



BAN CHẤP HÀNH TRUNG ƯƠNG

*

Số 03-QC/TW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 19 tháng 10 năm 2026

QUY CHẾ

tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng

- Căn cứ Điều lệ Đảng;
- Căn cứ Quy chế làm việc của Ban Chấp hành Trung ương, Bộ Chính trị và Ban Bí thư khoá XIV;
- Căn cứ Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;
- Căn cứ 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;
- Căn cứ Quyết định số 204-QĐ/TW, ngày 29/11/2024 của Ban Bí thư về việc phê duyệt Đề án Chuyển đổi số trong các cơ quan đảng;
- Căn cứ Quyết định số 487-QĐ/TW, ngày 29/9/2026 của Ban Bí thư về ban hành Khung Kiến trúc số của các cơ quan đảng, phiên bản 1.0;
- Căn cứ Quy định số 384-QĐ/TW, ngày 19/11/2025 của Ban Bí thư về kết nối, chia sẻ dữ liệu giữa các cơ quan đảng với các cơ quan, tổ chức khác trong hệ thống chính trị;
- Căn cứ Luật Chuyển đổi số số 148/2025/QH15;
- Căn cứ Luật Cơ yếu số 05/2011/QH13;
- Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;
- Căn cứ Luật An ninh mạng số 116/2025/QH15;
- Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;
- Căn cứ Luật Dữ liệu số 60/2024/QH15;
- Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;
- Căn cứ Luật Viễn thông số 24/2023/QH15;

- Căn cứ Quyết định số 33/2025/QĐ-TTg, ngày 15/9/2025 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

- Xét đề nghị của Văn phòng Trung ương Đảng.

Ban Bí thư ban hành Quy chế tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng.

Chương I **QUY ĐỊNH CHUNG**

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng để thống nhất áp dụng trong các cơ quan, tổ chức đảng từ Trung ương đến cấp xã, phường, đặc khu nhằm bảo đảm hoạt động liên tục, ổn định, hiệu quả, tin cậy, an toàn của mạng.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với các cơ quan, tổ chức đảng từ Trung ương đến cấp xã, phường, đặc khu, cá nhân có thiết bị, mạng máy tính kết nối, sử dụng hệ thống mạng máy tính của Đảng; tham gia cung cấp sản phẩm, dịch vụ, quản lý, giám sát, vận hành và khai thác hệ thống mạng máy tính của Đảng.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

Hệ thống mạng máy tính của Đảng bao gồm Mạng thông tin diện rộng của Đảng và Mạng Internet phục vụ cho các cơ quan, tổ chức đảng.

Mạng thông tin diện rộng của Đảng (mạng Intranet của Đảng) là hệ thống mạng máy tính thiết lập trên cơ sở hạ tầng kỹ thuật công nghệ thông tin và viễn thông quốc gia; sử dụng mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước để kết nối mạng máy tính nội bộ của các cơ quan, tổ chức đảng từ Trung ương đến địa phương (tỉnh uỷ, thành uỷ; đảng uỷ các xã, phường, đặc khu và các đơn vị trực thuộc đảng uỷ khi không cùng trụ sở, địa bàn xa trụ sở), một số cơ quan đặc thù phục vụ các quy trình nghiệp vụ của các cơ quan đảng, các hệ thống thông tin, trung tâm dữ liệu và mạng di động dùng riêng; tích hợp các giải pháp bảo mật của Ban Cơ yếu Chính phủ để xác thực, bảo mật thông tin, dữ liệu trên mạng.

Mạng Internet phục vụ cho cơ quan, tổ chức đảng là hệ thống mạng máy tính cung cấp cho người sử dụng khả năng truy nhập Mạng Internet, bao

gồm hạ tầng kết nối (có dây và không dây), các mạng máy tính nội bộ của các cơ quan, tổ chức đảng, các thiết bị máy tính, thiết bị di động thông minh và các thiết bị đầu cuối khác khi có nhu cầu kết nối và sử dụng để truy cập, khai thác các hệ thống thông tin, phần mềm ứng dụng, dịch vụ dùng chung của Đảng trên môi trường Internet.

Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước là mạng kết nối các cơ quan Đảng, Nhà nước, được tổ chức, quản lý thống nhất, bảo đảm chất lượng, an toàn, bảo mật thông tin để trao đổi, chia sẻ dữ liệu giữa các cơ quan Đảng, Nhà nước. Việc quản lý, vận hành, bảo đảm an ninh mạng, an ninh dữ liệu và các tiêu chuẩn kỹ thuật thực hiện theo quy định của Thủ tướng Chính phủ và các văn bản liên quan của Đảng, Nhà nước.

Mạng máy tính chuyên dùng được hiểu là mạng máy tính sử dụng xử lý thông tin chứa bí mật nhà nước, được tách biệt với mạng máy tính kết nối Internet.

Trung tâm dữ liệu của cơ quan đảng (sau đây gọi tắt là Trung tâm dữ liệu) là nơi tập hợp các máy chủ; thiết bị mạng; các hệ thống thông tin, cơ sở dữ liệu, phần mềm ứng dụng, dịch vụ dùng chung; hệ thống sao lưu, bảo vệ dữ liệu tập trung; hệ thống kiểm soát, giám sát, bảo đảm an ninh mạng; hạ tầng hệ thống phụ trợ.

Hạ tầng kỹ thuật là tập hợp máy tính (máy chủ, máy trạm), thiết bị ngoại vi (USB, ổ cứng cắm ngoài, máy in, máy quét), thiết bị kết nối mạng, thiết bị chuyên dụng, các phần mềm hệ thống và các thiết bị phụ trợ (lưu điện, camera, chống sét, phát hiện, cảnh báo, phòng, chống cháy nổ), mạng nội bộ (LAN), mạng diện rộng (WAN).

Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập để phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

Dịch vụ dùng chung là các dịch vụ hạ tầng, nền tảng, phần mềm hay tiện ích số được triển khai tập trung, thống nhất để nhiều cơ quan, tổ chức khai thác và sử dụng.

Ứng dụng số dùng chung là hệ thống phần mềm, nền tảng hoặc dịch vụ số được xây dựng và triển khai tập trung, cho phép nhiều cơ quan, tổ chức trong cùng một hệ thống (hoặc trên phạm vi toàn quốc) cùng khai thác, sử dụng để thực hiện nhiệm vụ quản lý, điều hành, cung cấp dịch vụ công và chia sẻ dữ liệu.

Cơ sở dữ liệu là tập hợp các dữ liệu được sắp xếp, tổ chức để truy cập, khai thác, quản lý và cập nhật thông qua phương tiện điện tử.

Mã độc hại là một phần mềm máy tính được chèn một cách bí mật vào hệ thống với mục đích làm tổn hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống.

Xác thực đa yếu tố là cơ chế xác thực yêu cầu tối thiểu 2 (hai) yếu tố xác thực khác nhau để xác minh danh tính người sử dụng trước khi truy cập hệ thống thông tin.

Cấp độ an ninh mạng hệ thống thông tin được hiểu là cấp độ hệ thống thông tin.

An ninh mạng bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra, bảo đảm cho các hệ thống thực hiện đúng chức năng một cách sẵn sàng, ổn định và tin cậy; an ninh mạng bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng máy tính.

Nền tảng kết nối, liên thông mạng mật của các cơ quan trong hệ thống chính trị (gọi tắt: Nền tảng kết nối, liên thông mạng mật) là hạ tầng kỹ thuật (bao gồm cả phần cứng, phần mềm) dùng chung để thực hiện việc kết nối, tích hợp, chia sẻ dữ liệu, gửi nhận văn bản điện tử giữa các cơ quan trong hệ thống chính trị.

Điều 4. Nguyên tắc chung

1. Hệ thống mạng máy tính của Đảng trong Khung Kiến trúc số của các cơ quan đảng được thiết lập từ Trung ương đến cơ sở, phù hợp với mô hình tổ chức của các cơ quan, tổ chức đảng; bảo đảm thống nhất trong tổ chức, quản lý, kết nối và bảo đảm an ninh mạng, an ninh dữ liệu; việc quản lý, trao đổi, khai thác, lưu trữ thông tin của cơ quan, tổ chức đảng thông qua hạ tầng kỹ thuật, các hệ thống thông tin, cơ sở dữ liệu, phần mềm ứng dụng phải bảo đảm chất lượng, an toàn, bảo mật thông tin.

