ỦY BAN NHÂN DÂN TỈNH BẮC KẠN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 22 /2021/QĐ-UBND	*Bắc Kạn, ngày 03 tháng 12 năm 2021*

QUYẾT ĐỊNH

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

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 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 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

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

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 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

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 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 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 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;

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-BTTTT ngày 05/11/2019 của Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của 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;

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 mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Kạn.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 13 tháng 12 năm 2021 và thay thế Quyết định số 2196/2010/QĐ-UBND ngày 14 tháng 10 năm 2010 của Ủy ban nhân dân tỉnh về việc ban hành quy chế đảm bảo an toàn thông tin trong các cơ quan nhà nước, các tổ chức đoàn thể trên địa bàn tỉnh Bắc Kạn.

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

Nơi nhận:
Gửi bản giấy:
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL - Bộ Tư pháp;

Gửi bản điện tử:
- Như Điều 3;
- TT Tỉnh ủy;
- TT HĐND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- CT, PCT UBND tỉnh;
- UBMTTQVN tỉnh và các tổ chức thành viên;
- BCĐ xây dựng CQĐT tỉnh;
- Báo Bắc Kạn, Đài PT&TH Bắc Kạn;
- LĐVP;
- Cổng TTĐT tỉnh;
- Lưu: VT, NCTH.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH BẮC KẠN

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

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

(Ban hành kèm theo Quyết định số 22 /2021/QĐ-UBND ngày 03 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh Bắc Kạn)

Chương I

NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Kạn.

Điều 2: Đối tượng áp dụng

1. Các cơ quan, đơn vị thuộc và trực thuộc Ủy ban nhân dân tỉnh; các cơ quan đơn vị thuộc, trực thuộc Ủy ban nhân dân huyện, thành phố; Ủy ban nhân dân xã, phường, thị trấn;

2. Cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị quy định tại Khoản 1 Điều này.

3. Các tổ chức, cá nhân khác khi sử dụng hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai hoặc liên quan.

Điều 3. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Mục đích bảo đảm an toàn thông tin mạng nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi 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. Hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị phải tuân thủ nguyên tắc bảo đảm an toàn thông tin mạng.

Điều 4. Các hành vi bị cấm

1. Tự ý lắp đặt các thiết bị tiếp sóng Wifi (*Wireless card, Wireless USB*), thiết bị ngoại vi khác có khả năng kết nối mạng (*điện thoại thông minh, máy tính bảng...*) trên máy tính có kết nối mạng nội bộ để truy cập mạng bên ngoài, khi chưa được sự đồng ý của lãnh đạo cơ quan, đơn vị.

2. Tự ý đăng lên, tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Yêu cầu chung về quản lý an toàn thông tin mạng

1. Đối với cơ quan, đơn vị:

a) Thực hiện phân loại thông tin do đơn vị mình sở hữu theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp theo quy định của pháp luật về bảo vệ bí mật nhà nước. Khi sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải xây dựng quy định, thủ tục để xử lý thông tin, xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

b) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn mất an toàn thông tin mạng xuất phát từ tần số, kho số, tên miền và địa chỉ Internet của mình. Phối hợp, cung cấp thông tin liên quan đến an toàn tài nguyên viễn thông theo yêu cầu của cơ quan nhà nước có thẩm quyền.

c) Tổ chức các biện pháp bảo vệ hệ thống thông tin, ngăn chặn xung đột thông tin trên mạng thuộc quyền quản lý và phối hợp chặt chẽ với cơ quan nghiệp vụ theo quy định của pháp luật để triển khai các biện pháp ngăn chặn xung đột thông tin trên mạng khi vượt quá thẩm quyền, khả năng.

d) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình. Hợp tác với các cơ quan chức năng xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài.

đ) Xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của cơ quan, đơn vị mình. Khi xử lý thông tin cá nhân phải có trách nhiệm bảo đảm an toàn thông tin mạng.

e) Phân công, bố trí cán bộ chuyên trách hoặc phụ trách về công nghệ thông tin, an toàn thông tin mạng phải có trình độ đào tạo hoặc được bồi dưỡng kiến thức, kỹ năng đáp ứng yêu cầu nhiệm vụ về an toàn thông tin.

g) Thường xuyên tuyên truyền, phổ biến, nâng cao nhận thức của cán bộ, công chức, viên chức, người lao động về trách nhiệm bảo đảm an toàn thông tin mạng. Khi tiếp nhận, tuyển dụng nhân sự mới phải quán triệt các quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng. Khi nhân sự chuyển công tác, nghỉ việc, nghỉ theo chế độ phải tổ chức bàn giao, thu hồi tài khoản, quyền truy nhập và tất cả tài sản liên quan tới các hệ thống thông tin của cơ quan, đơn vị.

