ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 3039/QĐ-UBND	*Quảng Nam, ngày 18 tháng 12 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành và khai thác Trung tâm tích hợp dữ liệu tỉnh Quảng Nam

ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15/11/2018;

Căn cứ Luật Giao dịch điện tử ngày 22/6/2023;

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

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; Nghị định số 27/2018/NĐ-CP ngày 01/3/2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 72/2013/NĐ-CP ngày 15/7/2013;

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

Căn cứ Nghị định số 151/2017/NĐ-CP ngày 26/12/2017 của Chính phủ về quy định chi tiết một số điều của Luật Quản lý, sử dụng tài sản công;

Căn cứ Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về Quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;

Căn cứ Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu; Thông tư số 23/2022/TT-BTTTT ngày 30/11/2022 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 370/TTr-STTTT ngày 25/11/2024.

QUYẾT ĐỊNH:

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

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc các Sở, Ban, ngành; Chủ tịch UBND các huyện, thị xã, thành phố; Thủ trưởng các cơ quan, đơn vị, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành quyết định này.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- TTTU, TT HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- CPVP;
- Lưu: VT, KGVX (H).

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

Hồ Quang Bửu

ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Quản lý, vận hành và khai thác Trung tâm tích hợp dữ liệu tỉnh Quảng Nam

(Kèm theo Quyết định số 3039 /QĐ-UBND ngày 18 /12/2024 của UBND tỉnh Quảng Nam)

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 tích hợp dữ liệu tỉnh Quảng Nam. 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, Chính quyền, Đoàn thể trên địa bàn tỉnh Quảng Nam (gọi tắt là cơ quan, đơn vị, địa phương); các tổ chức, cá nhân có liên quan tham gia quản lý, vận hành và khai thác Trung tâm Tích hợp dữ liệu tỉnh Quảng Nam.

Điều 3. Giải thích từ ngữ

1. Công nghệ thông tin (sau đây viết tắt là CNTT) là tập hợp các phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

2. Ứng dụng CNTT (trích dẫn theo khoản 5 Điều 4 Luật Công nghệ thông tin) là việc sử dụng CNTT vào các hoạt động thuộc lĩnh vực kinh tế - xã hội, đối ngoại, quốc phòng, an ninh và các hoạt động khác nhằm nâng cao năng suất, chất lượng, hiệu quả của các hoạt động này.

3. Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

4. Mạng diện rộng (tên tiếng Anh là Wide Area Network, viết tắt là WAN) của tỉnh được thiết lập trên cơ sở hạ tầng mạng viễn thông, thông qua đầu mối Trung tâm tích hợp dữ liệu tỉnh kết nối với mạng nội bộ các cơ quan, đơn vị, địa phương phục vụ công tác chuyên môn nghiệp vụ và công tác quản lý nhà nước trên địa bàn tỉnh, đồng thời kết nối với mạng truyền số liệu chuyên dùng của Chính phủ phục vụ công tác chỉ đạo điều hành từ Trung ương đến địa phương.

5. SD-WAN (viết tắt của cụm từ tiếng Anh: Software Defined - Wide Area Network) là một giải pháp mạng WAN được định nghĩa bằng phần mềm. SD-WAN sử dụng các công nghệ ảo hóa và quản lý tập trung bằng phần mềm để cải thiện hiệu quả, tính linh hoạt và an ninh mạng của tỉnh.

6. 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, viết tắt là mạng TSLCD). Mạng TSLCD bao gồm: mạng TSLCD cấp I và mạng TSLCD cấp II (được quy định tại 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).

7. Hệ thống thông tin (sau đây viết tắt là HTTT) là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

8. An toàn thông tin (sau đây viết tắt là ATTT) mạng là sự bảo vệ thông tin, HTTT trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

9. Sự cố ATTT là việc thông tin, HTTT bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

10. Trung tâm tích hợp dữ liệu của tỉnh (viết tắt là TTTHDL) là nơi tập trung các thiết bị CNTT và viễn thông chuyên dụng với khả năng lưu trữ, xử lý dữ liệu lớn, hệ thống bảo mật an toàn dữ liệu, hệ thống phụ trợ, mạng diện rộng, mạng chuyên dùng và toàn bộ các hệ thống phần mềm ứng dụng CNTT dùng chung của tỉnh và các cơ quan, đơn vị, địa phương trên địa bàn tỉnh, TTTHDL bao gồm:

a) Trung tâm tích hợp dữ liệu chính (tên tiếng Anh là Data Center, viết tắt là DC);

b) Trung tâm tích hợp dữ liệu dự phòng (tên tiếng Anh là Disaster Recovery, viết tắt là DR) là nơi dự phòng cho DC trong trường hợp DC gặp sự cố hoặc thực hiện bảo trì hệ thống.

11. UPS (viết tắt của cụm từ tiếng Anh: Uninterruptible Power Supply): là thiết bị được thiết kế để cung cấp nguồn điện không bị gián đoạn vào các thiết bị điện tử như máy tính, máy chủ hoặc các thiết bị đòi hỏi nguồn điện liên tục khác.

12. VPN (viết tắt của cụm từ tiếng Anh: Virtual Private Network): là mạng riêng ảo giúp tạo kết nối an toàn, mã hóa giữa thiết bị của người dùng và internet thông qua máy chủ trung gian.

Điều 4. Cơ quan chủ sở hữu, quản lý, vận hành và khai thác

1. Cơ quan chủ sở hữu TTTHDL: UBND tỉnh Quảng Nam (gọi tắt là cơ quan chủ quản).

2. Cơ quan quản lý: Sở Thông tin và Truyền thông tỉnh Quảng Nam (gọi tắt là cơ quan quản lý).

3. Đơn vị trực tiếp quản lý, vận hành và khai thác: Trung tâm Công nghệ thông tin và Truyền thông Quảng Nam trực thuộc Sở Thông tin và Truyền thông tỉnh Quảng Nam (gọi tắt là đơn vị quản lý, vận hành).

Điều 5. Kiến trúc của DC, DR và dịch vụ tại TTTHDL

1. Kiến trúc của DC được chia làm các phân hệ sau:

a) Hệ thống máy chủ: bao gồm các máy chủ được đầu tư phục vụ cho ứng dụng trong hoạt động CNTT với khả năng sẵn sàng nâng cấp, mở rộng số lượng máy chủ trong tương lai. Hệ thống máy chủ có khả năng cung cấp năng lực tính toán cho nhiều nền tảng với nhiều mục đích khác nhau như: các ứng dụng dùng chung, ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành và các hệ thống ứng dụng thông tin khác;

b) Hệ thống 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 DC 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;

c) Hệ thống lưu trữ: bao gồm các thiết bị lưu trữ chuyên dụng với năng lực quản lý tập trung và lưu trữ dữ liệu lớn đảm bảo cho mục đích sao lưu, khôi phục dữ liệu nếu có xảy ra sự cố. Hệ thống lưu trữ được thiết kế bảo đảm khả năng mở rộng đáp ứng nhu cầu phát triển nguồn dữ liệu trong tương lai;

d) Hệ thống đảm bảo ATTT

- Bao gồm các thiết bị tường lửa cho lớp mạng, dữ liệu và lớp ứng dụng, các thiết bị ngăn chặn xâm nhập trái phép, thiết bị cân bằng tải, phòng chống thất thoát dữ liệu, dịch vụ tình báo các mối đe dọa (Threat Intelligence), hệ thống kiểm soát ra/vào, camera giám sát và các ứng dụng an ninh HTTT. Mỗi thành phần trong hệ thống ATTT đều được thiết kế bảo đảm tính dự phòng và bổ sung, hỗ trợ lẫn nhau trong toàn hệ thống CNTT. Hệ thống đảm bảo ATTT theo các quy định của pháp luật hiện hành như: Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông và TCVN 11930:2017 về bảo đảm an toàn HTTT theo cấp độ. Việc đảm bảo ATTT của DC tuân thủ và đáp ứng các yêu cầu, tiêu chí trong bảo đảm an toàn HTTT cấp độ 3;

- Bảo đảm ATTT tại các cơ quan, đơn vị, địa phương: thực hiện đảm bảo an toàn các HTTT tại cơ quan, đơn vị, địa phương mình theo quy định. Đồng thời, các HTTT tại các cơ quan, đơn vị, địa phương sẽ được tăng cường hỗ trợ đảm bảo ATTT thông qua các thiết bị kết nối SD-WAN và được hỗ trợ giám sát ATTT bởi Trung tâm giám sát ATTT tỉnh Quảng Nam (Security Operation Center-SOC).

