ỦY BAN NHÂN DÂN **TỈNH BẮC NINH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 59/2025/QĐ-UBND	*Bắc Ninh, ngày 03 tháng 11 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm Tích hợp dữ liệu tỉnh Bắc Ninh

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

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15; Luật Sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật số 87/2025/QH15;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

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

Căn cứ Nghị định số 142/2016/NĐ-CP của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT 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 39/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông Ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Căn cứ Thông tư số 19/2023/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Quyết định số 8/2023/QĐ-TTg;

Căn cứ Thông tư số 12/2022/TT-BTTTT 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;

Căn cứ Thông tư số 03/2013/TT-BTTTT 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;

Căn cứ Thông tư số 23/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông Sửa đổi, bổ sung một số điều của Thông tư số 03/2013/TT-BTTTT;

Căn cứ Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Theo đề nghị của Giám đốc Sở Khoa học và Công nghệ tại Tờ trình số 66/TTr-SKHCN ngày 19 tháng 9 năm 2025.

Ủy ban nhân dân tỉnh ban hành Quyết định ban hành Quy chế quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm Tích hợp dữ liệu tỉnh Bắc Ninh.

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm Tích hợp dữ liệu tỉnh Bắc Ninh.

Điều 2. Quyết định này có hiệu lực kể từ ngày 15 tháng 11 năm 2025 và thay thế Quyết định số 03/2025/QĐ-UBND ngày 09/01/2025 của Ủy ban nhân dân tỉnh Bắc Giang ban hành Quy chế quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm Tích hợp dữ liệu tỉnh Bắc Giang và Quyết định số 15/2023/QĐ-UBND ngày 18/8/2023 của Ủy ban nhân dân tỉnh Bắc Ninh ban hành Quy chế quản lý, vận hành và sử dụng Trung tâm dữ liệu tỉnh Bắc Ninh.

Điều 3. Thủ trưởng các cơ quan, đơn vị thuộc Ủy ban nhân dân tỉnh; Chủ tịch UBND các xã, phường và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

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

Đã ký
Mai Sơn

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

QUY CHẾ

Quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm Tích hợp dữ liệu tỉnh Bắc Ninh

(Ban hành kèm theo Quyết định số 59/2025/QĐ-UBND ngày 03 tháng 11 năm 2025 của Ủy ban nhân dân tỉnh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định việc quản lý, vận hành, khai thác và bảo đảm an toàn thông tin đối với Trung tâm Tích hợp dữ liệu tỉnh Bắc Ninh (sau đây viết tắt là Trung tâm THDL).

2. Đối tượng áp dụng

a) Các cơ quan, đơn vị trên địa bàn tỉnh có hệ thống thông tin đặt tại Trung tâm THDL;

b) Cơ quan, tổ chức, cá nhân có kết nối, khai thác, sử dụng hệ thống thông tin tại Trung tâm THDL;

c) Các tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành và đảm bảo an toàn thông tin đối với Trung tâm THDL.

Điều 2. Giải thích từ ngữ

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

1. Mạng diện rộng cơ quan nhà nước tỉnh Bắc Ninh (sau đây viết tắt là mạng WAN) là mạng tin học được thiết lập bằng cách kết nối giữa Trung tâm THDL với mạng nội bộ của các cơ quan, đơn vị trên địa bàn tỉnh.

2. Mạng truyền số liệu chuyên dùng (sau đây viết tắt là mạng TSLCD) của các cơ quan Đảng, Nhà nước là hệ thống thông tin quan trọng quốc gia, được sử dụng

riêng trong hoạt động truyền số liệu và ứng dụng công nghệ thông tin của các cơ quan Đảng, Nhà nước trên toàn tỉnh.

3. Cơ sở dữ liệu (sau đây viết tắt là CSDL) là dữ liệu của các hệ thống phần mềm dùng chung, phần mềm chuyên ngành của các đơn vị được lưu trữ trên hệ thống lưu trữ đặt tại Trung tâm THDL.

4. Hạ tầng kỹ thuật là tập hợp thiết bị công nghệ thông tin, thiết bị điện, nhà trạm, hệ thống cáp, thiết bị phòng cháy, chữa cháy, thiết bị viễn thông, thiết bị ngoại vi, mạng diện rộng, mạng nội bộ, mạng truyền số liệu chuyên dùng và các thiết bị kỹ thuật chuyên dùng khác.

5. VLAN (Virtual Local Area Network) là một kỹ thuật ảo hóa mạng, cho phép phân chia một mạng vật lý lớn thành nhiều mạng logic nhỏ, độc lập với nhau.

6. Điểm yếu an toàn thông tin là các lỗi tồn tại trên sản phẩm phần cứng, phần mềm, dịch vụ hoặc hệ thống trong quá trình phát triển, cài đặt và thiết lập, có thể gây ra nguy cơ mất an toàn cho hệ thống thông tin khi bị tin tặc khai thác.

7. Chủ quản của hệ thống Trung tâm THDL: Ủy ban nhân dân (sau đây viết tắt là UBND) tỉnh Bắc Ninh.

8. Cơ quan chịu trách nhiệm quản lý Trung tâm THDL (viết tắt là Cơ quan quản lý): Sở Khoa học và Công nghệ tỉnh Bắc Ninh.

9. Đơn vị trực tiếp quản trị, vận hành Trung tâm THDL (viết tắt là Đơn vị quản trị, vận hành): Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Khoa học và Công nghệ.

Điều 3. Chức năng, kiến trúc và dịch vụ Trung tâm THDL

1. Trung tâm THDL có chức năng lưu trữ, xử lý, tích hợp, phân tích, quản lý và chia sẻ cơ sở dữ liệu; vận hành các hệ thống bảo mật, an toàn dữ liệu và các hệ thống phụ trợ; quản lý mạng WAN, mạng TSLCD, các hệ thống thông tin dùng chung và hệ thống thông tin chuyên ngành của các cơ quan, đơn vị.

