ĐẢNG BỘ TỈNH YÊN BÁI
HUYỆN UỶ YÊN BÌNH
*
Số 2021 - CV/HU
V/v triển khai thực hiện Quy định 3676-QĐ/VPTW ngày 27/3/2025 của Văn phòng Trung ương Đảng

ĐẢNG CỘNG SẢN VIỆT NAM

Yên Bình, ngày 11 tháng 4 năm 2025

Kính gửi: - Các cơ quan, tham mưu giúp việc Huyện uỷ;
- Trung tâm Chính trị huyện;
- Các đảng bộ, chi bộ cơ sở trực thuộc Huyện uỷ.

Thực hiện Công văn số 2579-CV/TU ngày 06/4/2025 của Ban Thường vụ Tỉnh uỷ Yên Bái về việc triển khai thực hiện Quy định 3676-QĐ/VPTW ngày 27/3/2025 của Văn phòng Trung ương Đảng về vận hành, đảm bảo an toàn thông tin đối với thiết bị, đường truyền kết nối trong các cơ quan đảng. Thường trực Huyện uỷ yêu cầu:

1. Các cơ quan chuyên trách tham mưu, giúp việc Huyện uỷ, Trung tâm Chính trị huyện; các đảng bộ, chi bộ cơ sở trực thuộc Huyện uỷ: (1) Lãnh đạo, chỉ đạo, tổ chức phổ biến, quán triệt, triển khai thực hiện nghiêm túc Quy định số 3676-QĐ/VPTW ngày 27/3/2025 của Văn phòng Trung ương Đảng; nâng cao nhận thức, trách nhiệm của cán bộ, đảng viên, nhất là người đứng đầu các cấp ủy, tổ chức đảng, cơ quan, đơn vị về an toàn thông tin. (2) Thường xuyên tự kiểm tra, giám sát, kịp thời phát hiện xử lý dấu hiệu có nguy cơ gây mất an toàn thông tin; chủ động phối hợp với Văn phòng Huyện uỷ xử lý sự cố về an toàn thông tin, an ninh mạng. (3) Người đứng đầu các cấp ủy, tổ chức đảng, cơ quan, đơn vị chịu trách nhiệm về việc vận hành, bảo đảm an toàn thông tin đối với thiết bị, đường truyền kết nối của cơ quan, đơn vị mình *(Có sao gửi Quy định số 3676-QĐ/VPTW ngày 27/3/2025 của Văn phòng Trung ương Đảng kèm theo).*

2. Văn phòng Huyện uỷ: (1) Chủ trì phối hợp với các cơ quan, đơn vị liên quan tham mưu triển khai các giải pháp nhằm vận hành, bảo đảm an toàn thông tin đối với thiết bị, đường truyền kết nối trong các cơ quan đảng huyện. (2) Theo dõi, hướng dẫn, đôn đốc, kiểm tra, giám sát việc thực hiện Quy định số 3676-QĐ/VPTW ngày 27/3/2025 của Văn phòng Trung ương Đảng; định kỳ hoặc khi có yêu cầu báo cáo cấp có thẩm quyền kết quả triển khai thực hiện theo quy định.

Yêu cầu các cơ quan, đơn vị nghiêm túc triển khai thực hiện, trong quá trình triển khai thực hiện có khó khăn, vướng mắc đề nghị gửi báo cáo về Thường trực Huyện uỷ (qua Văn phòng Huyện uỷ) để tổng hợp.

Nơi nhận:
- Như trên,
- Thường trực Huyện uỷ,
- Thường trực HĐND huyện,
- Lãnh đạo UBND huyện,
- Các đ/c UV BCH Đảng bộ huyện,
- Lưu VPHU.

