

CHỈ THỊ

Về việc tăng cường đảm bảo an toàn, an ninh thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Hà Nam

Thời gian qua, việc ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh được đẩy mạnh, góp phần nâng cao hiệu lực, hiệu quả hoạt động của các cơ quan nhà nước, từng bước xây dựng Chính quyền điện tử tỉnh Hà Nam. Tuy nhiên, công tác đảm bảo an toàn, an ninh thông tin mạng chưa được các cơ quan quan tâm đúng mức, chưa nhận thức đầy đủ tầm quan trọng của công tác đảm bảo an toàn thông tin trên môi trường mạng; 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.

Để khắc phục những tồn tại, hạn chế nêu trên, nhằm tăng cường công tác đảm bảo an toàn, an ninh thông tin mạng của các cơ quan Nhà nước trên địa bàn tỉnh, Chủ tịch Ủy ban nhân dân tỉnh yêu cầu:

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

a) Quán triệt và chỉ đạo cán bộ, công chức, viên chức thực hiện nghiêm túc Luật Bảo vệ bí mật Nhà nước, Luật An toàn thông tin mạng, Luật An ninh mạng, Luật Cơ yếu, Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư về tăng cường công tác bảo đảm an toàn thông tin mạng, Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới, Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại, 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, Quyết định 23/2017/QĐ-UBND ngày 28/7/2017 của Ủy ban nhân dân tỉnh Hà Nam ban hành Quy chế đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam.

b) Tuyên truyền, nâng cao nhận thức, trách nhiệm của cán bộ, công chức, viên chức về công tác đảm bảo an toàn, an ninh thông tin mạng; chủ động phòng tránh lộ lọt bí mật nhà nước.

c) Tổ chức kiểm tra, rà soát, đánh giá bảo đảm an toàn, an ninh các hệ thống thông tin, máy chủ, máy trạm, thiết bị mạng, phần cứng, phần mềm hệ thống, phần mềm ứng dụng...; kịp thời phát hiện và xử lý các sự cố, lỗ hổng về mặt kỹ thuật của hệ thống thông tin, ngăn chặn, bóc gỡ mã độc tấn công vào hệ thống mạng của cơ quan, đơn vị; thực hiện sao lưu định kỳ các cơ sở dữ liệu của cơ quan, đơn vị.

d) Bố trí đào tạo, bồi dưỡng, tuyển dụng cán bộ chuyên trách phụ trách về công nghệ thông tin có đủ năng lực trình độ chuyên môn để trực tiếp quản lý, vận hành hệ thống mạng và các hệ thống thông tin của cơ quan, đơn vị.

đ) 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 phải thực hiện theo dõi thường xuyên trong quá trình hoạt động 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.

e) 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.

g) 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.

h) Trường hợp xảy ra các sự cố, phát hiện tấn công mạng hoặc mã độc nguy hiểm cần kịp thời chủ động xử lý. Nếu ngoài khả năng thực hiện, các cơ quan, đơn vị phối hợp với Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các cơ quan liên quan để xử lý.

2. Sở Thông tin và Truyền thông

a) Triển khai đồng bộ giải pháp kỹ thuật thực hiện giám sát an toàn thông tin, tập trung cho các hệ thống thông tin quan trọng của tỉnh đảm bảo theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông và quy định của pháp luật; đầu mối chuyên trách về an toàn thông tin.

b) Chủ động phối hợp với Cục An toàn thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam thuộc Bộ Thông tin và Truyền thông thực hiện rà soát, phát hiện, cảnh báo và xử lý sự cố mất an toàn thông tin đối với các hệ thống thông tin quan trọng của tỉnh.

c) 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 Ủy ban nhân dân 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.

d) 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.

đ) 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.

3. Công an tỉnh

Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các ngành liên quan tăng cường nắm bắt, dự báo tình hình trong công tác đảm bảo an ninh thông tin mạng trên địa bàn tỉnh; triển khai các biện pháp, công tác 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.

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, Sở Kế hoạch và Đầu tư

Căn cứ khả năng ngân sách để bố trí kinh phí hàng năm triển khai hoạt động đảm bảo an toàn, an ninh mạng của các cơ quan nhà nước trên địa bàn tỉnh.

6. 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 và đào tạo nhận thức về an toàn thông tin cho toàn bộ công chức, viên chức của các cơ quan nhà nước trên địa bàn tỉnh.

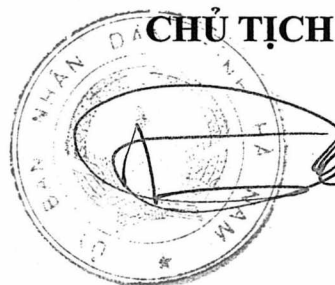
7. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet

Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác đảm bảo an toàn, an ninh thông tin mạng đối với hạ tầng viễn thông, Internet. Tham gia vào công tác ứng cứu và khắc phục sự cố cho các hệ thống thông tin quan trọng của tỉnh khi có yêu cầu.

Ủy ban nhân dân tỉnh yêu cầu Thủ trưởng các Sở, Ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thành phố; các tổ chức, cá nhân có liên quan triển khai thực hiện nghiêm túc Chỉ thị này; giao Sở Thông tin và Truyền thông theo dõi, đôn đốc và báo cáo Ủy ban nhân dân tỉnh kết quả thực hiện Chỉ thị./Đ

Nơi nhận:

- Bộ Thông tin và Truyền thông;
- TT Tỉnh ủy, TT HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các Sở, Ban, ngành;
- UBND các huyện, thành phố;
- Đài PTTH tỉnh; Báo Hà Nam;
- Công TTĐT tỉnh, Công báo tỉnh;
- Viễn thông Hà Nam; Viettel Hà Nam;
- VPUB: LĐVP, các CV, HC-TC, QT-TV;
- Lưu: VT, KGVX_(D).



Nguyễn Xuân Đông