ỦY BAN NHÂN DÂN TỈNH TRÀ VINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1289 /QĐ-UBND	*Trà Vinh, ngày 29 tháng 7 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành, khai thác và đảm bảo an toàn thông tin tại Trung tâm dữ liệu tỉnh Trà Vinh

ỦY BAN NHÂN DÂN TỈNH TRÀ VINH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 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 tháng 11 năm 2019;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

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

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ 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 tháng 7 năm 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 tháng 01 năm 2013 của Bộ trưởng 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 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 23/2022/TT-BTTTT ngày 30 tháng 11 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 03/2013/TT-BTTTT ngày 22 tháng 01 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành, khai thác và đảm bảo an toàn thông tin tại Trung tâm dữ liệu tỉnh Trà Vinh.

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

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 1383/QĐ-UBND ngày 26 tháng 7 năm 2019 của Ủy ban nhân dân tỉnh ban hành Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu tỉnh Trà Vinh.

Điều 4. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc các Sở: Thông tin và Truyền thông, Tài chính; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 4;
- CT, các PCT UBND tỉnh;
- LĐVP UBND tỉnh;
- Phòng HC-QT;
- Cổng TTĐT Trà Vinh;
- Lưu: VT, Phòng CNXD. 03

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

Nguyễn Quỳnh Thiện

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

QUY CHẾ
Quản lý, vận hành, khai thác và đảm bảo an toàn thông tin tại Trung tâm dữ liệu tỉnh Trà Vinh

(Kèm theo Quyết định số 1289/QĐ-UBND ngày 29 tháng 7 năm 2024 của Ủy ban nhân dân tỉnh Trà Vinh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc quản lý, vận hành, khai thác (hạ tầng kỹ thuật công nghệ thông tin và các dịch vụ ứng dụng dùng chung) và đảm bảo an toàn thông tin tại Trung tâm dữ liệu tỉnh Trà Vinh (sau đây gọi tắt là Trung tâm dữ liệu).

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với các sở, ban, ngành tỉnh, Ủy ban nhân dân các huyện, thị xã, thành phố và các cơ quan, tổ chức, cá nhân có liên quan tham gia quản lý, vận hành, khai thác và đảm bảo an toàn thông tin tại Trung tâm dữ liệu.

Điều 3. Giải thích từ ngữ

1. Cơ quan quản lý: Sở Thông tin và Truyền thông.

2. Cơ quan vận hành: Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông.

3. Người sử dụng: là cán bộ, công chức, viên chức, cá nhân có liên quan tham gia sử dụng các dịch vụ của Trung tâm dữ liệu.

4. Trung tâm dữ liệu: là nơi tập trung hệ thống máy chủ, thiết bị mạng, thiết bị bảo mật, hệ thống lưu trữ và các phần mềm ứng dụng, cơ sở dữ liệu, hệ thống phụ trợ và mạng diện rộng của tỉnh; tuân thủ các tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông; đảm bảo hệ thống hoạt động ổn định, có tính dự phòng và kết nối, chia sẻ dữ liệu với các hệ thống thông tin khác.

5. Hệ thống thông tin: là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

6. An toàn thông tin: là các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, dịch vụ và nội dung thông tin trước các nguy cơ do thiên tai hoặc do con người gây ra. Việc bảo vệ thông tin, thiết bị mạng, tài sản 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 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.

Điều 4. Kiến trúc của Trung tâm dữ liệu

1. Phân hệ mạng và truyền dẫn: bao gồm các kết nối Internet cho phép mở rộng khi có nhu cầu. Phân hệ mạng được chia làm nhiều vùng khác nhau, mỗi vùng được thiết lập các chính sách an ninh và truy cập riêng để phục vụ cho các mục đích khác nhau.

2. Phân hệ an toàn thông tin: bao gồm các thiết bị có liên quan nhằm bảo đảm sự an toàn về thông tin cho lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu nhằm ngăn chặn xâm nhập trái phép vào các hệ thống tại Trung tâm dữ liệu. Mỗi thiết bị trong phân hệ an toàn thông tin được thiết kế có tính dự phòng và bổ sung hỗ trợ lẫn nhau.

3. Phân hệ máy chủ: bao gồm hệ thống máy chủ đã được đầu tư phục vụ cho Chính quyền điện tử, Chuyển đổi số 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,...

4. Phân hệ lưu trữ: là hệ thống lưu trữ tập trung các hệ thống thông tin, cơ sở dữ liệu của tỉnh bảo đảm cho mục đích lưu trữ, sao lưu, phục hồi dữ liệu cho toàn bộ hệ thống. Hệ thống được thiết kế bảo đảm khả năng mở rộng trong gia tăng dữ liệu trong tương lai.

