ỦY BAN NHÂN DÂN TỈNH BẮC KẠN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 11 /2023/QĐ-UBND	*Bắc Kạn, ngày 18 tháng 5 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế quản trị, quản lý, vận hành, khai thác hệ thống hạ tầng, ứng dụng, cơ sở dữ liệu dùng chung tại Trung tâm tích hợp dữ liệu tỉnh Bắc Kạn

ỦY BAN NHÂN DÂN TỈNH BẮC KẠN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 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 tháng 11 năm 2019;

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

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

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

Căn cứ Thông tư số 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;

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

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan đảng, nhà nước;

Căn cứ Thông tư số 12/2019/TT-BTTT ngày 5 tháng 11 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông về sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan đảng, nhà nước;

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

Căn cứ Thông tư số 23/2022/TT-BTTTT ngày 30 tháng 11 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông về 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, kỹ thuật đối với trung tâm dữ liệu.

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản trị, quản lý, vận hành, khai thác hệ thống hạ tầng, ứng dụng, cơ sở dữ liệu dùng chung tại Trung tâm tích hợp dữ liệu tỉnh Bắc Kạn.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 29 tháng 5 năm 2023.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thành phố; Chủ tịch Ủy ban nhân dân các xã phường, thị trấn và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
Gửi bản giấy:
- Văn phòng chính phủ
- Vụ PC- Bộ Thông tin và Truyền thông;
- Cục kiểm tra VBQPPL- Bộ Tư pháp;

Gửi bản điện tử:
- Như Điều 3 (t/h);
- TT Tỉnh ủy;
- TT HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Ủy ban MTTQVN tỉnh;
- Đoàn ĐBQH tỉnh;
- Sở Tư pháp;
- LĐVP;
- Trung tâm CB-TH;
- Lưu: VT, Việt, Hòa.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Đăng Bình

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

QUY CHẾ

Quản trị, quản lý, vận hành, khai thác hệ thống hạ tầng, ứng dụng, cơ sở dữ liệu dùng chung tại Trung tâm tích hợp dữ liệu tỉnh Bắc Kạn

(Ban hành kèm theo Quyết định số: 11/2023/QĐ-UBND ngày 18 tháng 5 năm 2023 của Ủy ban nhân dân tỉnh Bắc Kạn)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh:

Quy chế này quy định việc quản trị, quản lý, vận hành, khai thác hệ thống hạ tầng, ứng dụng, cơ sở dữ liệu dùng chung và các biện pháp nhằm bảo đảm an toàn thông tin Trung tâm tích hợp dữ liệu.

2. Đối tượng áp dụng:

Các cơ quan hành chính, đơn vị sự nghiệp công lập, các tổ chức đoàn thể trên địa bàn tỉnh Bắc Kạn; các tổ chức, cá nhân có liên quan tham gia quản lý, vận hành, khai thác và đảm bảo an toàn thông tin Trung tâm tích hợp dữ liệu.

Điều 2. Giải thích từ ngữ

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

1. Trung tâm tích hợp dữ liệu: Là nơi tập trung các thiết bị công nghệ thông tin và viễn thông chuyên dụng với khả năng lưu trữ dữ liệu lớn, hệ thống kết nối, hệ thống mạng, hệ thống bảo mật an toàn dữ liệu, hệ thống phụ trợ và các phần mềm dùng chung.

2. Ứng dụng dùng chung: Là các phần mềm *(hệ phần mềm)* ứng dụng, cung cấp dịch vụ cho các cơ quan, đơn vị và người sử dụng được Ủy ban nhân dân tỉnh Bắc Kạn thống nhất triển khai đưa vào hoạt động tại Trung tâm tích hợp dữ liệu.

3. Mạng diện rộng *(Mạng WAN - Wide Area Network)*: Là mạng tin học được thiết lập bằng việc kết nối giữa Trung tâm tích hợp dữ liệu và mạng nội bộ của các cơ quan, đơn vị trên địa bàn tỉnh thông qua hạ tầng mạng của nhà cung cấp dịch vụ và cho phép kết nối với mạng của Chính phủ khi có yêu cầu.

4. Mạng truyền số liệu chuyên dùng trong các cơ quan nhà nước tỉnh Bắc Kạn*:* 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 do Cục Bưu điện Trung ương là chủ mạng, quản lý, điều hành hoạt động.

5. Hạ tầng kỹ thuật: Là tập hợp thiết bị công nghệ thông tin *(thiết bị định tuyến, thiết bị chuyển mạch, thiết bị lưu trữ dữ liệu, các thiết bị giám sát, bảo mật,*

máy chủ, máy trạm…), thiết bị điện *(điều hòa chính xác, tủ điện, chống sét, máng cáp điện…)*, nhà trạm, hệ thống cáp, thiết bị phòng cháy, chữa cháy, thiết bị viễn thông, thiết bị ngoại vi, mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng và các thiết bị kỹ thuật chuyên dùng khác.

6. An toàn an ninh thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin trước các nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, thiết bị mạng, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn, an ninh thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng. Là sự bảo vệ thông tin và hệ thống thông tin 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.

7. Cơ quan chủ quản Trung tâm tích hợp dữ liệu: Ủy ban nhân dân tỉnh Bắc Kạn.

8. Cơ quan chịu trách nhiệm quản lý Trung tâm tích hợp dữ liệu *(cơ quan quản lý)*: Sở Thông tin và Truyền thông tỉnh Bắc Kạn.

