ỦY BAN NHÂN DÂN **THÀNH PHỐ ĐỒNG NAI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /2026/QĐ-UBND	*Đồng Nai, ngày tháng năm 2026*

QUYẾT ĐỊNH
BAN HÀNH QUY CHẾ QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU THÀNH PHỐ ĐỒNG NAI

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 Dữ liệu số 60/2024/QH15;

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

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

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

Căn cứ Nghị định 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin.

Căn cứ Nghị định số 165/2025/NĐ-CP ngày 30 tháng 6 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

Căn cứ Nghị định số 194/2025/NĐ-CP ngày 03 tháng 7 năm 2025 của Chính phủ quy định chi tiết một số điều của Luật Giao dịch điện tử về cơ sở dữ liệu quốc gia, kết nối và chia sẻ dữ liệu, dữ liệu mở phục vụ giao dịch điện tử của cơ quan nhà nước;

Căn cứ Nghị định số 278/2025/NĐ-CP ngày 22 tháng 10 năm 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 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;

Căn cứ Thông tư số 42/2025/TT-BKHCN ngày 30 tháng 11 năm 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 /TTr-SKHCN ngày tháng 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 Thành phố Đồng Nai.

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Đồng Nai.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế cho Quy chế quản lý, vận hành và khai thác Trung tâm tích hợp dữ liệu tỉnh Đồng Nai được ban hành kèm theo Quyết định số 40/2019/QĐ-UBND ngày 14/10/2019.

Điều 3. Chánh văn phòng Ủy ban nhân dân thành phố, Giám đốc Sở Khoa học và Công nghệ, Thủ trưởng cơ quan, ban, ngành thành phố, Chủ tịch Ủy ban nhân dân xã, phường và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- TT: Thành ủy, HĐND, UBND TP;
- VP Thành ủy, các Ban đảng;
- UBMTTQVN và các Đoàn thể TP;
- Sở, ban, ngành TP;
- UBND xã, phường;
- Báo và PTTH Đồng Nai;
- Lưu: VT, KGVX.

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

ỦY BAN NHÂN DÂN THÀNH PHỐ ĐỒNG NAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

DỰ THẢO

QUY CHẾ
Quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Đồng Nai

(Ban hành kèm theo Quyết định số /2026/QĐ-UBND ngày…tháng…năm 2026 của UBND Thành phố Đồng Nai)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định việc quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Đồng Nai (gọi tắt là Trung tâm dữ liệu).

2. Quy chế này áp dụng đối với cơ quan Đảng, cơ quan Nhà nước thuộc Ủy ban nhân dân thành phố Đồng Nai, các tổ chức chính trị - xã hội và các tổ chức, cá nhân có liên quan tham gia 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. Chuyển đổi số trong cơ quan nhà nước: Là quá trình thay đổi tổng thể và toàn diện của cơ quan nhà nước về cách thức vận hành, quản lý và cung cấp dịch vụ công dựa trên công nghệ số, dữ liệu số và nền tảng số, nhằm nâng cao hiệu lực, hiệu quả hoạt động và chất lượng phục vụ người dân, doanh nghiệp theo quy định tại Luật Chuyển đổi số số 148/2025/QH15.

2. Hạ tầng kỹ thuật: là tập hợp thiết bị tính toán (máy chủ vật lý, máy chủ ảo, máy trạm), hệ thống lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng).

3. Hệ thống thông tin, cơ sở dữ liệu dùng chung: là tập hợp các phần mềm, nền tảng ứng dụng, hạ tầng kỹ thuật và dữ liệu điện tử được xây dựng, quản lý và khai thác tập trung để có thể ứng dụng trong nhiều cơ quan khác nhau.

4. Trung tâm dữ liệu thành phố Đồng Nai: là hạ tầng kỹ thuật công nghệ thông tin tập trung của thành phố Đồng Nai, được xây dựng nhằm lưu trữ, quản lý, khai thác, vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung của thành phố, phục vụ cho hoạt động của các cơ quan Đảng, cơ quan Nhà nước, các tổ chức chính trị - xã hội trên địa bàn thành phố. Trung tâm dữ liệu thành phố Đồng Nai hiện nay bao

gồm Trung tâm dữ liệu chính và Hệ thống dự phòng nhằm đảm bảo khả năng dự phòng, sao lưu và duy trì hoạt động liên tục của các hệ thống thông tin, cơ sở dữ liệu dùng chung của thành phố.

5. An ninh mạng: là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

6. Cơ quan quản lý, vận hành là Sở Khoa học và Công nghệ - cơ quan được Ủy ban nhân dân thành phố giao trách nhiệm quản lý nhà nước và tổ chức vận hành Trung tâm dữ liệu theo quy định tại Điều 23 Quy chế này. Đơn vị quản trị, vận hành là đơn vị được Sở Khoa học và Công nghệ giao hoặc ủy quyền trực tiếp thực hiện các nhiệm vụ quản trị kỹ thuật, vận hành hằng ngày của Trung tâm dữ liệu theo quy định tại Điều 24 Quy chế này.

Chương II

CÁC QUY ĐỊNH VỀ QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU THÀNH PHỐ

Điều 3. Nguyên tắc về quản lý, vận hành và khai thác Trung tâm dữ liệu

1. Tuân thủ các nguyên tắc, 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 tại các văn bản quy phạm pháp luật và các văn bản liên quan.

2. Bảo đảm các yêu cầu về an ninh mạng theo Luật An ninh mạng số 116/2025/QH15, Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và các quy định liên quan.

3. Việc thiết lập, vận hành hệ thống quản lý an ninh thông tin - ISMS (Information Security Management System) đảm bảo tuân thủ theo tiêu chuẩn quốc tế ISO/IEC 27001 về quản lý bảo mật thông tin và các văn bản pháp lý hiện hành.

4. Việc duy trì, vận hành, nâng cấp Trung tâm dữ liệu phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật tại Thông tư số 42/2025/TT-BKHCN ngày 30 tháng 11 năm 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.

5. Việc quản lý, kết nối và chia sẻ dữ liệu của Trung tâm dữ liệu phải tuân thủ theo Nghị định số 278/2025/NĐ-CP ngày 22 tháng 10 năm 2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị.

6. Việc tạo lập, lưu trữ, chia sẻ dữ liệu số chứa thông tin thuộc phạm vi bí mật Nhà nước được thực hiện theo quy định hiện hành.

7. Cơ quan quản lý, vận hành Trung tâm dữ liệu sử dụng, quản lý tài sản theo đúng các quy định hiện hành về quản lý, sử dụng tài sản công và được phép thuê dịch vụ đảm bảo vận hành các hệ thống thông tin theo quy định của pháp luật nhưng phải dựa trên cơ sở đảm bảo khai thác an toàn, hiệu quả hạ tầng Trung tâm dữ liệu hiện có.