2. Đối với cán bộ, công chức, viên chức, người lao động:

a) Tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng, có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý.

b) Khi tham gia quản lý và khai thác mạng máy tính của cơ quan, đơn vị phải nghiêm chỉnh chấp hành chế độ an toàn, bảo mật thông tin mạng.

c) Tự quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính làm ảnh hưởng đến an toàn thông tin mạng; không được truy cập các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không truy nhập vào các đường dẫn không rõ về nội dung; không thực hiện bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép.

d) Chỉ sử dụng tài khoản thư điện tử công vụ trong trao đổi công việc; không sử dụng các dịch vụ thư điện tử công cộng để trao đổi thông tin liên quan đến công việc chuyên môn của cơ quan, đơn vị.

đ) Khi phát hiện nguy cơ mất an toàn thông tin mạng hoặc dấu hiệu sự cố an toàn thông tin mạng phải báo cáo kịp thời với cấp trên và bộ phận, cán bộ chuyên trách/phụ trách công nghệ thông tin, an toàn thông tin mạng để xem xét xử lý, khắc phục.

Điều 6. Quản lý đăng nhập, truy nhập hệ thống thông tin

1. Đối với cơ quan, đơn vị chủ quản hệ thống thông tin:

a) Tổ chức cấp tài khoản truy nhập hệ thống thông tin phù hợp với mục đích, yêu cầu, nhiệm vụ quản trị, khai thác, sử dụng hệ thống; bảo đảm tài khoản của mỗi cơ quan, đơn vị, cá nhân đăng nhập, truy nhập vào hệ thống là duy nhất.

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (*05 lần*). Hệ thống tự động áp dụng thêm các biện pháp xác thực người dùng (*captcha, xác thực email, sử dụng mật khẩu 1 lần OTP...*) và cảnh báo đến quản trị hệ thống nếu liên tục đăng nhập sai vượt quá số lần quy định. Trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản.

c) Cơ quan, đơn vị quản lý, vận hành các hệ thống thông tin dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người khai thác, sử dụng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

2. Đối với cá nhân được giao quản trị, khai thác hệ thống thông tin:

a) Thiết lập mật mã truy nhập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả máy chủ, máy trạm trong hệ thống thông tin được giao quản lý.

b) Bảo vệ bí mật thông tin tài khoản của cá nhân hoặc tài khoản của cơ quan, đơn vị khi được phân công, 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 của cá nhân hoặc của cơ quan, đơn vị.

c) Thiết lập mật khẩu đăng nhập, truy nhập khai thác, sử dụng hệ thống thông tin có độ phức tạp cao (có độ dài từ 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và

ký tự đặc biệt như !, @, #, $, %). Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 90 ngày thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

Điều 7. Phòng, chống phần mềm độc hại

1. Tất cả máy chủ, máy trạm của cơ quan, đơn vị phải được trang bị 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. Đối với việc ghi nhớ mật khẩu có thể quy định chung để quản trị đơn vị cài đặt chế độ không ghi nhớ mật khẩu đối với máy tính tại cơ quan, đơn vị.

2. 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.

3. 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, đơn vị.

4. Tất cả các máy tính của cơ quan, đơn vị 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.

5. 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 cơ quan, đơn vị phải được bộ phận kỹ thuật chuyên trách kiểm duyệt, đảm bảo an toàn, bảo mật thông tin.

6. 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.

7. 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 (WAN) 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.

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

9. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: Hoạt động chậm bất thường, có cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau, nhất là có dấu hiệu bị thay đổi, mất dữ liệu, người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng nội bộ (LAN), mạng diện rộng (WAN), mạng Internet và báo cáo, thông báo trực tiếp cho cán bộ chuyên trách công nghệ thông tin, an toàn thông tin mạng hoặc bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

10. Đảm bảo an toàn, cập nhật các bản vá cho thiết bị mạng như Router, Switch

(*danh mục thiết bị được công bố các lỗ hổng thường xuyên trên bản tin An toàn thông tin*).