T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ THƯỜNG TRỰC

ĐẢNG CỘNG SẢN VIỆT NAM
HUYỆN ỦY YÊN BÌNH
ĐẢNG BỘ TỈNH YÊN BÁI

Nguyễn Lê Dũng

BAN CHẤP HÀNH TRUNG ƯƠNG
VĂN PHÒNG
*
Số 3676-QĐ/VPTW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 27 tháng 3 năm 2025

QUY ĐỊNH

Vận hành, bảo đảm an toàn thông tin đối với thiết bị, đường truyền kết nối trong các cơ quan đảng

---

- Căn cứ Luật Bảo vệ bí mật nhà nước;

- Căn cứ Luật An ninh mạng;

- Căn cứ Luật An toàn thông tin mạng;

- Căn cứ Quyết định số 259-QĐ/TW, ngày 24/01/2025 của Bộ Chính trị khoá XIII về chức năng, nhiệm vụ, tổ chức bộ máy của Văn phòng Trung ương Đảng;

- Căn cứ Quyết định số 204-QĐ/TW, ngày 29/11/2024 của Ban Bí thư phê duyệt Đề án Chuyển đổi số trong các cơ quan đảng;

- Căn cứ Thông báo kết luận số 06-TB/BCĐCĐS, ngày 18/3/2025 của Ban Chỉ đạo Chuyển đổi số trong các cơ quan đảng về việc giao Đảng uỷ Bộ Khoa học và Công nghệ chủ trì, phối hợp với Văn phòng Trung ương Đảng và các cơ quan liên quan triển khai hạ tầng kết nối mạng thông tin diện rộng của Đảng qua mạng truyền số liệu chuyên dùng với băng thông rộng, tốc độ cao, kết nối các cơ quan đảng từ Trung ương tới cơ sở;

- Xét đề nghị của Cục trưởng Cục Chuyển đổi số - Cơ yếu,

Văn phòng Trung ương Đảng quy định việc vận hành, bảo đảm an toàn thông tin đối với thiết bị, đường truyền kết nối trong các cơ quan đảng như sau:

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy định về việc vận hành, bảo đảm an toàn thông tin đối với các thiết bị, đường truyền kết nối trong các cơ quan đảng.

2. Các cơ quan khác có máy tính, đường truyền kết nối vào mạng thông tin diện rộng của Đảng cũng thuộc phạm vi điều chỉnh của Quy định này.

3. Đối với các thiết bị chuyên dụng do Ban Cơ yếu Chính phủ cung cấp sử dụng trong các cơ quan đảng được quản lý theo các quy định của ngành Cơ yếu.

Điều 2. Đối tượng áp dụng

1. Các thiết bị công nghệ thông tin, đường truyền mạng của các cơ quan đảng.

2. Máy tính, đường truyền của các cơ quan khác kết nối trực tiếp vào mạng thông tin diện rộng của Đảng.

Điều 3. Giải thích từ ngữ

1. Thiết bị tin học là thiết bị phần cứng được sử dụng cho hoạt động ứng dụng công nghệ thông tin, gồm: Máy tính (máy chủ, máy tính để bàn, máy tính xách tay...) và các thiết bị kèm theo như: Màn hình, bàn phím, chuột, loa...), các thiết bị ngoại vi (máy in, các loại thiết bị lưu trữ, máy quét, máy ghi hình, máy ghi âm, máy ảnh... cắm trực tiếp vào máy tính), các thiết bị kết nối mạng, các thiết bị bảo vệ, kiểm soát an toàn, an ninh mạng, các thiết bị bảo mật, các thiết bị phụ trợ khác (lưu điện, phát hiện và báo cháy, nổ...), các linh kiện, phụ kiện để thay thế, sửa chữa.

2. Thiết bị lưu trữ điện tử là các thiết bị có khả năng lưu giữ thông tin điện tử gồm: Đĩa cứng, đĩa mềm, đĩa quang, băng từ, các thiết bị lưu trữ dạng flash như: USB, ổ cứng di động, thẻ nhớ...

