

Số: 07 /CT-UBND

Cao Bằng, ngày 06 tháng 5 năm 2016

CHỈ THỊ

Về việc tăng cường công tác đảm bảo an toàn thông tin trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh Cao Bằng

Thời gian qua, tình hình an toàn thông tin có nhiều diễn biến phức tạp. Nhiều đối tượng, thế lực thù địch, các loại hình tội phạm công nghệ cao đã thực hiện tấn công có chủ đích vào hệ thống thông tin của các cơ quan, tổ chức nhà nước nhằm phá hoại và chống phá Đảng, Nhà nước làm ảnh hưởng xấu và tác động tiêu cực đến sự phát triển kinh tế - xã hội, quốc phòng, an ninh. Nhằm tăng cường bảo đảm an toàn thông tin trong thời gian tới, thực hiện trách nhiệm quản lý nhà nước về an toàn thông tin thông tin tại địa phương theo quy định, Chủ tịch Ủy ban nhân dân tỉnh yêu cầu thủ trưởng các sở, ban, ngành tỉnh, Chủ tịch Ủy ban nhân dân các huyện, thành phố khẩn trương thực hiện tốt một số nội dung sau:

1. Các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố

a) Tăng cường công tác đảm bảo an toàn thông tin trên môi trường mạng. Tuyên truyền, phổ biến cho cán bộ, công chức, viên chức hiểu rõ tầm quan trọng về đảm bảo an toàn thông tin, chủ động phòng ngừa lộ, lọt bí mật Nhà nước.

b) Nghiêm túc tuân thủ quy định của Ủy ban nhân dân tỉnh tại 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 (được ban hành tại Quyết định 50/2014/QĐ-UBND ngày 19/12/2014 của Ủy ban nhân dân tỉnh).

c) Các cơ quan, đơn vị có trang thông tin điện tử phải thực hiện chế độ trực thường xuyên theo dõi hoạt động của trang thông tin điện tử; phát hiện kịp thời và có giải pháp xử lý khi bị thay đổi thông tin, bị đăng tải những thông tin lạ.

d) Tổ chức quản lý chặt chẽ các tài khoản của các hệ thống thông tin, thường xuyên tổ chức kiểm tra các tài khoản của hệ thống thông tin nhằm tránh tình trạng truy cập trái phép vào hệ thống.

đ) Trao đổi văn bản, tài liệu điện tử chỉ thực hiện trên hệ thống thông tin của cơ quan nhà nước được trang bị như: Hệ thống thư điện tử công vụ; hệ thống quản lý văn bản điều hành. Không trao đổi văn bản, tài liệu điện tử qua mạng xã hội, qua thư điện tử công cộng (gmail, yahoo mail,...), không sử dụng dịch vụ lưu trữ trực tuyến (Google Drive, Dropbox, 4shared,...) để lưu trữ, chia sẻ văn bản, tài liệu của cơ quan.

e) Tăng cường sử dụng chữ ký số trên văn bản điện tử để đảm bảo xác định nguồn gốc, tính toàn vẹn của văn bản; sử dụng chữ ký số để mã hoá tài liệu quan trọng.

g) Khi phát hiện hoặc có thông tin trong hệ thống mạng bị lây nhiễm các phần mềm gián điệp, độc hại phải khẩn trương và kiên quyết khắc phục sớm. Nếu ngoài khả năng thực hiện, đơn vị cần phối hợp Sở Thông tin và Truyền thông cùng

các đơn vị liên quan khắc phục, giải quyết dứt điểm.

h) Quan tâm trong việc đầu tư, trang bị phương tiện an toàn thông tin. Duy trì thường xuyên công tác kiểm tra, đánh giá an toàn thông tin đối với hệ thống thông tin của đơn vị.

i) Chú trọng phát triển nguồn nhân lực có trình độ về công nghệ thông tin đặc biệt là an toàn thông tin để nâng cao năng lực bảo đảm an toàn thông tin. Tạo điều kiện cho cán bộ phụ trách công nghệ thông tin được đào tạo, bồi dưỡng nâng cao kỹ năng nghiệp vụ về an toàn thông tin.

