ỦY BAN NHÂN DÂN TỈNH LONG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 55/2021/QĐ-UBND	*Long An, ngày 20 tháng 12 năm 2021*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu tỉnh Long An

ỦY BAN NHÂN DÂN TỈNH LONG AN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật Sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

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

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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 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 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;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 2733/TTr-STTTT ngày 15/12/2021; ý kiến thẩm tra của Sở Tư pháp tại Công văn số 2666/STP-XDKTVB ngày 01/12/2021.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu tỉnh Long An.

Điều 2. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố và các cơ quan, đơn vị có liên quan tổ chức thực hiện quyết định này.

Quyết định này có hiệu lực thi hành kể từ ngày 31/12/2021.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông (b/c);
- Cục Kiểm tra VBQPPL – Bộ Tư pháp;
- TT.TU; TT.HĐND tỉnh (b/c);
- CT, các PCT UBND tỉnh;
- CVP, các PCVP;
- Trung tâm PVHCC tỉnh (đăng công báo);
- Phòng VHXH;
- Lưu: VT, lvt.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Văn Út

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

QUY CHẾ
Quản lý, vận hành và khai thác Trung tâm dữ liệu tỉnh Long An

(Kèm theo Quyết định số 55 /2021/QĐ-UBND ngày 20 /12/2021 của UBND tỉnh Long An)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định việc quản lý, vận hành và khai thác Trung tâm dữ liệu tỉnh Long An *(gọi tắt là Trung tâm dữ liệu)*.

2. Đối tượng áp dụng

Quy chế này áp dụng đối với cơ quan hành chính nhà nước, đơn vị sự nghiệp công lập trên địa bàn tỉnh Long An; các tổ chức chính trị - xã hội, tổ chức, cá nhân có liên quan tham gia quản lý, vận hành, khai thác Trung tâm dữ liệu.

Điều 2. Giải thích từ ngữ

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

1. Phần mềm dùng chung: là các hệ thống nền tảng, phần mềm *(hệ phần mềm)* ứng dụng sử dụng dùng chung, đồng bộ cho các cơ quan, đơn vị và người sử dụng được UBND tỉnh thống nhất triển khai đưa vào hoạt động tại Trung tâm dữ liệu.

2. Mạng diện rộng *(gọi tắt là mạng WAN)*: là mạng máy tính được thiết lập bằng việc kết nối giữa Trung tâm dữ liệu và 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 với mạng của Chính phủ khi có yêu cầu.

3. Mạng truyền số liệu chuyên dùng *(gọi tắt là mạng TSLCD)*: là hệ thống thông tin quan trọng quốc gia, được sử dụng trong hoạt động truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

4. Hạ tầng kỹ thuật: là tập hợp thiết bị công nghệ thông tin (thiết bị định tuyến, thiết bị chuyển mạch, thiết bị lưu trữ dữ liệu, các thiết bị giám sát, bảo mật, máy chủ, máy trạm), thiết bị điện (điều hòa chính xác, tủ điện, chống sét, máng cáp điện), thiết bị phòng cháy, chữa cháy, thiết bị viễn thông, thiết bị ngoại vi, mạng nội bộ, mạng WAN, mạng TSLCD và các thiết bị kỹ thuật chuyên dùng khác.

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

6. Cơ quan chủ quản Trung tâm dữ liệu: UBND tỉnh Long An.

7. Cơ quan chịu trách nhiệm quản lý Trung tâm dữ liệu *(gọi tắt là Đơn vị quản lý)*: Sở Thông tin và Truyền thông.

8. Đơn vị trực tiếp vận hành Trung tâm dữ liệu *(gọi tắt là Đơn vị vận hành)*: Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông.

Điều 3. Chức năng của Trung tâm dữ liệu

Trung tâm dữ liệu có chức năng lưu trữ dữ liệu lớn, hệ thống bảo mật an toàn dữ liệu, hệ thống phụ trợ, mạng WAN, mạng TSLCD, các hệ thống phần mềm ứng dụng dùng chung, phần mềm ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành của các cơ quan, đơn vị và hệ thống thông tin khác trên địa bàn tỉnh.

Điều 4. Hạ tầng kỹ thuật của Trung tâm dữ liệu

Hạ tầng kỹ thuật của Trung tâm dữ liệu được chia thành các thành phần sau:

1. Đường truyền: Trung tâm dữ liệu sử dụng mạng TSLCD để kết nối hệ thống mạng diện rộng của tỉnh, được lựa chọn chính để truyền dẫn, trao đổi dữ liệu, các giao dịch hành chính, khai thác sử dụng các hệ thống thông tin dùng chung trên môi trường mạng của các cơ quan nhà nước và sử dụng đường truyền dự phòng (qua internet) khi đường truyền chính bị sự cố.