3. Phần mềm tin học là các chương trình chạy trên máy tính, mạng máy tính để xử lý thông tin, gồm: Phần mềm hệ thống, hệ quản trị cơ sở dữ liệu; phần mềm giám sát; phần mềm quản trị mạng và ứng dụng; phần mềm chống virus; phần mềm an ninh bảo mật; phần mềm mã mật; phần mềm tiện ích; phần mềm ứng dụng và dữ liệu ứng dụng...

4. Bảo trì là công việc duy tu, bảo dưỡng thiết bị và phần mềm tin học trong quá trình sử dụng nhằm duy trì khả năng làm việc, tăng tuổi thọ, sớm phát hiện và ngăn chặn nguy cơ hỏng, mất an ninh, an toàn của thiết bị và phần mềm tin học.

Điều 4. Nguyên tắc quản lý thiết bị

1. Đáp ứng nhu cầu làm việc cần thiết theo chức năng, nhiệm vụ được giao.

2. Chất lượng tốt, sử dụng lâu, bền, hiện đại, thiết thực, hiệu quả, tránh lãng phí, đáp ứng yêu cầu công việc.

3. Bảo đảm an ninh, an toàn thông tin.

4. Cấu hình tối thiểu thiết bị, danh mục phần mềm được cài đặt thực hiện theo Phụ lục 1 và Phụ lục 2 kèm theo Quy định này.

Chương II
QUY ĐỊNH VỀ QUẢN LÝ, SỬ DỤNG THIẾT BỊ, ĐƯỜNG TRUYỀN KẾT NỐI MẠNG

Điều 5. Vị trí đặt thiết bị

1. Thiết bị phải đặt tại vị trí nơi làm việc của cơ quan, đơn vị bảo đảm điều kiện về hạ tầng kỹ thuật (diện tích, nhiệt độ, độ ẩm, ...) và việc hoạt động lâu dài của thiết bị, tránh tình trạng ẩm, mốc, hư hỏng các bộ phận phần cứng của thiết bị.

2. Người sử dụng không được tự ý di chuyển thiết bị khi chưa có sự đồng ý của lãnh đạo đơn vị quản lý.

Điều 6. Các hành vi bị nghiêm cấm trong quá trình sử dụng

1. Các hành vi bị nghiêm cấm được quy định tại Điều 7, Luật An toàn thông tin mạng năm 2015 và Điều 8 Luật An ninh mạng năm 2018 và Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng của các hệ thống; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và Internet bằng thiết bị kết nối Internet của cá nhân (USB 3G/4G/5G..., điện thoại di động, máy tính bảng, máy tính xách tay...).

3. Chuyển đổi mục đích sử dụng máy tính để soạn thảo, lưu trữ thông tin mật có nội dung bí mật nhà nước sang máy tính có kết nối Internet và ngược lại mà chưa làm sạch và thực hiện giải pháp huỷ dữ liệu triệt để.

4. Sử dụng chung các thiết bị ngoại vi với các máy tính khác. Nghiêm cấm sử dụng các thiết bị ngoại vi không được cấp phép tiến hành kết nối vào các hệ thống.

5. Tự ý sao chép, thay đổi, gỡ bỏ biện pháp an toàn thông tin (gỡ bỏ phần mềm giám sát, tắt phần mềm diệt virus, phần mềm mã hoá, phần mềm bảo mật cơ yếu (nếu có)); tự ý thay thế, lắp mới, trao đổi thành phần của máy tính phục vụ công việc.

6. Tạo ra, cài đặt, phát tán phần mềm độc hại gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin. Tự ý cài đặt phần mềm không thuộc danh sách các phần mềm được sử dụng (trong Phụ lục gắn kèm).

7. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy cập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

8. Bẻ khoá, trộm cắp, sử dụng mật khẩu, khoá mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng của hệ thống.

9. Các hành vi khác làm mất an ninh, an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng của hệ thống.

10. Thu thập, sử dụng, phát tán trái pháp luật thông tin nằm trong các hệ thống; lợi dụng sơ hở, điểm yếu của các hệ thống đặt tại Trung tâm dữ liệu để thu thập, khai thác trái phép thông tin.