9. Đơn vị trực tiếp quản trị, vận hành Trung tâm tích hợp dữ liệu *(đơn vị vận hành)*: Trung tâm Công nghệ Thông tin và Truyền thông - Sở Thông tin và Truyền thông Bắc Kạn.

Điều 3. Kiến trúc và dịch vụ của Trung tâm tích hợp dữ liệu

1. Kiến trúc của Trung tâm tích hợp dữ liệu được chia làm các phân hệ sau:

a) Phân hệ mạng và truyền dẫn: Phân hệ mạng được chia làm nhiều vùng khác nhau, mỗi vùng được thiết lập các chính sách an ninh và truy cập riêng để phục vụ các mục đích khác nhau. Trung tâm tích hợp dữ liệu sử dụng đường truyền số liệu chuyên dùng để kết nối mạng WAN của tỉnh phục vụ các cơ quan, địa phương, đơn vị trên địa bàn tỉnh khai thác hệ thống dữ liệu dùng chung, sử dụng đường truyền riêng để cung cấp dịch vụ truy cập qua Internet.

b) Phân hệ an ninh: Bao gồm các thiết bị tường lửa cho lớp mạng và lớp ứng dụng, các thiết bị ngăn chặn xâm nhập trái phép, thiết bị cân bằng tải và các ứng dụng an ninh hệ thống, an ninh máy chủ. Mỗi thành phần trong phân hệ an ninh đều được thiết kế bảo đảm tính dự phòng và bổ sung, hỗ trợ lẫn nhau trong toàn bộ hệ thống của Trung tâm tích hợp dữ liệu.

c) Phân hệ máy chủ: Bao gồm hệ thống máy chủ đã được đầu tư hoặc được đặt tại Trung tâm tích hợp dữ liệu với khả năng sẵn sàng cho việc mở rộng số lượng máy chủ trong tương lai. Hệ thống máy chủ có khả năng cung cấp năng lực tính toán cho nhiều nền tảng với nhiều mục đích khác nhau như: Các ứng dụng dùng chung của tỉnh, ứng dụng chuyên ngành và các hệ thống ứng dụng thông tin khác.

d) Phân hệ lưu trữ: Bao gồm hệ thống lưu trữ tập trung với năng lực xử lý ở mức cao, khả năng lưu trữ lớn và hệ thống sao lưu, phục hồi dữ liệu. Phân hệ

được thiết kế bảo đảm khả năng mở rộng, đáp ứng nhu cầu phát triển nguồn dữ liệu trong tương lai.

đ) Phân hệ cơ sở dữ liệu: Là hệ thống các hệ cơ sở dữ liệu dùng chung hoặc chuyên ngành được xây dựng nhằm liên kết, tích hợp các ứng dụng dùng chung và chuyên ngành phục vụ ứng dụng công nghệ thông tin trong các cơ quan, đơn vị và phục vụ công dân, doanh nghiệp.

e) Phân hệ các hệ thống phụ trợ: Bao gồm hệ thống nguồn điện, điều hòa chính xác, thiết bị lưu điện, máy phát điện, sàn nâng, hệ thống máng, cáp, hệ thống phòng cháy chữa cháy, camera an ninh và các thiết bị có liên quan khác.

2. Các ứng dụng và dịch vụ được cung cấp tại Trung tâm tích hợp dữ liệu bao gồm:

a) Các ứng dụng dùng chung phục vụ cho công tác chỉ đạo điều hành, tác nghiệp của các cơ quan Nhà nước, tổ chức chính trị, chính trị - xã hội trên địa bàn tỉnh.

b) Các dịch vụ:

- Dịch vụ máy chủ, máy chủ ảo.
- Dịch vụ phân vùng cài đặt, vận hành ứng dụng (Hosting).
- Dịch vụ tạo lập, số hóa, lưu trữ dữ liệu.
- Dịch vụ thư mục (Active Directory).
- Dịch vụ rà quét, đánh giá, ứng cứu, khắc phục sự cố bảo mật ứng dụng.
- Dịch vụ quản trị hạ tầng, vận hành ứng dụng.
- Dịch vụ hỗ trợ cung cấp kết nối, chia sẻ dữ liệu.
- Các dịch vụ công nghệ thông tin khác.

Điều 4. Nguyên tắc về quản lý, vận hành, khai thác hệ thống hạ tầng, ứng dụng, cơ sở dữ liệu dùng chung Trung tâm tích hợp dữ liệu

1. Tuân thủ các nguyên tắc, bảo đảm cơ sở hạ tầng và hệ thống thông tin phục vụ ứng dụng, phát triển công nghệ thông tin theo Luật Công nghệ thông tin.

2. Bảo đảm các yêu cầu về an toàn thông tin theo Luật An toàn thông tin mạng, Luật An ninh mạng và các văn bản pháp lý hiện hành.

3. Việc thiết lập, vận hành hệ thống quản lý An toàn thông tin *(ISMS)* đảm bảo tuân thủ theo tiêu chuẩn quốc tế ISO/IEC 27001:2013 về quản lý bảo mật thông tin.

4. Việc duy trì, vận hành, nâng cấp Trung tâm tích hợp dữ liệu phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật theo 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 về sửa đổi, bổ sung một số điều của 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, kỹ thuật đối với trung tâm dữ liệu và phù hợp với Kiến trúc Chính quyền điện tử tỉnh Bắc Kạn.

