BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC CHUYỂN ĐỔI SỐ

Số: 289 /QĐ-CĐS

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 29 tháng 12 năm 2025

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

CỤC TRƯỞNG CỤC CHUYỂN ĐỔI SỐ

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 01/VBHN-BTTTT ngày 13 tháng 02 năm 2023 của Bộ Thông tin và Truyền thông Quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm Dữ liệu;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 223/QĐ-NNMT ngày 01 tháng 3 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Chuyển đổi số;

Căn cứ Quyết định số 1921/QĐ-NNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường;

Theo nghị của Trưởng Phòng An toàn thông tin, Giám đốc Trung tâm Hạ tầng số, Giám đốc Trung tâm Dữ liệu Thông tin phía Nam.

QUYẾT ĐỊNH:

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

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế Quyết định số 87/QĐ-CNTT ngày 20 tháng 5 năm 2019 của Cục trưởng Cục Công nghệ thông

tin và Dữ liệu tài nguyên môi trường về việc ban hành Quy chế quản lý, vận hành, khai thác Trung tâm dữ liệu.

Điều 3. Chánh Văn phòng Cục, Trưởng Phòng An toàn thông tin, Giám đốc Trung tâm Hạ tầng số, Giám đốc Trung tâm Dữ liệu thông tin phía Nam, Thủ trưởng các đơn vị trực thuộc Cục Chuyển đổi số và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thứ trưởng Võ Văn Hưng (để b/c);
- Các đơn vị trực thuộc Bộ (để phối hợp);
- Cục trưởng Lê Phú Hà (để b/c);
- Các Phó Cục trưởng (để chỉ đạo);
- Các đơn vị trực thuộc Cục (để thực hiện);
- Lưu: VT, ATTT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CHUYỂN ĐỔI SỐ
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Nguyễn Bảo Trung

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC CHUYỂN ĐỔI SỐ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY CHẾ
QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU

(Ban hành kèm theo Quyết định số /QĐ - CĐS ngày tháng 12 năm 2025 của Cục trưởng Cục Chuyển đổi số)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về việc quản lý, vận hành và khai thác Trung tâm dữ liệu của Bộ Nông nghiệp và Môi trường do Cục Chuyển đổi số quản lý, vận hành (gọi tắt là Trung tâm dữ liệu) phục vụ hiệu quả các chương trình ứng dụng công nghệ thông tin, chuyển đổi số, phát triển Chính phủ điện tử hướng tới Chính phủ số ngành nông nghiệp và môi trường.

2. Đối tượng áp dụng: Quy chế này áp dụng đối với các đơn vị, cán bộ, công chức, viên chức, người lao động trong các đơn vị thuộc Cục Chuyển đổi số (gọi tắt là Cục); các tổ chức, cá nhân có liên quan tham gia quản lý, vận hành, khai thác và sử dụng dịch vụ của Trung tâm dữ liệu.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *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[1] của một hay nhiều tổ chức, cá nhân. Các Trung tâm dữ liệu của Bộ Nông nghiệp và Môi trường do Cục Chuyển đổi số quản lý, vận hành bao gồm:

- Trung tâm dữ liệu tại trụ sở Bộ, địa chỉ số 10 Tôn Thất Thuyết, Phường Cầu Giấy, Thành Phố Hà Nội.

- Trung tâm dữ liệu tại trụ sở Cục, địa chỉ số 28 Phạm Văn Đồng, Phường Nghĩa Đô, Thành phố Hà Nội.

- Trung tâm dữ liệu dự phòng tại Trung tâm Dữ liệu thông tin phía Nam, địa chỉ số 36 Lý Văn Phức, Phường Tân Định, Thành phố Hồ Chí Minh.

- Trung tâm Dữ liệu vùng đồng bằng sông Cửu Long, địa chỉ số 568 Võ Văn Kiệt, Phường Long Tuyền, Thành phố Cần Thơ.

- Trung tâm dữ liệu khác của Bộ Nông nghiệp và Môi trường được Bộ giao cho Cục Chuyển đổi số quản lý, vận hành và khai thác.

[1] Thông tư 01/VBHN-BTTTT ngày 13 tháng 02 năm 2023 của Bộ Thông tin và Truyền thông Quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm Dữ liệu.

2. *Ứng dụng dùng chung*: Là các phần mềm (hệ thống phần mềm) ứng dụng cung cấp dịch vụ cho các cơ quan, đơn vị, tổ chức, người dân và doanh nghiệp và người sử dụng được Bộ Nông nghiệp và Môi trường thống nhất triển khai đưa vào hoạt động tại Trung tâm dữ liệu.

3. *Mạng diện rộng (sau đây gọi tắt là Mạng WAN)*: Là mạng tin học được thiết lập bằng việc kết nối giữa Trung tâm dữ liệu và mạng nội bộ của các cơ quan, đơn vị trực thuộc Bộ thông qua hạ tầng mạng của nhà cung cấp dịch vụ và cho phép kết nối với mạng của Chính phủ khi có yêu cầu.

4. *Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước*: Là hệ thống thông tin quan trọng quốc gia, được sử dụng trong hoạt động truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước được tổ chức, quản lý thống nhất, bảo đảm chất lượng, an toàn, bảo mật thông tin để trao đổi, chia sẻ dữ liệu giữa các cơ quan Đảng, Nhà nước (sau đây gọi là mạng truyền số liệu chuyên dùng và viết tắt là "mạng TSLCD").

5.*Hạ tầng ảo hóa*: Sử dụng công nghệ ảo hóa để cấp phát tài nguyên tính toán (máy chủ, lưu trữ, mạng...) cho các dịch vụ công nghệ thông tin. Hạ tầng ảo hóa tại các Trung tâm dữ liệu do đơn vị quản lý, vận hành Trung tâm dữ liệu chịu trách nhiệm quản lý.

6. *Tài khoản VPN*: Là tài khoản dùng để đăng nhập vào dịch vụ Mạng Riêng Ảo (Virtual Private Network), cho phép tạo kết nối internet an toàn và riêng tư bằng cách mã hóa dữ liệu và ẩn địa chỉ IP thật của mình. Khi sử dụng tài khoản này, có thể truy cập internet như thể đang ở một địa điểm khác, bảo vệ thông tin cá nhân khỏi các bên thứ ba và truy cập nội dung không bị giới hạn địa lý.

7. *Thiết bị đầu cuối*: Là thiết bị phần cứng đặt ở điểm đầu hoặc điểm cuối của một mạng, có chức năng nhập và hiển thị dữ liệu từ máy tính hoặc hệ thống điện toán, bao gồm (Máy trạm, máy tính xách tay, điện thoại thông minh, máy in, máy quyét,...).

8. *Thiết bị công nghệ thông tin*: Là các thiết bị bao gồm thiết bị đầu cuối, máy chủ, thiết bị kết nối mạng, thiết bị đảm bảo an toàn thông tin, các thiết bị ngoại vi khác đấu nối trực tiếp vào máy tính qua giao diện kết nối mạng, USB và phần mềm hệ thống, phần mềm ứng dụng, phần mềm tiện ích, phần mềm công cụ được cài đặt trên máy tính.

9. *Hạ tầng kỹ thuật của Trung tâm dữ liệu*: Là tập hợp thiết bị công nghệ thông tin (hệ thống máy chủ, thiết bị bảo mật, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị lưu trữ dữ liệu, các thiết bị giám sát…), thiết bị điện (điều hòa chính xác, tủ điện, chống sét, máng cáp điện…), thiết bị phòng cháy, chữa cháy, thiết bị viễn thông, thiết bị ngoại vi, mạng nội bộ, mạng WAN, mạng TSLCD có kết nối với Trung tâm dữ liệu và các thiết bị kỹ thuật chuyên dùng khác.

10. *An toàn an ninh thông tin*: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin trước các nguy cơ tự nhiên hoặc do con người gây

ra. Việc bảo vệ thông tin, thiết bị mạng, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn an ninh thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng theo quy định.

11. *Quyết định số 1921/QĐ-BNNMT*: Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng của Bộ Nông nghiệp và Môi trường.

12. *Quyết định số 114/QĐ-CĐS*: Quyết định số 114/QĐ-CĐS ngày 14 tháng 7 năm 2025 của Cục trưởng Cục Chuyển đổi số ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng của Cục Chuyển đổi số.

Điều 3. Vai trò, chức năng, kiến trúc của Trung tâm dữ liệu

1. Phân công thực hiện các vai trò về quản lý, vận hành và khai thác Trung tâm dữ liệu:

a) Cơ quan chủ quản Trung tâm dữ liệu (gọi tắt là Cơ quan chủ quản): Bộ Nông nghiệp và Môi trường.

b) Cơ quan chịu trách nhiệm quản lý Trung tâm dữ liệu (gọi tắt là cơ quan quản lý); Đơn vị chuyên trách về an toàn thông tin mạng theo quy định: Cục Chuyển đổi số.

c) Đơn vị trực tiếp khai thác, vận hành và quản trị hệ thống Trung tâm dữ liệu (gọi tắt là đơn vị vận hành): Trung tâm Hạ tầng số, Trung tâm Dữ liệu thông tin phía Nam (trực thuộc Cục Chuyển đổi số).

d) Cơ quan, đơn vị tham gia sử dụng hạ tầng, dịch vụ, ứng dụng, hệ thống thông tin đặt Trung tâm dữ liệu (gọi tắt là cơ quan, đơn vị): Các đơn vị, cán bộ, công chức, viên chức, người lao động trong các đơn vị thuộc Cục Chuyển đổi số; các đơn vị trực thuộc Bộ và Cơ quan, đơn vị, tổ chức, cá nhân liên quan tham gia sử dụng hạ tầng, dịch vụ, hệ thống thông tin của Trung tâm dữ liệu.

đ) Phòng An toàn thông tin chịu trách nhiệm là đơn vị đầu mối giúp Cục Chuyển đổi số quản lý việc tiếp nhận, cung cấp hạ tầng, tài nguyên, công tác bảo đảm an toàn an ninh thông tin mạng, chính sách và các báo cáo liên quan Trung tâm dữ liệu theo quy định.

e) Trung tâm Hạ tầng số chịu trách nhiệm quản lý, vận hành hạ tầng Trung tâm dữ liệu tại trụ sở Bộ và trụ sở Cục và là đơn vị đầu mối chủ trì kết nối, vận hành các Trung tâm dữ liệu thuộc chức năng quản lý của Cục Chuyển đổi số.

g) Trung tâm Dữ liệu thông tin phía Nam chịu trách nhiệm quản lý, vận hành hạ tầng Trung tâm dữ liệu tại địa chỉ số 36 Lý Văn Phức, Phường Tân Định, Thành phố Hồ Chí Minh và Trung tâm Dữ liệu vùng đồng bằng sông Cửu Long, địa chỉ số 568 Võ Văn Kiệt, Phường Long Tuyền, Thành phố Cần Thơ (sơ đồ mặt bằng các Trung tâm dữ liệu kèm theo Quy chế này).

2. Trung tâm dữ liệu có chức năng: lưu trữ, xử lý, tích hợp, phân tích, quản lý và chia sẻ cơ sở dữ liệu; hệ thống bảo mật, an toàn dữ liệu; hệ thống phụ trợ; quản lý mạng WAN, mạng TSLCD; các hệ thống thông tin dùng chung; hệ thống thông tin chuyên ngành của các cơ quan, đơn vị và các hệ thống thông tin khác liên quan làm nền tảng số đẩy nhanh quá trình chuyển đổi số, phát triển chính phủ số, kinh tế số và xã hội số ngành Nông nghiệp và Môi trường.

3. Kiến trúc Trung tâm dữ liệu có các phân vùng sau đây:

a) Phân vùng mạng và truyền dẫn: Phân vùng mạng được chia làm nhiều vùng khác nhau, mỗi vùng được thiết lập các chính sách an toàn, an ninh và truy cập riêng để phục vụ các mục đích khác nhau. Trung tâm dữ liệu sử dụng mạng TSLCD để kết nối các mạng nội bộ (LAN), kết nối với Chính phủ, bộ ngành và địa phương với nhau để hình thành mạng diện rộng (WAN) nhằm phục vụ các cơ quan, đơn vị trực thuộc Bộ khai thác các hệ thống cơ sở dữ liệu dùng chung và cơ sở dữ liệu chuyên ngành, sử dụng đường truyền riêng để cung cấp dịch vụ truy cập qua Internet.

b) Phân vùng an toàn an ninh: Bao gồm các thiết bị tường lửa, thiết bị bảo mật cho các lớp mạng và lớp ứng dụng, các thiết bị ngăn chặn xâm nhập trái phép, thiết bị cân bằng tải và các ứng dụng an toàn an ninh hệ thống, an toàn an ninh máy chủ, an toàn dữ liệu. Mỗi thành phần trong phân hệ an toàn 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.

c) Phân vùng máy chủ: Bao gồm các hệ thống máy chủ vật lý độc lập (còn gọi là máy chủ phiến hay Blade Server) được đặt tại Trung tâm dữ liệu với khả năng sẵn sàng cho việc mở rộng số lượng máy chủ vật lý nhằm ảo hóa cung cấp tài nguyên cho Bộ, các cơ quan đơn vị nhà nước trong hoạt động ứng dụng công nghệ thông tin và chuyển đổi số. Hệ thống máy chủ có khả năng cung cấp năng lực xử lý, tính toán cho nhiều nền tảng với nhiều mục đích khác nhau như: Các cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và các hệ thống thông tin khác.

d) Phân vùng lưu trữ: Hệ thống quản trị với năng lực xử lý lưu trữ tập trung ở mức cao, khả năng lưu trữ lớn, có giải pháp sao lưu, phục hồi dữ liệu cho toàn bộ hệ thống. Hệ thống được thiết kế bảo đảm khả năng mở rộng trong gia tăng dữ liệu trong tương lai.