đ) Hệ thống 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 CNTT trong các cơ quan, địa phương và phục vụ người dân, doanh nghiệp đã được UBND tỉnh phê duyệt và cho phép triển khai;

e) Hệ thống mạng: hệ thống mạng được thiết kế theo mô hình mô-đun hóa với các vùng mạng chuyên biệt dành cho các mục đích, chức năng riêng biệt, cho phép áp dụng các chính sách bảo mật riêng cho mỗi vùng, thuận tiện cho việc quản lý và đầu tư thiết bị công nghệ. Hệ thống mạng tại DC được phân chia thành các vùng

mạng, bao gồm:

- Vùng mạng biên (Perimeter): gồm thiết bị tường lửa phục vụ kiểm soát các kết nối từ bên trong ra mạng ngoài và từ bên ngoài vào, thiết bị firewall sẽ thực hiện việc phân đoạn mạng thành các vùng khác nhau để kiểm soát vào ra. Thiết bị tường lửa tại vùng này cần cấu hình cao, hoạt động theo mô hình failover, có khả năng ảo hóa và phân tách thành nhiều tường lửa ảo để kiểm soát kết nối cho các kết nối khác nhau như Internet, TSLCD, ... Các chức năng chính cần có trên thiết bị tường lửa vùng mạng biên như: Firewall, URL Filtering, Anti-virus/Anti-malware, IPS (viết tắt của cụm từ tiếng Anh: Intrusion Prevention System là hệ thống phát hiện xâm nhập, với khả năng không chỉ theo dõi và cảnh báo mà còn có thể can thiệp và ngăn ngừa các tấn công). Ngoài ra, thiết bị tường lửa (tiếng Anh là Firewall) vùng mạng biên với chức năng kết nối SD-WAN sẽ giúp triển khai kết nối mạng WAN trên công nghệ SD-WAN toàn tỉnh và tập trung các kết nối đường truyền mạng Internet, mạng TSLCD;

- Vùng mạng lõi (Core): là vùng mạng tập trung lưu lượng giữa các vùng mạng trong nội bộ hệ thống. Các thiết bị chuyển mạch vùng mạng lõi có hiệu năng cao, độ trễ thấp nhằm đảm bảo kết nối giữa các vùng mạng nội bộ hệ thống với tốc độ cao, không gây trễ hoặc nghẽn mạng, đồng thời đảm bảo khả năng mở rộng hệ thống mạng trong tương lai. Phân vùng mạng lõi của hệ thống được thiết kế theo kiến trúc Spine - Leaf;

- Vùng mạng máy chủ (Server Farm): là nơi triển khai các hệ thống máy chủ ứng dụng, dịch vụ, dữ liệu và thiết bị lưu trữ dự phòng phục vụ triển khai các phần mềm ứng dụng nghiệp vụ dùng chung toàn tỉnh. Vùng mạng máy chủ được phân tách thành các vùng mạng nhỏ hơn, bao gồm:

+ Vùng mạng máy chủ ứng dụng, dịch vụ (SVR_APP): là nơi triển khai các máy chủ ứng dụng, dịch vụ các hệ thống;

+ Vùng mạng máy chủ cơ sở dữ liệu (SVR_DB): là nơi triển khai các máy chủ cơ sở dữ liệu phục vụ các hệ thống ứng dụng, dịch vụ;

+ Vùng mạng phục vụ phát triển, kiểm thử (DEV/TEST): là nơi triển khai các máy chủ ứng dụng, dịch vụ, dữ liệu phục vụ phát triển và kiểm thử các hệ thống ứng dụng, dịch vụ;

+ Vùng DMZ: là vùng mạng được phân tách về mặt logic, phục vụ triển khai các máy chủ được public ra môi trường mạng ngoài (ví dụ như máy chủ Proxy, các máy chủ web công cộng, …). Vùng mạng DMZ được tăng cường bảo đảm ATTT với các thiết bị, giải pháp ATTT như tường lửa ứng dụng Web (WAF), cân bằng tải ứng dụng (ADC);

+ Vùng mạng quản trị (Management): là vùng mạng phục vụ quản trị tập trung các trang thiết bị phục vụ hệ thống, cho phép cán bộ quản trị, vận hành có khả năng quản trị từ xa các thiết bị như thiết bị mạng, tường lửa, máy chủ, thiết bị lưu trữ dự phòng, … Ngoài ra, các thiết bị, giải pháp bảo đảm ATTT tập trung cũng sẽ được triển khai tại vùng mạng này;

+ Vùng mạng quản trị là vùng mạng tập trung toàn bộ các kết nối quản trị từ các thiết bị mạng tới thiết bị switch quản trị tập trung, vùng quản trị được thiết kế tách biệt với các phân vùng dữ liệu đảm bảo tránh xung đột với dữ liệu trong mạng;

+ Vùng mạng quản trị là nơi triển khai các thiết bị quản trị mạng SDN, phục vụ quản lý, điều khiển tập trung các trang thiết bị chuyển mạch Spine-Leaf cũng như cấu hình tập trung các chính sách mạng;

+ Vùng mạng quản trị cũng là nơi triển khai các giải pháp bảo đảm ATTT tập trung, phục vụ bảo vệ hệ thống DC-DR cũng như hỗ trợ bảo vệ hệ thống mạng tại các cơ quan, đơn vị, địa phương trên địa bàn tỉnh;

+ Vùng mạng nội bộ (LAN): là vùng mạng triển khai các trang thiết bị đầu cuối như máy tính cá nhân, máy tính xách tay, … phục vụ công tác vận hành, khai thác và quản trị toàn bộ hệ thống của các cán bộ kỹ thuật, quản trị viên.

g) Các hệ thống phụ trợ: hệ thống nguồn điện, hệ thống làm mát, thiết bị lưu điện UPS, thiết bị giám sát môi trường, máy phát điện dự phòng, sàn nâng, hệ thống phòng cháy và chữa cháy, hệ thống camera giám sát, hệ thống quản lý truy nhập (door access control), ... được thiết kế theo tiêu chuẩn TIA 942-TIER 3 bảo đảm các thiết bị luôn hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

2. Kiến trúc của DR được chia làm các phân hệ sau:

a) Hệ thống mạng

- Đường truyền kết nối Internet, WAN:

+ Đường truyền kết nối Internet: 02 đường Leasedline của 02 nhà cung cấp dịch vụ khác nhau, sử dụng giao thức định tuyến BGP (viết tắt của cụm từ tiếng Anh là Border Gateway Protocol) thiết lập và kiểm soát kết nối internet vào các hệ thống ứng dụng của DR.

+ Đường truyền kết nối WAN: kết nối đến mạng nội bộ tại các cơ quan, đơn vị, địa phương trên địa bàn tỉnh, sử dụng kết nối mạng truyền số liệu chuyên dùng để khai thác và sử dụng các ứng dụng bên trong DR và đường truyền cáp quang kênh trắng kết nối giữa DR và Sở Thông tin và Truyền thông.

- Thiết bị định tuyến vùng internet: sử dụng thiết bị có hiệu năng cao, dung lượng bộ nhớ RAM lớn để sẵn sàng cho việc lưu trữ các bảng định tuyến của giao thức BGP.

Ngoài các liên kết đến các thiết bị bảo mật thông qua thiết bị chuyển mạch lõi, về mặt logic thiết bị định tuyến vùng internet được kết nối trực tiếp đến phân vùng máy chủ Edge Server thuộc VLAN 40-50.

Về mặt vật lý, các kết nối giữa thiết bị chuyển mạch lõi và thiết bị định tuyến vùng internet sử dụng các đường cáp đồng 1GE và kết nối ra Internet qua những đường Leasedline do nhà cung cấp dịch vụ cung cấp, cụ thể: Thiết bị định tuyến vùng internet kết nối Leasedline Internet đến thiết bị chuyển mạch lõi, VLAN được thiết lập trên thiết bị chuyển mạch lõi đóng vai trò kết nối trung gian các thiết bị Router và Firewall.