5. Việc quản lý, kết nối và chia sẻ dữ liệu số không chứa thông tin bí mật nhà nước của Trung tâm tích hợp dữ liệu phải tuân thủ theo Nghị định số 47/2020/NĐ-CP ngày 09 tháng 04 năm 2020 của Chính phủ quy định về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước.

6. Việc chia sẻ dữ liệu số chứa thông tin thuộc phạm vi bí mật nhà nước được thực hiện theo Luật Bảo vệ bí mật nhà nước và các văn bản pháp lý hiện hành.

7. Đơn vị quản trị, vận hành 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 tích hợp dữ liệu hiện có.

8. Kinh phí ngân sách nhà nước thường xuyên hàng năm bảo đảm cho công tác duy trì, quản lý, vận hành Trung tâm tích hợp dữ liệu thực hiện theo quy định của Luật Ngân sách Nhà nước và các văn bản quy phạm pháp luật có liên quan.

Chương II
QUẢN LÝ, VẬN HÀNH, KHAI THÁC VÀ ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TẠI TRUNG TÂM TÍCH HỢP DỮ LIỆU

Mục 1
QUẢN LÝ, VẬN HÀNH, KHAI THÁC TRUNG TÂM TÍCH HỢP DỮ LIỆU

Điều 5. Làm việc; vào, ra Trung tâm tích hợp dữ liệu

1. Yêu cầu đối với cán bộ quản lý, vận hành hệ thống:

Cán bộ quản lý, vận hành hệ thống tại Trung tâm tích hợp dữ liệu thực hiện theo nhiệm vụ được giao. Không tự ý can thiệp vào các phần mềm, ứng dụng, dữ liệu do các cơ quan, đơn vị khác đang được cài đặt và triển khai tại Trung tâm tích hợp dữ liệu. 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.

2. Yêu cầu đối với tổ chức, cá nhân đến làm việc, sử dụng dịch vụ tại Trung tâm tích hợp dữ liệu:

a) Tuân thủ nghiêm ngặt theo các quy trình, quy định làm việc tại Trung tâm tích hợp dữ liệu.

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 *(máy chụp hình, máy quay phim, thiết bị lưu trữ...)* khi vào bên trong Trung tâm tích hợp dữ liệu, trừ các yêu cầu tác nghiệp đặc biệt của các cơ quan chức năng có thẩm quyền theo luật định.

Điều 6. Đảm bảo an toàn hoạt động

1. Trung tâm tích hợp dữ liệu chỉ được đặt các thiết bị đang hoạt động, thiết bị chuyên dụng phục vụ vận hành hệ thống; không đặt các thiết bị không đúng

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

2. Môi trường hoạt động: Đảm bảo khô ráo, sạch sẽ, độ ẩm, nhiệt độ phải phù hợp cho các thiết bị công nghệ thông tin.

3. Hệ thống phòng cháy, chữa cháy, hệ thống chống sét: Bắt buộc trang bị và được kiểm tra thường xuyên, vừa đảm bảo an toàn tuyệt đối cho toàn hệ thống thiết bị, vừa đảm bảo an toàn cho người quản trị các hệ thống tại Trung tâm tích hợp dữ liệu.

4. Hệ thống điện: Phải có ít nhất 2 nguồn ổn định, 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: Giám sát toàn bộ Trung tâm tích hợp dữ liệu liên tục 24/24 giờ trong ngày; dữ liệu hình ảnh phải được lưu trữ tối thiểu trong thời gian là 30 ngày.

6. Hệ thống quản lý vào ra *(Access Control)*: Phải hoạt động 24/24 giờ và ghi đầy đủ nhật ký nhằm đảm bảo an ninh, chính xác và linh hoạt cho Trung tâm tích hợp dữ liệu.

Điều 7. Quản lý thiết bị

1. Thiết bị công nghệ thông tin đặt tại Trung tâm tích hợp dữ liệu phải được đặt tên và dán nhãn tài sản nhà nước theo quy định.

2. Đơn vị vận hành có trách nhiệm tổng hợp tình hình quản lý, sử dụng thiết bị tại Trung tâm tích hợp dữ liệu hàng quý, năm và báo cáo đơn vị quản lý theo quy định.

3. Việc sửa chữa, thay thế thiết bị hỏng được thực hiện thường xuyên bởi đơn vị quản trị, vận hành trên nguồn ngân sách nhà nước cấp hàng năm cho đơn vị theo quy định.

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

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

Điều 8. Quản lý vận hành hạ tầng mạng

1. Hệ thống mạng phải bảo đảm:

a) Hoạt động liên tục 24/24 giờ trong ngày, ổn định, an toàn và đáp ứng được yêu cầu về băng thông cho các ứng dụng trong hệ thống.

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

c) Tuân theo các tiêu chuẩn của Trung tâm tích hợp dữ liệu về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức đi dây, đấu nối, phân bổ nút mạng.

d) Đối với các kết nối Internet phải có các giải pháp, chính sách bảo mật đảm bảo hệ thống không bị tấn công xâm nhập, lây lan virus, phần mềm độc hại từ bên ngoài; ngăn chặn, không để phát tán virus, phần mềm độc hại từ các thiết bị ngoại vi khác.

đ) Đường truyền Internet cho Trung tâm tích hợp dữ liệu tối thiểu phải từ 2 *(hai)* nhà cung cấp dịch vụ khác nhau, có giải pháp chia tải, cân bằng tải đường truyền để đảm bảo độ dự phòng cao và tính sẵn sàng cho hệ thống.

e) Cán bộ quản trị, vận hành hệ thống không được sử dụng trình duyệt hoặc các phần mềm để truy cập Internet từ các máy tính có IP chung hệ thống máy chủ thuộc Trung tâm tích hợp dữ liệu.

