ỦY BAN NHÂN DÂN TỈNH THÁI NGUYÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 117 /2026/QĐ-UBND	*Thái Nguyên, ngày 20 tháng 8 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên

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

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

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

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

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

Căn cứ Nghị định số 278/2025/NĐ-CP ngày 22/10/2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư số 42/2025/TT-BKHCN ngày 30/11/2025 của Bộ trưởng Bộ Khoa học và Công nghệ quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm Dữ liệu;

Theo đề nghị của Giám đốc Sở Khoa học và Công nghệ tại Tờ trình số 179/TTr-SKHCN ngày 07 tháng 7 năm 2026;

Ủy ban nhân dân tỉnh ban hành Quyết định ban hành Quy chế quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên.

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên.

Điều 2. Điều khoản thi hành

1. Quyết định này có hiệu lực thi hành kể từ ngày 05 tháng 9 năm 2026.

2. Các quyết định sau hết hiệu lực kể từ ngày Quyết định này có hiệu lực thi hành:

a) Quyết định số 28/2020/QĐ-UBND ngày 01 tháng 12 năm 2020 của Ủy ban nhân dân tỉnh về việc ban hành Quy chế quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên;

b) Quyết định số 54/2024/QĐ-UBND ngày 09 tháng 12 năm 2024 của Ủy ban nhân dân tỉnh về việc sửa đổi, bổ sung một số điều của Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu tỉnh Thái Nguyên ban hành kèm theo Quyết định số 28/2020/QĐ-UBND ngày 01 tháng 12 năm 2020 của Ủy ban nhân dân tỉnh Thái Nguyên.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các xã, phường; Thủ trưởng các cơ quan, đơn vị và các tổ chức có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Khoa học và Công nghệ;
- Cục Kiểm tra văn bản và Tổ chức thi hành pháp luật - Bộ Tư pháp;
- Thường trực Tỉnh ủy;
- Thường trực Hội đồng nhân dân tỉnh;
- Ủy ban nhân dân tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành thuộc tỉnh;
- Báo và phát thanh, truyền hình Thái Nguyên;
- UBND các xã, phường;
- Lãnh đạo VP UBND tỉnh;
- Trung tâm Thông tin tỉnh;
- Trung tâm PT KHCN&ĐMST - Sở Khoa học và Công nghệ;
- Lưu: VT, KGVX.

Thaidh/QPPL15

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

ỦY BAN NHÂN DÂN TỈNH THÁI NGUYÊN

Nguyễn Thị Loan

ỦY BAN NHÂN DÂN
TỈNH THÁI NGUYÊN

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 Thái Nguyên

(Ban hành kèm theo Quyết định số 117 /2026/QĐ-UBND)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về công tác quản lý, vận hành, khai thác đối với hạ tầng kỹ thuật, hệ thống, ứng dụng, dữ liệu và dịch vụ thuộc Trung tâm Dữ liệu tỉnh Thái Nguyên *(sau đây viết tắt là Trung tâm Dữ liệu).*

2. Đối tượng áp dụng:

Quy chế này áp dụng đối với:

a) Cơ quan chủ quản Trung tâm Dữ liệu: Ủy ban nhân dân tỉnh Thái Nguyên.

b) Cơ quan quản lý Trung tâm Dữ liệu (gọi tắt là cơ quan quản lý): Sở Khoa học và Công nghệ tỉnh Thái Nguyên.

c) Đơn vị vận hành Trung tâm Dữ liệu (gọi tắt là đơn vị vận hành): Trung tâm Phát triển Khoa học, Công nghệ và Đổi mới sáng tạo thuộc Sở Khoa học và Công nghệ tỉnh Thái Nguyên.

d) Cơ quan, tổ chức, đơn vị khai thác, sử dụng, kết nối, chia sẻ dữ liệu, ứng dụng, dịch vụ tại Trung tâm Dữ liệu.

đ) Tổ chức, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, dịch vụ hạ tầng, dịch vụ kỹ thuật, dịch vụ an ninh mạng có liên quan đến Trung tâm Dữ liệu.

e) Chủ quản các hệ thống thông tin, cơ sở dữ liệu, ứng dụng đặt tại Trung tâm Dữ liệu hoặc đặt tại hạ tầng thuê ngoài nhưng có kết nối, liên thông, đồng bộ, khai thác hoặc quản trị từ xa với Trung tâm Dữ liệu.

g) Cơ quan, tổ chức, cá nhân khác có liên quan đến việc quản lý, vận hành và 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. 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 diện rộng, mạng truyền số liệu chuyên dùng và các thiết bị kỹ thuật chuyên dùng khác.

2. Ứng dụng dùng chung là phần mềm dùng chung cho các cơ quan, đơn vị thuộc phạm vi của tỉnh được UBND tỉnh thống nhất triển khai đưa vào hoạt động tại Trung tâm Dữ liệu tỉnh.

3. Dữ liệu dùng chung là dữ liệu được nhiều cơ quan, đơn vị cùng sử dụng để phục vụ quản lý, điều hành, giải quyết thủ tục hành chính, cung cấp dịch vụ công và các nhiệm vụ khác theo thẩm quyền.

4. Tài khoản đặc quyền là tài khoản có quyền quản trị, cấu hình, giám sát hoặc truy cập vào các chức năng trọng yếu của hệ thống.

5. Nhật ký hệ thống là thông tin ghi lại quá trình hoạt động, truy cập, cấu hình, xử lý và sự kiện phát sinh trong hệ thống.

Điều 3. Chức năng, kiến trúc và dịch vụ của Trung tâm Dữ liệu

1. Trung tâm Dữ liệu có chức năng lưu trữ, trao đổi, xử lý, tích hợp, chia sẻ và bảo đảm an toàn đối với dữ liệu, cơ sở dữ liệu, ứng dụng và dịch vụ số của tỉnh; phục vụ hoạt động của cơ quan, tổ chức, đơn vị có liên quan theo quy định của pháp luật.

2. Kiến trúc của Trung tâm Dữ liệu gồm các thành phần cơ bản sau đây:

a) Phân hệ mạng và truyền dẫn: 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 các mục đích khác nhau. Trung tâm Dữ liệu sử dụng đường truyền số liệu chuyên dùng để kết nối mạng WAN của tỉnh phục vụ các cơ quan, địa phương, đơn vị trên địa bàn tỉnh khai thác hệ thống dữ liệu dùng chung, sử dụng đường truyền riêng để cung cấp dịch vụ truy cập qua Internet.

b) Phân hệ bảo đảm an ninh mạng: Bao gồm các thiết bị tường lửa cho lớp mạng và lớp ứng dụng, các thiết bị ngăn chặn xâm nhập trái phép, thiết bị cân bằng tải và các ứng dụng bảo đảm an toàn cho hệ thống. Mỗi thành phần trong phân hệ bảo đảm an ninh mạng đều được thiết kế bảo đảm tính dự phòng và bổ sung hỗ trợ lẫn nhau trong toàn bộ hệ thống của Trung tâm Dữ liệu.

c) Phân hệ máy chủ: Bao gồm hệ thống máy chủ phiến và các máy chủ đã được đầu tư hoặc được đặt tại Trung tâm Dữ liệu với khả năng sẵn sàng cho việc mở rộng số lượng máy chủ trong tương lai. Hệ thống máy chủ và nền tảng ảo hóa phục vụ triển khai, vận hành các ứng dụng, dịch vụ số, cơ sở dữ liệu dùng chung và chuyên ngành.

d) Phân hệ lưu trữ: Bao gồm hệ thống lưu trữ tập trung với năng lực xử lý ở mức cao, khả năng lưu trữ lớn và hệ thống sao lưu, phục hồi dữ liệu. Phân hệ được thiết kế bảo đảm khả năng mở rộng đáp ứng nhu cầu phát triển nguồn dữ liệu trong tương lai.