2. Các hạ tầng kỹ thuật, hệ thống thông tin, cơ sở dữ liệu, thiết bị đầu cuối khi kết nối vào hệ thống mạng máy tính của Đảng phải tuân thủ quy định về tiêu chuẩn, kỹ thuật, bảo đảm an ninh mạng, an ninh dữ liệu của Đảng, Nhà nước và Khung Kiến trúc số của các cơ quan đảng.

3. Không kết nối trực tiếp Mạng thông tin diện rộng của Đảng với Mạng Internet phục vụ cho cơ quan, tổ chức đảng. Chỉ thực hiện kết nối giữa hai mạng (Mạng thông tin diện rộng của Đảng với Mạng Internet) khi có tích hợp các giải pháp bảo mật cơ yếu và bảo đảm an ninh mạng được các cơ quan chức năng, có thẩm quyền xác nhận; việc trao đổi dữ liệu giữa hai phân hệ mạng này chỉ được thực hiện khi có giải pháp chuyển tiếp an toàn quy định tại Điểm c Khoản 1

Điều 5. Thiết bị đã kết nối với Mạng thông tin diện rộng của Đảng không được kết nối Mạng Internet, kể cả luân phiên và ngược lại.

4. Không sử dụng giải pháp truyền dẫn không dây để kết nối với mạng thông tin diện rộng của Đảng khi chưa có giải pháp bảo mật cơ yếu của Ban Cơ yếu Chính phủ và bảo đảm an ninh mạng theo quy định.

5. Các thiết bị công nghệ thông tin phải được kiểm tra an ninh, an toàn theo các quy định của Đảng và pháp luật của Nhà nước trước khi đưa vào sử dụng bởi cơ quan có thẩm quyền của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ.

6. Hoạt động bảo đảm an ninh mạng, an ninh dữ liệu phải được thực hiện thường xuyên, liên tục, kịp thời, hiệu quả và chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại mọi hành vi xâm phạm an ninh mạng.

7. Việc quản lý, sử dụng hệ thống phải tuân thủ nguyên tắc đúng thẩm quyền, chức năng, nhiệm vụ, phạm vi và thời gian; các hoạt động truy cập, quản trị, kết nối và giao dịch được ghi nhật ký, lưu vết phục vụ giám sát, kiểm tra và xử lý sự cố.

8. Việc thu thập, xử lý và sử dụng dữ liệu cá nhân trên hệ thống mạng máy tính của Đảng phải bảo đảm tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân, tôn trọng và bảo vệ quyền riêng tư hợp pháp của chủ thể dữ liệu.

9. Tuân thủ các tiêu chuẩn kỹ thuật, các yêu cầu về điện, điều hoà, phòng ốc, phòng, chống cháy, nổ để bảo đảm cho hệ thống hoạt động an toàn, ổn định, liên tục. Bảo đảm hệ thống điện dự phòng hoạt động 24/24h đến khi khôi phục lại điện lưới.

Chương II

TỔ CHỨC, QUẢN LÝ HỆ THỐNG MẠNG MÁY TÍNH CỦA ĐẢNG

Điều 5. Tổ chức, kết nối hệ thống mạng máy tính của Đảng

1. Hệ thống mạng máy tính của Đảng tổ chức thành 2 phân hệ mạng:

a) Mạng thông tin diện rộng của Đảng: Kết nối từ Trung ương đến địa phương và các tổ chức đảng (Trung ương, tỉnh uỷ/thành uỷ, đảng uỷ cấp xã/phường/đặc khu) sử dụng mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước với băng thông rộng, tốc độ cao đáp ứng yêu cầu chuyển đổi số, xử lý luồng nghiệp vụ, phục vụ công tác chuyên môn, chỉ đạo điều hành của lãnh đạo cấp uỷ các cấp. Hệ thống mạng máy tính này tích hợp các giải pháp bảo mật của Ban Cơ yếu Chính phủ và triển khai các giải pháp bảo đảm an ninh mạng đáp ứng yêu cầu triển khai các hệ thống thông tin, cơ sở dữ liệu có

chứa thông tin bí mật nhà nước (Tối mật đến các đảng uỷ trực thuộc Trung ương, tỉnh uỷ, thành uỷ, Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Chính phủ, Văn phòng Quốc hội, các ban đảng và đơn vị sự nghiệp của Trung ương; Mật đến đảng uỷ cấp xã/phường/đặc khu).

b) Mạng Internet phục vụ các cơ quan, tổ chức đảng: Có phạm vi kết nối rộng, phục vụ người dùng là cán bộ, công chức, viên chức, đảng viên, tổ chức đảng.

c) Dữ liệu liên thông giữa Mạng thông tin diện rộng của Đảng và Mạng Internet: Dữ liệu không thuộc phạm vi bảo vệ bí mật nhà nước truyền, nhận thông qua giải pháp chuyển tiếp an toàn, có kiểm soát, giám sát và được cơ quan có thẩm quyền thẩm định, xác nhận bảo đảm theo quy định của Luật An ninh mạng.

d) Các hệ thống thông tin, cơ sở dữ liệu, dịch vụ dùng chung triển khai tập trung tại Trung tâm dữ liệu của cơ quan đảng đặt tại Trung tâm dữ liệu quốc gia và trụ sở Văn phòng Trung ương Đảng.

2. Hệ thống Hội nghị truyền hình kết nối từ Trung ương đến cấp xã/phường/đặc khu sử dụng hạ tầng mạng truyền số liệu chuyên dùng; tích hợp giải pháp bảo mật của Ban Cơ yếu Chính phủ với phiên họp có nội dung mật.

3. Các mạng máy tính chuyên dùng khác được triển khai theo các mô hình riêng biệt, dựa trên các căn cứ đặc thù, đáp ứng yêu cầu thực hiện của cơ quan, tổ chức và do lãnh đạo cấp uỷ đơn vị đề xuất, lãnh đạo cấp uỷ quản lý xem xét, quyết định, đồng thời tuân thủ các quy định của pháp luật có liên quan và Khung Kiến trúc tổng thể quốc gia số, Khung Kiến trúc số của các cơ quan đảng.

Điều 6. Quản lý, vận hành hệ thống mạng máy tính của Đảng

1. Đối với Trung tâm dữ liệu của cơ quan đảng

a) Văn phòng Trung ương Đảng có trách nhiệm:

- Thiết lập khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định của Văn phòng Trung ương Đảng, Trung tâm dữ liệu quốc gia mới được phép vào khu vực Trung tâm dữ liệu. Quá trình vào, ra phải được ghi nhận vào nhật ký quản lý Trung tâm dữ liệu. Kiểm soát chặt chẽ tài khoản quản trị, tài khoản có quyền truy cập đặc quyền.

- Khi có sự cố mất điện lưới, phải bảo đảm hệ thống lưu điện, nguồn điện dự phòng (máy nổ) có đủ công suất để duy trì hoạt động của Trung tâm dữ liệu đến khi có điện lưới trở lại.

- Thiết lập cơ chế bảo vệ cho các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ; thường xuyên theo dõi, phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực.

- Triển khai các giải pháp hiện đại, đồng bộ để bảo đảm việc truyền nhận dữ liệu giữa mạng thông tin diện rộng của Đảng và Mạng Internet phục vụ các cơ quan, tổ chức đảng an toàn, an ninh, bảo mật dữ liệu.

- Xây dựng nội quy làm việc tại khu vực Trung tâm dữ liệu; phân công cán bộ thường xuyên giám sát thiết bị, hạ tầng của Trung tâm dữ liệu.

b) Cơ quan, tổ chức đảng thực hiện quản lý hệ thống thông tin sử dụng hạ tầng công nghệ thông tin trong Trung tâm dữ liệu có trách nhiệm xây dựng quy chế phối hợp với Văn phòng Trung ương Đảng quản lý, vận hành hệ thống; phân công đầu mối chịu trách nhiệm đối với hệ thống thông tin; tổ chức vận hành và bảo đảm an toàn, an ninh thông tin cho hệ thống thông tin của đơn vị mình; quản lý, sử dụng tài khoản đúng thẩm quyền, kịp thời thu hồi, điều chỉnh quyền truy cập khi người sử dụng thay đổi vị trí công tác, nghỉ việc hoặc không còn nhiệm vụ, quyền hạn liên quan.