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

Điều 9. Quản lý mạng truyền số liệu chuyên dùng

1. Đơn vị vận hành là đơn vị đầu mối triển khai các ứng dụng hoạt động trên Mạng truyền số liệu chuyên dùng tỉnh Bắc Kạn.

2. Các đơn vị sử dụng mạng truyền số liệu chuyên dùng kết nối vào các ứng dụng của Trung tâm tích hợp dữ liệu phải tuân thủ các quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng theo Thông tư số 12/2019/TT-BTTTT ngày 05 tháng 11 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông về sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan đảng, nhà nước; Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan đảng, nhà nước.

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 tích hợp dữ liệu phải có bản quyền và sử dụng theo đúng quy định của pháp luật.

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

a) Tất cả máy chủ, máy trạm tại Trung tâm tích hợp dữ liệu phải được trang bị hệ điều hành và phần mềm diệt vi rút có bản quyền và đã được cơ quan chức năng khuyến cáo sử dụng. Phần mềm diệt vi rút 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 tích hợp dữ liệu phải được bộ phận kỹ thuật chuyên trách kiểm duyệt, đảm bảo an toàn, bảo mật thông tin.

e) 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.

f) 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 tích hợp dữ liệu dưới bất kỳ hình thức nào khi chưa được sự đồng ý của cơ quan chủ quản.

Điều 11. Quản trị sao lưu, phục hồi dữ liệu

1. Thực hiện lưu trữ đầy đủ các dữ liệu của người dùng, 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 vận hành có trách nhiệm xây dựng và triển khai thực hiện Quy trình sao lưu, phục hồi dữ liệu dự phòng cho toàn Trung tâm tích hợp dữ liệu.

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 12. Quản lý hồ sơ

1. Danh sách các loại hồ sơ lưu trữ:

a) Quy định về quản lý, triển khai, vận hành các hệ thống.

b) Các quy trình vận hành kỹ thuật các hệ thống.

c) Các quy trình bảo hành, bảo trì, bảo dưỡng hệ thống.

d) Hồ sơ thiết kế, thuyết minh kỹ thuật, hoàn công.

đ) Hồ sơ quản trị các hệ thống thông tin.

e) Hồ sơ lưu các dịch vụ cung cấp.

g) Bảng thống kê danh sách thiết bị tại Trung tâm tích hợp dữ liệu. Danh sách các thiết bị hỏng, hết khấu hao sử dụng chờ thanh lý. Biên bản bàn giao thiết bị cho người quản trị, người sử dụng *(nếu có)*.

h) Tài liệu, biên bản kiểm tra, đánh giá của Trung tâm tích hợp dữ liệu.

i) Báo cáo quản trị hệ thống, nhật ký vận hành hệ thống.

k) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ phải được lưu bằng văn bản, tập tin bản mềm trên máy tính hoặc phần mềm quản lý điều hành và phải được cập nhật khi có sự thay đổi.

Điều 13. Xử lý sự cố trong quá trình quản lý, vận hành, khai thác

1. Khi phát hiện có sự cố, quản trị viên vận hành hoặc trực hệ thống có trách nhiệm báo cáo kịp thời cho lãnh đạo đơn vị vận hành, lãnh đạo cơ quan quản lý để có biện pháp cô lập và xác định nguyên nhân xảy ra sự cố, 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) Các sự cố thông thường *(không gây ảnh hưởng đến hoạt động của Trung tâm tích hợp dữ liệu)*: Đơn vị vận hành nhanh chóng xử lý sự cố.

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 Trung tâm tích hợp dữ liệu)*: Ngay sau khi phát hiện sự cố, đơn vị 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 thuộc Bộ Thông tin và Truyền thông hướng dẫn xử lý.

c) Các sự cố đặc biệt nghiêm trọng *(gây ngưng trệ đến toàn bộ hoạt động của Trung tâm tích hợp dữ liệu)*: Đơn vị 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 nhanh về Ủy ban nhân dân tỉnh để có chỉ đạo xử lý.

3. Quy định khắc phục sự cố:

a) Thực hiện sao lưu dữ liệu trước khi khắc phục sự cố *(ưu tiên dữ liệu quan trọng)*.

b) Đảm bảo an toàn cho người và thiết bị hệ thống.

c) Ghi nhật ký diễn biến sự cố, phương án khắc phục.

4. Đối với các sự cố vượt khả năng xử lý, đơn vị quản trị, vận hành phải báo cáo lãnh đạo Cơ quan quản lý để đề nghị đơn vị tư vấn, đơn vị cung cấp, các đơn vị chuyên trách thuộc Bộ Thông tin và Truyền thông để được hỗ trợ ứng phó và khắc phục sự cố.

Điều 14. Bảo trì, bảo dưỡng Trung tâm tích hợp dữ liệu

1. Đơn vị quản trị, vận hành có trách nhiệm thực hiện bảo trì, bảo dưỡng hệ thống theo quy trình và kế hoạch được cấp có thẩm quyền phê duyệt.

2. Việc thực hiện bảo trì, bảo dưỡng các hệ thống do đơn vị quản trị, vận hành thực hiện hoặc thuê dịch vụ.

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 bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến hoạt động của Trung tâm tích hợp dữ liệu. Quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, quy trình và ghi nhật ký về tình trạng hoạt động trước và sau khi thực hiện.

