ỦY BAN NHÂN DÂN TỈNH CAO BẰNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 35 /2021/QĐ-UBND	*Cao Bằng, ngày 29 tháng 10 năm 2021*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng

ỦY BAN NHÂN DÂN TỈNH CAO BẰNG

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 quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015; Luật Sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật ngày 18 tháng 6 năm 2020;

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

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

Căn cứ 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;

Căn cứ 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;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 09 năm 2017 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 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;

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 bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng.

Điều 2. Quyết định này có hiệu lực kể từ ngày 09 tháng 11 năm 2021 và thay thế Quyết định số 50/2014/QĐ-UBND ngày 19 tháng 12 năm 2014 của Uỷ ban nhân dân tỉnh Cao Bằng về việc ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng.

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

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL - Bộ Tư pháp;
- Thường trực Tỉnh uỷ;
- Thường trực HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Văn phòng Tỉnh ủy;
- Các Ban đảng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các Sở, Ban ngành đoàn thể tỉnh;
- UBND các huyện, thành phố;
- VP UBND tỉnh: LĐVP, TTTT, các CV;
- Lưu: VT, VX (M).

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

Hoàng Xuân Ánh

ỦY BAN NHÂN DÂN TỈNH CAO BẰNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng

(Kèm theo Quyết định số 35/2021/QĐ-UBND ngày 29 tháng 10 năm 2021 của Ủy ban nhân dân tỉnh Cao Bằng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung về bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng.

Điều 2. Đối tượng áp dụng

1. Các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng; các tổ chức chính trị - xã hội được ngân sách nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai và các tổ chức liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Cao Bằng (sau đây gọi tắt là cơ quan, đơn vị); cán bộ, công chức, viên chức và người lao động đang làm việc trong các cơ quan, đơn vị nêu trên.

2. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các cơ quan, đơn vị thuộc khoản 1 Điều này.

Điều 3. Giải thích từ ngữ

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

1. Các khái niệm *"an toàn thông tin mạng", "mạng", "hệ thống thông tin", "chủ quản hệ thống thông tin", "xâm phạm an toàn thông tin mạng", "sự cố an toàn thông tin mạng", "rủi ro an toàn thông tin mạng", "phần mềm độc hại", "xung đột thông tin"* được định nghĩa theo quy định tại các khoản 1, 2, 3, 5, 6, 7, 8, 11 và 14 Điều 3 Luật An toàn thông tin mạng năm 2015.

2. *Nguy cơ mất an toàn thông tin mạng* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

Điều 4. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an toàn thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan, đơn vị.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 4 Luật An toàn thông tin mạng

năm 2015; Điều 41 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Chương II
QUY ĐỊNH CỤ THỂ

Điều 5. Bảo đảm an toàn thiết bị và người dùng đầu cuối

1. Tất cả máy chủ, máy trạm của cơ quan, tổ chức phải được cài đặt hệ điều hành, phần mềm phòng chống mã độc có bản quyền; thiết lập chế độ tự động rà quét mã độc khi sao chép, mở các tập tin, mở thiết bị lưu trữ ngoài; chế độ rà quét máy tính định kỳ hằng tuần; thiết lập chế độ tự động cập nhật phiên bản, thường xuyên kiểm tra, cập nhật bản vá lỗ hổng bảo mật cho hệ điều hành, phần mềm; thiết lập, cấu hình vô hiệu hóa tính năng tự động thực thi các tệp tin trên các thiết bị lưu trữ di động kết nối vào. Cá nhân không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan, tổ chức.

2. Trên máy tính người dùng phải thiết lập mật khẩu truy nhập và mật khẩu chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy; không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng.

3. Trong quá trình sử dụng thiết bị đầu cuối, truy cập hệ thống thông tin, truy cập mạng, internet:

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. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị; thiết lập, quản lý mật khẩu đảm bảo an toàn, có mức độ bảo mật cao;

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

d) 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.

4. Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính, thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình bảo mật trước khi kết nối vào hệ thống.

