

Số: 116/2026/QĐ-UBND

Cà Mau, ngày 31 tháng 5 năm 2026

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành, sử dụng
Trung tâm dữ liệu tỉnh Cà Mau

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15;

Căn cứ Luật Sửa đổi, bổ sung một số điều của Luật ban hành văn bản quy phạm pháp luật số 87/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Luật Chuyển đổi số số 148/2025/QH15;

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 Quyết định số 33/2025/QĐ-TTg ngày 15 tháng 9 năm 2025 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Sở Khoa học và Công nghệ tại Tờ trình số 321/TTr-SKHCN ngày 27 tháng 5 năm 2026;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế quản lý, vận hành, sử dụng Trung tâm dữ liệu tỉnh Cà Mau.

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành, sử dụng Trung tâm dữ liệu tỉnh Cà Mau.

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực kể từ ngày 01 tháng 7 năm 2026.

2. Quyết định số 50/2024/QĐ-UBND ngày 01 tháng 11 năm 2024 của Ủy ban nhân dân tỉnh Bạc Liêu ban hành Quy chế quản lý, vận hành, sử dụng Trung tâm dữ liệu tỉnh Bạc Liêu hết hiệu lực kể từ ngày Quyết định này có hiệu lực thi hành.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Khoa học và Công nghệ; Giám đốc Sở Tài chính; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch

Ủy ban nhân dân các xã, phường; các đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:

- Như Điều 3;
- Bộ KH&CN (b/c);
- Cục KTVB&TCTHPL-Bộ Tư pháp;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Ủy ban MTTQVN tỉnh;
- CT, các PCT UBND tỉnh;
- LĐVP UBND tỉnh;
- Công Thông tin điện tử tỉnh (đăng công báo);
- Phòng: Nội chính; KGVX (B₂₀);
- Lưu: VT, KP351/6.

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



Nguyễn Minh Luân

QUY CHẾ
Quản lý, vận hành, sử dụng Trung tâm dữ liệu tỉnh Cà Mau
(Ban hành kèm theo Quyết định số 116/2026/QĐ-UBND)

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, sử dụng và các biện pháp bảo đảm an toàn thông tin cho Trung tâm dữ liệu tỉnh Cà Mau.

2. Đối tượng áp dụng

Quy chế này áp dụng đối với các cơ quan quản lý nhà nước, các đơn vị có hệ thống thông tin cài đặt tại Trung tâm dữ liệu tỉnh; các đơn vị, tổ chức và cá nhân có liên quan đến hoạt động kết nối, quản trị, vận hành, khai thác và sử dụng hệ thống thông tin được cung cấp tại Trung tâm dữ liệu tỉnh.

Điều 2: Nguyên tắc quản lý, vận hành, sử dụng và đảm bảo an toàn thông tin Trung tâm dữ liệu

1. Tuân thủ các nguyên tắc về bảo đảm hạ tầng kỹ thuật và hệ thống thông tin phục vụ ứng dụng, phát triển công nghệ thông tin và chuyển đổi số theo quy định hiện hành.

2. Bảo đảm các yêu cầu về an toàn, an ninh thông tin theo Luật An ninh mạng số 116/2025/QH15 và các văn bản pháp luật hiện hành.

3. Bảo đảm hoạt động ổn định, liên tục phục vụ nhu cầu sử dụng, khai thác của đối tượng sử dụng.

4. Tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật, các quy định hiện hành về công tác quản lý, vận hành, sử dụng Trung tâm dữ liệu. Kết nối, chia sẻ, nâng cấp Trung tâm dữ liệu phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật do Nhà nước quy định, phù hợp với Kiến trúc Chính quyền điện tử tỉnh.

5. Tuân thủ theo các quy định hiện hành về bảo mật, bảo vệ bí mật Nhà nước, bảo đảm an toàn thông tin theo cấp độ.

Điều 3. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm theo quy định tại Điều 8 của Luật An ninh mạng số 116/2025/QH15.