đ) Phân vùng cơ sở dữ liệu: Bao gồm các cơ sở dữ liệu dùng chung và cơ sở dữ liệu chuyên ngành được xây dựng nhằm kết nối, tích hợp, chia sẻ dữ liệu phục vụ ứng dụng công nghệ thông tin và chuyển đổi số trong các cơ quan, đơn vị trực thuộc Bộ, đồng thời phục vụ người dân, doanh nghiệp.

e) Các cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác phục vụ cho việc triển khai các ứng dụng công nghệ thông tin và chuyển đổi số cho các cơ quan quản lý nhà nước của Bộ bao gồm: Nền tảng kết nối, chia sẻ dữ liệu nội bộ (LGSP); Hệ thống Thư điện tử (@mae.gov.vn); Hệ thống Quản lý hồ sơ công việc; Hệ thống Dịch vụ công trực tuyến; Hệ thống cổng

thông tin điện tử và các ứng dụng dùng riêng, ứng dụng chuyên ngành của các cơ quan quản lý nhà nước của Bộ.

f) Phân vùng các hệ thống phụ trợ: Bao gồm hệ thống điện, điều hòa chính xác, thiết bị lưu điện UPS, máy phát điện, sàn nâng, hệ thống phòng cháy - chữa cháy, camera an ninh,... được thiết kế theo tiêu chuẩn quốc gia: TCVN 9250:2021: Trung tâm dữ liệu - Yêu cầu hạ tầng kỹ thuật viễn thông; bảo đảm các thiết bị luôn được hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

4. Các ứng dụng, dịch vụ được cung cấp tại Trung tâm dữ liệu:

a) Các ứng dụng được nhà nước đảm bảo toàn bộ kinh phí hàng năm bao gồm: các ứng dụng dùng chung phục vụ cho việc ứng dụng công nghệ thông tin, phát triển chính phủ điện tử và chuyển đổi số cho các cơ quan quản lý nhà nước của Bộ.

b) Các dịch vụ được cung cấp tại Trung tâm dữ liệu bao gồm: Các ứng dụng, máy chủ vật lý, máy chủ ảo - lưu trữ, lưu ký (Hosting) websites như: Các cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và nhiều hệ thống thông tin khác của các cơ quan quản lý nhà nước của Bộ. Vận hành, kết nối, tích hợp, chia sẻ các cơ sở dữ liệu dùng chung và chuyên ngành phục vụ cho ứng dụng công nghệ thông tin, phát triển chính phủ điện tử, chính phủ số và chuyển đổi số của Bộ Nông nghiệp và Môi trường. Vận hành ứng dụng, tạo lập, số hóa, lưu trữ dữ liệu, quản trị hạ tầng. Rà quét, đánh giá, ứng cứu, khắc phục sự cố bảo mật ứng dụng. Hỗ trợ cung cấp kết nối, chia sẻ dữ liệu. Phân quyền tài nguyên hệ thống, cấp tên miền, địa chỉ IP, an toàn bảo mật. Các dịch vụ khác theo quy định của cơ quan có thẩm quyền.

Điều 4. 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 chính phủ điện tử, chính phủ số và chuyển đổi số theo Luật Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 6 năm 2006 và các văn bản quy phạm pháp luật khác có liên quan.

2. Công tác duy trì, quản lý vận hành, khai thác và nâng cấp Trung tâm dữ liệu phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật sau:

a) Tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu theo Thông tư 01/VBHN-BTTTT ngày 13 tháng 02 năm 2023 của Bộ Thông tin và Truyền thông Quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm Dữ liệu.

b) Việc quản lý, kết nối và chia sẻ dữ liệu của Trung tâm dữ liệu phải tuân thủ theo Nghị định số 47/2020/NĐ-CP ngày 09/04/2020 của Chính phủ về Quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước.

c) Việc tạo lập, lưu trữ, quản lý, chia sẻ dữ liệu số chứa thông tin thuộc phạm vi bí mật Nhà nước được thực hiện theo Luật Bảo vệ bí mật Nhà nước và các văn bản pháp lý hiện hành.

d) Các quy định bảo đảm an toàn thông tin mạng, an ninh mạng đối với Trung tâm dữ liệu theo Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng của Bộ Nông nghiệp và Môi trường ban hành kèm theo Quyết định 1921/QĐ-BNNMT; và Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng của Cục Chuyển đổi số ban hành kèm theo Quyết định 114/QĐ-CĐS; tuân thủ Kiến trúc chính phủ số của Bộ Nông nghiệp và Môi trường.

3. Trung tâm dữ liệu được quản lý thống nhất, tập trung tại Cục Chuyển đổi số bảo đảm tính sẵn sàng, liên tục và an toàn; Mọi hoạt động vận hành, thay đổi cấu hình, bảo trì, cập nhật phần mềm, thiết bị đều phải ghi nhật ký, lưu vết và được phê duyệt; thực hiện bảo đảm an toàn hệ thống theo cấp độ được phê duyệt; định kỳ đánh giá, kiểm tra, cập nhật phương án ứng cứu sự cố; hạ tầng dùng chung được ưu tiên cho các hệ thống thông tin phục vụ chỉ đạo, điều hành, quản lý nhà nước, cung cấp dịch vụ công và chia sẻ dữ liệu liên thông.

4. Các cơ quan, đơn vị và tổ chức, cá nhân tham gia sử dụng dịch vụ Trung tâm dữ liệu phải tuân thủ các quy định của các cơ quan nhà nước về bảo đảm an toàn thông tin và chịu trách nhiệm cho mọi hoạt động trên tài khoản truy cập của mình.

5. Cán bộ kỹ thuật chuyên trách quản lý, vận hành Trung tâm dữ liệu phải luôn đề cao tinh thần trách nhiệm, đảm bảo an toàn và an ninh hệ thống, đảm bảo hệ thống hoạt động 24/24 giờ.

Điều 5. Các hành vi bị nghiêm cấm

1. Mọi hành vi liên quan đến phá hoại cơ sở hạ tầng thông tin, làm gián đoạn hoặc cản trở hoạt động chung của Trung tâm dữ liệu.

2. Sử dụng hoặc phát tán các thông tin cá nhân do Trung tâm dữ liệu nắm giữ vì mục đích vụ lợi, vi phạm quy định pháp luật hiện hành; trừ các yêu cầu đặc biệt của các cơ quan chức năng có thẩm quyền.

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

4. Sử dụng các công cụ, phần mềm có nguy cơ hoặc gây mất an toàn an ninh hệ thống, ảnh hưởng đến hoạt động chung của Trung tâm dữ liệu.

5. Khai thác, sử dụng cơ sở hạ tầng thông tin, dữ liệu, dịch vụ của Trung tâm dữ liệu cho mục đích: phá hoại, lưu trữ, truyền tải các nội dung không phù hợp với thuần phong mỹ tục, trái pháp luật, quy định của Nhà nước; khai thác trái phép các dịch vụ trên mạng Internet và các hoạt động vi phạm khác theo quy định của pháp luật.

Chương II

QUY ĐỊNH VỀ QUẢN LÝ VÀ VẬN HÀNH HẠ TẦNG VẬT LÝ TRUNG TÂM DỮ LIỆU

Điều 6. Quy định về kiểm soát vào, ra và chế độ làm việc tại Trung tâm dữ liệu

Mọi hoạt động vào, ra và chế độ làm việc tại Trung tâm dữ liệu phải được thực hiện theo nội quy quy định vào, ra Trung tâm dữ liệu, được ghi, lưu lại nhật ký và tuân theo các quy định sau:

1. Quy định đối với cơ quan quản lý và đơn vị vận hành:

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 7 ngày/tuần.

b) Duy trì chế độ trực vận hành và giám sát an toàn thông tin, đảm bảo có cán bộ kỹ thuật trực kỹ thuật tại Trung tâm dữ liệu trong và ngoài giờ hành chính (bao gồm: ngày nghỉ trong tuần và các ngày lễ, Tết).

2. Quy định đối với quản trị viên vận hành hệ thống:

a) Trong quá trình làm việc và trực vận hành tại Trung tâm dữ liệu phải tuân thủ nghiêm ngặt các quy trình, quy định, nội quy lao động; đảm bảo nguyên tắc hệ thống hoạt động ổn định và đảm bảo an toàn an ninh thông tin, không xảy ra tình trạng mất kết nối thông tin do nguyên nhân chủ quan của con người.

b) Quản trị viên quản trị, vận hành truy cập, khai thác thông tin tại Trung tâm dữ liệu theo nhiệm vụ, quyền hạn 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, để lộ thông tin ra bên ngoài; không được tự ý can thiệp vào các phần mềm ứng dụng, dữ liệu do các cơ quan, đơn vị khác triển khai tại Trung tâm dữ liệu.

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

3. Quy định đối với cơ quan, đơn vị, 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 Trung tâm dữ liệu - khi đến làm việc phải kê khai đầy đủ thông tin theo mẫu TTDL_BM_01 tại Phụ lục 02 của Quy chế này.

b) Các cơ quan, đơn vị, tổ chức, cá nhân khi đã được sự đồng ý của lãnh đạo cơ quan quản lý Trung tâm dữ liệu đến đăng ký làm việc 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 đến làm việc, thời gian làm việc (có thông tin về căn cước hoặc hộ chiếu kèm theo) và tuân thủ theo các quy định của đơn vị quản lý Trung tâm dữ liệu.

c) Không được tự ý sử dụng, mang theo các thiết bị như: điện thoại, máy tính xách tay, máy tính bảng, 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 hoặc lãnh đạo đơn vị vận hành Trung tâm dữ liệu.

Điều 7. Quy định về bảo đảm an toàn môi trường hoạt động của Trung tâm dữ liệu

1. Tuân thủ Điều 9 Quyết định số 1921/QĐ-BNNMT quy định về quản lý an toàn, an ninh thông tin vật lý đối với Trung tâm dữ liệu.

2. Trung tâm dữ liệu chỉ được đặt các thiết bị đang hoạt động, thiết bị chuyên dụng phục vụ vận hành hệ thống và các thiết bị khác phục vụ hoạt động của Trung tâm dữ liệu. Các thiết bị lỗi, hỏng, thiết bị chờ thanh lý, thiết bị hết khấu hao, tài liệu, vật tư… liên quan đến Trung tâm dữ liệu phải được lưu tại kho riêng không thuộc khu vực hoạt động của các thiết bị tại Trung tâm dữ liệu. Các loại hồ sơ thiết bị, tài liệu vận hành phải được lưu trữ tại tủ hồ sơ của khu vực phòng làm việc của cán bộ quản trị vận hành.

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 rọi trực tiếp. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định.

4. Hệ thống phòng cháy, chữa cháy của Trung tâm dữ liệu phải đảm bảo an toàn về cháy cho nhà và công trình theo quy định tại Thông tư số 06/2022/TT-BXD ngày 30/11/2022 của Bộ trưởng Bộ Xây dựng ban hành QCVN 06:2022/BXD quy chuẩn kỹ thuật quốc gia về an toàn cháy cho nhà và công trình và Thông tư số 09/2023/TT-BXD ngày 16/10/2023 của Bộ trưởng Bộ Xây dựng ban hành sửa đổi 1:2023 QCVN 06:2022/BXD quy chuẩn kỹ thuật quốc gia về an toàn cháy cho nhà và công trình.

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 30 ngày.

7. Các thiết bị, hệ thống đảm bảo điều kiện hoạt động cho Trung tâm dữ liệu phải có khả năng hoạt động liên tục và được kiểm tra, vận hành, bảo trì, bảo dưỡng theo quy trình quy định (theo các quy trình từ TTDL_QT_101 đến TTDL_QT_106 do đơn vị vận hành trung tâm dữ liệu ban hành).

8. Trung tâm dữ liệu phải đảm bảo yêu cầu cơ bản về an toàn vật lý tối thiểu cho hệ thống thông tin theo cấp độ 3 – TCVN 11930:2017 do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 8. Quy định về quản lý trang thiết bị của Trung tâm dữ liệu

1. Trang thiết bị công nghệ thông tin đặt tại Trung tâm dữ liệu phải được đánh số, đặt tên và dán nhãn theo đúng quy định tại Thông tư 01/VBHN-BTTTT ngày 13 tháng 02 năm 2023 của Bộ Thông tin và Truyền thông và Tiêu chuẩn quốc gia: TCVN 9250 - 2021.

2. Việc tiếp nhận, lắp đặt các thiết bị tại Trung tâm dữ liệu phải thực hiện theo quy trình quy định (theo quy trình TTDL_QT_207 tại Phụ lục 01 của Quy chế này).

3. Quá trình lắp đặt, bảo trì, bảo dưỡng thiết bị tại Trung tâm dữ liệu phải được giám sát thực hiện chặt chẽ về mặt thời gian và không gian, đảm bảo không trùng lặp với các công việc khác có liên quan tới hệ thống như: nâng cấp hệ điều hành, cập nhật bản vá, nâng cấp phần mềm hệ thống… nhằm giảm thiểu các rủi ro đối với hệ thống thông tin đang hoạt động.

4. Việc chuyển thiết bị vào hoặc ra Trung tâm dữ liệu phải được thực hiện theo quy định vào, ra Trung tâm dữ liệu và lưu nhật ký tại đơn vị vận hành (theo mẫu TTDL_BM_02 và TTDL_BM_03 tại Phụ lục 02 của Quy chế này).

5. Đơn vị vận hành hàng năm tổng hợp tình hình quản lý, sử dụng thiết bị tại Trung tâm dữ liệu; đề xuất bảo hành, thay thế, sửa chữa các thiết bị công nghệ thông tin và các thiết bị phụ trợ khác trong trường hợp bị hư hỏng và cần nâng cấp.

Điều 9. Quy định về quản lý hệ thống Mạng truyền dẫn của Trung tâm dữ liệu

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 chất lượng băng thông cho các ứng dụng hệ thống.

b) Hệ thống mạng cần quản lý quyền truy cập theo vai trò, nhiệm vụ và mức độ tin cậy nhằm đảm bảo tính bảo mật, hiệu suất cho các thành phần trong hệ thống mạng.

c) 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, các chính sách về an toàn dịch vụ mạng.

d) Tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật của Trung tâm dữ liệu về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức thi công dây, đấu nối, phân bổ nút mạng.

đ) 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 virus, phần mềm độc hại từ bên ngoài; ngăn chặn, không để phát tán virus, phần mềm độc hại từ các thiết bị ngoại vi hoặc từ mạng nội bộ của các cơ quan, đơn vị.

e) Đường truyền Internet cho Trung tâm dữ liệu tối thiểu phải từ 02 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.

g) Cán bộ 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.

h) 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 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.

3. Đơn vị vận hành hàng năm tổng hợp báo cáo, đề xuất Cục về thuê đường truyền Internet để đảm bảo tốc độ, băng thông cho hoạt động của các ứng dụng, hệ thống thông tin đặt tại Trung tâm dữ liệu.

Điều 10. Quy định về quản lý Mạng truyền số liệu chuyên dùng

1. Các cơ quan, đơn vị sử dụng mạng TSLCD kết nối tới 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 TSLCD theo quy định tại: Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ; Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước; Thông tư số 19/2023/TT-BTTTT ngày 25/12/2023 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước; và các quy chế, quy định về bảo đảm an toàn thông tin mạng, an ninh mạng của các cơ quan đơn vị và của Bộ Nông nghiệp và Môi trường.

2. Đơn vị cung cấp dịch vụ viễn thông phải cấu hình mạng TSLCD đảm bảo việc giám sát an toàn, an ninh thông tin tập trung tại Trung tâm dữ liệu, đồng thời báo cáo đột xuất khi có yêu cầu tình hình sử dụng mạng TSLCD của các cơ quan, đơn vị gửi đơn vị vận hành theo định kỳ.

Chương III

QUY ĐỊNH VỀ QUẢN LÝ VÀ KHAI THÁC HẠ TẦNG, HỆ THỐNG ỨNG DỤNG, PHẦN MỀM TRUNG TÂM DỮ LIỆU

Điều 11. Quy định về cung cấp, tiếp nhận thiết bị, phần cứng và phần mềm tại Trung tâm dữ liệu

1. Việc triển khai các dự án, chương trình, 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, phù hợp với kiến trúc chính phủ số của Bộ Nông nghiệp và Môi trường và được cơ quan có thẩm quyền thẩm định, phê duyệt giải pháp kỹ thuật công nghệ.