5. Phân hệ các hệ thống phụ trợ: bao gồm các hệ thống phụ trợ, giúp cho Trung tâm dữ liệu hoạt động ổn định, liên tục như: hệ thống điện, máy lạnh, thiết bị lưu điện (UPS), máy phát điện, hệ thống phòng cháy chữa cháy, hệ thống chống sét, camera an ninh.

Điều 5. Mục tiêu, nguyên tắc về quản lý, vận hành, khai thác và đảm bảo an toàn thông tin tại Trung tâm dữ liệu

1. Mục tiêu: đảm bảo Trung tâm dữ liệu hoạt động ổn định, liên tục tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của hệ thống thông tin.

2. Nguyên tắc

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

b) Tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật quy định áp dụng đối với Trung tâm dữ liệu theo Thông tư số 03/2013/TT-BTTTT ngày 22 tháng 01 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu; Thông tư số 23/2022/TT-BTTTT ngày 30 tháng 11 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 03/2013/TT-BTTTT ngày 22 tháng 01 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông quy định áp dụng tiêu

chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu; Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Tiêu chuẩn quốc gia TCVN ISO/IEC 27001:2013 về Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu; Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

c) Bảo đảm các yêu cầu về an toàn thông tin theo quy định của Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015.

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

đ) Cơ quan vận hành Trung tâm dữ liệu triển khai cung cấp dịch vụ cho các cơ quan, đơn vị theo quy định của pháp luật và trên cơ sở khai thác hiệu quả hạ tầng Trung tâm dữ liệu.

e) Khi sử dụng dịch vụ tại Trung tâm dữ liệu phải tuân thủ các quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền về bảo đảm an toàn thông tin và các quy định tại Quy chế này, người sử dụng chịu trách nhiệm cho mọi hoạt động trên tài khoản truy cập của mình.

g) Việc bảo đảm an toàn thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp.

h) Kinh phí ngân sách Nhà nước thường xuyên hàng năm bảo đảm cho công tác quản lý, vận hành, khai thác và đảm bảo an toàn thông tin tại Trung tâm dữ liệu.

Điều 6. Bảo đảm nguồn nhân lực tại Trung tâm dữ liệu

1. Viên chức được tuyển dụng vào vị trí làm việc về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin phù hợp với vị trí tuyển dụng.

2. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho viên chức vận hành.

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

Điều 7. Quy định chung về vận hành Trung tâm dữ liệu

1. Đảm bảo thiết bị phần cứng, phần mềm ứng dụng, hệ thống mạng, các hệ thống phụ trợ tại Trung tâm dữ liệu được hoạt động ổn định liên tục 24

giờ/ngày và 7 ngày/tuần.

2. Việc quản lý, vận hành các phân hệ tại Trung tâm dữ liệu phải thực hiện trong phạm vi, trách nhiệm được quy định; phải bảo đảm nguyên tắc bảo mật, không được phép cung cấp thông tin hệ thống ra bên ngoài khi chưa được sự cho phép của cơ quan quản lý.

3. Việc khai thác, cung cấp dịch vụ tại Trung tâm dữ liệu phải tuân thủ theo các nội quy, quy trình, quy định tại Trung tâm dữ liệu.

4. Việc cài đặt, nâng cấp các phân hệ tại Trung tâm dữ liệu phải được sự cho phép của cơ quan quản lý.

5. Chỉ những viên chức được giao nhiệm vụ trực tiếp quản lý, vận hành hệ thống mới được phép ra/vào Trung tâm dữ liệu. Trong các trường hợp đặc biệt như có đoàn công tác hoặc bảo trì, bảo dưỡng, sửa chữa thiết bị cần thiết vào trong Trung tâm dữ liệu thì phải được sự đồng ý của lãnh đạo cơ quan vận hành. Không được tự ý ghi âm, ghi hình khi vào bên trong Trung tâm dữ liệu, trừ trường hợp có sự đồng ý của lãnh đạo cơ quan quản lý hoặc lãnh đạo cơ quan vận hành Trung tâm dữ liệu.

6. Thực hiện vô hiệu hóa tất cả các quyền ra, vào Trung tâm dữ liệu; các quyền truy cập vào tài nguyên, quản trị hệ thống sau khi viên chức không còn thực hiện nhiệm vụ tại Trung tâm dữ liệu.