2. Kiến trúc của Trung tâm THDL được chia làm các phân hệ sau đây:

a) Hệ thống máy chủ: Bao gồm các máy chủ được đầu tư phục vụ triển khai các ứng dụng công nghệ thông tin (sau đây viết tắt là CNTT) với khả năng sẵn sàng

nâng cấp, mở rộng số lượng máy chủ trong tương lai; đảm bảo năng lực cung cấp các dịch vụ ứng dụng 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;

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 Trung tâm THDL; phục vụ công tác chỉ đạo, điều hành, tác nghiệp của các cơ quan, địa phương và người dân, doanh nghiệp trên toàn tỉnh;

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 đảm bảo khả năng mở rộng dung lượng lưu trữ dữ liệu trong tương lai;

d) Hệ thống đảm bảo an toàn thông tin: 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, hệ thống kiểm soát ra, vào, camera giám sát và các ứng dụng an ninh hệ thống thông tin. Mỗi thành phần trong hệ thống an toàn thông tin đều được thiết kế bảo đảm tính dự phòng và bổ sung hỗ trợ lẫn nhau trong toàn hệ thống CNTT;

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 để phục vụ ứng dụng CNTT trong các cơ quan, địa phương và phục vụ người dân, doanh nghiệp;

e) Hệ thống mạng: Bao gồm nhiều vùng mạng khác nhau để kết nối với hệ thống mạng TSLCD hay mở kết nối ra Internet, vùng mạng riêng (DMZ), vùng mạng quản trị nội bộ (LAN), phân vùng mạng dùng riêng cho các cơ quan, đơn vị; mỗi vùng mạng được thiết lập các chính sách an ninh và truy cập riêng cho một hoặc nhiều mục đích sử dụng khác nhau. Hệ thống mạng sử dụng đường truyền băng thông rộng và đường truyền số liệu chuyên dùng để phục vụ kết nối mạng WAN của tỉnh, kết nối các ứng dụng dùng chung, ứng dụng chuyên ngành, cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành phục vụ các cơ quan, địa phương khai

thác, sử dụng và giao dịch hành chính trên môi trường mạng;

g) Các hệ thống phụ trợ: Bao gồm các hệ thống nguồn điện, hệ thống điều hòa, thiết bị lưu điện, giám sát môi trường, máy phát điện, sàn nâng, hệ thống phòng cháy và chữa cháy, camera an ninh và các hệ thống phụ trợ có liên quan khác.

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

a) Dịch vụ đặt máy chủ;

b) Dịch vụ cung cấp máy chủ ảo, tài nguyên lưu trữ trực tuyến (hosting);

c) Dịch vụ cài đặt ứng dụng, CSDL;

d) Dịch vụ quản trị, vận hành, bảo trì, bảo hành phần mềm và CSDL;

đ) Dịch vụ lưu trữ;

e) Dịch vụ quản trị hạ tầng, vận hành ứng dụng đặt tại Trung tâm THDL;

g) Các dịch vụ CNTT khác.

Điều 4. Đầu mối tiếp nhận, phối hợp với các cơ quan, tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền trong việc quản lý, vận hành, khai thác và đảm bảo an toàn thông tin cho Trung tâm THDL tỉnh Bắc Ninh.

Sở Khoa học và Công nghệ là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền trong việc quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm THDL.

Trung tâm Công nghệ thông tin và Truyền thông là đầu mối phối hợp với các cơ quan đơn vị trong việc quản trị, vận hành hạ tầng tại trung tâm THDL.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin tại Trung tâm THDL.

Công an tỉnh là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối, xử lý sự cố về an toàn thông tin tại Trung tâm THDL.

3. Các cơ quan, đơn vị; UBND các xã, phường tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, có thẩm quyền.

Điều 5. Nguyên tắc về quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm THDL tỉnh

1. Tuân thủ các nguyên tắc, biện pháp bảo đảm cơ sở hạ tầng thông tin phục vụ ứng dụng và phát triển công nghệ thông tin theo Luật Công nghệ thông tin số 67/2006/QH11;

2. Tuân thủ nguyên tắc xây dựng, quản lý, khai thác, bảo vệ và duy trì cơ sở dữ liệu được quy định tại Điều 13 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;

3. Tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật quy định áp dụng đối với Trung tâm THDL theo quy định tại Thông tư số 23/2022/TT-BTTTT ngày 30 tháng 11 năm 2022 của Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 03/2013/TT-BTTTT ngày 22 tháng 01 năm 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. Đồng thời, tuân thủ theo các quy định hiện hành về bảo đảm an toàn, an ninh thông tin;

4. Đảm bảo các yêu cầu về an toàn, an ninh thông tin theo quy định của Luật an toàn thông tin mạng, 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;

5. Việc quản lý, kết nối và chia sẻ dữ liệu của Trung tâm THDL phải tuân thủ theo Nghị định số 47/2020/NĐ-CP ngày 09 tháng 4 năm 2020 của Chính phủ về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;

6. Việc tạo lập, lưu trữ, chia sẻ dữ liệu số chứa thông tin thuộc phạm vi bí mật Nhà nước được thực hiện theo Luật Bảo vệ bí mật Nhà nước số 29/2018/QH14 và các văn bản pháp lý hiện hành;

Chương II

QUY ĐỊNH CỤ THỂ

Mục 1

QUẢN LÝ, VẬN HÀNH, KHAI THÁC TRUNG TÂM THDL

Điều 6. Quy định về chế độ làm việc tại Trung tâm THDL

1. Quy định đối với đơn vị quản trị, vận hành Trung tâm THDL

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 THDL được hoạt động ổn định, thông suốt liên tục 24 giờ/ngày, 7 ngày/tuần;

b) Duy trì chế độ trực vận hành và giám sát an toàn thông tin, đảm bảo từ 01 - 02 viên chức, nhân viên quản trị, vận hành trực tại Trung tâm THDL ngoài giờ hành chính, ngày nghỉ trong tuần, lễ, tết.

