

BAN CHỈ ĐẠO VỀ PHÁT TRIỂN
KHCN, ĐMST VÀ CHUYỂN ĐỔI SỐ
PHƯỜNG VIỆT TRÌ
CƠ QUAN THƯỜNG TRỰC

ĐẢNG CỘNG SẢN VIỆT NAM

Việt Trì, ngày tháng 10 năm 2025

*

Số -CV/BCĐ

*V/v bảo đảm an ninh mạng, bảo mật thông tin,
an toàn dữ liệu trong cơ quan, đơn vị*

- Kính gửi:*
- Các cơ quan tham mưu, giúp việc của Đảng ủy;
 - Các phòng, ban, đơn vị thuộc HĐND, UBND phường;
 - Cơ quan Ủy ban MTTQ Việt Nam phường.

Trong thời gian vừa qua, công tác bảo đảm an toàn, bảo mật thông tin, dữ liệu tại các cơ quan tham mưu, giúp việc của Đảng ủy, các phòng, ban, đơn vị thuộc HĐND, UBND phường và cơ quan Ủy ban MTTQ Việt Nam phường (*sau đây gọi tắt là các cơ quan, đơn vị*) đã được quan tâm, chú trọng; hệ thống mạng internet được kết nối đến các cơ quan, đơn vị, đảm bảo phục vụ xử lý văn bản điện tử và dịch vụ công trực tuyến; đã trang bị máy tính, máy in, thiết bị văn phòng cơ bản cho cán bộ, công chức, viên chức, đoàn viên, hội viên; kịp thời, chủ động ứng dụng, sử dụng phần mềm điều hành tác nghiệp, quản lý văn bản điện tử, chữ ký số. Hạ tầng công nghệ thông tin của phường cơ bản đáp ứng được nhu cầu quản lý, điều hành, bước đầu triển khai công tác chuyển đổi số; hạ tầng mạng, đường truyền cơ bản ổn định, đáp ứng nhu cầu phục vụ họp trực tuyến và các hội nghị trực tuyến.

Tuy nhiên, hạ tầng kỹ thuật CNTT chưa đồng bộ, một số thiết bị trong các cơ quan, đơn vị đã cũ, tốc độ xử lý chậm; các thiết bị đầu cuối cơ bản vẫn sử dụng hệ điều hành và phần mềm của nước ngoài, tiềm ẩn nguy cơ bị cài cắm mã độc, bị chiếm quyền điều khiển từ xa hoặc bị đánh cắp dữ liệu.

Nhằm phòng ngừa, ngăn chặn nguy cơ rò rỉ, mất mát thông tin, bảo mật dữ liệu trong hoạt động điều hành và công tác chuyên môn, thực hiện đúng các quy định của Đảng, Nhà nước về công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu, Cơ quan thường trực Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số phường Việt Trì đề nghị các cơ quan, đơn vị triển khai một số nội dung và biện pháp về bảo đảm an toàn, bảo mật thông tin, dữ liệu như sau:

1. Các cơ quan, đơn vị, nhất là người đứng đầu phải xác định bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu là nhiệm vụ trọng yếu, thường xuyên, lấy phòng ngừa chủ động là chính, không để bất ngờ, bị động trong mọi tình huống; mọi nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an toàn dữ liệu phải được nhận diện và có biện pháp xử lý sớm.

2. Nâng cao nhận thức của cán bộ, công chức, viên chức, người lao động về bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu. Tiếp tục triển khai công tác tuyên truyền, phổ biến giáo dục pháp luật về bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu có chiều sâu, đa dạng về nội dung, hình thức.

3. Tuyệt đối tuân thủ các quy định của Đảng và Nhà nước về bảo mật, không đưa thông tin mật, thông tin nội bộ quan trọng lên các nền tảng ứng dụng AI. Khai thác, sử dụng công cụ AI cho các công việc phù hợp, có kiểm soát, ưu tiên sử dụng nền tảng, phần mềm, công cụ AI do cơ quan có thẩm quyền cho phép.

4. Thủ trưởng các cơ quan, đơn vị tổ chức quán triệt và thực hiện một số biện pháp cơ bản về bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu, cụ thể:

4.1. Về quản lý và sử dụng hệ thống CNTT:

- Chỉ sử dụng hạ tầng CNTT, mạng nội bộ, thiết bị máy tính, máy in... đã được phòng An ninh mạng, Công an tỉnh kiểm tra và dán tem “đảm bảo an ninh thông tin” để thực hiện cho công việc chuyên môn, đúng mục đích; không tự ý cài đặt các phần mềm, ứng dụng không rõ nguồn gốc.

- Trang bị, cập nhật thường xuyên phần mềm chống virus, tường lửa, bảo mật cho các máy tính, thiết bị lưu trữ. Trước mắt sử dụng ứng dụng bảo mật (tên gọi là *Windows Security*, trước đây còn gọi là *Windows Defender*) được tích hợp sẵn và cài đặt mặc định trên hệ điều hành Windows.