2. Hệ thống mạng và bảo mật: hệ thống mạng được chia thành nhiều vùng khác nhau, mỗi vùng được thiết lập các chính sách an toàn và truy cập riêng phục vụ cho các mục đích khác nhau. Hệ thống bảo mật bao gồm các thiết bị tường lửa cho lớp mạng vòng ngoài, lớp mạng vòng trong và lớp ứng dụng, thiết bị phòng chống xâm nhập trái phép được thiết kế đảm bảo an toàn cho các kết nối từ Trung tâm dữ liệu kết nối vào và ra hệ thống khác. Các máy chủ và máy chủ ảo được cài phần mềm diệt virus có bản quyền, các thiết bị khi kết nối với hệ thống máy chủ tại Trung tâm dữ liệu được quét và kiểm tra đảm bảo an toàn trước khi kết nối với hệ thống.

3. Hệ thống giám sát an toàn thông tin: được thiết kế nhằm thu thập và phân tích nhật ký, các sự kiện từ các máy chủ, thiết bị mạng và được lưu trữ tập trung, cho phép phân tích và báo cáo về các sự kiện an toàn thông tin mạng, giúp phát hiện sớm các cuộc tấn công mạng, lây nhiễm mã độc. Dữ liệu hệ thống

giám sát an toàn thông tin được cập nhật, chia sẻ với Trung tâm Giám sát không gian mạng quốc gia (NCSC).

4. Tài nguyên địa chỉ mạng IPv4, IPv6 và số hiệu mạng ASN độc lập: sử dụng dãy địa chỉ mạng IPv4, IPv6 được Bộ Thông tin và Truyền thông quy hoạch cấp cho cơ quan nhà nước và được phân hoạch đảm bảo tính hiệu quả và dự phòng. Đáp ứng yêu cầu về chuyển đổi từ IPv4 sang IPv6 phù hợp với lộ trình của quốc gia về IPv6.

5. Hệ thống máy chủ: bao gồm các hệ thống máy chủ đã được đầu tư phục vụ cho Chính quyền điện tử và các ứng dụng chuyên ngành với khả năng sẵn sàng cho việc mở rộng 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 dùng chung, ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác.

6. Hệ thống hội nghị truyền hình: bao gồm hệ thống thiết bị điều khiển đa điểm, quản lý cuộc gọi đã được đầu tư phục vụ cho họp trực tuyến từ tỉnh đến cấp huyện, cấp xã và khả năng sẵn sàng cho việc mở rộng trong tương lai.

7. Hệ thống lưu trữ: bao gồm thiết bị lưu trữ tập trung có năng lực xử lý lưu trữ ở mức cao, khả năng lưu trữ lớn và thiết bị sao lưu, phục hồi dữ liệu. Hệ thống được thiết kế bảo đảm khả năng mở rộng dung lượng lưu trữ trong tương lai.

8. Hệ thống phụ trợ: bao gồm hệ thống điện, điều hòa, thiết bị lưu điện, máy phát điện, sàn nâng, hệ thống phòng cháy, chữa cháy, camera an ninh, khóa điện tử... được thiết kế tương tự theo tiêu chuẩn TIA 942 - TIER 3 (tiêu chuẩn quốc tế về Trung tâm dữ liệu), bảo đảm các thiết bị luôn được hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

Điều 5. Cơ sở dữ liệu và phần mềm ứng dụng của Trung tâm dữ liệu

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

2. Các phần mềm ứng dụng dùng chung, phần mềm ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác phục vụ cho việc triển khai ứng dụng công nghệ thông tin cho các cơ quan nhà nước, tổ chức chính trị - xã hội, bao gồm: Nền tảng kết nối, chia sẻ dữ liệu tỉnh (LGSP); Hệ thống Thư điện tử tỉnh; Hệ thống Quản lý văn bản và điều hành; Hệ thống thông tin Một cửa điện tử; Hệ thống phần mềm Quản lý cán bộ công chức, viên chức tỉnh; Hệ thống phần mềm Kho cơ sở dữ liệu dùng chung của tỉnh; Hệ thống Hội nghị trực tuyến mềm; Nền tảng, dịch vụ đô thị thông minh của tỉnh và các ứng dụng dùng riêng, ứng dụng chuyên ngành của các cơ quan nhà nước trong tỉnh.

3. Căn cứ vào nhu cầu thực tế, UBND tỉnh chỉ đạo bổ sung các ứng dụng khác được vận hành tại Trung tâm dữ liệu.

Điều 6. Nguyên tắc quản lý, vận hành và khai thác Trung tâm dữ liệu

1. Bảo đảm các yêu cầu về an toàn, an ninh mạng theo Luật An toàn thông tin mạng, Luật An ninh mạng và các văn bản pháp lý hiện hành.

2. Thiết lập, vận hành hệ thống quản lý An toàn thông tin (ISMS) đảm bảo tuân thủ theo tiêu chuẩn quốc tế ISO/IEC 27001:2013 về quản lý bảo mật thông tin.