đ) Phân hệ cơ sở dữ liệu: Là hệ thống 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 công dân, doanh nghiệp.

e) Phân hệ phần mềm: Bao gồm hệ thống ứng dụng dùng chung, ứng dụng

chuyên ngành và các hệ thống phần mềm khác được triển khai tại Trung tâm Dữ liệu phục vụ công tác chỉ đạo, điều hành, tác nghiệp của các cơ quan, đơn vị, địa phương và người dân, tổ chức theo thiết kế được phê duyệt và đảm bảo yêu cầu trước khi đưa vào sử dụng.

g) Phân hệ các hệ thống phụ trợ: Bao gồm hệ thống nguồn điện, điều hòa chính xác, thiết bị lưu điện, máy phát điện, sàn nâng, hệ thống máng, cáp, hệ thống phòng cháy chữa cháy, kiểm soát ra vào, camera giám sát, và các thiết bị có liên quan khác.

h) Phân hệ thành phần khác theo quy định của pháp luật.

3. Các dịch vụ được cung cấp tại Trung tâm Dữ liệu, bao gồm:

a) Duy trì, vận hành các hệ thống, nền tảng, ứng dụng dùng chung phục vụ hoạt động của các cơ quan trong hệ thống chính trị, do Nhà nước bảo đảm kinh phí hoạt động: Nền tảng tích hợp và chia sẻ dữ liệu tỉnh Thái Nguyên, Hệ thống Thư điện tử công vụ, Hệ thống quản lý văn bản và điều hành; các dịch vụ kết nối, chia sẻ dữ liệu; Hệ thống phản ánh hiện trường (C-ThaiNguyen) và các hệ thống dùng chung khác của tỉnh.

b) Lưu trữ dữ liệu dự phòng cho các hệ thống, nền tảng, ứng dụng dùng chung của tỉnh được triển khai vận hành trên nền tảng điện toán đám mây.

c) Các dịch vụ khác theo nhu cầu của tổ chức, cá nhân bảo đảm phù hợp với quy định của pháp luật, bao gồm:

- Dịch vụ đặt, vận hành và quản trị máy chủ.

- Dịch vụ lưu trữ, sao lưu, phục hồi và xử lý dữ liệu.

- Dịch vụ cài đặt, tích hợp, khai thác và quản trị ứng dụng, cơ sở dữ liệu.

- Dịch vụ thư mục (Active Directory).

- Dịch vụ quản trị hạ tầng, cung cấp kết nối, chia sẻ dữ liệu.

- Dịch vụ kỹ thuật khác liên quan đến vận hành Trung tâm Dữ liệu theo quy định của pháp luật và phân công của cơ quan có thẩm quyền.

d) Căn cứ vào nhu cầu thực tế, khả năng đáp ứng của hạ tầng và quy định của pháp luật, Sở Khoa học và Công nghệ đề xuất Ủy ban nhân dân tỉnh xem xét việc bổ sung ứng dụng, dịch vụ vận hành tại Trung tâm Dữ liệu.

4. Việc khai thác, sử dụng các thành phần, dịch vụ của Trung tâm Dữ liệu phải bảo đảm đúng mục đích, đúng thẩm quyền, đúng quy trình kỹ thuật, có phân quyền truy cập, có nhật ký hệ thống và tuân thủ quy định về bảo vệ dữ liệu cá nhân, an ninh mạng.

Điều 4. Nguyên tắc quản lý, vận hành và khai thác Trung tâm Dữ liệu

1. Trung tâm Dữ liệu phải được quản lý theo nguyên tắc tập trung, thống nhất, phân công nhiệm vụ rõ ràng; mọi hoạt động truy cập, khai thác, thay đổi cấu hình, kết nối và chia sẻ dữ liệu phải được kiểm soát, ghi nhật ký và truy vết được.

2. Việc quản lý, vận hành, khai thác, kết nối, chia sẻ, sao lưu, phục hồi và bảo đảm an ninh mạng đối với Trung tâm Dữ liệu phải tuân thủ quy định của pháp luật

về chuyển đổi số, dữ liệu số, an ninh mạng, bảo vệ dữ liệu cá nhân và các quy định có liên quan.

3. Dữ liệu và hệ thống thông tin phải được phân loại theo mức độ quan trọng, yêu cầu bảo mật, phạm vi sử dụng và mức độ ảnh hưởng khi xảy ra sự cố; việc áp dụng biện pháp bảo vệ phải tương ứng với từng loại dữ liệu, từng hệ thống và từng dịch vụ.

4. Dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu thuộc phạm vi bí mật nhà nước và các dữ liệu quan trọng khác phải được bảo vệ theo quy định riêng tương ứng, bảo đảm đúng mục đích, đúng thẩm quyền, đúng phạm vi và đúng thời hạn sử dụng.

5. Hệ thống thông tin đặt tại Trung tâm Dữ liệu, hệ thống kết nối từ xa hoặc hệ thống đặt tại hạ tầng thuê ngoài nhưng có liên thông với Trung tâm Dữ liệu phải tuân thủ cùng một yêu cầu quản lý an toàn tối thiểu, bao gồm phân quyền truy cập, xác thực, sao lưu, giám sát, cảnh báo và xử lý sự cố.

6. Việc vận hành, khai thác, sử dụng dịch vụ của Trung tâm Dữ liệu phải bảo đảm liên tục, an toàn, tiết kiệm, hiệu quả.

7. Trường hợp phát sinh sự cố an ninh mạng, mất dữ liệu, lộ lọt dữ liệu cá nhân hoặc gián đoạn dịch vụ, đơn vị vận hành phải kịp thời áp dụng biện pháp khẩn cấp, cô lập sự cố, báo cáo cơ quan quản lý, chủ trì hoặc phối hợp xử lý theo quy trình được phê duyệt.

8. Đơn vị vận hành sử dụng, quản lý tài sản theo đúng các quy định hiện hành về quản lý, sử dụng tài sản công và được phép triển khai cung cấp các dịch vụ gia tăng được cho phép theo quy định nhưng phải dựa trên cơ sở đảm bảo khai thác an toàn, hiệu quả hạ tầng Trung tâm Dữ liệu hiện có.

Điều 5. Các hành vi bị cấm trong quản lý, vận hành và khai thác Trung tâm Dữ liệu

1. Phá hoại, cản trở làm gián đoạn hoạt động chung của Trung tâm Dữ liệu.

2. Sử dụng trái phép cơ sở hạ tầng, tài nguyên, dữ liệu của Trung tâm Dữ liệu hoặc dữ liệu của tổ chức, cá nhân được lưu trữ, xử lý tại Trung tâm Dữ liệu để phục vụ lợi ích cá nhân, trục lợi, xâm phạm an ninh quốc gia, trật tự, an toàn xã hội hoặc quyền, lợi ích hợp pháp của tổ chức, cá nhân.

3. Chia sẻ tài khoản quản trị giữa các quản trị viên.

4. Tự ý can thiệp, thay đổi, sao chép, chuyển giao hoặc cung cấp dữ liệu, phần mềm, cấu hình và tài nguyên hệ thống khi chưa được phép của cơ quan có thẩm quyền.

5. Đánh cắp, giả mạo tài khoản để truy cập trái phép vào các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm Dữ liệu.

6. Đấu nối thiết bị, cài đặt phần mềm không rõ nguồn gốc, thay đổi cấu hình hệ thống khi chưa được phê duyệt.

7. Phát tán mã độc từ bên trong, vô hiệu hóa hoặc làm gián đoạn dịch vụ của Trung tâm Dữ liệu.

Chương II

QUY ĐỊNH CỤ THỂ VỀ QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU

Điều 6. Quy định về chế độ làm việc, ra, vào Trung tâm Dữ liệu

1. Trung tâm Dữ liệu được tổ chức vận hành liên tục, bảo đảm khả năng hoạt động 24 giờ trong ngày, 07 ngày trong tuần đối với các hệ thống, dịch vụ trọng yếu theo yêu cầu của cơ quan có thẩm quyền.