8. Kinh phí bảo đảm cho công tác quản lý, vận hành và khai thác Trung tâm dữ liệu thực hiện theo quy định của Luật Ngân sách nhà nước số 89/2025/QH15 và các văn bản quy phạm pháp luật có liên quan.

9. Bảo đảm mô hình quản trị an ninh mạng theo 3 lớp: cơ quan chủ quản hệ thống thông tin, cơ sở dữ liệu; đơn vị quản trị, vận hành Trung tâm dữ liệu; và bộ phận giám sát an ninh thông tin, nhằm phân định rõ trách nhiệm khi xảy ra sự cố, thẩm quyền phê duyệt thay đổi và trách nhiệm giám sát tuân thủ quy định.

10. Việc ứng dụng trí tuệ nhân tạo trong công tác quản lý, vận hành và khai thác Trung tâm dữ liệu phải tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và bảo vệ dữ liệu cá nhân; không được sử dụng các công cụ, nền tảng trí tuệ nhân tạo để xử lý, lưu trữ dữ liệu thuộc phạm vi bí mật nhà nước hoặc dữ liệu cá nhân khi chưa được cơ quan có thẩm quyền cho phép.

Điều 4. Quy định về quản lý, vận hành và khai thác Trung tâm dữ liệu

1. Quy định vận hành hệ thống:

a) Đảm bảo tất cả các hoạt động của thiết bị phần cứng, phần mềm hệ thống, phần mềm ứng dụng, hệ thống mạng, các hệ thống thông tin, thiết bị phụ trợ tại Trung tâm dữ liệu được hoạt động ổn định, thông suốt liên tục 24 giờ/ngày và 07 ngày/tuần, trừ trường hợp xảy ra sự cố bất khả kháng như thiên tai, hỏa hoạn hoặc các sự kiện ngoài khả năng kiểm soát;

b) Duy trì chế độ trực vận hành và giám sát an ninh thông tin bảo đảm có từ 01 (một) đến 02 (hai) cán bộ kỹ thuật trực tại Trung tâm dữ liệu ngoài giờ hành chính, ngày nghỉ trong tuần, ngày nghỉ lễ, ngày tết;

c) Trong quá trình làm việc và trực vận hành tại Trung tâm dữ liệu phải tuân thủ nghiêm ngặt theo các quy trình, quy định, nội quy lao động;

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

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

e) Hệ thống vận hành tại Trung tâm dữ liệu phải được giám sát liên tục thông qua Trung tâm giám sát an ninh thông tin (SOC) tập trung; bảo đảm các bản ghi nhật ký hệ thống (Log) được đồng bộ thời gian thực và lưu trữ tập trung phục vụ công tác điều tra an ninh mạng khi có yêu cầu.

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

a) Tuân thủ nghiêm theo các quy trình, quy định làm việc, chế độ vào, ra tại Trung tâm dữ liệu;

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

c) 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 hoặc lãnh đạo đơn vị trực tiếp vận hành Trung tâm dữ liệu.

Điều 5. Cung cấp, tiếp nhận các hệ thống thông tin, cơ sở dữ liệu

1. Việc triển khai các dự án, nhiệm vụ ứng dụng công nghệ thông tin và chuyển đổi số tại 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 các hệ thống thông tin, cơ sở dữ liệu để triển khai ứng dụng trên hạ tầng kỹ thuật của Trung tâm dữ liệu: các cơ quan, đơn vị gửi văn bản đề nghị về Sở Khoa học và Công nghệ để xem xét, quyết định theo thẩm quyền; trường hợp vượt thẩm quyền, Sở Khoa học và Công nghệ tổng hợp, trình Ủy ban nhân dân thành phố xem xét, chấp thuận; đồng thời các cơ quan, đơn vị cần đảm bảo an ninh thông tin cấp độ theo quy định cho các hệ thống thông tin, cơ sở dữ liệu của mình triển khai.

3. Cơ quan, đơn vị chịu trách nhiệm quản trị, vận hành hệ thống thông tin, cơ sở dữ liệu của đơn vị mình khi đặt tại Trung tâm dữ liệu thực hiện từ xa hoặc trực tiếp. Cơ quan, đơn vị có thể ủy quyền toàn bộ hoặc một phần nhiệm vụ quản trị, vận hành hệ thống thông tin, cơ sở dữ liệu đặt tại Trung tâm dữ liệu cho cơ quan quản lý, vận hành. Việc ủy quyền phải được thể hiện trên văn bản ký kết, thống nhất giữa hai bên.

4. Trước khi tiếp nhận, đưa vào vận hành chính thức hệ thống thông tin, cơ sở dữ liệu mới tại Trung tâm dữ liệu, cơ quan quản lý, vận hành phối hợp với cơ quan, đơn vị chủ quản hệ thống tổ chức thẩm định an toàn, bao gồm: kiểm thử cấu hình, rà soát lỗ hổng bảo mật, kiểm tra phân quyền truy cập và kiểm tra phương án sao lưu

dữ liệu. Việc nghiệm thu, đưa hệ thống vào vận hành chính thức chỉ được thực hiện khi hệ thống đáp ứng đầy đủ cả yêu cầu về kỹ thuật và yêu cầu về an ninh thông tin.

Điều 6. Quản lý trang thiết bị

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

2. Cơ quan quản lý, vận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị tại Trung tâm dữ liệu hàng năm và báo cáo cơ quan quản lý theo quy định.

3. Việc nâng cấp, mở rộng hoặc sửa chữa, thay thế thiết bị hư hỏng được thực hiện hàng năm bởi cơ quan, quản lý vận hành dựa trên nguồn ngân sách nhà nước cấp hằng năm cho đơn vị.

4. Trường hợp thiết bị hỏng là thiết bị quan trọng gây ảnh hưởng đến hoạt động của Trung tâm dữ liệu; cơ quan quản lý, vận hành phải báo cáo ngay cơ quan quản lý để có biện pháp khắc phục nhanh chóng, kịp thời.

5. Ghi nhật ký, quy định thời gian lưu trữ các thông tin về hoạt động của các thiết bị, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra, giám sát về sau.

Điều 7. Quản lý các hệ thống thông tin, cơ sở dữ liệu

1. Danh sách ứng dụng được lập với các thông tin cơ bản gồm: tên tài sản, giá trị, mức độ quan trọng, mục đích sử dụng, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, nơi lưu giữ.

2. Cơ quan, đơn vị khai thác, vận hành các hệ thống thông tin, cơ sở dữ liệu 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 hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp quản lý, bảo vệ phù hợp.