- Thiết bị chuyển mạch lõi (tiếng Anh là Core Switch): Thiết bị Core Switch sử dụng chủng loại Switch Layer 3 cỡ lớn, thiết bị Core Switch cung cấp các dịch vụ mạng thiết yếu và liên thông giữa các phân hệ mạng, khả năng sẵn sàng và ổn định cao ở mức mạng, đồng thời cung cấp khả năng cân bằng lưu thông mạng ở tốc độ cao giữa các phân hệ bên trong DR.

b) Hệ thống bảo mật

Hệ thống bảo mật, bảo đảm ATTT theo các quy định của pháp luật hiện hành như: Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ. Việc bảo đảm an toàn các HTTT của DR tuân thủ và đáp ứng các yêu cầu, tiêu chí trong bảo đảm ATTT cấp độ 3.

- Thiết bị Firewall vùng mạng lõi:

Vùng mạng lõi tập trung toàn bộ các kết nối giữa vùng máy chủ ảo hóa tới các vùng khác của DR. Vùng mạng lõi là nơi có lưu lượng trao đổi dữ liệu rất lớn, bên cạnh đó mức độ quan trọng cao, thiết bị bảo mật tại vùng mạng lõi sử dụng thiết bị Firewall chuyên dụng đảm bảo năng lực xử lý cao, các tính năng bảo mật phải ở mức cao nhất. Kết nối từ Firewall tới thiết bị Core Switch là giao tiếp 1GE.

Thiết bị Firewall vùng mạng lõi kiểm soát các kết nối vào và ra giữa vùng Service Server, vùng Public Server với vùng Internal Server và thiết lập chính sách cho việc kết nối giữa các vùng mạng này với hệ thống mạng WAN của tỉnh.

Tính năng IPS giúp phát hiện và ngăn chặn các tấn công có thể xảy ra từ các vùng mạng WAN hoặc từ internet vào các vùng server.

Toàn bộ các server thuộc DR được cài đặt phần mềm antivirus để giảm thiểu nguy cơ lây nhiễm virus trong quá trình sử dụng, quá trình kết nối quản trị, cập nhật...

- Firewall vùng truy cập Internet:

Thành phần thiết bị bảo mật trong vùng này bao gồm thiết bị Firewall, thiết bị Web Application Firewall bảo vệ các ứng dụng Web và thiết bị bảo mật thư điện tử.

Kết nối từ Firewall đến Router internet là giao tiếp có tốc độ 1GE.

Kết nối từ Firewall vào vùng Core là giao tiếp có tốc độ 1GE.

c) Hệ thống máy chủ

Hệ thống máy chủ là hệ thống các máy chủ rack cỡ lớn với kết nối quang đến thiết bị Core Switch với băng thông 10 Gbps, có khả năng ảo hóa ra một số lượng lớn máy chủ để phục vụ nhiều ứng dụng độc lập cho nhiều cơ quan, đơn vị, địa phương khác nhau cùng khai thác trong DR.

d) Hệ thống lưu trữ

- Lưu trữ sử dụng SAN để đảm bảo hoạt động ở đường truyền FC tốc độ cao cũng như yêu cầu công nghệ tiên tiến sẵn sàng cao của tủ đĩa cũng như phần mềm ảo hóa. Các thành phần trong tủ đĩa như Controller, số cổng FC phải đảm bảo dự

phòng. Công nghệ RAID và ổ cứng SAS hay SATA.

- Sao lưu dữ liệu dự phòng ra hệ thống NAS chuyên dụng, có khả năng mở rộng cũng như dung lượng lớn, chuyên nghiệp, dễ dàng cho việc quản trị sao lưu tập trung.

Hệ thống Backup sao lưu dữ liệu thông qua môi trường Ethernet, thiết bị NAS sẽ được kết nối vào thiết bị Core Switch. Các máy chủ cần backup sẽ được kết nối với máy chủ điều khiển Backup thông qua Agent. Phần mềm điều khiển việc sao lưu sẽ được cài đặt lên 01 Server Backup để quản lý các máy chủ cần sao lưu dữ liệu. Máy chủ điều khiển backup sẽ điều khiển việc backup dữ liệu qua NAS như đặt lịch cho việc backup (thời gian backup, backup hàng ngày, backup định kỳ,..).

e) Hệ thống phụ trợ: hệ thống nguồn điện, hệ thống làm mát, thiết bị lưu điện UPS, thiết bị giám sát môi trường, máy phát điện dự phòng, sàn nâng, hệ thống phòng cháy và chữa cháy, hệ thống camera giám sát, hệ thống quản lý truy nhập (door access control), ... được thiết kế theo tiêu chuẩn TIA 942-TIER 3 bảo đảm các thiết bị luôn hoạt động trong môi trường tiêu chuẩn, ổn định với độ dự phòng cao.

3. Các dịch vụ, hệ thống phần mềm được cung cấp tại TTTHDL

a) Các dịch vụ, phần mềm, lưu trữ phục vụ cho việc triển khai các ứng dụng nền tảng số, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành của các cơ quan nhà nước trên địa bàn tỉnh.

b) Các dịch vụ CNTT khác, bao gồm:

- Vận hành máy chủ vật lý, máy chủ ảo, quản trị hạ tầng;

- Vận hành ứng dụng, số hóa;

- Lưu trữ, sao lưu, phục hồi dữ liệu;

- Rà quét, đánh giá, ứng cứu, khắc phục sự cố bảo mật ứng dụng;

- Tư vấn, tạo lập hồ sơ đề xuất cấp độ ATTT;

- Các dịch vụ khác theo quy định của cơ quan có thẩm quyền.

Chương II

QUY ĐỊNH TRONG QUẢN LÝ, VẬN HÀNH VÀ KHAI THÁC

Điều 6. Yêu cầu chung

1. Yêu cầu đối với quản trị viên vận hành hệ thống

a) Đảm bảo tất cả các hoạt động về thiết bị phần cứng, phần mềm ứng dụng, hệ thống mạng, HTTT, thiết bị phụ trợ tại TTTHDL được hoạt động ổn định liên tục 24 giờ/ngày và 7 ngày/tuần;

b) Trong quá trình làm việc và trực vận hành tại TTTHDL phải tuân thủ theo các quy định và nội quy lao động;

c) Cán bộ, nhân viên quản trị, vận hành truy cập, khai thác thông tin tại

TTTHDL 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, địa phương khác triển khai tại TTTHDL;

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

2. Yêu cầu đối với các cơ quan, đơn vị, địa phương, cá nhân đến làm việc tại TTTHDL

a) Tuân thủ theo các nội quy, quy định làm việc;

b) Trong quá trình làm việc, chuyển giao công nghệ và xử lý nâng cấp, tích hợp, cài đặt,… phải được ghi chép cụ thể vào sổ nhật ký;

c) Không được mang, sử dụng các thiết bị điện tử, vật dụng khác gây nguy hại đến hoạt động của các HTTT (trừ trường hợp đặc biệt được sự chỉ đạo của lãnh đạo cấp trên cho phép).

Điều 7. Bảo đảm nguồn nhân lực

1. Cán bộ được tuyển dụng có trình độ, chuyên ngành về lĩnh vực CNTT, ATTT, phù hợp với vị trí tuyển dụng.

2. Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

3. Xây dựng kế hoạch và định kỳ hằng năm tổ chức đào tạo, bồi dưỡng về ATTT cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

4. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc

a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức;

b) Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Điều 8. Nguyên tắc về quản lý, vận hành và khai thác

1. Tuân thủ các nguyên tắc, bảo đảm cơ sở hạ tầng và HTTT phục vụ ứng dụng, phát triển CNTT theo Luật Công nghệ thông tin ngày 29/6/2006.

2. Tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật quy định áp dụng đối với Trung tâm dữ liệu theo Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013, Thông tư số 23/2022/TT-BTTTT ngày 30/11/2022 sửa đổi, bổ sung một số điều của Thông tư số 03/2013/TT- BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông; Tiêu chuẩn quốc gia TCVN 9250:2021 Trung tâm dữ liệu - Yêu cầu về hạ tầng kỹ thuật viễn thông.

