ỦY BAN NHÂN DÂN THÀNH PHỐ HUẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 114/2026/QĐ-UBND	*Huế, ngày 04 tháng 11 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Huế

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

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 được sửa đổi, bổ sung bởi Luật số 87/2025/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 số 148/2025/QH15;

Căn cứ Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 165/2025/NĐ-CP 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 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 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 của Chính phủ quy định chi tiết một số điều của Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 224/2026/NĐ-CP của Chính phủ Quy định chi tiết một số điều và biện pháp thi hành Luật Chuyển đổi số;

Căn cứ Nghị định số 330/2026/NĐ-CP của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 331/2026/NĐ-CP của Chính phủ quy định về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 333/2026/NĐ-CP của Chính phủ Quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Quyết định số 33/2025/QĐ-TTg 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 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 42/2025/TT-BKHCN 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;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Huế.

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

Điều 2. Hiệu lực thi hành

Quyết định này có hiệu lực thi hành từ ngày 14 tháng 11 năm 2026.

Điều 3. Trách nhiệm thi hành

Chánh Văn phòng Ủy ban nhân dân thành phố; Giám đốc Sở Khoa học và Công nghệ; Thủ trưởng các sở, ban, ngành thành phố; Chủ tịch Ủy ban nhân dân các phường, xã; Các doanh nghiệp cung cấp dịch vụ mạng truyền số liệu chuyên dùng, dịch vụ kết nối Internet cho Trung tâm dữ liệu thành phố Huế và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Khoa học và Công nghệ (b/c);
- Bộ Công an (b/c);
- TT. Thành ủy;
- TT. HĐND thành phố;
- UBMTTQVN thành phố;
- CT, các PCT UBND thành phố;
- Các sở, ban, ngành thành phố;
- UBND các phường, xã;
- VP.UBND thành phố: CVP, PCVP;
- Cổng Thông tin điện tử thành phố;
- Công báo thành phố;
- Lưu: VT, TTr.

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



Trần Hữu Thùy Giang

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

QUY ĐỊNH
Quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Huế
(Ban hành kèm theo Quyết định số 114/2026/QĐ-UBND)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc quản lý, vận hành và khai thác Trung tâm dữ liệu thành phố Huế (sau đây gọi tắt là Trung tâm dữ liệu). Các nội dung khác không quy định tại Quy chế này thì thực hiện theo quy định của pháp luật hiện hành.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cơ quan Đảng, cơ quan Nhà nước thuộc Ủy ban nhân dân thành phố Huế, 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 3. Giải thích từ ngữ

Trung tâm dữ liệu là một công trình xây dựng, bao gồm hạ tầng kỹ thuật (nhà trạm, hệ thống cáp) và hệ thống máy tính cùng các thiết bị phụ trợ được lắp đặt vào đó để lưu trữ, trao đổi và quản lý tập trung dữ liệu của một hay nhiều tổ chức, cá nhân. Trung tâm dữ liệu bao gồm Trung tâm dữ liệu chính và Trung tâm dữ liệu 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.

Điều 4. Chủ quản, vận hành Trung tâm dữ liệu

1. Cơ quan chịu trách nhiệm quản lý Trung tâm dữ liệu (gọi tắt là cơ quan quản lý): Sở Khoa học và Công nghệ thành phố Huế.

2. Cơ quan trực tiếp quản lý, vận hành và khai thác (gọi tắt là đơn vị quản lý, vận hành): Trung tâm Giám sát, điều hành đô thị thông minh Huế trực thuộc Sở Khoa học và Công nghệ thành phố Huế.

Điều 5. Kiến trúc Trung tâm dữ liệu

1. Phân hệ mạng và truyền dẫn: Bao gồm các kết nối truyền dẫn nội mạng với băng thông từ 10 Gbps đến 20 Gbps, có hệ lên đến 100 Gbps cho các điểm kết nối lớp phân phối và băng thông 1 Gbps đến 10 Gbps cho các kết nối ở lớp truy cập. Việc kết nối Internet cho phép mở rộng khi có nhu cầu. Phân hệ mạng được chia làm nhiều vùng khác nhau, mỗi vùng được áp đặt các chính sách an ninh và truy cập riêng để phục vụ cho các mục đích khác nhau.

2. Phân hệ đảm bảo an toàn an ninh thông tin: Bao gồm các thiết bị tường lửa cho lớp mạng, dữ liệu và lớp ứng dụng, cádạc thiết bị ngăn chặn xâm nhập trái

phép, thiết bị cân bằng tải, phòng chống thất thoát dữ liệu, hệ thống kiểm soát ra/vào, camera giám sát và các ứng dụng an ninh hệ thống, an ninh máy chủ. Mỗi thành phần trong phân hệ an ninh 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.

3. Phân hệ máy chủ: Bao gồm hệ thống máy chủ đã được đầu tư phục vụ cho Chính quyền điện tử, với khả năng sẵn sàng cho việc mở rộng số lượng máy chủ trong tương lai. Hệ thống máy chủ có khả năng cung cấp năng lực tính toán cho nhiều mục đích khác nhau như ứng dụng chuyên ngành, trang thông tin điện tử, cơ sở dữ liệu chuyên ngành,… của thành phố.