2. Đối với các cơ quan, đơn vị có nhu cầu: đặt thiết bị công nghệ thông tin, sử dụng hạ tầng ảo hóa hoặc tài nguyên khác để cài đặt phần mềm, cơ sở dữ liệu để triển khai các ứng dụng trên nền tảng hạ tầng kỹ thuật của Trung tâm dữ liệu: Các cơ quan, đơn vị gửi văn bản đề nghị kèm phiếu yêu cầu kỹ thuật theo mẫu về cơ quan quản lý xem xét, quyết định trên cơ sở ý kiến đánh giá đáp ứng hệ

thống tại Trung tâm dữ liệu của đơn vị vận hành (theo mẫu TTDL_QT_413 tại Phụ lục 01 và biểu mẫu TTDL_BM_07 – tại Phụ lục 02 của Quy chế này).

3. Tiếp nhận thiết bị phần cứng và phần mềm của các cơ quan, đơn vị đặt tại Trung tâm dữ liệu:

a) Các cơ quan, đơn vị có máy móc, thiết bị muốn đặt hoặc cài đặt phần mềm tại Trung tâm dữ liệu lập văn bản đề nghị đặt máy chủ, cài đặt phần mềm và bàn giao tài sản tại Trung tâm dữ liệu gửi cơ quan quản lý.

b) Đơn vị quản trị, vận hành có trách nhiệm tiếp nhận máy móc, thiết bị, tiếp nhận cài đặt phần mềm tại Trung tâm dữ liệu theo quy định; quy trình tiếp nhận đặt máy chủ, cài đặt phần mềm và quản lý tài sản theo hướng dẫn của cơ quan quản lý.

c) Các thiết bị, ứng dụng trước khi cài đặt đưa vào sử dụng chính thức tại Trung tâm dữ liệu cần có đơn vị có năng lực chuyên môn đánh giá chi tiết toàn bộ hệ thống đảm bảo an toàn thông tin mạng.

4. Cơ quan, đơn vị chịu trách nhiệm quản trị, vận hành và đảm bảo an toàn thông tin cho các phần mềm, cơ sở dữ liệu, ứng dụng và nguồn tài nguyên đã được cung cấp triển khai tại Trung tâm dữ liệu.

5. Trường hợp đặt máy chủ tại Trung tâm dữ liệu, cơ quan, đơn vị có thể ủy quyền toàn bộ hoặc một phần nhiệm vụ quản trị, vận hành các thiết bị phần cứng, máy chủ cho đơn vị vận hành thông qua văn bản thống nhất hoặc biên bản ký kết giữa hai bên. Theo đó, đơn vị vận hành chịu trách nhiệm quản trị, vận hành máy móc, thiết bị phần cứng, máy chủ; cơ quan, đơn vị chịu trách nhiệm quản trị, vận hành phần mềm, cơ sở dữ liệu, ứng dụng được cài đặt tại Trung tâm dữ liệu.

6. Việc sử dụng các trang thiết bị, máy chủ, hạ tầng ảo hóa và tài nguyên phải đảm bảo tính hiệu lực, hiệu quả và được đánh giá định kỳ hoặc đột xuất. Trong trường hợp các tài nguyên được cung cấp nêu trên không được sử dụng đúng mục đích, hiệu quả, không phát sinh thông tin, dữ liệu,…trong thời gian nhất định theo quy định - đơn vị vận hành sẽ báo cáo cơ quan quản lý gửi thông báo yêu cầu giải trình và tạm khóa hoặc thu hồi các tài nguyên dư thừa hoặc sử dụng không đúng mục đích yêu cầu.

7. Việc quản lý an toàn, an ninh thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin đặt tại Trung tâm dữ liệu tuân thủ Điều 8 Quyết định số 1921/QĐ-BNNMT.

8. Đơn vị vận hành Trung tâm dữ liệu hàng năm lập báo cáo thống kê tình hình sử dụng trang thiết bị, hạ tầng, tài nguyên,… báo cáo cơ quan quản lý và thông báo tới các cơ quan, đơn vị để có kế hoạch sử dụng hiệu quả và đánh giá nhu cầu sử dụng, mở rộng theo kế hoạch để phù hợp với nhu cầu.

Điều 12. Quy định về quản lý, triển khai các hệ thống ứng dụng, phần mềm tại Trung tâm Dữ liệu

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

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

4. Hệ thống máy chủ tên miền (hệ thống DNS): chỉ cung cấp tên miền cho các ứng dụng tại Trung tâm dữ liệu. Trường hợp đặc biệt phải cung cấp tên miền đến địa chỉ IP ngoài Trung tâm dữ liệu phải có ý kiến của cơ quan quản lý và đơn vị sử dụng phải cam kết đảm bảo an toàn an ninh thông tin và chịu trách nhiệm về tên miền được cấp.

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

a) Đối với phần mềm cài đặt mới tại Trung tâm dữ liệu: Quy mô và kiến trúc của phần mềm phải đáp ứng được các yêu cầu về kỹ thuật, phù hợp với hồ sơ thiết kế thi công, phù hợp với kiến trúc chính phủ số của Bộ Nông nghiệp và Môi trường, được cơ quan có thẩm quyền phê duyệt.

b) Trước khi cài đặt phần mềm phải phối hợp với cơ quan quản lý, đơn vị vận hành hoặc đơn vị có năng lực chuyên môn đáp ứng theo quy định tiến hành đánh giá về an toàn thông tin; kiểm tra, rà quét (scan) virus, rà quét mã độc và sử dụng máy tính có ghi màn hình tất cả quá trình thao tác tại Trung tâm dữ liệu; kiểm thử phần mềm trước khi đưa vào sử dụng (theo quy định tại Khoản 2, Điều 13 Quy chế này).

c) Đối với các phần mềm đang sử dụng tại Trung tâm dữ liệu: Các cơ quan, đơn vị chịu trách nhiệm thường xuyên cập nhật thông tin, nội dung của các hệ thống thông tin, cơ sở dữ liệu, phần mềm chuyên ngành của cơ quan, đơn vị; 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.

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

Điều 13. Quy định về vận hành thử hệ thống, kiểm thử phần mềm đặt tại Trung tâm dữ liệu

1. Đối với các máy chủ của các cơ quan đơn vị có nhu cầu đặt tại Trung tâm dữ liệu: trước khi đưa vào sử dụng phải được vận hành thử tại Trung tâm dữ liệu để đánh giá hiệu năng, đánh giá hiệu suất hoạt động và định mức sử dụng

luồng dữ liệu tài nguyên mạng. Việc đánh giá này do đơn vị vận hành chủ trì phối hợp thực hiện.

2. Đối với các phần mềm nội bộ của các cơ quan đơn vị có nhu cầu đặt tại Trung tâm dữ liệu: trước khi đưa vào sử dụng chính thức phải được kiểm thử chấp nhận hoạt động (OAT) bao gồm: kiểm thử hiệu năng; kiểm thử an toàn, bảo mật; kiểm tra về tài liệu vận hành hệ thống (nếu có); kiểm tra một số yếu tố phi chức năng khác như khả năng kết nối, chia sẻ dữ liệu với các hệ thống khác (nếu cần thiết)…theo quy định tại Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông và các quy định về kiểm thử có liên quan. Quá trình kiểm thử do đơn vị vận hành phối hợp với đơn vị có chức năng nhiệm vụ và năng lực đáp ứng yêu cầu triển khai thực hiện.

Điều 14. Quy định về quản lý tài khoản và mật khẩu các hệ thống thông tin tại Trung tâm dữ liệu

1. Tài khoản truy cập vào các hệ thống Trung tâm dữ liệu là tập hợp thông tin định danh (tên đăng nhập & mật khẩu) hoặc thông tin xác thực khác, cho phép người dùng (cá nhân, tổ chức) đăng nhập, sử dụng, xác thực và được phân quyền truy cập vào một hệ thống thông tin, ứng dụng, dịch vụ số hoặc cơ sở dữ liệu cụ thể, nhằm thực hiện các chức năng và truy cập tài nguyên theo quyền hạn được cấp, đảm bảo an toàn và bảo mật; các loại tài khoản truy cập hệ thống Trung tâm dữ liệu bao gồm: tài khoản truy cập hệ thống – quy định tại Điểm a Khoản 1 Điều 10 Quyết định số 114/QĐ-CĐS, tài khoản quản trị hệ thống - quy định tại Điểm b Khoản 1 Điều 10 Quyết định số 114/QĐ-CĐS và tài khoản VPN.

2. Về quản lý an toàn, an ninh thông tin đối với tài khoản truy cập tuân thủ Khoản 1, Khoản 2, Khoản 3, Khoản 4 của Điều 11 Quyết định số 1921/QĐ-BNNMT.

3. Về quản lý an toàn, an ninh thông tin đối với mật khẩu của các tài khoản quản trị hệ thống, tài khoản của người sử dụng cần đảm bảo những yêu cầu tại Khoản 5 Điều 11 Quyết định số 1921/QĐ-BNNMT.

4. Về thời gian sử dụng tài khoản tạm thời (bao gồm tài khoản VPN) cấp cho cơ quan, đơn vị, cá nhân, đối tác và nhà thầu truy cập vào các hệ thống Trung tâm dữ liệu thì qui định thời gian sử dụng sẽ căn cứ vào nội dung, tính chất và thời gian thực hiện công việc giữa các bên liên quan theo qui định và sẽ ngắt tài khoản khi kết thúc công việc.

5. Trường hợp đặc biệt (có thay đổi đối với nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn thông tin), lãnh đạo đơn vị vận hành có thể yêu cầu các đơn vị quản lý vận hành hệ thống thông tin thay đổi mật khẩu của các tài khoản quản trị hệ thống.

6. Đơn vị quản lý vận hành hệ thống thông tin cung cấp mật khẩu quản trị hệ thống thông tin được niêm phong (gọi là mật khẩu niêm phong) và giao lại cho Văn phòng Cục quản lý. Khi có thay đổi mật khẩu quản trị, đơn vị quản lý vận hành hệ thống thông tin cung cấp lại mật khẩu niêm phong mới cho Văn phòng

Cục và nhận lại mật khẩu niêm phong cũ. Mật khẩu niêm phong sẽ được mở và sử dụng trong trường hợp xử lý sự cố về an toàn thông tin và được sự đồng ý của lãnh đạo cơ quan quản lý.

Điều 15. Quy định về bảo trì, bảo dưỡng

1. Đơn vị vận hành thực hiện xây dựng kế hoạch bảo trì, bảo dưỡng Trung tâm dữ liệu hàng năm. Trực tiếp thực hiện hoặc thuê dịch vụ để thực hiện bảo trì, bảo dưỡng Trung tâm dữ liệu.

2. Yêu cầu về bảo trì, bảo dưỡng:

a) Việc thực hiện bảo trì, bảo dưỡng phải hạn chế tối đa ảnh hưởng đến hoạt động của Trung tâm dữ liệu và các Hệ thống thông tin.

b) Quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kế hoạch và được ghi vào nhật ký, bao gồm tình trạng hoạt động trước và sau khi thực hiện.

c) Khi thực hiện bảo trì nếu phát hiện, phát sinh sự cố phải báo cáo cấp có thẩm quyền để xử lý.

Điều 16. Quy định về kiểm tra, báo cáo định kỳ

1. Thực hiện kiểm tra, báo cáo theo định kỳ tháng, quý, năm: Đơn vị 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 cơ quan quản lý.

2. Các nội dung kiểm tra bao gồm:

a) Về việc bảo đảm các điều kiện về môi trường cho hoạt động của Trung tâm dữ liệu.

b) Tình hình hoạt động, sử dụng tài nguyên tính toán của thiết bị mạng, máy chủ, hệ thống lưu trữ, các hệ thống thông tin.

c) Tình hình sử dụng kinh phí thực hiện nhiệm vụ duy trì, vận hành Trung tâm dữ liệu.

d) Tình hình đảm bảo an toàn an ninh thông tin tại Trung tâm dữ liệu.

đ) Công tác sao lưu, phục hồi dữ liệu của các hệ thống thông tin.

e) Hồ sơ: nhật ký vận hành, xử lý sự cố, cập nhật,...

g) Về việc tuân thủ các quy định khác nêu tại quy chế này.

3. Cơ quan quản lý 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 tối thiểu 06 tháng một lần hoặc theo yêu cầu. 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 giao đơn vị vận hành lập kế hoạch khắc phục xử lý.

Chương IV

QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG TRONG QUẢN LÝ VẬN HÀNH TRUNG TÂM DỮ LIỆU

Điều 17. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của Trung tâm dữ liệu:

a) Đơn vị vận hành thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của các thiết bị hệ thống trong Trung tâm dữ liệu;

b) Giải pháp giám sát hệ thống thông tin tập trung trong Trung tâm dữ liệu phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thiết bị hệ thống bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của thiết bị hệ thống, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực.

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Đơn vị vận hành lập và thực hiện kế hoạch sao lưu dữ liệu, xây dựng kịch bản sự cố liên quan đến mất mát dữ liệu và phương án khôi phục dựa trên nguyên tắc khôi phục dữ liệu và hoạt động của hệ thống thông tin nhanh nhất có thể.

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

- Với dữ liệu trên máy chủ, lưu trữ chuyên dụng, thực hiện sao lưu lên thiết bị sao lưu chuyên dụng.

- 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.

- 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.

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

c) Đối với dữ liệu quan trọng, bộ phận vận hành đề xuất cơ quan quản lý nâng cấp công nghệ sao lưu phù hợp, mở rộng không gian lưu trữ hoặc thuê Trung tâm dữ liệu dự phòng để ngăn ngừa, bảo đảm an toàn dữ liệu của hệ thống.

d) Kế hoạch sao lưu, phương án khôi phục dữ liệu phải phù hợp với loại dữ liệu và các quy định liên quan theo quy định.

đ) Hoạt động quản lý sao lưu, phục hồi dữ liệu theo mẫu quy trình TTDL_QT_601 do đơn vị vận hành trung tâm dữ liệu ban hành.

3. Truy cập và quản lý cấu hình hệ thống trong Trung tâm dữ liệu:

a) Chỉ cho phép truy cập, cấu hình thiết bị hệ thống từ vùng mạng quản trị;

b) Truy cập, cấu hình thiết bị hệ thống từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng;

d) Toàn bộ thao tác thay đổi, thiết lập cấu hình thiết bị hệ thống phải được ghi nhật ký hệ thống;

đ) Hệ thống thông tin cấp độ 4 trở lên, khi thực hiện truy cập, cấu hình thiết bị hệ thống phải thông qua hệ thống quản lý tài khoản đặc quyền.

4. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

5. Hoạt động quản lý an toàn mạng thực hiện theo Quy trình quản lý an toàn mạng do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 18. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ:

a) Đơn vị vận hành thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của hệ thống máy chủ và ứng dụng;

b) Tối thiểu các thông tin về hoạt động của máy chủ và ứng dụng, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU, RAM, Storage) và lưu lượng mạng xử lý theo thời gian thực.