2. Đơn vị vận hành có trách nhiệm bố trí nhân sự trực, giám sát và xử lý kỹ thuật phù hợp với mức độ quan trọng của hệ thống; bảo đảm tiếp nhận, ghi nhận, xử lý và báo cáo kịp thời các cảnh báo, sự cố phát sinh trong quá trình vận hành.

3. Cán bộ, viên chức, người lao động làm việc tại Trung tâm Dữ liệu phải tuân thủ nội quy, quy trình vận hành, quy trình bảo đảm an ninh mạng, quy trình ra vào khu vực kiểm soát và các quy định liên quan khác; không tự ý thay đổi cấu hình, cài đặt phần mềm, can thiệp dữ liệu hoặc thực hiện thao tác vượt quá thẩm quyền được giao.

4. Mọi thao tác kỹ thuật có ảnh hưởng đến hạ tầng, phần mềm, cơ sở dữ liệu, tài khoản, cấu hình hoặc dịch vụ của Trung tâm Dữ liệu phải được phân quyền, ghi nhật ký và thực hiện theo đúng quy trình đã được phê duyệt.

5. Khi chấm dứt công tác, thay đổi vị trí công việc hoặc không còn được giao nhiệm vụ liên quan, người làm việc tại Trung tâm Dữ liệu phải bàn giao đầy đủ tài liệu, thiết bị, tài khoản, thẻ truy cập, thông tin kỹ thuật và các tài sản khác có liên quan; đồng thời chấm dứt quyền truy cập theo quy định.

6. Tổ chức, cá nhân đến làm việc, kiểm tra, bảo trì, tham quan hoặc phối hợp kỹ thuật tại Trung tâm Dữ liệu phải chấp hành quy chế ra vào, kiểm soát thiết bị mang theo, đăng ký mục đích làm việc và chịu sự giám sát của đơn vị vận hành trong suốt thời gian có mặt tại khu vực kiểm soát.

7. Trường hợp làm việc với hệ thống, dữ liệu hoặc dịch vụ có chứa dữ liệu cá nhân hoặc dữ liệu quan trọng, đơn vị vận hành và người được giao nhiệm vụ phải áp dụng biện pháp bảo vệ phù hợp, bảo đảm tuân thủ quy định về bảo vệ dữ liệu cá nhân và an ninh mạng.

Điều 7. Quy định về an toàn hoạt động

1. Trung tâm Dữ liệu phải được bố trí, vận hành trong điều kiện bảo đảm an toàn về nhà trạm, môi trường, nguồn điện, điều hòa, phòng cháy, chữa cháy, kiểm soát ra vào và các hệ thống phụ trợ khác, đáp ứng yêu cầu hoạt động liên tục, ổn định và an toàn.

2. Khu vực đặt thiết bị và khu vực kỹ thuật phải bảo đảm khô ráo, sạch sẽ, được kiểm soát nhiệt độ, độ ẩm, bụi, cháy nổ, thấm dột, côn trùng và các yếu tố môi trường có nguy cơ ảnh hưởng đến hoạt động của thiết bị.

3. Hệ thống điện cấp cho Trung tâm Dữ liệu phải có nguồn cấp phù hợp, có thiết bị lưu điện, máy phát điện dự phòng và phương án chuyển đổi nguồn để bảo đảm duy trì hoạt động khi mất điện lưới hoặc xảy ra sự cố điện.

4. Hệ thống phòng cháy, chữa cháy, chống sét, giám sát môi trường và các thiết bị an toàn khác phải được lắp đặt đồng bộ, kiểm tra định kỳ và bảo trì theo quy định; khi phát hiện nguy cơ mất an toàn phải kịp thời xử lý và báo cáo cơ quan có thẩm quyền.

5. Hệ thống camera giám sát, kiểm soát ra vào và các giải pháp an ninh vật lý khác phải hoạt động liên tục, bảo đảm nhận diện, ghi nhận và truy vết được việc ra, vào khu vực hạn chế.

6. Tổ chức, cá nhân khi vào khu vực Trung tâm Dữ liệu phải tuân thủ quy định về đăng ký, kiểm soát phương tiện, thiết bị mang theo, thời gian làm việc và phạm vi tiếp cận; không được tự ý mang vào khu vực kiểm soát các thiết bị, vật dụng có nguy cơ gây mất an toàn hoặc ảnh hưởng đến hệ thống.

7. Đơn vị vận hành có trách nhiệm theo dõi thường xuyên các thông số kỹ thuật, tình trạng môi trường, trạng thái nguồn điện, thiết bị phụ trợ và an ninh vật lý; kịp thời phát hiện, cảnh báo, cô lập và xử lý sự cố để hạn chế tối đa ảnh hưởng đến hoạt động của Trung tâm Dữ liệu.

Điều 8. Quản lý thiết bị

1. Thiết bị công nghệ thông tin, thiết bị phụ trợ và các tài sản kỹ thuật khác sử dụng tại Trung tâm Dữ liệu phải được thống kê, phân loại, ghi mã, gắn nhãn và quản lý theo danh mục tài sản.

2. Đơn vị vận hành có trách nhiệm theo dõi tình trạng sử dụng, thời hạn bảo hành, lịch sử sửa chữa, thay thế, bảo trì và mức độ quan trọng của từng thiết bị; định kỳ kiểm kê, đánh giá và báo cáo cơ quan quản lý theo quy định.

3. Thiết bị đưa vào sử dụng tại Trung tâm Dữ liệu phải bảo đảm phù hợp với tiêu chuẩn kỹ thuật, yêu cầu an toàn và khả năng vận hành của hệ thống; việc mua sắm, điều chuyển, thay thế hoặc thanh lý phải thực hiện theo đúng thẩm quyền và quy định của pháp luật.

4. Khi thiết bị hỏng, suy giảm chất lượng hoặc có nguy cơ ảnh hưởng đến hoạt động của hệ thống, đơn vị vận hành phải kịp thời kiểm tra, cô lập, sửa chữa hoặc thay thế; đối với thiết bị quan trọng phải báo cáo ngay cơ quan quản lý để xử lý theo phương án ưu tiên.

5. Thiết bị lưu trữ, thiết bị có khả năng chứa dữ liệu, phương tiện sao lưu, thiết bị di động và thiết bị đầu cuối trước khi chuyển giao, thanh lý, sửa chữa bên ngoài hoặc hủy bỏ phải được xóa dữ liệu an toàn, bảo đảm không thể khôi phục trái phép.

6. Việc mang thiết bị ra khỏi khu vực Trung tâm Dữ liệu để bảo trì, bảo hành hoặc xử lý kỹ thuật phải được đăng ký, kiểm soát, giám sát và có biên bản bàn giao, nhận lại theo quy trình đã được phê duyệt.

7. Đơn vị vận hành có trách nhiệm theo dõi hiệu năng, tình trạng hoạt động và nguy cơ lỗi của thiết bị để chủ động kiến nghị bảo trì, nâng cấp, thay thế hoặc bổ sung khi cần thiết nhằm bảo đảm hoạt động liên tục của Trung tâm Dữ liệu.

Điều 9. Quản lý hệ thống mạng

1. Hệ thống mạng và truyền dẫn của Trung tâm Dữ liệu phải được thiết kế, triển

khai và vận hành bảo đảm hoạt động liên tục, ổn định, an toàn và đáp ứng yêu cầu kết nối, chia sẻ, lưu trữ, xử lý dữ liệu của các hệ thống, ứng dụng và dịch vụ liên quan.

2. Hệ thống mạng phải được phân vùng chức năng rõ ràng, bảo đảm tách biệt các khu vực mạng theo mục đích sử dụng, mức độ an toàn và phạm vi truy cập; mỗi vùng mạng phải có chính sách kiểm soát riêng về địa chỉ, kết nối, truy cập và giám sát.

3. Việc kết nối giữa Trung tâm Dữ liệu với mạng chuyên dùng, mạng nội bộ, mạng diện rộng, kết nối từ xa và các hệ thống ngoài Trung tâm Dữ liệu phải được kiểm soát, phê duyệt và ghi nhật ký; không được tự ý mở kết nối khi chưa bảo đảm điều kiện về an ninh mạng.