2. Đối với mạng thông tin diện rộng của Đảng

a) Văn phòng Trung ương Đảng là cơ quan trực tiếp quản lý mạng thông tin diện rộng của Đảng, bảo đảm:

- Mạng thông tin diện rộng của Đảng được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an ninh mạng, an ninh dữ liệu riêng), bao gồm: Vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng bên ngoài, vùng mạng kết nối với các hệ thống mạng khác, vùng mạng chứa các cơ sở dữ liệu và vùng quản trị; vùng mạng phục vụ xử lý thông tin bí mật nhà nước và các vùng mạng khác theo yêu cầu chức năng của từng nhiệm vụ. Việc tổ chức, quản lý, kết nối và sử dụng các vùng mạng này phải đáp ứng, tuân thủ các điều kiện, yêu cầu bảo vệ của Luật Bảo vệ bí mật nhà nước, Luật An ninh mạng, Luật Cơ yếu và các quy định khác của pháp luật.

- Tổ chức giám sát dữ liệu trao đổi giữa các vùng mạng, việc giám sát thực hiện bởi hệ thống các thiết bị bảo mật và giám sát an ninh mạng; thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

- Hệ thống giám sát an ninh mạng được tổ chức thực hiện giám sát tập trung, liên tục theo chế độ 24/7.

b) Các cơ quan, đơn vị, tổ chức, cá nhân tham gia sử dụng Mạng thông tin diện rộng của Đảng có trách nhiệm:

- Không tiết lộ thiết kế, thông số cấu hình hệ thống mạng nội bộ cho tổ chức, cá nhân khác; không được phép truy cập bất hợp pháp vào các khu vực không được cấp quyền.

- Không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

- Các cơ quan, tổ chức đảng khi có kết nối trực tiếp vào mạng của Đảng với mục đích phục vụ công việc, chia sẻ dữ liệu phải tuân theo các quy định, các tiêu chuẩn kỹ thuật của Đảng, Nhà nước (các cơ quan, tổ chức đặc thù khi kết nối vào mạng của Đảng cần được sự đồng ý bằng văn bản của Văn phòng Trung ương Đảng).

3. Đối với Mạng Internet phục vụ các cơ quan, tổ chức đảng

a) Văn phòng Trung ương Đảng có trách nhiệm phối hợp với các đơn vị chuyên môn áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an ninh mạng trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: Có hệ thống tường lửa và hệ thống bảo vệ các vùng truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo (VPN) thông dụng, có phần cứng mã hoá tích hợp để tăng tốc độ mã hoá dữ liệu, có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

b) Cơ quan, đơn vị trong các cơ quan đảng thực hiện quản lý, triển khai các hệ thống thông tin sử dụng hạ tầng tại Trung tâm dữ liệu của cơ quan đảng có trách nhiệm phối hợp với Văn phòng Trung ương Đảng từ bước thiết kế hệ thống thông tin, triển khai đầy đủ các giải pháp an ninh mạng, kiểm tra và đánh giá an ninh mạng đáp ứng theo cấp độ quy định của Đảng, Nhà nước trước khi đưa hệ thống vào sử dụng; phối hợp với Văn phòng Trung ương Đảng trong xử lý nguy cơ, sự cố an ninh mạng đối với hệ thống thuộc phạm vi quản lý; khi được cấp tài khoản truy cập vào hệ thống qua mạng riêng ảo (VPN) phải tuân thủ các yêu cầu về xác thực, phân quyền, bảo mật và giám sát theo quy định.

c) Đối với các cá nhân có liên quan

Cá nhân sử dụng mạng máy tính có kết nối Internet, sử dụng tài khoản truy cập hệ thống phải tuân thủ quy định tại Quy chế này. Khi phát hiện các nguy cơ mất an ninh mạng, kịp thời thông báo cho cán bộ công nghệ thông tin, chuyển đổi số tại đơn vị mình để phối hợp xử lý.

Điều 7. Kết nối liên thông giữa các cơ quan trong hệ thống chính trị thông qua Nền tảng kết nối, liên thông mạng mật bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu

1. Nền tảng kết nối, liên thông mạng mật do Văn phòng Trung ương Đảng quản lý, vận hành.

Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chính phủ và Cơ quan Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam kết nối và gửi, nhận văn bản, dữ liệu có độ mật "Mật", "Tối mật" thông qua Nền tảng kết nối, liên thông mạng mật.

Các cơ quan, tổ chức của Đảng, Quốc hội, Chính phủ và Ủy ban Mặt trận Tổ quốc Việt Nam gửi, nhận văn bản, dữ liệu có độ mật "Mật", "Tối mật" cho nhau được thực hiện thông qua đầu mối kết nối do Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chính phủ và Cơ quan Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam quản lý, vận hành; không kết nối trực tiếp đến Nền tảng kết nối, liên thông mạng mật.

2. Hạ tầng kỹ thuật, an ninh mạng, bảo mật dữ liệu và bảo vệ bí mật nhà nước đối với hệ thống thuộc phạm vi quản lý của cơ quan mình tự bảo đảm theo quy định của pháp luật và Quy chế này.

3. Việc kết nối các hệ thống thông tin vào Nền tảng kết nối, liên thông mạng mật chỉ được thực hiện khi đáp ứng đầy đủ các yêu cầu về cấp độ an ninh mạng hệ thống thông tin, yêu cầu bảo đảm an ninh mạng, bảo mật thông tin, bảo vệ dữ liệu, xác thực, phân quyền truy cập, mã hoá đường truyền bằng giải pháp mật mã cơ yếu và các điều kiện kỹ thuật khác theo quy định của Đảng và Nhà nước.

4. Cơ quan gửi, cơ quan đầu mối kết nối, cơ quan quản lý, vận hành Nền tảng kết nối, liên thông mạng mật và cơ quan nhận chịu trách nhiệm trong phạm vi chức năng, nhiệm vụ, thẩm quyền được giao đối với việc kiểm tra điều kiện kết nối, gửi, nhận, bảo vệ dữ liệu, xác nhận kết quả gửi, nhận và phối hợp xử lý lỗi, sự cố, gián đoạn, tạm ngừng, khôi phục kết nối.

Chương III

SỬ DỤNG HỆ THỐNG MẠNG MÁY TÍNH CỦA ĐẢNG

Điều 8. Các dịch vụ hệ thống

1. Dịch vụ bảo đảm kết nối, trao đổi, khai thác và xử lý dữ liệu, gồm: Dịch vụ tên miền (DNS), thư điện tử, dịch vụ (Web), dịch vụ truyền tệp (FTP), các hệ quản trị cơ sở dữ liệu, dịch vụ hội nghị trực tuyến, dịch vụ kết nối mạng riêng ảo (VPN)...

2. Dịch vụ bảo đảm hạ tầng tính toán, lưu trữ trên đám mây (Cloud server, Cloud storage, Bigdata, DataLake,...).

3. Dịch vụ bảo đảm an ninh mạng cho hệ thống và bảo mật dữ liệu, gồm: Dịch vụ dịch chuyển địa chỉ IP (NAT), dịch vụ lưu giữ và cung cấp dữ liệu tại

chỗ (Caching), dịch vụ phát hiện và ngăn chặn truy nhập trái phép (IDS, Firewall), dịch vụ giám sát truy nhập mạng và ứng dụng, dịch vụ phòng, chống tấn công mạng cho ứng dụng web, dịch vụ bảo đảm an toàn cho máy chủ cơ sở dữ liệu, dịch vụ bảo đảm an ninh mạng cho hệ thống thư điện tử, dịch vụ sao lưu và khôi phục dữ liệu, dịch vụ phát hiện và diệt virus, dịch vụ chứng thực chữ ký số, dịch vụ quản lý và phân phối khoá mã, dịch vụ mật mã.

