TỈNH ỦY THANH HÓA * Số 24 -CTr/TU	ĐẢNG CỘNG SẢN VIỆT NAM *Thanh Hóa, ngày 06 tháng 5 năm 2026*

CHƯƠNG TRÌNH HÀNH ĐỘNG
thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị

Thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư "về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị" *(sau đây viết tắt là Chỉ thị số 57-CT/TW)*, Ban Thường vụ Tỉnh ủy ban hành Chương trình hành động thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Quán triệt, triển khai thực hiện nghiêm túc, hiệu quả Chỉ thị số 57-CT/TW của Ban Bí thư, bảo đảm toàn Đảng bộ và hệ thống chính trị trong tỉnh nhận thức đầy đủ, sâu sắc về vị trí, vai trò, tầm quan trọng của công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

2. Cụ thể hóa đầy đủ các nhiệm vụ và giải pháp nêu trong Chỉ thị số 57-CT/TW của Ban Bí thư, các văn bản lãnh đạo, chỉ đạo của Trung ương, của Tỉnh về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo đảm phù hợp với nhiệm vụ chính trị và tình hình thực tế của tỉnh.

3. Việc tổ chức triển khai thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư phải nghiêm túc, hiệu quả, đồng bộ từ tỉnh đến cơ sở, gắn với thực hiện các nghị quyết, chỉ thị, kết luận của Trung ương, của tỉnh về chuyển đổi số, phát triển chính quyền số, cải cách hành chính, bảo vệ bí mật nhà nước, đấu tranh phòng, chống tội phạm và vi phạm pháp luật trên không gian mạng. Chủ động phòng ngừa từ sớm, từ xa, phát hiện và xử lý hiệu quả các nguy cơ, sự cố an ninh mạng; ưu tiên bảo vệ các hệ thống thông tin, dữ liệu quan trọng và bí mật nhà nước, đặc biệt là các hệ thống thông tin phục vụ công tác lãnh đạo, chỉ đạo, điều hành của cấp ủy, chính quyền các cấp.

4. Xác định rõ mục tiêu, nhiệm vụ và giải pháp, bảo đảm khả thi, hiệu quả, có trọng tâm, trọng điểm, lộ trình thực hiện rõ ràng; phân công trách nhiệm cụ thể cho các cấp, các ngành, cơ quan, đơn vị trong lãnh đạo, chỉ đạo, tổ chức thực hiện. Phát huy hiệu quả quản lý nhà nước, vai trò nòng cốt của lực lượng công an, quân đội, cơ yếu; đề cao trách nhiệm người đứng đầu trong tổ chức thực hiện.

5. Huy động, sử dụng hiệu quả các nguồn lực nhà nước và xã hội cho công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; tăng cường kiểm tra, giám sát, xử lý nghiêm các vi phạm; định kỳ sơ kết, tổng kết, báo cáo kết quả thực hiện theo đúng quy định.

II. MỤC TIÊU

1. Mục tiêu tổng quát

- Đảm bảo hoạt động của các cơ quan, đơn vị trong hệ thống chính trị của tỉnh an toàn, vững chắc trên không gian mạng; bảo vệ bí mật nhà nước, bí mật công tác, bí mật nội bộ theo quy định; bảo đảm an ninh mạng đối với hệ thống thông tin và dữ liệu phục vụ công tác lãnh đạo, chỉ đạo, điều hành phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh, đối ngoại, xây dựng Đảng và hệ thống chính trị trên địa bàn tỉnh.

- Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại mọi âm mưu, hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên địa bàn tỉnh.

- Xây dựng và vận hành hiệu quả kiến trúc bảo vệ an ninh mạng đa lớp, hiện đại, đồng bộ với các hệ thống thông tin của tỉnh, gắn kết chặt chẽ với kiến trúc bảo vệ an ninh mạng quốc gia và quy hoạch hạ tầng số.

2. Mục tiêu cụ thể đến năm 2030

- 100% cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc, các tổ chức chính trị - xã hội cấp tỉnh, cấp xã ban hành, thực hiện nghiêm quy chế nội bộ về bảo đảm an ninh mạng, bảo mật thông tin và bảo vệ bí mật nhà nước.