4. Hệ thống mạng phải có giải pháp bảo vệ trước nguy cơ tấn công, xâm nhập trái phép, lây nhiễm mã độc, phát tán dữ liệu và các nguy cơ mất an toàn khác; đồng thời phải có cơ chế giám sát, cảnh báo và phát hiện bất thường trong lưu lượng, kết nối và truy cập.

5. Việc cấu hình, thay đổi, nâng cấp, bổ sung hoặc loại bỏ thiết bị mạng, đường truyền và dịch vụ truyền dẫn phải được thực hiện theo thẩm quyền, quy trình kỹ thuật và kế hoạch đã được phê duyệt; các thay đổi quan trọng phải được thử nghiệm, ghi nhận và kiểm tra lại trước khi đưa vào vận hành chính thức.

6. Hệ thống mạng và truyền dẫn phải bảo đảm khả năng dự phòng, chuyển mạch, khôi phục và duy trì dịch vụ khi xảy ra sự cố; đối với hệ thống, dịch vụ trọng yếu phải có phương án dự phòng phù hợp với mức độ quan trọng và yêu cầu liên tục hoạt động.

7. Đơn vị vận hành có trách nhiệm thường xuyên theo dõi hiệu năng, độ ổn định, băng thông, trạng thái kết nối và an toàn của hệ thống mạng; kịp thời phát hiện, khắc phục sự cố và báo cáo cơ quan quản lý khi phát sinh vấn đề vượt quá khả năng xử lý.

Điều 10. Quản lý an ninh mạng trên hạ tầng Trung tâm Dữ liệu

1. Các hệ thống thông tin tại Trung tâm Dữ liệu phải đáp ứng các yêu cầu về tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an ninh mạng theo Luật An ninh mạng số 116/2025/QH15 và các quy định của pháp luật có liên quan.

2. Hệ thống thông tin từ cấp độ 3 trở lên đặt tại Trung tâm Dữ liệu phải được kiểm tra, đánh giá an ninh mạng định kỳ theo Luật An ninh mạng và quy định pháp luật có liên quan; kết quả kiểm tra, đánh giá được tổng hợp, báo cáo cơ quan có thẩm quyền theo quy định.

3. Thiết bị phần cứng, phần mềm hệ thống và ứng dụng trước khi đưa vào vận hành chính thức tại Trung tâm Dữ liệu phải được kiểm tra, đánh giá an ninh mạng theo quy định. Các cơ quan, đơn vị có nhu cầu kết nối hệ thống với Trung tâm Dữ liệu phải chứng minh đã thực hiện các nhiệm vụ hoặc biện pháp bảo vệ an ninh mạng đối với hệ thống theo quy định tại Điều 10 Luật An ninh mạng; việc kết nối được thực hiện khi hệ thống của cơ quan, đơn vị đáp ứng các yêu cầu về bảo đảm an ninh mạng theo quy định; trường hợp chưa đáp ứng, đơn vị vận hành có thể yêu cầu khắc phục, hoàn thiện các điều kiện bảo đảm an ninh mạng trước khi thực hiện kết nối.

4. Việc kết nối, chia sẻ dữ liệu giữa các cơ quan thuộc hệ thống chính trị được

thực hiện thông qua nền tảng tích hợp, chia sẻ dữ liệu của tỉnh hoặc nền tảng, hệ thống kết nối, chia sẻ dữ liệu khác được cấp có thẩm quyền cho phép, phù hợp với Nghị định số 278/2025/NĐ-CP và kiến trúc số của tỉnh; không tự ý thiết lập kết nối riêng lẻ ngoài phạm vi được phê duyệt.

5. Trung tâm Dữ liệu thực hiện kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng theo quy định của cơ quan có thẩm quyền.

Điều 11. Quản trị các hệ thống phần mềm

1. Phần mềm, ứng dụng, nền tảng và cơ sở dữ liệu sử dụng tại Trung tâm Dữ liệu phải được quản lý theo danh mục tài sản phần mềm, trong đó xác định rõ tên phần mềm, chức năng, phiên bản, mức độ quan trọng, phạm vi sử dụng, chủ sở hữu, đơn vị quản lý và tình trạng bản quyền.

2. Việc cài đặt, triển khai, cập nhật, thay thế, gỡ bỏ hoặc tạm dừng phần mềm phải được thực hiện theo đúng thẩm quyền, quy trình kỹ thuật và kế hoạch đã được phê duyệt; không được tự ý cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân hoặc phần mềm chưa được kiểm tra an toàn.

3. Hệ điều hành, phần mềm hệ thống, phần mềm ứng dụng và các thành phần liên quan phải có bản quyền hoặc quyền sử dụng hợp pháp, được cập nhật bản vá, sửa lỗi và khắc phục điểm yếu về an ninh mạng kịp thời; việc cập nhật phải được kiểm tra, sao lưu và ghi nhận đầy đủ trước, trong và sau khi thực hiện.

4. Đơn vị vận hành phải phân loại và đánh giá mức độ rủi ro dựa trên yêu cầu về tính bảo mật, tính toàn vẹn, tính sẵn sàng cho việc sử dụng của tài sản phần mềm để thực hiện các biện pháp quản lý, bảo vệ phù hợp.

5. Cài đặt và sử dụng các hệ thống phần mềm:

a) Đối với phần mềm cài đặt mới tại Trung tâm Dữ liệu:

- Phần mềm trước khi cài đặt phải bảo đảm đã được kiểm thử/vận hành thử và nghiệm thu đưa vào sử dụng;

- Khi cài đặt phải rà quét (scan) virus, mã độc… và sử dụng máy tính có ghi màn hình tất cả quá trình thao tác tại Trung tâm Dữ liệu.

b) Đối với các phần mềm đang sử dụng tại Trung tâm Dữ liệu:

- Các cơ quan, đơn vị, cá nhân chịu trách nhiệm thường xuyên cập nhật thông tin, nội dung thông tin của các hệ thống thông tin, cơ sở dữ liệu, phần mềm chuyên ngành của cơ quan, đơn vị mình; cung cấp thông tin ra ngoài phải đảm bảo các yêu cầu về an toàn, bảo mật, phạm vi cung cấp thông tin, tính đúng đắn, hợp pháp của thông tin.

- Thường xuyên cập nhật các bản vá lỗi đối với hệ điều hành, các phần mềm nền tảng, hệ thống mã nguồn theo khuyến nghị của nhà sản xuất.

6. Đơn vị vận hành có trách nhiệm định kỳ rà soát tình trạng phần mềm, thời hạn bản quyền, phiên bản đang sử dụng, cấu hình hệ thống và mức độ an toàn để kịp thời báo cáo, kiến nghị nâng cấp, thay thế hoặc khắc phục khi cần thiết.

7. Không phát tán, chia sẻ các hệ thống phần mềm tại Trung tâm Dữ liệu dưới bất kỳ hình thức nào khi chưa được sự đồng ý của cơ quan có thẩm quyền.

Điều 12. Quản trị sao lưu, phục hồi dữ liệu

1. Dữ liệu, cấu hình hệ thống, phần mềm, cơ sở dữ liệu và các thành phần quan trọng khác của Trung tâm Dữ liệu phải được sao lưu đầy đủ, định kỳ và có kiểm tra khả năng phục hồi.

2. Đơn vị vận hành có trách nhiệm xây dựng, trình phê duyệt và tổ chức thực hiện quy trình sao lưu, phục hồi dữ liệu phù hợp với mức độ quan trọng của từng hệ thống, từng dịch vụ và từng loại dữ liệu.

3. Dữ liệu phải được phân loại theo mức độ quan trọng, tần suất thay đổi, yêu cầu bảo mật và khả năng khôi phục để xác định phương án sao lưu phù hợp; đối với dữ liệu quan trọng phải có ít nhất một bản sao lưu dự phòng tại vị trí hoặc môi trường lưu trữ độc lập.