Điều 8. Quy định về bảo trì, bảo dưỡng

1. Việc bảo trì bảo dưỡng phải được thực hiện định kỳ hàng năm, gồm các phân hệ trong kiến trúc của Trung tâm dữ liệu quy định tại Điều 4 của Quy chế này.

2. Hàng năm, cơ quan vận hành Trung tâm dữ liệu lập dự toán kinh phí, kế hoạch, danh mục các thiết bị, hệ thống cần thuê dịch vụ sửa chữa, bảo trì, bảo dưỡng và tổ chức thực hiện theo quy định pháp luật hiện hành.

3. Yêu cầu về bảo trì, bảo dưỡng

a) Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn, ảnh hưởng đến quá trình hoạt động và cung cấp dịch vụ của Trung tâm dữ liệu.

b) Quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kế hoạch được phê duyệt.

Điều 9. Quy định về quản lý hồ sơ

1. Danh sách các loại hồ sơ lưu trữ

a) Các quy định 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).

d) Hồ sơ lưu các dịch vụ cung cấp.

đ) Bảng thống kê danh sách thiết bị; danh sách các thiết bị hỏng, hết khấu

hao sử dụng chờ thanh lý; biên bản bàn giao thiết bị.

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

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.

Điều 10. Quy định về an toàn hoạt động

1. Bảo đảm cho máy chủ, thiết bị, hệ thống giám sát hoạt động liên tục, ổn định và an toàn.

2. Trung tâm dữ liệu chỉ được đặt các thiết bị đang hoạt động phục vụ vận hành hệ thống, tuyệt đối không đặt các thiết bị khác: thiết bị hỏng, thiết bị chờ thanh lý, tài liệu, vật tư, các vật dụng dễ cháy nổ,...

3. Trung tâm dữ liệu phải đảm bảo vệ sinh công nghiệp: 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 công nghệ thông tin.

4. Hệ thống phòng cháy, chữa cháy phải được cấp giấy phép của Phòng Cảnh sát Phòng cháy, chữa cháy và Cứu nạn cứu hộ, Công an tỉnh Trà Vinh.

5. Hệ thống điện phải được trang bị, thiết bị tích điện, máy phát điện dự phòng để đảm bảo cho hệ thống hoạt động trong thời gian nguồn điện chính gặp sự cố.

6. Hệ thống điều hoà phải bảo đảm nhiệt độ cho phòng máy chủ theo đúng tiêu chuẩn quy định đối với Trung tâm dữ liệu.

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

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU

Điều 11. Quản lý an toàn mạng

1. Chỉ cho phép truy cập, cấu hình thiết bị hệ thống từ vùng mạng quản trị. Khi có yêu cầu cần truy cập, cấu hình thiết bị hệ thống từ bên ngoài hệ thống phải thông qua kết nối VPN.

2. Phân quyền truy cập từ bên ngoài vào hệ thống thông qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống dành cho viên chức quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng.

3. Mỗi viên chức quản trị, vận hành Trung tâm dữ liệu được cấp một tài khoản VPN và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

4. Viên chức quản lý hệ thống chịu trách nhiệm kiểm tra và loại bỏ tài

khoản của viên chức trên các hệ thống sau khi viên chức đó không còn làm việc tại cơ quan vận hành Trung tâm dữ liệu.

5. 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.

6. Viên chức vận hành hệ thống có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho viên chức quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

7. Toàn bộ thao tác thay đổi, thiết lập cấu hình thiết bị hệ thống phải được ghi nhật ký hệ thống.

8. Sơ đồ thiết kế hệ thống về logic và vật lý phải được cập nhật khi có sự thay đổi về thiết kế và được sao lưu dự phòng theo từng phiên bản khác nhau.

Điều 12. Quản lý an toàn máy chủ và ứng dụng

1. Truy cập mạng của máy chủ

a) Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Tường lửa hệ thống và tường lửa máy chủ phải được thiết lập để quản lý kết nối mạng từ các địa chỉ bên ngoài vào máy chủ theo ứng dụng, dịch vụ máy chủ cung cấp và địa chỉ nguồn truy cập. Các dịch vụ khác, không sử dụng phải vô hiệu hóa và chặn kết nối từ bên ngoài.

c) Tường lửa hệ thống và tường lửa máy chủ phải được thiết lập để quản lý kết nối mạng từ máy chủ đi ra các mạng bên ngoài; chỉ mở truy cập máy chủ theo hướng đi ra đối với các dịch vụ cơ bản như HTTP, HTTPS, các kết nối khác phục vụ cập nhật hệ điều hành và các dịch vụ nghiệp vụ cụ thể mà máy chủ yêu cầu phải kết nối ra bên ngoài.