2. Sở Thông tin và Truyền thông

a) Chủ trì, phối hợp, đôn đốc các cơ quan liên quan triển khai thực hiện Kế hoạch số 3833/KH-UBND ngày 31/12/2015 của Ủy ban nhân dân tỉnh về thực hiện Đề án “Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020” trên địa bàn tỉnh Cao Bằng. Tổ chức các hoạt động tuyên truyền, nâng cao nhận thức cho cán bộ, công chức của các cơ quan nhà nước, các tổ chức, doanh nghiệp và người dân về an toàn thông tin.

b) Theo dõi, đôn đốc việc chấp hành các quy định tại 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.

c) Đẩy mạnh và tăng cường công tác quản lý nhà nước về công tác đảm bảo an toàn thông tin mạng trên địa bàn tỉnh. Chủ động phối hợp với Cục An toàn thông tin, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam trong quá trình triển khai thực hiện nhiệm vụ an toàn thông tin mạng, kiểm tra, hướng dẫn cho các cơ quan, đơn vị trên địa bàn tỉnh.

d) Chủ trì, phối hợp với các cơ quan có liên quan tham mưu, đề xuất Ủy ban nhân dân tỉnh đầu tư trang bị các thiết bị, phần mềm bảo mật chuyên dùng để đáp ứng phương tiện, công cụ nâng cao năng lực đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước.

đ) Xây dựng chương trình, kế hoạch và tổ chức đào tạo bồi dưỡng kiến thức, kỹ năng về an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

3. Công an tỉnh

a) Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các ngành liên quan tham mưu cho Chủ tịch Ủy ban nhân dân tỉnh chỉ đạo công tác bảo vệ an ninh chính trị nội bộ; tăng cường nắm bắt, dự báo tình hình trong công tác đảm bảo an ninh thông tin mạng trên địa bàn tỉnh.

b) Phối hợp triển khai các biện pháp, công tác nghiệp vụ để phòng ngừa, phát hiện, ngăn chặn kịp thời, xử lý nghiêm minh các hành vi xâm phạm an toàn, an ninh thông tin mạng.

4. Bộ Chỉ huy quân sự tỉnh

Đẩy mạnh công tác đảm bảo an ninh thông tin mạng của hệ thống thông tin quân sự, quốc phòng; chủ động xây dựng các phương án phòng vệ trước các cuộc xâm nhập, tấn công hệ thống thông tin; chủ động và sẵn sàng tham gia các hoạt động ứng cứu các sự cố thông tin mạng trên địa bàn tỉnh.

5. Sở Tài chính

Tham mưu cho Ủy ban nhân dân tỉnh bố trí kinh phí từ nguồn chi thường xuyên hành chính sự nghiệp hàng năm cho các hoạt động đảm bảo an toàn thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh như: Hoạt động tuyên truyền, phổ biến, nâng cao nhận thức về an toàn thông tin; đào tạo bồi dưỡng kiến thức, kỹ năng về an toàn thông tin; kiểm tra, đánh giá, giám sát, ứng cứu sự cố an toàn thông tin.

6. Sở Kế hoạch và Đầu tư

Tham mưu cho Ủy ban nhân dân tỉnh bố trí kinh phí từ nguồn kinh phí chi đầu tư phát triển cho các hoạt động đảm bảo an toàn thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh như: Xây dựng, triển khai hạ tầng hệ thống an toàn thông tin; đầu tư trang thiết bị phần cứng, phần mềm phục vụ cho an toàn thông tin.

7 Sở Nội vụ

Phối hợp với Sở Thông tin và Truyền thông xây dựng, triển khai kế hoạch đào tạo, bồi dưỡng nguồn nhân lực an toàn thông tin của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng.

8. Đài Phát thanh và Truyền hình Cao Bằng, Báo Cao Bằng

Chủ động triển khai Kế hoạch số 3833/KH-UBND ngày 31/12/2015 của Ủy ban nhân dân tỉnh, đẩy mạnh các hoạt động tuyên truyền, nâng cao nhận thức về đảm bảo an toàn thông tin trên các phương tiện thông tin đại chúng.

9. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin

Có trách nhiệm chủ động phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác đảm bảo an toàn thông tin mạng đối với hạ tầng viễn thông, Internet; phối hợp với các đơn vị liên quan kiểm tra, phát hiện đối tượng vi phạm an toàn thông tin mạng.

Thủ trưởng các sở, ban, ngành, đoàn thể thuộc tỉnh, các cơ quan Trung ương đóng trên địa bàn tỉnh, Chủ tịch Ủy ban nhân dân các huyện, thành phố tổ chức thực hiện nghiêm Chỉ thị này. /.

Nơi nhận:

- Bộ Thông tin và Truyền thông (để b/c);
- Thường trực Tỉnh ủy (để b/c);
- Thường trực HĐND tỉnh (để b/c);
- Chủ tịch, các PCT UBND tỉnh;
- Thường trực UBND tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- LĐVP UBND tỉnh;
- Các sở, ban, ngành, hội, đoàn thể tỉnh;
- UBND các huyện, thành phố;
- Viễn thông Cao Bằng;
- Viettel Cao Bằng;
- MobiFone Cao Bằng;
- Công TTĐT tỉnh, Báo Cao Bằng, Đài PT-TH tỉnh;
- Lưu: VT, VX (G).

CHỦ TỊCH



Hoàng Xuân Ánh