4. 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 có trang bị hệ thống lưu trữ phục vụ mục đích sao lưu, đảm bảo phục hồi dữ liệu cho toàn bộ hệ thống. Hệ thống được thiết kế bảo đảm khả năng mở rộng cho việc phát triển dữ liệu trong tương lai.

5. Phân hệ các hệ thống phụ trợ: Bao gồm hệ thống nguồn điện, hệ thống điều hòa chính xác, thiết bị lưu điện, giám sát môi trường, máy phát điện, sàn nâng, hệ thống phòng cháy và chữa cháy và các hệ thống phụ trợ liên quan khác được thiết kế tuân theo tiêu chuẩn TIA-942 - TIER 3 (tiêu chuẩn quốc tế về Trung tâm dữ liệu), bảo đảm các thiết bị luôn được hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

6. 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, địa phương và người dân, doanh nghiệp theo thiết kế được phê duyệt và đảm bảo yêu cầu trước khi đưa vào sử dụng.

7. Phân hệ cơ sở dữ liệu: Bao gồm các phân 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, địa phương và phục vụ người dân, doanh nghiệp đã được Ủy ban nhân dân thành phố phê duyệt và cho phép triển khai.

Điều 6. Nguyên tắc về quản lý 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 toàn thông tin và 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 toàn 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 quy định áp dụng

tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu.

5. Việc kết nối và chia sẻ dữ liệu của Trung tâm dữ liệu phải tuân thủ theo Nghị định số 278/2025/NĐ-CP 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. Trung tâm dữ liệu là hạ tầng phục vụ kết nối và khai thác dữ liệu dùng chung; không thay thế các hệ thống thông tin, cơ sở dữ liệu chuyên ngành của Trung ương và không tự hình thành các chuẩn, cấu trúc dữ liệu hoặc phương thức kết nối riêng khi đã có tiêu chuẩn, quy chuẩn và nền tảng kết nối dùng chung được cơ quan có thẩm quyền ban hành.

8. Kinh phí bảo đảm cho công tác quản lý, khai thác và vận hành 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.

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

Điều 7. Quy định vận hành 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;

b) 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;

c) 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;

d) 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.

2. Quy định đối với tổ chức, cá nhân đến làm việc tại Trung tâm dữ liệu phải tuân thủ nghiêm theo các quy trình, quy định làm việc, chế độ vào, ra tại Trung tâm dữ liệu.

Điều 8. 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. 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 Trung tâm Giám sát, điều hành đô thị thông minh Huế là đơn vị trực tiếp quản lý, vận hành và khai thác. Việc ủy quyền trách nhiệm chủ quản hệ thống thông tin phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi của hệ thống, trách nhiệm của tổ chức được ủy quyền và thời hạn ủy quyền.

3. Ưu tiên cấp phát, đảm bảo tài nguyên hạ tầng (máy chủ, dung lượng lưu trữ, băng thông) đối với các phần mềm dùng chung phục vụ công tác chỉ đạo, điều hành trực tiếp của Ủy ban nhân dân thành phố, đảm bảo hệ thống hoạt động ổn định, không bị nghẽn mạng, gián đoạn trong giờ cao điểm.

Điều 9. 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. Trường hợp thiết bị hỏng là thiết bị quan trọng gây ảnh hưởng đến hoạt động của Trung tâm dữ liệu, đơn vị quản lý, vận hành phải báo cáo ngay cơ quan quản lý để có biện pháp khắc phục nhanh chóng, kịp thời.

3. 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 10. 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; đánh giá về an toàn 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 11. 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;

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 bằng văn bản, tập tin bản mềm và phải được cập nhật khi có sự thay đổi.

Điều 12. Quản lý mật khẩu

1. Đơn vị 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.

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: được thiết lập trên hệ thống định kỳ thay đổi 03 tháng/lần;

- Đối với mật khẩu của người quản trị hệ thống: được thiết lập trên hệ thống định kỳ phải thay đổi 03 tháng/lần;

- Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn thông tin thì lãnh đạo đơn vị 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.

Điều 13. Quản lý mạng truyền số liệu chuyên dùng

1. Đơn vị 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 Huế.

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 toàn thông tin trên mạng truyền số liệu chuyên dùng theo Quyết định số 33/2025/QĐ-TTg 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 toàn 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 theo định kỳ tháng, quý, năm.

Điều 14. An toàn hoạt động

1. Đơn vị 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.

Điều 15. Đảm bảo an toàn thông tin

1. 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 toàn thông tin theo quy định pháp luật hiện hành.

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

3. Hệ thống bảo mật được thiết lập, cấu hình và vận hành theo đúng quy định của pháp luật; bảo đảm 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 toàn thông tin và bảo mật dữ liệu cho Trung tâm dữ liệu.

4. 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 16. 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 toàn thông tin của Trung tâm dữ liệu;

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

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

đ) 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. Đơn vị quản lý, vận hành có trách nhiệm kiểm tra và vô hiệu tài khoản của chuyên viên quản trị viên 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 viên 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.