2. Truy cập, quản trị máy chủ và ứng dụng

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa máy chủ, phần mềm ứng dụng vào khai thác, sử dụng.

b) Cấp quyền quản lý truy cập máy chủ cho viên chức vận hành khi cài đặt, cập nhật hệ điều hành hoặc cài đặt, cập nhật dịch vụ trên máy chủ.

c) Các máy chủ thuộc phân vùng quản trị (MGMT), cơ sở dữ liệu (DB) không được phép truy cập internet trừ trường hợp phục vụ cập nhật bản vá hệ điều hành, phần mềm phòng chống mã độc, phiên bản phần mềm dịch vụ... Sau khi hoàn thành tiến hành ngắt kết nối đối với các máy chủ này.

d) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

đ) Chỉ cho phép truy cập, cấu hình thiết bị hệ thống từ vùng mạng quản trị. Khi có yêu cầu cần truy cập, cấu hình thiết bị hệ thống từ bên ngoài hệ thống phải thông qua kết nối VPN; kết nối VPN chỉ cho phép truy cập đến IP của máy chủ cần cấu hình, sau khi hoàn thành khóa tài khoản VPN.

3. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: thực hiện sao lưu đầy đủ mã nguồn, tập tin cấu hình, tập tin đính kèm, cơ sở dữ liệu của các ứng dụng; hệ điều hành máy chủ; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có). Dữ liệu sao lưu dự phòng phải được lưu trữ trên thiết bị và hệ thống lưu trữ độc lập.

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

a) Trước khi cài đặt hệ điều hành, dịch vụ, phần mềm trên hệ thống chính phải thực hiện cài đặt trên môi trường thử nghiệm để đánh giá mức độ an toàn, ổn định.

b) Định kỳ hàng tháng cập nhật bản vá hệ điều hành cho máy chủ.

c) Dịch vụ, phần mềm trên máy chủ ứng dụng không phục vụ hoạt động của máy chủ theo chức năng phải gỡ bỏ.

d) Xóa dữ liệu của hệ điều hành, dịch vụ, phần mềm sau khi được gỡ bỏ.

5. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống

a) Máy chủ hệ thống phải được kiểm tra, đánh giá và xử lý các điểm yếu an toàn thông tin; không còn tồn tại điểm yếu ở mức trung bình trở lên, trước khi kết nối vào hệ thống.

b) Máy chủ phải được cấu hình tối ưu và tăng cường bảo mật trước khi kết nối vào hệ thống.

c) Khi gỡ bỏ máy chủ khỏi hệ thống, toàn bộ chính sách bảo mật, cấu hình hệ thống phải được gỡ bỏ.

d) Toàn bộ dữ liệu, hệ điều hành máy chủ phải được xóa bỏ trước khi gỡ bỏ máy chủ khỏi hệ thống.

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

Điều 13. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp sao lưu dự phòng

a) Cơ quan vận hành có trách nhiệm xây dựng và triển khai thực hiện quy trình sao lưu dữ liệu dự phòng cho Trung tâm dữ liệu.

b) Dữ liệu phải được phân loại để lưu trữ theo thứ tự ưu tiên về mức độ quan trọng, sao lưu theo thời gian, loại thông tin, nơi lưu trữ. Thực hiện sao lưu đầy đủ các dữ liệu của người dùng, ứng dụng và hệ thống.

c) Dữ liệu phải được kiểm soát và đối chiếu sau khi sao lưu. Đối với các dữ liệu quan trọng, thay đổi liên tục phải thực hiện sao lưu dữ liệu hàng ngày.

2. 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.

Điều 14. Quản lý an toàn thiết bị đầu cuối

1. Thiết bị đặt tại Trung tâm dữ liệu phải được đặt tên và dán nhãn theo đúng quy định.

2. Viên chức vận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị tại Trung tâm dữ liệu hàng quý.

3. Cơ quan vận hành kịp thời đề xuất đầu tư, nâng cấp thêm thiết bị và các thiết bị phụ trợ khác trong trường hợp thiết bị hết bảo hành, bị hỏng. Thiết bị đầu cuối được trang bị phải tuân theo các tiêu chuẩn về thiết bị cho Trung tâm dữ liệu.

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

5. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

6. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 15. Quản lý phòng chống phần mềm độc hại

1. 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.

2. Các phần mềm, chương trình ứng dụng cài đặt tại Trung tâm dữ liệu phải có bản quyền sử dụng theo đúng quy định của pháp luật.