- Thường xuyên kiểm tra, cập nhật ngay phần mềm phiên bản mới nhất để tránh bị khai thác; định kỳ sao lưu dữ liệu quan trọng và lưu giữ tại vị trí an toàn; tuyệt đối không lưu trữ tài liệu mật trên thiết bị cá nhân (USB, ổ cứng di động, điện thoại).

4.2. Về quản lý tài khoản và mật khẩu:

- Mỗi cán bộ, công chức, viên chức sử dụng tài khoản cá nhân được cấp để truy cập hệ thống, không chia sẻ hoặc dùng chung tài khoản. Định kỳ (tối thiểu 03 tháng/lần) thực hiện thay đổi mật khẩu máy tính, mật khẩu các phần mềm, ứng dụng phục vụ công việc và phải đảm bảo có đủ độ phức tạp cao.

- Khi trong cơ quan, đơn vị có cán bộ, công chức nghỉ hưu, nghỉ việc hoặc chuyển công tác, người làm công tác văn thư tại các cơ quan, đơn vị phải thông báo về Văn phòng Đảng ủy để tổng hợp, báo cáo cấp có thẩm quyền thực hiện thu hồi, xóa bỏ tài khoản hoặc khóa tài khoản kịp thời.

4.3. Về bảo mật văn bản, tài liệu:

- Văn bản, tài liệu mật, tài liệu nội bộ chỉ được trao đổi qua mạng nội bộ hoặc thiết bị mật, không được gửi qua email cá nhân, các mạng xã hội hiện hành.

- Việc in ấn phải có sổ theo dõi và người phụ trách; khi thực hiện tiếp nhận, phát hành, sao chụp, photo tài liệu mật hoặc tài liệu mật khi không còn sử dụng, phải

tiêu hủy theo đúng quy định tại Quy định số 693-QĐ/VPTW ngày 15/12/2021 của Văn phòng Trung ương Đảng về công tác văn thư trong các cơ quan, tổ chức đảng.

4.4. Về sử dụng internet và mạng xã hội:

- Cán bộ, công chức, viên chức, đoàn viên, hội viên tuyệt đối không đăng tải, phát tán văn bản, hình ảnh, dữ liệu nội bộ của cơ quan lên mạng xã hội.
- Thận trọng khi truy cập các website lạ, không mở tệp đính kèm hoặc đường dẫn không rõ nguồn gốc để tránh nguy cơ bị cài mã độc, mất dữ liệu.

4.5. Về ứng phó khi xảy ra sự cố an ninh mạng, an toàn thông tin, dữ liệu:

- Khi phát hiện sự cố (máy tính bị nhiễm mã độc, mất dữ liệu, bị truy cập trái phép, lộ lọt tài liệu...), cán bộ, công chức, viên chức phải báo ngay cho lãnh đạo đơn vị hoặc cán bộ phụ trách về CNTT của cơ quan, đơn vị; không tự ý xử lý, xóa dấu vết sự cố khi chưa có hướng dẫn cơ quan chức năng có chuyên môn.
- Khoanh vùng, hạn chế thiệt hại, ngắt kết nối mạng đối với thiết bị bị nghi ngờ tấn công; tạm thời dừng sử dụng hệ thống/tài khoản bị lộ để tránh lan rộng; thực hiện sao lưu và bảo quản bản gốc dữ liệu nếu còn có thể khôi phục.
- Kịp thời, nhanh chóng báo cáo về Văn phòng Đảng ủy để phối hợp với các cơ quan, chức năng về an ninh mạng để khắc phục, xử lý sự cố.

5. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm tổ chức thực hiện, kiểm tra, đôn đốc cán bộ, công chức, viên chức, đoàn viên, hội viên về việc bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu thuộc đơn vị.

6. Văn phòng Đảng ủy (cơ quan thường trực của Ban Chỉ đạo phường) có trách nhiệm theo dõi, tổng hợp những khó khăn, vướng mắc; phối hợp với các cơ quan chức năng có thẩm quyền trong việc bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu và xử lý sự cố.

Đề nghị các cơ quan, đơn vị triển khai, thực hiện, đảm bảo an ninh mạng, bảo mật thông tin, an toàn dữ liệu hiệu quả./.

Nơi nhận:

- Như trên,
- Văn phòng Tỉnh ủy,
- Thường trực BCD phường,
- CVP, các PCVP, Cv phụ trách CDS,
- Lưu VPĐU.

CHÁNH VĂN PHÒNG ĐẢNG ỦY
kiêm
THÀNH VIÊN THƯỜNG TRỰC
BAN CHỈ ĐẠO

Nguyễn Giang Nam