

Số: /KH-UBND

Thanh Hoá, ngày tháng năm 2026

KẾ HOẠCH

Kiểm tra, đánh giá công tác đảm bảo an ninh mạng, an toàn thông tin và hỗ trợ ứng cứu sự cố an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn tỉnh Thanh Hóa năm 2026

Thực hiện 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; 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; Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị; Thông báo kết luận số 06-TB/CQTTBCĐ ngày 27/9/2025 của Cơ quan Thường trực Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu, Chủ tịch UBND tỉnh ban hành Kế hoạch kiểm tra, đánh giá công tác đảm bảo an ninh mạng, an toàn thông tin và hỗ trợ ứng cứu sự cố an toàn thông tin trên địa bàn tỉnh Thanh Hóa năm 2026 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Tổ chức kiểm tra, đánh giá thực trạng công tác bảo đảm an toàn, an ninh mạng tại các cơ quan, đơn vị, địa phương nhằm phát hiện hạn chế, sơ hở, thiếu sót, lỗ hổng bảo mật và tình trạng mất an toàn, an ninh mạng để kịp thời khắc phục.
2. Phòng ngừa, phát hiện sớm và xử lý kịp thời các sự cố an toàn thông tin mạng; tổ chức điều tra, truy vết nguồn gốc, nguyên nhân của sự cố nhằm ngăn chặn, khắc phục triệt để và hạn chế tối đa thiệt hại, không để sự cố lan rộng hoặc tái diễn.
3. Nâng cao vai trò, trách nhiệm của chủ quản hệ thống thông tin, người đứng đầu tổ chức, bộ phận chuyên trách trong công tác đảm bảo an ninh mạng, an toàn thông tin.
4. Tổng hợp kết quả kiểm tra, đánh giá, kiến nghị, giải quyết các vướng mắc của cơ quan, đơn vị và báo cáo Chính phủ, Tỉnh ủy chỉ đạo.
5. Quá trình triển khai thực hiện đảm bảo đúng quy định của pháp luật, đúng quy trình nghiệp vụ, đảm bảo tính khách quan, chính xác.

II. THỜI GIAN, ĐỐI TƯỢNG, NỘI DUNG, HÌNH THỨC KIỂM TRA

1. Thời gian

- Thời gian: Từ ngày ban hành kế hoạch đến hết ngày 31/12/2026.
- Dự kiến thời gian kiểm tra thực tế: 01 ngày làm việc/đơn vị.

2. Đối tượng kiểm tra

Các sở, ban, ngành, đơn vị cấp tỉnh; UBND cấp xã và các đơn vị trực thuộc (sau đây gọi tắt là các cơ quan, đơn vị).

3. Nội dung kiểm tra

- Việc phổ biến, quán triệt, tổ chức triển khai thực hiện chủ trương của Đảng, pháp luật Nhà nước, chỉ đạo của Tỉnh uỷ, UBND tỉnh và hướng dẫn của Công an tỉnh về bảo đảm an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước trên không gian mạng.

- Công tác tuyên truyền, nâng cao nhận thức về an ninh mạng, an toàn thông tin; phân công cán bộ thực hiện nhiệm vụ bảo đảm an ninh mạng, an toàn thông tin.

- Công tác bảo đảm an toàn thông tin theo cấp độ: Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; đánh giá hiệu quả các biện pháp bảo đảm an toàn hệ thống thông tin.

- Việc thực hiện các biện pháp bảo đảm an ninh thông tin đối với các thiết bị soạn thảo, lưu trữ bí mật nhà nước, các thiết bị kết nối hệ thống thông tin giải quyết thủ tục hành chính.

- Công tác bảo mật, xác thực: Kiểm tra việc quản trị, quản lý tài khoản xác thực các hệ thống phần mềm, ứng dụng dùng chung phục vụ công tác; quản lý, sử dụng thiết bị ký số, USB token, USB cơ yếu, USB an toàn.

- Hỗ trợ, hướng dẫn nghiệp vụ ứng cứu sự cố an toàn thông tin mạng, kiểm thử, rà quét mã độc, điểm yếu, lỗ hổng của hệ thống, thử nghiệm tấn công xâm nhập đối với các thiết bị trong hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống.

4. Hình thức kiểm tra

- Các đơn vị tự kiểm tra, báo cáo kết quả công tác đảm bảo an ninh mạng, an toàn thông tin về UBND tỉnh (qua Công an tỉnh - Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao).

