

*

Số 92 - CV/ĐU

Quang Lịch, ngày 04 tháng 6 năm 2026

v/v triển khai Luật An ninh mạng
năm 2025.

Kính gửi: Các phòng, ban, cơ quan Đảng, Chính quyền xã.

Thực hiện Kế hoạch số 14-KH/ĐU, ngày 22/01/2026 của Đảng ủy xã triển khai thực hiện nhiệm vụ về chuyển đổi số, đảm bảo an ninh mạng tại các phòng, ban cơ quan Đảng năm 2026 và nội dung Hội nghị tập huấn công tác đảm bảo an ninh mạng, diễn tập thực chiến phòng chống tấn công mạng năm 2026 (*chương trình theo Kế hoạch số 110-KH/UBND ngày 31/3/2026 của UBND tỉnh Hưng Yên*). Trong đó, có nội dung triển khai thi hành Luật An ninh mạng năm 2025:

Luật An ninh mạng năm 2025 được Quốc hội ban hành ngày 10/12/2025 và có hiệu lực từ ngày 01/7/2026, nhằm thiết lập khuôn khổ pháp lý thống nhất, đồng bộ và hiện đại về công tác quản lý Nhà nước đối với an ninh mạng từ “xử lý, khắc phục hậu quả” sang “chủ động phòng ngừa, phát hiện sớm, ngăn chặn từ sớm, từ xa” các nguy cơ đe dọa an ninh mạng, với những điểm mới về: (1) Hợp nhất Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 để thống nhất và mở rộng phạm vi áp dụng, (2) Ưu tiên tự chủ công nghệ (Make in VietNam), (3) Tăng ngân sách bắt buộc cho an ninh mạng, (4) Bổ sung đối tượng bảo vệ đặc biệt (trẻ em và người yếu thế), (5) Chuẩn hóa nhân sự an ninh mạng, (6) Quy định rõ các hành vi bị cấm, (7) Cụ thể các văn bản hỗ trợ và hiệu lực thi hành (Tài liệu gửi kèm theo).

Để nâng cao chất lượng công tác đảm bảo an ninh mạng trọng hoạt động tại các cơ quan Đảng, Chính quyền và an ninh mạng trên địa bàn xã, Ban Thường vụ Đảng ủy xã đề nghị các phòng, ban, cơ quan Đảng, Chính quyền xã triển khai thực hiện:

1. Công tác phổ biến, tuyên truyền.

- Tiếp tục tăng cường công tác phổ biến, quán triệt: Luật An ninh mạng năm 2025; Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường đảm bảo an ninh mạng trong hệ thống chính trị; Chương trình hành động thực hiện Chỉ thị số 57-CT/TW của Ban Thường vụ Tỉnh ủy đến toàn thể cán bộ, cán bộ, viên chức và người lao động, để thống nhất đầu mối, trách nhiệm quản lý nhà nước về công tác an ninh mạng¹ và nâng cao nhận thức trách nhiệm trong hoạt động trên môi trường

¹ 1 Mục 2- phần III - CTHĐ số 09-CTr/TU ngày 13/02/2026, Thống nhất đầu mối, trách nhiệm quản lý nhà nước đảm bảo hiệu lực, hiệu quả. Trong đó:

- Về an ninh mạng: Công an tỉnh chịu trách nhiệm trước BTV TU chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin, CSDL của toàn hệ thống Chính trị.....

mạng, góp phần thực hiện tốt các nhiệm vụ chuyển đổi số trong hệ thống chính trị trên địa bàn xã đáp ứng yêu cầu nhiệm vụ trong giai đoạn hiện nay.

- UBND xã chỉ đạo Phòng Văn hóa xã hội đăng tải nội dung Luật An ninh mạng năm 2025; Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường đảm bảo an ninh mạng trong hệ thống chính trị trên Cổng thông tin điện tử của xã phục vụ công tác thông tin tuyên truyền rộng rãi đến đảng viên và Nhân dân.

