UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 17 /CT-UBND	*Vĩnh Phúc, ngày 15 tháng 6 năm 2023*

CHỈ THỊ
Về việc tăng cường công tác bảo đảm an toàn thông tin mạng trong các cơ quan nhà nước tỉnh Vĩnh Phúc

Thời gian qua, tỉnh Vĩnh Phúc đã đẩy mạnh triển khai bảo đảm an toàn thông tin mạng gắn với chuyển đổi số, phát triển chính quyền số, kinh tế số và xã hội số. Công tác bảo đảm an toàn thông tin mạng bước đầu đã được Bộ Thông tin và Truyền thông ghi nhận, đánh giá cao về thứ hạng. Tuy nhiên, việc hướng dẫn, tổ chức thực thi pháp luật về an toàn thông tin mạng; xây dựng, ban hành các chỉ đạo, quy định, quy chế; triển khai các biện pháp kỹ thuật bảo vệ an toàn thông tin mạng chưa đáp ứng được yêu cầu của sự phát triển, phù hợp với nhu cầu thực tiễn. Nhận thức và trách nhiệm về bảo đảm an toàn thông tin mạng còn hạn chế; hoạt động giám sát, đánh giá, bảo vệ hệ thống thông tin trong của một số cơ quan, tổ chức nhà nước còn chưa đạt yêu cầu, dẫn đến một số hệ thống thông tin đã bị xâm nhập, mất an toàn hệ thống.

Trong thời gian tới, để tăng cường bảo đảm an toàn thông tin mạng, khắc phục các hạn chế tồn tài nêu trên, tạo môi trường số an toàn, lành mạnh, góp phần cải thiện Chỉ số xếp hạng an toàn thông tin mạng và Chỉ số Chuyển đổi số của tỉnh, UBND tỉnh yêu cầu:

1. Thủ trưởng các sở, ban, ngành; Chủ tịch UBND các huyện, thành phố; Giám đốc các đơn vị sự nghiệp trực thuộc UBND tỉnh thực hiện một số giải pháp sau:

a) Quán triệt nguyên tắc an toàn thông tin là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm tạo và duy trì môi trường mạng an toàn, tin cậy cho cơ quan, tổ chức và người dân khai thác, sử dụng dịch vụ; đầu tư cho an toàn thông tin mạng là đầu tư cho phát triển bền vững và tạo ra những giá trị mới; Thủ trưởng các cơ quan, đơn vị, địa phương chịu trách nhiệm trước Chủ tịch UBND tỉnh nếu để xảy ra mất an toàn thông tin mạng tại cơ quan, đơn vị mình quản lý.

b) Khẩn trương chỉ định, kiện toàn đầu mối phụ trách về an toàn thông tin mạng để làm tốt công tác tham mưu: thực thi pháp luật về an toàn thông tin mạng, triển khai các biện pháp bảo vệ an toàn thông tin mạng và ứng cứu sự cố an toàn thông tin mạng; công bố trên Cổng thông tin điện tử của cơ quan, đơn vị. Yêu cầu hoàn thành trước ngày 30/6/2023 và bổ sung cập nhật khi có sự thay đổi. Bảo đảm

100% cán bộ, công chức, viên chức được tuyên truyền và tham gia các chương trình đạo tạo, tập huấn về kỹ năng bảo đảm an toàn thông tin mạng.

c) Đối với bảo đảm an toàn hệ thống thông tin theo cấp độ: triển khai phương án an toàn thông tin phải phù hợp với cấp độ của từng hệ thống thông tin. Bảo đảm 100% hệ thống thông tin đang quản lý, vận hành được cấp có thẩm quyền thẩm định, phê duyệt cấp độ trước ngày 30/6/2023; triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước ngày 31/8/2023. Các hệ thống thông tin xây dựng mới phải ưu tiên triển khai sử dụng hạ tầng công nghệ thông tin, an toàn thông tin dùng chung tại Trung tâm dữ liệu của tỉnh; triển khai xây dựng hồ sơ cấp độ an toàn hệ thống thông tin, phê duyệt cùng quá trình phê duyệt dự án liên quan đến công nghệ thông tin.

d) Đối với công tác kiểm tra, đánh giá an toàn thông tin: định kỳ hàng năm, lựa chọn tổ chức, doanh nghiệp kiểm tra, đánh giá an toàn thông tin mạng cho hệ thống thông tin đã được phê duyệt cấp độ. Nội dung, tần suất, tiêu chuẩn đánh giá tuân thủ 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 và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 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.