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

a) Trong quá trình làm việc tại Trung tâm THDL phải tuân thủ nghiêm ngặt theo các quy trình, quy định, nội quy lao động đã được phê duyệt và phải chịu trách nhiệm nếu sự cố xảy ra nghiêm trọng;

b) Không tự ý can thiệp vào các phần mềm, ứng dụng, dữ liệu của các cơ quan, đơn vị khác đang được cài đặt và triển khai tại Trung tâm THDL. Việc khai thác thông tin, dữ liệu phải bảo đảm nguyên tắc bảo mật, an toàn thông tin, không được tự ý cung cấp thông tin, dữ liệu ra bên ngoài.

c) Khi thực hiện các nghiệp vụ chuyên môn có sự tác động đến các thiết bị, hệ thống của Trung tâm THDL phải được ghi chép cụ thể vào sổ Nhật ký hệ thống.

d) Khi chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, 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 (nếu có) thuộc sở hữu của cơ quan, đơn vị; thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống; lập bản cam kết giữ bí mật thông tin liên quan đến cơ quan, tổ chức.

3. Quy định đối với các tổ chức, cá nhân đến làm việc, tham quan tại Trung tâm THDL:

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

b) Không được mang, sử dụng các thiết bị điện thoại, máy tính xách tay, máy tính bảng hoặc các thiết bị điện tử cá nhân khác khi vào bên trong Trung tâm THDL, trừ trường hợp có sự đồng ý của lãnh đạo cơ quan quản lý hoặc lãnh đạo

đơn vị trực tiếp quản trị, vận hành Trung tâm THDL;

c) Các tổ chức, cá nhân đến đăng ký làm việc tại Trung tâm THDL phải cung cấp giấy giới thiệu của cơ quan, đơn vị hoặc văn bản đề nghị làm việc tại Trung tâm THDL; các thiết bị đưa vào, ra Trung tâm THDL phải đăng ký và lập biên bản đưa thiết bị vào, ra Trung tâm THDL;

d) Các tổ chức, cá nhân đến đăng ký tham quan tại Trung tâm THDL cần phải cung cấp giấy giới thiệu của cơ quan, đơn vị hoặc văn bản đề nghị tham quan Trung tâm THDL (theo Mẫu số 01 tại phụ lục ban hành kèm theo Quy chế này); danh sách những người tham quan (có thông tin về CCCD hoặc Hộ chiếu kèm theo) và phải được sự đồng ý của lãnh đạo cơ quan quản lý Trung tâm THDL (Sở Khoa học và Công nghệ tổng hợp, báo cáo của UBND tỉnh).

Điều 7. Đảm bảo an toàn hoạt động

1. Trung tâm THDL chỉ được đặt các thiết bị đang hoạt động, thiết bị chuyên dụng phục vụ vận hành hệ thống; không được phép đặt tại Trung tâm THDL các thiết bị không đúng mục đích.

2. Trung tâm THDL phải đảm bảo vệ sinh, môi trường khô ráo, sạch sẽ. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị CNTT.

3. Hệ thống phòng cháy, chữa cháy, chống sét phải đáp ứng theo tiêu chuẩn quy định, được cấp giấy phép của cơ quan có thẩm quyền và phải được kiểm tra thường xuyên nhằm đảm bảo an toàn tuyệt đối cho toàn hệ thống thiết bị và đảm bảo an toàn cho viên chức, nhân viên quản trị, vận hành các hệ thống tại Trung tâm THDL.

4. Hệ thống điện cấp cho Trung tâm THDL phải có ít nhất 2 nguồn ổn định, liên tục được trang bị hệ thống lưu điện (UPS) và máy phát điện dự phòng để đảm bảo cho hệ thống vẫn hoạt động trong thời gian nguồn điện lưới gặp sự cố.

5. Hệ thống camera thực hiện giám sát toàn bộ Trung tâm THDL liên tục 24 giờ/ngày, 7 ngày/tuần; dữ liệu hình ảnh phải được lưu trữ ít nhất trong thời gian là 30 ngày.

6. Hệ thống quản lý vào ra (Access Control) phải hoạt động 24 giờ/ngày, 7 ngày/tuần và ghi đầy đủ nhật ký nhằm đảm bảo an ninh, chính xác và linh hoạt cho

Trung tâm THDL.

Điều 8. Xử lý sự cố

1. Khi phát hiện có sự cố, người sử dụng hoặc viên chức, nhân viên quản trị, vận hành hệ thống có trách nhiệm báo cáo kịp thời cho lãnh đạo đơn vị quản trị, vận hành và lãnh đạo cơ quan quản lý để có biện pháp cô lập, thực hiện xử lý, xác định nguyên nhân xảy ra sự cố theo nguyên tắc hạn chế tối đa ảnh hưởng tới hoạt động của hệ thống;

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

a) Đối với các sự cố thông thường (không gây ảnh hưởng đến hoạt động của Trung tâm THDL): Đơn vị quản trị, vận hành nhanh chóng xử lý sự cố. Trường hợp không xử lý được, thông báo cơ quan quản lý để phối hợp giải quyết;

b) Đối với các sự cố nghiêm trọng (các 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 mát dữ liệu, gây ảnh hưởng trực tiếp đến hoạt động của Trung tâm THDL): Ngay sau khi phát hiện sự cố, đơn vị quản trị, vận hành cần đánh giá ảnh hưởng của sự cố và thực hiện báo cáo về cơ quan quản lý để có chỉ đạo xử lý và báo cáo UBND tỉnh;

c) Đối với các sự cố đặc biệt nghiêm trọng (gây ngưng trệ đến toàn bộ hoạt động của Trung tâm THDL): Đơn vị quản trị, vận hành và cơ quan quản lý phải có đánh giá ảnh hưởng của sự cố, phối hợp với các cơ quan bộ, ngành liên quan đồng thời thực hiện báo cáo kịp thời UBND tỉnh để xin ý kiến 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 quan trọng phải được sao lưu trước khi xử lý sự cố;

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

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

e) Lập báo cáo sự cố gửi cơ quan quản lý đối với các sự cố nghiêm trọng và đặc

biệt nghiêm trọng trong vòng 24 giờ kể từ khi phát hiện sự cố;

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

Điều 9. Kiểm soát truy cập và xác thực

1. Việc cấp phát quyền truy cập từ xa hoặc kết nối trực tiếp để sử dụng và khai thác ứng dụng, tài nguyên thuộc Trung tâm THDL phải đảm bảo chặt chẽ, đúng mục đích sử dụng. Mỗi người dùng sẽ chỉ được cấp một tài khoản, được phân quyền đủ để thực hiện nhiệm vụ được phân công.