11. Sau khi thành lập Trung tâm Giám sát an toàn thông tin mạng (SOC - Security Operation Center) tỉnh Bắc Kạn, Sở Thông tin và Truyền thông tổ chức kết nối, điều phối các đơn vị trên địa bàn tỉnh tham gia vào hệ thống 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 của Đội ứng cứu sự cố mạng, máy tính (BKCert) tỉnh, quản trị đơn vị tham mưu Ủy ban nhân dân tỉnh 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 tỉnh.

Điều 8. Sao lưu dữ liệu dự phòng

1. Cơ quan, đơn vị chủ quản hệ thống và cá nhân khai thác, sử dụng hệ thống thông tin thực hiện sao lưu dữ liệu dự phòng định kỳ đối với các dữ liệu quan trọng, tối thiểu mỗi tháng một lần; trường hợp cần thiết phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng ký số chứng thực.

2. Việc sao lưu dữ liệu dự phòng phải bảo đảm tính đầy đủ, toàn vẹn, và tin cậy. Sau khi sao lưu phải tổ chức lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài phù hợp, bảo đảm tính bảo mật và sẵn sàng cho việc phục hồi dữ liệu khi cần thiết.

Điều 9. Ứng cứu sự cố an toàn thông tin mạng

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

a) Sự cố mức độ trung bình: Sự cố ảnh hưởng đến một nhóm lớn người khai thác, sử dụng nhưng vẫn chưa gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị như: Hệ thống mạng của 01 (một) phòng, ban, đơn vị thuộc cơ quan, đơn vị bị ngưng hoạt động; phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 (một) phòng, ban đơn vị thuộc cơ quan, đơn vị.

b) Sự cố mức độ cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan, đơn vị như: Ứng dụng quản lý văn bản và điều hành, hệ thống một cửa điện tử, hệ thống thông tin báo cáo của cơ quan, đơn vị bị ngưng hoạt động; một số thiết bị công nghệ thông tin quan trọng (*bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tệp tin chung*) bị hư hỏng.

c) Sự cố có tính chất nghiêm trọng: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như toàn bộ hệ thống thiết bị công nghệ thông tin ngừng hoạt động; hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung; hoặc sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính, lấy cắp dữ liệu; có thể gây thiệt hại lớn cho các hệ thống thông tin quan trọng của tỉnh như: Trung tâm tích hợp dữ liệu tỉnh, Cổng thông tin điện tử, Cổng dịch vụ công và hệ thống thông tin một cửa điện tử, hệ thống quản lý văn bản và điều hành, hệ thống thông tin báo cáo, hệ thống thư điện tử công vụ và các hệ thống thông tin, cơ sở dữ liệu chuyên ngành của các sở, ban, ngành, địa phương, đòi hỏi

sự tham gia, điều phối ứng cứu sự cố của cáccơ quan, đơn vị trong tỉnh và sự hỗ trợ của các cơ quan, đơn vị chuyên trách về an toàn thông tin quốc gia để giải quyết.

2. 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, đơn vị 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 cung cấp sản phẩm, dịch vụ viễn thông, Internet, công nghệ thông tin, đơn vị triển khai ứng dụng phần mềm để được tư vấn, hỗ trợ ngăn chặn, xử lý, khắc phục.

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

4. Công chức, viên chức các đơn vị là thành viên Đội ứng cứu sự cố mạng, máy tính của tỉnh thực hiện nhiệm vụ theo quy chế hoạt động của 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.

Điều 10. Kế hoạch kiểm tra hằng năm

1. Đội Ứng cứu sự cố mạng, máy tính tỉnh Bắc Kạn (*cơ quan thường trực là Sở Thông tin và Truyền thông*) chủ trì, phối hợp với Công an tỉnh và các đơn vị liên quan tiến hành kiểm tra thường xuyên công tác đảm bảo an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn tỉnh theo Kế hoạch công tác hằng năm.

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin trên địa bàn tỉnh.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 11. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu, giúp Ủy ban nhân dân tỉnh, Ban Chỉ đạo xây dựng chuyển đổi số tỉnh Bắc Kạn tổ chức triển khai, hướng dẫn, đôn đốc, kiểm tra việc thực hiện Quy chế này; tổng hợp, thực hiện chế độ báo cáo định kỳ, đột xuất về tình hình, kết quả công tác bảo đảm an toàn thông tin mạng cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan theo quy định.

