TỈNH ỦY LÂM ĐỒNG
**BAN TỔ CHỨC**
*
Số 02 -QC/BTCTU

**ĐẢNG CỘNG SẢN VIỆT NAM**
*Lâm Đồng, ngày 20 tháng 4 năm 2026*

# QUY CHẾ
## tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Ban Tổ chức Tỉnh ủy

---

- Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;
- Căn cứ Luật Cơ yếu số 05/2011/QH13;
- Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;
- Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;
- Căn cứ Luật An ninh mạng số 24/2018/QH14;
- Căn cứ Luật Viễn thông số 24/2023/QH15;
- Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;
- Căn cứ Nghị định số 85/2016/NĐ-CP, ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
- 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;
- Căn cứ Quy chế số 07-QC/TU, ngày 09/3/2026 của Ban Thường vụ Tỉnh ủy Lâm Đồng về tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng;
- Căn cứ Quy chế làm việc số 01-QC/BTCTU, ngày 09/7/2025 của Ban Tổ chức Tỉnh ủy;

Xét đề nghị của Tổ kiêm nhiệm tham mưu, thực hiện về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số của cơ quan và của Văn phòng Ban,

Ban Tổ chức Tỉnh ủy ban hành Quy chế tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của cơ quan, cụ thể như sau:

## 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 Ban Tổ chức Tỉnh ủy để thống nhất áp dụng trong cơ quan 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 phòng, văn phòng trực thuộc Ban Tổ chức Tỉnh ủy *(gọi tắt là các phòng),* cá nhân có thiết bị, mạng máy tính kết nối, sử dụng hệ thống mạng máy tính của Đảng, tham gia cung cấp 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:

**1. 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.

**2. 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 cấp tỉnh đến cấp xã, phường, đặc khu, 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.

**3. 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.

**4. 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 toàn thông tin 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.

**5. 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.

**6. 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 toàn thông tin, an ninh mạng; hạ tầng hệ thống phụ trợ.

**7. 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).

**8. 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.

**9. 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.

**10. 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.

**11. 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.

**12. 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.

**13. An toàn thông tin:** 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 toàn thông tin 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.

**Điều 4. Nguyên tắc chung**

1. Hệ thống mạng máy tính của Đảng trong Kiến trúc chuyển đổi số trong các cơ quan Đảng theo Quyết định số 333-QĐ/TW, ngày 24/6/2025 được thiết lập từ Trung ương đến các xã, phường, đặc khu, 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 toàn thông tin; 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 toàn thông tin, an ninh mạng của Đảng, Nhà nước và Kiến trúc chuyển đổi số trong các cơ quan Đảng.

3. Không kết nối trực tiếp giữa mạng thông tin diện rộng của Đảng và mạng Internet của cơ quan Đảng. Chỉ thực hiện kết nối khi có các giải pháp bảo mật, bảo đảm an toàn, an ninh thông tin được các cơ quan chức năng xác nhận. Máy tính kết nối với mạng thông tin diện rộng của Đảng không được kết nối đồng thời hoặc luân phiên với mạng Internet 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 của Cơ yếu.

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.

6. Hoạt động bảo đảm an toàn thông tin, an ninh mạng 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 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.

8. Tuân thủ các tiêu chuẩn kỹ thuật, các yêu cầu về điện, phòng ốc, phòng, chống cháy, nổ để bảo đảm cho hệ thống hoạt động an toàn, ổn định, liên tục.

## CHƯƠNG II
## TỔ CHỨC, QUẢN LÝ HỆ THỐNG MẠNG MÁY TÍNH CỦA CƠ QUAN

### Điều 5. Tổ chức, kết nối hệ thống mạng máy tính của cơ quan

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

a) Mạng thông tin diện rộng của Đảng (mạng Intranet): kết nối từ Trung ương đến cấp tỉnh và Ban Tổ chức Tỉnh ủy sử dụng mạng truyền số liệu chuyên dùng phục vụ của cơ quan 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 ủy các cấp. Hệ thống mạng máy tính này tích hợp các giải pháp bảo mật của Ban Cơ yếu Chính phủ đáp ứng yêu cầu triển khai các hệ thống thông tin, cơ sở dữ liệu có chứa thông tin cấp độ từ "Tối mật" trở xuống *(Tối mật đến đảng ủy cấp tỉnh; Mật đến đảng ủy các 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 Intranet và mạng Internet: Dữ liệu giữa hai phân hệ mạng Intranet và Internet được truyền nhận theo các giải pháp bảo mật được cơ quan chức năng có thẩm quyền xác nhận, có kiểm soát, giám sát chặt chẽ và bảo đảm an toàn thông tin, an ninh mạng, bảo vệ thông tin bí mật nhà nước.