3. Chỉ được cài đặt và sử dụng các phần mềm đã mua bản quyền. Các phần mềm mã nguồn mở, phần mềm miễn phí phải được xác thực nguồn gốc và được cơ quan quản lý phê duyệt trước khi cài đặt; phải xử lý điểm yếu an toàn thông tin, cập nhật lên phiên bản mới nhất trước khi sử dụng.

4. Cơ quan vận hành tổ chức quản lý, theo dõi sử dụng các bản quyền phần mềm tại Trung tâm dữ liệu.

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

6. Kịp thời báo cáo đề xuất cơ quan quản lý mua sắm phần mềm khi sắp hết hạn.

7. Hệ thống phải được trang bị giải pháp kỹ thuật để quản lý và ngăn chặn truy cập đến các trang thông tin độc hại trên mạng.

8. Định kỳ hàng năm 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.

Điều 16. Quản lý giám sát an toàn hệ thống thông tin

1. Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, máy trạm, ứng dụng và dịch vụ có trong hệ thống.

2. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Chỉ được truy cập và quản trị hệ thống giám sát từ vùng mạng quản trị. Khi có yêu cầu cần truy cập, cấu hình, quản trị từ bên ngoài hệ thống phải thông qua kết nối VPN.

4. Loại thông tin cần được giám sát bao gồm tối thiểu các loại sau: thông tin giám sát lớp mạng, các máy chủ, các ứng dụng, cơ sở dữ liệu và thiết bị đầu cuối.

5. Lưu trữ và bảo vệ thông tin giám sát phải được lưu trữ tập trung đầy đủ các loại thông tin tại khoản 4 Điều này theo thời gian thực.

6. Toàn bộ thành phần trong hệ thống giám sát, máy chủ, thiết bị hệ thống và ứng dụng phải được đồng bộ thời gian.

7. Trung tâm điều hành an toàn thông tin mạng (SOC) thực hiện theo dõi, giám sát an toàn hệ thống thông tin 24 giờ/ngày và 7 ngày/tuần để kịp thời phát hiện và cảnh báo sự cố mất an toàn thông tin tại Trung tâm dữ liệu.

Điều 17. Quản lý điểm yếu an toàn thông tin

1. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ,...); phân loại mức độ nguy hiểm của điểm yếu, có phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Cơ quan vận hành làm đầu mối phối hợp với các đơn vị cung cấp dịch vụ (phần mềm, phần cứng) tiến hành xử lý điểm yếu an toàn thông tin tại Trung tâm dữ liệu.

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

4. Định kỳ hàng năm 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 đối với thành phần cụ thể trong hệ thống.

Điều 18. Quản lý sự cố an toàn thông tin

1. Khi phát hiện có sự cố, viên chức 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 báo cáo kịp thời cho Lãnh đạo cơ quan vận hành về tình hình sự cố để tham mưu, báo cáo lãnh đạo cơ quan quản lý chỉ đạo và có biện pháp khắc phục trong thời gian sớm nhất.

2. Tùy thuộc vào mức độ ảnh hưởng của sự cố, đánh giá và phân loại theo 02 mức: sự cố thông thường, sự cố nghiêm trọng. Từ đó lựa chọn phương án, quy trình xử lý phù hợp.

3. Đối với sự cố thông thường (không gây ảnh hưởng đến hoạt động của Trung tâm dữ liệu và người sử dụng): viên chức vận hành hệ thống phải có trách

nhiệm xử lý ngay. Sau khi xử lý xong phải báo cáo lãnh đạo cơ quan vận hành.

4. 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, cơ quan vận hành cần đánh giá ảnh hưởng của sự cố và thực hiện báo cáo về cơ quan quản lý để được hướng dẫn xử lý.

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

a) Phải tuân thủ các phương án, quy trình xử lý khắc phục sự cố do cơ quan quản lý Trung tâm dữ liệu phê duyệt và ban hành.

b) Đảm bảo tuyệt đối an toàn cho hệ thống.

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

d) 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.

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 trong vòng 24 giờ kể từ khi phát hiện sự cố.

6. Hàng năm tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

Điều 19. Quản lý an toàn người sử dụng đầu cuối

1. Quản lý truy cập, sử dụng tài nguyên nội bộ

a) Các cơ quan, đơn vị tuân thủ các quy định của pháp luật và quy định tại Quy chế này khi truy cập, sử dụng tài nguyên tại Trung tâm dữ liệu.

b) Không truy cập, quản trị các máy chủ tại Trung tâm dữ liệu từ xa thông qua internet. Việc truy cập quản trị các máy chủ tại Trung tâm dữ liệu thực hiện thông qua kết nối VPN (mạng riêng ảo).

c) Không kết nối các thiết bị lưu trữ di động bên ngoài vào các máy chủ tại Trung tâm dữ liệu. Trường hợp, người sử dụng cần thiết phải kết nối các thiết bị lưu trữ di động bên ngoài thì phải đề nghị và được bộ phận chuyên trách kiểm tra an toàn thông tin trước khi thực hiện.

