

Số: /CT-UBND

Lào Cai, ngày tháng năm 2020

CHỈ THỊ

Về việc tăng cường đảm bảo an toàn, an ninh thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai

Thời gian qua, tình hình an toàn thông tin mạng có nhiều diễn biến phức tạp. Các thế lực thù địch, phản động, tội phạm mạng tăng cường tấn công, thâm nhập hệ thống mạng thông tin trọng yếu của Đảng, Chính phủ, các tập đoàn kinh tế, tài chính, ngân hàng để thu thập, đánh cắp thông tin bí mật nhà nước, phát tán thông tin xấu độc, phá hoại, gây rối nội bộ..., gây ảnh hưởng xấu về chính trị, kinh tế, văn hóa và trật tự, an toàn xã hội. Trên địa bàn tỉnh Lào Cai đã có các hoạt động hướng dẫn về biện pháp phòng chống, khắc phục và cảnh báo các nguy cơ mất an toàn thông tin mạng. Tuy nhiên, công tác đảm bảo an toàn thông tin mạng chưa được các cơ quan quan tâm đúng mức, chưa nhận thức đầy đủ tầm quan trọng của công tác này; thậm chí một số cơ quan, tổ chức, cá nhân còn chủ quan, sơ hở trong quản lý thông tin nội bộ và thông tin bí mật nhà nước, dẫn đến nguy cơ mất an toàn thông tin.

Thực hiện chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; đồng thời, đẩy mạnh công tác đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai, Chủ tịch UBND tỉnh yêu cầu:

1. Thủ trưởng các sở, ban, ngành cấp tỉnh; Chủ tịch UBND cấp huyện:

- Triển khai các biện pháp tăng cường đảm bảo an toàn thông tin trên môi trường mạng ở mỗi cơ quan trong thẩm quyền quản lý của đơn vị, địa phương. Chịu trách nhiệm trước UBND tỉnh, Chủ tịch UBND tỉnh nếu để xảy ra sự cố lộ, lọt thông tin bí mật nhà nước tại cơ quan, đơn vị, địa phương mình.

- Quán triệt, chỉ đạo thực hiện nghiêm túc Luật An toàn thông tin mạng năm 2015; Luật Bảo vệ bí mật nhà nước năm 2018 (có hiệu lực từ ngày 01/7/2020); Luật An ninh mạng năm 2018; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Chỉ thị số 14/CT-TTg năm 2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam do Thủ tướng Chính phủ ban hành và các văn bản khác có liên quan.

- Cử cán bộ đầu mối chịu trách nhiệm về an toàn thông tin mạng tại cơ quan, đơn vị; tổ chức thực hiện công tác kiểm tra, đánh giá an toàn thông tin mạng, giám sát, bảo vệ hệ thống thông tin nội bộ của cơ quan, đơn vị (tùy quy mô của đơn vị có thể tự thực hiện hoặc lựa chọn đơn vị có đủ năng lực thực hiện). Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Tổ ứng cứu sự cố máy tính của tỉnh để thực hiện

giám sát, phòng ngừa và ứng cứu sự cố an toàn thông tin mạng cho các hệ thống thông tin tại cơ quan, đơn vị, địa phương mình. Khi phát hiện có sự cố hoặc có nguy cơ xảy ra sự cố về an toàn thông tin mạng, thông báo về Sở Thông tin và Truyền thông, Tổ ứng cứu sự cố máy tính của tỉnh để được hỗ trợ, ứng cứu.

- Yêu cầu mọi cá nhân quản lý chặt chẽ chữ ký số, các tài khoản được cấp để khai thác các hệ thống thông tin, phần mềm nghiệp vụ, bảo đảm tính bảo mật; tuân thủ quy định, quy chế sử dụng chữ ký số khi gửi, ban hành văn bản điện tử trên môi trường mạng.

- Chỉ sử dụng các hệ thống thông tin dùng chung của tỉnh: hệ thống thư điện tử công vụ; hệ thống quản lý văn bản và điều hành,... để gửi nhận, trao đổi văn bản, tài liệu công vụ (trừ các văn bản, tài liệu có nội dung bí mật nhà nước). Bảo đảm các hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Kiểm tra, đánh giá tổng thể về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, Thông tư số 03/2017/TT-BTTTT ngày 24/02/2017 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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ. Báo cáo đầy đủ và kịp thời về tình hình bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị, địa phương theo định kỳ hằng năm hoặc khi có yêu cầu.