Điều 15. Quản lý mật khẩu hệ thống Trung tâm tích hợp dữ liệu

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

a) Độ dài của mật khẩu:

- Đối với mật khẩu của nhân viên và người sử dụng *(dùng để đăng nhập thư điện tử, ứng dụng nghiệp vụ, máy tính cá nhân và các ứng dụng khác)*: Tối thiểu là 08 ký tự.

- Đối với mật khẩu quản trị 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 11 ký tự.

b) Nội dung mật khẩu:

- Không bao gồm các từ dễ nhớ như: Tên, ngày tháng năm sinh, số điện thoại.

- Đối với mật khẩu quản trị hệ thống phải bao gồm các loại ký tự sau: Chữ cái in thường, chữ cái in hoa, ký tự đặc biệt, số.

c) Thời gian sử dụng mật khẩu:

Đối với mật khẩu của nhân viên vận hành, của người quản trị hệ thống *(không phải quản trị cấp cao nhất)* định kỳ phải được thay đổi ít nhất 60 ngày một lần. Trường hợp có thay đổi về nhân sự hoặc yêu cầu tăng cường bảo mật về an toàn,

an ninh thông tin thì Thủ trưởng đơn vị vận hành Trung tâm tích hợp dữ liệu quyết định việc thay đổi toàn bộ mật khẩu quản trị của Trung tâm tích hợp dữ liệu.

d) Quy định lưu trữ mật khẩu:

- Không lưu trữ mật khẩu trên máy tính cá nhân, các thiết bị điện tử hoặc khi cần thiết phải lưu trữ trên máy tính và các thiết bị điện tử, mật khẩu phải được mã hóa an toàn.

- Các tài liệu liên quan đến mật mã được xem là tài liệu tối mật, không soạn thảo trên máy tính có nối mạng Internet.

Điều 16. Kiểm soát truy nhập và xác thực

1. 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 tích hợp dữ liệu phải đảm bảo chặt chẽ, đúng mục đích sử dụng. Mỗi người dùng sẽ chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

2. Hệ thống sẽ thực hiện khóa tạm thời tài khoản, không cho người sử dụng tiếp tục sử dụng tài khoản nếu 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 17. Cung cấp, tiếp nhận máy móc, thiết bị và phần mềm của các đơn vị tại Trung tâm tích hợp dữ liệu

1. Việc triển khai các dự án, nhiệm vụ ứng dụng Công nghệ thông tin trên hạ tầng Trung tâm tích hợp dữ liệu phải được quy định cụ thể trong thiết kế kỹ thuật được cơ quan có thẩm quyền phê duyệt.

2. Đối với các cơ quan, đơn vị có nhu cầu cung cấp hoặc đặt máy chủ để triển khai ứng dụng trên nền hạ tầng Trung tâm tích hợp dữ liệu: Các cơ quan, đơn vị gửi văn bản đề nghị về Sở Thông tin và Truyền thông xem xét, quyết định. Thủ tục cung cấp, tiếp nhận đặt máy chủ, cài đặt phần mềm và quản lý tài sản do đơn vị quản trị, vận hành quy định.

3. Các đơn vị có thiết bị hoặc ứng dụng đặt tại Trung tâm tích hợp dữ liệu chịu trách nhiệm quản trị nội dung, phần mềm của cơ quan mình *(thực hiện từ xa hoặc trực tiếp);* đồng thời, tuân thủ các nguyên tắc và đảm bảo an toàn an ninh hệ thống.

4. Đảm bảo yêu cầu về quản lý thiết kế, xây dựng hệ thống *(quy định chi tiết tại Điều 33 quy chế này).*

Điều 18. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Đơn vị quản trị, vận hành sử dụng, quản lý tài sản theo đúng các quy định hiện hành về quản lý, sử dụng tài sản công

1. Hàng năm, cơ quan quản lý, vận hành thực hiện tổng hợp, cập nhật tình hình quản lý, sử dụng hệ thống phần mềm, thiết bị.

2. Đối với thiết bị hỏng còn bảo hành, cơ quan 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.

3. Trường hợp thiết bị hỏng là thiết bị quan trọng *(máy chủ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị tường lửa),* cơ quan quản lý, vận hành phải có biện pháp khắc phục nhanh.

4. Hàng năm, đơn vị quản trị, vận hành phải phân loại, đánh giá mức độ an toàn thông tin để đề xuất, thực hiện các giải pháp quản lý, bảo vệ, nâng cấp cho phù hợp, đáp ứng các quy định hiện hành của pháp luật.

Mục 2
ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TẠI TRUNG TÂM TÍCH HỢP DỮ LIỆU

Điều 19. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin:

Bảo vệ thông tin, hệ thống thông tin 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 các Hệ thống thông tin thuộc Trung tâm tích hợp dữ liệu.

2. Nguyên tắc:

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn thông tin cho các hệ thống thông tin thuộc Trung tâm tích hợp dữ liệu được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 20. 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 21 quy chế này

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

a) Cán bộ quản lý, nhân viên 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.

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 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 21. 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 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) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin 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. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

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, hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

Điều 22. 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. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. 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.

Điều 23. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm:

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 24. 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. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm *(ví dụ: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm*

phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

3. 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.