2. Hệ thống thực hiện khóa tạm thời tài khoản, khi thực hiện xác thực sai liên tiếp 05 lần trong vòng 30 phút. Tài khoản chỉ được mở khóa khi có đề nghị của chủ thể sở hữu tài khoản.

3. Tạm dừng quyền sử dụng đối với tài khoản đã hết hạn thời gian đăng ký trên hệ thống và những tài khoản không làm việc trong hệ thống từ 30 ngày trở lên.

Điều 10. Quản trị các hệ thống 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 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 Trung tâm THDL phải có bản quyền và sử dụng theo đúng quy định của pháp luật.

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

a) Tất cả máy chủ, máy trạm tại Trung tâm THDL phải được trang bị hệ điều hành và phần mềm diệt virus có bản quyền và đã được cơ quan chức năng khuyến cáo sử dụng. Phần mềm diệt virus phải được thiết lập chế độ tự động cập nhật và chế độ tự động quét phần mềm độc hại khi sao chép, mở các tệp tin và phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp tin trên các thiết bị lưu trữ thiết bị ngoại vi kết nối hệ thống.

b) Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

c) Máy tính xách tay, thiết bị di động (máy tính bảng, điện thoại thông minh, thiết bị có phần mềm hệ điều hành) trước khi kết nối vào mạng nội bộ (LAN) của Trung tâm THDL phải được bộ phận kỹ thuật chuyên trách kiểm duyệt, đảm bảo an toàn, bảo mật thông tin.

d) Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và không phục vụ công việc.

đ) Tất cả các tệp tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng, truyền đưa, trao đổi.

5. Không phát tán, chia sẻ các hệ thống phần mềm tại Trung tâm THDL dưới bất kỳ hình thức nào khi chưa được sự đồng ý của cơ quan chủ quản.

Điều 11. Chính sách thiết lập và quản lý mật khẩu

Mật khẩu phải bảo đảm độ phức tạp về độ dài, nội dung và thời gian sử dụng, cụ thể:

1. Độ dài của mật khẩu:

a) Đối với mật khẩu của cán bộ, công chức, viên chức và người sử dụng *(*dùng để đăng nhập các hệ thống thông tin dùng chung, ứng dụng nghiệp vụ chuyên ngành khác): Tối thiểu là 08 ký tự;

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

2. Nội dung mật khẩu:

a) Không bao gồm các từ dễ nhớ như tên, ngày sinh, số điện thoại;

b) Không được đặt theo ký tự chữ cái, ký tự chữ số tuần tự hoặc một dãy các ký tự giống nhau;

c) Mật khẩu được đặt phải kết hợp các loại ký tự sau: Chữ cái in thường, chữ cái in hoa, ký tự số và các ký tự đặc biệt.

3. Thời gian sử dụng mật khẩu:

a) Mật khẩu phải được thay đổi ít nhất 03 tháng 01 lần;

b) Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn thông tin thì lãnh đạo đơn vị quản trị, vận hành Trung tâm THDL quyết định việc thay đổi toàn bộ mật khẩu quản trị của Trung tâm THDL.

4. Quy định sử dụng và lưu trữ mật khẩu:

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

b) Không được chia sẻ mật khẩu cho người khác;

c) Phải tiến hành thay đổi mật khẩu ngay khi nghi ngờ bị lộ lọt thông tin mật khẩu; mật khẩu mới thay đổi phải đảm bảo không trùng với những mật khẩu đã từng sử dụng trước đó;

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

Điều 12. Sao lưu, phục hồi dữ liệu

1. Thực hiện lưu trữ đầy đủ các dữ liệu của người dùng, các ứng dụng và hệ thống. Tùy theo từng loại dữ liệu, thực hiện lưu trữ đúng và đủ thời hạn, đảm bảo phục hồi nguyên trạng khi có sự cố xảy ra.

2. Đơn vị quản trị, vận hành có trách nhiệm xây dựng và triển khai thực hiện Quy trình sao lưu, phục hồi dữ liệu dự phòng cho Trung tâm THDL.

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. Đối với các dữ liệu quan trọng phải được lưu trữ tối thiểu tại hai thiết bị hoặc hai địa điểm cách biệt nhau.

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

Điều 13. Quản lý thiết bị

1. Thiết bị CNTT cài đặt tại Trung tâm THDL phải đặt tên và dán nhãn theo đúng quy định.

2. Đơn vị quản trị, vận hành phải thực hiện tổng hợp tình hình quản lý, sử dụng thiết bị tại Trung tâm THDL định kỳ hàng quý, hàng năm hoặc khi có thay đổi. Thực hiện báo cáo cơ quan quản lý theo đúng quy định.

3. Đơn vị quản trị, vận hành đề xuất mua thêm thiết bị CNTT và các thiết bị phụ trợ khác trong trường hợp thiết bị hết bảo hành hoặc bị hỏng. Thiết bị được trang bị phải tuân theo các tiêu chuẩn về thiết bị cho Trung tâm THDL.

4. Đối với thiết bị hỏng còn bảo hành, đơn vị quản trị, vận hành yêu cầu đơn vị cung cấp sửa chữa. Thiết bị hỏng đã hết bảo hành, đơn vị quản trị, vận hành báo cáo cơ quan quản lý về phương án sửa chữa.

