

HƯỚNG DẪN

Quản lý, sử dụng máy tính có cài đặt phần mềm bảo mật phục vụ soạn thảo, lưu trữ, xử lý văn bản có nội dung bí mật nhà nước

Căn cứ Công văn số 07-CV/CQTTBCĐ ngày 27/9/2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về việc triển khai mạng truyền số liệu chuyên dùng của Đảng và Nhà nước theo hướng thống nhất, dùng chung cho các cơ quan trong hệ thống chính trị để phục vụ việc trao đổi, xử lý văn bản mật; Quyết định 629/QĐ-BCY ngày 20/10/2025 của Trưởng ban Ban Cơ yếu Chính phủ phê duyệt giải pháp bảo mật hệ thống gửi, nhận văn bản và xử lý hồ sơ cấp độ Mật, Tối mật từ Trung ương đến cấp xã cho 4 khối cơ quan trong hệ thống chính trị để phục vụ việc trao đổi, xử lý văn bản. Văn phòng Thành ủy hướng dẫn quản lý, sử dụng máy tính có cài đặt phần mềm bảo mật phục vụ soạn thảo, lưu trữ, xử lý văn bản có nội dung bí mật nhà nước, cụ thể như sau:

I. HƯỚNG DẪN CHUNG

1. Phạm vi điều chỉnh

Văn bản này hướng dẫn tạm thời việc quản lý, sử dụng các máy tính có cài đặt phần mềm bảo mật của Ban Cơ yếu Chính phủ kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật.

Các máy tính tham gia kết nối mạng Internet, mạng khác không thuộc phạm vi điều chỉnh của Hướng dẫn này.

2. Đối tượng áp dụng

Văn bản này áp dụng đối với các cơ quan, tổ chức đảng, các cơ quan Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội từ thành phố đến các xã, phường, đặc khu.

3. Giải thích từ ngữ

- Phần mềm bảo mật: là phần mềm mã hóa do Ban Cơ yếu Chính phủ cung cấp phục vụ việc mã hóa, giải mã, tạo lập phân vùng lưu trữ văn bản mật trên ổ cứng máy tính.

- Phân vùng mã hóa: là phân vùng dùng lưu trữ văn bản mật, được tạo lập từ phần mềm mã hóa của Ban Cơ yếu Chính phủ và được mở bằng mật khẩu do người cài đặt tạo ra.

- Máy tính được kiểm tra an ninh, an toàn: là máy tính của cơ quan, tổ chức đã được công an thành phố kiểm tra an ninh, an toàn, có biên bản kiểm tra và được dán tem theo quy định.

- Máy tính kết nối mạng nội bộ phục vụ gửi nhận văn bản mật (gọi tắt là Máy tính Mật) là máy tính có cài đặt phần mềm bảo mật của Ban Cơ yếu Chính phủ kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật.

4. Yêu cầu

Việc quản lý, sử dụng Máy tính Mật của các cơ quan, tổ chức đảng, các cơ quan Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị xã hội từ thành phố đến các xã, phường, đặc khu thực hiện theo hướng dẫn này và các quy định khác của pháp luật về bảo vệ bí mật nhà nước.

5. Trách nhiệm của cơ quan, tổ chức

- Tổ chức quản lý, sử dụng các máy tính có cài đặt phần mềm bảo mật của Ban Cơ yếu Chính phủ tham gia kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật theo quy định.

- Phân công cán bộ quản lý, theo dõi số lượng máy tính mật, các thiết bị mạng triển khai tại đơn vị mình.

- Thực hiện báo cáo định kỳ 6 tháng 1 lần hoặc đột xuất theo yêu cầu của Văn phòng Thành ủy.

- Khi chuyển đổi mục đích sử dụng máy tính mật, phải phối hợp với Văn phòng Thành ủy để gỡ phần mềm bảo mật đã cài đặt, loại bỏ bí mật nhà nước đã lưu trên máy tính.

- Thông báo cho Văn phòng Thành ủy (qua Phòng Chuyển đổi số - Cơ yếu) khi phát hiện các nguy cơ mất an toàn cho máy tính mật và thiết bị tham gia kết nối mạng nội bộ; nguy cơ lộ, mất bí mật nhà nước trên mạng nội bộ.

