ mọi nội quy, quy định của các cơ quan chức năng khi vào tham quan Trung tâm tích hợp dữ liệu tỉnh./.

Thủ trưởng đơn vị
(Ký, đóng dấu)

Mẫu số 02

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NHẬT KÝ SỰ CỐ KỸ THUẬT TRUNG TÂM TÍCH HỢP DỮ LIỆU

STT	Người phát hiện	Người xử lý	Thời gian phát hiện (Ngày, giờ)	Thời gian xử lý xong (Ngày, giờ)	Mô tả sự cố	Nguyên nhân	Cách xử lý	Xác nhận của Cán bộ quản lý

Mẫu số 03

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Số: /BC-TTCNTT&TT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Quảng Ninh, ngày tháng năm 20...

BÁO CÁO
Về tình hình hoạt động của Trung tâm tích hợp dữ liệu

Trung tâm Công nghệ thông tin và Truyền thông báo cáo định kỳ tình hình hoạt động của Trung tâm tích hợp dữ liệu tỉnh Quý … năm …. như sau:

I. THÔNG TIN CHUNG

1. Kỳ báo cáo: Quý … năm …..

2. Điện thoại: ..... Fax: ..... Email: .....

3. Tổng băng thông Internet (trong nước/quốc tế): ..... Mbps/..... Mbps

4. Tỷ lệ khai thác hệ thống (%):

- Về đường truyền Internet: .....
- Về cung cấp các dịch vụ hạ tầng CNTT: .....

5. Tình hình nhân sự:

- Số lượng cán bộ, viên chức quản lý: .....
- Số lượng viên chức, nhân viên kỹ thuật: .....

II. CÔNG TÁC ĐÃ TRIỂN KHAI

1. Duy trì vận hành các hệ thống, ứng dụng đã triển khai

.....

(Xem chi tiết tại Phụ lục kèm theo)

2. Tiếp nhận hệ thống ứng dụng, triển khai mới, bổ sung *(nếu có)*

.....

3. Về công tác phát hiện và khắc phục sự cố

a) Tổng số lần hệ thống bị sự cố: .....

b) Chi tiết công tác xử lý sự cố:

STT	Thời điểm bị sự cố	Mô tả sự cố và nội dung khắc phục	Thời gian khắc phục (giờ)	Năng lực xử lý	
				Tự thực hiện	Nhờ chuyên gia ngoài

4. Về công tác bảo đảm an toàn, an ninh thông tin

.....

5. Công tác khác

.....

III. KẾ HOẠCH CÔNG TÁC TRIỂN KHAI

.....

.....

.....

IV. KHÓ KHĂN, VƯỚNG MẮC *(Nếu có)*

.....

.....

.....

IV. KIẾN NGHỊ, ĐỀ XUẤT

- Về tập huấn nghiệp vụ, đào tạo nâng cao trình độ chuyên môn: .....
- Về mua sắm trang thiết bị: .....
- Về các vấn đề khác:

.....

.....

.....

.....

Trung tâm Công nghệ thông tin và Truyền thông báo cáo./.

Thủ trưởng đơn vị
(Ký, đóng dấu)

Nơi nhận:
- Sở TT&TT (b/c);
- Lưu: VT, P.QLTTTHDL.

PHỤ LỤC:

Thống kê các website/ ứng dụng của cơ quan nhà nước lưu ký tại Trung tâm tích hợp dữ liệu tỉnh

(Kèm theo Báo cáo số /BC-TTCNTT&TT ngày ...../..... /20.....
của Trung tâm Công nghệ thông tin và Truyền thông)

STT	Đơn vị chủ quản	Tên website/ ứng dụng	Ghi chú
I. Danh sách các website cơ quan nhà nước			
II. Danh sách các ứng dụng dịch vụ hành chính công			

Mẫu số 04

Tên cơ quan:	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số:	*....., ngày ..... tháng ..... năm 20....*

ĐỀ NGHỊ CUNG CẤP DỊCH VỤ TRUNG TÂM TÍCH HỢP DỮ LIỆU

Kính gửi:

- Sở Thông tin và Truyền thông;
- Trung tâm Công nghệ thông tin và Truyền thông.

A. Thông tin chung

Tên cơ quan: .....

Địa chỉ: .....

Điện thoại: ..... Fax: .....

Đầu mối liên hệ (Tên cán bộ, địa chỉ email, số điện thoại): .....

.....

B. Phần đề nghị

Chúng tôi đề nghị được sử dụng dịch vụ của Trung tâm tích hợp dữ liệu tỉnh như sau:

1. Tên dịch vụ: .....

2. Mục đích: .....

.....

3. Thời gian sử dụng:

.....

4. Các yêu cầu kỹ thuật cụ thể khác: .....

.....

.....

Chúng tôi cam kết tuân thủ các quy định về quản lý, vận hành và khai thác Trung tâm tích hợp dữ liệu tỉnh./.

Thủ trưởng đơn vị
(Ký, đóng dấu)

Mẫu số 05

Tên Cơ quan
.....
Số

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU YÊU CẦU

Về việc đưa thiết bị vào/ra Trung tâm Tích hợp dữ liệu
Số: ...../20....

I. Thông tin chung của đơn vị yêu cầu

1. Tên cơ quan: .....
2. Họ và tên lãnh đạo: .....
3. Chức vụ: ..... Điện thoại:.....Email: .....
4. Tên công việc yêu cầu:

4.1 Vị trí

☐ Phòng NOC ☐ Phòng server
☐ Phòng MAN ☐ Phòng UPS
☐ Phòng Staging ☐ .....