3. Bảo đảm ATTT mạng theo Luật An toàn thông tin mạng ngày 19/11/2015; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông và bảo đảm các yêu cầu về ATTT theo Quy chế bảo đảm ATTT trong hoạt động ứng dụng CNTT của cơ quan nhà nước trên địa bàn tỉnh.

4. Việc quản lý, kết nối và chia sẻ dữ liệu của TTTHDL phải tuân thủ theo Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ.

5. Cơ quan quản lý, đơn vị quản lý, vận hành TTTHDL sử dụng, quản lý tài sản theo đúng các quy định hiện hành về quản lý, sử dụng tài sản công và được phép thuê dịch vụ đảm bảo vận hành các hệ thống thông tin, triển khai cung cấp các dịch vụ sự nghiệp công theo quy định của pháp luật trên cơ sở đảm bảo khai thác an toàn, hiệu quả hạ tầng hiện có.

6. Các cơ quan, đơn vị, địa phương sử dụng dịch vụ của TTTHDL phải tuân thủ và chịu trách nhiệm về mọi hoạt động theo các quy định của cơ quan nhà nước về ứng dụng CNTT và bảo đảm an toàn, an ninh thông tin.

7. Các hệ thống CNTT đã, đang sử dụng mà thường xuyên không phát sinh dữ liệu hoặc không sử dụng 06 tháng liên tục sẽ bị thu hồi tài nguyên để phục vụ cho các hệ thống khác nhằm tối ưu tài nguyên của TTTHDL.

Điều 9. Quy định quản trị hệ thống mạng, bảo mật mạng

1. Hệ thống mạng hoạt động liên tục 24/7, ổn định, an toàn và đáp ứng được yêu cầu về băng thông cho các ứng dụng trong hệ thống.

2. 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:

a) Thực hiện kết nối từ xa bằng các hình thức kết nối đã được thiết lập các chính sách truy cập giới hạn quyền sử dụng theo quy định ATTT do đơn vị quản lý, vận hành cung cấp;

b) Các hình thức kết nối sẽ bị vô hiệu hóa khi vi phạm các chính sách ATTT;

c) Đơn vị quản lý, vận hành khi phát hiện các trường hợp truy cập hệ thống có dấu hiệu bất thường tiến hành ngăn chặn, thu hồi, khóa quyền truy cập và thông báo đến cơ quan, đơn vị sử dụng.

3. 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 phần mềm độc hại từ bên ngoài; cũng như ngăn chặn, không để phát tán phần mềm độc hại từ các thiết bị ngoại vi khác.

4. Đường truyền Internet cho TTTHDL tối thiểu phải từ 02 (hai) nhà cung cấp dịch vụ khác nhau để đảm bảo độ dự phòng cao và tính sẵn sàng cho hệ thống.

Điều 10. Quy định quản lý trang thiết bị, phần mềm

1. Thiết bị CNTT và các thiết bị phụ trợ đặt tại TTTHDL phải được đặt tên và dán nhãn tài sản nhà nước theo đúng tiêu chuẩn quy định.

2. Hằng năm đơn vị quản lý, vận hành thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị, thực hiện khấu hao tài sản và báo cáo về cơ quan quản lý theo quy định.

3. Đối với các trang thiết bị, phần mềm của TTTHDL

a) Đơn vị quản lý, vận hành đề xuất cập nhật bản quyền sử dụng, nâng cấp phần mềm, mua thêm thiết bị CNTT và các thiết bị phụ trợ khác trong trường hợp thiết bị hết hạn bảo hành, hư hỏng. Thiết bị được trang bị phải tuân theo các tiêu chuẩn về thiết bị cho TTTHDL;

b) Đối với thiết bị hỏng còn bảo hành, đơn vị quản lý, vận hành yêu cầu đơn vị cung cấp sửa chữa. Thiết bị hỏng đã hết bảo hành, xây dựng phương án sửa chữa, thay thế;

c) Thiết bị hư hỏng tại TTTHDL đơn vị quản lý, vận hành phải lập biên bản sự cố và báo cáo lên cơ quan quản lý để có biện pháp khắc phục kịp thời.

4. Đối với các trang thiết bị, phần mềm của cơ quan, đơn vị, địa phương đặt tại TTTHDL

a) Khi có nhu cầu lắp đặt trang thiết bị, phầm mềm hoặc cần cung cấp tài nguyên để cài đặt phần mềm, cơ sở dữ liệu để triển khai các ứng dụng trên nền tảng hạ tầng kỹ thuật của TTTHDL, các cơ quan, đơn vị, địa phương gửi văn bản đề nghị về cơ quan quản lý xem xét, quyết định;

b) Các cơ quan, đơn vị, địa phương phải thực hiện kiểm tra và phê duyệt cấp độ ATTT trước khi triển khai trên nền tảng hạ tầng kỹ thuật của TTTHDL, đồng thời các trang thiết bị, phần mềm được kết nối đến TTTHDL đáp ứng các yêu cầu về bảo đảm ATTT theo Quy chế này và các quy định hiện hành;

c) Cơ quan, đơn vị, địa phương chịu trách nhiệm quản trị, vận hành trang thiết bị, phần mềm của đơn vị mình (thực hiện từ xa hoặc trực tiếp) hoặc ủy quyền cho đơn vị quản lý, vận hành thực hiện; việc ủy quyền phải được thể hiện bằng văn bản ký kết, thống nhất giữa các bên;

d) Các trang thiết bị, phần mềm đặt tại TTTHDL là tài sản của cơ quan, đơn vị, địa phương được đơn vị quản lý, vận hành quy hoạch không gian, vị trí lắp đặt đáp ứng theo tiêu chuẩn của TTTHDL.

Điều 11. Quy định quản lý các hệ thống ứng dụng, phần mềm

1. Danh sách tài sản phần mềm 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 quản lý, 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, chương trình ứng dụng sử dụng tại TTTHDL phải được kiểm tra đánh giá ATTT trước khi sử dụng theo đúng quy định của pháp luật.

4. Đơn vị quản lý, vận hành phải thường xuyên theo dõi, cập nhật thời hạn sử

dụng các phần mềm, chương trình ứng dụng trình cấp có thẩm quyền phê duyệt để kịp thời có kế hoạch gia hạn hay nâng cấp.

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

a) Đối với phần mềm cài đặt mới tại TTTHDL

Phần mềm trước khi cài đặt phải đáp ứng được các yêu cầu về mặt kỹ thuật, đúng với hồ sơ thiết kế thi công được cơ quan có thẩm quyền phê duyệt; trước khi cài đặt phải rà quét nguy cơ tồn tại mã độc, phần mềm độc hại.

b) Đối với các hệ thống phần mềm đang khai thác sử dụng tại TTTHDL

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

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

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

Điều 12. Quy định sao lưu, phục hồi dữ liệu

1. Thực hiện lưu trữ các dữ liệu của người dùng, ứng dụng và hệ thống. Tùy theo từng loại dữ liệu, thực hiện lưu trữ đủ và đúng thời hạn theo quy trình sao lưu, phục hồi dữ liệu dự phòng cho các hệ thống tại TTTHDL.

2. Đơn vị quản lý, vận hành có trách nhiệm xây dựng và triển khai thực hiện quy trình sao lưu, phục hồi dữ liệu dự phòng cho các hệ thống tại TTTHDL theo hướng dẫn tại Công văn số 2517/BTTTT-CATTT ngày 27/6/2024 của Bộ Thông tin và Truyền thông về việc hướng dẫn một giải pháp tăng cường bảo đảm an toàn HTTT.

3. Dữ liệu phải được phân loại để lưu trữ theo thứ tự ưu tiên về mức độ quan trọng, sao lưu theo thời gian, loại thông tin, nơi lưu trữ.

4. Tần suất sao lưu tùy thuộc vào mức độ quan trọng dữ liệu và phải được kiểm soát và đối chiếu sau khi sao lưu.

Điều 13. Quy định quản trị bảo mật hệ thống

1. Duy trì, cập nhật, theo dõi thường xuyên đối với hệ thống bảo mật (thiết bị tường lửa, phần mềm phòng chống mã độc tập trung, thiết bị giám sát phát hiện, ngăn chặn xâm nhập trái phép và các thiết bị chuyên dụng có liên quan khác) để bảo đảm an toàn, bảo mật cho TTTHDL.