- Các cơ quan, đơn vị có Trang thông tin điện tử tổng hợp, Cổng thông tin điện tử, các hệ thống thông tin có kết nối Internet thực hiện theo dõi thường xuyên nhằm phát hiện và xử lý kịp thời các sự cố xảy ra; kiểm soát chặt chẽ các thông tin trước khi đưa lên trên Trang thông tin điện tử tổng hợp, Cổng thông tin điện tử và các hệ thống thông tin khác; không soạn thảo, in ấn tài liệu mật trên máy tính có kết nối mạng, điện thoại thông minh, máy tính bảng; bố trí máy tính độc lập, không kết nối mạng để soạn thảo, in ấn tài liệu mật; không lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật nhà nước trên máy tính kết nối mạng Internet, mạng nội bộ. Cần phải loại bỏ triệt để khi chuyển đổi mục đích sử dụng các thiết bị đã lưu cơ sở dữ liệu, tài liệu lưu trữ có chứa thông tin thuộc phạm vi bí mật nhà nước.

- Thường xuyên rà soát, thực hiện nâng cấp, phát triển, chuẩn hóa hạ tầng kỹ thuật công nghệ thông tin, áp dụng công nghệ mới hiện đại, đáp ứng yêu cầu triển khai các phần mềm ứng dụng chuyên ngành, phần mềm dùng chung của UBND tỉnh đảm bảo tăng cường năng lực và tính sẵn sàng của các hệ thống công nghệ thông tin duy trì ổn định, an toàn.

- Tăng cường nâng cao nhận thức, trách nhiệm, phổ biến, quán triệt thực hiện các quy định về an toàn thông tin, an ninh mạng cho toàn thể cán bộ, công chức, viên chức trong cơ quan, đơn vị mình. Bố trí cán bộ, công chức, viên chức tham gia đầy đủ các lớp tập huấn, bồi dưỡng, đào tạo chuẩn kỹ năng ứng dụng công nghệ thông tin, kỹ năng sử dụng khai thác hệ thống thông tin, an toàn thông tin.

2. Sở Thông tin và Truyền thông:

- Tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn thông tin mạng trong các cơ quan nhà nước của tỉnh.

- Làm đầu mối chuyên trách về an toàn thông tin mạng, tổ chức triển khai các giải pháp và điều phối tổ chức xử lý nguy cơ, ứng cứu sự cố mất an toàn thông tin mạng trong hệ thống cơ quan nhà nước trên địa bàn tỉnh. Phối hợp chặt chẽ với các cơ quan chuyên trách về an toàn, an ninh mạng của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng trong giám sát, chia sẻ thông tin, kiểm tra, đánh giá an toàn thông tin mạng và xử lý nguy cơ, ứng cứu sự cố; đồng thời, tăng cường công tác phối hợp với Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh trong hoạt động bảo đảm an toàn thông tin mạng phù hợp với tình hình thực tiễn của địa phương.

- Tăng cường công tác tuyên truyền, phổ biến kiến thức, trách nhiệm của cán bộ, công chức, viên chức cũng như người dân, doanh nghiệp trên địa bàn tỉnh về Luật An toàn thông tin mạng năm 2015; Luật Bảo vệ bí mật nhà nước năm 2018; Luật An ninh mạng năm 2018; các văn bản quy định chi tiết và hướng dẫn thi hành; các Nghị định của Chính phủ về xử lý vi phạm hành chính trong lĩnh vực an toàn, an ninh mạng, bảo vệ bí mật nhà nước; các quy định của bộ Luật hình sự có nội dung liên quan... nhằm nâng cao nhận thức, ý thức chấp hành pháp luật cho mọi tầng lớp nhân dân.

- Chủ trì, phối hợp với các cơ quan liên quan tổ chức thực hiện tốt Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

- Chủ động rà soát, ban hành hoặc tham mưu cấp có thẩm quyền ban hành mới hoặc sửa đổi, bổ sung các quy chế, quy định về đảm bảo an toàn an ninh mạng, giao dịch điện tử, chữ ký số... đảm bảo đồng bộ với các hệ thống văn bản quy phạm pháp luật. Hướng dẫn các cơ quan, đơn vị kiểm tra đánh giá mức độ an toàn thông tin mạng cho hệ thống thông tin thuộc thẩm quyền quản lý theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Chủ trì, phối hợp với Sở Kế hoạch và Đầu tư, Sở Tài chính và các cơ quan có liên quan tham mưu, đề xuất UBND tỉnh đầu tư trang thiết bị hạ tầng kỹ thuật, phần mềm bảo mật chuyên dùng để nâng cao năng lực đảm bảo an toàn, an ninh thông tin mạng trong hoạt động của các cơ quan nhà nước; xây dựng chương trình, kế hoạch và tổ chức đào tạo bồi dưỡng kiến thức thực hành kỹ năng về an toàn, bảo mật thông tin mạng cho đội ngũ cán bộ chuyên trách công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh. Tăng cường công tác thanh tra, kiểm tra và xử lý các tổ chức, cá nhân vi phạm quy định về đảm bảo an toàn thông tin. Phối hợp với Công an tỉnh trong hoạt động phòng, chống tội phạm trong lĩnh vực công nghệ thông tin.