- MTTQ và các tổ chức chính trị xã hội xã tích cực tuyên truyền đến hội viên, đoàn viên và Nhân dân trên địa bàn xã Luật an ninh mạng, tập trung tuyên truyền các quy định về: phòng chống xâm hại trẻ em trên không gian mạng, các hành vi bị cấm nghiêm cấm về an ninh mạng, để nâng cao ý thức trách nhiệm công dân, cộng đồng trong hoạt động trên mạng, đặc biệt là việc bảo vệ an toàn dữ liệu cá nhân và các quy định về hoạt động sử dụng, truyền đưa thông tin trên nền tảng mạng xã hội.

- Khuyến khích đảng viên, cán bộ, công chức, viên chức tại các cơ quan Đảng, Chính quyền xã nêu cao tinh thần gương mẫu, tuyên truyền những điểm mới, trọng tâm của Luật An ninh mạng năm 2025 đến người thân, nhân dân nơi cư trú, góp phần huy động sức mạnh toàn dân trong xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng theo chỉ đạo của Trung ương, Tỉnh.

2. Một số nhiệm vụ cụ thể.

- Các cơ quan, đơn vị chỉ đạo phòng chuyên môn căn cứ quy định tại Luật An ninh mạng năm 2025 và các văn bản hướng dẫn của Trung ương, Tỉnh rà soát, cập nhật quy chế, quy định tại cơ quan về hoạt động quản lý, vận hành và các nghiệp vụ trên môi trường điện tử đảm bảo phù hợp với quy định hiện hành.

- Toàn thể cán bộ công chức tiếp tục thực hiện nghiêm: các bước bảo mật thiết bị (máy tính, điện thoại di động cá nhân, các thiết bị điện tử khác), quản lý, sử dụng các tài khoản mật khẩu trong các giao dịch điện tử, các nghiệp vụ trên môi trường mạng để bảo vệ dữ liệu cá nhân và đảm bảo an ninh mạng.

Nhận được Công văn đề nghị các phòng, ban, cơ quan tích cực thực hiện.

Nơi nhận:

- Như kính gửi;
- BTV ĐU xã (để báo cáo);
- BCĐ, Tổ Giúp việc PTKHCN&CĐS xã (p/h);
- Lưu: VT.

T/L BAN THƯỜNG VỤ

CHÁNH VĂN PHÒNG



Nguyễn Thị Loan

TÀI LIỆU THAM KHẢO



Sáng ngày 10/12, Quốc hội chính thức thông qua Luật An ninh mạng 2025.

Luật An ninh mạng 2025 là sự hợp nhất giữa Luật An ninh mạng 2018 và Luật An toàn thông tin mạng 2015. Mục tiêu của việc hợp nhất này là đơn giản hóa cơ cấu quản lý, tránh chồng chéo, và tạo ra hành lang pháp lý thống nhất.

Luật này bao gồm 8 chương và 45 điều, quy định về an ninh mạng, quyền và nghĩa vụ của tổ chức, cá nhân, các hoạt động bảo vệ an ninh mạng, các hành vi bị cấm, phối hợp liên ngành và đầu tư hạ tầng. Nó cũng bổ sung nhiều khái niệm mới và điều chỉnh các quy định cũ để kịp thời đối phó với sự phát triển nhanh chóng của công nghệ và gia tăng các rủi ro trên không gian mạng, nhằm bảo vệ người dùng tốt hơn.

Nâng cao năng lực tự chủ về an ninh mạng

Một điểm mới quan trọng trong Luật An ninh mạng 2025 là việc mở rộng phạm vi bảo vệ đối với các nhóm yếu thể trên không gian mạng. Theo đó, trẻ em, người cao tuổi và những người gặp khó khăn trong nhận thức được xác định là đối tượng ưu tiên trong công tác phổ biến kiến thức và hướng dẫn kỹ năng an ninh mạng.