11. Khai thác dữ liệu thông tin trái phép, sử dụng thông tin trái mục đích (dữ liệu lưu trên hệ thống hay thông tin lưu trữ dưới dạng giấy tờ).

12. Sử dụng tài khoản của người khác quản lý khi chưa có sự đồng ý của chủ tài khoản.

13. Thay đổi cấu hình trên thiết bị máy tính (địa chỉ mạng, cấu hình để truy cập vào sản phẩm mật mã, tên máy tính,...).

14. Sử dụng các thiết bị để truy cập vào hệ thống tại Trung tâm dữ liệu không đúng mục đích (lưu trữ thông tin không thuộc hệ thống,...).

15. Phá hoại tài sản, thiết bị phục vụ truy cập vào hệ thống.

Điều 7. Quản lý sử dụng thiết bị

1. Các thiết bị tin học khi đem ra ngoài sửa chữa, bảo hành, thanh lý phải được tháo toàn bộ các ổ đĩa cứng và thẻ nhớ; các ổ đĩa cứng, thẻ nhớ có thể được sử dụng tiếp tục trong cơ quan sau khi xoá hoàn toàn (không thể phục hồi) dữ liệu hoặc tiêu huỷ.

2. Đối với các thiết bị trang cấp mới, phối hợp cơ quan chức năng của Bộ Công an kiểm tra an ninh, an toàn thông tin thiết bị trước khi đưa vào sử dụng. Khi thiết bị hỏng hóc và không thể sửa chữa, thay thế sẽ tiến hành thu hồi để đưa vào thanh lý, tiêu huỷ.

3. Đối với các thiết bị khi chuyển mục đích sử dụng phải được thực hiện xoá, làm sạch dữ liệu cũ và cài mới hệ điều hành, ứng dụng trước khi bàn giao.

Điều 8. Quản lý tài khoản, mật khẩu

1. Người sử dụng thực hiện quản lý tài khoản, mật khẩu được cấp; định kỳ 2 tháng đổi mật khẩu một lần. Mật khẩu phải đặt tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

2. Tài khoản cấp cho người dùng để sử dụng trong công việc. Khi chuyển công tác, nghỉ hưu hoặc thay đổi công việc, cần thực hiện việc thay đổi quyền hoặc thu hồi tài khoản.

Điều 9. Xử lý dấu hiệu có nguy cơ gây mất an toàn thông tin

1. Trong quá trình vận hành, khai thác sử dụng thiết bị, cán bộ trong các cơ quan phát hiện các trường hợp có dấu hiệu vi phạm, các hành vi bị nghiêm cấm theo Điều 6 tại Quy định này có trách nhiệm báo cáo lãnh đạo cấp trên để thực hiện xử lý.

2. Trong trường hợp phát hiện lây nhiễm mã độc (theo nhiều hình thức phát hiện từ phần mềm phòng, chống mã độc, các trường hợp đã được các cấp hướng dẫn bằng văn bản,...) có nguy cơ mất an toàn thông tin trên diện rộng. Cán bộ kỹ thuật thực hiện đánh giá nguy cơ theo hướng dẫn, thực hiện cô lập thiết bị không cho phép truy cập (trực tiếp hay gián tiếp) vào các hệ thống. Sau đó, thực hiện chế độ báo cáo theo các cấp để tiến hành xử lý sự cố về an toàn thông tin.

Điều 10. Công tác tự kiểm tra, giám sát

1. Cơ quan, đơn vị có trách nhiệm xây dựng kế hoạch kiểm tra định kỳ 6 tháng/lần và đột xuất, trong đó thực hiện kiểm tra các nội dung (*các nội dung cụ thể trong các khoản bên dưới*).