3. Các phần mềm, ứng dụng sử dụng tại Trung tâm dữ liệu phải có bản quyền và sử dụng theo đúng quy định của pháp luật.

4. Cài đặt và sử dụng các hệ thống thông tin, cơ sở dữ liệu:

a) Đối với hệ thống thông tin, cơ sở dữ liệu cài đặt mới tại Trung tâm dữ liệu: hệ thống thông tin, cơ sở dữ liệu trước khi cài đặt phải đáp ứng được các yêu cầu về kỹ thuật, phù hợp với hồ sơ thiết kế thi công được cơ quan có thẩm quyền phê duyệt; trước khi cài đặt phải đánh giá về an ninh thông tin, kiểm tra, rà quét 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 hệ thống thông tin, cơ sở dữ liệu đang sử dụng tại Trung tâm dữ liệu: các cơ quan, đơn vị chịu trách nhiệm thường xuyên cập nhật thông tin, nội dung thông tin của các hệ thống thông tin, cơ sở dữ liệu 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.

Điều 8. Quản lý hồ sơ

1. Danh sách các loại hồ sơ lưu trữ:

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

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

c) Hồ sơ quản trị các hệ thống thông tin (báo cáo định kỳ, báo cáo sự cố, nhật ký hệ thống, nhật ký hoạt động);

d) Hồ sơ lưu các dịch vụ cung cấp cho khách hàng;

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

e) Tài liệu, biên bản kiểm tra, đánh giá;

g) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ phải được lưu trữ dưới hình thức văn bản, tệp tin điện tử; phải được cập nhật kịp thời khi có sự thay đổi và đảm bảo thời hạn lưu trữ theo quy định của pháp luật chuyên ngành về lưu trữ và an ninh thông tin mạng.

Điều 9. Quản lý mạng truyền số liệu chuyên dùng

1. Cơ quan quản lý, vận hành là đơn vị đầu mối triển khai các ứng dụng hoạt động trên mạng truyền số liệu chuyên dùng thành phố Đồng Nai.

2. Các cơ quan, đơn vị sử dụng mạng truyền số liệu chuyên dùng kết nối với các ứng dụng của Trung tâm dữ liệu phải tuân thủ các quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an ninh thông tin trên mạng truyền số liệu chuyên dùng theo 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.

3. Đơn vị cung cấp dịch vụ viễn thông phải cấu hình mạng truyền số liệu chuyên dùng đảm bảo việc giám sát an ninh thông tin tập trung tại Trung tâm dữ liệu, đồng thời báo cáo tình hình sử dụng mạng truyền số liệu chuyên dùng của các cơ quan, đơn vị gửi cơ quan quản lý, vận hành theo định kỳ tháng, quý, năm.

Điều 10. An toàn hoạt động

1. Cơ quan quản lý, vận hành phải xây dựng và ban hành nội quy làm việc, kế hoạch trực vận hành đối với chuyên viên và được giám sát thường xuyên thông qua hệ thống kiểm soát ra vào.

2. Trung tâm dữ liệu chỉ được thiết lập các thiết bị đang hoạt động, thiết bị chuyên dụng phục vụ vận hành hệ thống, tuyệt đối không đặt các thiết bị không đúng

mục đích sử dụng (các thiết bị hỏng, thiết bị chờ thanh lý, tài liệu, vật tư, vật dụng dễ gây cháy nổ).

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

4. Hệ thống phòng cháy, chữa cháy phải được kiểm tra, thẩm định cấp giấy phép và đảm bảo yêu cầu phòng, chống cháy nổ cho Trung tâm dữ liệu.

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

6. Hệ thống camera thực hiện giám sát toàn bộ Trung tâm dữ liệu liên tục 24/24 giờ; dữ liệu hình ảnh phải được lưu trữ ít nhất trong thời gian là 180 (một trăm tám mươi) ngày.

7. Hệ thống quản lý vào ra (Access Control) hoạt động 24/24 giờ và ghi đầy đủ nhật ký, lưu trữ ít nhất trong thời gian là 180 (một trăm tám mươi) ngày nhằm đảm bảo an ninh, chính xác và linh hoạt cho Trung tâm dữ liệu.

Điều 11. Hệ thống mạng và truyền dẫn

1. Hệ thống mạng phải bảo đảm:

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

b) Áp dụng các giải pháp kiểm soát việc truy cập mạng để đảm bảo các quy định về an ninh, các chính sách bảo mật;

c) Tuân theo các tiêu chuẩn của Trung tâm dữ liệu về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức thi công dây, đấu nối, phân bổ nút mạng;

d) Đối với các kết nối Internet phải có các giải pháp, chính sách bảo mật đảm bảo hệ thống không bị tấn công xâm nhập, lây lan mã độc, phần mềm độc hại từ bên ngoài; ngăn chặn, không để phát tán mã độc, phần mềm độc hại từ các thiết bị ngoại vi hoặc từ mạng cục bộ (LAN) từ các cơ quan, đơn vị;

đ) Đường truyền Internet cho Trung tâm dữ liệu tối thiểu phải từ 02 (hai) nhà cung cấp dịch vụ khác nhau, có giải pháp chia tải, cân bằng tải đường truyền để đảm bảo độ dự phòng cao và tính sẵn sàng cho hệ thống;

e) Chuyên viên quản trị, vận hành hệ thống không được sử dụng trình duyệt hoặc các phần mềm để truy cập Internet từ các máy tính có địa chỉ IP chung hệ thống máy chủ thuộc Trung tâm dữ liệu;

g) Hệ thống mạng không dây (mạng Wifi) tại Trung tâm dữ liệu là đường truyền riêng biệt không có kết nối với hệ thống mạng tại Trung tâm dữ liệu.

2. Cơ quan quản lý, vận hành chịu trách nhiệm giám sát, kiểm tra nội dung và băng thông truy cập, ngăn chặn, đề xuất các biện pháp xử lý các hành vi vi phạm.

Điều 12. Sao lưu, phục hồi dữ liệu

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

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

b) Chu kỳ sao lưu: đối với máy chủ thực hiện sao lưu đầy đủ ít nhất 02 lần/tháng, sao lưu dữ liệu đầy đủ ít nhất 04 lần/tháng; chu kỳ sao lưu dữ liệu thay đổi ít nhất 01 lần/ngày;

c) Đối chiếu, xóa bản sao lưu: đảm bảo nguyên tắc có ít nhất 01 bản sao lưu đầy đủ gần nhất, thực hiện đối chiếu, thử nghiệm khôi phục đảm bảo bản sao lưu hoạt động bình thường khi tiến hành khôi phục;

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

2. Đối với dữ liệu quan trọng sẽ được lưu thêm tại Hệ thống dự phòng để ngăn ngừa, bảo đảm an toàn dữ liệu của hệ thống.

Điều 13. Bảo trì, bảo dưỡng

1. Thực hiện bảo trì, bảo dưỡng:

a) Cơ quan quản lý, vận hành trực tiếp thực hiện hoặc thuê dịch vụ để thực hiện bảo trì, bảo dưỡng các hệ thống;

b) Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến tình hình cung cấp dịch vụ của Trung tâm dữ liệu;

c) 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.

