

UBND TỈNH LÀO CAI
SỞ TƯ PHÁP

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: /STP-VP
Vv triển khai nhiệm vụ tăng cường
công tác bảo đảm an ninh mạng, phòng,
chống tấn công mạng

Lào Cai, ngày tháng năm 2024

Kính gửi:

- Các tổ chức tham mưu, tổng hợp; các phòng nghiệp vụ thuộc Sở;
- Các đơn vị sự nghiệp trực thuộc Sở.

Căn cứ hướng dẫn tại Công văn số 5316/TBATANM ngày 24/09/2024 của Tiểu ban An toàn, An ninh mạng - Công an tỉnh Lào Cai về việc tăng cường công tác bảo đảm an ninh mạng, phòng, chống tấn công mạng, Sở Tư pháp tỉnh Lào Cai đề nghị các phòng, đơn vị sự nghiệp trực thuộc Sở thực hiện một số nhiệm vụ tăng cường công tác bảo đảm an ninh mạng, phòng, chống tấn công mạng, nội dung cụ thể như sau:

1. Đối với các phòng, đơn vị sự nghiệp trực thuộc Sở:

a) Tuyên truyền, quán triệt công chức, viên chức và người lao động thuộc thẩm quyền quản lý:

- Thực hiện nghiêm các văn bản chỉ đạo về bảo đảm an toàn, an ninh mạng, bí mật nhà nước trên không gian mạng, bảo vệ dữ liệu cá nhân: Luật Bảo vệ bí mật nhà nước; Nghị định số 26/2020/NĐ-CP ngày 28/2/2020 của Chính phủ Quy định chi tiết một số điều của Luật Bảo vệ bí mật nhà nước; Công văn số 4114/BCA-ANCTNB ngày 25/11/2022 của Bộ Công an về việc hướng dẫn một số quy định của Luật Bảo vệ bí mật nhà nước; Công điện số 33/CĐ-TTg ngày 07/4/2024 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn thông tin mạng; Thông báo số 2009/TB-A05-TTANMQG ngày 11/4/2024 của Trung tâm An ninh mạng Quốc gia-Bộ Công an hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia ... và các văn bản khác liên quan đến thực hiện nhiệm vụ bảo đảm an toàn, an ninh mạng, bí mật nhà nước trên không gian mạng, bảo vệ dữ liệu cá nhân.

- Truy cập kênh Zalo OA “**Công an Lào Cai - Phòng ngừa tội phạm**” kích hoạt chế độ “**Quan tâm**” để thường xuyên được cập nhật thông tin, cảnh báo phòng ngừa các loại tội phạm hàng ngày, nâng cao cảnh giác với các loại tội phạm đặc biệt là tội phạm mạng công nghệ cao (sử dụng điện thoại thông minh quét mã QR Code kèm theo để kích hoạt chế độ “**Quan tâm**” cập nhật thông tin).

- Nâng cao ý thức cảnh giác khi thực hiện các hoạt động trên mạng internet, mạng viễn thông, như: Chia sẻ thông tin cá nhân trên mạng xã hội, sử dụng các hình thức thanh toán trực tuyến, mua bán hàng hóa, đầu tư tiền ảo, tiền điện tử,

huy động vốn... không để tội phạm lợi dụng hoạt động, trở thành nạn nhân của tội phạm sử dụng công nghệ cao; tích cực, chủ động tố giác tội phạm.

- Thực hiện bảo vệ dữ liệu cá nhân, không chia sẻ, lưu trữ thông tin cá nhân, thẻ căn cước công dân, mã số thuế cá nhân... trên các trang mạng xã hội, máy tính, phần mềm được kết nối với mạng Internet, tiềm ẩn nhiều nguy cơ mất an toàn, an ninh thông tin trên không gian mạng.

- Thực hiện nghiêm túc các quy định của pháp luật về đảm bảo an toàn, an ninh mạng, bảo vệ bí mật nhà nước. Không truy cập vào các trang thông tin độc hại, không tự động cài đặt các phần mềm không có bản quyền, phần mềm không phục vụ cho công tác chuyên môn. Khi kết nối thiết bị lưu trữ ngoài (USB, ổ cứng di động, thẻ nhớ ...) vào máy tính trạm phục vụ, thực hiện chế độ tự động quét virus cho các thiết bị.

- Khi sử dụng hộp thư điện tử công vụ cảnh giác và không mở các tập tin hay đường liên kết được gửi qua các trang mạng xã hội, không truy cập vào các tập tin đính kèm, hình ảnh lạ được gửi từ người lạ, mạo danh hoặc hộp thư điện tử không rõ nguồn gốc...

- Nghiêm túc việc thực hiện 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 của nhà nước trên máy tính kết nối mạng Internet (dữ liệu trên máy tính cá nhân, USB, thư mục); loại bỏ triệt để khi chuyển đổi mục đích sử dụng các thiết bị đã lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật của nhà nước (ổ cứng di động, ổ cứng máy vi tính cho, tặng các cơ quan, đơn vị, các xã nông thôn mới).

b) Phối hợp thông báo kịp thời với Văn phòng Sở khi phát hiện máy tính phục vụ chuyên môn của mình bị nhiễm virus, mã độc để cùng giải quyết, khắc phục.

c) Các đơn vị sự nghiệp thuộc Sở chỉ đạo công tác bảo đảm an toàn, an ninh mạng, bí mật nhà nước trên không gian mạng, bảo vệ dữ liệu cá nhân của đơn vị; chịu trách nhiệm trước Giám đốc Sở nếu đơn vị thuộc phạm vi quản lý không tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ hoặc để xảy ra mất an toàn thông tin, lộ lọt thông tin, dữ liệu cá nhân, bí mật nhà nước.

2. Đối với Văn phòng Sở

a) Tham mưu rà soát, tăng cường các giải pháp bảo đảm an toàn thông tin mạng cho các hệ thống thông tin, ưu tiên các giải pháp giám sát, cảnh báo sớm;

b) Phối hợp với Sở Thông tin và Truyền thông đảm bảo thực hiện hiệu quả, thực chất, thường xuyên, liên tục, ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng đối với các cơ sở dữ liệu, hệ thống thông tin quan trọng, dùng chung.

c) Bố trí nhân lực bảo vệ an ninh mạng; cử cán bộ tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng cho cán bộ, đảng viên, đội ngũ chuyên trách công nghệ thông tin, an ninh mạng tại đơn vị đáp ứng năng lực, yêu cầu bảo vệ an ninh mạng và bí mật nhà nước trên không gian mạng.

Đề nghị các phòng, các đơn vị sự nghiệp trực thuộc Sở nghiêm túc triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Lãnh đạo Sở;
- Lưu: VT, VP

Mã QR



GIÁM ĐỐC

Lê Ngọc Quỳnh