2. Kiểm tra việc quản lý thiết bị, tài sản, sử dụng, quản lý, phân quyền tài khoản khai thác các hệ thống thông tin.

3. Kiểm tra việc bảo đảm an toàn thông tin, an ninh mạng, các dấu hiệu gây mất an toàn thông tin trong quá trình khai thác hệ thống.

4. Việc kiểm tra chấp hành các quy định phải đánh giá đúng ưu điểm, hạn chế; phát hiện những sơ hở, điểm yếu, lỗ hổng và kiến nghị các biện pháp khắc phục, xử lý kỷ luật (nếu có).

5. Trong quá trình kiểm tra, cán bộ kỹ thuật được sử dụng các công cụ để thực hiện kiểm tra, đánh giá an toàn thông tin, an ninh mạng.

Điều 11. Quy trình trang bị, sửa chữa thiết bị

1. Thủ trưởng các đơn vị trực thuộc gửi yêu cầu trang bị, sửa chữa, thay thế thiết bị và phần mềm tin học đến đơn vị phụ trách về công nghệ thông tin. Trong một số trường hợp, đơn vị phụ trách về công nghệ thông tin chủ động khảo sát, rà soát để xác định nhu cầu trang bị, sửa chữa, thay thế thiết bị trong cơ quan.

2. Thẩm định, xác nhận, tổng hợp, trả lời yêu cầu của các đơn vị sau 5 ngày kể từ ngày nhận yêu cầu.

3. Thực hiện sửa chữa ngay sau khi nhận được yêu cầu của các đơn vị.

4. Thực hiện việc mua sắm theo quy định.

5. Khi người sử dụng xử lý văn bản mật thì được trang bị máy tính riêng tách biệt hoàn toàn với mạng máy tính khác.

Điều 12. Kiểm tra an ninh

1. Kiểm tra an ninh với thiết bị mua mới gồm: Kiểm tra cháy nổ; kiểm tra đo phát sóng, tín hiệu.

2. Kiểm tra an ninh với phần mềm mua mới, bảo hành và nâng cấp, gồm: Kiểm tra các lỗ hổng bảo mật, virus, mã độc.

3. Các thiết bị được kiểm tra an ninh phải dán tem của cơ quan chức năng xác nhận an toàn và biên bản chứng nhận được phép đưa thiết bị vào sử dụng.

Điều 13. Điều chuyển, thu hồi

1. Cán bộ, nhân viên được điều chuyển công tác trong nội bộ cơ quan tiếp tục quản lý, sử dụng thiết bị và phần mềm tin học đã được giao ở đơn vị cũ, thông báo các thay đổi về hiện trạng hoạt động (nếu có) với bộ phận công nghệ thông tin. Riêng đối với phần mềm ứng dụng chuyên dùng của đơn vị cũ phải bàn giao lại cho cán bộ, nhân viên thay thế.

2. Thiết bị và phần mềm tin học được thu hồi khi cán bộ, nhân viên được điều chuyển công tác đến cơ quan khác, nghỉ hưu, nghỉ chế độ, thôi việc, đi học tập trung, dài hạn từ 1 năm trở lên hoặc khi thiết bị và phần mềm tin học bị hỏng, không sử dụng được.

3. Khi điều chuyển, thu hồi thiết bị và phần mềm tin học: (1) Lập biên bản xác nhận hiện trạng kỹ thuật và kiến nghị xử lý. (2) Xoá dữ liệu cá nhân trên máy tính hoặc huỷ ổ đĩa cứng trong trường hợp thu hồi, bị hỏng. (3) Thực hiện việc thu hồi, điều chuyển hoặc thanh lý.