3. Duy trì, vận hành, nâng cấp Trung tâm dữ liệu (cơ sở hạ tầng, hệ thống thông tin, cơ sở dữ liệu chuyên ngành) phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật do Nhà nước quy định và phù hợp với Kiến trúc Chính quyền điện tử tỉnh. Đồng thời, tuân thủ các quy định hiện hành về bảo đảm an toàn, an ninh mạng.

4. Quản lý, kết nối và chia sẻ dữ liệu số không chứa thông tin bí mật nhà nước của Trung tâm dữ liệu phải tuân thủ theo Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ quy định về Quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước.

5. Việc chia sẻ dữ liệu số chứa thông tin thuộc phạm vi bí mật nhà nước được thực hiện theo Luật Bảo vệ bí mật nhà nước và các văn bản pháp luật hiện hành. 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.

6. Các tổ chức, cá nhân sử dụng các hệ thống thông tin của Trung tâm dữ liệu phải tuân thủ các quy định chung về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình.

7. Đơn vị quản lý Trung tâm dữ liệu chịu trách nhiệm quản lý tài sản hoặc phân cấp quản lý tài sản theo quy định hiện hành về quản lý, sử dụng tài sản công.

8. Đơn vị vận hành Trung tâm dữ liệu chịu trách nhiệm quản lý tài sản theo phân cấp, quản trị, vận hành đảm bảo khai thác an toàn hiệu quả hạ tầng kỹ thuật Trung tâm dữ liệu hiện có.

9. Ngân sách nhà nước hàng năm bảo đảm cho công tác duy trì, quản lý, vận hành và bảo trì, bảo dưỡng, thay thế các thiết bị hỏng hóc, bổ sung bản quyền (license) các thiết bị, phần mềm tại Trung tâm dữ liệu đầy đủ, kịp thời để phục vụ nhiệm vụ chung.

Chương II
QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU

Điều 7. Quy định làm việc, chế độ vào, ra Trung tâm dữ liệu

1. Quy định đối với quản trị viên hệ thống

a) Trong quá trình làm việc tại Trung tâm dữ liệu phải tuân thủ nghiêm ngặt theo các quy trình, quy định làm việc, chế độ vào, ra đã được đơn vị vận hành phê duyệt.

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

c) 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...) vào bên trong Trung tâm dữ liệu.

2. Quy định đối với tổ chức, cá nhân đến làm việc tại Trung tâm dữ liệu

a) Yêu cầu:

- Tuân thủ nghiêm ngặt theo các quy trình, quy định làm việc, chế độ vào, ra tại Trung tâm dữ liệu.

- 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 dữ liệu, trừ các yêu cầu tác nghiệp đặc biệt của các cơ quan chức năng có thẩm quyền theo luật định.

b) Các tổ chức, cá nhân đến đăng ký làm việc, tham quan phải cung cấp giấy giới thiệu của cơ quan, đơn vị hoặc văn bản đề nghị làm việc tại Trung tâm dữ liệu; danh sách những người tham quan (có thông tin về số CMND/CCCD hoặc Hộ chiếu kèm theo) và tuân thủ theo các quy định của đơn vị quản lý Trung tâm dữ liệu.

Điều 8. Quy định về an toàn hoạt động

1. Trung tâm dữ liệu phải có nội quy vận hành và được giám sát thường xuyên thông qua hệ thống kiểm soát vào, ra. Không đặt các thiết bị hỏng, thiết bị chờ thanh lý, các thiết bị của cá nhân, các vật dụng dễ cháy nổ… vào Trung tâm dữ liệu.

2. Trung tâm dữ liệu phải được trang bị hệ thống quản lý môi trường (nhiệt độ, độ ẩm), hệ thống điều hòa chính xác bảo đảm độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị, hạ tầng kỹ thuật hoạt động ổn định, được bảo trì, bảo dưỡng ít nhất 04 lần/năm hoặc theo khuyến cáo của nhà sản xuất.

3. Trung tâm dữ liệu phải được trang bị hệ thống lưu điện dự phòng (UPS) cung cấp điện cho các thiết bị, hạ tầng kỹ thuật, được bảo trì, bảo dưỡng ít nhất 02 lần/năm và máy phát điện dự phòng để bảo đảm cho hệ thống hoạt động liên tục, ổn định kể cả khi có sự cố về nguồn điện lưới, được bảo trì, bảo dưỡng ít nhất 02 lần/năm, thay thế thiết bị hư hỏng, cấp phiếu nhiên liệu kịp thời.

4. Hệ thống phòng cháy, chữa cháy phải đáp ứng theo tiêu chuẩn quy định, vừa đảm bảo an toàn tuyệt đối cho toàn hệ thống thiết bị, vừa đảm bảo an

toàn cho người quản trị tại Trung tâm dữ liệu. Hệ thống được bảo trì, bảo dưỡng ít nhất 01 lần/năm.