- Phối hợp với Văn phòng Thành ủy, Công an thành phố khi có yêu cầu kiểm tra máy tính mật tham gia kết nối mạng nội bộ.

6. Trách nhiệm cá nhân

- Quản lý, sử dụng máy tính mật được cơ quan, đơn vị triển khai theo hướng dẫn này và các quy định khác của pháp luật về bảo vệ bí mật nhà nước.

- Khi chuyển công tác, nghỉ hưu, thôi việc có trách nhiệm bàn giao lại máy tính mật cho cơ quan, đơn vị quản lý theo quy định.

- Báo cáo ngay cho cơ quan, tổ chức khi phát hiện sự cố, nguy cơ mất an toàn máy tính mật và thiết bị tham gia kết nối mạng nội bộ; nguy cơ lộ, mất bí mật nhà nước trên mạng nội bộ.

II. HƯỚNG DẪN CỤ THỂ

1. Tạo lập máy tính mật

Máy tính tham gia kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật được tạo lập theo các bước sau:

Bước 1: Các đơn vị đề nghị Công an thành phố kiểm tra an ninh, an toàn và dán tem theo quy định (*Mẫu công văn đề nghị tại Phụ lục I kèm theo*).

Bước 2: Cài đặt phần mềm bảo mật của Ban Cơ yếu Chính phủ; tạo phân vùng mã hoá để lưu trữ văn bản có nội dung bí mật nhà nước.

Đơn vị thực hiện: Phòng Chuyển đổi số - Cơ yếu, Văn phòng Thành uỷ (hoặc cán bộ Chuyển đổi số của các đơn vị đã được huấn luyện, triển khai và chuyển giao phần mềm).

(*Mẫu công văn đề nghị tại Phụ lục II kèm theo*).

Bước 3: Đặt địa chỉ IP theo quy hoạch của cơ quan, đơn vị; cài đặt phần mềm điều hành tác nghiệp theo Kế hoạch triển khai của các khối cơ quan.

Bước 4: Dán tem, ghi thông số máy tính mật phục vụ việc quản lý, theo dõi (*Mẫu tem dán máy tại Phụ lục III kèm theo*).

2. Quản lý, sử dụng máy tính mật

Khi sử dụng máy tính tham gia kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật, người quản lý, sử dụng phải tuân thủ các quy định sau:

- Không kết nối máy tính với mạng Internet, 3G/4G/5G, Wifi, Bluetooth, thiết bị di động (điện thoại, máy tính bảng...);
- Không kết nối máy tính với USB thương mại, thẻ nhớ, ổ cứng gắn ngoài;
- Không cho phép người không có trách nhiệm sử dụng, sửa chữa, thay thế thiết bị;
- Không tự ý chuyển đổi mục đích sử dụng máy tính;
- Không tự ý gỡ bỏ, thay thế ổ cứng máy tính;
- Không lưu tài khoản, mật khẩu trên trình duyệt;
- Phải đặt mật khẩu đăng nhập Windows trên máy tính.

3. Sửa chữa, bảo hành máy tính mật

- Việc sửa chữa máy tính mật phải do bộ phận chuyên môn của cơ quan, đơn vị thực hiện; nếu đưa ra đơn vị dịch vụ sửa chữa phải thực hiện tháo ổ cứng để lưu giữ, quản lý tại cơ quan, đơn vị.

- Nếu máy tính còn thời hạn bảo hành, khi gửi bảo hành phải tháo giữ lại ổ cứng (nếu ổ cứng hỏng, **TUYỆT ĐỐI KHÔNG ĐƯỢC BẢO HÀNH Ổ CỨNG**).

- Sau khi hoàn thành việc bảo hành, sửa chữa máy tính, các đơn vị phải tiến hành kiểm tra an ninh, an toàn lại trước khi đưa vào sử dụng (nếu phải thay ổ cứng phải thực hiện các bước tạo lập máy tính mật từ đầu).

- Việc bảo hành, sửa chữa, thay thế thiết bị phải được cán bộ làm công tác công nghệ thông tin của đơn vị ghi vào sổ quản lý, theo dõi.