2. Tất cả các máy chủ, máy trạm tại TTTHDL phải được cài đặt phần mềm phòng chống mã độc tập trung và luôn được cập nhật kịp thời các bản sửa lỗi, các mẫu mã độc mới. Các thiết bị ngoại vi như ổ cứng di động, ổ cứng gắn ngoài và các thiết bị lưu trữ khác phải được kiểm tra, rà quét ATTT trước khi kết nối vào hệ thống.

3. Những máy tính khi phát hiện có phần mềm độc hại phải cách ly ngay khỏi hệ thống để tránh lây nhiễm sang các máy tính khác.

4. Việc thay đổi cấu hình của hệ thống bảo mật tại TTTHDL phải được sự thống nhất của cấp có thẩm quyền.

Điều 14. Quy định về an toàn hoạt động

1. TTTHDL phải có nội quy được giám sát thông qua các hệ thống kiểm soát truy cập và vào/ra.

2. TTTHDL chỉ được đặt các thiết bị đang hoạt động phục vụ vận hành hệ thống, tuyệt đối không đặt các thiết bị khác: thiết bị hỏng, thiết bị chờ thanh lý, thanh hủy, tài liệu, vật tư, các vật dụng dễ cháy nổ,…

3. TTTHDL phải đảm bảo vệ sinh: môi trường khô ráo, sạch sẽ, không dột, không thấm nước, không bị ánh nắng chiếu rọi trực tiếp. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị CNTT.

4. Hệ thống phòng cháy và chữa cháy phải đáp ứng theo tiêu chuẩn quy định cho TTTHDL, hằng năm thực hiện kiểm tra để đảm bảo an toàn cho người và hệ thống thiết bị.

5. Hệ thống điện phải ổn định, liên tục, được trang bị hệ thống lưu điện UPS và máy phát điện dự phòng đảm bảo cho các hệ thống hoạt động liên tục.

6. Hệ thống camera thực hiện giám sát toàn bộ TTTHDL hoạt động liên tục 24/7; dữ liệu hình ảnh phải được lưu trữ ít nhất trong thời gian là 30 ngày.

7. Hệ thống quản lý vào/ra hoạt động liên tục 24/7 và ghi đầy đủ nhật ký nhằm đảm bảo an ninh cho TTTHDL.

Điều 15. Quy định xử lý sự cố

1. Khi phát hiện sự cố cán bộ quản lý, vận hành thực hiện cô lập, hạn chế tối đa ảnh hưởng tới hoạt động của hệ thống đồng thời báo cáo cho lãnh đạo đơn vị quản lý, vận hành và đơn vị sử dụng về sự cố.

2. Tùy thuộc vào mức độ ảnh hưởng, các sự cố được đánh giá và phân loại như sau:

a) Các sự cố thông thường (không gây ảnh hưởng đến hoạt động của TTTHDL), đơn vị quản lý, vận hành phải nhanh chóng xử lý khắc phục;

b) Các sự cố nghiêm trọng (sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố liên quan đến an ninh thông tin, mất dữ liệu... gây ảnh hưởng trực tiếp đến hoạt động của TTTHDL), ngay sau khi phát hiện sự cố đơn vị quản lý, vận hành cần đánh giá ảnh hưởng của sự cố và thực hiện báo cáo về cơ quan quản lý để phối hợp với các đơn vị chuyên trách hướng dẫn xử lý khắc phục sự cố;

c) Các sự cố đặc biệt nghiêm trọng gây ngưng trệ đến toàn bộ hoạt động của TTTHDL, cơ quan quản lý, đơn vị vận hành phải có đánh giá ảnh hưởng của sự cố, phối hợp với các cơ quan chuyên môn liên quan đồng thời thực hiện báo cáo nhanh

về cơ quan chủ quản để có chỉ đạo 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 sự cố;

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

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

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

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

e) Tổng hợp báo cáo kết quả khắc phục sự cố về cơ quan quản lý cấp trên.

4. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố ATTT: tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin - Bộ Thông tin và Truyền thông, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) và Cục Kỹ thuật nghiệp vụ (A06) của Bộ Công an, Bộ Tư lệnh tác chiến Không gian mạng (BTL86) của Bộ Quốc phòng và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố.

Điều 16. Quy định duy trì, bảo trì, bảo dưỡng các hệ thống

1. Đơn vị quản lý, vận hành có trách nhiệm thực hiện duy trì, bảo trì, bảo dưỡng các hệ thống.

2. Đơn vị quản lý, vận hành quyết định lựa chọn hình thức duy trì, bảo trì, bảo dưỡng các hệ thống bằng hình thức tự thực hiện hoặc thuê dịch vụ đảm bảo tiết kiệm, hiệu quả, theo đúng quy định hiện hành.

3. Thời gian bảo trì, bảo dưỡng từng thiết bị, phần mềm thực hiện theo yêu cầu thực tiễn và khuyến nghị của nhà cung cấp. Bảo trì, bảo dưỡng tổng thể toàn bộ các hệ thống ít nhất 01 lần/01 năm.

4. Việc thực hiện duy trì, bảo trì, bảo dưỡng phải được thông báo bằng văn bản đến các tổ chức, đơn vị liên quan, hạn chế làm ảnh hưởng đến hoạt động các hệ thống của TTTHDL.

Điều 17. Quy định quản lý mật khẩu

1. Đơn vị quản lý, vận hành có trách nhiệm quản lý mật khẩu quản trị hệ thống.

2. Quản trị viên được giao quản lý mật khẩu quản trị hệ thống phải thực hiện đổi mật khẩu ít nhất 03 tháng/lần. Việc đổi mật khẩu quản trị hệ thống phải tuân thủ theo đúng quy định tại Công văn số 2517/BTTTT-CATTT ngày 27/6/2024.

3. Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn an ninh thông tin thì đơn vị quản lý, vận hành thực hiện việc thay đổi toàn bộ mật khẩu quản trị.

4. Thông tin mật khẩu không tiết lộ với bất kỳ ai, trường hợp bàn giao công việc hiện tại hoặc trường hợp khẩn cấp thì phải được sự đồng ý của lãnh đạo đơn vị

quản lý, vận hành.

5. 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) tối thiểu là 8 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 ký tự.

b) Nội dung mật khẩu:

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

- Không đặt theo ký tự chữ cái, chữ số tuần tự hoặc một dãy các ký tự giống nhau (ví dụ: 123456789, ABCDEFGH, …);

- Không đặt theo tên cơ quan, tổ chức, tên thiết bị, chức năng thiết bị;

- Mật khẩu phải bao gồm chữ cái thường, chữ cái in hoa, chữ số và ký tự đặc biệt;

- Mật khẩu không dùng chung với các thiết bị khác.

Điều 18. Quy định về kiểm tra, báo cáo

1. Cơ quan quản lý tổ chức kiểm tra việc tuân thủ các quy định về quản lý, vận hành và khai thác sử dụng TTTHDL. Các vấn đề phát hiện (nếu có) sau khi kiểm tra phải được tổng hợp, đánh giá phân tích mức độ ảnh hưởng hoạt động của TTTHDL và giao đơn vị quản lý, vận hành lập kế hoạch khắc phục xử lý.

2. Đơn vị quản lý, vận hành báo cáo định kỳ hằng quý, hằng năm cho cơ quan quản lý để tổng hợp báo cáo cơ quan chủ quản về kết quả vận hành, khai thác TTTHDL.

Chương III

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG VẬN HÀNH TTTHDL

Điều 19. 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) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn;

b) Thường xuyên kiểm tra cấu hình, các tệp nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có;

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm;

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp;

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc

không còn nhu cầu sử dụng;

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ

Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng như bên ngoài vào hệ thống.

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

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng;

b) Toàn bộ máy chủ và thiết bị CNTT không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

4. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm 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;

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

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

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 20. Quản lý an toàn dữ liệu

1. Xây dựng chính sách dự phòng và khôi phục dữ liệu

a) Xác định mục tiêu phục hồi, phạm vi dữ liệu cần sao lưu, dữ liệu quan trọng, hệ thống ứng dụng: cấu hình, cơ sở dữ liệu, mã nguồn, hệ điều hành;

b) Lựa chọn phương pháp sao lưu: sao lưu trực tuyến và sao lưu ngoại tuyến;

c) Lựa chọn công cụ và công nghệ: chọn phần mềm hoặc giải pháp sao lưu dữ liệu phù hợp với nhu cầu. Triển khai các công cụ tự động hóa sao lưu để giảm thiểu sai sót do con người và đảm bảo sao lưu đúng thời gian.