4. Việc sao lưu phải bảo đảm tính toàn vẹn, bí mật và khả năng truy xuất của dữ liệu; trường hợp dữ liệu có chứa thông tin cá nhân hoặc dữ liệu nhạy cảm thì phải áp dụng biện pháp bảo vệ phù hợp theo quy định của pháp luật.

5. Đơn vị vận hành phải định kỳ kiểm tra, thử nghiệm phục hồi dữ liệu để bảo đảm bản sao lưu có thể sử dụng được khi xảy ra sự cố; việc kiểm thử phải được ghi nhận, đánh giá và khắc phục các tồn tại nếu có.

6. Trường hợp xảy ra sự cố, mất dữ liệu, hư hỏng dữ liệu hoặc có nguy cơ mất an toàn dữ liệu, đơn vị vận hành phải ưu tiên khôi phục dữ liệu quan trọng, bảo đảm hoạt động liên tục của các dịch vụ thiết yếu và báo cáo cơ quan quản lý theo quy định.

7. Việc lưu trữ, vận chuyển, sao chép, phục hồi và hủy bản sao dữ liệu phải được kiểm soát chặt chẽ, không để lộ lọt, thất thoát hoặc sử dụng trái phép dữ liệu trong bất kỳ trường hợp nào.

Điều 13. Quản lý hồ sơ

1. Danh sách các loại hồ sơ lưu trữ:

a) Quy định về quản lý, triển khai, vận hành các hệ thống.

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

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

d) Hồ sơ thiết kế, thuyết minh kỹ thuật.

đ) Hồ sơ quản trị các hệ thống thông tin.

e) Hồ sơ lưu các dịch vụ cung cấp.

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

h) Tài liệu, biên bản kiểm tra, đánh giá của Trung tâm Dữ liệu.

i) Báo cáo quản trị hệ thống, nhật ký vận hành hệ thống.

k) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ được lập, cập nhật, quản lý và lưu trữ dưới dạng giấy hoặc điện tử theo quy định của pháp luật về lưu trữ, giao dịch điện tử, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và quy định có liên quan.

Điều 14. Xử lý sự cố

1. Khi phát hiện có sự cố, người sử dụng hoặc cán bộ vận hành, cán bộ trực hệ thống có trách nhiệm báo cáo kịp thời cho lãnh đạo đơn vị vận hành, lãnh đạo cơ quan quản lý để kiểm tra, xử lý, khắc phục theo quy trình đã được phê duyệt.

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

a) Các sự cố thông thường *(không gây ảnh hưởng đến hoạt động của Trung tâm Dữ liệu),* đơn vị vận hành nhanh chóng 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 gây ảnh hưởng trực tiếp đến hoạt động của Trung tâm Dữ liệu),* ngay sau khi phát hiện sự cố, đơn vị vận hành phải kịp thời cô lập, bảo vệ dữ liệu, đánh giá ảnh hưởng của sự cố, báo cáo cơ quan quản lý để phối hợp, điều phối xử lý.

c) Các sự cố đặc biệt nghiêm trọng *(gây ngưng trệ đến toàn bộ hoạt động của Trung tâm Dữ liệu),* ngay sau khi phát hiện sự cố, đơn vị vận hành phải kịp thời cô lập, bảo vệ dữ liệu, báo cáo cơ quan quản lý đánh giá ảnh hưởng của sự cố, báo cáo UBND tỉnh chỉ đạo để phối hợp, điều phối xử lý.

3. Quy định khắc phục sự cố:

a) Báo cáo kịp thời cơ quan quản lý Trung tâm Dữ liệu với các sự cố nghiêm trọng hoặc đặc biệt nghiêm trọng.

b) Thông báo đến các cơ quan đang khai thác các ứng dụng, dịch vụ của Trung tâm Dữ liệu về thời gian dự kiến hoàn thành xử lý, khắc phục sự cố.

c) Thực hiện sao lưu dữ liệu trước khi khắc phục sự cố.

d) Bảo đảm an toàn cho người và thiết bị hệ thống.

e) Ghi nhật ký diễn biến sự cố, phương án khắc phục.

4. Việc xử lý sự cố phải ưu tiên khôi phục các dịch vụ thiết yếu, phục hồi dữ liệu quan trọng và ghi nhận đầy đủ quá trình xử lý để phục vụ kiểm tra, đánh giá, rút kinh nghiệm sau sự cố.

Điều 15. Bảo trì, bảo dưỡng Trung tâm Dữ liệu

1. Trung tâm Dữ liệu phải được bảo trì, bảo dưỡng định kỳ đối với toàn bộ hạ tầng, thiết bị, phần mềm, hệ thống phụ trợ và các thành phần liên quan nhằm bảo đảm hoạt động liên tục, ổn định và an toàn.

2. Đơn vị vận hành có trách nhiệm xây dựng kế hoạch bảo trì, bảo dưỡng định kỳ, xác định rõ nội dung, thời gian, phạm vi, phương án kỹ thuật và biện pháp bảo đảm an toàn trong quá trình thực hiện; kế hoạch này phải được cơ quan có thẩm quyền xem xét, phê duyệt theo quy định.

3. Việc bảo trì, bảo dưỡng phải thực hiện theo đúng quy trình, có thông báo trước cho các đơn vị, hệ thống bị ảnh hưởng và phải được ghi nhận đầy đủ trước, trong và sau khi thực hiện.

4. Trường hợp bảo trì, bảo dưỡng có nguy cơ làm gián đoạn dịch vụ trọng yếu, đơn vị vận hành phải bố trí phương án dự phòng, thời điểm thực hiện phù hợp và biện pháp giảm thiểu ảnh hưởng đến hoạt động của Trung tâm Dữ liệu.

5. Sau khi hoàn thành bảo trì, bảo dưỡng, đơn vị vận hành phải kiểm tra, chạy thử, xác nhận trạng thái hoạt động và đánh giá mức độ an toàn, ổn định của hệ thống trước khi đưa trở lại vận hành chính thức.

6. Đối với phần mềm, thiết bị, hệ thống có dấu hiệu suy giảm hiệu năng, lỗi kỹ thuật hoặc nguy cơ mất an toàn, đơn vị vận hành phải chủ động đề xuất sửa chữa, thay thế, nâng cấp hoặc điều chỉnh cấu hình kịp thời để bảo đảm hoạt động của Trung tâm Dữ liệu.

7. Việc bảo trì, bảo dưỡng thuê ngoài phải tuân thủ quy định của pháp luật, bảo đảm bảo mật thông tin, an toàn dữ liệu và trách nhiệm của các bên trong suốt quá trình thực hiện.

Điều 16. Quản lý mật khẩu hệ thống Trung tâm Dữ liệu

1. Đơn vị vận hành có trách nhiệm thiết lập, tiếp nhận, quản lý, giám sát sử dụng hệ thống mật khẩu quản trị của Trung tâm Dữ liệu, đảm bảo khả năng truy cập bằng tài khoản quản trị hệ thống ở mức cao nhất trong mọi trường hợp.

2. Mật khẩu sử dụng cho tài khoản truy cập hệ thống, ứng dụng, cơ sở dữ liệu và dịch vụ tại Trung tâm Dữ liệu phải bảo đảm độ dài, độ phức tạp và thời hạn sử dụng phù hợp với mức độ quan trọng của tài khoản:

a) Độ dài của mật khẩu:

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

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

b) Nội dung mật khẩu:

- Không bao gồm các từ dễ nhớ như: Tên, ngày, tháng, năm sinh, số điện thoại.