Điều 9. Cung cấp, quản lý, sử dụng dịch vụ hệ thống

1. Dịch vụ hệ thống chỉ được sử dụng để phục vụ việc quản lý hạ tầng kỹ thuật, vận hành, khai thác, sử dụng, bảo vệ và bảo mật các hệ thống thông tin, cơ sở dữ liệu, phần mềm ứng dụng.

2. Văn phòng Trung ương Đảng chủ trì, phối hợp với các cơ quan, đơn vị liên quan quản lý, vận hành, cung cấp tập trung các dịch vụ hệ thống dùng chung để sử dụng thống nhất trên mạng thông tin diện rộng của Đảng và Mạng Internet.

3. Bộ Khoa học và Công nghệ có trách nhiệm bảo đảm kết nối Mạng truyền số liệu chuyên dùng thông suốt từ Trung ương đến cấp tỉnh, xã, phường, đặc khu, đáp ứng yêu cầu về băng thông, chất lượng dịch vụ và an ninh mạng theo yêu cầu của các cơ quan đảng; vận hành dịch vụ hội nghị truyền hình từ Trung ương đến cấp tỉnh theo yêu cầu của Văn phòng Trung ương Đảng và các ban đảng ở Trung ương.

4. Ban Cơ yếu Chính phủ phối hợp cung cấp, quản lý, triển khai các sản phẩm mật mã cơ yếu, dịch vụ chứng thực chữ ký số chuyên dùng công vụ; hướng dẫn và kiểm tra chuyên môn đối với việc triển khai, quản lý, sử dụng, thay đổi, thu hồi và bảo vệ sản phẩm bảo mật của Ban Cơ yếu Chính phủ trên hệ thống mạng máy tính của Đảng; các sản phẩm phải đáp ứng các yêu cầu, tiêu chuẩn kỹ thuật phục vụ chuyển đổi số trong các cơ quan đảng.

5. Các cơ quan đảng ở Trung ương, các tỉnh uỷ, thành uỷ, đảng uỷ các xã, phường, đặc khu và các cơ quan, tổ chức tham gia mạng máy tính của Đảng có trách nhiệm phối hợp tổ chức cung cấp, quản lý, sử dụng các dịch vụ hệ thống trên mạng máy tính của cơ quan và Mạng thông tin diện rộng của Đảng theo Quy chế này; quản lý, sử dụng sản phẩm mật mã theo quy định.

6. Cán bộ, công chức, viên chức, đảng viên khi sử dụng các dịch vụ hệ thống theo nhiệm vụ được giao phải tuyệt đối tuân thủ những quy định về quản lý, sử dụng các dịch vụ hệ thống theo Quy chế này.

Điều 10. Các nền tảng số, ứng dụng số, dữ liệu số

1. Các nền tảng số, ứng dụng số, dữ liệu số phải phù hợp Khung Kiến trúc tổng thể quốc gia số và Khung Kiến trúc số của các cơ quan đảng; trước khi

triển khai phải được kiểm tra, thẩm định, đánh giá an ninh mạng, an ninh dữ liệu theo quy định.

2. Thông tin, dữ liệu có cấp độ "Mật", "Tối mật" chỉ được soạn thảo, trao đổi, xử lý và lưu trữ trên Mạng thông tin diện rộng của Đảng khi có giải pháp bảo mật của Ban Cơ yếu Chính phủ theo Luật Cơ yếu, tuân thủ theo Luật Bảo vệ bí mật nhà nước, Luật An ninh mạng và các quy định liên quan.

3. Tuân thủ quy trình, quy định kiểm tra, đánh giá định kỳ về an ninh mạng, an ninh dữ liệu, bảo mật theo quy định của pháp luật hiện hành.

4. Việc nghiên cứu, phát triển, cung cấp, quản lý và sử dụng các nền tảng, ứng dụng trí tuệ nhân tạo trong các cơ quan, tổ chức đảng phải bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước và dữ liệu theo quy định của pháp luật.

Điều 11. Cung cấp, quản lý, sử dụng các nền tảng số, ứng dụng số, dữ liệu số

1. Quy trình tổ chức thực hiện

a) Văn phòng Trung ương Đảng chủ trì hướng dẫn, phê duyệt danh mục, tiêu chuẩn kỹ thuật, phương án bảo đảm an ninh mạng các nền tảng số, ứng dụng số, dữ liệu số dùng chung và xây dựng danh mục hệ thống thông tin, cơ sở dữ liệu, phần mềm ứng dụng dùng chung của Đảng.

b) Các cơ quan, đơn vị chịu trách nhiệm xây dựng, quản lý, cập nhật và khai thác các hệ thống thông tin theo đúng Quy chế, tiêu chuẩn và hướng dẫn chung; ban hành quy trình thẩm định, nghiệm thu hệ thống trước khi đưa vào khai thác.

c) Bộ Công an chủ trì, phối hợp với Ban Cơ yếu Chính phủ trong kiểm tra, giám sát an ninh mạng; Ban Cơ yếu Chính phủ cung cấp, triển khai giải pháp mật mã cơ yếu phù hợp với cấp độ của hệ thống thông tin, độ mật của thông tin, tính chất dữ liệu và yêu cầu nghiệp vụ theo quy định.

2. Yêu cầu kỹ thuật và bảo mật

a) Trước khi đưa vào vận hành, khai thác

Hệ thống phải được kiểm tra, đánh giá an ninh mạng, phân loại cấp độ hệ thống thông tin; triển khai đầy đủ phương án bảo đảm an toàn theo cấp độ được phê duyệt theo các quy định và hướng dẫn của Đảng, Nhà nước.

b) Khi vận hành

- Chỉ phân quyền truy cập cho người dùng có trách nhiệm để thực hiện các nhiệm vụ theo thẩm quyền được giao.

- Cập nhật thường xuyên các bản vá lỗi bảo mật.
- Dữ liệu chứa thông tin bí mật nhà nước phải được mã hoá bằng sản phẩm mật mã chuyên dùng của ngành Cơ yếu.
- Định kỳ báo cáo, đánh giá hiệu quả khai thác, an ninh mạng, an ninh dữ liệu của các hệ thống.

3. Chủ quản hệ thống thông tin và xác định cấp độ hệ thống thông tin

Cơ quan, tổ chức được giao làm chủ quản hệ thống thông tin có trách nhiệm tổ chức xác định, lập, thẩm định, phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin theo thẩm quyền; tổ chức triển khai đầy đủ các biện pháp bảo vệ an ninh mạng tương ứng với cấp độ được phê duyệt và chịu trách nhiệm về công tác bảo đảm an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý theo quy định của pháp luật.

Chương IV **BẢO VỆ HỆ THỐNG MẠNG MÁY TÍNH CỦA ĐẢNG**

Điều 12. An ninh mạng, an ninh dữ liệu

1. Yêu cầu bảo đảm an ninh mạng, an ninh dữ liệu

a) Bảo đảm đầy đủ điều kiện hạ tầng kỹ thuật, giải pháp công nghệ, thường xuyên cập nhật thông tin, dữ liệu, các mẫu phân tích. Việc kết nối, thu thập, phân tích dữ liệu được tập trung nhằm phục vụ giám sát an ninh mạng cho hệ thống thông tin dùng chung của các cơ quan đảng.

b) Có khả năng phát hiện sớm, cảnh báo kịp thời, chính xác về các sự kiện, sự cố, dấu hiệu, hành vi, mã độc xâm phạm, nguy cơ, điểm yếu, lỗ hổng có khả năng gây mất an ninh mạng, an ninh dữ liệu đối với các hệ thống thông tin dùng chung cho các cơ quan đảng. Tăng cường an toàn cho các ứng dụng web bằng cập nhật các biện pháp bảo vệ mới nhất.

c) Bảo đảm năng lực tích hợp, xử lý và phân tích lượng dữ liệu lớn, liên tục; năng lực phân tích, phát hiện tấn công và đưa ra cảnh báo một cách chính xác, nhanh chóng và kịp thời.

d) Tăng cường khả năng phòng thủ trước các mối hiểm họa từ các truy cập vào/ra hệ thống được kiểm soát chặt chẽ tối đa.