2. Hệ thống điện, lưu điện (UPS):

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi 06 tháng/lần;

b) Các công việc bảo trì, bảo dưỡng hệ thống:

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

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

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

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

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

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

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

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

3. Hệ thống điều hòa, hệ thống thông gió:

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi quý (03 tháng) thực hiện 01 lần.

b) Các công việc bảo trì, bảo dưỡng hệ thống tối thiểu gồm:

- Hệ thống điều hòa:

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

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

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

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

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

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

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

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

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

- Hệ thống phát hiện chất lỏng:

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

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

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

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

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

- Hệ thống giám sát môi trường:

+ Vệ sinh các đầu cảm biến;

+ Kiểm tra tính chính xác của đầu cảm biến;

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

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

4. Hệ thống kiểm soát an ninh:

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi 06 tháng/lần;

b) Các công việc bảo trì, bảo dưỡng hệ thống:

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

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

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

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

5. Hệ thống phòng cháy, chữa cháy:

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi 06 tháng/lần;

b) Các công việc bảo trì, bảo dưỡng hệ thống:

- Vệ sinh công nghiệp toàn bộ hệ thống;

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

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

- Kiểm tra áp suất bình khí chữa cháy;

- Kiểm thử hoạt động của hệ thống chữa cháy;

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

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

6. Hệ thống mạng:

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi quý (03 tháng) thực hiện 01 lần;

b) Các công việc bảo trì, bảo dưỡng hệ thống:

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

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

- Kiểm tra đánh giá tình trạng vật lý thiết bị mạng;

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

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

7. Hệ thống máy chủ:

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi 06 tháng/lần;

b) Các công việc bảo trì, bảo dưỡng hệ thống:

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

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

- Kiểm tra đánh giá tình trạng vật lý máy chủ;

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

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

8. Hệ thống lưu trữ, sao lưu, khôi phục dữ liệu:

a) Tần suất thực hiện bảo trì, bảo dưỡng: tối thiểu mỗi 06 tháng/lần;

b) Các công việc bảo trì, bảo dưỡng hệ thống:

- Vệ sinh công nghiệp toàn bộ hệ thống;

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

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

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

Điều 14. Xử lý sự cố

1. Khi phát hiện có sự cố, cơ quan, đơn vị khai thác, 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 đến hoạt động của hệ thống; đồng thời phải thông báo cho cơ quan, đơn vị quản lý, sử dụng và các cơ quan, đơn vị có liên quan về tình hình sự cố.

2. Phân nhóm sự cố an ninh thông tin mạng được thực hiện theo quy định tại Điều 9 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng

Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an ninh thông tin mạng quốc gia. Trên cơ sở đó, căn cứ thực tế địa phương và mức độ ảnh hưởng của sự cố đối với hoạt động của Trung tâm dữ liệu, tiến hành đánh giá và phân loại sự cố theo 02 (hai) mức, bao gồm: sự cố thông thường và sự cố nghiêm trọng:

a) Đối với các sự cố thông thường (không gây ảnh hưởng đến hoạt động của Trung tâm dữ liệu): cơ quan, đơn vị khai thác, sử dụng dịch vụ nhanh chóng tổ chức xử lý sự cố. Trường hợp không xử lý được, thông báo cho cơ quan quản lý, vận hành để phối hợp giải quyết;

b) Đối với các sự cố nghiêm trọng (gây ảnh hưởng trực tiếp đến hoạt động của Trung tâm dữ liệu): ngay sau khi phát hiện sự cố, cơ quan quản lý, vận hành cần tiến hành các biện pháp khắc phục tạm thời, cô lập, hạn chế thiệt hại, đánh giá ảnh hưởng, đề xuất phương án xử lý sự cố và thực hiện báo cáo lãnh đạo cơ quan quản lý, vận hành để thống nhất, quyết định phương án xử lý.

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

a) Phải tuân thủ quy trình xử lý, khắc phục sự cố theo quy định pháp luật;

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

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

d) Ghi nhật ký sự cố kỹ thuật phát sinh tại chỗ;

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

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

g) Lập báo cáo sự cố báo cáo lãnh đạo cơ quan quản lý, vận hành đối với các sự cố nghiêm trọng và đặc biệt nghiêm trọng trong vòng 24 (hai mươi bốn) giờ kể từ khi phát hiện sự cố;

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

Điều 15. Kiểm tra, báo cáo định kỳ

1. Thực hiện kiểm tra, báo cáo theo định kỳ tháng, quý, năm: cơ quan quản lý, vận hành phải tiến hành kiểm tra định kỳ, đánh giá phân tích hiệu quả hoạt động của Trung tâm dữ liệu và tổng hợp báo cáo.

2. Các nội dung kiểm tra:

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

b) Tình hình sử dụng thiết bị, khai thác ứng dụng của hệ thống;

c) Hoạt động của các hệ thống máy chủ, máy trạm, các dịch vụ (cập nhật nâng cấp, bản vá lỗi, tài nguyên, hiệu năng sử dụng);

d) Tình hình an ninh, bảo mật hệ thống, đánh giá hiệu quả của hệ thống bảo mật;

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

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

3. Cơ quan quản lý, vận hành tổ chức kiểm tra việc tuân thủ các quy định về quản lý kỹ thuật, triển khai, vận hành và khai thác sử dụng Trung tâm dữ liệu theo các quy định tại Quy chế này. Các vấn đề phát hiện sau khi kiểm tra phải được tổng hợp, đánh giá phân tích mức độ ảnh hưởng với hoạt động của Trung tâm dữ liệu và lập kế hoạch khắc phục xử lý.

Điều 16. Quy trình cấp phát hạ tầng phục vụ triển khai hệ thống thông tin, cơ sở dữ liệu

1. Việc cấp phát tài nguyên hạ tầng (máy chủ, hệ điều hành, kết nối mạng, tài nguyên lưu trữ) cho cơ quan, đơn vị có nhu cầu triển khai hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu được thực hiện theo trình tự các bước sau:

a) Bước 1 – Gửi yêu cầu sizing: Cơ quan, đơn vị có nhu cầu gửi văn bản và file yêu cầu cấu hình tài nguyên (sizing) gồm các thông số về CPU, RAM, dung lượng lưu trữ, hệ điều hành, phần mềm dự kiến cài đặt về cơ quan quản lý, vận hành để xem xét, phê duyệt;

b) Bước 2 – Tạo hệ điều hành (OS): Sau khi yêu cầu sizing được phê duyệt, cơ quan quản lý, vận hành tiến hành khởi tạo máy chủ/máy ảo và cài đặt hệ điều hành theo đúng cấu hình đã được phê duyệt;

c) Bước 3 – Gửi yêu cầu VPN: Cơ quan, đơn vị gửi yêu cầu cấp tài khoản, cấu hình kết nối VPN (đối với trường hợp quản trị, vận hành từ xa) để phục vụ việc truy cập, cài đặt hệ thống;

d) Bước 4 – Cấp quyền truy cập cài đặt hệ thống: Cơ quan quản lý, vận hành cấp tài khoản, phân quyền truy cập tương ứng để cơ quan, đơn vị hoặc đầu mối kỹ thuật được chỉ định thực hiện cài đặt, cấu hình hệ thống thông tin, cơ sở dữ liệu;