Điều 14. Bảo trì thiết bị tin học

1. Các thiết bị và phần mềm tin học trong cơ quan được bảo trì định kỳ mỗi năm 2 đợt.

2. Bảo trì thiết bị tin học gồm: (1) Kiểm tra tình trạng hoạt động của thiết bị, cấu hình, tốc độ; làm vệ sinh công nghiệp. (2) Kiểm tra, diệt quét virus, mã độc. (3) Phát hiện, kiến nghị và sửa chữa, thay thế các thiết bị hư hỏng hoặc hết hạn sử dụng.

Điều 15. Thanh lý thiết bị

1. Các thiết bị và phần mềm tin học cũ, hỏng, không sử dụng được trong cơ quan, được đưa vào danh sách đề nghị thanh lý.

2. Các thiết bị tin học khi đề nghị thanh lý phải được tháo toàn bộ các ổ đĩa cứng và thẻ nhớ; các ổ đĩa cứng, thẻ nhớ có thể được sử dụng tiếp tục trong cơ quan sau khi xoá hoàn toàn (không thể khôi phục) dữ liệu hoặc tiêu huỷ.

Điều 16. Tiêu huỷ thiết bị lưu trữ điện tử

1. Thống kê hiện trạng, xây dựng danh sách thiết bị, đề xuất kế hoạch tiêu huỷ thiết bị lưu trữ điện tử với lãnh đạo cơ quan.

2. Thành lập Hội đồng tiêu huỷ thiết bị lưu trữ điện tử để kiểm tra, thẩm định, lập biên bản, báo cáo kết quả tiêu huỷ (trừ các thiết bị do Ban Cơ yếu Chính phủ cấp).

3. Thực hiện tiêu huỷ thiết bị lưu trữ điện tử sử dụng phương pháp huỷ vật lý: đập, nghiền vỡ, đốt cháy.

4. Làm sạch môi trường sau khi tiêu huỷ.

Điều 17. Tiêu chuẩn đường truyền kết nối

1. Các mô hình, giải pháp kỹ thuật kết nối các hệ thống mạng máy tính với nhau phải tuân thủ Kiến trúc chuyển đổi số thống nhất trong các cơ quan Đảng và Nhà nước.

2. Băng thông tối thiểu:

Đường truyền kết nối cần bảo đảm tốc độ kênh truyền tối thiểu 10Mbps đối với cấp cơ sở, 50Mbps đối với cấp tỉnh và bảo đảm không tắc nghẽn (*mức chiếm dụng băng thông trung bình giữa lưu lượng dữ liệu truyền qua đường truyền trong một đơn vị thời gian và tốc độ tối đa của đường truyền của kết nối <= 80%, băng thông tính bằng Mbps*).

3. An toàn, bảo mật:

a) Toàn bộ dữ liệu truyền qua mạng phải được mã hoá bằng giao thức bảo mật VPN hoặc các giao thức khác theo hướng dẫn của Văn phòng Trung ương Đảng.

b) Sử dụng thống nhất, đồng bộ các giải pháp giám sát an ninh mạng và bảo mật thông tin.

c) Dữ liệu cấp độ mật phải được mã hoá bằng giải pháp bảo mật của Ban Cơ yếu Chính phủ.

4. Kết nối mạng cấp cơ sở vào mạng thông tin diện rộng của Đảng sử dụng đường truyền Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước tại địa phương; các yêu cầu kỹ thuật về kênh truyền, yêu cầu chất lượng kênh truyền, mô hình kết nối, đối tượng kết nối cần tuân thủ các quy định pháp luật hiện hành về mạng truyền số liệu chuyên dùng phục vụ cơ quan Đảng, Nhà nước.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 18. Trách nhiệm của Văn phòng Trung ương Đảng

1. Chủ trì, phối hợp với các cơ quan đảng ở Trung ương và các tỉnh uỷ, thành uỷ triển khai, tổ chức, hướng dẫn thực hiện Quy định.