2. Quản lý truy cập tài nguyên trên Internet

a) Viên chức vận hành Trung tâm dữ liệu không sử dụng máy tính quản trị để truy cập các trang thông tin không rõ nguồn gốc hoặc có nội dung độc hại.

b) Máy chủ/máy tính tại Trung tâm dữ liệu phải triển khai giải pháp bảo mật đảm bảo không bị tấn công xâm nhập, lây lan virus từ bên ngoài.

3. Cài đặt và sử dụng máy tính an toàn

a) Đặt mật khẩu cho các tài khoản của hệ điều hành theo quy tắc: tối thiểu 11 ký tự; bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt. Định kỳ ít nhất 06 tháng thay đổi mật khẩu; trường hợp đặc biệt hoặc khi có thay đổi về nhân sự

hoặc yêu cầu tăng cường bảo mật về an toàn thông tin thì lãnh đạo cơ quan vận hành Trung tâm dữ liệu quyết định việc thay đổi toàn bộ mật khẩu quản trị của của các hệ thống tại Trung tâm dữ liệu.

b) Khóa máy tính khi tạm thời rời khỏi vị trí làm việc. Đóng các phiên làm việc của ứng dụng khi đã hoàn tất, trừ khi đã có cơ chế bảo vệ thích hợp.

c) Không tự ý thay đổi cấu hình đã được thiết lập, việc thay đổi phải thông báo đến bộ phận liên quan.

Điều 20. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro: thực hiện rà soát, kiểm tra, đánh giá an toàn thông tin cho máy chủ, ứng dụng để xác định các mối đe dọa, tiến hành xử lý.

2. Quy trình đánh giá và quản lý rủi ro

a) Thiết lập bối cảnh: thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần tại Trung tâm dữ liệu cần bảo vệ.

b) Đánh giá rủi ro: thực hiện nhận biết rủi ro, phân tích và ước lượng rủi ro để biết mức ảnh hưởng đối với Trung tâm dữ liệu khi rủi ro xảy ra để ưu tiên xử lý.

c) Xử lý rủi ro: đưa ra các phương án và xác định phương án xử lý rủi ro, bao gồm các biện pháp quản lý và kỹ thuật để có thể xử lý, giảm thiểu các mối đe dọa có thể xảy ra đối với Trung tâm dữ liệu.

3. Biện pháp kiểm soát rủi ro: các yêu cầu về quản lý và yêu cầu về kỹ thuật phải đảm bảo các yêu cầu cơ bản theo Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

Điều 21. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Cơ quan vận hành Trung tâm dữ liệu thực hiện các biện pháp kỹ thuật xóa bỏ toàn bộ thông tin, dữ liệu trên các thiết bị với sự xác nhận của chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ, bảo đảm không có khả năng phục hồi. Trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc vật lý đối với thiết bị lưu trữ dữ liệu.

2. Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

Điều 22. Thiết kế an toàn hệ thống thông tin

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

Điều 23. Thuê khoán phần mềm/ứng dụng chuyên ngành

Đối với các cơ quan, đơn vị có thực hiện thuê khoán phần mềm/ứng dụng chuyên ngành triển khai cài đặt tại Trung tâm dữ liệu, cần tuân thủ các quy định sau:

1. Có biên bản, hợp đồng và các cam kết nội dung liên quan phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Điều 24. Thử nghiệm và nghiệm thu hệ thống

Đối với các hệ thống đầu tư (gồm: hạ tầng, thiết bị công nghệ thông tin và phần mềm/ứng dụng/cơ sở dữ liệu) triển khai tại Trung tâm dữ liệu cần tuân thủ các quy định sau:

1. Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

3. Có bộ phận chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

4. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Chương IV
TRÁCH NHIỆM TRONG VIỆC QUẢN LÝ, VẬN HÀNH, KHAI THÁC VÀ ĐẢM BẢO AN TOÀN THÔNG TIN TẠI TRUNG TÂM DỮ LIỆU

Điều 25. Sở Thông tin và Truyền thông (Cơ quan quản lý)

1. Tham mưu Ủy ban nhân dân tỉnh về chính sách khai thác, sử dụng các dịch vụ tại Trung tâm dữ liệu đáp ứng nhu cầu ứng dụng công nghệ thông tin trên địa bàn tỉnh.