- 100% hệ thống thông tin quan trọng của tỉnh (hệ thống dùng chung, cơ sở dữ liệu chuyên ngành, trung tâm điều hành thông minh, các hệ thống phục vụ chỉ đạo, điều hành của Tỉnh ủy, HĐND, UBND, Ủy ban MTTQ Việt Nam tỉnh) được phân loại, phê duyệt cấp độ an ninh mạng; xây dựng phương án bảo đảm an ninh mạng; tổ chức giám sát, kiểm tra, đánh giá, diễn tập định kỳ theo quy định.

- Hằng năm, 100% cán bộ phụ trách công tác chuyển đổi số, công nghệ thông tin, an ninh mạng cấp tỉnh, cấp xã được bồi dưỡng, cập nhật kiến thức, kỹ năng chuyên môn, nghiệp vụ. Phấn đấu đến năm 2030, 100% cán bộ quản trị, vận hành hệ thống thông tin cốt lõi cấp tỉnh có chứng chỉ/chuyên môn sâu về an ninh mạng.

- Xây dựng Trung tâm an ninh mạng của tỉnh gắn với Trung tâm giám sát, điều hành thông minh (IOC); thiết lập cơ chế chia sẻ thông tin, cảnh báo, phối hợp xử lý sự cố đối với các hệ thống thông tin, các nền tảng điều hành an ninh mạng quốc gia theo quy định.

- Ngăn chặn hiệu quả các cuộc tấn công mạng, xâm nhập trái phép; phòng ngừa lộ, lọt bí mật nhà nước trên không gian mạng và dữ liệu nội bộ của các cơ quan, tổ chức trong hệ thống chính trị trên địa bàn tỉnh; kiên quyết không để xảy ra sự cố an ninh mạng nghiêm trọng do nguyên nhân chủ quan trong công tác quản lý, vận hành, sử dụng hệ thống thông tin.

III. NHIỆM VỤ VÀ GIẢI PHÁP

1. Tăng cường sự lãnh đạo của cấp ủy Đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Các cấp ủy đảng, chính quyền, Mặt trận Tổ quốc và các tổ chức chính trị-xã hội đẩy mạnh nghiên cứu, học tập, quán triệt đầy đủ, sâu sắc trong hệ thống chính trị và toàn xã hội về Chỉ thị số 57-CT/TW và Chương trình hành động này. Quán triệt sâu sắc quan điểm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách; là trách nhiệm của cả hệ thống chính trị và toàn dân, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước. Lực lượng Công an nhân dân, Quân đội nhân dân đóng vai trò chủ chốt. Huy động sức mạnh tổng hợp của toàn dân, xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng.

- Quán triệt phương châm "Tự chủ, tự lực, tự cường" trong xây dựng tiềm lực an ninh mạng. Tập trung phát triển, khai thác, sử dụng hệ sinh thái sản phẩm, dịch vụ an ninh mạng Việt Nam, ưu tiên làm chủ công nghệ lõi, giải pháp bảo mật tiên tiến, ứng dụng mạnh mẽ trí tuệ nhân tạo, công nghệ mới vào lĩnh vực an ninh mạng, coi đây là những nhiệm vụ chiến lược để bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Áp dụng cơ chế đột phá, đặc thù, ưu đãi trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo để phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng, an ninh dữ liệu.

- Bảo đảm an ninh mạng, an ninh dữ liệu là yếu tố nền tảng, yêu cầu bắt buộc ngay từ khâu quy hoạch, thiết kế, xây dựng, vận hành hệ thống thông tin. Hệ thống chưa bảo đảm an ninh mạng thì kiên quyết không đưa vào sử dụng. Thường xuyên rà soát, kiểm tra, đánh giá an toàn thông tin, an ninh mạng đối với các hệ thống công nghệ thông tin. Việc thu thập, quản lý, khai thác dữ liệu số phải được bảo vệ ở mức cao nhất; tuyệt đối không để lộ, lọt bí mật nhà nước, dữ liệu nhạy cảm, kể cả trong quá trình thử nghiệm.

- Chuyển dịch tư duy chiến lược từ "Phòng bị chủ động" sang "Phòng thủ chủ động", "Phòng thủ tích cực", xây dựng "Thế trận an ninh mạng chủ động, toàn diện"; những nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu phải được nhận diện và xử lý từ sớm, từ xa, sẵn sàng có các biện pháp phòng vệ tương xứng để răn đe, vô hiệu hóa các nguy cơ, bảo vệ lợi ích quốc gia, dân tộc.