5. Trường hợp thiết bị hỏng là thiết bị quan trọng (máy chủ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị tường lửa), đơn vị quản trị, vận hành phải báo cáo ngay về cơ quan quản lý để có biện pháp khắc phục nhanh chóng, kịp thời.

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

Điều 14. Hệ thống mạng và truyền dẫn

1. Hệ thống mạng và truyền dẫn phải đảm bảo hiệu năng cho các ứng dụng, khả năng sẵn sàng và có các giải pháp để đảm bảo an toàn hệ thống.

2. Hệ thống mạng và truyền dẫn phải bảo đảm:

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

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

c) Tuân thủ theo các tiêu chuẩn của Trung tâm THDL về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức đi dây, đấu nối, phân bổ nút mạng;

d) Tuân thủ quy định về các phân vùng chức năng đã được quy hoạch. Mỗi phân vùng trong Trung tâm THDL ứng với dải địa chỉ IP cấp phát riêng và VLAN tương ứng, đồng thời được thiết lập các chính sách an ninh và truy cập khác nhau.

3. Hạ tầng 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 vị khác.

4. Đơn vị quản trị, vận hành chịu trách nhiệm giám sát, kiểm tra nội dung và băng

thông truy cập, ngăn chặn, đề xuất các biện pháp xử lý các hành vi vi phạm.

Điều 15. Bảo trì, bảo dưỡng

1. Đơn vị quản trị, vận hành Trung tâm THDL có trách nhiệm xây dựng, tham mưu cơ quan quản lý ban hành quy trình bảo trì, bảo dưỡng toàn bộ hệ thống.

2. Cơ quan quản lý quyết định lựa chọn hình thức duy trì, bảo trì, bảo dưỡng các hệ thống thuộc Trung tâm THDL bằng hình thức tự thực hiện hoặc thuê dịch vụ đảm bảo tiết kiệm, hiệu quả, theo đúng quy định.

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 hệ thống ít nhất 01 lần/năm.

4. Việc thực hiện duy trì, bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến tình hình hoạt động của Trung tâm THDL; quá trình duy trì, bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, quy trình và ghi nhật ký về tình trạng hoạt động trước và sau khi thực hiện.

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

1. Hằng tháng, đơn vị quản trị, vận hành Trung tâm THDL thực hiện báo cáo về việc quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm THDL (theo mẫu số 02 tại phụ lục ban hành kèm theo Quy chế này) gửi về cơ quan quản lý. Trong trường hợp phát hiện các bất cập, lỗi liên quan đến các hệ thống, cần thực hiện báo cáo nhanh và xây dựng kế hoạch khắc phục.

2. Cơ quan quản lý tổ chức kiểm tra việc tuân thủ các quy định về quản lý, triển khai, vận hành và khai thác sử dụng Trung tâm THDL theo các quy định tại Quy chế này định kỳ theo quý hoặc kiểm tra đột xuất khi có các vấn đề phát sinh cần làm rõ.

3. Các nội dung kiểm tra:

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

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

c) Hoạt động của hệ thống máy chủ, máy trạm, các dịch vụ (cập nhật các bản vá,

bản sửa lỗi, dung lượng ổ cứng, hiệu năng sử dụng);

d) Tình hình an ninh bảo mật hệ thống, đánh giá hiệu quả (khả năng phát hiện và ngăn chặn) của hệ thống bảo mật;

đ) Công tác sao lưu, lưu trữ, phục hồi dữ liệu;

e) Quản lý hồ sơ: ghi nhật ký, cập nhật, tổng hợp thiết bị, báo cáo;

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

Điều 17. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thiết bị CNTT có chứa dữ liệu khi bị hỏng phải được viên chức, nhân viên quản trị, 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.

2. Trước khi tiến hành thanh lý, hủy bỏ thiết bị CNTT cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người sử dụng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: 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.

Mục 2
BẢO ĐẢM AN TOÀN THÔNG TIN ĐỐI VỚI TRUNG TÂM TÍCH HỢP DỮ LIỆU

Điều 18. Quản lý thiết kế, xây dựng hệ thống

Các cơ quan, đơn vị có hệ thống thông tin đặt tại Trung tâm THDL phải đáp ứng các yêu cầu về quản lý thiết kế, xây dựng hệ thống, cụ thể như sau:

1. Thiết kế an toàn hệ thống thông tin:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

b) Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin;

c) Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ;

d) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn

thông tin;

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.

2. Phát triển phần mềm thuê khoán:

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê dịch vụ các nội dung liên quan đến việc phát triển phần mềm thực hiện theo hình thức thuê dịch vụ.

b) Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

c) Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

d) Kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.

3. Vận hành thử, kiểm thử và nghiệm thu hệ thống:

a) Thực hiện vận hành thử, kiểm thử và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

b) Có nội dung, kế hoạch, quy trình thực hiện vận hành thử, kiểm thử và nghiệm thu hệ thống.

c) Có bộ phận có trách nhiệm thực hiện tham gia vận hành thử/kiểm thử và nghiệm thu hệ thống.

d) 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 vận hành thử/kiểm thử và nghiệm thu hệ thống.

đ) Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Điều 19. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ theo khoản 1 Điều 20 Quy chế này.

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

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ;

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống;

c) Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

d) Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

3. Truy cập và quản lý cấu hình hệ thống:

a) Viên chức, nhân viên quản trị, 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 công chức, viên chức quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm;

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

c) Quy trình kết nối thiết bị đầu cuối 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 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 file 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) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ

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 hết hạn phục

vụ cho việc gia hạn.

2. Bảo đảm các kết nối, truy cập 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) Cấp quyền quản lý truy cập trên máy chủ cài đặt hệ điều hành;

c) 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; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet;

d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu thay đổi thông tin xác thực định kỳ;

đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống;

e) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

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

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

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

Điều 21. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa:

a) Phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích

hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin;

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

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

3. Có cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

5. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

7. Định kỳ 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).

Điều 22. Quản lý an toàn thiết bị đầu cuối

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

3. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 23. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

3. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; 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.