- Thành lập Đoàn kiểm tra tiến hành kiểm tra thực tế tại các cơ quan, đơn vị (Lịch kiểm tra thực tế theo Phụ lục I kèm theo Kế hoạch).

III. KINH PHÍ THỰC HIỆN

Nguồn ngân sách của tỉnh cấp cho thực hiện nhiệm vụ ứng cứu sự cố, bảo đảm an toàn thông tin mạng và các nguồn tài chính hợp pháp khác.

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Chủ trì tổ chức triển khai thực hiện kế hoạch này, thành lập Đoàn kiểm tra và thông báo đến các đơn vị được kiểm tra theo lịch.

- Tiến hành kiểm tra, đánh giá thực tế công tác bảo đảm an ninh mạng, an toàn thông tin; hỗ trợ ứng cứu sự cố an toàn thông tin đối với các cơ quan, đơn vị; đảm bảo các điều kiện cần thiết về phương tiện, công cụ, trang thiết bị phục vụ công tác kiểm tra, ứng cứu sự cố.

- Tổng hợp kết quả kiểm tra, đánh giá, kiến nghị, giải quyết các khó khăn, vướng mắc của các cơ quan, đơn vị; xử lý theo thẩm quyền hoặc kiến nghị xử lý các tổ chức, cá nhân vi phạm và báo cáo UBND tỉnh chỉ đạo.

2. Các cơ quan, đơn vị

- Các cơ quan, đơn vị chưa có lịch kiểm tra thực tế: Tự kiểm tra các nội dung theo Kế hoạch và báo cáo về UBND tỉnh (qua Công an tỉnh - Phòng An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao) trước ngày **31/5/2026** (có Đề cương báo cáo tại phụ lục II kèm theo kế hoạch).

- Các cơ quan, đơn vị được lựa chọn kiểm tra thực tế: Chuẩn bị đầy đủ nội dung, điều kiện làm việc, phân công lãnh đạo, đại diện các phòng, ban, đơn vị trực thuộc và cán bộ phụ trách để làm việc với Đoàn kiểm tra theo lịch. Khi có sự thay đổi về lịch hoặc thời gian làm việc của cơ quan, đơn vị cần thông báo cho Đoàn kiểm tra.

Đề nghị các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm túc¹. Quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, đơn vị trao đổi về Công an tỉnh (qua đồng chí Trung tá Nguyễn Văn Hà, Phòng An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao; số điện thoại: 0913.809.636) để phối hợp, hướng dẫn./.

Nơi nhận:

- Chủ tịch UBND tỉnh (để b/c);
- Các Phó Chủ tịch UBND tỉnh;
- Các sở, ban, ngành, đơn vị cấp tỉnh;
- Công an tỉnh;
- CVP, các PCVP UBND tỉnh;
- UBND các xã, phường.
- Lưu: VT, CNXDKH, TDNC.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Cao Văn Cường

¹ Đồng thời thông báo đến các đơn vị trực thuộc để triển khai các nội dung kế hoạch kiểm tra.

**PHỤ LỤC I: DỰ KIẾN LỊCH KIỂM TRA THỰC TẾ CÔNG TÁC
BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN**

*(Ban hành kèm theo Kế hoạch số /KH-UBND ngày / /2026
của UBND tỉnh)*

TT	Tên đơn vị	Thời gian kiểm tra	Ghi chú
1	UBND xã Đồng Lương	22/6/2026	
2	UBND xã Thường Xuân	23/6/2026	
3	Bệnh viện Nội tiết	24/6/2026	
4	Bệnh viện đa khoa tỉnh	25/6/2026	
5	Bệnh viện Phụ sản	26/6/2026	
6	UBND phường Đông Sơn	06/7/2026	
7	UBND xã Kiên Thọ	07/7/2026	
8	UBND xã Thiệu Hoá	08/7/2026	
9	UBND xã Thiệu Toán	09/7/2026	
10	Trường Cao đẳng Y Thanh Hoá	10/7/2026	
11	Bệnh viện đa khoa Hạc Thành	13/7/2026	
12	UBND phường Trúc Lâm	14/7/2026	
13	UBND phường Nam Sầm Sơn	15/7/2026	
14	UBND xã Ngọc Lặc	16/7/2026	
15	UBND xã Mường Lát	17/7/2026	
16	UBND xã Trung Lý	20/7/2026	
17	UBND xã Thiên Phú	21/7/2026	
18	UBND xã Hồi Xuân	22/7/2026	