Điều 17. 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) của 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 tại Trung tâm dữ liệu là đường truyền riêng biệt không có kết nối với hệ thống mạng tại Trung tâm dữ liệu.

2. Đơn vị 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 18. 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, 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. Dữ liệu quan trọng phải được sao lưu tại Trung tâm dữ liệu dự phòng để ngăn ngừa, bảo đảm an toàn dữ liệu của hệ thống.

Điều 19. Bảo trì, bảo dưỡng

1. Thực hiện bảo trì, bảo dưỡng

a) Đơn vị 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, nhật ký 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 20. 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 toàn thông tin mạng được thực hiện theo quy định tại Điều 9 Quyết định số 05/2017/QĐ-TTg ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn 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 đơn vị 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 đơn vị 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 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 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 toàn thông tin, ưu tiên sử dụng cách xử lý sự cố có tính chất tương tự.

Điều 21. Bảo vệ dữ liệu cá nhân và ứng phó sự cố rò rỉ dữ liệu cá nhân

1. Việc thu thập, xử lý, lưu trữ, sử dụng và chia sẻ dữ liệu cá nhân trong quá trình quản lý, vận hành và khai thác Trung tâm dữ liệu phải tuân thủ quy định của Luật Bảo vệ dữ liệu cá nhân và pháp luật có liên quan; bảo đảm nguyên tắc hợp pháp, minh bạch, đúng mục đích, giới hạn phạm vi, chính xác, an toàn và chỉ lưu trữ trong thời gian cần thiết.

2. Cơ quan quản lý, đơn vị quản lý, vận hành có trách nhiệm tổ chức phát hiện, ghi nhận kịp thời sự cố rò rỉ, mất mát, xâm phạm dữ liệu cá nhân; đánh giá phạm vi, mức độ ảnh hưởng và nguy cơ đối với quyền, lợi ích hợp pháp của chủ thể dữ liệu.

3. Khi xảy ra sự cố, đơn vị quản lý, vận hành phải thực hiện ngay các biện pháp cô lập, ngăn chặn, khắc phục sự cố, hạn chế tối đa thiệt hại và ngăn ngừa tái diễn; đồng thời lưu vết, lập hồ sơ sự cố và báo cáo cơ quan quản lý theo quy định.

4. Cơ quan quản lý, đơn vị quản lý, vận hành có trách nhiệm thông báo kịp thời, minh bạch cho người bị ảnh hưởng và cơ quan nhà nước có thẩm quyền về sự cố rò rỉ dữ liệu cá nhân theo quy định của pháp luật; phối hợp với Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội trong phạm vi chức năng, nhiệm vụ để giám sát và bảo vệ quyền, lợi ích hợp pháp của người dân.

5. Sau khi khắc phục sự cố, cơ quan quản lý, đơn vị quản lý, vận hành phải rà soát, đánh giá nguyên nhân, rút kinh nghiệm, hoàn thiện biện pháp bảo vệ dữ liệu cá nhân và báo cáo kết quả xử lý sự cố theo quy định.

Điều 22. Kiểm tra, báo cáo định kỳ

1. Thực hiện kiểm tra, báo cáo theo định kỳ theo năm: đơn vị 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) Công tác sao lưu, lưu trữ, phục hồi dữ liệu;

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

3. Đơn vị 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.

Chương III
TỔ CHỨC THỰC HIỆN

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

1. Triển khai thực hiện nhiệm vụ của cơ quan quản lý Trung tâm dữ liệu theo quy định.

2. 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.

3. 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.

4. Tiếp nhận đề nghị cung cấp dịch vụ, hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu 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.

5. 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.

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

7. 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 tại Trung tâm dữ liệu ngoài giờ hành chính, ngày nghỉ trong tuần, ngày nghỉ lễ, ngày tết.

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

9. 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.

10. 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.

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

12. 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.

13. 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.

14. Tạo điều kiện thuận lợi, hỗ trợ hạ tầng, môi trường kiểm thử cho các đơn vị triển khai hệ thống tại Trung tâm dữ liệu trước khi thực hiện cài đặt mới, nâng cấp, cập nhật, chỉnh sửa các hệ thống trước khi triển khai chính thức.

15. 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.

16. Thực hiện báo cáo định kỳ 01 (một) năm 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 toàn thông tin tại Trung tâm dữ liệu gửi Ủy ban nhân dân thành phố.

Điều 24. 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, đơn vị 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 toàn 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;

b) Đã được phê duyệt hồ sơ đề xuất cấp độ và phương án đảm bảo an toàn thông tin cho hệ thống thông tin, cơ sở dữ liệu; các thiết bị phải được rà quét an toàn 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, đơn vị quản lý, vận hành trong công tác bảo đảm an toàn 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.

4. Trường hợp phát sinh sự cố, phải thông báo ngay cho cán bộ kỹ thuật của đơn vị 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 25. 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. 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.

4. Phối hợp với cán bộ kỹ thuật của đơn vị quản lý, vận hành trong việc xử lý

sự cố và xác nhận kết quả xử lý.

Điều 26. 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./.