đ) Bước 5 – Gửi rule firewall: Cơ quan, đơn vị gửi văn bản và danh sách yêu cầu mở rule (luồng kết nối) tường lửa (firewall) phục vụ hoạt động của hệ thống, bao gồm thông tin về địa chỉ IP nguồn, đích, cổng dịch vụ (port), giao thức và mục đích sử dụng;

e) Bước 6 – Bộ phận an ninh thông tin (ANTT) thẩm định rule firewall và cài đặt agent ATTT: Bộ phận ATTT của cơ quan quản lý, vận hành thực hiện rà soát, đánh giá sự phù hợp và mức độ an toàn của các rule firewall được đề nghị trước khi

phê duyệt; đồng thời thực hiện cài đặt các agent/phần mềm giám sát an ninh thông tin trên hệ thống mới trước khi đưa vào vận hành;

g) Bước 7 – Mở rule firewall, công bố (public) hệ thống: Sau khi các rule firewall được phê duyệt và agent ATTT đã được cài đặt, cơ quan quản lý, vận hành thực hiện mở các rule firewall tương ứng và công bố (public) hệ thống để đưa vào khai thác, sử dụng;

h) Bước 8 – Sao lưu (backup) hệ thống: Ngay sau khi hệ thống được đưa vào vận hành, cơ quan quản lý, vận hành thực hiện cấu hình, đưa hệ thống vào danh sách sao lưu định kỳ theo quy định tại Điều 12 Quy chế này.

2. Mỗi bước tại khoản 1 Điều này phải được xác nhận hoàn thành (bằng văn bản, email hoặc trên hệ thống quản lý yêu cầu dịch vụ) trước khi chuyển sang bước tiếp theo; thời gian xử lý yêu cầu cấp phát hạ tầng (từ bước 1 đến bước 7) tối đa là 05 (năm) ngày làm việc theo quy định tại khoản 6 Điều 23 Quy chế này, kể từ khi nhận được đầy đủ thông tin yêu cầu, trừ trường hợp có thỏa thuận khác giữa các bên.

3. Cơ quan quản lý, vận hành có trách nhiệm lưu trữ đầy đủ hồ sơ, văn bản yêu cầu và kết quả xác nhận của từng bước trong quy trình này vào hồ sơ quản trị hệ thống theo quy định tại Điều 8 Quy chế này.

Điều 17. Quản lý thay đổi

1. Quản lý thay đổi là việc kiểm soát các thay đổi đối với hạ tầng kỹ thuật, hệ thống mạng, hệ thống bảo mật, máy chủ, hệ điều hành, phần mềm hệ thống và ứng dụng đang vận hành tại Trung tâm dữ liệu, bao gồm nhưng không hạn chế: thay đổi cấu hình thiết bị, nâng cấp phiên bản, mở/đóng rule firewall, cấp/thu hồi quyền truy cập hệ thống trọng yếu, thay đổi kiến trúc mạng, di chuyển hoặc thay thế thiết bị.

2. Nguyên tắc quản lý thay đổi:

a) Mọi thay đổi phải được lập đề nghị (yêu cầu thay đổi) bằng văn bản hoặc trên hệ thống quản lý yêu cầu, nêu rõ nội dung thay đổi, lý do, phạm vi ảnh hưởng, thời gian dự kiến thực hiện và phương án dự phòng (rollback);

b) Đề nghị thay đổi phải được đánh giá rủi ro và mức độ ảnh hưởng đến hoạt động chung của Trung tâm dữ liệu và các hệ thống thông tin, cơ sở dữ liệu liên quan trước khi phê duyệt;

c) Thay đổi có ảnh hưởng đến hệ thống trọng yếu hoặc có nguy cơ gây gián đoạn dịch vụ phải được lập kế hoạch thực hiện ngoài giờ hành chính hoặc trong khung giờ thấp điểm và thông báo trước cho các cơ quan, đơn vị liên quan;

d) Mọi thay đổi phải được phê duyệt bởi lãnh đạo cơ quan quản lý, vận hành hoặc cấp có thẩm quyền theo phân cấp trước khi triển khai, trừ trường hợp xử lý sự cố khẩn cấp theo quy định tại Điều 14 Quy chế này;

đ) Sau khi thực hiện thay đổi, phải kiểm tra, xác nhận kết quả, cập nhật tài liệu cấu hình, sơ đồ hệ thống liên quan và ghi nhận đầy đủ vào sổ nhật ký hệ thống theo quy định tại Điều 4 Quy chế này;

e) Trường hợp thay đổi gây ra lỗi, sự cố ngoài dự kiến, phải thực hiện ngay phương án dự phòng (rollback) để khôi phục trạng thái hoạt động ổn định của hệ thống và báo cáo theo quy định tại Điều 14 Quy chế này.

3. Cơ quan quản lý, vận hành có trách nhiệm xây dựng, ban hành quy trình quản lý thay đổi (change management) chi tiết, phân loại mức độ thay đổi (thay đổi nhỏ, thay đổi lớn, thay đổi khẩn cấp) và quy định cụ thể về thẩm quyền phê duyệt tương ứng với từng mức độ.

Điều 18. Quản lý năng lực hạ tầng (Capacity Management)

1. Cơ quan quản lý, vận hành có trách nhiệm theo dõi, giám sát thường xuyên mức độ sử dụng tài nguyên của Trung tâm dữ liệu, bao gồm: tài nguyên tính toán (CPU, RAM), dung lượng lưu trữ, băng thông đường truyền, số lượng cổng kết nối mạng, không gian đặt thiết bị (rack, tủ rack) và công suất hệ thống điện, làm lạnh.

2. Định kỳ hàng quý, cơ quan quản lý, vận hành tổng hợp, báo cáo tình hình sử dụng tài nguyên theo khoản 1 Điều này, xác định các thành phần có mức sử dụng vượt ngưỡng cảnh báo (từ 80% công suất thiết kế trở lên) và đề xuất kế hoạch nâng cấp, mở rộng tương ứng.

3. Việc tiếp nhận, phê duyệt cấp phát tài nguyên mới cho các cơ quan, đơn vị theo quy định tại Điều 16 Quy chế này phải được đối chiếu với năng lực hạ tầng hiện có và kế hoạch sử dụng tài nguyên tổng thể của Trung tâm dữ liệu, đảm bảo không gây quá tải, ảnh hưởng đến hoạt động của các hệ thống đang vận hành.