đ) Thống kê tình hình tấn công vào các ứng dụng (số lỗi, kỹ thuật tấn công, tần suất, nguồn gốc tấn công), tra cứu thông tin phục vụ quá trình điều tra.

e) Hệ thống giám sát nhanh chóng phát hiện, đưa ra cảnh báo về các lỗ hổng bảo mật đặc biệt là các lỗi diện rộng. Thống kê về các lỗi bảo mật, các

điểm yếu trên mạng. Có dữ liệu thống kê nhanh theo lỗi bảo mật, nguồn địa chỉ IP, tổ chức...

g) Cung cấp báo cáo, thống kê hiện trạng an ninh mạng như: Phát hiện tấn công, lỗ hổng bảo mật, kết quả dò quét hệ thống được tự động hoá.

h) Các giải pháp hạ tầng và an ninh mạng giúp hệ thống bảo mật an toàn an ninh thông tin toàn diện, tránh khỏi các rủi ro và nguy cơ đã được đề cập.

i) Tăng cường ứng dụng công nghệ tiên tiến và các giải pháp kỹ thuật phù hợp để nâng cao năng lực theo dõi, thu thập, phân tích, phát hiện sự cố và điều phối, ứng phó sự cố trên toàn mạng lưới; bảo đảm có hệ thống lưu trữ log phục vụ công tác điều tra số khi có sự cố xảy ra.

k) Bảo đảm các điều kiện cho toàn bộ hệ thống hoạt động liên tục, sẵn sàng.

l) Bảo đảm hệ thống giám sát an ninh mạng được kết nối, chia sẻ thông tin giám sát với các cơ quan, đơn vị khác như Bộ Quốc phòng, Bộ Công an, Ban Cơ yếu Chính phủ.

2. Các tổ chức, cá nhân khi tham gia quản lý, vận hành, cập nhật, lưu giữ, trao đổi và khai thác thông tin, dữ liệu trên Mạng thông tin diện rộng của Đảng phải tuân thủ các quy định của Đảng, Nhà nước và pháp luật liên quan và các quy định sau:

a) Các hệ thống thông tin, cơ sở dữ liệu, phần mềm ứng dụng trên Mạng thông tin diện rộng của Đảng phải bảo đảm các yêu cầu về an ninh mạng, an ninh dữ liệu.

b) Thông tin, dữ liệu không thuộc bí mật nhà nước được áp dụng các biện pháp bảo vệ phù hợp với tính chất, mức độ nhạy cảm của dữ liệu, cấp độ của hệ thống thông tin và yêu cầu bảo đảm an ninh mạng, an ninh dữ liệu. Thông tin bí mật nhà nước cấp độ "Mật", "Tối mật" khi truyền đưa, lưu giữ trên Mạng thông tin diện rộng của Đảng phải được bảo vệ bằng mật mã cơ yếu; thông tin bí mật nhà nước độ "Tuyệt mật" thực hiện theo quy định về mạng liên lạc cơ yếu và các quy định có liên quan.

c) Cấm truy cập trái phép vào các hệ thống thông tin, cung cấp, sao chép, lưu giữ, trao đổi các dữ liệu không thuộc thẩm quyền; không được tiết lộ thông số, tài liệu kỹ thuật về mạng; phải có trách nhiệm quản lý, bảo vệ bí mật tài khoản, mật khẩu, thiết bị lưu giữ an toàn, thiết bị lưu khoá bí mật được cấp...

d) Cấm sử dụng hệ thống mạng máy tính của Đảng để lan truyền, phát tán các thông tin nhằm chống phá các chủ trương, đường lối, chính sách, pháp luật của Đảng và Nhà nước, lây nhiễm virus, gửi thư rác,...

đ) Việc sao chép dữ liệu từ máy tính kết nối Internet, các máy tính khác vào máy tính kết nối trong Mạng thông tin diện rộng của Đảng phải được thực hiện thông qua thiết bị hoặc giải pháp chuyển dữ liệu an toàn theo quy định của cơ quan có thẩm quyền; đồng thời, thiết bị và dữ liệu phải được kiểm tra, quét mã độc, bảo đảm an ninh mạng, an ninh dữ liệu trước khi sử dụng.

e) Không chụp, quay màn hình hoặc sử dụng USB, thiết bị lưu trữ và thiết bị cá nhân không được cấp phép để thực hiện hành vi sao chép, lưu trữ đối với tài liệu không được quyền tiếp cận; việc chuyển thông tin, dữ liệu từ Mạng thông tin diện rộng của Đảng ra Mạng Internet hoặc các mạng khác phải được kiểm soát chặt chẽ, thực hiện theo thẩm quyền; đối với thông tin, dữ liệu thuộc bí mật nhà nước thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước, pháp luật về cơ yếu và các quy định có liên quan.

Điều 13. An toàn hệ thống

1. Hạ tầng kỹ thuật phải tuân thủ các tiêu chuẩn kỹ thuật, công nghệ tiêu chuẩn quốc gia và quốc tế; phải được xây dựng, quản lý, vận hành, duy trì hoạt động, đáp ứng các yêu cầu kỹ thuật về điện, điều hoà, an toàn, an ninh mạng, bảo mật theo quy định của pháp luật và của Đảng.

2. Các mạng máy tính kết nối với mạng thông tin diện rộng của Đảng phải bảo đảm:

a) Thiết bị, phần mềm phải có nguồn gốc, xuất xứ rõ ràng; được cập nhật bản vá và phiên bản mới nhất.

b) Trước khi kết nối vào mạng thông tin diện rộng của Đảng phải được kiểm tra phần cứng, phần mềm về an ninh mạng và triển khai các giải pháp bảo mật theo quy định của Đảng và pháp luật.

c) Được rà soát, kiểm tra, đánh giá an ninh mạng định kỳ hằng năm và kịp thời bổ sung, điều chỉnh hoặc thay thế các giải pháp bảo vệ đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật và duy trì tính sẵn sàng của hệ thống.

3. Các hệ thống thông tin kết nối vào Mạng thông tin diện rộng của Đảng phải:

a) Được cấp có thẩm quyền đánh giá, xác nhận cấp độ hệ thống thông tin theo quy định.

b) Bảo đảm tính sẵn sàng cao, hoạt động ổn định, liên tục và bảo đảm người dùng có thể truy cập dịch vụ mọi lúc, mọi nơi, đúng phạm vi và quyền được cấp.

4. Đối với thông tin, dữ liệu ứng dụng, thông tin hệ thống, thông tin người dùng phải được thực hiện:

a) Sao lưu định kỳ.

b) Dữ liệu sao lưu phải xác định danh sách thông tin, dữ liệu và sao lưu bảo đảm quy tắc 3 - 2 - 1: 3 bản sao dữ liệu - 2 loại phương tiện lưu trữ khác nhau - 1 bản sao lưu ở vị trí địa lý khác.

c) Định kỳ kiểm tra kết quả sao lưu, bảo vệ, khôi phục dữ liệu. Quản lý sao lưu dự phòng tập trung bằng hệ thống và giải pháp quản lý lưu trữ tập trung. Giải pháp sao lưu, dự phòng giúp bảo vệ dữ liệu, phục hồi hoạt động khi hệ thống gặp sự cố, thiên tai, bị mã hoá dữ liệu trái phép.

5. Các thiết bị lưu giữ dữ liệu phải được quản lý, định kỳ kiểm kê hằng năm và tiêu huỷ theo đúng quy định của Luật Bảo vệ bí mật nhà nước.

6. Thiết lập, duy trì hệ thống phần mềm diệt virus, mã độc hại để phát hiện, ngăn chặn, xử lý kịp thời việc lây lan, tấn công của các loại virus, mã độc hại trên mạng thông tin diện rộng của Đảng.

7. Các máy chủ, máy trạm, máy tính xách tay trong Mạng thông tin diện rộng của Đảng phải được định danh, cài đặt phần mềm diệt virus, mã độc hại. Những máy tính khi phát hiện có virus, mã độc hại phải được tách khỏi mạng; phải diệt virus, mã độc hại và kiểm tra trước khi đưa vào sử dụng trong mạng.

8. Phần mềm diệt virus, mã độc hại phải được cập nhật thường xuyên, kịp thời các bản vá lỗi, các mẫu virus mới, mã độc hại mới.