2. Tự ý đầu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

7. Mua bán, trao đổi, chia sẻ dữ liệu trái quy định của pháp luật.

8. Phá hoại cơ sở hạ tầng thông tin, làm gián đoạn việc kết nối, chia sẻ dữ liệu trong Trung tâm dữ liệu tỉnh.

9. Đánh cắp, giả mạo tài khoản, thông tin cá nhân để truy cập trái phép vào hệ thống, phần mềm, cơ sở dữ liệu trong Trung tâm dữ liệu tỉnh.

10. Sử dụng các công cụ, thiết bị, phần mềm có nguy cơ gây mất an toàn dữ liệu, lộ lọt thông tin làm mất an ninh, an toàn thông tin cho các hệ thống trong Trung tâm dữ liệu tỉnh.

Chương II

QUẢN LÝ, VẬN HÀNH VÀ SỬ DỤNG TRUNG TÂM DỮ LIỆU TỈNH

Điều 4. Đơn vị quản lý, vận hành Trung tâm dữ liệu tỉnh

Trung tâm Chuyển đổi số thuộc Sở Khoa học và Công nghệ trực tiếp quản lý, vận hành hệ thống tại Trung tâm dữ liệu tỉnh, bao gồm: Hạ tầng thiết bị, thiết bị máy chủ, đường truyền và các thiết bị phụ trợ khác lắp đặt tại Trung tâm dữ liệu tỉnh; các ứng dụng, website, hệ thống thông tin, nền tảng số dùng chung được cài đặt tại Trung tâm dữ liệu tỉnh.

Điều 5. Quản lý thiết bị

1. Thiết bị lắp đặt tại Trung tâm dữ liệu tỉnh phải được kiểm tra an toàn thông tin trước khi lắp đặt theo quy định.

2. Các thiết bị phải được đặt tên và dán nhãn để theo dõi, quản lý.

3. Trường hợp thiết bị hư hỏng cần sửa chữa, thay thế, đơn vị quản lý, vận hành phải có phương án thay thế, khắc phục kịp thời, đảm bảo không làm gián đoạn hoạt động của các hệ thống tại Trung tâm dữ liệu.

4. Việc sửa chữa, thay thế thiết bị hư hỏng thực hiện theo đúng quy định hiện hành.

Điều 6. Quản lý kết nối

1. Kết nối mạng truyền số liệu chuyên dùng

Kết nối, sử dụng mạng truyền số liệu chuyên dùng tại Trung tâm dữ liệu tỉnh thực hiện theo các quy định về quản lý, vận hành và sử dụng mạng truyền số liệu chuyên dùng tại các Điều 7, 8 và 9 Quyết định số 33/2025/QĐ-TTg ngày 15 tháng 9 năm 2025 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước.

2. Kết nối mạng Internet

a) Đối với các kết nối Internet phải thiết lập các giải pháp bảo mật, phòng, chống tấn công xâm nhập, lây lan virus, phần mềm độc hại từ bên ngoài;

b) Đường truyền Internet cho Trung tâm dữ liệu phải có tối thiểu 02 đường truyền của 02 nhà cung cấp khác nhau để đảm bảo dự phòng cho hệ thống.

Điều 7. Quản lý bản quyền phần mềm

1. Phần mềm hệ thống, các phần mềm ứng dụng được cài đặt 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.

2. 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. Cơ quan quản lý, vận hành phải theo dõi việc sử dụng các bản quyền phần mềm tại Trung tâm dữ liệu. Lập dự toán và báo cáo các cơ quan liên quan về gia hạn bản quyền, đảm bảo hoạt động liên tục, ổn định 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 8. Quản lý, lưu giữ hồ sơ

1. Hồ sơ có liên quan đến hệ thống Trung tâm dữ liệu tỉnh phải được lưu bằng văn bản, tập tin bản mềm trên máy tính hoặc phần mềm quản lý điều hành và phải được cập nhật khi có sự thay đổi.

2. Danh sách các loại hồ sơ quản lý, lưu giữ

a) Các chính sách, quy định liên quan đến công tác quản lý, vận hành, sử dụng, triển khai, nâng cấp Trung tâm dữ liệu;

b) Các quy trình vận hành kỹ thuật các hệ thống;

c) Các quy trình bảo hành, bảo trì, bảo dưỡng các hệ thống;

d) Hồ sơ thiết kế, thuyết minh kỹ thuật, hoàn công;

đ) Hồ sơ quản lý, quản trị các hệ thống thông tin;

e) Hồ sơ lưu các dịch vụ cung cấp;

g) Báo cáo quản trị hệ thống, nhật ký vận hành hệ thống;

h) Bảng thống kê danh sách thiết bị tại Trung tâm dữ liệu. Danh sách các thiết bị hư hỏng, hết khấu hao sử dụng chờ thanh lý. Biên bản bàn giao thiết bị cho người quản trị, người sử dụng (nếu có);

i) Các hồ sơ, tài liệu kỹ thuật khác.