2. Truy cập mạng của máy chủ:

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

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

3. Truy cập và quản trị máy chủ và ứng dụng:

a) Chỉ cho phép truy cập, cấu hình máy chủ từ vùng mạng quản trị; cấu hình ứng dụng từ vùng mạng quản trị hoặc nghiệp vụ;

b) Truy cập, cấu hình máy chủ và ứng dụng từ bên ngoài hệ thống phải thông qua kết nối VPN;

c) Phân quyền truy cập từ bên ngoài hệ thống qua kết nối VPN theo địa chỉ IP nguồn đối với truy cập quản trị hệ thống đối với người quản trị và truy cập sử dụng tài nguyên, ứng dụng, dịch vụ đối với người sử dụng.

4. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

a) Khi có thay đổi, cập nhật cấu hình, mã nguồn ứng dụng, toàn bộ tập tin cấu hình, mã nguồn ứng dụng phải được sao lưu dự phòng trên thiết bị và hệ thống lưu trữ độc lập;

b) Thực hiện lưu trạng thái ảnh của hệ điều hành ảo hóa (take snapshot) tại thời điểm trước và sau khi cập nhật máy chủ và ứng dụng;

c) Định kỳ hàng tháng lưu trữ ảnh của hệ điều hành máy chủ trên thiết bị và hệ thống lưu trữ độc lập.

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

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

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

c) Thực hiện lưu trạng thái ảnh của hệ điều hành ảo hóa (take snapshot) tại thời điểm trước và sau khi gỡ bỏ dịch vụ, phần mềm;

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

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

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

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

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

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

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

8. Hoạt động quản lý an toàn máy chủ và ứng dụng thực hiện theo Quy trình quản lý an toàn máy chủ và ứng dụng theo quy trình TTDL_QT_206 do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 19. Quản lý an toàn dữ liệu

1. Việc quản lý an toàn, an ninh thông tin đối với dữ liệu tại Trung tâm dữ liệu phải tuân thủ các quy định tại Điều 13 Quyết định số 1921/QĐ-BNNMT.

2. Yêu cầu an toàn đối với phương pháp mã hóa

a) Toàn bộ cơ sở dữ liệu, dữ liệu nghiệp vụ của hệ thống trong Trung tâm dữ liệu khi lưu trữ trên thiết bị và hệ thống lưu trữ độc lập phải được mã hóa và kèm theo mã kiểm tra tính toàn vẹn;

b) Dữ liệu được sao lưu dự phòng theo từng phiên bản và có nhật ký ghi lại thông tin dữ liệu sau mỗi lần thực hiện sao lưu, dự phòng;

c) Độ dài của khóa bí mật dùng để mã hóa dữ liệu tối thiểu 128 bit.

3. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa

a) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu hệ thống (tệp tin cấu hình, ảnh hệ điều hành,…) được quản lý bởi đơn vị vận hành;

b) Khóa bí mật sử dụng để mã hóa và giải mã dữ liệu nghiệp vụ (tệp tin dữ liệu, cơ sở dữ liệu,…) được quản lý bởi bộ phận nghiệp vụ tương ứng;

c) Thông tin khóa bí mật phải được lưu trữ mã hóa, kèm theo mã kiểm tra tính toàn vẹn trên thiết bị và hệ thống lưu trữ độc lập;

d) Chỉ có bộ phận/cán bộ có chức năng có quyền quản lý và truy cập khóa bí mật;

đ) Thông tin mỗi khóa bí mật phải có thông tin nhật ký quản lý, cán bộ quản lý tại mỗi thời điểm.

4. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu không được sử dụng không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Khoa học và Công nghệ công bố.

5. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ phải được mã hóa đáp ứng yêu cầu ở trên.

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ phải được đồng bộ theo thời gian thực;

7. Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có) theo Quy trình tại điểm 5 Điều này.

8. Hoạt động quản lý an toàn dữ liệu thực hiện theo Quy trình quản lý an toàn dữ liệu do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 20. Quản lý an toàn thiết bị đầu cuối

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối:

a) Thiết bị đầu cuối của cán bộ thuộc cơ quan, đơn vị, tổ chức khi kết nối vào mạng Trung tâm dữ liệu phải được quản lý truy cập theo địa chỉ IP và địa chỉ MAC.

b) Trạng thái hoạt động (UP/DOWN) của thiết bị đầu cuối phải được quản lý bởi hệ thống quản lý truy cập lớp mạng tập trung.

c) Ngăn chặn toàn bộ các thiết bị đầu cuối chưa được quản lý kết nối vào mạng Trung tâm dữ liệu.

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa:

a) Chỉ cho phép truy cập, sử dụng thiết bị đầu cuối từ bên ngoài hệ thống phải thông qua kết nối VPN.

b) Tất cả truy cập từ các thiết bị đầu cuối từ các mạng khác nhau trong hệ thống phải được kiểm soát truy cập bởi tường lửa lớp mạng.

c) Mọi máy trạm trong mạng phải thiết lập chức năng tường lửa của hệ điều hành.

đ) Mọi máy trạm trong mạng phải cài đặt phần mềm phòng chống mã độc trước khi kết nối vào hệ thống trong Trung tâm dữ liệu.

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống

b) Máy trạm phải được cấu hình tối ưu và tăng cường bảo mật trước khi kết nối vào hệ thống trong Trung tâm dữ liệu;

c) Toàn bộ dữ liệu, hệ điều hành máy trạm phải được xóa bỏ trước khi gỡ bỏ máy chủ khỏi hệ thống trong Trung tâm dữ liệu.

4. Hoạt động quản lý an toàn thiết bị đầu cuối thực hiện theo Quy trình quản lý an toàn thiết bị đầu cuối do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 21. Quản lý phòng chống phần mềm độc hại

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động:

a) Máy tính, máy chủ và thiết bị công nghệ thông tin phải được cập nhật phần mềm phòng chống mã độc trước khi kết nối vào hệ thống.

b) Phần mềm phòng, chống mã độc trên máy tính, máy chủ và thiết bị công nghệ thông tin phải được thiết lập chế độ tự động cập nhật dấu hiệu mã độc từ nhà cung cấp và chế độ bảo vệ theo thời gian thực.

c) Triển khai giải pháp phòng, chống mã độc có chức năng quản lý tập trung.

2. Cài đặt, sử dụng phần mềm trên máy tính, thiết bị công nghệ thông tin và việc truy cập các trang thông tin trên mạng:

a) Phần mềm trước khi cài đặt trên máy tính, thiết bị công nghệ thông tin phải kiểm tra mã độc;

b) Phần mềm trước khi cài đặt trên máy tính, thiết bị công nghệ thông tin phải xác thực nguồn gốc từ nhà sản xuất theo mã kiểm tra tính toàn vẹn;

c) Phần mềm sau khi cài đặt phải được xử lý điểm yếu an toàn thông tin và cập nhật lên phiên bản mới nhất;

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

3. Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động phải thực hiện qua kênh kết nối an toàn sử dụng giao thức mã hóa, xác thực không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Thông tin và Truyền thông công bố.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống quan trọng; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống trong Trung tâm dữ liệu.

5. Hoạt động quản lý phòng chống phần mềm độc hại thực hiện theo Quy trình quản lý phòng chống phần mềm độc hại do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 22. Quản lý giám sát an toàn hệ thống thông tin

1. Việc quản lý giám sát an toàn thông tin mạng đối với dữ liệu tại Trung tâm dữ liệu phải tuân thủ các quy định tại Điều 15 Quyết định số 1921/QĐ-BNNMT.

2. Quản lý, vận hành hoạt động bình thường của hệ thống giám sát

a) Đơn vị vận hành thực hiện giám sát hệ thống 24/7 bảo đảm tính khả dụng của các thành phần của hệ thống giám sát;

b) Giải pháp giám sát hệ thống thông tin tập trung phải được thiết lập chế độ tự động cảnh báo đến người quản trị khi các thành phần của hệ thống giám sát bị quá tải theo một ngưỡng được thiết lập trước hoặc bị dừng hoạt động;

c) Tối thiểu các thông tin về hoạt động của các thành phần của hệ thống giám sát, bao gồm các thông tin: trạng thái (Up/Down), hiệu năng xử lý (CPU/RAM) và lưu lượng mạng xử lý theo thời gian thực;

3. Đối tượng giám sát bao gồm tối thiểu bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ.

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

5. Truy cập và quản trị hệ thống giám sát chỉ được thực hiện từ vùng mạng quản trị; trường hợp truy cập và quản trị từ mạng bên ngoài thì phải thông qua kênh kết nối VPN.

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

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

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

9. Bộ phận SOC thực hiện giám sát giám sát an toàn hệ thống thông tin 24/7 để thực hiện theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.

10. Việc tổ chức hoạt động giám sát các hệ thông thông tin bảo đảm hạ tầng Trung tâm dữ liệu thực hiện theo Quy trình TTDL_QT_101 do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 23. Quản lý điểm yếu an toàn thông tin

1. Quản lý thông tin các thành phần có trong Trung tâm dữ liệu có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống nếu có.

2. Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định.

a) Đơn vị vận hành định kỳ ngày 01 lần truy cập và cập nhật thông tin về điểm yếu an toàn thông tin được cung cấp bởi tối thiểu 02 tổ chức trong nước và quốc tế.

b) Điểm yếu an toàn thông tin được phân nhóm theo mức độ nghiêm trọng (Nghiên trọng - Critical, Cao - High, Trung bình – Medium và Thấp - Low).

c) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Critical Đơn vị vận hành phải xử lý trong vòng 03 giờ.

d) Khi phát hiện điểm yếu an toàn thông tin ở mức độ High Đơn vị vận hành phải xử lý trong vòng 03 giờ.

đ) Khi phát hiện điểm yếu an toàn thông tin ở mức độ Medium Đơn vị vận hành phải xử lý trong vòng 24 giờ.

3. Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin

a) Bên cung cấp phần mềm, giải pháp, ứng dụng phải có trách nhiệm hỗ trợ xử lý điểm yếu an toàn thông tin theo yêu cầu của bên sử dụng.

b) Đơn vị vận hành là đầu mối phối hợp với các bên việc phối hợp xử lý điểm yếu an toàn thông tin từ các nhóm chuyên gia, bên cung cấp dịch vụ.

4. Việc kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng, đông thời tuân thủ các quy định tại Điều 16 Quyết định số 1921/QĐ-BNNMT.

5. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

6. Khi phát hiện điểm yếu an toàn thông tin tồn tại trong hệ thống thực hiện theo Quy trình Quản lý điểm yếu an toàn thông tin do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 24. Quản lý ứng cứu xử lý sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố:

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin.

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

d) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị; cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân nhóm sự cố an toàn thông tin:

a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Sự cố do bị tấn công mạng: Từ chối dịch vụ; giả mạo; sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; thay đổi giao diện; mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

c) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

d) Sự cố do lỗi của người quản trị, vận hành hệ thống.

đ) Sự cố liên quan đến các loại thiên tai như bão, lốc, sét, động đất,... Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố. Việc phân loại sự cố quy định tại Khoản 3 điều này.

3. Phân loại sự cố an toàn thông tin:

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp.

4. Khi phát hiện có sự cố, đơn vị vận hành Trung tâm dữ liệu, đơn vị vận hành hệ thống thông tin thực hiện các biện pháp cô lập và xác định nguyên nhân xảy ra sự cố; lập biên bản, ghi nhận về sự cố và thiết bị hư hỏng (có xác nhận của chủ sở hữu tài sản, thiết bị bị hư hỏng), thông báo cho các đơn vị có liên quan về sự cố.

5. Thông tin về sự cố, phương án xử lý phải được ghi nhận trong nhật ký xử lý sự cố.

6. Thông báo cho các đơn vị liên quan về kết quả xử lý sự cố.

7. Trường hợp có sự cố ở mức độ cao, nghiêm trọng hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị. Lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và cơ quan có thẩm quyền về an toàn thông tin để được hướng dẫn, hỗ trợ triển khai thực hiện.

8. Khi phát hiện sự cố an toàn thông tin tồn tại trong hệ thống thực hiện theo Quy trình TTDL_QT_103 do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 25. Quản lý an toàn người sử dụng đầu cuối

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

a) Người sử dụng đầu cuối phải tuân thủ các quy định của pháp luật và quy định tại Quy chế này khi truy cập, sử dụng tài nguyên nội bộ trong Trung tâm dữ liệu.

b) Không truy cập từ xa vào trực tiếp các máy tính trong mạng nội bộ của đơn vị. Trường hợp, người sử dụng cần truy cập từ xa thì phải truy cập gián tiếp qua giao thức mạng an toàn, có hỗ trợ mã hóa bảo mật thông tin như VPN.

c) Không kết nối các thiết bị lưu trữ di động của khách bên ngoài vào các máy tính để bàn của đơn vị. Trường hợp, người sử dụng cần thiết phải kết nối các thiết bị lưu trữ di động của khách bên ngoài thì phải đề nghị và được bộ phận chuyên trách kiểm tra an toàn thông tin trước khi thực hiện.

2. Quản lý truy cập mạng và tài nguyên trên Internet:

a) Không truy cập trang thông tin theo đường link, mở tệp tin đính kèm từ những thư điện tử lần đầu tiên nhận được, không rõ nguồn gửi hoặc nghi ngờ có

thể gây hại. Trường hợp, người sử dụng cần thiết phải truy cập hoặc mở tệp tin đính kèm thì đề nghị bộ phận chuyên trách kiểm tra an toàn thông tin trước khi truy cập hoặc mở tệp tin.

b) Không truy cập các trang thông tin không rõ nguồn gốc hoặc có nội dung độc hại;

c) Thiết bị di động của người sử dụng được kết nối vào mạng không dây công cộng của đơn vị nhưng không kết nối thiết bị di động vào mạng ngang hàng với mạng máy tính để bàn của cán bộ. Trường hợp, người sử dụng cần thiết phải kết nối vào mạng ngang hàng thì phải đề nghị bộ phận chuyên trách kiểm tra an toàn thông tin cho thiết bị di động trước khi thực hiện;

d) Thiết bị di động khi kết nối vào mạng nội bộ của đơn vị phải được quản lý truy cập ra các vùng mạng khác của hệ thống và mạng Internet.

đ) Thiết bị di động phải được quản lý cấp phát DHCP theo địa chỉ MAC (trừ các thiết bị kết nối vào mạng không dây công cộng).

3. Cài đặt và sử dụng máy tính an toàn

a) Đặt mật khẩu cho các tài khoản của hệ điều hành theo quy định tại điều 14 của quy chế này.

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

c) Không tự ý thay đổi cấu hình thiết bị đã được thiết lập, việc thay đổi phải thông báo đến bộ phận chuyên trách

4. Hoạt động quản lý an toàn người sử dụng đầu cuối thực hiện theo Quy trình Quản lý an toàn người sử dụng đầu cuối do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 26. Quản lý rủi ro an toàn thông tin

1. Hệ thống phải được xây dựng phương án Quản lý rủi ro an toàn thông tin.

2. Phương án Quản lý an toàn thông tin trong Trung tâm dữ liệu phải được ban hành cùng Quy chế bảo đảm an toàn thông tin trước khi đưa hệ thống vào vận hành, khai thác.