9. Chủ động kiểm tra, phát hiện, kịp thời vá lỗi phần mềm hệ thống và phần mềm ứng dụng.

10. Triển khai các phương án bảo đảm an ninh mạng:

a) Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin theo quy định của pháp luật hoạt động truy cập, quản trị từ xa phải sử dụng kênh kết nối, sản phẩm hoặc giải pháp mật mã cơ yếu được tổ chức cơ yếu có thẩm quyền cung cấp, triển khai, quản lý theo quy định.

b) Phương án quản lý truy cập giữa các vùng mạng và phòng, chống xâm nhập sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc giải pháp phòng, chống xâm nhập lớp mạng.

c) Phương án phòng, chống tấn công mạng cho ứng dụng web; sử dụng giải pháp tường lửa ứng dụng web đối với các hệ thống thông tin theo quy định của pháp luật.

d) Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có).

đ) Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng giải pháp tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí theo quy định của pháp luật.

e) Phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương.

g) Phương án phòng, chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc giải pháp phòng, chống tấn công từ chối dịch vụ đối với các hệ thống trung tâm dữ liệu, điện toán đám mây, hệ thống định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí theo quy định của pháp luật.

h) Phương án bảo đảm an ninh mạng, an ninh dữ liệu cho hệ thống thư điện tử; sử dụng giải pháp bảo đảm an ninh mạng, an ninh dữ liệu cho hệ thống thư điện tử đối với hệ thống thư điện tử, đáp ứng tiêu chí theo quy định của pháp luật.

i) Phương án quản lý truy cập lớp mạng; sử dụng giải pháp quản lý truy cập lớp mạng đối với hệ thống mạng nội bộ, trung tâm giám sát điều hành an ninh mạng, đáp ứng tiêu chí theo quy định của pháp luật.

k) Phương án quản lý phần mềm phòng, chống mã độc trên máy chủ, máy tính người dùng, sử dụng giải pháp phòng, chống mã độc và/hoặc giải pháp phát hiện và phản ứng sự cố an ninh mạng trên thiết bị đầu cuối, có chức năng quản lý tập trung.

l) Phương án phòng, chống thất thoát dữ liệu; sử dụng giải pháp phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin theo quy định của pháp luật.

m) Có phương án quản lý rủi ro an ninh mạng, quản lý tài sản phần cứng, phần mềm và thông tin, quản lý cấu hình, quản lý nhật ký, quản lý tài khoản và quyền truy cập, quản trị ứng phó, khắc phục sự cố.

Điều 14. Xử lý sự cố máy tính, mạng máy tính

1. Công tác phối hợp xử lý sự cố mạng máy tính thực hiện theo quy định của Văn phòng Trung ương Đảng và các cơ quan chức năng của Bộ Quốc phòng, Bộ Công an, Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ.

2. Các cơ quan, tổ chức đảng xây dựng quy trình, phân công trách nhiệm, phối hợp khắc phục sự cố, bảo đảm sự cố được khắc phục trong thời gian ngắn nhất; giảm thiểu tối đa khả năng lặp lại sự cố.

3. Tăng cường đầu tư cơ sở vật chất kỹ thuật và bố trí cán bộ chuyên trách công nghệ thông tin, bảo đảm phòng ngừa, kịp thời phát hiện, nhanh chóng xử lý, khắc phục hậu quả sự cố.

4. Chuẩn hoá và diễn tập quy trình ứng phó sự cố để tăng tính thực tiễn cụ thể:

a) Ban hành quy định về phối hợp khắc phục, xử lý sự cố, cấp độ cảnh báo làm cơ sở cho các cơ quan, đơn vị thực hiện.

b) Tổ chức diễn tập định kỳ các kịch bản sự cố (ví dụ: Tấn công mã độc tổng tiền, tấn công từ chối dịch vụ, rò rỉ dữ liệu) với sự phối hợp của các đơn vị liên quan (Ban Cơ yếu Chính phủ, Bộ Công an, Bộ Quốc phòng) để bảo đảm khả năng phản ứng nhanh chóng và hiệu quả khi có sự cố thật.

5. Khi phát hiện sự cố máy tính, mạng máy tính, các cơ quan, tổ chức, cá nhân có trách nhiệm kịp thời thông báo cho đầu mối có thẩm quyền để phối hợp xử lý. Đối với sự cố nghiêm trọng, người có thẩm quyền phải thông báo ngay cho đơn vị chuyên trách (Cục Chuyển đổi số - Cơ yếu, Văn phòng Trung ương Đảng) để tổ chức phối hợp ứng phó, xử lý và báo cáo cơ quan có thẩm quyền theo quy định. Việc thông báo, báo cáo và phối hợp xử lý sự cố thực hiện theo quy trình xử lý sự cố và quy định có liên quan.

Chương V TỔ CHỨC THỰC HIỆN

Điều 15. Tổ chức thực hiện

1. Văn phòng Trung ương Đảng

a) Tổ chức hướng dẫn, thực hiện

- Văn phòng Trung ương Đảng có trách nhiệm hướng dẫn, kiểm tra thực hiện Quy chế; hướng dẫn việc bảo đảm kinh phí để thực hiện Quy chế.

- Bảo đảm các điều kiện về cơ sở vật chất, kinh phí để duy trì, vận hành Trung tâm dữ liệu của cơ quan đảng và Trung tâm điều hành, giám sát an ninh mạng của các cơ quan đảng.

- Quản lý, vận hành Nền tảng kết nối, liên thông mạng mật giữa các cơ quan trong hệ thống chính trị; hướng dẫn kết nối, ngắt kết nối; thực hiện giám sát, điều phối, ứng cứu sự cố. Định kỳ hoặc đột xuất tổ chức đánh giá việc tuân thủ các yêu cầu về kết nối, an ninh mạng, bảo mật thông tin và an ninh dữ liệu của các cơ quan tham gia.

- Chủ trì, phối hợp với các cơ quan đầu mối kết nối hướng dẫn quy trình gửi, nhận văn bản, dữ liệu qua Nền tảng kết nối, liên thông mạng mật; kiểm tra điều kiện kết nối; xác nhận việc gửi, nhận; xác định đầu mối phối hợp xử lý lỗi, gián đoạn, tạm ngừng và khôi phục kết nối. Quy định, hướng dẫn cụ thể về quy trình nghiệp vụ, phương thức xác nhận, chế độ lưu trữ nhật ký và phối hợp xử lý các tình huống phát sinh trong quá trình gửi, nhận văn bản, dữ liệu.

- Chỉ đạo, hướng dẫn các cơ quan, đơn vị thực hiện việc cập nhật, khai thác, sử dụng, trao đổi thông tin đúng quy định.

- Ban hành hoặc trình cấp có thẩm quyền ban hành các văn bản để việc ứng dụng công nghệ thông tin, chuyển đổi số được triển khai hiệu quả, thống nhất trong các cơ quan, tổ chức đảng.

- Ban hành quy chế phối hợp giữa Văn phòng Trung ương Đảng và các cơ quan đảng trong quản lý vận hành các hệ thống công nghệ thông tin, áp dụng thống nhất trong các cơ quan đảng.

- Văn phòng Trung ương Đảng xây dựng và ban hành quy định phối hợp khắc phục, xử lý sự cố, làm cơ sở cho các cơ quan, đơn vị thực hiện.

- Hằng năm, tổ chức kiểm tra, đánh giá định kỳ hoặc đột xuất khi có sự việc liên quan đến thực hiện Quy chế này và đề xuất xử lý các vi phạm theo quy định của Đảng, pháp luật của Nhà nước.

b) Tổ chức quản lý, vận hành

- Chịu trách nhiệm quản lý và vận hành: (1) Trung tâm dữ liệu của cơ quan đảng. (2) Trung tâm điều hành mạng (NOC) và giám sát an ninh mạng (SOC). (3) Mạng thông tin diện rộng của Đảng.

- Bảo đảm hạ tầng kỹ thuật cho Trung tâm dữ liệu của cơ quan đảng, mạng máy tính và trang thiết bị đầu cuối của Đảng uỷ các cơ quan Đảng Trung ương, các ban đảng ở Trung ương hoạt động ổn định, an toàn.

- Bố trí kinh phí, tổ chức bảo trì, bảo dưỡng, sửa chữa, nâng cấp trang thiết bị và các dịch vụ hệ thống, nền tảng số, ứng dụng số dùng chung tại Trung tâm dữ liệu của cơ quan đảng, Trung tâm điều hành, giám sát an ninh mạng.