Điều 9. Chế độ làm việc tại Trung tâm dữ liệu tỉnh

1. Quy định vận hành Trung tâm dữ liệu tỉnh

a) Trung tâm dữ liệu tỉnh đảm bảo duy trì hoạt động liên tục 24 giờ/ngày và 7 ngày/tuần;

b) Đảm bảo chế độ trực vận hành Trung tâm dữ liệu ngoài giờ hành chính, ngày nghỉ, ngày Lễ, ngày Tết.

2. Quy định đối với người được giao nhiệm vụ quản trị, vận hành hệ thống

a) Trong quá trình làm việc và trực vận hành phải tuân thủ nghiêm ngặt theo các quy định về quy trình quản lý, xử lý sự cố và nội quy của Trung tâm dữ liệu;

b) Được phép truy cập, khai thác thông tin tại Trung tâm dữ liệu theo trách nhiệm được giao và theo phân quyền; 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 dữ liệu;

c) Quá trình làm việc, thực hiện các nghiệp vụ chuyên môn có sự tác động đến các thiết bị thuộc các phân hệ của Trung tâm dữ liệu phải được ghi chép cụ thể vào sổ nhật ký hệ thống;

d) Có trách nhiệm theo dõi, phát hiện kịp thời các trường hợp truy cập hệ thống trái phép hoặc có hành vi vượt quá giới hạn phải báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm;

đ) Cán bộ thực hiện nhiệm vụ quản lý, vận hành khi chấm dứt hoặc thay đổi công tác phải thu hồi tài khoản truy cập và vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống và có cam kết giữ bí mật thông tin liên quan đến Trung tâm dữ liệu sau khi nghỉ việc.

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

a) Tuân thủ nghiêm theo các nội quy, quy định tại Trung tâm dữ liệu;

b) Không được sử dụng, mang theo các thiết bị điện thoại, máy tính xách tay, máy tính bảng hoặc các thiết bị điện tử cá nhân khác (thiết bị ghi âm, ghi hình, lưu trữ) khi vào bên trong Trung tâm dữ liệu, trừ trường hợp có sự đồng ý của lãnh đạo cơ quan quản lý, vận hành Trung tâm dữ liệu;

c) Các tổ chức, cá nhân muốn khảo sát Trung tâm dữ liệu phải được cơ quan quản lý cho phép và xác định rõ nội dung trước khi khảo sát;

d) Các tổ chức, cá nhân tham quan Trung tâm dữ liệu phải được sự đồng ý của cơ quan quản lý Trung tâm dữ liệu tỉnh gồm: Công văn hoặc Giấy giới thiệu;

danh sách những người tham quan. Việc tham quan không được phép kèm nội dung khảo sát, không được ghi lại thông tin dưới bất kỳ hình thức nào.

Điều 10. Sao lưu, phục hồi dữ liệu

1. Đơn vị vận hành triển khai giải pháp hoặc phương tiện lưu trữ độc lập để sao lưu dự phòng. Thực hiện lưu trữ đầy đủ các dữ liệu của người dùng, ứng dụng và hệ thống. Tùy theo từng loại dữ liệu, thực hiện lưu trữ đúng và đủ thời hạn, đảm bảo phục hồi nguyên trạng khi có sự cố xảy ra. Tần suất sao lưu tùy thuộc vào mức độ quan trọng của dữ liệu.

2. Triển khai giải pháp sao lưu ngoại tuyến. Có ít nhất 03 (ba) bản sao lưu dữ liệu được lưu trữ trên 02 (hai) phương tiện lưu trữ khác nhau cùng với 01 (một) bản sao lưu ngoại tuyến.