Điều 24. Quản lý giám sát an toàn hệ thống thông tin

1. Các hệ thống thông tin đặt tại Trung tâm THDL bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và việc khai thác, sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

2. Đối tượng giám sát về cơ bản bao gồm máy chủ, thiết bị mạng, thiết bị bảo mật, máy chủ, dịch vụ, ứng dụng, các thiết bị đầu cuối và điểm giám sát đường truyền, cụ thể: giám sát lớp mạng, giám sát lớp máy chủ, giám sát lớp ứng dụng và giám sát lớp đầu cuối.

3. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo đúng quy định tại Thông tư số 31/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông Quy định hoạt động giám sát an toàn hệ thống thông tin.

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

5. Phải đảm bảo được thực hiện thường xuyên, liên tục. Chủ động theo dõi, phân tích, phòng ngừa nhằm kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

6. Đảm bảo ổn định, bí mật cho thông tin cung cấp, trao đổi trong quá trình giám sát.

Điều 25. Quản lý điểm yếu an toàn thông tin

1. Quản lý điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống, phân loại mức độ nguy hiểm của điểm yếu. Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Báo cáo lãnh đạo, viên chức quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin 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 an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

4. Đơn vị quản trị, vận hành và chủ quản hệ thống thông tin 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 an toàn thông tin đối với các điểm yếu khi cần thiết.

5. 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.

6. 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.

Điều 26. Quản lý sự cố an toàn thông tin

Đơn vị quản trị, vận hành và các cơ quan, đơn vị có hệ thống thông tin đặt tại Trung tâm THDL thực hiện quản lý sự cố an toàn thông tin như sau:

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an 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.

2. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng.

3. Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

5. Đơn vị quản trị, vận hành Trung tâm THDL quyết định toàn diện về mặt kỹ thuật đối với các cơ quan, đơn vị trong quá trình khắc phục sự cố về an toàn thông tin; hỗ trợ, phối hợp và hướng dẫn các cơ quan, đơn vị khắc phục sự cố mất an toàn thông tin; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông

tin của các cơ quan, đơn vị nhằm phục vụ công tác khắc phục sự cố về an toàn thông tin; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo của cơ quan quản lý.

6. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

7. Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin tối thiểu 01 lần/năm.

Điều 27. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính, thiết bị đầu cuối vào hệ thống:

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, đơn vị;

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, phụ trách về an toàn thông tin;

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

2. Cài đặt và sử dụng máy tính an toàn:

a) Chỉ cài đặt phần mềm hợp lệ, thuộc danh mục phần mềm được phép sử dụng do cơ quan, đơn vị có thẩm quyền ban hành (nếu có) trên máy tính được cơ quan, đơn vị cấp;

b) Cài đặt phần mềm phòng, chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét mã độc sau khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải tắt máy tính, báo cáo ngay với cấp trên và bộ phận chuyên trách/phụ trách về an toàn thông

tin để kịp thời ngăn chặn, xử lý;

d) Chỉ truy nhập vào các cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động;

đ) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà được giao sử dụng; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, bộ nhớ đệm và tệp dữ liệu trong trình duyệt trên máy tính;

e) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan, đơn vị.

3. Trong quá trình sử dụng:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin 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 an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách CNTT của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do tỉnh hoặc đơn vị chuyên môn tổ chức.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 28. Trách nhiệm của Sở Khoa học và Công nghệ

1. Chủ trì, hướng dẫn các cơ quan, đơn vị, tổ chức, cá nhân có liên quan thực hiện Quy chế này và các quy định khác về công tác quản lý, vận hành, khai thác và đảm bảo an toàn thông tin đối với Trung tâm THDL.

2. Tham mưu UBND tỉnh về công tác quản lý, vận hành, nâng cấp mở rộng và

đảm bảo an toàn thông tin đối với Trung tâm THDL.

3. Ban hành các văn bản hướng dẫn chuyển giao máy móc, thiết bị, cài đặt phần mềm, quản lý tài sản tại Trung tâm THDL; phê duyệt quy trình vận hành, bảo trì, bảo dưỡng và khắc phục sự cố Trung tâm THDL.

4. Thực hiện kiểm tra, giám sát việc vận hành, khai thác dịch vụ và đảm bảo an toàn thông tin đối với đơn vị quản trị, vận hành Trung tâm THDL. Tiếp nhận và tổng hợp ý kiến phản ánh của các cơ quan, đơn vị để chỉ đạo Trung tâm Công nghệ thông tin và Truyền thông báo cáo, đề xuất giải pháp nâng cao chất lượng và mở rộng tài nguyên của Trung tâm THDL.

5. Xây dựng kế hoạch đào tạo, bồi dưỡng, đảm bảo nguồn nhân lực quản lý, quản trị, vận hành có chuyên môn đáp ứng yêu cầu, được trang bị kiến thức liên quan tới hoạt động của Trung tâm THDL. Đảm bảo các vị trí được tuyển dụng làm việc tại Trung tâm THDL phải có trình độ, chuyên môn đáp ứng với yêu cầu vị trí việc làm.

6. Định kỳ hằng năm hoặc đột xuất, thực hiện báo cáo UBND tỉnh về tình hình hoạt động của Trung tâm THDL.

Điều 29. Trách nhiệm của Công an tỉnh

Phối hợp với Sở Khoa học và Công nghệ bảo đảm an toàn thông tin cho Trung tâm THDL; kiểm tra an toàn thông tin đối với các máy chủ, thiết bị và ứng dụng CNTT của các cơ quan Nhà nước trước khi cài đặt vận hành tại Trung tâm THDL.

Điều 30. Trách nhiệm của Sở Tài chính

Chủ trì thẩm định, tham mưu và bố trí kinh phí để duy trì hoạt động của Trung tâm THDL theo đề xuất của Sở Khoa học và Công nghệ để trình UBND tỉnh phê duyệt kinh phí hằng năm đối với công tác quản lý, vận hành, bảo trì, bảo dưỡng Trung tâm THDL.