5. Khuyến khích các cơ quan, đơn vị đầu tư, mua sắm thiết bị công nghệ thông tin sản xuất trong nước. Nếu mua sắm thiết bị công nghệ thông tin nhập khẩu thuộc danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông quy định tại Thông tư số

04/2018/TT-BTTTT ngày 8/5/2018 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định Danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông thì phải có giấy phép nhập khẩu sản phẩm an toàn thông tin mạng và đăng ký kiểm tra nhà nước về chất lượng hàng hóa nhập khẩu.

Điều 6. Quản lý tài khoản và chữ ký số chuyên dùng chính phủ

1. Cá nhân được giao sử dụng tài khoản truy cập hệ thống chứng thực chữ ký số chuyên dùng Chính phủ (https://ca.gov.vn), cá nhân sử dụng chứng thư số, cá nhân được giao quản lý, sử dụng chứng thư số phải tuân thủ các quy định tại khoản 1, khoản 2, khoản 3, khoản 4 Điều 5 Quy chế này.

2. Chủ thuê bao chứng thư số không chia sẻ, giao quyền tài khoản, mật khẩu cho người khác; không sử dụng chứng thư số trái phép.

3. Tài khoản thư điện tử công vụ, chứng thư số chuyên dùng Chính phủ để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác.

4. Tài khoản quản lý, truy cập hệ thống chứng thực chữ ký số được giao cho công chức, viên chức chuyên trách, phụ trách công nghệ thông tin, an toàn thông tin. Khi cá nhân được giao sử dụng tài khoản truy cập hệ thống chứng thực chữ ký số có sự đổi vị trí công tác, thuyên chuyển, thôi việc, nghỉ hưu, phải bàn giao lại tài khoản cho cơ quan, tổ chức.

Điều 7. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a) Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin của các cơ quan Nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao;

b) Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ, hạn chế sử dụng mô hình mạng ngang hàng. Trang bị thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan, đơn vị khi kết nối với hệ thống bên ngoài; xây dựng hoặc thuê hệ thống giám sát an toàn thông tin để kiểm soát, phát hiện truy cập trái phép vào hệ thống;

c) Đối với các cơ quan, đơn vị có nhiều phòng, đơn vị trực thuộc có trụ sở làm việc không nằm trong cùng một khu vực, khi cấu hình kết nối trên hệ thống mạng phải thiết lập mạng riêng ảo để tăng cường an toàn cho hạ tầng mạng nội bộ;

d) Khi thực hiện truy nhập từ xa vào mạng nội bộ thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin và thiết lập mật khẩu có độ phức tạp cao;

đ) Không tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ cơ quan, đơn vị;

e) Không tự ý thay đổi, gỡ bỏ biện pháp, giải pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc. Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập, cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, mật khẩu có độ phức tạp cao, cấp phép truy nhập đối với địa chỉ vật lý, mã hóa dữ liệu;

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật;

c) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài, cơ quan, đơn vị vận hành phải tạo thêm một tên riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 8. Bảo đảm an toàn máy chủ

1. Trên hệ thống máy chủ

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

b) Khi kết nối từ xa vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa. Khuyến khích sử dụng mạng diện rộng của tỉnh được thiết lập trên nền tảng mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước để truy nhập, khai thác các hệ thống thông tin dùng chung của tỉnh.

2. Cơ quan chủ quản có trách nhiệm trang bị phần mềm phòng chống mã độc có bản quyền cho hệ thống máy chủ; cơ quan, đơn vị vận hành thiết lập chế độ tự động cập nhật phiên bản mới, các bản vá lỗi; chế độ tự động quét mã độc khi sao chép, mở các tập tin; chế độ quét toàn bộ máy tính định kỳ hằng tuần.

3. Định kỳ hằng tuần, cơ quan, đơn vị vận hành phải kiểm tra các tiến trình trên máy chủ nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy chủ.

4. Quản lý tệp tin lưu trữ sự kiện: Cơ quan, đơn vị vận hành phải thường xuyên kiểm tra, quản lý, sao lưu các tập tin nhật ký của máy chủ và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro an toàn thông tin mạng và mức độ nghiêm trọng các rủi ro đó. Thời gian lưu trữ trên máy chủ và thiết bị tùy thuộc theo cấp độ của hệ thống, hạn chế tình trạng tràn tệp tin nhật ký gây ảnh hưởng đến hoạt động của hệ thống.