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

6. Hệ thống quản lý vào, ra *(Access Control)* hoạt động 24/24 giờ nhằm đảm bảo an ninh, chính xác và linh hoạt cho Trung tâm dữ liệu.

Điều 9. Quy định về an toàn, an ninh mạng cho hệ thống

1. Các hệ thống thông tin tại Trung tâm dữ liệu phải đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật về đảm bảo an toàn thông tin cấp độ 3 theo Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông và Quyết định phê duyệt cấp độ an toàn thông tin đối với Trung tâm dữ liệu tỉnh Long An của cơ quan nhà nước có thẩm quyền.

2. Theo dõi, kiểm tra, xử lý các cảnh báo của hệ thống giám sát an toàn thông tin của Trung tâm dữ liệu, ghi nhận đầy đủ các sự kiện, biện pháp xử lý. Thực hiện rà soát, đánh giá theo hướng dẫn nghiệp vụ của Cục An toàn thông tin, Trung tâm Giám sát không gian mạng quốc gia (NCSC) và Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC).

3. Các hệ thống thông tin từ cấp độ 3 trở lên thuộc Trung tâm dữ liệu phải được kiểm tra, đánh giá an toàn thông tin theo định kỳ ít nhất 01 lần/năm bởi đơn vị vận hành hoặc doanh nghiệp, tổ chức độc lập thực hiện việc kiểm tra, đánh giá và tổng hợp, báo cáo theo định kỳ.

4. Thường xuyên kiểm tra kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia: Trung tâm giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

5. Hệ thống bảo mật được thiết lập cấu hình, cập nhật tự động các dấu hiệu, phương thức tấn công mới để hệ thống ở trạng thái hoạt động tốt nhất nhằm ngăn chặn, xử lý hiệu quả dấu hiệu tấn công mạng, bảo đảm an toàn, bảo mật cho Trung tâm dữ liệu.

6. Tất cả các máy chủ vận hành tại Trung tâm dữ liệu phải được thiết lập cập nhật bản vá tự động hoặc thủ công đảm bảo trạng thái hoạt động tốt nhất.

Điều 10. Quy định về an toàn hệ thống mạng

1. Hệ thống mạng phải bảo đảm

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

b) Thường xuyên theo dõi, phát hiện, xử lý kịp thời những cảnh báo của hệ thống kiểm soát truy cập mạng, bảo đảm các quy định về an toàn, an ninh thông tin và các chính sách bảo mật.

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

d) Đường truyền Internet cho Trung tâm dữ liệu phải kết nối từ 02 nhà cung cấp dịch vụ khác nhau, thực hiện kết nối đa hướng (multi-home) với tài nguyên địa chỉ mạng IPv4, IPv6 và ASN độc lập để đảm bảo dự phòng và tính sẵn sàng cho toàn hệ thống.

đ) Các kết nối Internet, kết nối mạng TSLCD cấp I, cấp II phải có các giải pháp, chính sách bảo mật bảo đảm hệ thống tránh bị xâm nhập, tấn công mạng, lây nhiễm virus, phần mềm độc hại từ bên ngoài; ngăn chặn, không để phát tán virus, phần mềm độc hại từ các thiết bị ngoại vi khác. Các đơn vị sử dụng mạng TSLCD kết nối vào Trung tâm dữ liệu phải tuân thủ các quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng TSLCD theo Thông tư số 12/2019/TT-BTTTT ngày 05/11/2019 của Bộ Thông tin và Truyền thông, Quyết định số 07/2019/QĐ-UBND ngày 30/01/2019 của UBND tỉnh và các quy định hiện hành.

e) Mạng không dây (wifi) tại Trung tâm dữ liệu là đường truyền riêng biệt để quản trị viên kết nối quản lý hệ thống, quản trị viên không được tiết lộ thông tin kết nối cho bất kỳ cá nhân hay tổ chức đến làm việc, tham quan Trung tâm dữ liệu tỉnh.

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

Điều 11. Quy định quản lý thiết bị

1. Thiết bị công nghệ thông tin đặt tại Trung tâm dữ liệu phải được đặt tên và dán nhãn theo quy định. Định kỳ hàng năm thực hiện kiểm kê, khấu hao tài sản theo quy định.

2. Đơn vị quản lý thực hiện bàn giao tài sản theo quy định để đơn vị vận hành quản trị, vận hành khai thác phục vụ nhiệm vụ chung của tỉnh. Đơn vị vận hành phải thực hiện tổng hợp tình hình sử dụng thiết bị tại Trung tâm dữ liệu định kỳ 06 tháng/lần hoặc khi có yêu cầu và báo cáo đơn vị quản lý theo quy định.

3. Việc sửa chữa, nâng cấp, thay thế thiết bị hỏng được đơn vị vận hành báo cáo đề xuất bằng văn bản cho đơn vị quản lý. Đơn vị quản lý có biện pháp xử lý, khắc phục kịp thời dựa trên nguồn ngân sách nhà nước cấp hàng năm. Thiết bị được thay thế, nâng cấp phải tuân theo các tiêu chuẩn về thiết bị cho Trung tâm dữ liệu.