Điều 31. Trách nhiệm của cơ quan, đơn vị có hệ thống thông tin đặt tại Trung tâm THDL

1. Cơ quan, đơn vị sử dụng, khai thác dịch vụ của Trung tâm THDL, trong phạm vi chức năng, nhiệm vụ của mình có trách nhiệm tổ chức thực hiện các quy định tại

Quy chế này và các hướng dẫn khác của cơ quan quản lý, đơn vị quản trị, vận hành Trung tâm THDL.

2. Phân công ít nhất 01 công chức, viên chức có trình độ về liên quan về CNTT làm công tác quản trị các hệ thống thông tin liên quan đến cơ quan, đơn vị sử dụng; là đầu mối liên hệ, phối hợp xử lý các sự cố mất an toàn thông tin xảy ra tại cơ quan, đơn vị mình.

3. Chịu trách nhiệm về nội dung, thông tin lưu trữ tại Trung tâm THDL do cơ quan, đơn vị cung cấp, cập nhật đúng quy định pháp luật. Phối hợp với các đơn vị liên quan trong công tác bảo đảm an toàn, an ninh thông tin; duy trì hoạt động các hệ thống thông tin của cơ quan mình đặt tại Trung tâm THDL.

4. Khi có nhu cầu sử dụng các dịch vụ của Trung tâm THDL, đăng ký sử dụng các dịch vụ của Trung tâm THDL (theo Mẫu số 03 tại phụ lục ban hành kèm theo Quyết định này).

5. Kịp thời báo cáo sự cố mất an toàn thông tin về Công an tỉnh, Sở Khoa học và Công nghệ, đơn vị quản trị, vận hành Trung tâm THDL (theo Mẫu số 04 tại phụ lục ban hành kèm theo Quyết định này); chủ động phối hợp trong quá trình xử lý, khắc phục và xác nhận kết quả sau khắc phục.

6. Khi có kế hoạch đặt hệ thống, thiết bị CNTT tại Trung tâm THDL cần phải xác định và trình cấp có thẩm quyền phê duyệt cấp độ hệ thống thông tin; thực hiện triển khai đầy đủ các biện pháp đảm bảo an toàn thông tin cho các hệ thống được phê duyệt cấp độ. Các thiết bị trước khi lắp đặt phải được kiểm tra và đánh giá đảm bảo an toàn thông tin và chịu trách nhiệm khi có sự cố về mất an toàn, an ninh thông tin do hệ thống thuộc đơn vị mình gây ra.

Điều 32. Trách nhiệm của đơn vị quản trị, vận hành Trung tâm THDL

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

2. Ban hành nội quy làm việc tại Trung tâm THDL; xây dựng kế hoạch trực

Trung tâm THDL và bố trí bộ phận trực vận hành hệ thống Trung tâm THDL 24/24 giờ.

3. Tham mưu về quy định thủ tục chuyển giao thiết bị, cài đặt phần mềm và quản lý tài sản của Trung tâm THDL; 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.

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

5. Tham mưu các giải pháp, phương án kỹ thuật, kế hoạch phát triển Trung tâm THDL để nâng cao năng lực quản lý nhà nước, tăng cường giải pháp ứng dụng công nghệ số và chuyển đổi số cấp tỉnh.

6. Đơn vị quản trị, vận hành Trung tâm THDL sử dụng, quản lý tài sản theo đúng các quy định hiện hành về quản lý, sử dụng tài sản công và đảm bảo khai thác an toàn, hiệu quả hạ tầng Trung tâm THDL hiện có.

7. 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 phần mềm và thiết bị tại Trung tâm THDL.

8. Thực hiện báo cáo định kỳ hàng quý cho cơ quan quản lý về tình hình hoạt động và cung cấp dịch vụ của Trung tâm THDL và báo cáo đột xuất khi có yêu cầu.

Điều 33. Trách nhiệm của Cơ quan, tổ chức, cá nhân có kết nối, khai thác, sử dụng hệ thống thông tin tại Trung tâm THDL

1. Tuân thủ các quy định của pháp luật, Quy chế này và hướng dẫn của cơ quan quản lý, đơn vị quản trị, vận hành Trung tâm THDL trong quá trình kết nối, khai thác và sử dụng hệ thống thông tin.

2. Thực hiện nghiêm các quy định về bảo mật, an toàn thông tin; không thực hiện các hành vi truy cập trái phép, gây gián đoạn, làm sai lệch hoặc hủy hoại hệ thống thông tin.

3. Phối hợp với Trung tâm THDL trong việc kiểm tra, giám sát, xử lý sự cố, khắc phục rủi ro liên quan đến hệ thống thông tin do mình sử dụng.

4. Quản lý, phân quyền sử dụng tài khoản truy cập các hệ thống thông tin dùng chung của tỉnh; đảm bảo chỉ những người được phân công nhiệm vụ mới được phép sử dụng; chịu trách nhiệm khi để lộ, lọt, mất quyền kiểm soát tài khoản, mật khẩu gây ảnh hưởng đến an toàn hệ thống.

5. Kịp thời thông báo cho cơ quan quản lý, đơn vị quản trị, vận hành Trung tâm THDL khi phát hiện sự cố, nguy cơ mất an toàn thông tin hoặc khi có thay đổi về hạ tầng, dữ liệu, ứng dụng có liên quan đến việc kết nối, khai thác hệ thống.

Điều 34. Điều khoản thi hành

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

Phụ lục

DANH MỤC MẪU BIỂU QUY ĐỊNH HOẠT ĐỘNG QUẢN LÝ, KHAI THÁC, VẬN HÀNH VÀ ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI TRUNG TÂM TÍCH HỢP DỮ LIỆU TỈNH

(Ban hành kèm theo Quyết định số 59/2025/QĐ-UBND ngày 03/11/2025 của Uỷ ban nhân dân tỉnh)

STT	Danh mục	Ký hiệu
1	Đề nghị tham quan Trung tâm Tích hợp dữ liệu	Mẫu số 01
2	Báo cáo về tình hình hoạt động của Trung tâm Tích hợp dữ liệu	Mẫu số 02
3	Đề nghị cung cấp dịch vụ Trung tâm Tích hợp dữ liệu	Mẫu số 03
4	Đề nghị về việc đề nghị khắc phục, xử lý sự cố an toàn thông tin	Mẫu số 04

Mẫu số 01

TÊN TỔ CHỨC **……**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ... V/v Đề nghị tham quan Trung tâm Tích hợp dữ liệu tỉnh Bắc Ninh	*....., ngày ..... tháng ..... năm 20....*

Kính gửi: Sở Khoa học và Công nghệ

A. Thông tin chung

Tên cơ quan:.....