4. 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 25. Giám sát thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống

1. Toàn bộ thiết bị trong hệ thống phải được giám sát vận hành và giám sát an ninh liên tục.

2. Toàn bộ dữ liệu báo cáo, xử lý sự cố, quản lý ticket… hình thành cũng như trao đổi qua hệ thống.

3. Dữ liệu cần phải được mã hóa trong quá trình truyền trên mạng giữa nhà cung cấp dịch vụ và các điểm giám sát, cũng như với bộ phận giám sát tại Trung tâm tích hợp dữ liệu của tỉnh tối thiểu đạt AES 256 bit và gửi qua mail mã hóa hoặc kênh mã hóa riêng.

4. Hệ thống phải có cơ chế có thể chủ động truy cập và giám sát hoạt động từ xa.

Điều 26. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát

1. Sở Thông tin và Truyền thông tổ chức kết nối, điều phối các cơ quan, đơn vị trên địa bàn tỉnh tham gia vào hệ thống đảm bảo an toàn, an ninh thông tin (SOC) để đảm bảo an toàn thông tin cho các hoạt động của cơ quan nhà nước trên không gian mạng; đặc biệt nêu cao vai trò giám sát hệ thống và xử lý sự cố, lỗ hổng, điểm yếu bảo mật của Đội ứng cứu sự cố mạng, máy tính *(BKCert)* tỉnh, quản trị đơn vị tham mưu Ủy ban nhân dân tỉnh.

2. Xây dựng, quản lý, vận hành hệ thống phòng, chống phần mềm độc hại tập trung cho các máy chủ, máy trạm của các cơ quan nhà nước trên địa bàn tỉnh.

3. Tổ chức kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia: Kết nối, chia sẻ thông tin giám sát an toàn thông tin với Trung tâm giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

Điều 27. 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 *(hệ điều hành, máy chủ, ứng dụng, dịch vụ…),* 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. Quản trị hệ thống hoặc trực hệ thống báo cáo lãnh đạo/cán bộ 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 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 28. Quản lý sự cố an toàn thông tin

Đơn vị vận hành và cơ quan đơn vị có hệ thống thông tin đặt tại Trung tâm tích hợp dữ liệu 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 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

2. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

3. Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

4. Đơn vị vận hành quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về an toàn thông tin, hỗ trợ, phối hợp và hướng dẫn các cơ quan 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 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 hướng dẫn của đơn vị chuyên trách về an toàn thông tin.

5. 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.

6. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo hướng dẫn của đơn vị chuyên trách về an toàn thông tin.

Điều 29. 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) 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, tổ chức.

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 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 của Bộ Thông tin và Truyền thông ban hành *(nếu có)* trên máy tính được cơ quan, đơn vị cấp cho mình; không tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

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

c) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính *(máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...)*, phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

d) Chỉ truy nhập vào các trang/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 bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn *cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...)* và định kỳ 90 ngày thay đổi mật khẩu; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ cache và cookie 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.

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 công nghệ thông tin 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 được tỉnh hoặc đơn vị chuyên môn tổ chức.

Điều 30. Quản lý giám sát an toàn hệ thống thông tin

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

a) Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

b) Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin

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

d) Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Giám sát an toàn thông tin mạng toàn diện 24/7. Bố trí nhân sự xử lý các sự cố theo hình thức từ xa và tại chỗ.

3. Giám sát an toàn thông tin liên tục và phát hiện mối đe dọa an ninh *(24/7 Security monitoring & Threat response)*: Đảm bảo mọi sự kiện an toàn thông tin được phát hiện và xử lý kịp thời để ngăn chặn các mối đe dọa an toàn an ninh thông tin.

4. Xử lý sự cố an toàn thông tin: Quy định quy trình, trình tự xử lý đối với tất cả các sự cố an toàn thông tin xảy ra đối với hệ thống mạng, hệ thống Công nghệ thông tin, máy chủ, máy tính người dùng, dịch vụ, ứng dụng *(như sự cố website bị tấn công xâm nhập, sự cố mất an toàn thông tin do mã độc gây ra, sự cố tấn công từ chối dịch vụ, ...)*.

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

a) Hoạt động giám sát, phát hiện, cảnh báo sự cố an toàn thông tin thông tin phải được cơ quan nghiệp vụ và chủ quản hệ thống thông tin thực hiện thường xuyên, liên tục, các hệ thống thông tin quan trọng quốc gia phải được triển khai các giải pháp giám sát, phát hiện và cảnh báo cố an toàn thông tin.

b) Chủ quản hệ thống thông tin, phải có trách nhiệm phối hợp với cơ quan nghiệp vụ để xây dựng, triển khai, huấn luyện, duy trì hệ thống giám sát, phát hiện và cảnh báo sự cố an toàn thông tin.

c) Thông tin giám sát phải được cơ quan nghiệp vụ tiếp nhận, phân tích, xử lý và cảnh báo đến các tổ chức, cá nhân liên quan.

6. Thông tin về nhật ký an toàn thông tin từ tất cả các thiết bị, các nguồn dữ liệu - từ phi cấu trúc, có cấu trúc, liên quan ngữ cảnh thông qua syslog, API, JDBC, WMI… hoặc công cụ giám sát máy chủ, các agent:

a) Các thiết bị mạng, thiết bị bảo mật như: Router, Switch, Firewall/IPS/IDS, Sandbox, WAF, Network APT...

b) Các máy chủ hệ thống *(cả máy chủ vật lý và ảo hóa)* trên các nền tảng khác nhau: Windows, Linux, Unix...

c) Các ứng dụng: (1) ứng dụng phục vụ hoạt động của hệ thống: DHCP, DNS, NTP, VPN, Proxy Server...; (2) ứng dụng cung cấp dịch vụ: Web, Mail, FPT, TFTP và các hệ quản trị cơ sở dữ liệu Oracle, SQL, MySQL.

d) Các thiết bị đầu cuối: Máy tính người sử dụng, máy in, máy fax, IP Phone, IP Camera...