2. Theo dõi, đôn đốc, kiểm tra, hướng dẫn việc thực hiện Quy định này; đề xuất sửa đổi, bổ sung nếu cần thiết.

3. Chủ trì theo dõi, phối hợp với các đơn vị có liên quan kiểm tra tình trạng hoạt động máy trạm, công tác bảo đảm an toàn thông tin trong việc sử dụng thiết bị thuộc các hệ thống đặt tại Trung tâm dữ liệu theo định kỳ hoặc theo kế hoạch nhằm phát hiện, ngăn chặn kịp thời sự cố ảnh hưởng đến quá trình sử dụng thiết bị.

4. Phối hợp với các cơ quan, đơn vị địa phương thực hiện công tác tuyên truyền nâng cao nhận thức của người sử dụng.

5. Chủ động theo dõi, giám sát an ninh mạng các máy tính trạm của các cơ quan, đơn vị tại địa phương có kết nối, khai thác sử dụng các dịch vụ từ Trung tâm dữ liệu của cơ quan đảng, phối hợp để thực hiện xử lý các nguy cơ về an toàn, an ninh mạng.

Điều 19. Trách nhiệm của các cơ quan đảng

1. Căn cứ Quy định này và tình hình thực tiễn, các cơ quan đảng bố trí kinh phí đầy đủ, kịp thời trong kế hoạch ngân sách hằng năm bảo đảm trang bị, sửa chữa thiết bị, phần mềm.

2. Chỉ đạo các cơ quan, đơn vị cấp dưới về xử lý sự cố về an toàn thông tin, an ninh mạng.

3. Chỉ đạo các cơ quan, đơn vị cấp dưới phối hợp với Cục Cơ yếu Đảng - Chính quyền, Ban Cơ yếu Chính phủ quản lý, theo dõi và hướng dẫn sử dụng sản phẩm mật mã theo đúng quy định.

4. Quản lý, giám sát tình trạng thiết bị đầu cuối trang cấp cho cơ quan, đơn vị sử dụng cài đặt phần mềm tuân thủ theo quy định bảo đảm an ninh, an toàn thông tin.

5. Tổ chức kiểm tra, giám sát, đánh giá tình trạng hoạt động, tiếp nhận và xử lý các sự cố về an ninh, an toàn thông tin.

Điều 20. Trách nhiệm của Ban Cơ yếu Chính phủ

1. Bảo đảm các sản phẩm, thiết bị mật mã trang bị, đáp ứng yêu cầu sử dụng.

2. Phối hợp triển khai các giải pháp bảo mật cho các cơ quan đảng khi có yêu cầu.

Điều 21. Trách nhiệm của cá nhân quản lý, sử dụng thiết bị

1. Bảo đảm an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân theo thẩm quyền được giao.

2. Chủ động báo cáo kết quả tình trạng hoạt động, sự cố khi sử dụng thiết bị không đảm bảo an ninh, an toàn.

3. Có trách nhiệm quản lý tài khoản, thiết bị truy cập hệ thống thông tin được quản lý và chịu trách nhiệm nếu vi phạm theo các nội dung tại Quy định này.

4. Thực hiện đúng quy định hiện hành của Đảng và Nhà nước về quản lý, sử dụng thiết bị, phần mềm.

5. Bảo quản, giữ gìn, bảo đảm sử dụng lâu bền, tiết kiệm, thiết thực, hiệu quả.

6. Phối hợp với đơn vị chuyên trách về công nghệ thông tin của đơn vị trong việc bảo trì thiết bị và phần mềm tin học, sao lưu dữ liệu (nếu cần thiết), xoá dữ liệu trong máy tính trước khi bàn giao, điều chuyển hoặc thanh lý.

7. Bàn giao các thiết bị tin học, thiết bị lưu trữ điện tử khi không còn công tác tại cơ quan. Giao nộp kịp thời các thiết bị lưu trữ điện tử cũ, hỏng, không sử dụng được và không được phép tự huỷ, hoặc để thất thoát ra bên ngoài cơ quan.