Điều 35 trong luật lần đầu tiên xác nhận rõ trách nhiệm của Nhà nước trong việc khuyến khích, phối hợp với tổ chức, doanh nghiệp và cá nhân triển khai các chương trình giáo dục để nâng cao nhận thức và năng lực tự bảo vệ cho các nhóm này.

So với các quy định trước đây, nơi chỉ dừng lại ở mức “phổ biến kiến thức về an ninh mạng,” Luật An ninh mạng 2025 đã cụ thể hóa đối tượng ưu tiên, đáp ứng nhu cầu thực tế, khi nhóm yếu thể đang trở thành mục tiêu của nhiều hình thức lừa đảo, xâm hại dữ liệu cá nhân và tấn công tâm lý trên mạng.

Một điểm mới đáng chú ý khác là Điều 37, lần đầu tiên ghi nhận việc nâng cao năng lực tự chủ về an ninh mạng. Nhà nước khuyến khích và tạo điều kiện để cơ quan, tổ chức và cá nhân nâng cao năng lực tự chủ về an ninh mạng, đồng thời tăng cường khả năng sản xuất, kiểm tra, đánh giá và kiểm định thiết bị số, dịch vụ mạng và ứng dụng mạng.

Đặc biệt, hoạt động đầu tư xây dựng hạ tầng công nghiệp an ninh mạng được xác định là ngành nghề đặc biệt ưu đãi đầu tư, hưởng nhiều ưu đãi theo pháp luật về đầu tư, thuế và đất đai. Nhà nước

sẽ ưu tiên bố trí ngân sách phát triển các cơ sở nghiên cứu, thí nghiệm, trung tâm dữ liệu lớn, khu công nghiệp an ninh mạng tập trung, tổ hợp công nghiệp an ninh mạng.

Các hành vi bị nghiêm cấm

Luật An ninh mạng 2025 dành một điều quan trọng để xác định rõ các hành vi bị nghiêm cấm, nhằm tạo cơ sở pháp lý vững chắc để cơ quan chức năng xử lý vi phạm và bảo vệ người dân trước các rủi ro trên mạng. Danh mục hành vi cấm trong luật này đã được quy định chi tiết hơn rất nhiều so với các luật trước đây, bao quát hầu hết các hành vi nguy hiểm và phổ biến hiện nay.

Một trong những hành vi bị cấm là việc đăng tải và phát tán thông tin chống Nhà nước, tuyên truyền xuyên tạc, kích động chiến tranh, chia rẽ dân tộc, tôn giáo, xúc phạm lãnh tụ, anh hùng dân tộc hoặc phá hoại khối đại đoàn kết toàn dân tộc. Các nội dung xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, kích động phân biệt đối xử về giới và chủng tộc cũng bị nghiêm cấm.

Một nhóm hành vi quan trọng khác bị cấm là việc phát tán thông tin bịa đặt, sai sự thật, gây ảnh hưởng đến kinh tế - xã hội, gây hoang mang trong nhân dân hoặc làm gián đoạn hoạt động của các cơ quan nhà nước. Điều này đặc biệt quan trọng trong bối cảnh các tin giả về tài chính, ngân hàng, chứng khoán hay giá cả thị trường đang lan rộng trên mạng xã hội.

Luật cũng liệt kê các hành vi vi phạm phổ biến như: xúc phạm danh dự, nhân phẩm người khác; lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc online; quảng cáo, mua bán hàng hóa cấm; vi phạm bản quyền; giao dịch trái phép thông tin thẻ tín dụng, tài sản mã hóa; làm giả trang thông tin điện tử của cơ quan, tổ chức.

Một điểm mới đặc biệt là việc cấm sử dụng trí tuệ nhân tạo hoặc các công nghệ mới để giả mạo hình ảnh, giọng nói, video của người khác trái pháp luật. Đây là bước điều chỉnh quan trọng trong bối cảnh công nghệ deepfake đang ngày càng trở thành công cụ lừa đảo và xâm phạm đời tư một cách nghiêm trọng.