2. Thiết lập quy trình sao lưu: định kỳ sao lưu dữ liệu theo tần suất phù hợp;

quy định thời gian lưu trữ sao lưu và phương thức quản lý các phiên bản sao lưu; sao lưu phải được lưu trữ ở một hoặc nhiều vị trí an toàn; đảm bảo quy trình sao lưu và khôi phục dữ liệu tuân thủ các quy định và tiêu chuẩn ngành.

Điều 21. Quản lý an toàn thiết bị đầu cuối

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

a) Cài đặt hệ điều hành và phần mềm bảo mật; cài đặt các phần mềm ứng dụng cần thiết; cấu hình chính sách bảo mật;

b) Quản lý triển khai thiết bị: Sử dụng các phần mềm quản lý thiết bị đầu cuối để triển khai các cấu hình bảo mật, phần mềm, và cập nhật cho các thiết bị từ xa.

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

a) Xác thực đa yếu tố: yêu cầu người dùng phải cung cấp nhiều yếu tố xác thực như mật khẩu kết hợp với mã OTP gửi qua email, SMS hoặc ứng dụng xác thực;

b) Chính sách kiểm soát truy cập được áp dụng để đảm bảo chỉ có quyền truy cập vào các tài nguyên được phép.

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

a) Cài đặt thiết bị đầu cuối: kiểm tra phần cứng, phần mềm cần thiết, hệ điều hành, phần mềm bảo mật;

b) Kết nối thiết bị đầu cuối vào mạng: cấu hình kết nối mạng, kiểm tra kết nối đảm bảo thiết bị truy cập Internet, máy chủ, tài nguyên và các dịch vụ cần thiết;

c) Gỡ bỏ thiết bị đầu cuối: trước khi gỡ bỏ thiết bị khỏi hệ thống, đảm bảo ngắt kết nối mạng của thiết bị để ngăn chặn truy cập; gỡ bỏ các phần mềm, các công cụ quản lý thiết bị, phần mềm bảo mật, và các ứng dụng chuyên dụng; đảm bảo dữ liệu không bị rò rỉ; đảm bảo kết nối đã bị ngắt.

Điều 22. Quản lý điểm yếu ATTT

1. Quản lý thông tin điểm yếu ATTT đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); phân loại mức độ nguy hiểm của điểm yếu và xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Khi phát hiện điểm yếu ATTT ở mức độ nghiêm trọng cán bộ quản lý, vận hành thực hiện cảnh báo và xử lý điểm yếu ATTT theo chỉ đạo, việc xử lý điểm yếu ATTT phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu ATTT chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT đối với các điểm yếu khi cần thiết.

5. Kiểm tra, đánh giá và xử lý điểm yếu ATTT cho thiết bị hệ thống, máy chủ,

dịch vụ trước khi đưa vào sử dụng.

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

7. Nghiêm cấm thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của HTTT để thu thập, khai thác thông tin cá nhân.

Điều 23. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Khi truy cập, sử dụng tài nguyên hệ thống, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm ATTT;

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT;

c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

2. Trong quá trình sử dụng

a) Nghiêm túc chấp hành Quy chế này và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

c) Khi phát hiện nguy cơ hoặc sự cố mất ATTT mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách CNTT để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, bồi dưỡng, hội nghị về ATTT mạng được các cơ quan hoặc đơn vị chuyên môn tổ chức.

Điều 24. Quản lý hồ sơ, thiết kế, xây dựng hệ thống

1. Danh sách các loại hồ sơ lưu trữ:

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

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

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

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

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

e) Các hồ sơ, tài liệu kỹ thuật khác.

2. Thiết kế an toàn HTTT gồm:

a) Tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý

vận hành HTTT;

b) Tài liệu mô tả thiết kế và các thành phần của HTTT;

c) Tài liệu mô tả phương án bảo đảm ATTT theo cấp độ;

d) Tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT;

đ) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

3. Phát triển phần mềm thuê khoán gồm:

a) Biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán;

b) Các đơn vị xây dựng, phát triển hệ thống phải có trách nhiệm cung cấp mã nguồn phần mềm;

c) Phải thực hiện kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng;

d) Phần mềm, ứng dụng phải được kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng.

Điều 25. Vận hành thử hệ thống, kiểm thử phần mềm đặt tại TTTHDL

1. Đối với trang thiết bị của các cơ quan, đơn vị, địa phương có nhu cầu đặt tại TTTHDL: trước khi đưa vào sử dụng phải được vận hành thử 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 quản lý, vận hành chủ trì, phối hợp thực hiện.

2. Đối với các phần mềm nội bộ của các cơ quan, đơn vị, địa phương có nhu cầu đặt tại TTTHDL: trước khi đưa vào sử dụng chính thức phải được kiểm thử chấp nhận hoạt động 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 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 quản lý, vận hành phối hợp với đơn vị có chức năng, nhiệm vụ và năng lực đáp ứng yêu cầu triển khai thực hiện.

3. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

4. Báo cáo vận hành thử hệ thống, kiểm thử phần mềm phải được xác nhận của bộ phận chuyên trách và phê duyệt của cơ quan quản lý trước khi đưa vào sử dụng.

Chương IV

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ, ĐỊA PHƯƠNG, CÁ NHÂN TRONG VIỆC QUẢN LÝ, KHAI THÁC VÀ VẬN HÀNH - TỔ CHỨC THỰC HIỆN

Điều 26. 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, sửa đổi và mở rộng quy mô TTTHDL.

2. Hướng dẫn, triển khai các giải pháp bảo đảm ATTT mạng đối với các HTTT thuộc TTTHDL đảm bảo phù hợp với các quy định theo tình hình thực tế; quy hoạch tài nguyên hệ thống, các giải pháp, phương án kỹ thuật, các kế hoạch phát triển TTTHDL.

3. Thanh tra, kiểm tra và giám sát việc quản lý, vận hành, sử dụng khai thác dịch vụ của đơn vị quản lý, vận hành TTTHDL.

4. Thực hiện chế độ báo cáo định kỳ hằng năm và báo cáo đột xuất cho cơ quan chủ quản về tình hình hoạt động TTTHDL; đề xuất kinh phí ngân sách nhà nước thường xuyên hằng năm cho công tác quản lý, vận hành và bảo trì, bảo dưỡng, sửa chữa, duy trì đảm bảo hoạt động ổn định của các hệ thống, thiết bị tại TTTHDL.

5. Chịu trách nhiệm trước UBND tỉnh về việc quản lý, vận hành, khai thác TTTHDL đảm bảo ổn định, thông suốt, liên tục, an toàn bảo mật thông tin, quản lý tài sản theo đúng quy định.

6. Chủ trì tổ chức triển khai, hướng dẫn thực hiện Quy chế này; theo dõi, kiểm tra định kỳ báo cáo UBND tỉnh tình hình hoạt động và an toàn thông tin của TTTHDL.

Điều 27. Trách nhiệm của đơn vị quản lý, vận hành

1. Quản lý, vận hành và khai thác bảo đảm ATTT, hoạt động của các HTTT tại TTTHDL theo các quy định của Quy chế này; chịu trách nhiệm trước cơ quan quản lý về việc quản lý, tổ chức thực hiện vận hành toàn bộ hệ thống TTTHDL theo quy định.

2. Xây dựng và ban hành nội quy làm việc, các quy trình về vận hành, bảo trì, bảo dưỡng và khắc phục sự cố; quy trình cung cấp dịch vụ.

3. Tiếp nhận và triển khai các yêu cầu cung cấp dịch vụ của các cơ quan, đơn vị, địa phương trong phạm vi quy định; hướng dẫn các cơ quan, đơn vị sử dụng các dịch vụ của TTTHDL.

4. Phối hợp với các đơn vị chuyên môn thực hiện kiểm tra, xử lý và đánh giá hoạt động của các hệ thống; tham mưu cơ quan quản lý các giải pháp, phương án kỹ thuật, kế hoạch phát triển TTTHDL.

