UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 31/2018/QĐ-UBND	*Vĩnh Phúc, ngày 17 tháng 12 năm 2018*

QUYẾT ĐỊNH
Ban hành Quy định bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc

ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức Chính quyền địa phương số 77/2015/QH13 ngày 19 tháng 6 năm 2015;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 80/2015/QH13 ngày 22/6/2015;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 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 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 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 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 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 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 67/TTr-STTTT ngày 03 tháng 12 năm 2018,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc.

Điều 2. Quyết định này có hiệu lực kể từ ngày 01 tháng 01 năm 2019 và thay thế Quyết định số 56/2014/QĐ-UBND ngày 28 tháng 11 năm 2014 của UBND tỉnh.

Điều 3. Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở, ban, ngành; Chủ tịch UBND huyện, thành phố và các cá nhân, đơn vị liên quan có trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- Cục KTVBQPPL - Bộ Tư pháp;
- TTTU, HĐND tỉnh, Đoàn ĐBQH tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- CPVP UBND tỉnh;
- Như Điều 3;
- UB MTTQ, các tổ chức đoàn thể;
- Cổng thông tin điện tử Chính phủ;
- TT Thông tin - Công báo (để đăng);
- Báo Vĩnh Phúc, Đài PTTH tỉnh, Cổng TTĐT tỉnh;
- Lưu: VT, VX3 (H- b)

TM.ỦY BAN NHÂN DÂN
CHỦ TỊCH

(Đã ký)

Nguyễn Văn Trì

UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY ĐỊNH
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc

(Ban hành kèm theo Quyết định số 31/2018/QĐ-UBND Ngày 17 tháng 12 năm 2018 của Ủy ban nhân dân tỉnh Vĩnh Phúc)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc (sau đây gọi tắt là cơ quan).

Điều 2. Đối tượng áp dụng

1. Quy định này được áp dụng đối với các cơ quan nhà nước tỉnh Vĩnh Phúc và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc.

2. Khuyến khích các tổ chức, doanh nghiệp, cá nhân khác trên địa bàn tỉnh thực hiện Quy định này.

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin mạng được quy định tại Khoản 1, Điều 3, Luật An toàn thông tin mạng.

2. Hệ thống thông tin được quy định tại Khoản 3, Điều 3, Luật An toàn thông tin mạng.

3. Hạ tầng kỹ thuật được quy định tại Khoản 7, Điều 3, 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.

4. Phần mềm độc hại được quy định tại Khoản 11, Điều 3, Luật An toàn thông tin mạng.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

Hoạt động ứng dụng công nghệ thông tin của các cơ quan phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 4, Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015.

Điều 5. Các hành vi bị cấm

Các hành vi bị cấm được quy định tại Điều 7, Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015.

Chương II
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Bảo đảm an toàn vật lý và môi trường

1. Các khu vực xử lý, lưu trữ thông tin, phương tiện xử lý thông tin, phương tiện bảo đảm an toàn thông tin mạng phải được đặt ở vị trí an toàn, bảo vệ bằng tường bao và kiểm soát ra vào, bảo đảm chỉ có người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Các khu vực tại khoản 1, Điều này phải có biện pháp bảo vệ phòng chống cháy nổ, ngập lụt, động đất, chống sét, tác động của môi trường và các thảm họa khác do thiên nhiên và con người gây ra.

3. Khu vực an toàn, bảo mật phải được kiểm soát và cách ly với khu vực sử dụng chung.

4. Bảo đảm thiết bị lưu trữ dữ liệu quan trọng, phần mềm bản quyền lưu trữ trên thiết bị phải được kiểm tra, xóa hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

Điều 7. Bảo đảm an toàn trong phát triển hệ thống thông tin, trao đổi thông tin trên môi trường mạng.

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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.

2. Phân loại thông tin theo các tiêu chí về giá trị và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ để áp dụng phương thức bảo vệ thích hợp.

3. Việc gửi thông tin trên mạng phải bảo đảm:

a) Không giả mạo nguồn gốc gửi thông tin;

b) Tuân thủ Quy định này và quy định của pháp luật có liên quan.

4. Khi kết nối từ xa vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa.

5. Khuyến khích sử dụng Mạng truyền số liệu chuyên dùng của tỉnh để truy cập, khai thác các hệ thống thông tin dùng chung của tỉnh.

6. Chỉ sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin do các cơ quan Nhà nước hoặc tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu trong hoạt động công vụ.

Điều 8. Quản lý truy cập

1. Các hệ thống thông tin, mạng phải sử dụng tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào hệ thống nội bộ.

2. Phải có quy định về quản lý truy cập vào hệ thống thông tin, mạng tại mỗi đơn vị.

3. Mỗi tài khoản truy cập vào hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

4. Cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập thông tin theo đúng chức năng, trách nhiệm, quyền hạn của mình.