- Tổ chức kiểm tra, đánh giá mức độ bảo đảm an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 theo hướng dẫn của Bộ Thông tin và Truyền thông. Triển khai hoạt động Tổ ứng cứu sự cố máy tính của tỉnh theo chức năng, nhiệm vụ. Tổ

chức đào tạo, tập huấn, nâng cao kỹ năng nghiệp vụ, diễn tập ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh; tham mưu mua sắm các trang thiết bị cần thiết đảm bảo Tổ ứng cứu sự cố máy tính của tỉnh hoạt động hiệu quả.

- Phối hợp, hướng dẫn và hỗ trợ các sở, ban, ngành tỉnh, UBND cấp huyện trong việc giám sát, rà soát, quét lỗ hổng bảo mật, ứng cứu sự cố đối với Cổng thông tin điện tử và các hệ thống thông tin đang được ứng dụng tại các cơ quan, đơn vị, địa phương.

3. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh:

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông cùng các cơ quan liên quan thực hiện công tác bảo đảm về an ninh mạng, tội phạm mạng và bảo vệ dữ liệu cá nhân trên địa bàn tỉnh.

- Chủ động thực hiện, triển khai các biện pháp, nghiệp vụ để phòng ngừa, phát hiện, ngăn chặn kịp thời, xử lý nghiêm các hành vi xâm phạm an toàn, an ninh thông tin mạng trên địa bàn tỉnh.

- Phối hợp với Sở Thông tin và Truyền thông trong các nhiệm vụ về đảm bảo an toàn, an ninh mạng theo chức năng và thẩm định cấp độ bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng của tỉnh.

4. Sở Tài chính, Sở Kế hoạch và Đầu tư:

Tham mưu ưu tiên bố trí nguồn kinh phí hằng năm cho hoạt động bảo đảm an toàn thông tin mạng của các cơ quan nhà nước trên địa bàn tỉnh và hoạt động của Tổ ứng cứu sự cố máy tính của tỉnh.

5. Sở Giáo dục và Đào tạo:

Triển khai các chương trình tuyên truyền, phổ biến, nâng cao nhận thức về an toàn, an ninh mạng trong các cơ sở đào tạo và các trường học trên địa bàn, coi đây là một nhiệm vụ bắt buộc phải được triển khai thực hiện, nhằm phòng ngừa vi phạm về an toàn, an ninh mạng trong trường học và cơ sở đào tạo.

6. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet (ISP) trên địa bàn tỉnh:

- Thiết lập, kiện toàn đầu mỗi đơn vị chuyên trách an toàn thông tin mạng trực thuộc để bảo vệ hệ thống, khách hàng của mình; tham gia hỗ trợ các cơ quan, tổ chức nhà nước giám sát, bảo vệ, kiểm tra, đánh giá an toàn thông tin mạng dưới sự điều phối, hướng dẫn của Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thông.

- Triển khai các biện pháp kỹ thuật bảo vệ trẻ em trên môi trường mạng theo hướng dẫn của Bộ Thông tin và Truyền thông.

7. Báo Lào Cai, Đài Phát thanh - Truyền hình, Cổng Thông tin điện tử tỉnh:

Phối hợp với các cơ quan, đơn vị, địa phương đẩy mạnh công tác tuyên truyền, nâng cao nhận thức về bảo đảm an toàn, an ninh mạng phục vụ cải cách hành chính, xây dựng Chính quyền điện tử và phát triển đô thị thông minh trên địa bàn tỉnh.

Yêu cầu Thủ trưởng các sở, ban, ngành cấp tỉnh; Chủ tịch UBND cấp huyện; Giám đốc các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn tỉnh thực hiện nghiêm túc Chỉ thị này./.

Nơi nhận:

- Bộ Thông tin và Truyền thông;
- TT: TU, HĐND, UBND tỉnh;
- TT Đoàn ĐBQH tỉnh;
- UBMTTQVN và các Đoàn thể tỉnh;
- Các sở, ban, ngành thuộc UBND tỉnh;
- Các cơ quan ngành dọc trên địa bàn tỉnh;
- Công an tỉnh; BCH Quân sự tỉnh;
- Viettel, VNPT, FPT Lào Cai;
- Báo Lào Cai, Đài PTTH tỉnh;
- Cổng TTĐT tỉnh;
- Lãnh đạo VPUBND tỉnh;
- Lưu: VT, TH1, NC1, VX1.

CHỦ TỊCH

Đặng Xuân Phong