- Phải bao gồm các loại ký tự sau: Chữ cái in thường, chữ cái in hoa, ký tự đặc biệt, số.

c) Thời gian sử dụng mật khẩu:

Mật khẩu sử dụng cho tài khoản truy cập hệ thống, ứng dụng, cơ sở dữ liệu và dịch vụ tại Trung tâm Dữ liệu phải được thay đổi theo chu kỳ phù hợp với chính sách an ninh mạng, cấp độ hệ thống thông tin và mức độ rủi ro. Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật để bảo đảm an ninh mạng thì Thủ trưởng 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 lưu trữ mật khẩu:

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

- Không lưu mật khẩu dưới dạng văn bản rõ trên bất kỳ tài liệu, tệp tin hay cơ sở dữ liệu nào.

3. Người sử dụng phải thay đổi mật khẩu khi đăng nhập lần đầu, khi hết thời hạn sử dụng, khi có nghi ngờ lộ lọt, hoặc khi có yêu cầu của cơ quan, đơn vị có thẩm quyền.

4. Tài khoản quản trị và tài khoản truy cập vào hệ thống có chứa dữ liệu cá nhân, dữ liệu quan trọng hoặc hệ thống kết nối từ xa phải áp dụng cơ chế bảo vệ tăng cường, bao gồm xác thực đa yếu tố, hạn chế số lần đăng nhập sai và kiểm soát chặt chẽ việc khôi phục mật khẩu.

5. Người sử dụng không được chia sẻ, cho mượn, ghi chép công khai, lưu trữ không an toàn hoặc tiết lộ mật khẩu và thông tin xác thực; mọi hành vi vi phạm phải được ghi nhận và xử lý theo quy định.

6. Đơn vị vận hành có trách nhiệm cấu hình, giám sát, kiểm tra và định kỳ rà soát chính sách mật khẩu; trường hợp phát hiện tài khoản không bảo đảm an toàn phải yêu cầu thay đổi hoặc vô hiệu hóa ngay để bảo vệ hệ thống.

Điều 17. Kiểm soát truy nhập và xác thực

1. Việc cấp, quản lý và thu hồi quyền truy cập đối với Trung tâm Dữ liệu phải bảo đảm đúng người, đúng việc, đúng thẩm quyền và đúng thời hạn sử dụng; mỗi người sử dụng chỉ được cấp một tài khoản, trừ trường hợp đặc biệt do cơ quan có thẩm quyền quyết định.

2. Tài khoản phải được phân quyền theo nguyên tắc tối thiểu cần thiết, phù hợp với chức năng, nhiệm vụ được giao; việc cấp quyền quản trị, quyền truy cập từ xa, quyền khai thác dữ liệu và quyền sử dụng ứng dụng phải được kiểm soát riêng.

3. Hệ thống phải áp dụng cơ chế xác thực an toàn, bao gồm mật khẩu đủ độ mạnh, thay đổi định kỳ, khóa tài khoản khi đăng nhập sai nhiều lần (nhập sai liên tiếp 05 lần trong vòng 30 phút) và các biện pháp xác thực tăng cường đối với tài khoản quản trị hoặc truy cập từ xa. Tài khoản bị khóa chỉ được mở lại thông qua các phương thức xác thực được từng hệ thống quy định.

4. Việc truy cập vào hệ thống, cơ sở dữ liệu, ứng dụng và tài nguyên tại Trung tâm Dữ liệu phải được ghi nhật ký đầy đủ, bảo đảm truy vết được thời điểm, tài khoản, thiết bị, địa chỉ truy cập và thao tác thực hiện.

5. Tài khoản không còn sử dụng, tài khoản hết hạn, tài khoản của người chuyển công tác, thôi việc hoặc thay đổi vị trí công tác phải được thu hồi, vô hiệu hóa hoặc điều chỉnh quyền truy cập kịp thời theo quy định.

6. Trường hợp truy cập từ xa, truy cập qua hạ tầng thuê ngoài hoặc truy cập vào hệ thống liên thông với Trung tâm Dữ liệu, đơn vị vận hành phải áp dụng biện pháp kiểm soát bổ sung phù hợp với mức độ rủi ro, bảo đảm an ninh mạng và bảo vệ dữ liệu cá nhân.

Điều 18. Quản lý tài khoản đặc quyền và giám sát truy cập hệ thống

1. Việc cấp phát, thu hồi, phân quyền tài khoản đặc quyền (tài khoản quản trị máy chủ, mạng, cơ sở dữ liệu) tại Trung tâm Dữ liệu phải được phê duyệt bằng văn bản của Lãnh đạo đơn vị vận hành và tuân thủ nguyên tắc "quyền hạn tối thiểu" (chỉ cấp đúng quyền cần thiết để hoàn thành nhiệm vụ).

2. Mọi phiên truy cập quản trị cấu hình phải được thực hiện qua các hệ thống máy chủ an toàn, có xác thực đa yếu tố.

3. Nhật ký hoạt động của tài khoản đặc quyền và sự kiện an ninh mạng phải được lưu trữ tập trung tại phân hệ độc lập, bảo đảm tính toàn vẹn, chống sửa, xóa trái phép; thời gian lưu trữ tối thiểu 24 tháng hoặc dài hơn theo yêu cầu của pháp luật, cấp độ hệ thống thông tin và phương án bảo vệ được phê duyệt.

Điều 19. Quy định về cung cấp, tiếp nhận máy móc, 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 công nghệ thông tin 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 cung cấp hoặc đặt máy chủ để triển khai ứng dụng trên hạ tầng Trung tâm Dữ liệu: Các cơ quan, đơn vị gửi văn bản đề nghị về Sở Khoa học và Công nghệ xem xét, quyết 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 *(thực hiện từ xa hoặc trực tiếp)* đồng thời tuân thủ các nguyên tắc và đảm bảo an toàn an ninh hệ thống.

Điều 20. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Khi chấm dứt vận hành, thay thế, nâng cấp, thanh lý hoặc hủy bỏ thiết bị, phần mềm, hệ thống hoặc dịch vụ tại Trung tâm Dữ liệu, đơn vị vận hành phải xây dựng phương án xử lý bảo đảm an toàn cho dữ liệu, tài khoản, cấu hình, nhật ký và các thông tin liên quan.

2. Trước khi chuyển giao, sửa chữa, thanh lý hoặc hủy bỏ thiết bị, phương tiện lưu trữ, thiết bị đầu cuối, máy chủ, ổ cứng, thẻ nhớ, USB, băng từ và các thiết bị có khả năng lưu chứa dữ liệu, phải thực hiện xóa dữ liệu an toàn, bảo đảm không thể phục hồi trái phép.

3. Trường hợp thiết bị hoặc phương tiện lưu trữ chứa dữ liệu cá nhân, dữ liệu quan trọng hoặc dữ liệu thuộc phạm vi bí mật nhà nước thì việc xử lý, xóa, tiêu hủy, chuyển giao hoặc hủy bỏ phải tuân thủ quy định pháp luật có liên quan và các biện pháp bảo vệ tương ứng.

4. Đối với thiết bị hỏng phải mang ra ngoài để sửa chữa, bảo hành hoặc giám định, đơn vị vận hành phải kiểm soát chặt chẽ việc bàn giao, niêm phong, vận chuyển và tiếp nhận lại; trường hợp cần thiết phải xóa hoặc gỡ bỏ dữ liệu trước khi chuyển ra ngoài để tránh lộ lọt thông tin.

5. Việc thanh lý, hủy bỏ thiết bị, phần mềm, hệ thống hoặc dữ liệu phải được

lập hồ sơ, biên bản, có xác nhận của các bên có liên quan và lưu trữ theo chế độ quản lý tài sản, quản lý hồ sơ, tài liệu của cơ quan, đơn vị.

6. Đơn vị vận hành có trách nhiệm theo dõi, đánh giá tình trạng thiết bị đến thời điểm kết thúc sử dụng để đề xuất phương án xử lý phù hợp, bảo đảm an toàn kỹ thuật, an ninh mạng và tiết kiệm ngân sách.

7. Quá trình kết thúc vận hành, thanh lý, hủy bỏ không được làm phát sinh nguy cơ mất an toàn cho hệ thống đang hoạt động, không được để sót dữ liệu, tài khoản, khóa mã hóa hoặc thành phần cấu hình có thể gây ảnh hưởng đến Trung tâm Dữ liệu trong giai đoạn tiếp theo.