4.2 Nâng cấp, bảo trì thiết bị

Máy chủ : ☐ Mạng : ☐
ACCU : ☐ Đường truyền : ☐
UPS : ☐ Thiết bị khác : ☐

4.3 Lắp thiết bị mới

Máy chủ : ☐ Mạng : ☐
ACCU : ☐ Đường truyền : ☐
UPS : ☐ Thiết bị khác : ☐

4.4 Di dời thiết bị

Máy chủ : ☐ Mạng : ☐
ACCU : ☐ Đường truyền : ☐
UPS : ☐ Thiết bị khác : ☐

5.5 Công việc khác

Mô tả chi tiết:
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
Thời gian thực hiện:
Từ ... giờ … đến … giờ … ngày …../...../20.....
Tên người thực hiện:
.....
.....
Chữ ký người thứ 1 Chữ ký người thứ 2

.....
.....
.....

II. Thông tin của Trung tâm THDL

1. Họ tên cán bộ phân công giám sát: .....

2. Tình trạng công việc sau khi xử lý:

2.1 Hoàn thành: Có o Không o

2.2 Ảnh hưởng đến HT khác: Có o Không o

2.3 Kiểm tra vệ sinh: Có o Không o

2.4 Tình trạng của các hệ thống khác có bình thường:

Có o Không o

2.5 Đề nghị khác: Có o Không o

Mô tả chi tiết:

.....

.....

.....

.....

.....

.....

.....

Thời gian ra khỏi Trung tâm tích hợp dữ liệu lúc: ..... giờ ....., ngày ...../...../20.....

Chữ ký người giám sát thứ 1 **Chữ ký người giám sát thứ 2**

Quảng Ninh, ngày ..... tháng ..... năm 20.....

Xác nhận của đơn vị yêu cầu *(ký, ghi rõ họ tên)*

Xác nhận của CB Quản lý DC *(ký, ghi rõ họ tên)*

Xác nhận của BGĐ *(ký, ghi rõ họ tên)*

Mẫu số 06

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN BẢN ĐƯA THIẾT BỊ VÀO/RA TRUNG TÂM THDL

Hôm nay, vào lúc giờ, ngày tháng năm 20 , tại Trung tâm THDL, Tầng 4, tòa nhà VNPT, chúng tôi gồm có:

I. Đại diện Phòng Quản lý Trung tâm THDL

1. Ông: ..... Chức vụ: .....

2. Ông: ..... Chức vụ: .....

II. Đại diện đơn vị (đưa thiết bị vào/ra Trung tâm THDL)

1. Ông: ..... Chức vụ: .....

2. Ông: ..... Chức vụ: .....

Chúng tôi cùng ký vào biên bản xác nhận ..... mang thiết bị vào/ra Trung tâm THDL với các nội dung như sau:

1. Các thông số kỹ thuật của thiết bị đưa vào/ra

STT	Tên thiết bị	ĐVT	Số lượng	Mã số	Ghi chú
1					
2					
3					

2. Thông tin hạ tầng

- Vị trí lắp đặt: Tủ: ..... Phòng: .....
- Nguồn điện: .....

3. Thông tin khác

.....

.....

.....

Biên bản được lập thành 02 bản, mỗi bên giữ 01 bản có giá trị như nhau./.

Đại diện Phòng QLTTTHDL

(ký, ghi rõ họ tên)

Đại diện đơn vị đưa thiết bị vào/ra Trung tâm THDL

(ký, ghi rõ họ tên)

Mẫu số 07

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN BẢN BÀN GIAO

Hôm nay, vào lúc giờ phút, ngày tháng năm 20 , tại Trung tâm THDL, Tầng 4, tòa nhà VNPT, chúng tôi gồm có:

I. Bên giao

Ông/bà: ..... Chức vụ: .....

Cơ quan/phòng/ban: .....

Địa chỉ: .....

Điện thoại:..... Email: .....

II. Bên nhận

Ông/bà: ..... Chức vụ: .....

Cơ quan/phòng/ban: .....

Địa chỉ: .....

Điện thoại: ..... Email: .....

Chúng tôi cùng ký vào biên bản xác nhận việc bàn giao tài khoản quản trị, vận hành hệ thống bao gồm các quyền hạn sau đây:

STT	Tên hệ thống	Quyền hạn quản trị	Ghi chú
1			
2			
3			

Biên bản được lập thành 02 bản, mỗi bên giữ 01 bản có giá trị như nhau./.

Bên giao
(ký, ghi rõ họ tên)

Bên nhận
(ký, ghi rõ họ tên)

Mẫu số 08

Tên cơ quan:	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số:	*....., ngày ..... tháng ..... năm 20....*

ĐỀ NGHỊ
Về việc khắc phục sự cố .....

Kính gửi:
- Sở Thông tin và Truyền thông;
- Trung tâm Công nghệ thông tin và Truyền thông.

A. Thông tin chung

- Tên cơ quan: .....
- Địa chỉ: .....
- Điện thoại: ..... Fax: .....
- Người liên hệ (Họ tên, địa chỉ email, số điện thoại): .....

.....

B. Thông tin sự cố

1. Mô tả sơ bộ về sự cố:

.....

.....

.....

.....

.....

2. Thời gian xảy ra sự cố:.....

3. Hệ thống xảy ra sự cố (*dịch vụ xảy ra sự cố: phần mềm, email, chat,....*) .....

.....

4. Các biện pháp phòng vệ: .....

5. Yêu cầu khắc phục sự cố:.....

.....

.....

.....

.....

Chúng tôi cam đoan việc báo cáo sự cố trên là hoàn toàn đúng sự thật. Đề nghị quý cơ quan hỗ trợ khắc phục sự cố./.

Thủ trưởng đơn vị
(Ký, ghi rõ họ tên, đóng dấu)