- Chủ trì tổ chức các khoá đào tạo, tập huấn hằng năm về an ninh mạng; tổ chức diễn tập thực chiến về an ninh mạng và các chiến dịch nâng cao nhận thức an ninh mạng định kỳ; quản trị, vận hành các nền tảng số, ứng dụng số do Văn phòng Trung ương Đảng triển khai tập trung, dùng chung cho các cơ quan đảng.

2. Các cơ quan trong hệ thống chính trị khi tham gia kết nối, liên thông mạng mật

a) Phải tuân thủ các quy định tại Quy chế này và quy định của cơ quan đầu mối kết nối.

b) Các cơ quan tham gia kết nối có trách nhiệm phối hợp với Văn phòng Trung ương Đảng trong việc kiểm tra điều kiện kết nối, giám sát an ninh mạng, chia sẻ thông tin về nguy cơ, cảnh báo và sự cố; thực hiện các yêu cầu kỹ thuật nhằm bảo đảm Nền tảng kết nối, liên thông mạng mật hoạt động an toàn, thông suốt và ổn định.

c) Khi phát hiện sự cố hoặc nguy cơ có thể ảnh hưởng đến Nền tảng kết nối, liên thông hoặc các cơ quan khác, cơ quan phát hiện phải chủ động cô lập phạm vi ảnh hưởng, triển khai biện pháp xử lý ban đầu, thông báo ngay cho Văn phòng Trung ương Đảng và các cơ quan liên quan để phối hợp khắc phục; đồng thời không được che giấu, trì hoãn hoặc tự ý xóa bỏ dữ liệu, nhật ký phục vụ công tác điều tra, xác minh nguyên nhân sự cố.

3. Đảng uỷ Công an Trung ương

Chỉ đạo Bộ Công an chủ trì, phối hợp với Văn phòng Trung ương Đảng:

a) Thực hiện bảo đảm hạ tầng và các điều kiện cho Trung tâm dữ liệu của cơ quan đảng đặt tại Trung tâm dữ liệu quốc gia.

b) Tổ chức thực hiện kết nối liên thông, trao đổi, chia sẻ dữ liệu giữa cơ sở dữ liệu quốc gia về dân cư, cơ sở dữ liệu tổng hợp quốc gia, các hệ thống thông tin của Bộ Công an với hệ thống thông tin của cơ quan đảng.

c) Thẩm định, xây dựng giải pháp và hướng dẫn triển khai các biện pháp bảo đảm an ninh mạng, an ninh dữ liệu và bảo vệ bí mật nhà nước; hướng dẫn, kiểm tra, đánh giá an ninh mạng; tổ chức giám sát, cảnh báo, phát hiện và xử lý nguy cơ, sự cố an ninh mạng theo chức năng, nhiệm vụ; phát hiện, cảnh báo nguy cơ, hỗ trợ ứng cứu và phối hợp ứng cứu, điều tra, xử lý hành vi xâm phạm an ninh mạng theo quy định của pháp luật; tổ chức diễn tập an ninh mạng, tập huấn, đào tạo, bồi dưỡng cho cán bộ các cơ quan đảng về kiến thức, kỹ năng công nghệ thông tin, an ninh mạng.

4. Quân uỷ Trung ương

Chỉ đạo Bộ Quốc phòng phối hợp với Văn phòng Trung ương Đảng, Bộ Công an, Bộ Khoa học và Công nghệ nghiên cứu, triển khai các giải pháp kỹ thuật nhằm nâng cao khả năng bảo vệ hệ thống mạng máy tính của Đảng trước các nguy cơ, sự cố và hoạt động tấn công trên không gian mạng; tham gia ứng phó các tình huống an ninh mạng nghiêm trọng, hỗ trợ khắc phục sự cố kỹ thuật và chia sẻ thông tin, kinh nghiệm chuyên môn nhằm nâng cao năng lực bảo vệ hệ thống mạng máy tính của Đảng theo chức năng, nhiệm vụ được giao; tổ chức diễn tập phòng thủ, ứng cứu sự cố, tập huấn đào tạo, bồi dưỡng cho cán bộ các cơ quan đảng về kiến thức, kỹ năng an ninh mạng.

5. Đảng uỷ các cơ quan Đảng Trung ương và các cơ quan đảng ở Trung ương

a) Người đứng đầu cơ quan chịu trách nhiệm tổ chức thực hiện Quy chế; trực tiếp chỉ đạo, kiểm tra việc tổ chức, quản lý, sử dụng và bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thuộc phạm vi quản lý. Ban hành hoặc trình cấp có thẩm quyền ban hành các văn bản quy định, hướng dẫn các cơ quan, tổ chức đảng triển khai các nền tảng số, ứng dụng số, dữ liệu số; tổ chức rà soát quy trình, tái cấu trúc quy trình, phối hợp với Văn phòng Trung ương Đảng thực hiện nâng cấp, hoàn thiện các phần mềm.

b) Ban hành quy trình xử lý sự cố áp dụng cho đơn vị bảo đảm không bị gián đoạn công tác nghiệp vụ trong trường hợp các hệ thống liên quan, mạng thông tin diện rộng của các cơ quan đảng gặp sự cố.

c) Chịu trách nhiệm quản trị nội dung, vận hành và bảo đảm an ninh mạng, an ninh dữ liệu khi khai thác các hệ thống thông tin, phần mềm, ứng dụng của cơ quan mình được đặt tại Trung tâm dữ liệu của cơ quan đảng.

d) Thường xuyên rà soát, gửi danh sách cá nhân được giao quản trị các hệ thống thông tin cho Văn phòng Trung ương Đảng để quản lý và cấp tài khoản truy cập vào hệ thống. Quản lý quyền, tài khoản quản trị, quản lý người dùng thuộc đơn vị mình.

đ) Bố trí kinh phí đầu tư và sử dụng, bảo trì, sửa chữa, nâng cấp các trang thiết bị, phần mềm theo quy định.

e) Chỉ đạo các đơn vị, cán bộ, nhân viên thực hiện đúng các quy định, quy chế và hướng dẫn của Đảng, Nhà nước trong việc quản lý, cập nhật, khai thác sử dụng, trao đổi thông tin trên mạng máy tính.

g) Cử cán bộ chuyên trách chuyển đổi số thực hiện nhiệm vụ quản trị, vận hành, bảo đảm an ninh mạng, an ninh dữ liệu đối với các hệ thống thông tin, phần mềm, ứng dụng của đơn vị đặt tại Trung tâm dữ liệu của cơ quan đảng.

6. Các tỉnh uỷ, thành uỷ

a) Người đứng đầu cơ quan chịu trách nhiệm tổ chức thực hiện Quy chế; xây dựng, ban hành quy định cụ thể hoá quy chế, quy định cho cơ quan, tổ chức; trực tiếp chỉ đạo, kiểm tra việc tổ chức, quản lý, sử dụng và bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thuộc phạm vi quản lý; làm tốt công tác tuyên truyền, nâng cao nhận thức, phối hợp thực hiện Quy chế.

b) Giao văn phòng tỉnh uỷ, thành uỷ là đầu mối quản lý, phối hợp vận hành các hệ thống, nền tảng số, cơ sở dữ liệu dùng chung của Đảng được triển khai tại địa phương theo phân cấp; quản lý tài khoản, phối hợp hỗ trợ kỹ thuật và bảo đảm an ninh mạng trong phạm vi được giao.

c) Thường xuyên rà soát, gửi danh sách cá nhân được giao quản trị các hệ thống thông tin cho Văn phòng Trung ương Đảng để quản lý và cấp tài khoản truy cập vào hệ thống. Thực hiện quản lý quyền, tài khoản quản trị, quản lý người dùng thuộc đơn vị mình.

d) Bố trí kinh phí đầu tư và sử dụng, bảo trì, sửa chữa, nâng cấp các trang thiết bị, phần mềm theo quy định.