3. 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. Đối với các dữ liệu quan trọng phải được lưu trữ tối thiểu tại hai thiết bị hoặc lưu trữ tại hai địa điểm cách biệt nhau.

4. Đơn vị quản lý, vận hành xây dựng quy trình sao lưu, phục hồi dữ liệu và lập lịch sao lưu theo quy trình cho các hệ thống tại Trung tâm dữ liệu theo hướng dẫn và các quy định hiện hành.

Điều 11. An toàn vận hành

1. Không được phép đặt tại Trung tâm dữ liệu các thiết bị hư hỏng, thiết bị chờ thanh lý, tài liệu, vật tư, các vật dụng dễ cháy nổ.

2. Trung tâm dữ liệu phải đảm bảo vệ sinh, môi trường khô ráo, sạch sẽ, không thấm nước, không bị ánh nắng chiếu trực tiếp. Độ ẩm, nhiệt độ môi trường đạt tiêu chuẩn quy định.

3. Hệ thống phòng cháy, chữa cháy, chống sét phải đáp ứng theo tiêu chuẩn quy định đảm bảo an toàn tuyệt đối cho toàn bộ thiết bị, đảm bảo an toàn cho người quản trị các hệ thống tại Trung tâm dữ liệu.

4. Hệ thống điện cấp cho Trung tâm dữ liệu phải ổn định, liên tục. Trung tâm dữ liệu phải được trang bị hệ thống lưu điện và máy phát điện dự phòng để đảm bảo cho hệ thống hoạt động liên tục, ổn định trong thời gian nguồn điện lưới gặp sự cố.

5. Hệ thống camera thực hiện giám sát toàn bộ Trung tâm dữ liệu liên tục 24/7. Dữ liệu hình ảnh phải được lưu trữ ít nhất trong thời gian là 30 ngày.

6. Hệ thống quản lý vào ra hoạt động 24/7 và ghi đầy đủ nhật ký nhằm đảm bảo an ninh, chính xác và linh hoạt cho Trung tâm dữ liệu.

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

8. Thực hiện các biện pháp đảm bảo an toàn thông tin khác theo hướng dẫn, quy định hiện hành.

Điều 12. Xử lý sự cố

1. Khi phát hiện có sự cố, đơn vị vận hành hệ thống thực hiện các biện pháp cô lập và xác định nguyên nhân xảy ra sự cố, hạn chế tối đa ảnh hưởng tới hoạt động của Trung tâm dữ liệu. Đồng thời, có trách nhiệm báo cáo kịp thời cho lãnh đạo đơn vị quản lý, vận hành hệ thống và các đơn vị có liên quan để có biện pháp xử lý kịp thời.

2. Tùy thuộc vào mức độ ảnh hưởng của sự cố, cần đánh giá và phân loại theo 03 mức như sau:

a) Các sự cố thông thường (không gây ảnh hưởng đến hoạt động của Trung tâm dữ liệu): Đơn vị quản lý, vận hành nhanh chóng phối hợp với các cơ quan, tổ chức, đơn vị liên quan thực hiện xử lý sự cố;

b) Các sự cố nghiêm trọng (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 dữ liệu, gây ảnh hưởng trực tiếp đến hoạt động của Trung tâm dữ liệu): Đơn vị quản lý, vận hành cần đánh giá ảnh hưởng của sự cố và phối hợp với các đơn vị chuyên trách để được hướng dẫn xử lý;

c) Các sự cố đặc biệt nghiêm trọng (gây ngưng trệ một phần hoặc toàn bộ hoạt động của Trung tâm dữ liệu): Đơn vị quản lý, vận hành phải có đánh giá ảnh hưởng của sự cố, phối hợp với các cơ quan Bộ, ngành liên quan, đồng thời thực hiện báo cáo nhanh về Ủy ban nhân dân tỉnh để có chỉ đạo xử lý.

3. Quy định khắc phục sự cố

a) Tuân thủ theo Quy trình xử lý, ứng cứu sự cố do cơ quan quản lý ban hành và các văn bản pháp luật hiện hành;

b) Thực hiện sao lưu dữ liệu trước khi khắc phục sự cố;

c) Đảm bảo tuyệt đối an toàn cho người và thiết bị của Trung tâm dữ liệu;

d) Ghi nhật ký diễn biến sự cố, phương án khắc phục;

đ) Thông báo cho các cơ quan, đơn vị liên quan về thời gian dự kiến khắc phục xong sự cố;

e) Báo cáo kết quả khắc phục, xử lý sự cố đến cơ quan quản lý tùy theo mức độ ảnh hưởng của sự cố.