Điều 12. Quy định quản lý kiểm soát truy cập và xác thực

1. Các nguyên tắc kiểm soát truy cập

a) Tất cả các thông tin quan trọng trong hệ thống phải được bảo vệ khỏi truy cập trái phép thông qua chính sách kiểm soát truy cập.

b) Quyền truy cập được thiết lập dựa trên yêu cầu nghiệp vụ và yêu cầu về an toàn thông tin của Trung tâm dữ liệu.

c) Quyền truy cập phải được rà soát, định kỳ.

d) Quyền truy cập phải được loại bỏ khi không còn nhu cầu sử dụng.

đ) Ghi nhật ký, theo dõi giám sát người sử dụng truy cập vào hệ thống thông tin quan trọng.

2. Cấp phát quyền truy cập từ xa hoặc truy cập trực tiếp để sử dụng và khai thác ứng dụng, tài nguyên của Trung tâm dữ liệu phải đảm bảo chặt chẽ, đúng mục đích sử dụng. Khuyến khích sử dụng xác thực 02 lớp (qua tin nhắn, token) để đảm bảo an toàn thông tin mạng. Mỗi người dùng, quản trị viên hệ thống chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

3. Lãnh đạo đơn vị vận hành chịu trách nhiệm kiểm tra và vô hiệu tài khoản của quản trị viên hệ thống trên hệ thống trong vòng 01 giờ sau khi quản trị viên hệ thống không còn làm việc.

4. Giới hạn số lần đăng nhập không thành công vào hệ thống là 05 lần. Sau 05 lần không đăng nhập thành công, tài khoản sẽ bị khóa trong 30 phút.

5. Quản trị viên hệ thống có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc hành vi vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập các tài khoản vi phạm.

Điều 13. Quy định quản lý chính sách thiết lập và quản lý mật khẩu

1. Lãnh đạo đơn vị vận hành 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 trị viên hệ thống có biên bản kèm theo, lưu vào nơi an toàn. Các tài liệu liên quan đến mật khẩu được bảo quản ở chế độ "mật".

2. Sau khi tiếp nhận, quản trị viên hệ thống phải thực hiện đổi tài khoản, mật khẩu trong vòng 01 ngày. Việc đổi mật khẩu cán bộ quản trị viên hệ thống phải tuân thủ theo quy định, hướng dẫn về mật khẩu an toàn.

3. 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 người sử dụng (dùng để đăng nhập sử dụng các hệ thống thông tin dùng chung, các ứng dụng chuyên ngành): Tối thiểu là 8 ký tự.

- Đối với mật khẩu quản trị hệ thống (sử dụng cho quản trị các hệ thống mạng, bảo mật, máy chủ, ứng dụng dùng chung): 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 quản trị hệ thống phải kết hợp các loại ký tự sau: Chữ cái in thường (a, b, c), chữ cái in hoa (A, B, C), ký tự số (1, 2, 3) và các ký tự đặc biệt (!, @, #).

c) Thời gian sử dụng mật khẩu:

- Đối với mật khẩu của người sử dụng: Được thiết lập trên hệ thống định kỳ 3 tháng thay đổi một lần.

- Đối với mật khẩu của người quản trị hệ thống: Được thiết lập trên hệ thống định kỳ phải thay đổi ít nhất 03 tháng một lần.

Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn, an ninh thông tin thì lãnh đạo đơn vị vận hành Trung tâm dữ liệu quyết định việc thay đổi toàn bộ mật khẩu quản trị của Trung tâm dữ liệu.

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 tiết lộ mật khẩu của cá nhân, tổ chức; trường hợp bàn giao tài khoản truy cập ứng dụng phải có biên bản bàn giao.

- 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 bảo quản ở chế độ "mật".

Điều 14. Quy định quản lý giám sát lỗ hổng an toàn thông tin

1. Đơn vị vận hành thực hiện lập danh sách các nút mạng (Node), các thiết bị, các máy chủ đang quản lý trên hệ thống. Danh sách bao gồm tối thiểu các thông tin như địa chỉ IP, chức năng, hệ điều hành, phiên bản, cán bộ quản trị, vận hành.

2. Đơn vị vận hành đăng ký nhận thông tin, bản tin về bảo mật từ các hãng cung cấp hạ tầng công nghệ thông tin và dịch vụ phần mềm đã triển khai tại Trung tâm dữ liệu. Thực hiện cập nhật bản vá lỗ hổng an toàn thông tin đối với các hệ điều hành, cơ sở dữ liệu, ứng dụng, nâng cấp phiên bản đối với các thiết bị bảo mật.

3. Khi phát hiện có lỗ hổng an toàn thông tin hoặc nhận được các cảnh báo về lỗ hổng an toàn thông tin từ nhà cung cấp hoặc các tổ chức, đối tác chuyên nghiệp, đơn vị vận hành cần thông báo tới đơn vị quản lý và triển khai phương án xử lý, khắc phục.