đ) Đối với ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý: Nghiêm túc thực hiện khắc phục kịp thời các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng; chuyển hoạt động ứng cứu sự cố sang chủ động săn lùng các mối nguy hại để phòng ngừa, ngăn chặn. Mỗi hệ thống thông tin phải xây dựng và ban hành phương án, kịch bản ứng cứu sự cố. Thời hạn hoàn thành trước ngày 31/12/2023 và cập nhật kịp thời khi có thay đổi.

e) Đối với phòng chống mã độc: Rà soát, nâng cấp, thay thế, bổ sung để bảo đảm 100% máy chủ, máy trạm của đơn vị được cài đặt phần mềm phòng chống mã độc tập trung đáp ứng yêu về cầu tính năng kỹ thuật theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại. Thực hiện xong trước ngày 31/12/2023. Các cơ quan, đơn vị phối hợp với Sở Thông tin và Truyền thông hoàn thành triển khai đến cấp xã trước 31/12/2024, mở rộng đến các đơn vị sự nghiệp giáo dục, y tế trong giai đoạn 2025-2026; tham gia các chiến dịch làm sạch không gian mạng hàng năm do Sở Thông tin và Truyền thông tổ chức.

g) Đối với bảo về dữ liệu cá nhân: Chỉ đạo các đơn vị triển khai hoạt động thu thập, xử lý, sử dụng, lưu trữ thông tin cá nhân phải tuân thủ quy định tại mục 2, Chương II, Luật An toàn thông tin mạng, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn có liên quan; Phát triển phần mềm nội bộ tuân thủ các tiêu chuẩn, quy chuẩn và hướng dẫn bảo đảm an toàn thông tin của Bộ thông tin và Truyền thông; các hệ

thống thử nghiệm có thu thập, xử lý, lưu trữ thông tin cá nhân phải được bảo đảm an toàn thông tin như hệ thống đang vận hành thật.

h) Đối với tuyên truyền, nâng cao nhận thức và đào đào tạo nhân lực về an toàn thông tin mạng: Sở Thông tin và Truyền thông; Sở Giáo dục và Đào tạo; Sở Lao động, Thương binh và Xã hội; UBND các huyện, thành phố và các sở, ban, ngành liên quan khẩn trương, nghiêm túc thực hiện có hiệu quả Kế hoạch số 224/KH-UBND ngày 26/8/2021 của UBND tỉnh tuyên truyền, nâng cao nhận thức, phổ biến kiến thức và đào tạo nguồn nhân lực về an toàn thông tin giai đoạn 2021-2025 trên địa bàn tỉnh Vĩnh Phúc.

i) Bảo đảm bố trí tối thiểu đạt 10% trong tổng kinh phí cho hạng mục an toàn thông tin trong kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin (trong trường hợp chủ đầu tư chưa có 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).

k) Quán triệt, cử và tạo điều kiện cho cán bộ, chuyên viên phụ trách công nghệ thông tin, an toàn thông tin tham gia đầy đủ, nghiêm túc các đợt tập huấn, diễn tập về an toàn thông tin mạng.

2. Sở Thông tin và Truyền thông

a) Căn cứ chỉ đạo của Chính phủ, Thủ tướng Chính phủ, Bộ Thông tin và Truyền thông tham mưu với Tỉnh ủy, HĐND, UBND cụ thể hóa thành cơ chế, chính sách, khung pháp lý, nhiệm vụ bảo đảm an toàn thông tin mạng của tỉnh.

b) Tăng cường công tác kiểm tra tuân thủ quy định của pháp luật về an toàn thông tin mạng. Hàng năm chủ trì, phối hợp tổ chức tối thiểu 02 đợt kiểm tra, đánh giá tuân thủ các quy định pháp luật về an toàn thông tin đối với các đơn vị, tổ chức, doanh nghiệp thuộc phạm vi quản lý (Ưu tiên, tập trung kiểm tra tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định của Luật An toàn thông tin mạng).

c) Duy trì và nâng cao hiệu quả của mô hình bảo đảm an toàn thông tin "4 lớp" (Lực lượng tại chỗ; Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia) theo Kế hoạch số 188-KH/TU ngày 17/7/2020 của Ban Thường vụ Tỉnh ủy về việc thực hiện Chỉ thị số 41-CT/TW ngày 24/3/2020 của Ban Bí thư về tăng cường phối hợp và triển khai đồng bộ các biện pháp bảo đảm an toàn, an ninh mạng.

d) Khẩn trương đầu tư, nâng cấp, triển khai Trung tâm giám sát an toàn thông tin mạng để thực hiện giám sát, phát hiện, cảnh báo an toàn thông tin mạng tập trung cho các hệ thống thông tin của tỉnh (trên cơ sở kiện toàn bộ máy hiện có, không làm phát sinh đơn vị, tổ chức mới).