3. Thực hiện đánh giá và xây dựng phương án xử lý rủi ro cho hệ thống trước khi đưa vào vận hành, khai thác.

4. Thực hiện đánh giá và quản lý rủi ro an toàn thông tin cho hệ thống theo Quy trình Quản lý rủi ro an toàn thông tin do đơn vị vận hành trung tâm dữ liệu ban hành.

Điều 27. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Yêu cầu đối với việc thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin:

a) Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

c) Các phương tiện và thiết bị thiết bị công nghệ thông tin: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin thực hiện theo Quy trình kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin do đơn vị vận hành trung tâm dữ liệu ban hành.

Chương V

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC, CÁ NHÂN TRONG VIỆC QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC TRUNG TÂM DỮ LIỆU

Điều 28. Trách nhiệm của cơ quan quản lý

1. Tham mưu cơ quan chủ quản về việc quy hoạch hệ thống, các giải pháp, phương án kỹ thuật, các kế hoạch phát triển, nâng cấp và mở rộng Trung tâm dữ liệu để đáp ứng theo yêu cầu.

2. Tham mưu cơ quan chủ quản ban hành theo thẩm quyền về định mức, đơn giá kỹ thuật các dịch vụ của Trung tâm dữ liệu; Ban hành các văn bản hướng dẫn chuyển giao trang thiết bị, máy móc, cài đặt phần mềm và quản lý tài sản tại Trung tâm dữ liệu; phê duyệt quy trình vận hành, bảo trì, bảo dưỡng và khắc phục sự cố Trung tâm dữ liệu.

3. Hướng dẫn triển khai các giải pháp bảo đảm an toàn, an ninh thông tin mạng đối với các hệ thống thông tin thuộc Trung tâm dữ liệu; Quy hoạch tài nguyên hệ thống, các giải pháp, phương án kỹ thuật, các kế hoạch phát triển Trung tâm dữ liệu.

4. Xây dựng kế hoạch đào tạo bồi dưỡng đảm bảo nguồn nhân lực quản lý, vận hành có chuyên môn đáp ứng yêu cầu, được trang bị các kiến thức chuyên môn nâng cao tới hoạt động của Trung tâm dữ liệu.

5. Kiểm tra, giám sát việc vận hành, khai thác hạ tầng, ứng dụng, dịch vụ của đơn vị vận hành Trung tâm dữ liệu trong việc tuân thủ các nội dung quy định

tại Quy chế này và các quy định khác liên quan đến quản lý, vận hành và khai thác Trung tâm dữ liệu.

6. Thực hiện chế độ báo cáo định kỳ, báo cáo đột xuất về cơ quan chủ quản về tình hình hoạt động của Trung tâm dữ liệu.

Điều 29. Trách nhiệm của đơn vị vận hành

1. Chịu trách nhiệm về việc quản trị, vận hành và khai thác có hiệu quả hoạt động của Trung tâm dữ liệu theo quy định.

2. 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 giờ, 7 ngày/tuần và quy định chế độ trực vận hành, giám sát an toàn thông tin tại Trung tâm dữ liệu ngoài giờ hành chính, ngày nghỉ trong tuần, ngày nghỉ lễ, ngày tết.

3. Quản trị, vận hành Trung tâm dữ liệu đảm bảo hiệu quả, đảm bảo an toàn an ninh thông tin gồm các hệ thống ứng dụng dùng chung sau đây:

a) Quản trị cơ sở hạ tầng kỹ thuật Trung tâm dữ liệu của Bộ.

b) Quản trị các phần mềm dùng chung, phân quyền, giám sát tài khoản người dùng.

c) Quản trị tên miền: “mae.gov.vn”; quy hoạch, vận hành, kiểm tra, đánh giá tài nguyên hệ thống.

4. Giám sát hệ thống, quản lý tài khoản quản trị; kiểm soát truy cập giữa các vùng mạng, kiểm soát ứng dụng, giao thức kết nối; kiểm soát cổng kết nối; tăng cường giải pháp giám sát an toàn an ninh thông tin.

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

6. Xây dựng các quy trình vận hành, phương án ứng cứu xử lý sự cố cho các hệ thống quan trọng tại Trung tâm dữ liệu.

7. Tham mưu cơ quan quản lý các giải pháp, phương án kỹ thuật, kế hoạch phát triển, mở rộng Trung tâm dữ liệu để nâng cao năng lực quản lý nhà nước, tăng cường giải pháp ứng dụng công nghệ số, chính phủ số và chuyển đổi số của Bộ, ngành.

8. Tiếp nhận các yêu cầu cung cấp hạ tầng, dịch vụ của các cơ quan, đơn vị trong phạm vi quy định và triển khai cung cấp theo đúng với tiêu chuẩn chất lượng, quy trình và trên cơ sở khai thác, sử dụng hiệu quả hạ tầng Trung tâm hợp dữ liệu.

9. Hàng năm xây dựng kinh phí đảm bảo duy trì hoạt động, vận hành, bảo dưỡng, sửa chữa, thay thế trang thiết bị, xây dựng hoặc nâng cấp, cập nhật phần mềm quản lý, duy trì bản quyền (licence) phần mềm và thiết bị tại Trung tâm dữ

liệu và thanh toán chế độ trực 24/24 giờ cho cán bộ quản trị, vận hành, tổng hợp dự toán trình cấp có thẩm quyền phê duyệt.

10. Đào tạo, cập nhật và trang bị các kiến thức chuyên môn chuyên sâu liên quan tới hoạt động của Trung tâm dữ liệu cho cán bộ quản lý, cán bộ quản trị, vận hành để đáp ứng yêu cầu thực tiễn.

11. Thực hiện báo cáo định kỳ hoặc đột xuất cho cơ quan quản lý về tình hình hoạt động, cung cấp hạ tầng của Trung tâm dữ liệu.

Điều 30. Trách nhiệm của cơ quan, đơn vị, tổ chức, cá nhân tham gia sử dụng hạ tầng, ứng dụng, dịch vụ của Trung tâm dữ liệu

1. Sử dụng cơ sở hạ tầng kỹ thuật, ứng dụng, dịch vụ của Trung tâm dữ liệu theo quy định của Quy chế này và các quy định khác có liên quan.

2. Tuân thủ quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, chính phủ số và chuyển đổi số của Bộ Nông nghiệp và Môi trường và các quy định về an toàn, bảo mật thông tin trong quản lý, vận hành và khai thác Trung tâm dữ liệu.

3. Đối với cơ quan, đơn vị có thiết bị công nghệ thông tin, hệ thống thông tin đặt tại Trung tâm dữ liệu:

a) Chịu trách nhiệm về các nội dung, thông tin lưu trữ tại Trung tâm dữ liệu do cơ quan, đơn vị cung cấp, sao lưu dữ liệu định kỳ của đơn vị theo quy định và dưới sự hướng dẫn của đơn vị vận hành; thường xuyên cập nhật các bản vá hệ điều hành, phần mềm mã nguồn và ứng dụng theo khuyến cáo của nhà sản xuất.

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

c) Xây dựng các quy trình vận hành, phương án ứng cứu xử lý sự cố cho các hệ thống quan trọng do cơ quan đơn vị quản lý, vận hành đặt tại Trung tâm dữ liệu theo quy định.

d) Hàng năm, xây dựng kinh phí đảm bảo duy trì, vận hành, nâng cấp trang thiết bị phần cứng và cập nhật phần mềm đặt tại Trung tâm dữ liệu; tổng hợp chung trong dự toán chi nghiệp vụ chuyên môn của cơ quan, đơn vị, trình cấp có thẩm quyền phê duyệt.

4. Đối với người sử dụng:

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

b) Không được thực hiện các hành vi đánh cắp, giả mạo tài khoản, truy cập trái phép, sử dụng các công cụ, phần mềm làm tổn hại đến hoạt động của Trung tâm dữ liệu; không được cung cấp thông tin về tài khoản, mật khẩu người dùng cho người khác và các hành vi bị nghiêm cấm quy định tại Điều 5 Quy chế này.

5. Trường hợp phát sinh sự cố phải thông báo ngay cho cán bộ kỹ thuật của đơn vị vận hành để phối hợp xử lý sự cố và xác nhận kết quả xử lý.

Chương VI

TỔ CHỨC THỰC HIỆN

Điều 31. Điều khoản thi hành

1. Cục Chuyển đổi số: Là đơn vị chủ trì, chịu trách nhiệm trước Bộ Nông nghiệp và Môi trường về việc quản lý, khai thác và vận hành Trung tâm dữ liệu đảm bảo ổn định, thông suốt, liên tục, an toàn bảo mật thông tin, quản lý tài sản theo đúng quy định; chủ trì tổ chức triển khai tuyên truyền – phổ biến, hướng dẫn thực hiện Quy chế này; theo dõi, kiểm tra định kỳ báo cáo cơ quan chủ quản tình hình triển khai của các cơ quan, đơn vị.

2. Các Trung tâm Hạ tầng số, Dữ liệu thông tin phía Nam: Chịu trách nhiệm trước Cục Chuyển đổi số về việc quản trị, vận hành và khai Trung tâm dữ liệu đảm bảo ổn định, thông suốt, liên tục, an toàn bảo mật thông tin, quản lý tài sản theo đúng quy định; thực hiện báo cáo cơ quan quản lý theo định kỳ, đột xuất tình hình hoạt động của Trung tâm dữ liệu; Căn cứ nhu cầu đáp ứng để trang bị, duy trì, quản trị, vận hành hoạt động hàng năm của Trung tâm dữ liệu – đề xuất, xây dựng kế hoạch kèm dự toán gửi Phòng Tài chính – Thống kê để tổng hợp, thẩm định và trình cấp có thẩm quyền xem xét phê duyệt.

3. Phòng An toàn thông tin chủ trì, phối hợp với đơn vị vận hành và các đơn vị liên quan tổ chức đánh giá an toàn thông tin đối với trang thiết bị công nghệ thông tin, các hệ thống thông tin, ứng dụng,… trước khi đưa vào lắp đặt, vận hành tại Trung tâm dữ liệu – hàng năm xây dựng kế hoạch kiểm tra, giám sát hoạt động.

4. Phòng Tài chính – Thống kê: Thẩm định, trình Cục phê duyệt kế hoạch, dự toán chi tiết kinh phí duy trì hoạt động của Trung tâm dữ liệu hằng năm của các đơn vị.

5. Các đơn vị trực thuộc Cục, các cơ quan, đơn vị, tổ chức, cá nhân sử dụng dịch vụ tại Trung tâm dữ liệu:

a) Trình phê duyệt cấp độ đối với hệ thống thông tin đặt tại Trung tâm dữ liệu; quản trị, vận hành hệ thống thông tin của đơn vị mình đảm bảo hiệu quả, đảm bảo an toàn an ninh thông tin.

b) Chủ động phối hợp với đơn vị quản lý, đơn vị vận hành khi phát hiện những vấn đề liên quan ảnh hưởng đến an toàn thông tin, an toàn dữ liệu, mất kết nối thông tin để phối hợp khắc phục và xử lý kịp thời.

Điều 32. Xử lý vi phạm

1. Đối với các Cơ quan, đơn vị, cán bộ, công chức, viên chức, người lao động vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định pháp luật hiện hành.

2. Đối với các tổ chức, cá nhân khác tham gia sử dụng dịch vụ của Trung tâm dữ liệu vi phạm Quy chế này thì xử lý vi phạm theo các điều khoản tại Hợp đồng đã ký kết giữa các bên có liên quan và theo quy định của pháp luật.

Điều 33. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Cục Chuyển đổi số có trách nhiệm tổ chức thực hiện nghiêm túc các quy định tại Quy chế này.

2. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin hoặc 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, tổ chức, cá nhân kịp thời phản ánh về cơ quan quản lý, đơn vị vận hành Trung tâm dữ liệu để tổng hợp, trình Cục trưởng xem xét, sửa đổi, bổ sung cho phù hợp./.

PHỤ LỤC 01 - DANH MỤC QUY TRÌNH

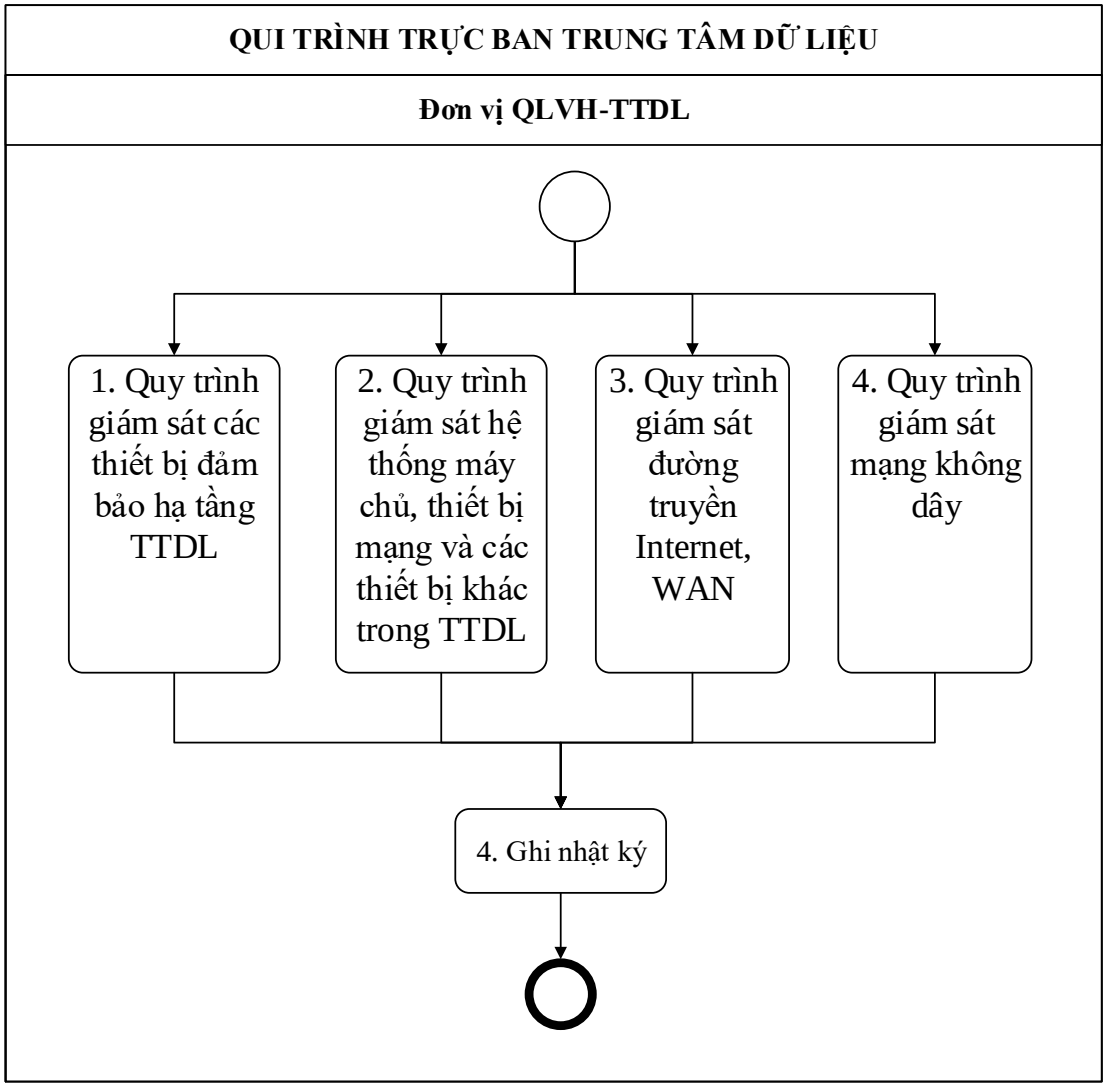
(Ban hành kèm theo Quyết định số /QĐ-CĐS ngày tháng năm 2025 của Cục trưởng Cục Chuyển đổi số)

STT	Mã số	Phiên bản	Tên quy trình
1	TTDL_QT_105	2.0	Quy trình trực ban tại Trung tâm dữ liệu
2	TTDL_QT_207	2.0	Quy trình tiếp nhận, lắp đặt các thiết bị CNTT tại Trung tâm dữ liệu
3	TTDL_QT_413	2.0	Quy trình cấp hạ tầng, tài nguyên tại Trung tâm dữ liệu
4	TTDL_QT_514	2.0	Quy trình cấp phát, thu hồi tài khoản mạng riêng ảo (VPN) truy cập hệ thống Trung tâm dữ liệu
5	TTDL_QT_515	2.0	Quy trình cấp phát, thu hồi tài khoản người dùng

TTDL_QT_105 - Quy trình trực ban Trung tâm dữ liệu

Phiên bản	2.0
Thời gian hoàn thành	…./…./20…
Nội dung	Mô tả công việc thực hiện khi trực ban Trung tâm dữ liệu

Lược đồ



Thuyết minh

1. Trực ban Trung tâm dữ liệu

- Mục đích: thực hiện các quy trình giám sát nhằm đảm bảo tình trạng hoạt động, sớm phát hiện sự cố để xử lý kịp thời đối với các thiết bị hạ tầng TTDL, hệ thống máy chủ, hệ thống mạng.