2. Tham mưu Ủy ban nhân dân tỉnh nâng cấp, mở rộng Trung tâm dữ liệu đảm bảo việc ứng dụng công nghệ thông tin và xây dựng chính quyền điện tử hướng tới chính quyền số của tỉnh.

3. Thực hiện trách nhiệm của cơ quan chuyên trách về an toàn thông tin theo quy định của pháp luật theo quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; chịu trách nhiệm đối với các hệ thống thông tin thuộc phạm vi quản lý.

4. Tiếp nhận và điều phối xử lý các sự cố về an toàn thông tin mạng tại Trung tâm dữ liệu.

5. Hàng năm xây dựng và triển khai các chương trình đào tạo, tập huấn, diễn tập về công tác bảo đảm an toàn thông tin mạng cho viên chức kỹ thuật phụ trách quản lý, vận hành Trung tâm dữ liệu.

6. Tổ chức tuyên truyền, phổ biến, hướng dẫn cán bộ, công chức, viên chức các cơ quan, đơn vị, địa phương về việc sử dụng và đảm bảo an toàn thông tin các dịch vụ tại Trung tâm dữ liệu.

7. Tiếp nhận các đề nghị của cơ quan, đơn vị, địa phương về cung cấp hạ tầng, dịch vụ tại Trung tâm dữ liệu. Phản hồi cung cấp dịch vụ, hệ thống phần mềm tại Trung tâm dữ liệu đảm bảo thời gian theo quy định.

8. Chỉ đạo mở hoặc dừng đột xuất một số dịch vụ tại Trung tâm dữ liệu theo yêu cầu của Ủy ban nhân dân tỉnh.

9. Phê duyệt các quy trình về quản lý, vận hành, bảo trì, bảo dưỡng, ứng cứu sự cố tại Trung tâm dữ liệu.

10. Quản lý, kiểm tra, giám sát việc vận hành, khai thác dịch vụ, hệ thống, phần mềm, ứng dụng, cơ sở dữ liệu,... tại Trung tâm dữ liệu.

11. Xây dựng các giải pháp, phương án kỹ thuật, kế hoạch phát triển Trung tâm dữ liệu.

12. Hàng năm hoặc đột xuất báo cáo Ủy ban nhân dân tỉnh về tình hình hoạt động của Trung tâm dữ liệu.

Điều 26. Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông (Cơ quan vận hành)

1. Chịu trách nhiệm trước cơ quan quản lý về việc quản lý kỹ thuật, tổ chức thực hiện vận hành, khai thác toàn bộ hệ thống Trung tâm dữ liệu hiệu quả, đảm bảo hạ tầng, ứng dụng hoạt động thông suốt an toàn thông tin theo quy định.

2. Ban hành nội quy làm việc tại Trung tâm dữ liệu; xây dựng kế hoạch, bố trí viên chức quản lý, vận hành hệ thống Trung tâm dữ liệu.

3. Tham mưu về quy định, quy trình, thủ tục chuyển giao thiết bị, cài đặt phần mềm và quản lý tài sản của Trung tâm dữ liệu; ban hành quy trình vận hành và tổ chức thực hiện sao lưu dữ liệu, bảo trì, bảo dưỡng, sửa chữa thiết bị và khắc phục sự cố hệ thống.

4. Đào tạo viên chức quản lý, vận hành có chuyên môn đáp ứng yêu cầu, trang bị các kiến thức liên quan đến hoạt động của Trung tâm dữ liệu.

5. Tham mưu Sở Thông tin và Truyền thông việc cung cấp hạ tầng kỹ thuật công nghệ thông tin và các dịch vụ ứng dụng dùng chung tại Trung tâm dữ liệu khi có yêu cầu của các cơ quan, đơn vị, địa phương.

6. Quy hoạch, vận hành, kiểm tra, đánh giá tài nguyên hệ thống, tham mưu cơ quan quản lý các giải pháp, phương án kỹ thuật, kế hoạch nâng cấp Trung tâm dữ liệu.

7. Hàng năm dự trù kinh phí vận hành, bảo dưỡng, mua sắm, sửa chữa, thay thế trang thiết bị, đánh giá an toàn thông tin, nâng cấp, cập nhật các phần mềm, máy chủ, thiết bị mạng, thiết bị bảo mật, các trang thiết bị phụ trợ,...

8. Tham mưu, đề xuất nội dung đào tạo, cập nhật kiến thức chuyên môn cho viên chức kỹ thuật, đảm bảo đáp ứng các yêu cầu quản lý vận hành Trung tâm dữ liệu.