4. Trên cơ sở báo cáo tình hình sử dụng và dự báo nhu cầu tài nguyên, cơ quan quản lý, vận hành tham mưu Ủy ban nhân dân thành phố kế hoạch đầu tư, nâng cấp hạ tầng Trung tâm dữ liệu theo quy định tại khoản 4 Điều 23 Quy chế này, đảm bảo đáp ứng nhu cầu ứng dụng công nghệ thông tin và chuyển đổi số trong trung hạn và dài hạn

Chương III

ĐẢM BẢO AN NINH MẠNG

Điều 19. Yêu cầu bảo đảm an ninh mạng Trung tâm dữ liệu Thành phố Đồng Nai và hệ thống tin kết nối

1. Trung tâm dữ liệu Thành phố Đồng Nai phục vụ các cơ quan nhà nước tại Thành phố Đồng Nai đạt tối thiểu cấp độ 3 theo quy định Nghị định 331/2026/NĐ-CP ngày 19 tháng 8 năm 2016 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin.

2. Hệ thống thông tin kết nối vào Trung tâm dữ liệu Thành phố Đồng Nai phải thực hiện các công việc kết nối để bảo đảm an ninh mạng và triển khai các dịch vụ, ứng dụng của Trung tâm dữ liệu Thành phố Đồng Nai.

3. Hệ thống thông tin phải được triển khai đầy đủ phương án bảo đảm an ninh mạng theo quy định trước khi kết nối vào Trung tâm dữ liệu Thành phố Đồng Nai; được kiểm tra định kỳ theo quy định.

4. Phần vùng mạng tham gia kết nối vào Trung tâm dữ liệu Thành phố Đồng Nai phải được thiết kế phân tách độc lập và có phương án quản lý truy cập với các phần vùng mạng khác.

5. Khi hệ thống thông tin kết nối vào Trung tâm dữ liệu Thành phố Đồng Nai bị phát hiện không bảo đảm an ninh mạng thì đơn vị quản lý, vận hành hệ thống thông tin cần phối hợp thực hiện xử lý theo hướng dẫn của Công an Thành phố, Bộ Công an.

6. Các hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu phải đáp ứng các yêu cầu trong tiêu chuẩn, quy chuẩn kỹ thuật về đảm bảo an ninh mạng theo quy định pháp luật hiện hành.

7. Các hệ thống thông tin, cơ sở dữ liệu thuộc Trung tâm dữ liệu phải được kiểm tra, đánh giá an ninh mạng theo quy định.

8. Hệ thống bảo mật được thiết lập, cấu hình và vận hành theo đúng quy định của pháp luật; đảm bảo việc cập nhật tự động, kịp thời phát hiện các dấu hiệu, hình thức và phương thức tấn công mạng mới. Hệ thống duy trì trạng thái hoạt động ổn định, liên tục nhằm phát hiện, ngăn chặn và xử lý hiệu quả các nguy cơ, hành vi xâm nhập trái phép, qua đó bảo đảm an ninh mạng và bảo mật dữ liệu cho Trung tâm dữ liệu.

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

Điều 20. Công tác giám sát an ninh mạng và kiểm soát truy nhập của Trung tâm dữ liệu Thành phố Đồng Nai

1. Chủ trì phối hợp với các đơn vị có liên quan giám sát trạng thái hoạt động, lưu lượng mạng, cấu hình hiệu năng của cổng kết nối, thiết bị mạng phục vụ kết nối hệ thống thông tin, thông qua sử dụng nền tảng, hệ thống quản lý tập trung, triển khai chia sẻ dữ liệu, giám sát theo yêu cầu.

2. Xác định quyền hạn và trách nhiệm các đơn vị sử dụng hệ thống Trung tâm dữ liệu Thành phố Đồng Nai và đơn vị cung cấp hạ tầng trong hợp đồng cung cấp dịch vụ. Trong đó, quy định nghĩa vụ của các bên phải tuân thủ pháp luật và các quy định đảm bảo an ninh mạng cho hệ thống.

3. Chịu trách nhiệm trước Ủy ban nhân dân Thành phố nếu không thực hiện đúng và đầy đủ quyền hạn và trách nhiệm đã được giao.

4. Cổng kết nối phải có các biện pháp quản lý truy nhập, phát hiện xâm nhập và phòng chống mã độc trên môi trường mạng.

5. Máy chủ, máy trạm và thiết bị công nghệ thông tin khác kết nối vào Trung tâm dữ liệu Thành phố Đồng Nai phải được cài đặt phần mềm phòng chống mã độc và được giám sát an ninh mạng tập trung.

6. Bảo đảm các yêu cầu về dung lượng, tốc độ, chất lượng dịch vụ và an ninh mạng của Trung tâm dữ liệu Thành phố Đồng Nai

7. Thiết lập và đảm bảo duy trì bộ phận tiếp nhận sự cố Trung tâm dữ liệu Thành phố Đồng Nai hoạt động 24/24.

8. Hằng năm (hoặc đột xuất nếu có phản ánh về chất lượng dịch vụ) kiểm tra, khảo sát chất lượng, tốc độ đường truyền nhằm đảm bảo chất lượng cho nhà nước phục vụ cho việc triển khai các ứng dụng công nghệ thông tin của Thành phố.

9. Triển khai các giải pháp, biện pháp cần thiết để ngăn chặn việc sử dụng, lợi dụng mạng lưới, thiết bị, các cổng phụ nhằm cung cấp, phát tán dữ liệu nhiễu, gây rối loạn, làm hư hỏng, hủy hoại hoạt động của Trung tâm dữ liệu Thành phố Đồng Nai.

10. Tổng hợp báo cáo tình hình khai thác, sử dụng Trung tâm dữ liệu Thành phố Đồng Nai gửi Công an thành phố định kỳ 01 lần/năm hoặc đột xuất theo yêu cầu của cơ quan nhà nước cấp trên.

Điều 21. Quản lý mật khẩu

1. Cơ quan quản lý, vận hành Trung tâm dữ liệu có trách nhiệm tiếp nhận mật khẩu quản trị hệ thống sau khi hệ thống được bàn giao và đưa vào sử dụng; sau đó tiến hành bàn giao cho chuyên viên quản trị hệ thống có biên bản kèm theo. Áp dụng phương thức xác thực đa yếu tố (MFA/2FA) bắt buộc đối với toàn bộ tài khoản quản trị hệ thống và các tài khoản truy cập hệ thống trọng yếu.

2. Người sử dụng được giao mật khẩu truy cập hệ thống từ chuyên viên quản trị hệ thống phải thực hiện đổi mật khẩu sau khi tiếp nhận trong vòng 03 (ba) ngày. Việc đổi mật khẩu phải tuân thủ theo đúng quy định hướng dẫn về mật khẩu được quy định tại khoản 3 Điều này.