5. Khi thiết lập cung cấp các dịch vụ ra môi trường mạng, cơ quan, đơn vị vận hành yêu cầu nhà cung cấp dịch vụ cấu hình trên máy chủ ứng dụng những dịch vụ thiết yếu nhất để bảo đảm hoạt động của hệ thống, không kích hoạt những chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không sử dụng; không thiết lập cấu hình các dịch vụ ra môi trường mạng đối với máy chủ cơ sở dữ liệu.

Điều 9. Bảo đảm an toàn dữ liệu

1. Cơ chế mã hóa và sao lưu dữ liệu phải đảm bảo tính toàn vẹn của dữ liệu.

2. Các cơ quan, đơn vị xây dựng danh mục các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi dữ liệu, phần mềm.

3. Dữ liệu quan trọng phải được sao lưu định kỳ tối thiểu mỗi tháng một lần, lưu trữ ở nơi an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần thiết; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

4. Đảm bảo an toàn khi thực hiện kết nối, chia sẻ tài nguyên, dữ liệu theo Điều 28 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.

5. Dữ liệu trên hệ thống máy chủ, máy trạm, thiết bị lưu trữ phục vụ hệ thống thông tin dùng chung của tỉnh, của cơ quan, đơn vị phải được đảm bảo an toàn dữ liệu, tránh lộ lọt khi mang khi vận chuyển, bảo dưỡng, sửa chữa, thanh lý.

6. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

Điều 10. Bảo đảm nguồn nhân lực

1. Cơ quan, tổ chức đảm bảo các điều kiện cho cán bộ chuyên trách được thường xuyên học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin; tham gia các chương trình tập huấn, bồi dưỡng kỹ năng an toàn thông tin, huấn luyện, diễn tập ứng cứu sự cố mạng máy tính.

2. Cán bộ được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; 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.

3. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho tổ chức cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

Điều 11. Bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Các hoạt động liên quan đến xây dựng, nâng cấp, mở rộng, quản lý, vận hành hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng. Cơ quan, tổ chức chủ quản hệ thống thông tin phải xây dựng, triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng và tổ chức giám sát, kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý.

2. Công tác quản lý, hướng dẫn và tổ chức thực hiện việc xác định cấp độ và

phương án bảo đảm an toàn thông tin mạng; thẩm định, phê duyệt hồ sơ đề xuất cấp độ; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; giám sát an toàn hệ thống thông tin; xây dựng kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng; kiểm tra, đánh giá an toàn thông tin mạng; báo cáo, chia sẻ thông tin theo quy định tại 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; 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 và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP.

Điều 12. Quản lý thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan, đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ công nghệ thông tin

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý;

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan;

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

3. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm;

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ;

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ;

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại.

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin;

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 13. Giám sát an toàn thông tin

1. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu được cài đặt tại Trung tâm dữ liệu tỉnh đều bắt buộc giám sát an toàn thông tin.

2. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu được cài đặt trên hệ thống máy chủ riêng của cơ quan, đơn vị, hoặc thuê đặt tại doanh nghiệp ngoài, chủ quản hệ thống thông tin có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ lưu ký đảm các yêu cầu giám sát an toàn thông tin tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

Điều 14. Ứng cứu sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

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

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

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

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

2. Phân loại sự cố an toàn thông tin:

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

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

c) Sự cố do lỗi của người quản trị, vận hành hệ thống;

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

3. Phân loại mức độ nghiêm trọng sự cố:

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

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

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

đ) Sự cố mức độ đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Khi có nguy cơ mất an toàn thông tin mạng hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ thấp thì cơ quan, tổ chức vận hành chỉ đạo bộ phận, cán bộ chuyên trách công nghệ thông tin, an toàn thông tin mạng phối hợp với cá nhân bị ảnh hưởng thực hiện tự ngăn chặn, xử lý, khắc phục hoặc liên hệ với đơn vị liên quan để được tư vấn, hỗ trợ ngăn chặn, xử lý, khắc phục.

5. Khi có nguy cơ mất an toàn thông tin mạng hoặc xảy ra sự cố an toàn thông tin mạng ở mức độ trung bình trở lên, hoặc gặp nguy cơ, sự cố thông thường mà cơ quan, tổ chức xét thấy không có khả năng tự ngăn chặn, xử lý được thì thực hiện thông báo hoặc báo cáo cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh để tổ chức điều phối, hỗ trợ ứng cứu.

6. Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh thực hiện nhiệm vụ theo quy chế hoạt động do Ủy ban nhân dân tỉnh ban hành và theo hướng dẫn tại Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 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.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 15. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc bảo đảm an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh.

2. Tham mưu Ủy ban nhân dân tỉnh xây dựng, đầu tư, nâng cấp các chính sách, giải pháp, hạ tầng kỹ thuật, công nghệ phục vụ quản lý, vận hành và bảo đảm an toàn thông tin mạng; tổ chức thực hiện xác định cấp độ, phương án bảo đảm an toàn thông tin mạng, giám sát, kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin dùng chung của tỉnh.

3. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Ủy ban nhân dân tỉnh đối với các cơ quan nhà nước trong tỉnh. Hướng dẫn, giám

sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy định nội bộ và thực hiện việc bảo đảm an toàn thông tin mạng cho hệ thống thông tin theo quy định.

4. Hàng năm, 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, tổ chức 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.

5. Phối hợp với Công an tỉnh, các cơ quan chức năng, có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội.

6. Chỉ đạo, hướng dẫn về nghiệp vụ quản lý vận hành, kỹ thuật bảo đảm an toàn thông tin; hỗ trợ giải quyết sự cố khi có yêu cầu.

7. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu an toàn thông tin mạng quốc gia 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. Là cơ quan đầu mối, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh.

Điều 16. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan xây dựng kế hoạch, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin, môi trường mạng gây phương hại đến an ninh quốc gia, lợi ích quốc gia, an ninh, trật tự, an toàn xã hội trên địa bàn tỉnh.

2. Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về công tác bảo đảm an toàn thông tin mạng.

3. Điều tra và xử lý các tổ chức, cá nhân vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

Điều 17. Trách nhiệm của Sở Tài chính

Sở Tài chính phối hợp với Sở Thông tin và Truyền thông; các cơ quan, đơn vị, căn cứ khả năng ngân sách địa phương tham mưu Ủy ban nhân dân tỉnh bảo đảm nguồn kinh phí triển khai công tác bảo đảm an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh, duy trì, phát triển hệ thống phòng, chống phần mềm độc hại tập trung của tỉnh.

Điều 18. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định

tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin của cơ quan, đơn vị mình.

2. Thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT hướng dẫn thực hiện Nghị định số 85/2016/NĐ-CP.

3. Nghiêm túc triển khai thực hiện các lệnh điều phối ứng cứu sự cố, thông tin cảnh báo nguy cơ lỗ hổng, mã độc của cơ quan chức năng, Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia ban hành.

4. Phân công bộ phận hoặc công chức, viên chức chuyên trách bảo đảm an toàn thông tin của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; tạo điều kiện để các công chức, viên chức phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin đối với các vị trí cần tuyển dụng hoặc phân công.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các cơ quan, đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin kịp thời, nhanh chóng và đạt hiệu quả.

6. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin.

7. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện.

8. Các cơ quan, đơn vị cử 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. Phân công lãnh đạo phụ trách công tác đảm bảo an toàn thông tin đối với các hệ thống thông tin và cơ sở dữ liệu do đơn vị quản lý.

9. Thực hiện báo cáo về an toàn thông tin khi được Sở Thông tin và Truyền thông yêu cầu.

Điều 19. Trách nhiệm của công chức, viên chức và người lao động tại các cơ quan, đơn vị

1. Trách nhiệm của công chức, viên chức phụ trách an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị:

a) Chịu trách nhiệm bảo đảm an toàn thông tin của cơ quan, đơn vị;

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các tổ chức, cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin;

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

2. Trách nhiệm của công chức, viên chức và người lao động trong các cơ quan, đơn vị:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ và các và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

c) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin do các cơ quan, đơn vị chuyên môn hoặc Sở Thông tin và Truyền thông tổ chức.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 20. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn tỉnh và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện trong phạm vi quản lý của mình.

2. Sở Thông tin và Truyền thông có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân tỉnh theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

3. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét điều chỉnh, bổ sung./.