9. Định kỳ 06 tháng, năm hoặc đột xuất báo cáo Sở Thông tin và Truyền thông về tình hình hoạt động và cung cấp dịch vụ của Trung tâm dữ liệu; định kỳ hàng tháng, báo cáo Sở Thông tin và Truyền thông về tình hình an toàn thông tin tại Trung tâm dữ liệu để nắm, chỉ đạo.

Điều 27. Các sở, ban, ngành tỉnh, Ủy ban nhân dân các huyện, thị xã, thành phố và các tổ chức, cá nhân có kết nối về Trung tâm dữ liệu.

1. Các cơ quan, đơn vị khi có nhu cầu sử dụng hạ tầng, dịch vụ, hệ thống phần mềm tại Trung tâm dữ liệu để phục vụ hoạt động ứng dụng công nghệ thông tin phải gửi đề nghị về Sở Thông tin và Truyền thông xem xét, cấp phát tài nguyên phù hợp với quy hoạch hạ tầng kỹ thuật chung của tỉnh và công năng toàn hệ thống Trung tâm dữ liệu. Sử dụng hạ tầng, dịch vụ tại Trung tâm dữ liệu phải tuân thủ theo Quy chế này và các quy định, hướng dẫn khác của cơ quan quản lý, cơ quan vận hành Trung tâm dữ liệu.

2. Đối với cơ quan, đơn vị có hệ thống thông tin đặt tại Trung tâm dữ liệu

a) Chịu trách nhiệm về các nội dung, thông tin lưu trữ của đơn vị mình tại Trung tâm dữ liệu theo quy định pháp luật. Thường xuyên sao lưu dữ liệu của đơn vị, theo sự hướng dẫn của cơ quan vận hành.

b) Phối hợp với cơ quan quản lý, cơ quan vận hành trong công tác bảo đảm an toàn, an ninh thông tin, duy trì hoạt động các hệ thống thông tin của cơ quan mình đặt tại Trung tâm dữ liệu.

c) Xây dựng hồ sơ cấp độ an toàn hệ thống thông tin đối với các phần mềm, ứng dụng do đơn vị quản lý, đảm bảo theo Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

d) Hàng năm dự trù kinh phí đảm bảo duy trì, vận hành, bảo dưỡng, sửa chữa, trang thiết bị, đường truyền và nâng cấp, cập nhật phần mềm, đánh giá an toàn thông tin do đơn vị mình quản lý, tổng hợp chung trong dự toán chi nghiệp vụ chuyên môn của cơ quan, đơn vị trình cấp có thẩm quyền phê duyệt.

3. Đối với người sử dụng

a) Viên chức vận hành tuân thủ các quy định về an toàn bảo mật thông tin trong quá trình quản lý, khai thác và vận hành Trung tâm dữ liệu.

b) Người sử dụng chịu trách nhiệm về thông tin tài khoản, mật khẩu đăng nhập vào các hệ thống; đồng thời có trách nhiệm thay đổi mật khẩu ngay khi được cơ quan vận hành cung cấp.

c) Không được thực hiện các hành vi đánh cắp, giả mạo tài khoản, truy cập trái phép, sử dụng các công cụ, phần mềm làm tổn hại đến hoạt động của Trung tâm dữ liệu.

4. Trường hợp phát sinh sự cố, phải thông báo ngay cho viên chức kỹ thuật của cơ quan vận hành để phối hợp trong việc xử lý sự cố và xác nhận kết quả xử lý.

Điều 28. Trách nhiệm Sở Tài chính

Hàng năm theo khả năng cân đối ngân sách phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan tham mưu cấp thẩm quyền bố trí kinh phí để thực hiện công tác quản lý, vận hành, bảo trì, bảo dưỡng và đảm bảo an toàn thông tin cho Trung tâm dữ liệu theo quy định của Luật Ngân sách nhà nước và phân cấp ngân sách nhà nước hiện hành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 29. Điều khoản thi hành

1. Các sở, ban, ngành tỉnh, Ủy ban nhân dân các huyện, thị xã, thành phố và các cơ quan, đơn vị, cá nhân có liên quan căn cứ chức năng, nhiệm vụ được giao và các quy định của pháp luật hiện hành tổ chức triển khai thực hiện Quy chế này.

2. Sở Thông tin và Truyền thông có trách nhiệm theo dõi, kiểm tra và đôn đốc việc thực hiện Quy chế này.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc cần điều chỉnh nội dung quy chế, cơ quan, đơn vị, địa phương kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét./.