4. Chuyển đổi mục đích sử dụng máy tính mật

Đơn vị có nhu cầu chuyển đổi mục đích sử dụng máy tính mật (chuyển sang sử dụng Internet, thôi dùng, đưa ra khỏi danh sách tài sản quản lý) phải thực hiện các bước sau:

Bước 1: Có văn bản đề nghị Văn phòng Thành uỷ (qua Phòng Chuyển đổi số - Cơ yếu) gỡ bỏ phần mềm bảo mật, loại bỏ bí mật nhà nước đã lưu giữ trong máy tính theo quy định của Luật Bảo vệ bí mật nhà nước.

Bước 2: Phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Thành uỷ tiến hành các giải pháp kỹ thuật để gỡ bỏ phần mềm bảo mật, loại bỏ bí mật nhà nước đã lưu trữ trong máy tính.

Bước 3: Chuyển máy tính trên kèm biên bản gỡ bỏ phần mềm bảo mật đến Công an thành phố (Phòng PA06) để tháo, bóc tem đảm bảo an ninh thông tin.

Bước 4: Đưa máy tính đã gỡ bỏ phần mềm bảo mật, loại bỏ bí mật nhà nước ra khỏi danh sách máy tính mật do cơ quan đơn vị quản lý.

5. Theo dõi, thống kê, báo cáo

- Các cơ quan đơn vị có trách nhiệm thống kê, quản lý, theo dõi máy tính mật, thiết bị ngoại vi kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật.

- Thực hiện báo cáo định kỳ, đột xuất theo yêu cầu (*Biểu mẫu báo cáo tại Phụ lục IV kèm theo*).

6. Đầu mối hỗ trợ

- Hỗ trợ cài đặt phần mềm bảo mật, cấp thiết bị ký số, mã hoá: Phòng Chuyển đổi số - Cơ yếu, Văn phòng Thành uỷ, Tầng 14, Toà nhà A, Trung tâm Chính trị - Hành chính, thành phố Hải Phòng (điện thoại: 08031246).

- Hỗ trợ kiểm tra an ninh, an toàn: Phòng PA06, Công an thành phố, số 82A, đường Cầu Đất (Trung tá Phạm Thị Ly, Đội trưởng Đội 1, điện thoại: 0914.238968).

III. TỔ CHỨC THỰC HIỆN

1. Hướng dẫn này có hiệu lực kể từ ngày ký.
2. Thủ trưởng các cơ quan đơn vị có máy tính tham gia kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước để phục vụ việc trao đổi, xử lý văn bản mật có trách nhiệm tổ chức thực hiện hướng dẫn này và các quy định khác của pháp luật về bảo vệ bí mật nhà nước.
3. Giao Phòng Chuyển đổi số - Cơ yếu theo dõi, hướng dẫn, đôn đốc việc thực hiện Hướng dẫn này; tham mưu việc kiểm tra thực hiện hướng dẫn; đề xuất sửa đổi, bổ sung, thay thế hướng dẫn khi cần thiết.

Nơi nhận:

- TTTU (để báo cáo);
- UBNDTP, HĐNDTP, UB MTTQVN TP,
- Các ban, cơ quan Thành uỷ, các đảng uỷ trực thuộc Thành uỷ,
- Các sở, ban, ngành thành phố,
- Đảng uỷ, HĐND, UBND, Ủy ban MTTQVN các xã, phường, đặc khu,
- Phòng PA06, CATP,
- VPTU: + Các đồng chí lãnh đạo,
- + Các phòng chuyên môn,
- + Lưu.

**K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG**

Nguyễn Mạnh Thắng

PHỤ LỤC I**Mẫu văn bản đề nghị kiểm tra an ninh, an toàn máy tính, thiết bị mạng**

ĐẢNG BỘ THÀNH PHỐ HẢI PHÒNG
ĐẢNG ỦY XÃ

ĐẢNG CỘNG SẢN VIỆT NAM

*

Hải Phòng, ngày tháng năm 2025

Số -CV/ĐU

*V/v đề nghị kiểm tra ANAT máy tính, thiết bị
 mạng tham gia kết nối mạng nội bộ*

Kính gửi: Phòng PA06 - Công an thành phố Hải Phòng.