Điều 13. Bảo trì, bảo dưỡng

1. Đơn vị vận hành có trách nhiệm

a) Trực tiếp thực hiện hoặc thuê dịch vụ bảo trì, bảo dưỡng các hệ thống theo quy định;

b) Thực hiện bảo trì, bảo dưỡng theo kế hoạch được phê duyệt.

2. Yêu cầu về bảo trì, bảo dưỡng

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

b) Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến hoạt động của Trung tâm dữ liệu.

Điều 14. Cấp phát, tiếp nhận tài nguyên

1. Các cơ quan, đơn vị có nhu cầu sử dụng hạ tầng Trung tâm dữ liệu phải có văn bản đề nghị gửi đơn vị quản lý, vận hành xem xét cấp phát tài nguyên theo yêu cầu nhưng phải đảm bảo tính ổn định, tương thích giữa các phân hệ của Trung tâm dữ liệu.

2. Các cơ quan, đơn vị có nhu cầu lắp đặt máy chủ, cài đặt thiết bị vào Trung tâm dữ liệu phải có văn bản đề nghị gửi đơn vị quản lý, vận hành xem xét nhưng phải đảm bảo tính đồng bộ, tương thích với hạ tầng, thiết bị Trung tâm dữ liệu.

3. Cơ quan, đơn vị chịu trách nhiệm quản lý máy chủ, thiết bị, hệ thống của mình đặt tại Trung tâm dữ liệu và phân công người làm đầu mối phối hợp, hỗ trợ cho đơn vị quản lý, vận hành trong quá trình sử dụng. Trường hợp không đảm bảo nhân lực quản trị hệ thống thì chuyển toàn bộ hoặc một phần nhiệm vụ trên cho đơn vị quản lý, vận hành (phải được ký kết, thống nhất giữa hai bên).

Điều 15. Quản lý và sử dụng tài khoản, mật khẩu

1. Đơn vị vận hành quy định cụ thể về tiếp nhận, quản lý, sử dụng, lưu trữ tài khoản quản trị, tài khoản được cấp phát và sử dụng mật khẩu đối với các hệ thống tại Trung tâm dữ liệu theo đúng quy định hiện hành.

2. Đối với mật khẩu tài khoản quản trị phải bảo đảm độ an toàn về độ phức tạp, giới hạn thời gian sử dụng

a) Độ dài của mật khẩu: Đối với mật khẩu quản trị hệ thống sử dụng cho quản trị các phân hệ của Trung tâm dữ liệu phải có ít nhất 12 ký tự. Đối với mật khẩu cấp cho người sử dụng dùng để đăng nhập các hệ thống thông tin tại Trung tâm dữ liệu phải có ít nhất 08 ký tự;

b) Mật khẩu không bao gồm các từ dễ nhớ như: Họ tên, ngày sinh, số điện thoại, các dãy số, dãy ký tự. Mật khẩu phải bao gồm chữ in hoa, chữ thường, số và ký tự đặc biệt;

c) Thời gian sử dụng mật khẩu: Đối với mật khẩu của người được giao nhiệm vụ quản trị, vận hành định kỳ phải được 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 thực hiện thay đổi toàn bộ mật khẩu quản trị của Trung tâm dữ liệu.

3. Quy định sử dụng và lưu trữ mật khẩu

a) Người sử dụng phải thay đổi mật khẩu được cấp mới ngay từ lần đăng nhập đầu tiên và chịu trách nhiệm về việc quản lý mật khẩu được cấp. Khi có dấu hiệu bị lộ, lọt thông tin liên quan thì phải tiến hành thay đổi mật khẩu trên các hệ thống thông tin đang vận hành tại Trung tâm dữ;

b) 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;

c) Các tài liệu liên quan đến mật khẩu được quản lý nghiêm, không soạn thảo, lưu trữ trên máy tính có nối mạng Internet;

d) Các hệ thống thông tin tại Trung tâm dữ liệu phải có cơ chế bắt buộc người sử dụng thay đổi mật khẩu cho lần truy cập tiếp theo nhằm hạn chế tình trạng người sử dụng không thay đổi mật khẩu mặc định được cấp.