Điều 22. Điều khoản thi hành

1. Quy định này có hiệu lực thi hành từ ngày ký.

2. Người đứng đầu các cơ quan đảng và các cơ quan, tổ chức, đơn vị, cá nhân có liên quan chịu trách nhiệm thi hành Quy định này.

3. Trong quá trình thực hiện Quy định này, nếu có khó khăn, vướng mắc, các cơ quan đảng kịp thời thông báo tới Văn phòng Trung ương Đảng (qua Cục Chuyển đổi số - Cơ yếu) để tổng hợp, báo cáo lãnh đạo xem xét, quyết định.

Nơi nhận:
- Các cơ quan đảng ở Trung ương,
- Các tỉnh uỷ, thành uỷ,
- Ban Cơ yếu Chính phủ,
- Lưu Văn phòng Trung ương Đảng.

CHÁNH VĂN PHÒNG

VĂN PHÒNG TRUNG ƯƠNG ĐẢNG
03-01-2025 10:12:45 +07:00

Lê Hoài Trung

PHỤ LỤC 1

Cấu hình tối thiểu thiết bị

(Kèm theo Quy định số 3676-QĐ/VPTW, ngày 27/3/2025 của Văn phòng Trung ương Đảng)

STT	Thiết bị	Yêu cầu tối thiểu
1	Máy tính	- Bộ xử lý Intel Core i5, thế hệ 12 - Bộ nhớ: 8GB DDR4 - Ổ cứng SSD 250GB - Màn hình máy tính để bàn 19" - Hệ điều hành (có bản quyền): Windows 10 trở lên hoặc tương đương - Phần mềm cài đặt (có bản quyền): MS Office 2016 hoặc tương đương; bộ gõ tiếng Việt Unikey; trình duyệt Chrome; phần mềm diệt virus
2	Máy in	- In laser đen trắng - 2 mặt tự động - Tương thích hệ điều hành Windows
3	Máy quét tài liệu số hoá	- Tính năng quét hai mặt, quét nhiều trang - Khay ADF tối thiểu 40 - Tốc độ quét tối thiểu 30ppm (2 mặt) - Khổ giấy A4 - Tương thích hệ điều hành Windows
4	Máy quét tài liệu lưu trữ lịch sử	Quét 2 mặt tự động; tích hợp khay quét phẳng (flatbed); ADF: CIS x 2; Flatbed: Color CCD x 1; tối đa: 215,9 x 355,6 mm; tối thiểu: 48 x 50 mm; quét giấy dài: 6.096 mm; có khả năng quét hộ chiếu và sổ đóng ghim, thẻ nhựa; một mặt: 70 ppm, hai mặt: 140 ipm (A4, quét màu, 300dpi); Flatbed: 1,7 giây (200 dpi/ 300 dpi); 100 tờ (A4: 80 g/m2) 10.000 trang/ngày; USB 3.2 Gen1x1 / USB 2.0 / USB 1.1; LAN: 10BASE-T, 100BASE-TX, 1000BASE-T; A3 gập đôi; và quét bì thư; kèm theo phần mềm (OCR)
5	Ổ USB	Do Ban Cơ yếu Chính phủ cấp phát.

PHỤ LỤC 2

Danh mục phần mềm

(Kèm theo Quy định số 3676-QĐ/VPTW, ngày 27/3/2025 của Văn phòng Trung ương Đảng)

- Hệ điều hành máy trạm: Windows 10 trở lên hoặc tương đương.
- Office: MS Office 2016 trở lên hoặc tương đương.
- Bộ gõ tiếng Việt: Unikey.
- Trình duyệt web: MS Edge, Google Chrome.
- Mail: Webmail hoặc Mail Client.
- Phần mềm diệt virus.
- Phần mềm công cụ (ví dụ: Acrobat Reader, Photoshop, ...).
- Phần mềm chống thất thoát dữ liệu (khi có yêu cầu).
- Phần mềm giám sát an ninh (khi có yêu cầu).