3. Mật khẩu phải bảo đảm độ an toàn về độ phức tạp, thời gian sử dụng:

a) Độ dài của mật khẩu:

- Đối với mật khẩu của cán bộ, công chức, viên chức và người sử dụng (dùng để đăng nhập thư điện tử, ứng dụng nghiệp vụ, máy tính cá nhân) tối thiểu là 08 (tám) ký tự;

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

b) Nội dung mật khẩu:

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

- Không được đặt theo ký tự chữ cái, ký tự chữ số tuần tự hoặc một dãy các ký tự giống nhau (ví dụ: ABCDEFGH, 12345678 hoặc @@@@@@@@@);

- Đối với mật khẩu quản trị hệ thống phải kết hợp các loại ký tự sau: chữ cái in thường (a, b, c), chữ cái in hoa (A, B, C), ký tự số (1, 2, 3) và ký tự đặc biệt (! @ #...).

c) Thời gian sử dụng mật khẩu:

- Đối với mật khẩu của người sử dụng: không bắt buộc thay đổi định kỳ theo thời gian nếu tài khoản đã được kích hoạt xác thực đa yếu tố (MFA); trường hợp tài khoản chưa áp dụng MFA, thực hiện thay đổi mật khẩu định kỳ tối đa 06 (sáu) tháng/lần.

- Đối với mật khẩu của người quản trị hệ thống: bắt buộc kích hoạt xác thực đa yếu tố (MFA/2FA) cho toàn bộ tài khoản quản trị; thực hiện thay đổi mật khẩu định kỳ tối đa 06 (sáu) tháng/lần và bắt buộc thay đổi ngay khi có cảnh báo từ hệ thống giám sát an ninh thông tin về dấu hiệu lộ, lọt hoặc đăng nhập bất thường.

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

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

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

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

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

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

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

- Các tài liệu liên quan đến mật khẩu được bảo quản ở chế độ mật.

Điều 22. Kiểm soát truy cập và xác thực

1. Các nguyên tắc kiểm soát truy cập:

a) Tất cả các hệ thống thông tin tại Trung tâm dữ liệu phải được bảo vệ khỏi truy cập trái phép thông qua chính sách kiểm soát truy cập;

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

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

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

đ) Theo dõi giám sát người sử dụng truy cập vào hệ thống thông tin quan trọng.

2. Cấp phát quyền truy cập từ xa hoặc truy cập trực tiếp để sử dụng và khai thác ứng dụng, tài nguyên của Trung tâm dữ liệu phải đảm bảo chặt chẽ, đúng mục đích sử dụng. Mỗi người dùng, chuyên viên quản trị hệ thống chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

3. Cơ quan quản lý, vận hành có trách nhiệm kiểm tra và vô hiệu tài khoản của chuyên viên quản trị hệ thống trên hệ thống sau khi nhận thông báo từ các cơ quan, đơn vị sử dụng dịch vụ tại Trung tâm dữ liệu khi có chuyên viên quản trị hệ thống không còn làm việc hoặc không còn nhiệm vụ liên quan.

4. Giới hạn số lần đăng nhập không thành công vào hệ thống là 05 (năm) lần. Nếu nhập sai quá số lần cho phép, tài khoản sẽ bị tạm khóa.

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

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 23. Trách nhiệm của Sở Khoa học và Công nghệ

1. Sở Khoa học và Công nghệ là cơ quan chịu trách nhiệm quản lý, vận hành Trung tâm dữ liệu (gọi tắt là cơ quan quản lý, vận hành).

2. Triển khai thực hiện nhiệm vụ của cơ quan quản lý, vận hành Trung tâm dữ liệu theo quy định.

3. Hướng dẫn việc thực hiện các quy định của Quy chế này đến các cơ quan, cán bộ, công chức, viên chức và tổ chức, cá nhân sử dụng dịch vụ Trung tâm dữ liệu.

4. Tham mưu Ủy ban nhân dân thành phố nâng cấp Trung tâm dữ liệu bảo đảm cho việc ứng dụng công nghệ thông tin và xây dựng chính quyền điện tử, chính quyền số của thành phố.

5. Tham mưu Ủy ban nhân dân thành phố phê duyệt chính sách khai thác và sử dụng các dịch vụ của Trung tâm dữ liệu để đáp ứng nhu cầu ứng dụng công nghệ thông tin trên địa bàn thành phố.

6. Tiếp nhận đề nghị cung cấp dịch vụ, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu thành phố và xem xét, quyết định cấp phát phù hợp. Thời gian gửi phản hồi cung cấp dịch vụ, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu

tối đa là 05 (năm) ngày làm việc, kể từ khi nhận được đầy đủ thông tin yêu cầu; thời gian phản hồi thông tin đề nghị khắc phục sự cố tối đa là 01 (một) ngày làm việc.

7. Kiểm tra và giám sát việc vận hành, khai thác dịch vụ, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu.

8. Chịu trách nhiệm về quản lý kỹ thuật, vận hành và khai thác an toàn, có hiệu quả Trung tâm dữ liệu.

9. Ban hành nội quy làm việc tại Trung tâm dữ liệu; xây dựng kế hoạch trực các ngày lễ, ngày tết; xây dựng lịch trực hàng tuần và bố trí cán bộ trực vận hành hệ thống đảm bảo 24 giờ/ngày, 7 ngày/tuần và quy định chế độ trực vận hành, giám sát an ninh thông tin tại Trung tâm dữ liệu ngoài giờ hành chính, ngày nghỉ trong tuần, ngày nghỉ lễ, ngày tết.

10. Bảo đảm các yêu cầu về hạ tầng kỹ thuật, chất lượng dịch vụ, an ninh thông tin và hoạt động thông suốt Trung tâm dữ liệu.

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

12. Trực tiếp tiếp nhận đề nghị khắc phục sự cố từ các cơ quan, đơn vị và thực hiện việc khắc phục sự cố hoặc hướng dẫn thực hiện việc sửa chữa, bảo trì có liên quan đến các dịch vụ, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu. Đồng thời, gửi báo cáo kết quả về cơ quan quản lý để biết. Thời gian phản hồi thông tin đề nghị khắc phục sự cố tối đa là 01 (một) ngày làm việc, kể từ khi nhận đầy đủ thông tin yêu cầu.

13. Xây dựng, ban hành quy trình quản lý và khắc phục sự cố của Trung tâm dữ liệu.

14. Triển khai cung cấp dịch vụ theo đúng với tiêu chuẩn chất lượng, quy trình và trên cơ sở khai thác hiệu quả hạ tầng Trung tâm dữ liệu.

15. Tuân thủ và thực hiện đúng các quy định của Nhà nước, quy định của ngành và các quy định nêu trong Quy chế này.

16. Đề xuất kinh phí cho công tác quản lý kỹ thuật, vận hành và bảo trì, bảo dưỡng Trung tâm dữ liệu về cơ quan quản lý phê duyệt theo quy định.

17. Thực hiện báo cáo định kỳ 06 (sáu) tháng một lần về tình hình hoạt động và cung cấp dịch vụ, hệ thống thông tin, cơ sở dữ liệu của Trung tâm dữ liệu và báo cáo đột xuất khi có yêu cầu. Hàng năm, thực hiện tổng hợp, báo cáo định kỳ hoặc đột xuất về tình hình khai thác, sử dụng và an ninh thông tin tại Trung tâm dữ liệu gửi Ủy ban nhân dân thành phố.