2. Tham mưu cho Ủy ban nhân dân tỉnh ban hành cơ chế, chính sách và kiểm tra đánh giá việc thực hiện xác định cấp độ an toàn hệ thống thông tin cho các đơn vị theo Khoản 1 Điều 2 Quy chế này.

3. 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.

4. 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.

5. 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; chủ trì, phối hợp với các cơ quan, đơn vị liên quan thanh tra, kiểm tra, kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trên địa bàn tỉnh.

6. Thực hiện chức năng của Đơn vị thường trực, chuyên trách về ứng cứu sự cố mạng, máy tính của tỉnh. Tham mưu UBND tỉnh tổ chức thực hiện Quy chế hoạt động của Đội ứng cứu sự cố mạng, máy tính trên địa bàn tỉnh. Tham gia các hoạt động điều phối, ứng cứu sự cốvề an toàn thông tin mạng quốc gia khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc Trung tâm ứng cứu giám sát an toàn không gian mạng quốc gia (NCSC).

7. Phối hợp với Công an tỉnh, Tiểu ban An toàn, An ninh mạng tỉnh Bắc Kạn tổ chức triển khai các hội nghị tập huấn, thành lập các đoàn công tác thực hiện nhiệm vụ tăng cường công tác đảm bảo an toàn, an ninh mạng. Phối hợp 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 và xử lý các tổ chức, cá nhân vi phạm pháp luật về an toàn, an ninh thông tin mạng theo thẩm quyền.

Điều 12. Trách nhiệm của Sở Tài chính

Căn cứ khả năng cân đối ngân sách chủ trì, phối hợp với Sở Thông tin và Truyền thông, các cơ quan, đơn vị rà soát, tham mưu cho Ủy ban nhân dân tỉnh bố trí kinh phí triển khai công tác bảo đảm an toàn thông tin các hệ thống thông tin dùng chung của tỉnh, hệ thống thông tin của các cơ quan, đơn vị và xây dựng, duy trì, phát triển hệ thống phòng,chống phần mềm độc hại tập trung của tỉnh.

Điều 13. Trách nhiệm của các Sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố.

1. Thực hiện các yêu cầu chung và quản lý an toàn thông tin theo quy định tại Điều 5, 6 Quy chế này.

2. Khi có sự cố mất an toàn thông tin tại đơn vị kịp thời phối hợp, cung cấp thông tin cho Đội ứng cứu sự cố mạng, máy tính của tỉnh và các đơn vị liên quan

triển khai công tác kiểm tra, hỗ trợ ngăn chặn, xử lý, khắc phục nguy cơ, sự cố an toàn thông tin mạng kịp thời, nhanh chóng, hiệu quả.

3. Tham gia, phối hợp các hoạt động ứng cứu, khắc phục sự cố an toàn thông tin mạng khi có yêu cầu, điều phối của Ủy ban nhân dân tỉnh, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và cơ quan, đơn vị khác có thẩm quyền.

Điều 14. Trách nhiệm của cán bộ phụ trách về an toàn thông tin, công nghệ thông tin tại cơ quan, đơn vị

1. Chịu trách nhiệm bảo đảm an toàn thông tin mạng hệ thống thông tin của cơ quan, đơn vị.

2. Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, công tác quản trị hệ thống, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

3. Thực hiện việc giám sát, đánh giá mức độ nghiêm trọng, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro gây mất an toàn thông tin mạng.

4. Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

5. 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.

Điều 15. Trách nhiệm của các tổ chức, cá nhân khác có liên quan

Các tổ chức, cá nhân khác khi sử dụng các hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Kạn phải tuân thủ các quy định tại Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 16. Tổ chức thực hiện

1. Các cơ quan, đơn vị và cá nhân nêu tại Điều 2 có trách nhiệm tổ chức thực hiện có hiệu quả Quy chế này.

2. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, Thủ trưởng cơ quan, đơn vị và cá nhân có liên quan kịp thời báo cáo UBND tỉnh (*qua Sở Thông tin và Truyền thông*) để tổng hợp, xem xét, sửa đổi, bổ sung cho phù hợp với yêu cầu thực tiễn./.