đ) Thông tin về điểm giám sát trên đường truyền: Điểm giám sát biên tại giao diện kết nối của thiết bị định tuyến biên với các mạng bên ngoài; điểm giám sát tại mỗi vùng mạng của hệ thống.

7. Lưu trữ và bảo vệ thông tin giám sát *(nhật ký hệ thống)*:

a) Lưu trữ thông tin, dữ liệu hình thành trong quá trình giám sát tối thiểu 6 tháng.

b) Việc lưu trữ phải quy định đầy đủ về: Tần suất sao lưu dự phòng, phương tiện, thời gian lưu trữ, nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ.

c) Dữ liệu giám sát khi lưu trữ phải được mã hóa để đảm bảo tính an toàn cho thông tin, bảo vệ dữ liệu số khi lưu trữ.

8. Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát:

a) Có khả năng giám sát một cách chủ động trạng thái an ninh của toàn bộ hệ thống theo thời gian thực trên một giao diện quản lý tập trung duy nhất; quản lý nhật ký và phản hồi; kịp thời phát hiện và có biện pháp xử lý các lỗ hổng trong hệ thống. Xếp hạng cảnh báo bất thường tại từng nút mạng hoặc trên từng thiết bị, mức độ nghiêm trọng tỉ lệ thuận với mức độ khẩn trương loại bỏ mối đe dọa.

b) Cảnh báo sớm các điểm yếu, nguy cơ an ninh có thể xảy ra và điều chỉnh phòng thủ. Hỗ trợ ứng cứu và xử lý các sự cố an ninh mạng.

c) Thông báo các sự cố qua thư điện tử *(email),* theo dõi qua tài khoản từ hệ thống theo các cấp độ quản lý.

d) Thu thập, xử lý, phân tích log: Có khả năng tiếp nhận log của 04 nguồn log thiết yếu *(thiết bị mạng (router, switch)*, thiết bị bảo mật *(firewall, nids, endpoint server)*, hệ điều hành *(linux, windows),* ứng dụng *(web, mail).*

e) Phân tích phát hiện tấn công dựa vào phân tích lưu lượng mạng: Có khả năng phát hiện tấn công cơ bản lớp mạng và có khả năng phát hiện kết nối đến máy chủ điều khiển của mã độc.

f) Phân tích phát hiện tấn công Endpoints, Server: Có khả năng phát hiện các hành vi bất thường.

g) Quản lý, phân tích, cảnh báo: Có hệ thống ticket đảm bảo có các thông tin chi tiết về sự cố, tương quan giữa các sự kiện, mức độ, tình trạng xử lý.

Điều 31. Kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

1. Nội dung kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin:

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin:

a) Định kỳ theo kế hoạch của chủ quản hệ thống thông tin.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

Điều 32. Bảo đảm nguồn nhân lực

1. Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.

3. Trách nhiệm bảo đảm an toàn thông tin cho cán bộ quản lý và vận hành hệ thống.

a) Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

b) Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

c) Các cơ quan, địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên 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 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 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 33. Quản lý thiết kế, xây dựng hệ thống

1. Thiết kế an toàn hệ thống thông tin, phải có tài liệu mô tả về:

a) Quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

b) Thiết kế và các thành phần của hệ thống thông tin.

c) Phương án bảo đảm an toàn thông tin theo cấp độ.

d) 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 khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

b) Đơn vị cung cấp dịch vụ, phát triển phần mềm phải cung cấp mã nguồn phần mềm cho chủ quản hệ thống thông tin và đơn vị vận hành.

c) Phần mềm phải được kiểm thử, kiểm tra, đánh giá an toàn thông tin và nghiệm thu trước khi đưa vào sử dụng.

3. Thử nghiệm và nghiệm thu hệ thống:

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

b) Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

c) Việc thử nghiệm và nghiệm thu hệ thống được thực hiện bởi 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.

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 34. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin

1. Phân loại mức độ sự cố an toàn thông tin mạng:

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

b) Sự cố mức độ trung bình: Thực hiện theo điểm a, khoản 1, Điều 9 Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Kạn ban hành kèm theo Quyết định số 22/2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh.

c) Sự cố mức độ cao: Thực hiện theo điểm b, khoản 1, Điều 9 Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Kạn ban hành kèm theo Quyết định số 22/2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh.

d) Sự cố có tính chất nghiêm trọng: Thực hiện theo điểm c, khoản 1, Điều 9 Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Kạn ban hành kèm theo Quyết định số 22/2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh.

2. Xử lý ban đầu sự cố an toàn thông tin: Thực hiện theo khoản 2, khoản 3, khoản 4 Điều 9 Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Kạn ban hành kèm theo Quyết định số 22/2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng: Thực hiện theo Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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.

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

Điều 35. Trách nhiệm của Sở Thông tin và Truyền thông

1. Chịu trách nhiệm trước Ủy ban nhân dân tỉnh về việc quản lý, vận hành sử dụng Trung tâm tích hợp dữ liệu đảm bảo ổn định, liên tục, an toàn bảo mật thông tin, quản lý tài sản,… theo đúng quy định.