5. Hằng năm, lập dự toán kinh phí duy trì và đảm bảo hoạt động ổn định của các thiết bị và kinh phí vận hành, bảo trì, bảo dưỡng, sửa chữa, thay thế trang thiết

bị hoặc nâng cấp, cập nhật phần mềm quản lý, các chi phí khác để quản lý TTTHDL, chế độ trực 24/24 giờ cho nhân sự quản trị, vận hành tổng hợp chung trong dự toán chi của đơn vị, trình cấp có thẩm quyền phê duyệt.

6. Xây dựng kế hoạch tuyển dụng, đào tạo, bồi dưỡng, bố trí nhân sự quản lý, vận hành đảm bảo các hệ thống tại TTTHDL hoạt động an toàn, liên tục 24/7, kể cả các ngày nghỉ lễ, nghỉ tết.

7. Định kỳ hằng quý, hằng năm lập báo cáo công tác quản lý, vận hành về cơ quan quản lý.

Điều 28. Trách nhiệm của cơ quan, đơn vị, địa phương

1. Sử dụng cơ sở hạ tầng, dịch vụ của TTTHDL theo 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 và chuyển đổi số của các cơ quan nhà nước trên địa bàn tỉnh và các quy định về an toàn, bảo mật thông tin trong quản lý, vận hành và khai thác.

3. Đối với cơ quan, đơn vị có hệ thống thông tin đặt tại TTTHDL:

a) Chịu trách nhiệm về các nội dung, thông tin lưu trữ tại TTTHDL do cơ quan, đơn vị, địa phương cung cấp. Sao lưu dữ liệu thường xuyên của đơn vị theo sự hướng dẫn của đơn vị quản lý, 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 đơn vị quản lý, vận hành trong công tác bảo đảm an toàn, an ninh thông tin, duy trì hoạt động các hệ thống thông tin đặt tại TTTHDL;

c) Phối hợp với cơ quan quản lý và các đơn vị có liên quan trong công tác xây dựng, bảo trì, nâng cấp hệ thống bảo đảm an toàn, an ninh thông tin của đơn vị;

d) Hủy bỏ quyền truy cập vào HTTT, thu hồi lại các tài liệu, hồ sơ, thông tin liên quan tới tài khoản của CBCCVC chuyển công tác, nghỉ hưu hoặc chấm dứt hợp đồng;

đ) Thường xuyên tổ chức thực hiện tự kiểm tra, rà soát, phân tích, đánh giá, báo cáo rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với HTTT của cơ quan, đơn vị, địa phương;

e) Phối hợp với cơ quan quản lý và các đơn vị có liên quan trong công tác xây dựng, bảo trì, nâng cấp hệ thống bảo đảm an toàn, an ninh thông tin của đơn vị;

g) Xây dựng quy chế nội bộ về đảm bảo an toàn, an ninh thông tin phù hợp với Quy chế này và các quy định của pháp luật;

h) Phối hợp, cung cấp thông tin và tạo điều kiện cho các cơ quan có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng, hiệu quả;

i) Khi có sự cố hoặc nguy cơ mất ATTT phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị, địa phương và

thông báo bằng văn bản cho Sở Thông tin và Truyền thông, cơ quan cấp trên quản lý trực tiếp biết. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho Sở Thông tin và Truyền thông hoặc cơ quan quản lý cấp trên để phối hợp xử lý;

k) Phối hợp chặt chẽ với các cơ quan chức năng trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin;

l) Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông định kỳ hằng năm (trước ngày 20 tháng 12);

m) Hằng năm, xây dựng kinh phí đảm bảo duy trì, vận hành, nâng cấp trang thiết bị và cập nhật phần mềm đặt tại TTTHDL; tổng hợp chung trong dự toán chi nghiệp vụ chuyên môn của cơ quan, đơn vị, địa phương 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;

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 TTTHDL; không được cung cấp thông tin về tài khoản, mật khẩu người dùng cho người khác và các hành vi vi phạm Quy chế này.

Điều 29. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông: Là đơn vị chủ trì, chịu trách nhiệm trước UBND tỉnh, Chủ tịch UBND tỉnh về việc quản lý, khai thác và vận hành TTTHDL 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, hướng dẫn thực hiện Quy chế này; theo dõi, kiểm tra định kỳ báo cáo UBND tỉnh tình hình triển khai của các cơ quan, đơn vị, địa phương.

2. Sở Kế hoạch và Đầu tư: Phối hợp các cơ quan, đơn vị liên quan tham mưu UBND tỉnh cân đối kế hoạch nguồn vốn đầu tư theo quy định của Luật Đầu tư công trong khả năng cân đối của ngân sách tỉnh để đầu tư, nâng cấp, mở rộng TTTHDL đảm bảo việc quản lý, khai thác và vận hành, phục vụ hiệu quả cho việc triển khai Chính quyền số và đảm bảo an toàn, an ninh thông tin.

3. Sở Tài chính: Hàng năm, căn cứ khả năng cân đối và phân cấp ngân sách nhà nước, phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh bố trí kinh phí chi thường xuyên để đảm bảo thực hiện nhiệm vụ nâng cấp và duy trì hoạt động hiệu quả, đảm bảo an toàn an ninh thông tin TTTHDL theo quy định hiện hành.

4. Các cơ quan, đơn vị, địa phương, cá nhân sử dụng dịch vụ tại TTTHDL: Chủ động phối hợp với đơn vị quản lý, 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.

5. Những nội dung khác liên quan đến hoạt động quản lý, vận hành và khai thác TTTHDL không quy định tại Quy chế này được thực hiện theo quy định của pháp luật hiện hành.

Điều 30. Khen thưởng, xử lý vi phạm

1. Hằng năm, UBND tỉnh đánh giá việc quản lý, vận hành, sử dụng TTTHDL và có hình thức khen thưởng phù hợp đối với cơ quan, đơn vị, địa phương, cá nhân có liên quan.

2. Đối với các cơ quan, đơn vị, địa phương, 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 theo quy định của pháp luật.

Điều 31. Sửa đổi, bổ sung Quy chế

Trong quá trình triển khai thực hiện khi có thay đổi chính sách ATTT kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung hoặc có những vấn đề phát sinh cần điều chỉnh, bổ sung, các cơ quan, đơn vị, địa phương phản ánh kịp thời về Sở Thông tin và Truyền thông tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định sửa đổi, bổ sung Quy chế cho phù hợp./.

Chương V
DANH SÁCH BIỂU MẪU

STT	Mã số	Tên biểu mẫu
1.	TTDL_BM_01	Biên bản đưa thiết bị vào/ra TTTHDL
2.	TTDL_BM_02	Nhật ký quản lý, vận hành TTTHDL
3.	TTDL_BM_03	Biên bản đặt thiết bị tại TTTHDL
4.	TTDL_BM_04	Báo cáo tình hình hoạt động của TTTHDL
5.	TTDL_BM_05	Đăng ký sử dụng dịch vụ tại TTTHDL

Mẫu TTDL_BM_01

…….
…….

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

BIÊN BẢN ĐƯA THIẾT BỊ VÀO/RA TTTHDL

Hôm nay, vào lúc giờ phút, ngày tháng năm 20…..;
Tại Trung tâm tích hợp dữ liệu tỉnh Quảng Nam
Địa điểm:……..
……..
Chúng tôi gồm có:
I. Đại diện .....
1. Ông: ..... Chức vụ: .....
2. Ông: ..... Chức vụ: .....
II. Đại diện .....
1. Ông/bà: ..... Chức vụ: .....
2. Ông/bà: ..... Chức vụ: .....

Chúng tôi cùng ký vào biên bản xác nhận mang thiết bị vào/ra Trung tâm tích hợp dữ liệu tỉnh Quảng Nam như sau:

1. Thông số kỹ thuật:

STT	Tên thiết bị	ĐVT	Số lượng	Mã số	Ghi chú

2. Thông tin hạ tầng:

- Vị trí: .....

3. Thông tin khác: .....

Biên bản được lập thành 02 bản, mỗi bên giữ 01 bản có giá trị như nhau./.