5. Các hệ thống thông tin phải giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Thiết lập chế độ tự động khoá tạm thời tài khoản nếu liên tục đăng nhập sai vượt quá số lần quy định.

6. Hủy bỏ quyền truy cập vào hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin của cơ quan (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử công vụ, máy vi tính, tài khoản) khi cán bộ, công chức, viên chức và người lao động chuyển công tác, nghỉ hưu hoặc chấm dứt lao động hợp đồng.

7. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau tối đa 10 phút không sử dụng.

8. Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây. Mật khẩu được đặt theo quy định tại Khoản 9, Điều này.

9. Mật khẩu truy cập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt) và phải thiết lập chính sách hết hạn mật khẩu phù hợp với mức độ quan trọng của hệ thống thông tin.

10. Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng.

Điều 9. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải

được thiết lập chế độ tự động cập nhật; chế độ tự động quét phần mềm độc hại khi sao chép, mở các tập tin.

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

3. Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính trạm khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

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 các nhân và mục đích khác, không phục vụ công việc.

7. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm, người sử dụng phải kịp thời thông báo cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 10. Sao lưu dữ liệu dự phòng

1. Các cơ quan phải ban hành, thực hiện quy trình sao lưu dữ liệu dự phòng và phục hồi phù hợp cho các hệ thống thông tin và dữ liệu.

2. Các cơ quan phải lập danh sách dữ liệu cần sao lưu, phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra khả năng phục hồi hệ thống từ dữ liệu sao lưu.

3. Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên bảo đảm khả năng sẵn sàng cho việc sử dụng khi cần. Có kế hoạch kiểm tra khả năng phục hồi từ dữ liệu sao lưu.

Điều 11. Quản lý nhật ký trong quá trình vận hành hệ thống thông tin

1. Các cơ quan phải thực hiện việc ghi nhật ký (log) các thiết bị mạng, bảo mật, máy chủ, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu. Bảo đảm các sự kiện xảy ra đều được ghi nhận và lưu giữ.

2. Nhật ký phải được bảo vệ an toàn phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các công việc tối thiểu cần phải được ghi nhật ký gồm: quá trình truy cập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Thường xuyên theo dõi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo mức độ nghiêm trọng của các rủi ro có thể xảy ra.

Điều 12. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan;

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán hay đình trệ hoạt động chính của cơ quan;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và có ảnh hưởng đến hoạt động của cơ quan;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

2. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải chỉ đạo tạm dừng hoạt động của hệ thống đồng thời báo cáo khẩn cấp cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

4. Quy trình ứng cứu sự cố thực hiện theo quy định tại Điều 11, Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

Điều 13. Quy định sử dụng các hệ thống thông tin dùng chung của tỉnh

1. Các hệ thống thông tin dùng chung của tỉnh được cài đặt tại Trung tâm Hạ tầng thông tin gồm:

a) Hệ thống Cổng Thông tin - Giao tiếp điện tử của tỉnh; các cổng thông tin điện tử thành phần của các cơ quan, đơn vị; các dịch vụ công trực tuyến;

b) Hệ thống phần mềm quản lý văn bản và điều hành;

c) Hệ thống thư điện tử công vụ của tỉnh;

d) Hệ thống phần mềm một cửa điện tử;

e) Hệ thống người dùng tập trung toàn tỉnh;

f) Hệ thống phân giải tên miền nội bộ của tỉnh (Hệ thống DNS);

g) Các hệ thống thông tin khác có chức năng liên thông, tích hợp, luân chuyển dữ liệu giữa các cơ quan nhà nước của tỉnh.

2. Nghiêm cấm tiết lộ tài khoản truy cập, đấu nối, truy cập trái phép vào các hệ thống thông tin dùng chung của tỉnh;

3. Tài khoản truy cập các hệ thống thông tin dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được cấp và tối thiểu 06 tháng phải thay đổi 01 lần. Mật khẩu phải tuân thủ theo quy định tại Khoản 9, Điều 8 Quy định này.

Điều 14. Bảo vệ bí mật Nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Không được sử dụng máy tính nối mạng để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và thông tin bí mật nhà nước trên mạng.

2. Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng.

3. Khi sửa chữa, khắc phục sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo và có sự giám sát, quản lý chặt chẽ của người có thẩm quyền trong cơ quan.

4. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản, các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Tuân thủ các quy định có liên quan về công tác bảo vệ bí mật nhà nước.