2. Tham mưu Ủy ban nhân dân tỉnh nâng cấp và mở rộng Trung tâm tích hợp dữ liệu đáp ứng nhu cầu cho các ứng dụng công nghệ thông tin, xây dựng chính quyền điện tử, đô thị thông minh của tỉnh Bắc Kạn.

3. Thanh tra, kiểm tra và giám sát việc vận hành, khai thác dịch vụ của đơn vị vận hành Trung tâm tích hợp dữ liệu.

4. Thực hiện chế độ báo cáo định kỳ hàng năm, báo cáo đột xuất cho Ủy ban nhân dân tỉnh về tình hình hoạt động Trung tâm tích hợp dữ liệu.

5. Nghiên cứu, đề xuất nhiệm vụ tích hợp chung theo hướng chuẩn hóa, thống nhất các ứng dụng Công nghệ thông tin trên Trung tâm tích hợp dữ liệu.

6. Hằng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định.

7. Xây dựng và triển khai các chương trình đào tạo, bồi dưỡng, tập huấn, diễn tập, các hội nghị, hội thảo tuyên truyền, phổ biến, cập nhật kiến thức, kỹ năng an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh; thường xuyên cập nhật thông tin, thông báo cho các cơ quan, đơn vị biết và có biện pháp phòng ngừa, ngăn chặn các rủi ro, nguy

cơ mất an toàn thông tin do phần mềm độc hại, xung đột thông tin, tấn công mạng gây ra.

Điều 36. Trách nhiệm của Trung tâm Công nghệ thông tin và Truyền thông

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin trong việc thực hiện, tiếp nhận và xử lý các sự cố về an toàn thông tin các Hệ thống thông tin tại Trung tâm tích hợp dữ liệu: Tùy theo mức độ sự cố, phối hợp với các cơ quan, đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

2. Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị theo chức năng nhiệm vụ để thực hiện việc quản lý và xử lý sự cố về an toàn thông tin các Hệ thống thông tin tại Trung tâm tích hợp dữ liệu.

3. Ban hành nội quy làm việc tại Trung tâm tích hợp dữ liệu; xây dựng kế hoạch, bố trí cán bộ trực vận hành hệ thống Trung tâm tích hợp dữ liệu 24/24 giờ.

4. Quy định thủ tục chuyển giao thiết bị, cài đặt phần mềm và quản lý tài sản của Trung tâm tích hợp dữ liệu; ban hành quy trình vận hành, tổ chức thực hiện sao lưu dữ liệu, bảo trì, bảo dưỡng, sửa chữa thiết bị và khắc phục sự cố hệ thống.

5. Quy hoạch tài nguyên hệ thống, tham mưu cơ quan quản lý các giải pháp, phương án kỹ thuật, kế hoạch phát triển Trung tâm tích hợp dữ liệu.

6. 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 tích hợp dữ liệu.

7. Hàng năm, xây dựng kinh phí đảm bảo duy trì, vận hành, bảo dưỡng, sửa chữa, thay thế trang thiết bị, xây dựng hoặc nâng cấp, cập nhật phần mềm quản lý Trung tâm tích hợp dữ liệu và chế độ trực 24/24 giờ cho cán bộ quản trị, vận hành tổng hợp chung trong dự toán chi nghiệp vụ chuyên môn của đơn vị, trình cấp có thẩm quyền phê duyệt.

8. Đào tạo cán bộ quản lý, vận hành có chuyên môn đáp ứng yêu cầu, được trang bị các kiến thức liên quan tới hoạt động của Trung tâm tích hợp dữ liệu.

9. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

Điều 37. Trách nhiệm của các cơ quan, đơn vị, người sử dụng dịch vụ

1. Sử dụng hạ tầng, dịch vụ của Trung tâm tích hợp dữ liệu theo quy chế này và các hướng dẫn khác của đơn vị quản lý, đơn vị vận hành Trung tâm tích hợp dữ liệu.

2. Tuân thủ theo Quyết định số 22/2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh Bắc Kạn về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan

nhà nước trên địa bàn tỉnh Bắc Kạn, các quy định về an toàn bảo mật thông tin trong quản lý, vận hành và khai thác Trung tâm tích hợp dữ liệu.

3. Đối với cơ quan, đơn vị: Tuân thủ các quy định về an toàn bảo mật thông tin, duy trì hoạt động các ứng dụng, hệ thống thông tin đồng thời chịu trách nhiệm về các nội dung, thông tin lưu trữ tại Trung tâm tích hợp dữ liệu do cơ quan, đơn vị cung cấp, cập nhật phù hợp với quy định pháp luật. Sao lưu dữ liệu thường xuyên của đơn vị, theo sự hướng dẫn của đơn vị vận hành.

4. Đối với người sử dụng: Sử dụng dịch vụ Trung tâm tích hợp dữ liệu trong phạm vi cho phép, tuân thủ các quy định về an toàn bảo mật thông tin, quản lý vận hành Trung tâm tích hợp dữ liệu.

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

Điều 38. Tổ chức thực hiện

1. Trường hợp các văn bản quy phạm pháp luật được dẫn chiếu trong Quy chế này mà sửa đổi, bổ sung, thay thế thì áp dụng theo văn bản được sửa đổi, bổ sung, thay thế đó.

2 . Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh mà cần sửa đổi, bổ sung, các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định./.