- Phương pháp: thực hiện các quy trình kiểm tra, giám sát đối với các đối tượng trong TTDL.

- Các quy trình cần thực hiện:

+ Quy trình giám sát các thiết bị đảm bảo hạ tầng TTDL.

+ Quy trình giám sát hệ thống máy chủ, thiết bị mạng và các thiết bị khác trong TTDL.

+ Quy trình giám sát đường truyền Internet, WAN.

+ Quy trình giám sát mạng không dây.

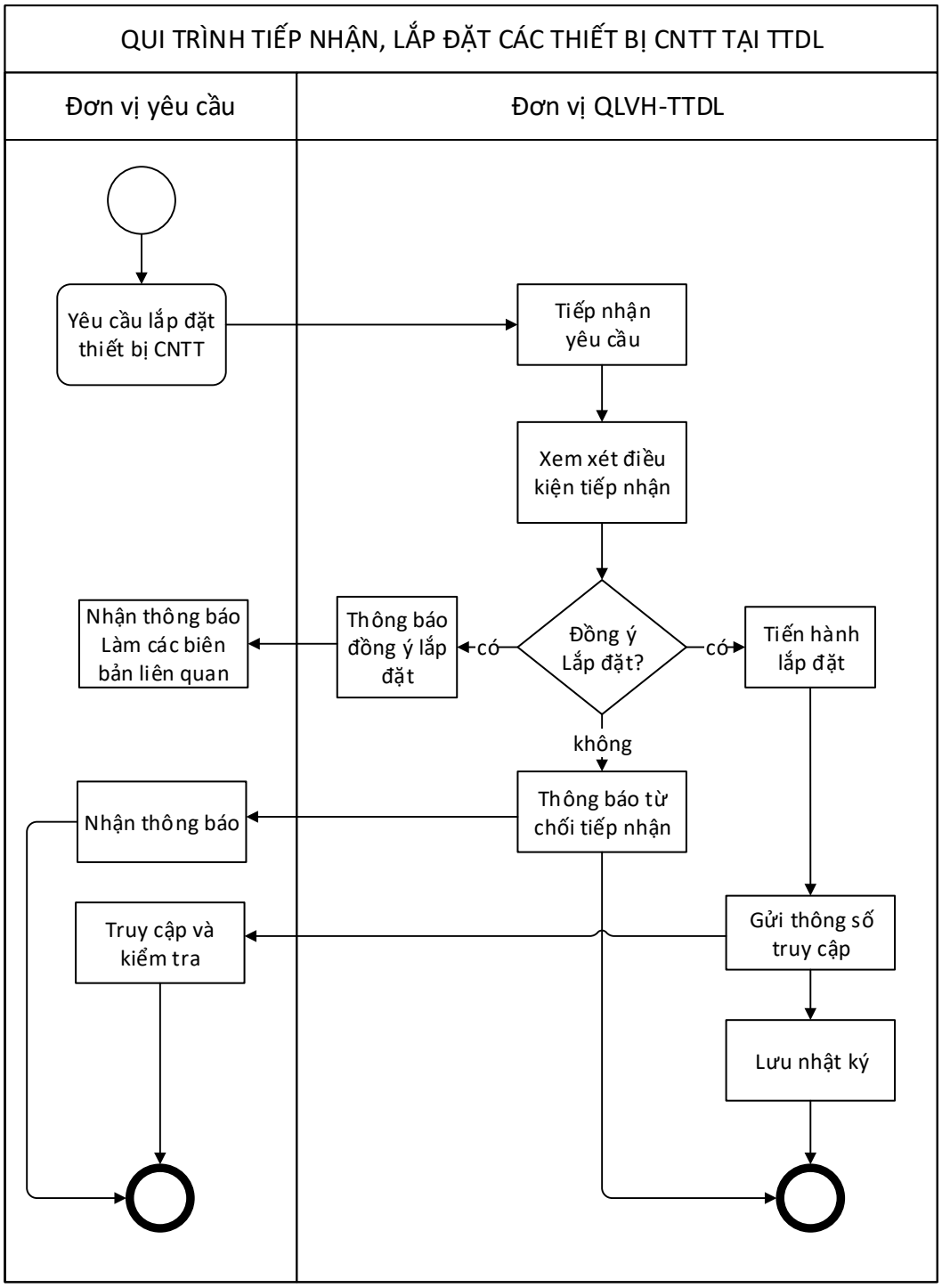
2. Ghi nhật ký

- Cập nhật thông tin nhật ký theo biểu mẫu của từng quy trình tương ứng.

TTDL_QT_207 - Quy trình tiếp nhận, lắp đặt thiết bị CNTT tại Trung tâm dữ liệu

Phiên bản	2.0
Thời gian hoàn thành	…./…./20….
Nội dung	Quy trình tiếp nhận, lắp đặt các thiết bị công nghệ thông tin tại Trung tâm dữ liệu

Lược đồ



Thuyết minh

1. Đơn vị yêu cầu

- Đơn vị yêu cầu lắp đặt thiết bị CNTT tại TTDL gửi công văn về Cục Chuyển đổi số.

- Đơn vị yêu cầu sau đó đợi phản hồi từ đơn vị QLVH-TTDL. Sau khi có thông tin phải hồi đồng ý lắp đặt đơn vị yêu đầu điền thông tin và biểu mẫu TTDL_BM_02 "Đăng ký mang thiết bị vào TTDL".

- Tiếp nhận và kiểm tra truy cập thiết bị sau khi nhận được thông tin truy cập đơn vị QLVH-TTDL.

2. Đơn vị QLVH-TTDL

- Tiếp nhận yêu cầu hạ tầng ảo hóa từ đơn vị yêu cầu.

- Tiến hành kiểm tra các điều kiện để lắp đặt:

+ Trường hợp không đủ điều kiện lắp đặt, thông báo từ chối tới đơn vị yêu cầu.

+ Trường hợp đủ điều kiện lắp đặt, thông báo đồng ý cấp phát tới đơn vị yêu cầu và tiến hành lắp đặt.

+ Làm biên bản đặt thiết bị theo biểu mẫu TTDL_BM_5 "Biên bản đặt thiết bị trong TTDL".

3. Sau khi hoàn thành lắp đặt

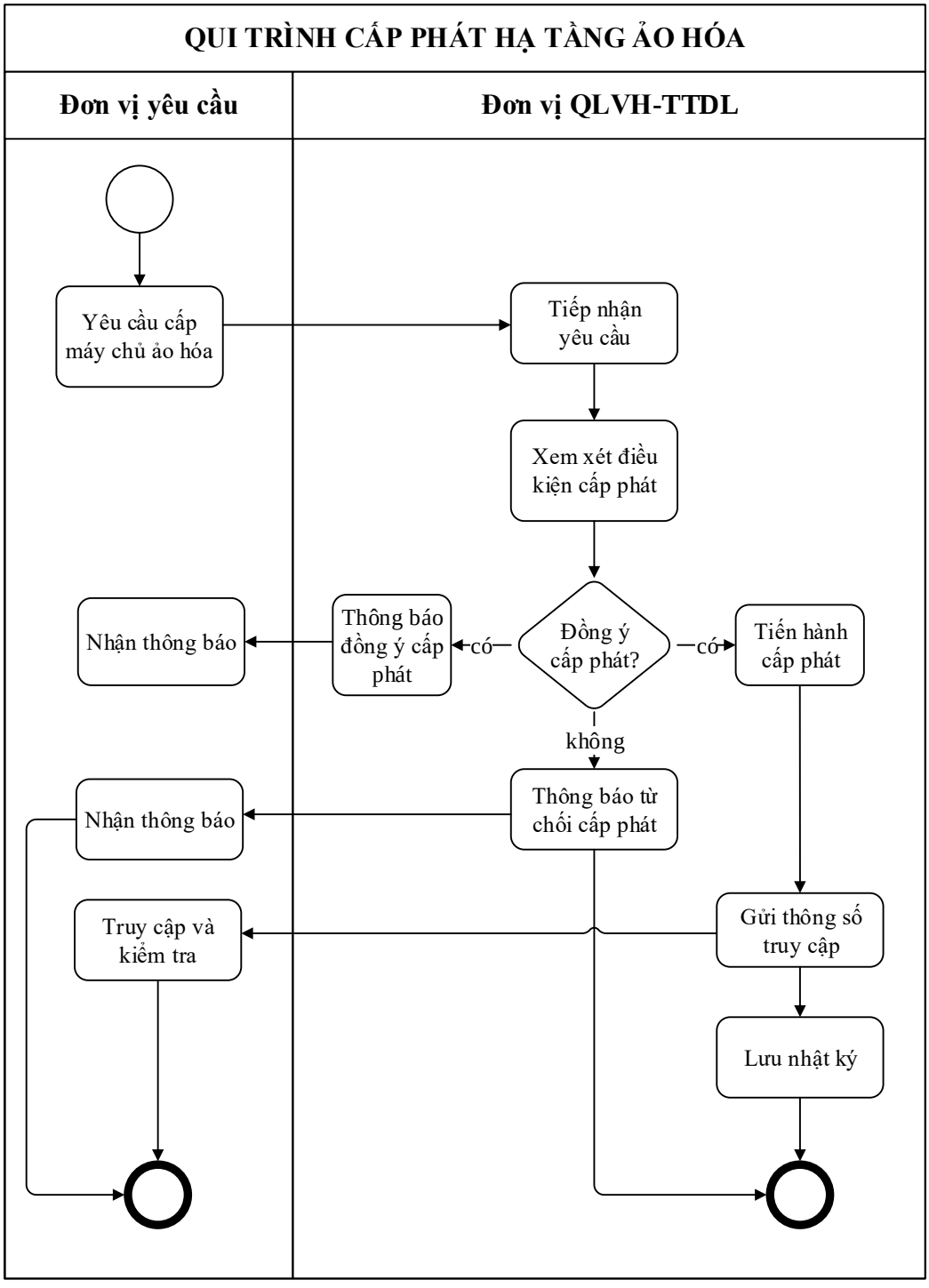
- Gửi thông tin truy cập tới đơn vị yêu cầu.

- Cập nhật thông tin vào TTDL_BM_06 "Hồ sơ thiết bị đặt trong TTDL".

TTDL_QT_413 - Quy trình cấp hạ tầng, tài nguyên trung tâm dữ liệu

Phiên bản	2.0
Thời gian hoàn thành	…../…../20….
Nội dung	Mô tả quy trình cấp phát máy chủ ảo hóa

Lược đồ



Thuyết minh

1. Đơn vị yêu cầu

- Đơn vị yêu cầu hạ tầng ảo hóa, tài nguyên khác điền thông tin yêu cầu theo mẫu TTDL_BM_07, sau đó gửi cho đơn vị: Cục Chuyển đổi số.

- Đơn vị yêu cầu sau đó đợi phản hồi từ đơn vị: Cục Chuyển đổi số.

- Tiếp nhận và kiểm tra truy cập máy chủ ảo khi nhận được thông tin truy cập đơn vị: Cục Chuyển đổi số.

2. Đơn vị Cục chuyển đổi số

- Tiếp nhận yêu cầu hạ tầng ảo hóa từ đơn vị yêu cầu.

- Tiến hành kiểm tra các điều kiện để cấp phát:

+ Trường hợp không đủ điều kiện cấp phát, thông báo từ chối cấp phát tới đơn vị yêu cầu.

+ Trường hợp đủ điều kiện cấp phát, thông báo đồng ý cấp phát tới đơn vị yêu cầu và tiến hành cấp phát.