- Đưa nội dung an ninh mạng, bảo mật thông tin, an ninh dữ liệu vào chương trình đào tạo, bồi dưỡng, cập nhật kiến thức cho cán bộ diện Ban Thường vụ Tỉnh ủy quản lý; chương trình đào tạo, bồi dưỡng tại Trường Chính trị tỉnh và các cơ sở bồi dưỡng lý luận chính trị. Biên soạn, phát hành tài liệu tuyên truyền

về an ninh mạng, an ninh dữ liệu, phòng chống tội phạm, vi phạm pháp luật trên không gian mạng để sử dụng trong sinh hoạt chi bộ, sinh hoạt cơ quan, đoàn thể và các hoạt động tuyên truyền pháp luật ở cơ sở.

- Người đứng đầu cấp uỷ đảng, chính quyền, cơ quan, đơn vị chịu trách nhiệm trực tiếp, toàn diện về công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước tại địa phương, đơn vị mình. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động hằng năm. Thường xuyên lãnh đạo, chỉ đạo, kiểm tra, giám sát, tăng cường phối hợp giữa các cơ quan, đơn vị trong tổ chức triển khai thực hiện; kịp thời biểu dương, khen thưởng tập thể, cá nhân điển hình, có thành tích xuất sắc.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng; đẩy mạnh tuyên truyền trên các phương tiện thông tin đại chúng, mạng xã hội, nền tảng số, cổng/trang thông tin điện tử của các sở, ban, ngành, địa phương và hệ thống thông tin cơ sở. Nội dung tuyên truyền tập trung vào việc thực hiện Chỉ thị số 57-CT/TW, kết hợp chặt chẽ giữa tuyên truyền bảo đảm an ninh mạng với chuyển đổi số, phòng chống tội phạm công nghệ cao và phổ cập kỹ năng số an toàn cho người dân.

2. Hoàn thiện cơ chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước

- Rà soát, sửa đổi, bổ sung, ban hành các quy chế, quy định nội bộ về quản lý, vận hành, khai thác hệ thống thông tin; quản lý, sử dụng thiết bị, bảo mật tài khoản đăng nhập các phần mềm, ứng dụng, thư điện tử công vụ; sử dụng mạng xã hội, thiết bị cá nhân trong thực hiện nhiệm vụ công; phân loại, lưu trữ, chia sẻ, hủy dữ liệu, bảo đảm phù hợp với quy định pháp luật hiện hành.

- Rà soát, sửa đổi, bổ sung các quy định về bảo vệ bí mật nhà nước trong điều kiện chuyển đổi số, sử dụng môi trường mạng; quản lý, khai thác, sử dụng hệ thống hội nghị trực tuyến, hệ thống làm việc trên môi trường điện tử, bảo đảm an toàn, bảo mật theo quy định. Chủ động rà soát công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu thuộc phạm vi quản lý; xác định lỗ hổng, nguy cơ và xây dựng kế hoạch khắc phục triệt để, định kỳ báo cáo cơ quan chức năng theo quy định.

- Tăng cường công tác quản lý nhà nước đối với hoạt động ứng dụng công nghệ thông tin, chuyển đổi số, an ninh mạng, an ninh dữ liệu và bảo vệ dữ liệu cá nhân. Thường xuyên kiểm tra, đánh giá việc triển khai thực hiện đối với các cơ quan, địa phương, đơn vị có hệ thống thông tin, dữ liệu quan trọng.

- Lồng ghép nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu vào các chương trình, kế hoạch, đề án, dự án công nghệ thông tin, chuyển

đổi số; tích hợp các mục tiêu, chỉ tiêu, nhiệm vụ về an ninh mạng, an ninh dữ liệu vào chương trình, kế hoạch chuyển đổi số của tỉnh, bảo đảm đồng bộ với Chiến lược chuyển đổi số quốc gia.

- Triển khai thực hiện hiệu quả nhiệm vụ định danh, xác thực không gian mạng; rà soát, xử lý triệt để SIM rác, tài khoản ảo, nặc danh; thực hiện xác thực danh tính bắt buộc đối với người dùng mạng xã hội theo hướng dẫn của Trung ương; tăng cường kiểm soát độ tuổi, bảo vệ trẻ em trên không gian mạng.