đ) Phối hợp quản lý, triển khai các hệ thống nền tảng số, ứng dụng số, dữ liệu số dùng chung của các cơ quan đảng bảo đảm thông suốt, an toàn.

e) Bảo mật tài khoản quản trị đối với các máy chủ, phần mềm ứng dụng, cơ sở dữ liệu của đơn vị mình. Bảo mật các thông tin của hệ thống mạng máy tính theo quy định.

g) Chủ trì tổ chức hoặc tham gia các lớp đào tạo, bồi dưỡng kiến thức, kỹ năng triển khai, sử dụng ứng dụng số.

h) Bảo đảm an ninh mạng và tham gia ứng cứu sự cố về an ninh mạng theo yêu cầu của Văn phòng Trung ương Đảng.

i) Ban hành quy trình xử lý sự cố áp dụng cho đơn vị bảo đảm không bị gián đoạn công tác nghiệp vụ trong trường hợp các hệ thống liên quan, mạng thông tin diện rộng của các cơ quan đảng gặp sự cố.

7. Đảng uỷ Bộ Khoa học và Công nghệ

Chỉ đạo Cục Bưu điện Trung ương bảo đảm kết nối, quản trị, vận hành Mạng truyền số liệu chuyên dùng thông suốt từ Trung ương đến cấp tỉnh, xã,

phường, đặc khu đáp ứng yêu cầu về băng thông, chất lượng dịch vụ và an ninh mạng theo yêu cầu của các cơ quan đảng; vận hành dịch vụ hội nghị truyền hình từ Trung ương đến cấp tỉnh theo yêu cầu của Văn phòng Trung ương Đảng và các ban đảng ở Trung ương.

8. Ban Cơ yếu Chính phủ

a) Chủ trì, phối hợp với Văn phòng Trung ương Đảng trong việc cung cấp, quản lý và triển khai các sản phẩm mật mã cơ yếu và dịch vụ chứng thực chữ ký số chuyên dùng công vụ để bảo vệ thông tin bí mật nhà nước và thông tin phục vụ lãnh đạo, chỉ đạo của Đảng.

b) Chủ trì, phối hợp với Văn phòng Trung ương Đảng trong việc triển khai giám sát an ninh, an toàn sản phẩm mật mã cơ yếu, các hệ thống thông tin cơ yếu, dịch vụ chứng thực chữ ký số chuyên dùng công vụ; chủ trì xác minh, đánh giá và xử lý các sự cố liên quan đến an toàn mật mã cơ yếu, sản phẩm mật mã cơ yếu, khoá mật mã, hệ thống thông tin cơ yếu và dịch vụ chứng thực chữ ký số chuyên dùng công vụ; phối hợp với Bộ Công an, Văn phòng Trung ương Đảng trong công tác bảo đảm an ninh mạng tổng thể.

c) Bố trí nguồn lực, phối hợp với Văn phòng Trung ương Đảng và các cơ quan, đơn vị liên quan kiểm định, đánh giá an toàn các hệ thống, nền tảng, dữ liệu dùng chung có sử dụng giải pháp bảo mật của Ban Cơ yếu Chính phủ trước khi đưa vào vận hành, sử dụng.

9. Đảng uỷ các xã, phường, đặc khu

a) Làm tốt công tác tuyên truyền, nâng cao nhận thức, phối hợp thực hiện quy chế, quy định; định kỳ hằng năm báo cáo tình uỷ, thành uỷ kết quả thực hiện và đề xuất, kiến nghị bổ sung, sửa đổi quy chế, quy định (nếu có).

b) Tổ chức đào tạo, tập huấn, hỗ trợ cho người sử dụng trong phạm vi cơ quan thực hiện các kỹ năng sử dụng máy tính an toàn.

c) Bảo đảm an ninh mạng và tham gia ứng cứu sự cố về an ninh mạng theo yêu cầu cấp trên.

d) Quản lý người dùng, bảo trì, sửa chữa, nâng cấp, bổ sung và thay thế các trang thiết bị, phần mềm theo quy định.

10. Các cơ quan khác liên quan

a) Quản trị, quản lý các dịch vụ mạng, tài nguyên, phần mềm hệ thống và thực hiện công tác bảo đảm an ninh mạng tại cơ quan, đơn vị.

b) Quản lý người dùng, bố trí kinh phí đầu tư và sử dụng, bảo trì, sửa chữa, nâng cấp các trang thiết bị, phần mềm theo quy định của Đảng, Nhà nước.

c) Ban hành các quy định, quy trình nội bộ, triển khai sử dụng các nền tảng số, ứng dụng số, dữ liệu số và các biện pháp bảo đảm an ninh mạng.

d) Tổ chức đào tạo, tập huấn, hỗ trợ cho người sử dụng trong phạm vi cơ quan thực hiện các kỹ năng sử dụng máy tính an toàn.

đ) Phối hợp bảo đảm an ninh mạng, tham gia ứng cứu sự cố về an ninh mạng theo yêu cầu của Văn phòng Trung ương Đảng.

11. Cá nhân

a) Chấp hành nghiêm túc Quy chế này, các quy định, quy trình nội bộ của cơ quan, đơn vị và các quy định của pháp luật hiện hành về bảo đảm an ninh mạng; trường hợp vi phạm thì tùy theo tính chất, mức độ phải chịu trách nhiệm và bị xử lý theo quy định của Đảng, pháp luật và quy định của cơ quan, đơn vị.

b) Quản lý, bảo quản thiết bị, tài khoản mà mình được giao sử dụng. Thường xuyên cập nhật, nâng cao kỹ năng sử dụng máy tính an toàn.

c) Sử dụng tài khoản được cấp đúng chức năng, nhiệm vụ của mình; bảo mật thông tin tài khoản của cá nhân, thông tin của hệ thống và thông tin của các tổ chức, cá nhân có liên quan.

d) Khi phát hiện sự cố hoặc dấu hiệu mất an ninh mạng phải thông báo ngay với đơn vị, cá nhân vận hành hệ thống thông tin để kịp thời xử lý.

đ) Tham gia nghiêm túc các chương trình đào tạo, bồi dưỡng về an ninh mạng.

12. Tổ chức, doanh nghiệp

Tổ chức, doanh nghiệp tham gia cung cấp sản phẩm, dịch vụ, giám sát, vận hành hệ thống mạng máy tính của Đảng có trách nhiệm tuân thủ các yêu cầu về bảo mật, bảo vệ thông tin, dữ liệu và an ninh mạng; thực hiện cam kết bảo mật đối với thông tin, dữ liệu được tiếp cận trong quá trình thực hiện nhiệm vụ và chịu trách nhiệm theo hợp đồng, thoả thuận bảo mật và các quy định của pháp luật có liên quan.

13. Chế độ báo cáo

Hàng năm, các cơ quan, đơn vị quy định tại Khoản 5, Khoản 6 và Khoản 10 Điều này có trách nhiệm báo cáo Văn phòng Trung ương Đảng tình hình khai thác, sử dụng các dịch vụ hệ thống, nền tảng số, ứng dụng số, dữ liệu số và an ninh mạng thuộc phạm vi quản lý, trước ngày 10/12 hằng năm để tổng hợp.

Điều 16. Điều khoản thi hành

1. Quy chế này có hiệu lực kể từ ngày ký. Quy chế này thay thế Quy chế số 07-QC/TW, ngày 31/10/2025 của Ban Bí thư về tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng.

2. Trường hợp các văn bản quy phạm pháp luật hoặc quy định được viện dẫn trong Quy chế này được sửa đổi, bổ sung, thay thế hoặc bãi bỏ thì việc áp dụng được thực hiện theo quy định đang có hiệu lực tại thời điểm áp dụng.

3. Trong quá trình tổ chức thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, tổ chức kịp thời phản ánh về Văn phòng Trung ương Đảng để tổng hợp, trình Ban Bí thư xem xét, bổ sung, sửa đổi.

Nơi nhận:

- Các đồng chí Ủy viên Ban Bí thư;
- Các đảng ủy trực thuộc Trung ương;
- Các cơ quan đảng ở Trung ương;
- Văn phòng: Chủ tịch nước, Chính phủ, Quốc hội;
- Các tỉnh ủy, thành ủy;
- Các đơn vị sự nghiệp của Trung ương;
- Lưu Văn phòng Trung ương Đảng.

T/M BAN BÍ THƯ**Trần Cẩm Tú**