- Sau khi hoàn thành cấp phát:

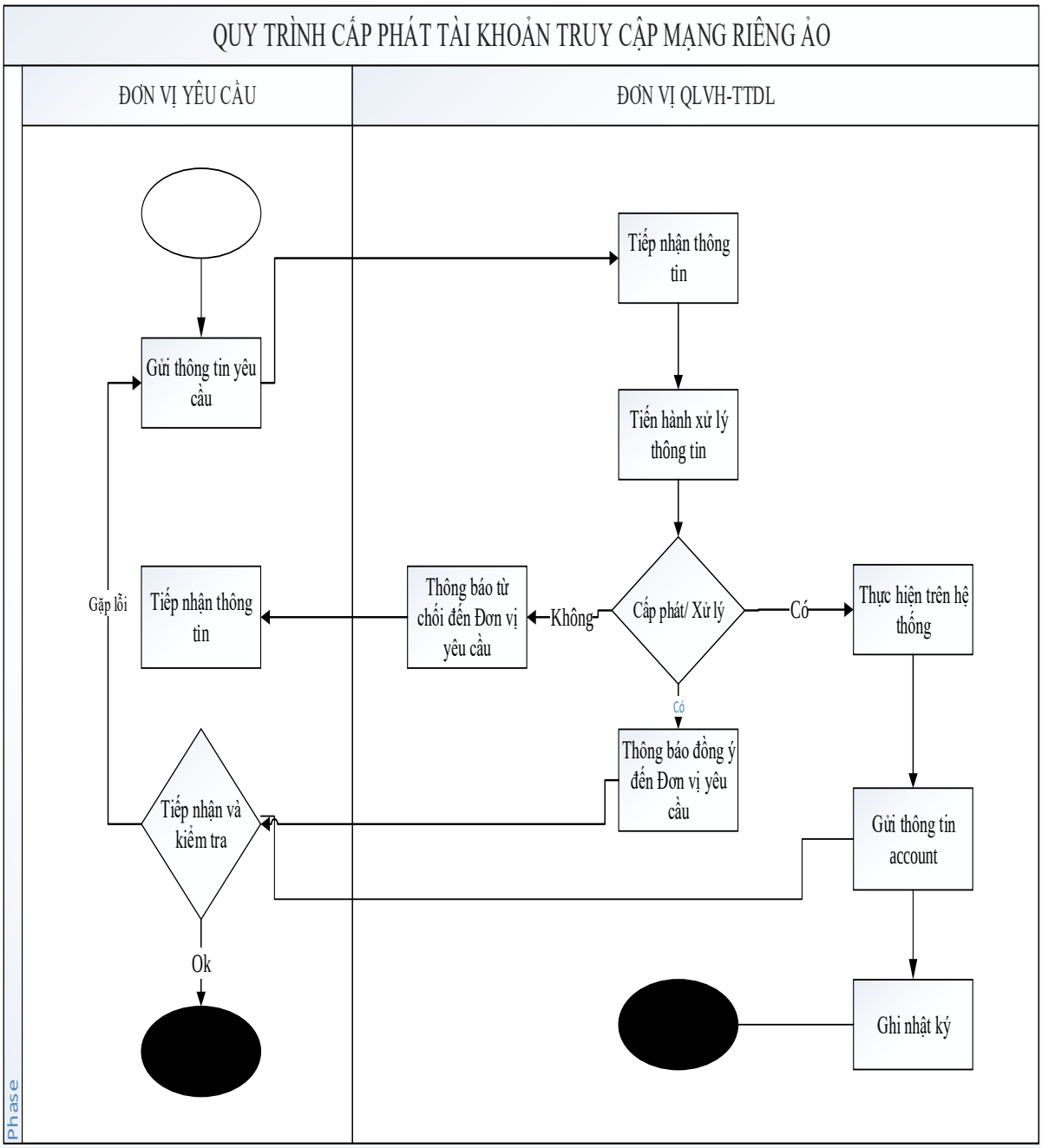
+ Gửi thông tin truy cập tới đơn vị yêu cầu.

+ Cập nhật thông tin vào nhật ký cấp phát hạ tầng ảo hóa.

TTDL_QT_514 – Quy trình cấp phát, thu hồi tài khoản truy cập mạng riêng ảo (VPN)

Phiên bản	2.0
Thời gian hoàn thành	…./…./20….
Nội dung	Mô tả quy trình cấp phát, thu hồi tài khoản truy cập mạng riêng ảo (VPN)

Lược đồ



Thuyết minh

1. Đơn vị yêu cầu

- Đơn vị yêu cầu cung cấp tài khoản truy cập mạng riêng ảo điền thông tin yêu cầu theo mẫu TTDL_BM_08, sau đó gửi cho đơn vị QLVH-TTDL.

- Đơn vị yêu cầu sau đó đợi phản hồi từ đơn vị QLVH-TTDL.

- Tiếp nhận và tiến hành kiểm tra tài khoản mạng riêng ảo khi nhận được thông tin truy cập từ đơn vị QLVH-TTDL.

- Trong trường hợp tài khoản truy cập được cấp phát không hoạt động, Đơn vị yêu cầu gửi lại thông tin yêu cầu kiểm tra lại tài khoản cũng như lỗi phát sinh đến đơn vị QLVH-TTDL để tiến hành xử lý.

2. Đơn vị QLVH-TTDL

- Tiếp nhận yêu cầu cung cấp tài khoản truy cập mạng riêng ảo từ đơn vị yêu cầu.

- Tiến hành kiểm tra các điều kiện để cấp phát:

+ Trường hợp không đủ điều kiện cấp phát, thông báo từ chối cấp phát tới đơn vị yêu cầu. (trường hợp không đủ điều kiện bao gồm: account không có địa chỉ email: …@mae.gov.vn; hoặc trước đó account có phát sinh những hoạt động có thể gây ảnh hướng đến an toàn hệ thống v.v…)

+ Trường hợp đủ điều kiện cấp phát, thông báo đồng ý cấp phát tới đơn vị yêu cầu và tiến hành cấp phát.

- Sau khi hoàn thành cấp phát:

+ Gửi thông tin truy cập tới đơn vị yêu cầu.

+ Cập nhật thông tin vào nhật ký cấp phát tài khoản truy cập mạng riêng ảo

- Trong trường hợp phát sinh lỗi tài khoản từ Đơn vị yêu cầu:

+ Tiến hành tiếp nhận và xử lý lỗi phát sinh.

+ Tiến hành trao đổi thông tin với Đơn vị yêu cầu khi phát hiện ra những lỗi của tài khoản có liên quan đến Đơn vị yêu cầu.

+ Gửi thông tin đến Đơn vị yêu cầu sau khi đã xử lý thành công.

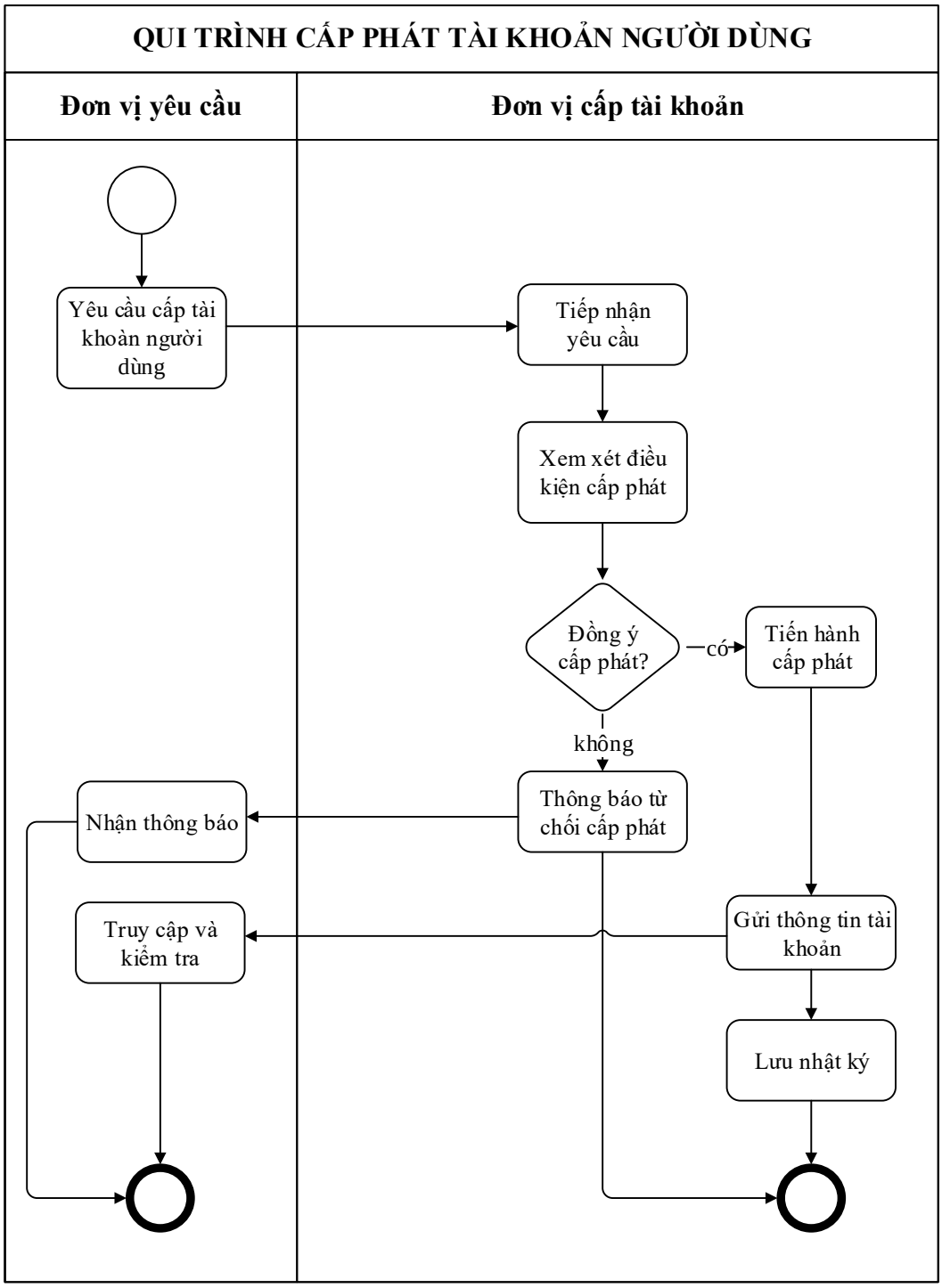
Tiến hành ghi nhật ký về việc ghi nhận thông tin quản lý khởi tạo các tài khoản mạng riêng ảo.

TTDL_QT_515 - Quy trình cấp phát, thu hồi tài khoản người dùng

Phiên bản	2.0
Thời gian hoàn thành	…/…/20….
Nội dung	Quy trình cấp phát, thu hồi tài khoản người dùng

Quy trình cấp phát tài khoản người dùng

<u>Lược đồ</u>



Thuyết minh

1. Đơn vị yêu cầu

- Đơn vị yêu cầu cung cấp tài khoản người dùng gửi thông tin yêu cầu theo công văn về Cục Chuyển đổi số hoặc qua thư điện tử về địa chỉ email: hatangso@mae.gov.vn

- Đơn vị yêu cầu sau đó đợi phản hồi từ đơn vị cấp phát.

- Tiếp nhận và tiến hành kiểm tra tài khoản người dùng khi nhận được thông tin truy cập từ đơn vị cấp phát.

- Trong trường hợp tài khoản truy cập được cấp phát không hoạt động, Đơn vị yêu cầu gửi lại thông tin yêu cầu kiểm tra lại tài khoản cũng như lỗi phát sinh đến đơn vị cấp phát để tiến hành xử lý.

2. Đơn vị cấp phát

- Tiếp nhận yêu cầu cung cấp tài khoản người dùng ảo từ đơn vị yêu cầu.

- Tiến hành kiểm tra các điều kiện để cấp phát:

+ Trường hợp không đủ điều kiện cấp phát, thông báo từ chối cấp phát tới đơn vị yêu cầu.

+ Trường hợp đủ điều kiện cấp phát, thông báo đồng ý cấp phát tới đơn vị yêu cầu và tiến hành cấp phát.

- Sau khi hoàn thành cấp phát:

+ Gửi thông tin truy cập tới đơn vị yêu cầu.

+ Cập nhật thông tin vào nhật ký cấp phát tài khoản người dùng.

- Trong trường hợp phát sinh lỗi tài khoản từ Đơn vị yêu cầu:

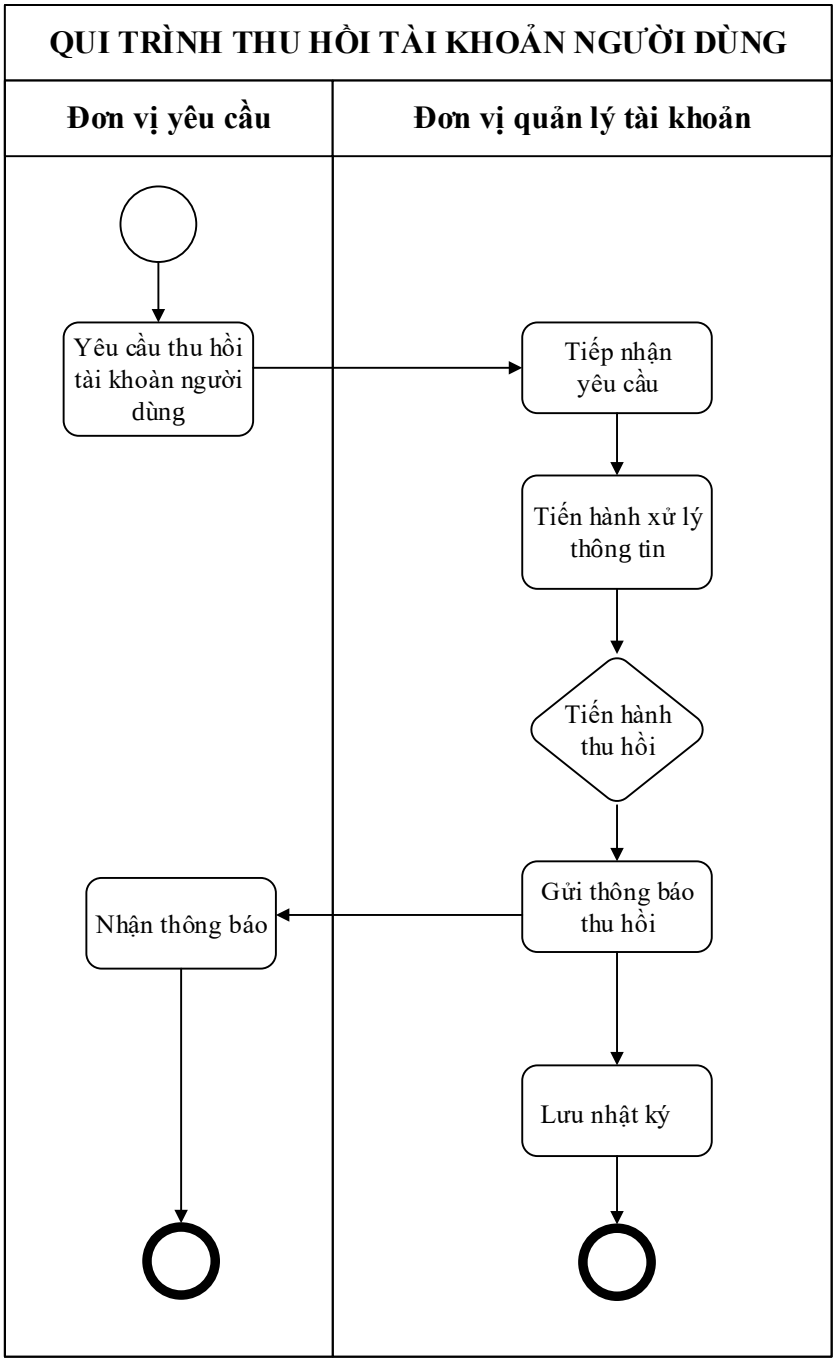
+ Tiến hành tiếp nhận và xử lý lỗi phát sinh.

+ Tiến hành trao đổi thông tin với Đơn vị yêu cầu khi phát hiện ra những lỗi của tài khoản có liên quan đến Đơn vị yêu cầu.

+ Gửi thông tin đến Đơn vị yêu cầu sau khi đã xử lý thành công.

Quy trình thu hồi tài khoản người dùng

Lược đồ



Thuyết minh

1. Đơn vị yêu cầu

- Đơn vị yêu cầu thu hồi tài khoản người dùng theo công văn về Cục Chuyển đổi số hoặc qua thư điện tử về địa chỉ email: hatangso@mae.gov.vn

- Đơn vị yêu cầu sau đó đợi phản hồi từ đơn vị quản lý.