Điều 16. Kiểm soát truy cập và xác thực

1. Đơn vị vận hành phải có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn. Cấp phát quyền truy cập từ xa hoặc kết nối trực tiếp để sử dụng và khai thác tài nguyên thuộc Trung tâm dữ liệu phải đảm bảo chặt chẽ, đúng mục đích sử dụng.

2. Một người dùng chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công. Đơn vị vận hành xem xét khóa các tài khoản truy cập vượt quá giới hạn cho phép.

3. Đơn vị vận hành tạm khóa quyền sử dụng đối với tài khoản đã được đăng ký nhưng không sử dụng hoặc không thay đổi mật khẩu mặc định được cấp từ 30 ngày trở lên, tính từ ngày được thông báo tạo lập tài khoản. Tài khoản chỉ được mở khóa khi có đề nghị bằng văn bản của chủ thể sở hữu tài khoản.

4. Đơn vị vận hành theo dõi và nếu phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

Điều 17. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thiết bị công nghệ thông tin có chứa dữ liệu khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành. Các thiết bị công nghệ thông tin bị hỏng không thể sửa chữa, khắc phục được thực hiện theo quy định khoản 2 Điều này.

2. Trước khi tiến hành thanh lý, hủy bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người sử dụng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị công nghệ thông tin khi kết thúc vận hành, khai thác: Máy tính cá nhân, máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Điều 18. Công tác kiểm tra định kỳ

Hàng năm, cơ quan quản lý nhà nước về khoa học và công nghệ (Sở Khoa học và Công nghệ) tổ chức kiểm tra việc tuân thủ các quy định của Quy chế này đối với đơn vị được giao nhiệm vụ quản lý, vận hành hệ thống tại Trung tâm dữ liệu. Các nội dung kiểm tra, bao gồm:

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

2. Tình hình an toàn, an ninh thông tin.
3. Công tác quản lý, lưu trữ dữ liệu.
4. Công tác quản lý, lưu trữ hồ sơ.
5. Công tác quản lý tài sản công.
6. Tình hình hoạt động của các phân hệ.
7. Việc tuân thủ các quy định tại Quy chế này.

Chương III

ĐẢM BẢO AN TOÀN ĐỐI VỚI HỆ THỐNG THÔNG TIN

TẠI TRUNG TÂM DỮ LIỆU TỈNH

Điều 19. An toàn thiết kế cho các hệ thống thông tin

Các cơ quan, đơn vị có hệ thống thông tin cài đặt tại Trung tâm dữ liệu tỉnh phải đáp ứng các yêu cầu về thiết kế hệ thống, cụ thể như sau:

1. Thiết kế an toàn hệ thống thông tin
 - a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;
 - b) Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin;
 - c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;
 - d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;
 - đ) 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.
2. Phát triển phần mềm thuê khoán
 - a) Có biên bản, hợp đồng và các cam kết đối với bên thuê dịch vụ các nội dung liên quan đến việc phát triển phần mềm thực hiện theo hình thức thuê dịch vụ;
 - b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm;
 - c) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng;
 - d) Kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.
3. Vận hành thử hoặc kiểm thử và nghiệm thu hệ thống
 - a) Thực hiện vận hành thử hoặc kiểm thử và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng;
 - b) Có nội dung, kế hoạch, quy trình thực hiện vận hành thử/kiểm thử và nghiệm thu hệ thống;

c) Có bộ phận có trách nhiệm thực hiện tham gia vận hành thử/kiểm thử và nghiệm thu hệ thống;

d) 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 vận hành thử hoặc kiểm thử và nghiệm thu hệ thống;

đ) 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.

Điều 20. Bảo đảm an toàn thông tin theo cấp độ

1. Tất cả các hệ thống thông tin trước khi triển khai tại Trung tâm dữ liệu phải được phê duyệt cấp độ an toàn thông tin theo quy định.

2. Các hệ thống thông tin phải được trang bị và triển khai đầy đủ các biện pháp đảm bảo an toàn thông tin theo cấp độ được phê duyệt.