19	UBND xã Thiết Ống	23/7/2026	
20	UBND xã Bá Thước	24/7/2026	
21	UBND xã Hoa Lộc	03/8/2026	
22	UBND xã Nông Cống	04/8/2026	
23	UBND xã Thọ Phú	05/8/2026	
24	UBND xã Thăng Bình	06/8/2026	
25	UBND xã Như Xuân	07/8/2026	
26	UBND xã Nga Sơn	10/8/2026	
27	UBND xã Định Hoà	11/8/2026	
28	UBND phường Hải Lĩnh	12/8/2026	
29	UBND xã Hà Long	24/8/2026	
30	UBND xã Lĩnh Toại	25/8/2026	
31	UBND xã Xuân Hoà	26/8/2026	
32	UBND xã Hoàng Giang	07/9/2026	
33	UBND phường Nguyệt Viên	08/9/2026	
34	UBND xã Thạch Bình	09/9/2026	
35	Bệnh viện đa khoa Thạch Thành	10/9/2026	
36	UBND xã Tam Lư	11/9/2026	
37	Bệnh viên đa khoa Quan Sơn	14/9/2026	
38	UBND xã Na Mèo	15/9/2026	
39	UBND xã Tây Đô	16/9/2026	
40	UBND xã Cẩm Thủy	17/9/2026	
41	UBND xã Tân Ninh	18/9/2026	

42	UBND phường Quang Trung	05/10/2026	
43	UBND xã Yên Ninh	06/10/2026	
44	UBND xã An Nông	07/10/2026	
45	UBND xã Trường Lâm	08/10/2026	
46	UBND xã Ba Đình	09/10/2026	
47	UBND xã Hậu Lộc	12/10/2026	
48	UBND xã Yên Phú	13/10/2026	
49	UBND xã Pù Luông	14/10/2026	
50	UBND xã Yên Thọ	15/10/2026	
51	UBND xã Cẩm Tú	16/10/2026	
52	UBND xã Hoá Quý	19/10/2026	
53	Sở Công Thương	20/10/2026	
54	Sở Tài chính	21/10/2026	
55	Thanh tra tỉnh	22/10/2026	
56	Sở Nội vụ	23/10/2026	
57	Sở Ngoại vụ	26/10/2026	
58	Sở Y tế	27/10/2026	
59	Văn phòng UBND tỉnh	28/10/2026	
60	Ban Quản lý Khu kinh tế Nghi Sơn và khu công nghiệp tỉnh	29/10/2026	

**PHỤ LỤC II: ĐỀ CƯƠNG BÁO CÁO CÔNG TÁC KIỂM TRA
AN TOÀN, AN NINH THÔNG TIN VÀ BẢO MẬT**
(Ban hành kèm theo Kế hoạch số /KH-UBND ngày / /2026
của UBND tỉnh)

I. THÔNG TIN CHUNG

- Tên cơ quan, đơn vị.
- Đầu mối liên hệ.
- Danh sách các hệ thống thông tin của đơn vị quản lý (hoặc thuê dịch vụ).
- Danh sách các ứng dụng, phần mềm đang sử dụng tại đơn vị (*Hệ thống quản lý văn bản, hồ sơ công việc; Hệ thống thông tin giải quyết thủ tục hành chính; Hệ thống thông tin quản lý các hoạt động du lịch; Hệ thống mail công vụ; Trang thông tin điện tử...*)
- Danh sách tài khoản ứng dụng, trang thiết bị cấp cho Lãnh đạo, cán bộ, công chức, viên chức đơn vị (*Phụ lục III gửi kèm kế hoạch*).

Lưu ý: Các sở, ngành, đơn vị cấp xã, đơn vị trực thuộc (có hệ thống thông tin riêng) triển khai thực hiện các nội dung theo kế hoạch.

II. CÁC TÀI LIỆU LIÊN QUAN

- Các văn bản, tài liệu liên quan đến công tác đảm bảo an ninh, an toàn thông tin của đơn vị.
- Các văn bản, tài liệu liên quan đến công tác quản lý, vận hành, khai thác sử dụng Hệ thống thông tin.
- Quy định, quy chế về quản lý sử dụng chữ ký số, USB token, USB cơ yếu, USB an toàn.