3. Hoàn thiện hạ tầng kỹ thuật, xây dựng kiến trúc bảo vệ an ninh mạng đa lớp, hiện đại, đáp ứng yêu cầu bảo đảm an ninh mạng, an ninh dữ liệu

- Phát triển hạ tầng số, hạ tầng dữ liệu bảo đảm hiện đại, đồng bộ, an toàn. Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số phải có cấu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng. Tích hợp đầy đủ yêu cầu về an ninh mạng trong toàn bộ quá trình thiết kế, thẩm định, thi công và triển khai Kiến trúc Chính quyền số tỉnh Thanh Hóa và các hệ thống cơ sở dữ liệu của địa phương, bảo đảm liên thông an toàn, an ninh thông tin với Khung kiến trúc tổng thể quốc gia số.

- Tổ chức đánh giá, phân loại, phê duyệt cấp độ an ninh mạng cho các hệ thống thông tin theo quy định; xây dựng và triển khai phương án bảo đảm an ninh mạng phù hợp với từng cấp độ và mô hình an toàn thông tin 4 lớp theo hướng dẫn của các cơ quan Trung ương. Định kỳ tổ chức diễn tập về an ninh mạng; xây dựng, cập nhật kịch bản, phương án ứng phó, khắc phục sự cố an ninh mạng cấp tỉnh và tại từng cơ quan, đơn vị.

- Xây dựng, hoàn thiện, đưa vào vận hành hiệu quả Trung tâm an ninh mạng của tỉnh, gắn với Trung tâm giám sát, điều hành thông minh (IOC); kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng với Trung tâm An ninh mạng quốc gia và Hệ thống phòng vệ mạng quốc gia theo hướng dẫn của Bộ Công an và các bộ, ngành Trung ương, bảo đảm giám sát, cảnh báo sớm, ngăn chặn, ứng phó, khắc phục kịp thời các sự cố an ninh mạng.

- Đầu tư, nâng cấp hạ tầng kỹ thuật công nghệ thông tin, hạ tầng số, ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Make in Vietnam"; triển khai các giải pháp sao lưu, phục hồi dữ liệu, phân vùng mạng, phân quyền truy cập, mã hóa dữ liệu phù hợp.

- Ưu tiên bố trí ngân sách nhà nước hằng năm cho các nhiệm vụ, dự án bảo đảm an ninh mạng, an ninh dữ liệu; bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, giải pháp, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số. Khuyến khích xã hội hóa, huy động các nguồn lực hợp pháp tham gia cung cấp dịch vụ an ninh mạng cho cơ quan nhà nước, đơn vị sự nghiệp công lập.

4. Kiện toàn tổ chức bộ máy, phát huy lực lượng nòng cốt và phát triển nguồn nhân lực

- Thường xuyên rà soát, kiện toàn Tiểu ban An ninh mạng tỉnh Thanh Hóa; phân công rõ đầu mối tham mưu, giúp việc cấp ủy, chính quyền về công tác an ninh mạng. Kiện toàn Đội ứng cứu sự cố an ninh mạng của tỉnh, Tổ ứng cứu sự cố an ninh mạng ở các cơ quan, đơn vị, địa phương do người đứng đầu trực tiếp phụ trách. Bố trí cán bộ, bộ phận phụ trách an ninh mạng các cấp đáp ứng yêu cầu nhiệm vụ; tăng cường công tác phối hợp, thiết lập kênh kết nối trao đổi thông tin thống nhất về dữ liệu phục vụ giám sát, công tác điều phối ứng cứu, khắc phục sự cố an ninh mạng với lực lượng chuyên trách bảo vệ an ninh mạng của tỉnh.

Phát huy vai trò nòng cốt của lực lượng vũ trang nhân dân và lực lượng cơ yếu trong tham mưu, hướng dẫn, kiểm tra, đôn đốc bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu. Xây dựng, thực hiện nghiêm quy chế phối hợp giữa các cơ quan chức năng với các doanh nghiệp công nghệ thông tin, viễn thông để chia sẻ thông tin, cảnh báo, ứng cứu sự cố, điều tra và xử lý các hành vi vi phạm pháp luật trên không gian mạng.

- Phát triển nguồn nhân lực an ninh mạng chất lượng cao; nghiên cứu ban hành cơ chế, chính sách thu hút, đãi ngộ chuyên gia giỏi tham gia phục vụ công tác an ninh mạng trên địa bàn tỉnh. Tổ chức đào tạo, bồi dưỡng, huấn luyện thực chiến thường xuyên cho đội ngũ cán bộ chuyên trách, kiêm nhiệm về công nghệ thông tin và quản trị mạng. Tổ chức tập huấn, bồi dưỡng kiến thức, kỹ năng bảo đảm an ninh thông tin cho đội ngũ cán bộ lãnh đạo, quản lý, cán bộ làm công tác báo chí, truyền thông và báo cáo viên các cấp. Phát huy hiệu quả mô hình hợp tác *"3 nhà": Nhà nước - Nhà trường - Doanh nghiệp* trong đào tạo nguồn nhân lực; xây dựng mạng lưới chuyên gia an ninh mạng của tỉnh để sẵn sàng huy động tham gia ứng phó, khắc phục sự cố và các tình huống khẩn cấp về an ninh mạng.