Điều 21. Kiểm tra, báo cáo định kỳ

1. Công tác kiểm tra

a) Cơ quan quản lý tổ chức kiểm tra định kỳ 6 tháng một lần hoặc kiểm tra đột xuất việc tuân thủ quy định về quản lý, triển khai, vận hành, khai thác Trung tâm Dữ liệu theo Quy chế này.

b) Nội dung kiểm tra bao gồm: Việc bảo đảm các điều kiện về môi trường cho hoạt động của Trung tâm Dữ liệu; tình hình sử dụng thiết bị, ứng dụng của hệ thống; hoạt động của các hệ thống máy chủ, máy trạm, các dịch vụ; tình hình bảo đảm an ninh mạng, đánh giá hiệu quả của hệ thống bảo mật; công tác sao lưu, lưu trữ, phục hồi dữ liệu; công tác quản lý hồ sơ: hồ sơ đầu tư mua sắm, nhật ký vận hành, báo cáo, danh mục thiết bị, ứng dụng, tài khoản, nhân sự, các hoạt động có sự tham gia của các cơ quan, đơn vị khác đối với Trung tâm Dữ liệu; việc tuân thủ các quy định khác nêu tại Quy chế này.

2. Chế độ báo cáo định kỳ về hoạt động của Trung tâm Dữ liệu

a) Tên báo cáo: Báo cáo định kỳ tình hình quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên.

b) Đối tượng thực hiện báo cáo: Đơn vị vận hành Trung tâm Dữ liệu.

c) Cơ quan nhận báo cáo: Cơ quan quản lý Trung tâm Dữ liệu.

d) Tần suất thực hiện báo cáo: Định kỳ 6 tháng.

đ) Nội dung yêu cầu báo cáo: Đánh giá phân tích hiệu quả hoạt động, hiện trạng hạ tầng kỹ thuật, tình hình cung cấp dịch vụ dùng chung và các dịch vụ khác, công tác bảo đảm an ninh mạng, các sự cố kỹ thuật phát sinh và phương án xử lý, định hướng kế hoạch vận hành trong thời gian tiếp theo.

e) Thời gian chốt số liệu báo cáo: Thời gian chốt số liệu 6 tháng đầu năm được tính từ ngày 15 tháng 12 năm trước kỳ báo cáo đến ngày 14 tháng 6 của kỳ báo cáo. Thời gian chốt số liệu 6 tháng cuối năm được tính từ ngày 15 tháng 6 đến ngày 14 tháng 12 của kỳ báo cáo.

g) Thời hạn gửi báo cáo: Đơn vị vận hành gửi báo cáo chậm nhất vào ngày 18 tháng 6 của kỳ báo cáo 6 tháng đầu năm, vào ngày 18 tháng 12 của kỳ báo cáo 6 tháng cuối năm.

h) Phương thức gửi, nhận báo cáo: Báo cáo được thể hiện dưới dạng văn bản điện tử có ký số hợp pháp của đơn vị, gửi qua Hệ thống quản lý văn bản và điều hành của tỉnh.

i) Mẫu đề cương và biểu mẫu số liệu báo cáo tại Phụ lục kèm theo.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 22. Trách nhiệm của Sở Khoa học và Công nghệ

1. Chủ trì, hướng dẫn các cơ quan, đơn vị, tổ chức, cá nhân có liên quan thực hiện Quy chế này, chủ trì tham mưu UBND tỉnh về công tác quản lý, vận hành, khai thác và đảm bảo an ninh mạng cho Trung tâm Dữ liệu.

2. Đảm bảo việc triển khai Trung tâm Dữ liệu và các thành phần hệ thống thuộc Trung tâm Dữ liệu tuân thủ Khung kiến trúc tổng thể quốc gia số, Khung kiến trúc số tỉnh Thái Nguyên và các tiêu chuẩn, quy chuẩn kỹ thuật khác có liên quan.

3. Phê duyệt quy trình vận hành, bảo trì, bảo dưỡng và khắc phục sự cố đối với Trung tâm Dữ liệu.

4. Kiểm tra, giám sát hoạt động của Trung tâm Dữ liệu, chỉ đạo Trung tâm Phát triển Khoa học, Công nghệ và Đổi mới sáng tạo trong công tác quản lý, vận hành, khai thác Trung tâm Dữ liệu và thực hiện kết nối, tích hợp, chia sẻ dữ liệu theo các đề án, chương trình, kế hoạch của Trung ương.

5. Tổng hợp tình hình hoạt động của Trung tâm Dữ liệu, báo cáo Ủy ban nhân dân tỉnh theo quy định.

Điều 23. Trách nhiệm của Công an tỉnh

Theo chức năng, nhiệm vụ và quy định của pháp luật, phối hợp với Sở Khoa học và Công nghệ đảm bảo an ninh mạng cho Trung tâm Dữ liệu, thực hiện kiểm tra, đánh giá an ninh mạng đối với các hệ thống đưa vào triển khai duy trì, vận hành tại Trung tâm Dữ liệu; phối hợp hướng dẫn, đánh giá, ứng phó, xử lý và khắc phục các sự cố về an ninh mạng khi có Chỉ đạo của Chủ tịch UBND tỉnh hoặc đề nghị của Sở Khoa học và Công nghệ.

Điều 24. Trách nhiệm của Sở Tài chính

Trên cơ sở đề xuất dự toán của các sở, ban, ngành và các đơn vị có liên quan để thực hiện Quy chế này, căn cứ các quy định chế độ chi ngân sách hiện hành, quy định về bảo đảm kinh phí thực hiện nhiệm vụ bảo vệ an ninh mạng theo quy định của Luật An ninh mạng; Sở Tài chính tổng hợp, tham mưu UBND tỉnh bố trí dự toán kinh phí ngân sách trong dự toán giao đầu năm của các cơ quan, tổ chức, đơn vị để thực hiện nhiệm vụ theo phân cấp ngân sách.

Điều 25. Trách nhiệm của đơn vị vận hành Trung tâm Dữ liệu

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

2. Ban hành nội quy làm việc; tham mưu ban hành và tổ chức thực hiện các quy trình vận hành, bảo trì, bảo dưỡng và khắc phục sự cố đối với Trung tâm Dữ liệu; xây dựng kế hoạch, bố trí cán bộ trực vận hành hệ thống Trung tâm Dữ liệu 24/24 giờ. Quy định thủ tục chuyển giao thiết bị, quản lý tài sản của Trung tâm Dữ liệu.

3. Đơn vị vận hành phối hợp với các chủ quản hệ thống thông tin rà soát, nâng cấp các biện pháp kỹ thuật và tổ chức bảo vệ an ninh mạng tương ứng với tiêu chuẩn, điều kiện quy định tại Luật An ninh mạng số 116/2025/QH15.

4. Xây dựng lộ trình, chuẩn bị sẵn sàng hạ tầng kết nối kỹ thuật, điều kiện an toàn, an ninh mạng phục vụ việc kết nối, chia sẻ, đồng bộ dữ liệu với Trung tâm dữ liệu quốc gia và các hệ thống dùng chung cấp trung ương theo lộ trình và Kế hoạch triển khai cụ thể của các Bộ, ngành.

5. Thực hiện giám sát thường xuyên hoạt động của hệ thống; kịp thời phát hiện, cảnh báo, ngăn chặn và báo cáo cơ quan quản lý đối với nguy cơ, sự cố hoặc hành vi vi phạm quy định về an ninh mạng, bảo vệ dữ liệu cá nhân trong quá trình vận hành Trung tâm Dữ liệu.

6. Quy hoạch tài nguyên hệ thống, tham mưu cơ quan quản lý các giải pháp, phương án kỹ thuật, kế hoạch phát triển Trung tâm Dữ liệu.