III. NỘI DUNG BÁO CÁO

1. Công tác phổ biến, quán triệt triển khai thực hiện các văn bản, chỉ đạo hướng dẫn trong đảm bảo an toàn, an ninh mạng.
 - Chủ trương của Đảng, pháp luật Nhà nước, nghị quyết, chỉ thị của Trung ương, Tỉnh ủy, UBND tỉnh về bảo đảm an ninh mạng, an toàn thông tin ².

² Luật An ninh mạng; Luật An toàn thông tin mạng; Luật Bảo vệ bí mật nhà nước; Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ quy định về bảo vệ dữ liệu cá nhân; Chỉ thị số 01/CT-TTg ngày 18/02/2021 của Thủ tướng Chính phủ và Chỉ thị số 16/CT-UBND ngày 12/7/2021 của Chủ tịch UBND tỉnh về tăng cường công tác bảo đảm an ninh mạng trong tình hình hiện nay; Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; Công văn số 13228/UBND-KSTTHCNC ngày 10/9/2024 của Chủ tịch UBND tỉnh về bảo đảm an ninh mạng phòng ngừa lừa đảo, mất thông tin, dữ liệu nội bộ, dữ liệu cá nhân trên môi trường mạng; Công văn số 14748/UBND-KSTTHCNC ngày 03/10/2023 của Chủ tịch UBND tỉnh về tăng cường bảo vệ dữ liệu cá nhân trên địa bàn Thanh Hóa theo Nghị định số 13/2023/NĐ-CP ngày 14/7/2023; Thông báo kết luận số 06-TB/CQTTBCĐ ngày 27/9/2025 của Cơ quan Thường trực Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng

- Các văn bản khác liên quan về an ninh mạng, an toàn thông tin.

2. Việc bố trí nguồn nhân lực, tuyên truyền bảo đảm an toàn, an ninh mạng và bảo mật.

- Nhân lực bảo đảm an toàn, an ninh mạng, an toàn thông tin (tổ chức bộ máy và phân công nhiệm vụ; số lượng và trình độ cán bộ chuyên trách; công tác tham gia đào tạo, tập huấn; cơ chế, chính sách với bộ phận chuyên trách...).

- Nhận thức về an ninh mạng, an toàn thông tin của cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị (mức độ hiểu biết, kỹ năng, kiến thức về an ninh mạng, an toàn thông tin; việc tuân thủ các quy định và quy trình bảo mật; công tác tổ chức tuyên truyền, phổ biến kiến thức...).

3. Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ

a) Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ

- Việc tuân thủ trách nhiệm của đơn vị vận hành: Xây dựng hồ sơ cấp độ, phương án ứng cứu sự cố an toàn thông tin, kế hoạch tập huấn, tuyên truyền, kiện toàn tổ ứng cứu sự cố; việc báo cáo định kỳ (báo cáo năm công tác bảo đảm an toàn thông tin trước 15/9 hằng năm), đột xuất theo yêu cầu của cơ quan chuyên trách, chủ quản hệ thống thông tin...

- Việc tổ chức thực thi các biện pháp bảo đảm an toàn hệ thống thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt: trang bị thiết bị tường lửa, bộ chuyển mạch trung tâm và dự phòng; số lượng thiết bị được cài đặt phần mềm phòng, chống mã độc (%).

- Việc tổ chức triển khai phương án ứng phó, khắc phục sự cố an ninh mạng: xây dựng và ban hành phương án, tổ chức lực lượng, phân công nhiệm vụ, triển khai thực hiện...

b) Kiểm tra, đánh giá hiệu quả các biện pháp bảo đảm an toàn hệ thống thông tin

tạo và chuyển đổi số về công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu; Kế hoạch số 266-KH/TU ngày 26/4/2024 của Ban Thường vụ Tỉnh ủy về thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị và Nghị quyết số 71/NQ-CP ngày 01/4/2025 của Chính phủ; Kế hoạch số 285-KH/TU ngày 27/6/2025 của Ban Thường vụ Tỉnh ủy về thực hiện Kế hoạch số 02-KH/BCĐTW ngày 19/6/2025 của Ban Chỉ đạo Trung ương về thúc đẩy chuyển đổi số liên thông, đồng bộ, nhanh, hiệu quả đáp ứng yêu cầu sắp xếp tổ chức bộ máy của hệ thống chính trị trên địa bàn tỉnh Thanh Hóa; Công văn số 9572/UBND-CNXXDKH ngày 23/6/2025 của Chủ tịch UBND tỉnh chỉ đạo yêu cầu tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; Công văn số 2451/CAT-ANCTNB ngày 04/7/2025 của Công an tỉnh về tăng cường đảm bảo an ninh mạng, an toàn thông tin, bảo vệ BMNN, bảo vệ dữ liệu cá nhân; Công văn số 4264/CAT-ANM&PCTPSCNC ngày 28/10/2025 về bảo đảm an toàn thông tin trong quá trình chuyển đổi số, số hoá hồ sơ, kết nối các cơ sở dữ liệu bộ, ngành và triển khai thực hiện Nghị quyết số 57, Kế hoạch số 02...

- Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt: Định kỳ 3 năm phải đánh giá lại tính phù hợp của Quy chế.

- Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin.

- Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt: Cấu hình phân tách các vùng mạng.

- Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt: Thiết lập ghi nhật ký, đồng bộ thời gian, kiểm soát truy cập đối với tường lửa, máy chủ, ứng dụng, cơ sở dữ liệu...

- Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống: Quy hoạch IP tĩnh gắn với cán bộ, thiết lập cấu hình bảo mật cho tường lửa, ứng dụng, cơ sở dữ liệu và các thiết bị đầu cuối (máy tính người dùng)...

- Rà soát hoạt động phần mềm phòng chống mã độc tập trung của tỉnh trên các máy trạm của cơ quan, đơn vị và hướng dẫn cho các Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, đơn vị triển khai quy trình bóc gỡ mã độc và các giải pháp phòng ngừa để tránh tình trạng tái lây nhiễm.

4. Kiểm tra công tác bảo mật, xác thực.

- Kiểm tra việc quản trị, quản lý tài khoản xác thực các hệ thống phần mềm, ứng dụng phục vụ công việc: Cấp và thu hồi các tài khoản...

- Việc quản lý sử dụng chữ ký số, USB token, USB cơ yếu, USB an toàn.

5. Các vụ việc, sự cố về an toàn, an ninh mạng, lộ, mất bí mật nhà nước trên không gian mạng đã ghi nhận, phát hiện (nếu có). Kết quả khắc phục, xử lý.

IV. NHẬN XÉT, ĐÁNH GIÁ VÀ KIẾN NGHỊ

1. Nhận xét, đánh giá

- Ưu điểm.

- Khó khăn, vướng mắc, hạn chế và nguyên nhân.

2. Kiến nghị, đề xuất

- Kiến nghị, đề xuất./.

PHỤ LỤC III: DANH SÁCH TÀI KHOẢN ỨNG DỤNG, TRANG THIẾT BỊ CẤP CHO LÃNH ĐẠO, CÁN BỘ, CÔNG CHỨC, VIÊN CHỨC ĐƠN VỊ

1. Danh sách máy tính cấp cho Lãnh đạo, Cán bộ, Công chức, Viên chức tại đơn vị

STT	HỌ TÊN	CHỨC VỤ	HỆ ĐIỀU HÀNH	ĐỊA CHỈ IP	ĐỊA CHỈ MAC	GHI CHÚ
01	Nguyễn Văn Anh	Chủ tịch	Windows 10	10.21.1.16	70-08-94-76-A1-9F	
...						

2. Danh sách các tài khoản, ứng dụng cấp cho Lãnh đạo, cán bộ, công chức, viên chức

STT	Họ tên	Chức vụ	Tài khoản mail công vụ	Tài khoản giải quyết thủ tục hành chính	 (Bổ sung thêm các phần mềm, ứng dụng đang triển khai tại đơn vị)
01	Nguyễn Văn Anh	Chủ tịch	anhnv@trieuson.gov.vn	anhnv.trieuson	...
02	Lê Văn Hoàng	Phó Chủ tịch	hoanglv@trieuson.gov.vn	Hoanglv.trieuson	...
...	...	...	...	...	...

* Hướng dẫn lấy địa chỉ IP, MAC:

- Trên Windows mở **CMD** (nhấn Windows+R, gõ cmd, Enter) và nhập lệnh **ipconfig /all**.

- Địa chỉ MAC nằm ở mục “Physical Address”, địa chỉ IP nằm ở mục “IPv4 Address” của card mạng tương ứng (đối với mạng LAN là mục “Ethernet adapter Ethernet”, đối với mạng Wifi là mục “Wireless LAN adapter Wi-Fi”).