Điều 24. Trách nhiệm của đơn vị quản trị, vận hành

1. Đơn vị quản trị, vận hành chịu trách nhiệm về quản trị, vận hành và khai thác có hiệu quả hoạt động của Trung tâm dữ liệu.

2. Có trách nhiệm khảo sát nhu cầu sử dụng các cơ quan hành chính, sự nghiệp công lập để lập, chấp hành dự toán, thực hiện chế độ kế toán, chịu trách nhiệm quản lý và sử dụng các nguồn tài chính, tài sản và cơ sở vật chất được giao theo quy định của pháp luật.

3. Xây dựng và tham mưu cho cơ quan quản lý ban hành các quy trình cung cấp dịch vụ, các quy trình vận hành, bảo trì, bảo dưỡng, khắc phục sự cố và Quy trình sao lưu, phục hồi dữ liệu của Trung tâm dữ liệu và triển khai thực hiện sau khi được phê duyệt.

4. Có trách nhiệm lập hồ sơ đề xuất thẩm định cấp độ đối với hệ thống thông tin tại Trung tâm dữ liệu theo quy định tại Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ gửi về cơ quan quản lý, cơ quan có thẩm quyền thẩm định xem xét, phê duyệt.

5. Bảo đảm các yêu cầu về hạ tầng kỹ thuật, chất lượng dịch vụ, an ninh thông tin và hoạt động thông suốt của Trung tâm dữ liệu.

6. 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.

7. Phối hợp cung cấp thông tin trong tư vấn, hỗ trợ người dân, doanh nghiệp sử dụng dịch vụ Trung tâm dữ liệu.

8. Xây dựng kế hoạch hợp tác, khai thác Trung tâm dữ liệu với các tổ chức có liên quan và triển khai các nhiệm vụ khác có liên quan.

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

10. Thực hiện báo cáo định kỳ hằng tháng cho cơ quan quản lý về tình hình hoạt động và cung cấp dịch vụ của Trung tâm dữ liệu và báo cáo đột xuất khi có yêu cầu.

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

Điều 25. Trách nhiệm của Công an thành phố

1. Chủ trì, phối hợp với Sở Khoa học và Công nghệ và các cơ quan liên quan tiến hành kiểm tra, đánh giá an ninh mạng định kỳ (hoặc đột xuất) đối với hệ tầng kỹ thuật, các hệ thống thông tin trọng yếu đặt tại Trung tâm dữ liệu; kịp thời phát hiện, kiến nghị khắc phục các lỗ hổng bảo mật và điểm yếu an ninh mạng.

2. Phối hợp với Sở Khoa học và Công nghệ trong công tác phòng chống, ngăn chặn và xử lý các cuộc tấn công mạng quy mô lớn, có chủ đích (APT), mã hóa dữ liệu tống tiền (Ransomware) hướng vào hệ thống nền tảng của thành phố.

3. Phối hợp với Sở Khoa học và Công nghệ thẩm định các yêu cầu về an ninh mạng, an ninh thông tin đối với các hệ thống thông tin, cơ sở dữ liệu lớn trước khi đưa vào vận hành chính thức tại Trung tâm dữ liệu thành phố.

Điều 26. Trách nhiệm của các cơ quan, đơn vị khai thác, sử dụng dịch vụ tại Trung tâm dữ liệu

1. Có trách nhiệm thực hiện theo Quy chế này khi tham gia sử dụng hạ tầng, dịch vụ của Trung tâm dữ liệu và các hướng dẫn khác của cơ quan quản lý, vận hành Trung tâm dữ liệu.

2. Có trách nhiệm rà soát, thông báo về Sở Khoa học và Công nghệ khi chuyên viên quản trị hệ thống không còn làm việc hoặc không còn nhiệm vụ liên quan để thực hiện thu hồi và vô hiệu hóa các tài khoản quản trị hệ thống, đảm bảo an ninh thông tin.

3. Đối với cơ quan, đơn vị đề nghị cấp tài nguyên máy chủ, vị trí đặt máy chủ, thiết bị tại Trung tâm dữ liệu để cài đặt hệ thống thông tin:

a) Có văn bản đề nghị cung cấp dịch vụ, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu thành phố;

b) Đã được phê duyệt hồ sơ đề xuất cấp độ và phương án đảm bảo an ninh thông tin cho hệ thống thông tin, cơ sở dữ liệu; các thiết bị phải được rà quét an ninh thông tin trước khi đặt tại Trung tâm dữ liệu;

c) Cử đầu mối tiếp nhận và vận hành máy chủ, chịu trách nhiệm về việc sử dụng các máy chủ được cấp;

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

đ) Tuân thủ các quy định về an toàn bảo mật thông tin, quản lý vận hành và khai thác Trung tâm dữ liệu;

e) Chịu trách nhiệm giám sát các hệ thống thông tin, cơ sở dữ liệu đặt tại Trung tâm dữ liệu; chịu trách nhiệm về hỏng hóc và thay thế các thiết bị;

g) Phối hợp với cơ quan quản lý, vận hành trong công tác bảo đảm an ninh thông tin.

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

5. Hàng năm, báo cáo tình hình khai thác, sử dụng các dịch vụ Trung tâm dữ liệu trong hoạt động ứng dụng công nghệ thông tin tại đơn vị mình (chậm nhất vào ngày 30 tháng 11 hàng năm) gửi về Sở Khoa học và Công nghệ để tổng hợp, báo cáo, tham mưu, trình Ủy ban nhân dân thành phố xem xét, chỉ đạo kịp thời.

Điều 27. Trách nhiệm của người sử dụng

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

2. Tuân thủ các quy định về an toàn bảo mật thông tin, quản lý, khai thác và vận hành Trung tâm dữ liệu.

3. Không được thực hiện các hành vi đánh cắp, giả mạo tài khoản để truy cập vào các hệ thống thông tin thuộc Trung tâm dữ liệu.

4. Không được sử dụng các công cụ, phần mềm gây mất an toàn hệ thống, ảnh hưởng đến hoạt động chung của Trung tâm dữ liệu.

5. Trường hợp phát sinh sự cố, thông báo cho cán bộ kỹ thuật tại cơ quan để được hướng dẫn và hỗ trợ khắc phục tại chỗ.

6. Phối hợp với cán bộ kỹ thuật của cơ quan quản lý, vận hành trong việc xử lý sự cố và xác nhận kết quả xử lý.

Điều 28. Sửa đổi, bổ sung Quy chế

Trong quá trình triển khai thực hiện Quy chế, nếu có khó khăn, vướng mắc hoặc có vấn đề phát sinh, các cơ quan, đơn vị kịp thời phản ánh về Sở Khoa học và Công nghệ để tổng hợp, tham mưu, trình Ủy ban nhân dân thành phố điều chỉnh, bổ sung Quy chế cho phù hợp với thực tiễn.