5. Không trao đổi thông tin, gửi dữ liệu mang nội dung bí mật nhà nước qua mạng xã hội, thư điện tử công vụ, thư điện tử công cộng dưới mọi hình thức, trừ trường hợp thông tin, dữ liệu đã được mã hóa theo quy định của Luật Cơ yếu.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 15. Trách nhiệm của Ban chỉ đạo ứng dụng công nghệ thông tin tỉnh

Đảm nhiệm chức năng Ban chỉ đạo ứng cứu sự cố an toàn thông tin mạng tại Vĩnh Phúc và có trách nhiệm, quyền hạn theo quy định tại Điều 5, 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.

Điều 16. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Chấp hành các quy định, quy trình nội bộ, Quy định này và các quy định 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) Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm an toàn cho các thiết bị mà mình được giao sử dụng;

c) Khi phát hiện sự cố mất an toàn thông tin mạng phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách công nghệ thông tin để kịp thời ngăn chặn, xử lý;

d) Tham gia đầy đủ các chương trình đào tạo, tập huấn về an toàn thông tin mạng do Ủy ban nhân dân tỉnh chỉ đạo hoặc cơ quan chuyên trách về an toàn thông tin tổ chức.

2. Trách nhiệm của cán bộ chuyên trách, phụ trách công nghệ thông tin:

Ngoài các quy định tại Khoản 1 Điều này, cán bộ chuyên trách, phụ trách công nghệ thông tin có trách nhiệm:

a) Chủ trì tham mưu với lãnh đạo cơ quan thực hiện các nội dung quy định của Quy định này và các quy định pháp luật có liên quan đến an toàn thông tin;

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

c) Trực tiếp thiết lập các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin;

d) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay thủ trưởng cơ quan các sự cố mất an toàn thông tin mạng và mức độ nghiêm trọng của các sự cố đó;

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

Điều 17. Trách nhiệm của các cơ quan

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Văn bản này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình.

2. Phân công bộ phận hoặc cán bộ chuyên trách bảo đảm an toàn thông tin mạng của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ về an toàn thông tin mạng; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng trong cơ quan; xác định các yêu cầu, trách nhiệm đảm bảo an toàn thông tin mạng đối với các vị trí cần tuyển dụng hoặc phân công.

3. Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin mạng phù hợp với văn bản này và các quy định của pháp luật.

4. Các cơ quan, đơn vị có trách nhiệm thực hiện xác định cấp độ an toàn thông tin và đảm bảo 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 ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng 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 đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

7. Định kỳ mỗi 6 tháng các cơ quan lập báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin và Truyền thông).

Điều 18. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu giúp UBND tỉnh về công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của tỉnh.

2. Thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và đảm bảo an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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.

3. Hàng 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. Chủ trì, phối hợp với các cơ quan liên quan thanh tra, kiểm tra định kỳ hoặc đột xuất; 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.

5. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

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

7. 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 của Nhà nước.

8. 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.

9. Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan.

Điều 19. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với sở Thông tin và Truyền thông và các cơ quan, đơn vị 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 gây phương hại đến an ninh quốc gia, gây mất an ninh trật tự và an toàn thông tin mạng trong cơ quan nhà nước trên địa bàn tỉnh.

2. Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về 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 20. Trách nhiệm của đơn vị vận hành hệ thống thông tin dùng chung của tỉnh trực thuộc Sở Thông tin và Truyền thông

1. Bảo đảm an toàn thông tin mạng cho hạ tầng kỹ thuật công nghệ thông tin, các hệ thống thông tin dùng chung của tỉnh; tài nguyên Internet của tỉnh.

2. Thường xuyên rà soát, kiểm tra, đánh giá bảo đảm an toàn thông tin cho hạ tầng kỹ thuật công nghệ thông tin, hệ thống thông tin dùng chung của tỉnh.

3. Thường xuyên cập nhật các nguy cơ gây mất an toàn thông tin mạng và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

4. Là đầu mối để tiếp nhận, phối hợp, hỗ trợ các cơ quan, đơn vị giải quyết các sự cố mất an toàn thông tin mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 21. Các hành vi vi phạm Quy định này, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

Điều 22. Thủ trưởng sở, ban, ngành, Chủ tịch UBND các huyện, thành phố, tổ chức triển khai Quy định tại cơ quan, đơn vị, địa phương mình.

Điều 23. Sở Tài Chính chủ trì, phối hợp với Sở Kế hoạch và Đầu tư tham mưu, đề xuất với UBND tỉnh ưu tiên bố trí kinh phí để thực hiện các nhiệm vụ bảo đảm an toàn thông tin mạng của tỉnh; kịp thời tham mưu UBND tỉnh bổ sung kinh phí ngoài dự toán khi phát sinh sự cố khẩn cấp, bảo đảm hệ thống nhanh chóng được khắc phục.

Điều 24. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

(Đã ký)

Nguyễn Văn Trì