7. Tiếp nhận các yêu cầu cung cấp hạ tầng, dịch vụ của các tổ chức, cá nhân trong phạm vi quy định và triển khai cung cấp theo đúng với tiêu chuẩn chất lượng, quy trình và trên cơ sở khai thác, sử dụng hiệu quả hạ tầng Trung tâm Dữ liệu.

8. Hằng năm, lập dự toán kinh phí bảo đảm duy trì hoạt động, vận hành, bảo dưỡng, sửa chữa, thay thế, nâng cấp trang thiết bị, phần mềm tại Trung tâm Dữ liệu, kinh phí bảo vệ an ninh mạng theo quy định của Luật An ninh mạng và chế độ trực 24/24 giờ cho cán bộ quản trị, vận hành, tổng hợp chung trong dự toán chi nghiệp vụ chuyên môn của đơn vị, trình cấp có thẩm quyền xem xét, quyết định.

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

10. Hướng dẫn, hỗ trợ kỹ thuật cho các cơ quan, đơn vị trong quá trình kết nối, khai thác dữ liệu, sử dụng các nền tảng dùng chung của tỉnh tại Trung tâm Dữ liệu; kịp thời tiếp nhận, phối hợp xử lý vướng mắc kỹ thuật phát sinh.

11. Thực hiện báo cáo định kỳ 6 tháng cho cơ quan quản lý về tình hình hoạt động, cung cấp hạ tầng của Trung tâm Dữ liệu đồng thời xây dựng báo cáo đột xuất khi có yêu cầu.

Điều 26. Trách nhiệm của các cơ quan, tổ chức, cá nhân có kết nối, khai thác, sử dụng dịch vụ của Trung tâm Dữ liệu

1. Tuân thủ các quy định tại Quy chế này và các hướng dẫn khác của cơ quan quản lý, đơn vị vận hành.

2. 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. Sao lưu dữ liệu thường xuyên của đơn vị, theo sự hướng dẫn của đơn vị vận hành.

3. Đảm bảo thực hiện các nhiệm vụ, biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin của mình đặt tại Trung tâm Dữ liệu, đồng thời phối hợp trong công tác kiểm tra, giám sát, xử lý sự cố; chịu trách nhiệm trong phân công, phân quyền cho cán bộ được phép truy cập hệ thống; chịu trách nhiệm khi để lộ, mất quyền kiểm soát tài khoản quản trị gây mất an toàn hệ thống; chịu trách nhiệm về tính chính xác, bảo mật của dữ liệu nghiệp vụ do mình quản lý.

4. Cung cấp 01 đầu mối lãnh đạo và 01 đầu mối kỹ thuật phối hợp với đơn vị vận hành Trung tâm Dữ liệu trong quá trình duy trì hoạt động, quản trị, vận hành, khai thác hệ thống của đơn vị tại Trung tâm Dữ liệu.

Điều 27. Điều khoản thi hành

1. Trường hợp các văn bản quy phạm pháp luật viện dẫn trong Quy chế này được sửa đổi, bổ sung hoặc thay thế thì thực hiện theo quy định, hướng dẫn của các văn bản đã được sửa đổi, bổ sung hoặc thay thế.

2. Trong quá trình triển khai thực hiện Quy chế này, nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung, các cơ quan, đơn vị phản ánh về Sở Khoa học và Công nghệ để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

PHỤ LỤC
MẪU ĐỀ CƯƠNG VÀ BIỂU MẪU SỐ LIỆU BÁO CÁO ĐỊNH KỲ

(Kèm theo Quy chế quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên)

MẪU ĐỀ CƯƠNG BÁO CÁO

Báo cáo tình hình quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh Thái Nguyên 6 tháng đầu năm/cuối năm [năm]

I. TÌNH HÌNH TỔ CHỨC VÀ QUẢN LÝ

1. Công tác chỉ đạo, ban hành văn bản hướng dẫn, quy định liên quan đến quản lý, vận hành Trung tâm Dữ liệu.

2. Tình hình tổ chức bộ máy, nhân sự và phân công nhiệm vụ của đơn vị vận hành Trung tâm Dữ liệu.

3. Công tác phối hợp giữa các đơn vị liên quan (cơ quan quản lý, đơn vị vận hành, các cơ quan, đơn vị khai thác, sử dụng dịch vụ tại Trung tâm Dữ liệu).

II. KẾT QUẢ QUẢN LÝ, VẬN HÀNH HẠ TẦNG KỸ THUẬT

1. Tình hình vận hành các phân hệ: Mạng và truyền dẫn, máy chủ, lưu trữ, cơ sở dữ liệu, phần mềm *(bao gồm cung cấp danh sách các ứng dụng, nền tảng, cơ sở dữ liệu được duy trì, vận hành tại Trung tâm Dữ liệu đến thời điểm báo cáo).*

2. Công tác đảm bảo an ninh mạng: Giám sát, phát hiện và xử lý sự cố về an ninh mạng.

3. Công tác bảo trì, bảo dưỡng hệ thống phụ trợ (điện, điều hòa, phòng cháy chữa cháy, camera giám sát...).

4. Tình hình sao lưu và phục hồi dữ liệu.

III. KẾT QUẢ KHAI THÁC, SỬ DỤNG DỊCH VỤ TẠI TRUNG TÂM DỮ LIỆU

1. Các ứng dụng, dịch vụ dùng chung đã triển khai.

2. Tình hình cung cấp các dịch vụ: Đặt máy chủ, lưu trữ, quản trị ứng dụng…

3. Kết quả kết nối, chia sẻ dữ liệu của các cơ quan, đơn vị tại Trung tâm Dữ liệu.

IV. ĐÁNH GIÁ CHUNG

1. Kết quả đạt được trong 6 tháng.

2. Những khó khăn, vướng mắc trong quá trình quản lý, vận hành và khai thác.

3. Nguyên nhân (chủ quan, khách quan).

V. PHƯƠNG HƯỚNG, NHIỆM VỤ 6 THÁNG TIẾP THEO

1. Kế hoạch trọng tâm cần thực hiện.

2. Các giải pháp tháo gỡ khó khăn, vướng mắc.

3. Kiến nghị, đề xuất (nếu có).

BIỂU MẪU SỐ LIỆU *(kèm theo Báo cáo…)*

(Kỳ báo cáo: 6 tháng đầu năm/cuối năm [năm])

Biểu 01: Tình hình hạ tầng và tài nguyên máy chủ

STT	Loại tài nguyên	Đơn vị	Tổng dung lượng/số lượng	Đã sử dụng	Tỷ lệ sử dụng (%)	Ghi chú
1	Máy chủ vật lý	Chiếc				
2	Máy chủ ảo hóa	Chiếc				
3	Dung lượng lưu trữ	TB				
4	Băng thông Internet	Mbps				
5	…					

Biểu 02: Chỉ số vận hành và bảo đảm an ninh mạng

STT	Chỉ tiêu kỹ thuật	Đơn vị	Số liệu kỳ này	So sánh với kỳ trước	Ghi chú
1	Thời gian hệ thống hoạt động ổn định (Uptime)	%			
2	Số lượng sự cố kỹ thuật phát sinh	Vụ			
3	Số lượng cuộc tấn công mạng bị chặn	Cuộc			
4	Tỷ lệ hệ thống thông tin đã được phê duyệt cấp độ an ninh mạng	%			
5	…				

Biểu 03: Tình hình kết nối, chia sẻ dữ liệu (theo Nghị định số 278/2025/NĐ-CP ngày 22/10/2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị)

STT	Tên cơ sở dữ liệu/Hệ thống	Số lượng kết nối (API)	Lưu lượng giao dịch dữ liệu	Đơn vị khai thác chính
1	…			
2	…			

Biểu 04: Tổng hợp dịch vụ cung cấp

STT	Tên dịch vụ	Số lượng đơn vị sử dụng	Doanh thu/Chi phí (nếu có)	Đánh giá chất lượng
1	Dịch vụ quản trị, vận hành			
2	Dịch vụ thuê máy chủ ảo			
3	…			