5. Tăng cường hợp tác trong nước và quốc tế trên lĩnh vực an ninh mạng

- Đẩy mạnh hợp tác, liên kết với các ban, bộ, ngành Trung ương, các viện nghiên cứu, trường đại học, Hiệp hội An ninh mạng quốc gia và các tập đoàn công nghệ, viễn thông lớn trên lĩnh vực an ninh mạng. Trọng tâm là hợp tác nghiên cứu, chuyển giao công nghệ, tư vấn giải pháp, đào tạo nguồn nhân lực chất lượng cao và phát triển hệ sinh thái đổi mới sáng tạo, chuyển đổi số an toàn trên địa bàn tỉnh.

- Tích cực tham gia các hoạt động hợp tác quốc tế về an ninh mạng theo chỉ đạo, hướng dẫn của Trung ương. Tăng cường phối hợp chặt chẽ với các địa phương của nước Cộng hòa dân chủ nhân dân Lào có chung đường biên giới với tỉnh trong việc trao đổi thông tin, phòng ngừa, ngăn chặn và đấu tranh hiệu quả với tội phạm mạng, tội phạm sử dụng công nghệ cao xuyên quốc gia.

- Tạo điều kiện thuận lợi thu hút các đối tác, doanh nghiệp nước ngoài có năng lực, uy tín đầu tư vào lĩnh vực công nghệ số, linh kiện điện tử, hạ tầng dữ liệu tại các khu kinh tế, khu công nghiệp của tỉnh, gắn với yêu cầu bảo đảm tuyệt đối an ninh quốc gia, chủ quyền quốc gia trên không gian mạng.

IV. TỔ CHỨC THỰC HIỆN

1. Ban Thường vụ Đảng ủy UBND tỉnh lãnh đạo UBND tỉnh xây dựng chương trình, kế hoạch, đề án và bố trí nguồn lực để triển khai thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư và Chương trình này; phân công trách nhiệm cụ thể cho các sở, ngành, đơn vị cấp tỉnh, UBND các xã, phường; thường xuyên kiểm tra, giám sát, đôn đốc việc tổ chức triển khai thực hiện.

2. Các ban, sở, ngành, MTTQ, cơ quan, đơn vị cấp tỉnh, Đảng ủy các xã, phường, các đảng ủy trực thuộc Tỉnh ủy căn cứ Chương trình này và tình hình thực tế của cơ quan, đơn vị, xây dựng kế hoạch thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư và tập trung lãnh đạo, chỉ đạo thực hiện nghiêm túc, hiệu quả, bảo đảm hoàn thành nhiệm vụ được giao; chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy về kết quả công tác bảo đảm an ninh mạng tại địa phương, cơ quan, đơn vị mình; định kỳ báo cáo Ban Thường vụ Tỉnh ủy (qua Đảng ủy Công an tỉnh) kết quả thực hiện.

3. Giao Đảng ủy Công an tỉnh chủ trì, phối hợp với các đơn vị liên quan theo dõi, kiểm tra, đôn đốc việc thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư và Chương trình này; định kỳ báo cáo Ban Thường vụ Tỉnh ủy kết quả thực hiện.

Chương trình này được phổ biến đến các Chi bộ./.

T/M BAN THƯỜNG VỤ
BÍ THƯ

TỈNH ỦY THANH HÓA

Lê Đức Thái

Nơi nhận:
- Ban Bí thư Trung ương Đảng (b/c),
- BCĐ Trung ương về phát triển KHCN, ĐMST và chuyển đổi số (b/c),
- Văn phòng Trung ương Đảng (b/c),
- Đảng ủy Công an Trung ương,
- Các đồng chí Tỉnh ủy viên,
- Các ban, UBKT, Văn phòng Tỉnh ủy,
- Đảng ủy các xã, phường; các đảng ủy trực thuộc,
- Các sở, ngành, MTTQ, đoàn thể, đơn vị cấp tỉnh,
- Lưu Văn phòng Tỉnh ủy.