4. Việc xử lý các lỗ hổng an toàn thông tin đối với các máy chủ, thiết bị mạng quan trọng cần phải có phân tích ảnh hưởng hoặc thử nghiệm trước khi áp dụng vào hệ thống đang hoạt động và có phương án dự phòng hoặc khôi phục lại hệ thống trong trường hợp xử lý không thành công. Quá trình xử lý được ghi

nhận đầy đủ các bước, các thao tác trong hệ thống quản lý sự kiện an toàn thông tin, được tái sử dụng nếu có lỗ hổng tương tự.

5. Đối với các lỗ hổng an toàn thông tin cần cài đặt các bản vá lỗi để xử lý, bản vá lỗi phải được tải về từ nguồn tin cậy (là trang web chính thức của nhà cung cấp) hoặc có biện pháp kiểm tra nguồn gốc của bản vá lỗi.

Điều 15. Quy định quản lý sao lưu dữ liệu

1. Tạo lập chế độ lưu trữ thông tin theo quy định với những yêu cầu sau

a) Với dữ liệu trên máy chủ, lưu trữ chuyên dụng, thực hiện sao lưu lên thiết bị sao lưu chuyên dụng.

b) Chu kỳ sao lưu: đối với máy chủ thực hiện sao lưu đầy đủ ít nhất 02 lần/tháng, sao lưu dữ liệu đầy đủ ít nhất 04 lần/tháng; chu kỳ sao lưu dữ liệu thay đổi ít nhất 01 lần/ngày. Có ít nhất 01 bản sao lưu đầy đủ gần nhất được lưu trữ trên hạ tầng thuê lưu trữ dự phòng của doanh nghiệp bên ngoài (nếu có).

c) Đối chiếu, xóa bản sao lưu: đảm bảo nguyên tắc có ít nhất 02 bản sao lưu đầy đủ gần nhất, thực hiện đối chiếu, thử nghiệm khôi phục đảm bảo bản sao lưu hoạt động bình thường khi tiến hành khôi phục.

d) Thông tin về tất cả các lần sao lưu đều được ghi rõ trong nhật ký sao lưu dữ liệu. Các thiết bị 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.

2. Đối với dữ liệu quan trọng, đơn vị vận hành đề xuất đơn vị quản lý thuê Trung tâm dữ liệu dự phòng để ngăn ngừa, bảo đảm an toàn dữ liệu của hệ thống.

Điều 16. Quy định quản lý sự cố, 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 đơn vị quản lý, 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 dữ liệu), đơn vị vận hành nhanh chóng tổ chức 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 dữ liệu), ngay sau khi phát hiện sự cố đơn vị vận hành cần tiến hành các biện pháp khắc phục tạm thời, cô lập, hạn chế thiệt hại, đánh giá ảnh hưởng, đề xuất phương án xử lý sự cố, liên hệ đơn vị giám sát, bảo vệ

chuyên nghiệp để được hướng dẫn và thực hiện thông cáo đến đơn vị quản lý để thống nhất, quyết định phương án xử lý.

c) Đối với các sự cố đặc biệt nghiêm trọng (gây ngưng trệ đến toàn bộ hoạt động của Trung tâm dữ liệu), đơn vị vận hành và cơ quan quản lý phải tiến hành các biện pháp cô lập, ngăn chặn sự cố lây lan hoặc tạm ngưng hệ thống; đánh giá ảnh hưởng của sự cố và thực hiện báo cáo ngay về UBND tỉnh, các cơ quan liên quan (Cục An toàn thông tin, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)) 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, khắc phục sự cố do đơn vị quản lý Trung tâm dữ liệu phê duyệt và ban hành theo tiêu chuẩn ISO 27001.

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.

đ) Trường hợp sự cố vượt quá khả năng tự xử lý, thông báo cho Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam phối hợp ngăn chặn, khắc phục sự cố.

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

g) 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.

h) Ghi nhận chi tiết quá trình xử lý sự cố vào hệ thống quản lý sự kiện an toàn thông tin, ưu tiên sử dụng cách xử lý sự cố có tính chất tương tự.

Điều 17. Quy định quản lý bản quyền phần mềm, ứng dụng

1. Các gói phần mềm trên thiết bị, các phần mềm, ứng dụng sử dụng tại Trung tâm dữ liệu 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 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 hoặc người có thẩm quyền đồng ý trước khi cài đặt.

3. Đơn vị vận hành theo dõi việc sử dụng bản quyền các phần mềm trên thiết bị và các phần mềm, ứng dụng tại Trung tâm dữ liệu. Lập dự toán và báo cáo đề xuất cơ quan quản lý gia hạn bản quyền, đảm bảo bản quyền được gia hạn kịp thời, liên tục cho toàn bộ hệ thống.