- Tiếp nhận và tiến hành kiểm tra tài khoản người dùng khi nhận được thông tin truy cập từ đơn vị cấp phát.

- Trong trường hợp tài khoản truy cập được cấp phát không hoạt động, Đơn vị yêu cầu gửi lại thông tin yêu cầu kiểm tra lại tài khoản cũng như lỗi phát sinh đến đơn vị cấp phát để tiến hành xử lý.

2. Đơn vị quản lý tài khoản

- Tiếp nhận yêu cầu thu hồi tài khoản người dùng ảo từ đơn vị yêu cầu.

- Tiến hành kiểm tra các thông tin và thực hiện thu hồi.

- Sau khi hoàn thành thu hồi tài khoản:

+ Gửi thông tin truy cập tới đơn vị yêu cầu.

+ Cập nhật thông tin vào nhật ký cấp phát tài khoản người dùng.

PHỤ LỤC 02 - DANH SÁCH BIỂU MẪU

(Ban hành kèm theo Quyết định số /QĐ-CĐS ngày tháng năm 2025 của Cục trưởng Cục Chuyển đổi số)

STT	Mã số	Phiên bản	Tên biểu mẫu
1	TTDL_BM_01	2.0	Đăng ký vào ra Trung tâm dữ liệu
2	TTDL_BM_02	2.0	Đăng ký mang thiết bị vào, ra khỏi Trung tâm dữ liệu
3	TTDL_BM_03	2.0	Nhật ký vào ra Trung tâm dữ liệu
4	TTDL_BM_05	2.0	Biểu mẫu biên bản đặt thiết bị tại Trung tâm dữ liệu
5	TTDL_BM_06	2.0	Hồ sơ thiết bị đặt tại Trung tâm dữ liệu
6	TTDL_BM_07	2.0	Biểu mẫu cấp hạ tầng, tài nguyên Trung tâm dữ liệu
7	TTDL_BM_08	2.0	Biểu mẫu đề nghị cấp tài khoản mạng riêng ảo (VPN) truy cập hệ thống tại Trung tâm dữ liệu

TTDL_BM_01 - Biểu mẫu phiếu yêu cầu vào, ra TTDL

PHIẾU ĐĂNG KÝ VÀO, RA TRUNG TÂM DỮ LIỆU
Số: ...../20….

I. Thông tin chung của đơn vị yêu cầu

1. Tên cơ quan/đơn vị: .....

2. Họ và tên: .....

3. Chức vụ: ..... Điện thoại:..... Email: .....

4. Mục đích, công việc yêu cầu:

4.1. Vị trí

□ Phòng nguồn □ Phòng server

□ …….

4.2. Nâng cấp, bảo trì thiết bị

Máy chủ : □ Mạng : □

Lưu trữ : □ Đường truyền : □

Thiết bị khác: □……

4.3. Lắp thiết bị mới

Máy chủ : □ Mạng : □

Lưu trữ : □ Đường truyền : □

Thiết bị khác: □……

4.4. Di dời thiết bị

Máy chủ : □ Mạng : □

Lưu trữ : □ Đường truyền : □

Thiết bị khác: □……

4.5. Công việc khác

.....

Mô tả chi tiết:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Thời gian thực hiện:

Từ ... giờ … đến … giờ … ngày …../...../20.....

Tên người thực hiện:

II. Thông tin của đơn vị quản lý, vận hành TTDL

1. Họ và tên cán bộ phân công giám sát: .....

2. Tình trạng công việc sau khi xử lý:

2.1. Hoàn thành: Có ○ Không ○

2.2. Ảnh hưởng đến HT khác: Có ○ Không ○

2.3. Kiểm tra vệ sinh: Có ○ Không ○

2.4. Tình trạng của các hệ thống khác có bình thường:

Có ○ Không ○

2.5. Đề nghị khác: Có ○ Không ○

Mô tả chi tiết:

.....

.....

.....

.....

.....

.....

.....

Thời gian cán bộ ra khỏi Trung tâm dữ liệu lúc: ..... giờ ....., ngày ...../...../20.....

……, ngày ….. tháng ….. năm 20….

Xác nhận của đơn vị yêu cầu	**Xác nhận của cán bộ quản lý, vận hành TTDL**
(ký, ghi rõ họ tên)	*(ký, ghi rõ họ tên)*

TTDL_BM_02 - Biểu mẫu đăng ký mang thiết bị vào ra TTDL

ĐĂNG KÝ MANG THIẾT BỊ VÀO RA TRUNG TÂM DỮ LIỆU

THÔNG TIN NGƯỜI ĐĂNG KÝ

Họ và tên:	Đơn vị:
Chức vụ:	Email:
Mã nhân viên:	Điện thoại:

ĐĂNG KÝ MANG THIẾT BỊ VÀO, RA TRUNG TÂM DỮ LIỆU

☐ MANG THIẾT BỊ VÀO

☐ MANG THIẾT BỊ RA

DANH SÁCH

STT	Tên thiết bị	Mã thiết bị (Serial)	Mục đích	Ghi chú

Người đăng ký	Chữ ký	Ngày
Trưởng bộ phận người đăng ký	Chữ ký	Ngày
Lãnh đạo Trung tâm Hạ tầng số	Chữ ký	Ngày

TTDL_BM_03 - Biểu mẫu Nhật ký vào ra TTDL

NHẬT KÝ VÀO, RA TRUNG TÂM DỮ LIỆU

Nhật ký truy cập Trung tâm dữ liệu							
Họ và tên	**Số CMND/Hộ chiếu**	**Mục đích**	**Thời gian vào**	**Thời gian ra**	**Chữ ký**	**Người giám sát**	**Chữ ký**

TTDL_BM_05 - Biểu mẫu biên bản đặt thiết bị tại TTDL

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN BẢN ĐẶT THIẾT BỊ TẠI TRUNG TÂM DỮ LIỆU

Căn cứ ……..……

Hôm nay, ngày …. tháng …. năm ……, tại ……, chúng tôi gồm:

BÊN GIAO (Bên A): ……..……

Địa chỉ: ……..…

Điện thoại: ……..……..…. Fax: ……..……..……

Đại diện:

- Ông/Bà: …… Chức vụ: ……...……

- Ông/Bà: …… Cán bộ bàn giao thiết bị

BÊN NHẬN (Bên B): ……..……..……

Địa chỉ: ……..…

Điện thoại: ……..……..…. Fax: ……..……..……

Đại diện:

- Ông/Bà: …… Chức vụ: ……...……

- Ông/Bà: …… Cán bộ tiếp nhận thiết bị

I. Hai bên cùng tiến hành bàn giao các thiết bị theo danh sách sau:

TT	Tên thiết bị	Mô tả thiết bị	Đơn vị	Số lượng	Serial Number
1					
…					

Hai bên xác nhận đã giao và nhận đầy đủ danh mục thiết bị theo danh sách nêu trên.

1. Thông tin hạ tầng

- Vị trí lắp đặt: Tủ: ……..… Phòng: ……

- Nguồn điện: ……

2. Thông tin khác

……..

……..

II. Quyền hạn và trách nhiệm của hai bên

1. Bên A

Bên A tự cài đặt hệ điều hành và các phần mềm trên máy chủ đặt tại TTDL, đảm bảo các các phần mềm này không chứa phần mềm, tiện ích, công cụ phá hoại TTDL. Trường hợp Bên A vi phạm nghĩa vụ này, Bên A phải hoàn toàn chịu trách nhiệm theo quy định của pháp luật.

Bảo mật: bên A chủ động tự bảo mật các tài khoản đăng nhập vào hệ thống và dữ liệu được cài trên máy chủ.

Sao lưu (backup) dữ liệu: Việc quản lý dữ liệu, cập nhật và dự phòng hệ thống do Bên A tự thực hiện.

Có trách nhiệm bảo mật quyền truy nhập từ xa do Bên B cấp. Trường hợp bên A sử dụng hoặc cung cấp cho bên thứ ba quyền truy nhập từ xa để thực hiện các hành vi vi phạm pháp luật thì Bên A hoàn toàn chịu trách nhiệm về hành vi của mình.

Tuân thủ theo đúng các quy định của Nhà nước về sử dụng dịch vụ Internet, quyền sở hữu công nghiệp, bản quyền phần mềm cài đặt trên máy chủ (nếu có).

Cung cấp cho bên B đầu mối liên lạc về mặt kỹ thuật và điều hành chung cho bên A và thông báo ngay khi có thay đổi.

- Lãnh đạo phụ trách trực tiếp:

- Cán bộ kỹ thuật đầu mối:

2. Bên B

Cung cấp đầy đủ các hạ tầng vật lý, mạng (network), tường lửa (firewall) đã được đầu tư tại TTDL, hướng dẫn Bên A thực hiện đúng quy trình khai thác dịch vụ.

Quản trị máy chủ máy chủ bao gồm các công việc: theo dõi về mặt vật lý các máy chủ đặt tại TTDL, cập nhật các bản vá lỗi của chương trình diệt virus (nếu có),...; không chịu trách nhiệm các trường hợp máy chủ bị tấn công trực tiếp do lỗi từ website hay các phần mềm chuyên dùng do Bên A cài đặt trên máy chủ.

Trường hợp máy chủ bên A có sự cố liên quan đến các thiết bị phần cứng, Bên B có trách nhiệm thông báo cho Bên A và phối hợp với Bên A lên phương án thay thế thiết bị khác.

Bảo đảm hệ thống hoạt động thông suốt 24/24 giờ trong ngày, 07 (bảy) ngày trong tuần ngoại trừ các trường hợp bất khả kháng (như: thiên tai, địch họa, lũ lụt, bão, hoả hoạn, động đất hoặc các hiểm họa thiên tai khác; hay bất kỳ sự kiện nào khác xảy ra ngoài tầm kiểm soát của bất kỳ Bên nào và không thể lường trước được).

Đầu mối liên hệ của bên B:

- Lãnh đạo phụ trách trực tiếp:

- Cán bộ kỹ thuật đầu mối:

- Số điện thoại đơn vị:

Biên bản được lập thành 02 (hai) bản, mỗi bên giữ 01 (một) bản có giá trị pháp lý như nhau./.

Cán bộ tiếp nhận thiết bị	**Cán bộ bàn giao thiết bị**
(Ký, ghi rõ họ tên)	*(Ký, ghi rõ họ tên)*
ĐẠI DIỆN BÊN NHẬN	**ĐẠI DIỆN BÊN GIAO**
(Ký, đóng dấu, ghi rõ chức vụ, họ tên)	*(Ký, đóng dấu, ghi rõ chức vụ, họ tên)*

TTDL_BM_06 - Hồ sơ thiết bị đặt trong TTDL

HỒ SƠ THIẾT BỊ ĐẶT TRONG TRUNG TÂM DỮ LIỆU

Thiết bị	**Mô tả** *(đơn vị quản lý, cán bộ kỹ thuật, dịch vụ, ...)*	**Serial/ MAC/ Service tag của thiết bị**	**IP**	**Ghi Chú**
				- Ngày đưa Thiết bị vào Trung tâm dữ liệu: .../.../20...
				- Ngày đưa thiết bị vào TTDL: .../.../20....
…	…	…	..	…

TTDL_BM_07 - Biểu mẫu đề nghị cấp hạ tầng, tài nguyên TTDL

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG **<TÊN ĐƠN VỊ>**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:……./…….	*Hà Nội, ngày tháng năm*

V/v đề nghị cấp hạ tầng, tài nguyên trung tâm dữ liệu

Kính gửi: Cục Chuyển đổi số

Căn cứ Quy chế quản lý, vận hành và khai thác Trung tâm dữ liệu (ban hành kem theo Quyết định số…../QĐ-CĐS ngày / /2025 của Cục trưởng Cục Chuyển đổi số);

Căn cứ pháp lý khác có liên quan khác;

Để thuận tiện trong việc triển khai các nhiệm vụ được giao trên môi trường điện tử, <Cơ quan, đơn vị> trân trọng đề nghị Cục Chuyển đổi số cấp hạ tầng, tài nguyên,…tại Trung tâm dữ liệu cho <Cơ quan, đơn vị> *(thông tin chi tiết thông hạ tầng, tài nguyên cung cấp tại Phụ lục I, Phụ lục II gửi kèm công văn này).*

Đầu mối trao đổi thông tin xin liên hệ: Ông/bà:……., tên đơn vị, số điện thoại di động, email.

Trân trọng./.

Nơi nhận: - Như trên; -….. -Lưu: VT.	**THỦ TRƯỞNG ĐƠN VỊ** *(Ký, Họ và tên, đóng dấu)*

PHỤ LỤC I: THÔNG TIN CẤU HÌNH MÁY CHỦ ẢO ĐỀ NGHỊ CUNG CẤP

(Kèm theo công văn số……/…..ngày tháng năm của <Đơn vị>)

TT	**Mô tả mục đích sử dụng máy chủ**	**Tên dự án**	**Cấu hình**				**Yêu cầu Băng thông mạng**		**Cổng kết nối mạng nội bộ**			**Cổng public ra internet**			**Thông tin về phần mềm cài đặt**			**Đầu mối kỹ thuật và quản lý**			
			CPU (core)	RAM (GB)	Lưu trữ (GB)	Dự kiến tăng trưởng (03 năm)	Băng thông internet tối đa dự kiến (Up/Down Mbps)	Băng thông nội bộ tối đa dự kiến (Up/Down Mbps)	Cổng mở trên máy chủ/ đường dẫn website, dịch vụ	Đối tượng truy cập	Mục đích sử dụng	Cổng mở trên chủ	Đối tượng truy cập	Mục đích sử dụng	Tên phần mềm	Phiên bản	Bản quyền	Tên	Đơn vị	Email	Số ĐT
..																					
..																					

PHỤ LỤC II: THÔNG TIN THIẾT BỊ SỬ DỤNG ĐỂ TRUY CẬP MẠNG RIÊNG ẢO (VPN) PHỤC VỤ QUẢN TRỊ MÁY CHỦ ỨNG DỤNG, PHẦN MỀM, CƠ SỞ DỮ LIỆU

(Kèm theo công văn số……/.....ngày tháng năm của <Đơn vị>)

TT	**Loại thiết bị** (Laptop, PC,…)	**Cán bộ quản trị thiết bị**	**Thiết bị của** (cá nhân, đơn vị)	**Đơn vị quản lý thiết bị**	**Các địa chỉ MAC của thiết bị**	**Hệ điều hành sử dụng**	**Các phần mềm cài đặt phục vụ quản trị**	**Danh sách IP, Port phục vụ quản trị của máy chủ, thiết bị cần kết nối**	**Loại kết nối quản trị**
..									
..									

TTDL_BM_08 - Biểu mẫu đề nghị cấp tài khoản VPN trung tâm dữ liệu

THÔNG TIN ĐĂNG KÝ CẤP TÀI KHOẢN VPN

(Kèm theo công văn số……/.....ngày tháng năm của <Đơn vị>)

TT	Họ và tên	Đơn vị	Số CMND/Hộ chiếu	Địa chỉ	Điện thoại	Cán bộ phụ trách tài khoản VPN	Mục đích sử dụng tài khoản VPN	Ghi chú
…								