Thực hiện Công văn số 07-CV/CQTTBCĐ ngày 27/9/2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về việc triển khai mạng truyền số liệu chuyên dùng của Đảng và Nhà nước theo hướng thống nhất, dùng chung cho các cơ quan trong hệ thống chính trị để phục vụ việc trao đổi, xử lý văn bản mật; Công văn số về việc hướng dẫn triển khai bảo đảm an ninh, bảo mật hạ tầng thiết bị đầu cuối tại các cơ quan, đơn vị, địa phương.

Đảng uỷ xã đề nghị Phòng PA06 - Công an thành phố Hải Phòng phối hợp, kiểm tra an ninh, an toàn..... máy tính để phục vụ trao đổi, xử lý văn bản mật.

Đảng uỷ xã phân công đồng chí, Chức vụ, số điện thoại làm đầu mối phối hợp, thực hiện.

Đề nghị Phòng PA06 - Công an thành phố Hải Phòng quan tâm thực hiện.

Nơi nhận:

- Như trên,
- Lưu VP.

T/M BAN THƯỜNG VỤ
BÍ THƯ

.....

PHỤ LỤC II
Mẫu văn bản đề nghị cài đặt phần mềm bảo mật

ĐẢNG BỘ THÀNH PHỐ HẢI PHÒNG
ĐẢNG ỦY XÃ

ĐẢNG CỘNG SẢN VIỆT NAM

*

Hải Phòng, ngày tháng năm 2025

Số -CV/ĐU

*V/v đề nghị cài đặt phần mềm bảo mật cho
máy tính tham gia kết nối mạng nội bộ*

*Kính gửi: Phòng Chuyển đổi số - Cơ yếu,
Văn phòng Thành ủy.*

Thực hiện Công văn số 07-CV/CQTTBCĐ ngày 27/9/2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về việc triển khai mạng truyền số liệu chuyên dùng của Đảng và Nhà nước theo hướng thống nhất, dùng chung cho các cơ quan trong hệ thống chính trị để phục vụ việc trao đổi, xử lý văn bản mật; Công văn số về việc hướng dẫn triển khai bảo đảm an ninh, bảo mật hạ tầng thiết bị đầu cuối tại các cơ quan, đơn vị, địa phương.

Đảng ủy xã đề nghị Phòng Chuyển đổi số - Cơ yếu, Văn phòng Thành ủy cài đặt phần mềm bảo mật cho máy tính để kết nối mạng nội bộ phục vụ trao đổi, xử lý văn bản mật.

Đảng ủy xã phân công đồng chí, Chức vụ:, số điện thoại làm đầu mối phối hợp, thực hiện.

Đề nghị Phòng Chuyển đổi số - Cơ yếu, Văn phòng Thành ủy quan tâm, thực hiện.

Nơi nhận:

- Như trên,
- Lưu VP.

T/M BAN THƯỜNG VỤ
BÍ THƯ

.....

PHỤ LỤC III
Mẫu tem dán máy tính, thiết bị mạng tham gia kết nối mạng mật

1. Tem dán máy

MÁY TÍNH KẾT NỐI MẠNG NỘI BỘ PHỤC VỤ XỬ LÝ VĂN BẢN MẬT
MÁY SỐ: ĐƠN VỊ:..... Người quản lý: Chức vụ: Mã ổ cứng: Địa chỉ IP: NGHIÊM CẤM: ☐ Kết nối Internet, 3G/4G/5G, Wifi, Bluetooth, thiết bị di động (điện thoại, máy tính bảng...); ☐ Kết nối với USB thương mại, thẻ nhớ, ổ cứng gắn ngoài; ☐ Cho người không có trách nhiệm sử dụng, sửa chữa, thay thế thiết bị; ☐ Tự ý chuyển đổi mục đích sử dụng; ☐ Tự ý thay thế ổ cứng.
PHÒNG CHUYÊN ĐỔI SỐ - CƠ YẾU, VPTU Điện thoại: 080.31246

2. Mẫu tem dán cáp mạng, switch

NỘI BỘ	NỘI BỘ
NB	
SWITCH NỘI BỘ NGHIÊM CẤM KẾT NỐI INTERNET	

PHỤ LỤC IV
Mẫu báo cáo danh sách máy tính mật

STT	Họ tên người quản lý	Chức vụ/ Đơn vị	Mã số ổ cứng	Ghi chú
1	Nguyễn Văn A	Bí thư/ Đảng uỷ ..	xxxxxx	