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

Điều 18. Quy định an toàn trong phát triển phần mềm

Hệ thống phần mềm, ứng dụng khi được phát triển và triển khai tại Trung tâm dữ liệu cần đảm bảo:

1. Các ứng dụng đều được kiểm tra dữ liệu đầu vào một cách chặt chẽ và nghiêm ngặt để giảm thiểu các lỗ hổng phổ biến đối với an toàn, an ninh ứng dụng.

2. Có cơ chế rà soát kiểm tra và thử nghiệm mô phỏng khai thác tấn công đối với tất cả những vị trí có tính năng tải tập tin (Upload File) bên trong ứng dụng.

3. Đơn vị phát triển phần mềm cần phải đảm bảo áp dụng các tiêu chuẩn, quy trình về chất lượng cũng như an toàn, an ninh thông tin tương ứng hoặc cao hơn Trung tâm dữ liệu.

4. Trước khi tiến hành chạy hay thử nghiệm phần mềm có cơ chế thực hiện kiểm tra và phát hiện các đoạn chương trình gián điệp và mã độc hại.

Điều 19. Quy định về vận hành, bảo trì, bảo dưỡng

1. Đơn vị quản lý thực hiện

a) Xây dựng và ban hành kế hoạch vận hành, bảo trì, bảo dưỡng hệ thống sử dụng nguồn ngân sách được cấp hàng năm.

b) Thực hiện đặt hàng cung cấp sản phẩm, dịch vụ công về vận hành, bảo trì, bảo dưỡng cho đơn vị vận hành theo quy định của pháp luật.

2. Yêu cầu về vận hành, bảo trì, bảo dưỡng

a) Việc thực hiện vận hành, bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến tình hình vận hành của Trung tâm dữ liệu.

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

Điều 20. Quy định về cung cấp, tiếp nhận thiết bị và phần mềm của các đơn vị tại Trung tâm dữ liệu

1. Việc triển khai các dự án, nhiệm vụ ứng dụng CNTT trên hạ tầng Trung tâm dữ liệu phải được quy định cụ thể trong thiết kế kỹ thuật được cơ quan có thẩm quyền phê duyệt.

2. Đối với các cơ quan, đơn vị có nhu cầu đặt máy chủ để triển khai các ứng dụng dùng riêng cho cơ quan, đơn vị mình trên hạ tầng Trung tâm dữ liệu: Các cơ quan, đơn vị xin chủ trương UBND tỉnh cho ý kiến triển khai; sau khi có chủ trương của UBND tỉnh đồng ý triển khai, đơn vị quản lý sẽ tiến hành thực hiện thủ tục cung cấp, tiếp nhận đặt máy chủ, cài đặt phần mềm và quản lý tài sản do cơ quan quản lý quy định.

3. Các đơn vị có thiết bị hoặc ứng dụng đặt tại Trung tâm dữ liệu chịu trách nhiệm quản trị nội dung, phần mềm của cơ quan mình đồng thời tuân thủ các nguyên tắc và đảm bảo an toàn, an ninh thông tin của hệ thống.

Điều 21. Quy định về quản lý tài liệu liên quan hoạt động của Trung tâm dữ liệu

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) 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.

đ) Tài liệu, biên bản kiểm tra, đánh giá của Trung tâm dữ liệu.

e) 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 22. Quy định kiểm tra, báo cáo định kỳ

1. Hàng tuần, quản trị viên hệ thống vận hành Trung tâm dữ liệu thực hiện báo cáo tình hình hoạt động của Trung tâm dữ liệu đến lãnh đạo đơn vị vận hành, hàng tháng đơn vị vận hành có báo cáo tình hình hoạt động đến lãnh đạo đơn vị quản lý và phòng chuyên môn.

2. Đơn vị quản lý tổ chức kiểm tra việc tuân thủ các quy định về quản lý, triển khai, vận hành và khai thác sử dụng Trung tâm dữ liệu theo các quy định tại Quy chế này tối thiểu 06 tháng một lần.

3. Các nội dung kiểm tra

a) Việc bảo đảm các điều kiện về môi trường cho hoạt động của Trung tâm dữ liệu.

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

c) Hoạt động của hệ thống máy chủ 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, 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 đơn vị vận hành tiến hành kiểm tra, tổng hợp, báo cáo đánh giá phân tích hiệu quả hoạt động của Trung tâm dữ liệu đến đơn vị 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 CÁC CƠ QUAN, TỔ CHỨC, CÁ NHÂN TRONG VIỆC QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU

Điều 23. Trách nhiệm của các cơ quan, đơn vị, người dùng

1. Sử dụng hạ tầng, phần mềm ứng dụng của Trung tâm dữ liệu theo Quy chế này và các hướng dẫn khác của đơn vị quản lý, đơn vị vận hành Trung tâm dữ liệu.

2. Tuân thủ các quy định về đảm bảo an toàn, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước; các quy định về an toàn, bảo mật thông tin, quản lý, vận hành và khai thác Trung tâm dữ liệu.