Địa chỉ:.....

Điện thoại:..... Email:.....

Đầu mối liên hệ (Họ và tên, địa chỉ email, số điện thoại):.....

…….

……

B. Phần đề nghị

Chúng tôi đề nghị được tham quan Trung tâm Tích hợp dữ liệu tỉnh:

1. Mục đích:

.....

2. Thời gian đến tham quan:

.....

3. Thành phần đoàn tham quan: *(Kèm theo danh sách chi tiết)*

.....

……..

4. Các đề nghị khác: *(Nếu có)*

.....

Chúng tôi cam kết tuân thủ mọi nội quy, quy định của các cơ quan chức năng khi vào tham quan Trung tâm Tích hợp dữ liệu tỉnh./.

Nơi nhận: - Như kính gửi; - Lưu: VT,….	**Thủ trưởng đơn vị** *(Ký, đóng dấu)*

Mẫu số 02

TÊN TỔ CHỨC **…….**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /BC-…	*……, ngày tháng năm 20…*

BÁO CÁO

Về tình hình hoạt động của Trung tâm Tích hợp dữ liệu

I. THÔNG TIN CHUNG

1. Kỳ báo cáo:

2. Điện thoại: …..... Fax: …..... Email: ….....

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

4. Tỷ lệ khai thác hệ thống (%):

- Về đường truyền Internet: .....
- Về cung cấp các dịch vụ hạ tầng CNTT:.....

5. Tình hình nhân sự:

- Số lượng công chức, viên chức quản lý: .....
- Số lượng viên chức, nhân viên quản trị, vận hành: .....

II. CÔNG TÁC ĐÃ TRIỂN KHAI

1. Duy trì vận hành các hệ thống, ứng dụng *(theo Mẫu biểu thống kê tại Phụ lục kèm theo)*

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

.....

3. Về 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	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. Về công tác bảo đảm an toàn, an ninh thông tin

.....

5. Công tác khác

.....

III. KẾ HOẠCH CÔNG TÁC TRIỂN KHAI

.....

.....

.....

IV. KHÓ KHĂN, VƯỚNG MẮC *(Nếu có)*

.....

.....

.....

IV. 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:

.....

.....

.....

.....

Nơi nhận:
- Sở KH&CN *(b/c);*
- Lưu: VT,….

Thủ trưởng đơn vị
(Ký, đóng dấu)

Phụ lục

MẪU BIỂU THỐNG KÊ CÁC WEBSITE/ỨNG DỤNG CỦA CƠ QUAN NHÀ NƯỚC LƯU KÝ TẠI TRUNG TÂM THDL

(Kèm theo Báo cáo số /BC-... ngày .../... /20... của...)

STT	Đơn vị chủ quản	Tên website/ứng dụng	Ghi chú
I. Danh sách các website cơ quan nhà nước			
1			
2			
3			
4			
…			
II. Danh sách các ứng dụng dịch vụ hành chính công			
1			
2			
3			
4			
…			

Mẫu số 03

TÊN TỔ CHỨC ……	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ... V/v đề nghị cung cấp sử dụng dịch vụ Trung tâm Tích hợp dữ liệu	*....., ngày ..... tháng ..... năm 20....*

Kính gửi: Sở Khoa học và Công nghệ

A. Thông tin chung

Tên cơ quan:.....

Địa chỉ:.....

Điện thoại:..... Email:.....

Đầu mối liên hệ (Họ và tên, địa chỉ email, số điện thoại): .....

B. Phần đề nghị

Chúng tôi đề nghị được sử dụng dịch vụ của Trung tâm Tích hợp dữ liệu tỉnh như sau:

1. Tên dịch vụ:.....

2. Mục đích:.....

.....

3. Thời gian sử dụng:

.....

4. Các yêu cầu kỹ thuật cụ thể khác:.....

.....

Chúng tôi cam kết tuân thủ các quy định về quản lý, vận hành và khai thác Trung tâm Tích hợp dữ liệu tỉnh./.

Nơi nhận: - Như trên; - Lưu: VT,....	**Thủ trưởng đơn vị** *(Ký, đóng dấu)*

Mẫu số 04

TÊN TỔ CHỨC **……**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ..... V/v đề nghị khắc phục, xử lý sự cố an toàn thông tin	*....., ngày ..... tháng ..... năm 20....*

Kính gửi: - Sở Khoa học và Công nghệ;
- Công an tỉnh.

A. Thông tin chung

- Tên cơ quan:.....
- Địa chỉ:.....
- Điện thoại:..... Fax:.....
- Người liên hệ (Họ tên, địa chỉ email, số điện thoại):.....

……

……

B. Thông tin sự cố

1. Mô tả sơ bộ về sự cố:

.....

.....

2. Thời gian xảy ra sự cố:.....

3. Hệ thống xảy ra sự cố *(dịch vụ xảy ra sự cố: Phần mềm, email,….)*

.....

4. Các biện pháp phòng vệ:.....

5. Yêu cầu khắc phục sự cố:.....

.....

.....

Chúng tôi cam đoan việc báo cáo sự cố trên là hoàn toàn đúng sự thật. Đề nghị quý cơ quan hỗ trợ khắc phục, xử lý sự cố an toàn thông tin./.

Nơi nhận: - Như trên; - Lưu: VT,….	**Thủ trưởng đơn vị** *(Ký, đóng dấu)*