Đại diện……..	**Đại diện……**
(Ký ghi rõ họ, tên)	*(Ký ghi rõ họ, tên)*

Mẫu TTDL_BM_02

NHẬT KÝ QUẢN LÝ, VẬN HÀNH TRUNG TÂM TÍCH HỢP DỮ LIỆU

I. Thông tin chung

- Tên trung tâm tích hợp dữ liệu: ……
- Ngày/Thời gian: ……
- Cán bộ quản lý, vận hành:
- 1.

……

- 2.

……

II. Tình trạng hệ thống trong ca trực

Hạng mục	Trạng thái	Ghi chú
Hệ thống máy chủ	☐ Bình thường ☐ Sự cố	
Hệ thống lưu trữ dữ liệu	☐ Bình thường ☐ Sự cố	
Hệ thống sao lưu, phục hồi dữ liệu	☐ Bình thường ☐ Sự cố	
Hệ thống mạng	☐ Bình thường ☐ Sự cố	
An toàn thông tin	☐ Bình thường ☐ Bất thường	
Phần mềm/Ứng dụng	☐ Bình thường ☐ Sự cố	
Hệ thống phụ trợ	☐ Bình thường ☐ Sự cố	
Hệ thống khác		

III. Thông tin chi tiết khác (nếu có): ……

.....
.....
.....
.....
.....
.....
.....
.....

IV. Xác nhận tình trạng hệ thống và bàn giao ca trực kế tiếp

- Thời gian kết thúc ca hiện tại .....
- Thời gian bàn giao ca trực kế tiếp .....
- Công việc cần tiếp tục xử lý (nếu có) .....

Xác nhận của cán bộ quản lý, vận hành ca trực hiện tại	Xác nhận của cán bộ quản lý, vận hành ca trực kế tiếp

Mẫu TTDL_BM_03

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

BIÊN BẢN ĐẶT THIẾT BỊ TẠI TRUNG TÂM TÍCH HỢP DỮ LIỆU (DC, DR) TỈNH QUẢNG NAM

Căn cứ.....

Hôm nay, ngày …. tháng …. năm……

Tại .....……., chúng tôi gồm:

BÊN GIAO (Bên A):.....

Địa chỉ:……

Điện thoại: ……

Đại diện:

Ông/Bà:…….. Chức vụ: ……

Ông/Bà:…… Chức vụ: …….

BÊN NHẬN (Bên B):……..

Địa chỉ:……

Điện thoại: ……

Đại diện:

Ông/Bà:…….. Chức vụ: ……

Ông/Bà:…… Chức vụ: …….

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

STT	Tên thiết bị	Mô tả thiết bị	Đơn vị	Số lượng	Serial Number/MAC /Service tag

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: ……

2. Thông tin khác

…….

II. Thông tin phối hợp của hai bên

1. Bên A

- Đầu mối điều hành: …… Số điện thoại:……

- Đầu mối về kỹ thuật: …… Số điện thoại:……

2. Bên B

- Đầu mối điều hành: …… Số điện thoại:……

- Đầu mối về kỹ thuật: …… Số điện thoại:……

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)*

Mẫu TTDL_BM_04

…….
…….

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

Số:…/...

Quảng Nam, ngày tháng năm 20…

BÁO CÁO
Tình hình hoạt động của Trung tâm tích hợp dữ liệu tỉnh Quảng Nam

……*(tên đơn vị báo cáo)* trân trọng báo cáo định kỳ tình hình hoạt động của Trung tâm tích hợp dữ liệu tỉnh Quảng Nam tháng …. năm …. như sau:

I. THÔNG TIN CHUNG

1. Kỳ báo cáo: Quý…../năm…..

2. Điện thoại…….. Email:……

3. Tổng băng thông Internet (trong nước/quốc tế):…..Mbps/…….Mbps

……...

4. Tỷ lệ khai thác hệ thống (%):

- Về đường truyền Internet:
- Về mạng TSLCD:
- Về cung cấp dịch vụ hạ tầng CNTT:
- ……..

5. Tình hình nhân sự:

- Số lượng nhân viên quản lý:
- Số lượng nhân viên kỹ thuật:

II. CÔNG TÁC ĐÃ TRIỂN KHAI

1. Duy trì vận hành các hệ thống, ứng dụng đã triển khai

(Xem chi tiết tại phụ lục kèm theo)

2. Tiếp nhận hệ thống ứng dụng, triển khai mới, bổ sung *(nếu có)*

3. Công tác phát hiện và khắc phục sự cố

a) Tổng số lần hệ thống bị sự cố:……..

b) Chi tiết công tác xử lý sự cố:

STT	Tên hệ thống bị sự cố	Thời điểm bị sự cố	Mô tả sự cố và nội dung khắc phục	Thời gian khắc phục (giờ)	Năng lực xử lý	
					Tự thực hiện	Nhờ chuyên gia ngoài

4. Công tác bảo đảm ATTT:……

5. Công tác khác:……

III. KẾ HOẠCH CÔNG TÁC TRIỂN KHAI

.....
.....
.....
.....

IV. KHÓ KHĂN, VƯỚNG MẮC ***(Nếu có)***

.....
.....
.....
.....

V. KIẾN NGHỊ, ĐỀ XUẤT

- Về tập huấn nghiệp vụ, đào tạo nâng cao trình độ chuyên môn:.....
- Về mua sắm trang thiết bị:.....
- Về các vấn đề khác: .....

.....
.....
.....
.....

…….*(tên đơn vị báo cáo)* trân trọng báo cáo./.

Nơi nhận:
- ……...;
- Lưu: VT,….

Thủ trưởng đơn vị
(Ký tên, đóng dấu)

Phụ lục: Thống kê các website/ứng dụng của cơ quan nhà nước lưu ký tại Trung tâm tích hợp dữ liệu tỉnh Quảng Nam

(Kèm theo Báo cáo số:……/…… ngày ...../...../20…
của ……)

STT	Đơn vị chủ quản	Tên website/ứng dụng	Ghi chú
I. Danh sách các website/ứng dụng cơ quan nhà nước (ứng dụng dùng chung)			
II. Danh sách các phần mềm, ứng dụng dịch vụ công (các cơ quan đơn vị trong tỉnh)			

Mẫu TTDL_BM_05

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

ĐĂNG KÝ SỬ DỤNG DỊCH VỤ CỦA TRUNG TÂM TÍCH HỢP DỮ LIỆU TỈNH QUẢNG NAM

I. THÔNG TIN ĐĂNG KÝ:

1. Thông tin đơn vị đăng ký: Địa chỉ: Người đại diện/chức vụ: Thông tin liên hệ:	…… …… …… ……
2. Hệ thống thông tin đăng ký:	……
3. Quản lý kỹ thuật dịch vụ: Họ tên/Chức vụ: Số điện thoại/Email: Phòng/Ban công tác:	…… …… …… ……
Dịch vụ 01: Tên dịch vụ: Mục đích sử dụng: Địa chỉ IP/Cấu hình: *(Thông tin đơn vị cung cấp dịch vụ)*	…… …… …… …… ……
Dịch vụ 02: Tên dịch vụ: Mục đích sử dụng: Địa chỉ IP/Cấu hình: *(Thông tin đơn vị cung cấp dịch vụ)*	…… …… …… …… ……

II. THÔNG TIN PHÊ DUYỆT:

1. Phê duyệt của Đơn vị quản lý, vận hành: ☐ Đồng ý ☐ Không đồng ý

2. Ý kiến khác (nếu có: ……

Các cơ quan, đơn vị, địa phương có nhu cầu đăng ký sử dụng dịch vụ cam kết tuân thủ mọi quy định, chính sách và hướng dẫn do Trung tâm tích hợp dữ liệu tỉnh Quảng Nam ban hành và theo quy định pháp luật hiện hành.

Bản đăng ký này được lập thành 02 (hai) bản, mỗi bên giữ 01 (một) bản có giá trị pháp lý như nhau.

Quảng Nam, ngày……tháng……năm 20…..

ĐẠI DIỆN ĐƠN VỊ VẬN HÀNH TTTHDL	**ĐẠI DIỆN ĐƠN VỊ ĐĂNG KÝ SỬ DỤNG DỊCH VỤ**
(Ký; đóng dấu; ghi rõ họ, tên)	*(Ký; đóng dấu; ghi rõ họ, tên)*