3. Cơ quan, đơn vị phân công ít nhất một công chức, viên chức có trình độ về công nghệ thông tin/an toàn thông tin hoặc am hiểu về công nghệ thông tin làm công tác quản trị hệ thống. Người này có nhiệm vụ triển khai công tác kỹ thuật quản trị đối với hệ thống mạng cục bộ tại đơn vị, tuân thủ kết nối về Trung tâm dữ liệu để thống nhất về cấu trúc hạ tầng và cấu trúc vật lý của toàn bộ hệ thống. Là đầu mối phối hợp thực hiện các nhiệm vụ ứng cứu sự cố an toàn thông tin mạng tại đơn vị.

4. Duy trì hoạt động các ứng dụng, hệ thống thông tin đồng thời chịu trách nhiệm về các nội dung, thông tin lưu trữ tại Trung tâm dữ liệu do cơ quan, đơn vị cung cấp, cập nhật phù hợp với quy định pháp luật.

5. Người dùng ở các cơ quan, đơn vị chịu trách nhiệm về thông tin tài khoản, mật khẩu đăng nhập vào hệ thống; tuân thủ quy định về mật khẩu theo Điều 13 Quy chế này. 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).

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

Điều 24. Trách nhiệm của đơn vị vận hành

1. Đơn vị vận hành chịu trách nhiệm về vận hành và khai thác có hiệu quả hoạt động của Trung tâm dữ liệu. Tuân thủ và tổ chức thực hiện các quy định liên quan theo Quy chế này.

2. Ban hành quy chế làm việc tại Trung tâm dữ liệu; xây dựng kế hoạch, bố trí cán bộ trực vận hành hệ thống Trung tâm dữ liệu đảm bảo hệ thống vận hành thông suốt, liên tục trong vòng 24 giờ/ngày, 07 ngày/tuần kể cả các ngày lễ, Tết trong năm.

3. Xây dựng và tham mưu cho đơn vị quản lý ban hành các quy trình vận hành hệ thống quản lý An toàn thông tin theo tiêu chuẩn quốc tế ISO/IEC 27001:2013.

4. Rà soát, lập hồ sơ đề xuất cấp độ đối với hệ thống thông tin tại Trung tâm dữ liệu theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của

Chính phủ, gửi về cơ quan quản lý, cơ quan có thẩm quyền thẩm định xem xét, phê duyệt.

5. 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 dữ liệu.

6. Đào tạo quản trị viên hệ thống có chuyên môn đáp ứng yêu cầu, được trang bị các kiến thức liên quan tới hoạt động của Trung tâm dữ liệu.

7. Xây dựng kế hoạch hợp tác, khai thác Trung tâm dữ liệu với các tổ chức có liên quan và triển khai các nhiệm vụ được cấp trên giao.

8. Thực hiện báo cáo định kỳ hàng tháng, quý cho đơn vị quản lý về tình hình hoạt động của Trung tâm dữ liệu và báo cáo đột xuất khi có yêu cầu.

Điều 25. Trách nhiệm của đơn vị quản lý (Sở Thông tin và Truyền thông)

1. Tham mưu UBND tỉnh thực hiện quản lý, vận hành; đầu tư, thuê nâng cấp, mở rộng Trung tâm dữ liệu đáp ứng nhu cầu cho các ứng dụng công nghệ thông tin, xây dựng chính quyền điện tử hướng tới chính quyền số và dịch vụ đô thị thông minh của tỉnh. Triển khai công tác đào tạo nâng cao trình độ, năng lực quản trị viên hệ thống có chuyên môn đáp ứng yêu cầu. Thanh tra, kiểm tra và giám sát việc vận hành, khai thác hệ thống thông tin của đơn vị vận hành Trung tâm dữ liệu.

2. Đề xuất kinh phí cho công tác vận hành, bảo trì, bảo dưỡng Trung tâm dữ liệu.

3. Hướng dẫn các cơ quan, đơn vị, tổ chức và người dùng khai thác Trung tâm dữ liệu; triển khai các giải pháp bảo đảm an toàn, an ninh thông tin đối với các hệ thống thông tin tại Trung tâm dữ liệu.

4. Định kỳ hằng năm hoặc đột xuất, thực hiện báo cáo UBND tỉnh về tình hình hoạt động, đảm bảo an toàn thông tin của Trung tâm dữ liệu.

Điều 26. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

Phối hợp với các cơ quan liên quan căn cứ khả năng cân đối ngân sách và phân cấp ngân sách tham mưu UBND tỉnh bố trí kinh phí để duy trì hoạt động, quản lý, vận hành, bảo trì, bảo dưỡng; đầu tư nâng cấp, mở rộng cho Trung tâm dữ liệu theo quy định.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 27. 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 nghiêm Quy chế này. Trong quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, các cơ quan, đơn vị, địa phương kịp thời phản ánh, đề xuất về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Văn Út