đ) Tham mưu tổ chức, kiện toàn lại Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về an toàn thông tin mạng do Bộ Thông tin và Truyền thông quy định. Công bố số điện thoại đường dây nóng 24/24 trên Cổng thông tin – Giao tiếp điện tử của tỉnh để tiếp nhận thông tin báo cáo sự cố và hướng dẫn kịp thời cách phòng, ngừa, xử lý.

e) Khai thác, sử dụng Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia do Cục An toàn thông tin triển khai tại địa chỉ irlab.vn trong công tác báo cáo sự cố, ứng cứu sự cố, huấn luyện, diễn tập để nâng cao năng lực cán bộ và được hỗ trợ khi xảy ra sự cố an toàn thông tin mạng. Mỗi năm tham mưu UBND tỉnh chỉ đạo, triển khai tối thiểu 01 chiến dịch làm sạch không gian mạng cho các cơ quan nhà nước của tỉnh.

g) Chủ trì, phối hợp với Sở Nội vụ tham mưu UBND tỉnh kiện toàn tổ chức, biên chế, phê duyệt vị trí việc làm về an toàn thông tin mạng cho đơn vị chuyên trách về an toàn thông tin mạng; kết hợp giữa sử dụng nguồn nhân lực tại chỗ và thuê ngoài các chuyên gia để bảo đảm nguồn nhân lực cho công tác bảo đảm an toàn thông tin mạng của tỉnh.

h) Hàng năm phối hợp với các cơ quan, đơn vị tổ chức tối thiểu 01 đợt tập huấn kết hợp diễn tập an toàn thông tin mạng thực chiến cho các hệ thống thông tin cấp độ 3 trở lên.

i) Hướng dẫn các sở ngành, địa phương, đơn vị xây dựng và ban hành phương án, kịch bản ứng cứu sự cố.

k) Chịu trách nhiệm toàn diện về công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

l) Định kỳ hàng năm (trước ngày 15/12) báo cáo kết quả thực hiện Chỉ thị này với UBND tỉnh.

3. Công an tỉnh

a) Chủ trì phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh ban hành Kế hoạch của UBND tỉnh triển khai Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030. Hoàn thành trước ngày 30/9/2023.

b) Phối hợp với Sở Thông tin và Truyền thông triển khai các hoạt động thực thi bảo đảm an toàn thông tin mạng; hoạt động thanh tra, kiểm tra về bảo đảm an toàn thông tin mạng và ứng cứu sự cố an toàn thông tin mạng; các nhiệm vụ khác về an toàn thông tin mạng theo chức năng, nhiệm vụ được giao và chỉ đạo của Bộ Công an.

4. Sở Nội vụ: Phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh kiện toàn tổ chức, biên chế và phê duyệt vị trí việc làm về an toàn thông tin mạng cho cơ quan chuyên trách về an toàn thông tin mạng.

5. Sở Tài chính: Phối hợp với các cơ quan, đơn vị để rà soát, đề xuất nhu cầu kinh phí cho công tác bảo đảm an toàn thông tin mạng tại các cơ quan, đơn vị, địa phương trên địa bàn tỉnh theo đúng quy định.

6. Đài Phát thanh và Truyền hình tỉnh, Báo Vĩnh Phúc, Cổng Thông tin – Giao tiếp điện tử: Tăng cường đa dạng hóa hình thức tuyên truyền về an toàn thông tin mạng trên các nền tảng số. Tập trung thực hiện các nhiệm vụ được giao theo Kế hoạch số 224/KH-UBND ngày 26/8/2021 của UBND tỉnh tuyên truyền, nâng cao nhận thức, phổ biến kiến thức và đào tạo nguồn nhân lực về an toàn thông tin giai đoạn 2021-2025 trên địa bàn tỉnh Vĩnh Phúc.

7. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin: Có trách nhiệm phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác bảo đảm an toàn thông tin mạng, ứng cứu sự cố đối với hạ tầng viễn thông, Internet; thực hiện công bố thông tin đầu mối tiếp nhận sự cố trên cổng/trang thông tin điện tử; cảnh báo đến khách hàng và hỗ trợ xử lý sự cố đối với dịch vụ do doanh nghiệp cung cấp.

Yêu cầu Thủ trưởng các Sở, ban, ngành; Chủ tịch UBND các huyện, thành phố; Giám đốc các đơn vị sự nghiệp trực thuộc UBND tỉnh và các cơ quan, đơn vị, cá nhân liên quan có trách nhiệm thực hiện nghiêm Chỉ thị này./.

Nơi nhận:
- Bộ TT&TT (B/c);
- TT Tỉnh ủy; TT HĐND tỉnh (B/c);
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- CPVP UBND tỉnh;
- Các Sở, ban, ngành;
- Công an tỉnh; Bộ CHQS tỉnh;
- UBND các huyện, thành phố;
- UBND các xã, phường, thị trấn;
- Báo Vĩnh Phúc; Đài PTTT tỉnh; Công TTGTĐT tỉnh;
- Các Doanh nghiệp viễn thông trên địa bàn tỉnh;
- Lưu: VT, CVNCTH; VX3;

(H- b)

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Vũ Chí Giang