3. Các hệ thống thông tin đã được phê duyệt cấp độ an toàn thông tin phải được kiểm tra, đánh giá an toàn thông tin định kỳ hàng năm theo quy định và hướng dẫn hiện hành.

Chương IV TỔ CHỨC THỰC HIỆN

Điều 21. Sở Khoa học và Công nghệ

1. Tham mưu Ủy ban nhân dân tỉnh thực hiện đầu tư, nâng cấp và mở rộng Trung tâm dữ liệu tỉnh đáp ứng yêu cầu phục vụ nhiệm vụ chuyển đổi số, xây dựng chính quyền điện tử của tỉnh; thực hiện công tác bảo trì, bảo dưỡng hệ thống tại Trung tâm dữ liệu định kỳ; tham mưu Ủy ban nhân dân tỉnh quy hoạch hệ thống, các giải pháp, phương án kỹ thuật, kế hoạch phát triển Trung tâm dữ liệu đáp ứng nhu cầu chuyển đổi số của tỉnh, phù hợp với Khung Kiến trúc số tỉnh, Chính quyền điện tử tỉnh.

2. Xem xét, cấp phát tài nguyên, hạ tầng, dịch vụ dùng chung theo nhu cầu của các cơ quan, đơn vị nhằm phục vụ nhiệm vụ chuyển đổi số tại các cơ quan, đơn vị, địa phương trong tỉnh.

3. Dự toán kinh phí hàng năm bảo đảm cho duy trì hoạt động Trung tâm dữ liệu liên tục, ổn định, đảm bảo an toàn thông tin.

4. Tổ chức kiểm tra việc tuân thủ các quy định của Quy chế này theo quy định tại Điều 18 Quy chế này.

Điều 22. Sở Tài chính

Phối hợp với Sở Khoa học và Công nghệ tham mưu bố trí kinh phí đảm bảo cho hoạt động của Trung tâm dữ liệu theo quy định.

Điều 23. Các cơ quan, đơn vị và người sử dụng

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

a) Phối hợp, hỗ trợ theo quy định trong quá trình quản lý, vận hành, sử dụng Trung tâm dữ liệu nhằm đảm bảo khả năng xử lý, ứng cứu các sự cố;

b) Tuân thủ các quy định về triển khai, tiếp nhận, quản lý, cấp phát máy chủ, tài nguyên trong Quy chế này. Đồng thời, bảo đảm an toàn thông tin theo quy định tại Hồ sơ cấp độ đã được phê duyệt.

2. Đối với người sử dụng

a) Tuân thủ các quy định được ban hành tại Quy chế này;

b) Tuân thủ các quy định về an toàn bảo mật thông tin, quản lý, vận hành, sử dụng Trung tâm dữ liệu. 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.

Điều 24. Triển khai thực hiện

1. Sở Khoa học và Công nghệ chủ trì tổ chức triển khai, phổ biến, hướng dẫn thực hiện Quy chế này; theo dõi, kiểm tra định kỳ và báo cáo Ủy ban nhân dân tỉnh tình hình hoạt động Trung tâm dữ liệu tỉnh hàng năm.

2. Đơn vị quản lý, vận hành Trung tâm dữ liệu tỉnh tổ chức thực hiện tuân thủ các quy định của Quy chế này. Báo cáo tình hình quản lý, vận hành, sử dụng Trung tâm dữ liệu tỉnh định kỳ hàng năm và đột xuất theo yêu cầu của Sở Khoa học và Công nghệ.

3. Các cơ quan, đơn vị có liên quan căn cứ chức năng, nhiệm vụ tổ chức triển khai, kiểm tra việc thực hiện Quy chế này. Phối hợp với Sở Khoa học và Công nghệ xem xét, tích hợp các hệ thống thông tin riêng lẻ của cơ quan, đơn vị để tập trung quản lý, vận hành, sử dụng tại Trung tâm dữ liệu nhằm mục tiêu tận dụng tối đa nguồn tài nguyên, giảm thiểu rủi ro, bảo đảm an toàn, an ninh thông tin.

4. Trong quá trình thực hiện Quy chế này, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị kịp thời phản ánh về Sở Khoa học và Công nghệ để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định.