2. Hệ thống Hội nghị truyền hình kết nối từ Ban Tổ chức Trung ương đến Ban Tổ chức Tỉnh ủy và từ Ban Tổ chức Tỉnh ủy đến các đảng ủy trực thuộc Tỉnh ủy 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 ủy đơn vị đề xuất, lãnh đạo cấp ủy quản lý xem xét, quyết định, đồng thời tuân thủ các quy định pháp luật có liên quan và Khung kiến trúc chính phủ số Việt Nam, Kiến trúc chuyển đổi số trong các cơ quan Đảng.

**Điều 6. Quản lý, vận hành hệ thống mạng máy tính của cơ quan**

1. Đối với Trung tâm dữ liệu của Tỉnh ủy

Phối hợp với Văn phòng Tỉnh ủy xây dựng quy chế phối hợp quản lý, vận hành hệ thống, giao Tổ 57 cơ quan, chủ trì phối hợp với các phòng làm 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 cơ quan.

2. Đối với mạng thông tin diện rộng của Đảng

a) Tổ 57 cơ quan, chủ trì phối hợp với Văn phòng Ban 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 toàn thông tin 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 cơ sở dữ liệu và các vùng mạng khác theo yêu cầu chức năng của từng nhiệm vụ.

- 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 toàn, an ninh thông tin, 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.

b) Các phòng, 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 phòng 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 (khi kết nối vào mạng của Đảng cần được sự đồng ý bằng văn bản của Văn phòng Tỉnh ủy).

3. Đối với mạng Internet phục vụ hoạt động của cơ quan

a) Văn phòng Ban có trách nhiệm phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy và các đơn vị chuyên môn áp dụng các biện pháp kỹ thuật cần thiết đảm bảo an toàn thông tin 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 cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo (VPN) thông dụng, có phần cứng, mã hóa tích hợp để tăng tốc độ mã hóa 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 cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

b) Tổ 57 cơ quan và các phòng thực hiện quản lý, triển khai các hệ thống thông tin sử dụng hạ tầng tại Trung tâm dữ liệu của Tỉnh ủy có trách nhiệm phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy từ bước thiết kế hệ thống thông tin, kiểm tra và đánh giá an toàn thông tin đáp ứng yêu cầu theo cấp độ quy định của Đảng, Nhà nước trước khi đưa hệ thống vào sử dụng và các hệ thống thông tin sử dụng hạ tầng tại Trung tâm dữ liệu của Tỉnh ủy khi được cấp tài khoản truy cập vào hệ thống qua mạng riêng ảo (VPN).

c) Đối với các cá nhân

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 toàn, 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.

## CHƯƠNG III
## SỬ DỤNG HỆ THỐNG MẠNG MÁY TÍNH CỦA ĐẢNG

### Điều 7. 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 toàn thông tin, 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 toàn thông tin 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 8. 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 Ban chủ trì, phối hợp với Tổ 57 cơ 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. Văn phòng Ban phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng

Tỉnh ủy và Viettel Lâm Đồng, VNPT Lâm Đồng có trách nhiệm bảo đảm về dung lượng, tốc độ, chất lượng dịch vụ và an toàn thông tin của mạng truyền số liệu chuyên dùng, dịch vụ hội nghị trực tuyến theo yêu cầu.

4 Văn phòng Ban phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy tiếp nhận, sử dụng các giải pháp, sản phẩm về chứng thực chữ ký số, quản lý và phân phối khóa mật mã, thực hiện mã hóa, giám sát an toàn thông tin trên mạng thông tin diện rộng của Đảng, phù hợp với các ứng dụng công nghệ thông tin trong hoạt động của cơ quan.

5. Các phòng 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 cấp ủy theo Quy chế này; quản lý, sử dụng sản phẩm mật mã theo quy định.

6. Cán bộ, công 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 9. Các nền tảng số, ứng dụng số, dữ liệu số**

1. Các nền tảng số, ứng dụng số, dữ liệu số phải phù hợp Kiến trúc chuyển đổi số trong các cơ quan Đảng; trước khi triển khai phải được kiểm tra, thẩm định, đánh giá an toàn thông tin 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, tuân thủ theo Luật Bảo vệ bí mật nhà nước và các quy định liên quan.

3. Tuân thủ quy trình, quy định kiểm tra, đánh giá định kỳ về an toàn thông tin, bảo mật theo quy định của pháp luật hiện hành.

4. Cần cụ thể hoá các nội dung: Quy trình vận hành, bảo trì, nâng cấp hệ thống; trách nhiệm sao lưu, phục hồi dữ liệu; cơ chế giám sát, kiểm tra, đánh giá hiệu quả khai thác.

**Điều 10. Cung cấp, quản lý, sử dụng các nền tảng số, ứng dụng số, dữ liệu số**

1. Quy trình tổ chức thực hiện

a) Tổ 57 cơ quan, Văn phòng Ban phối hợp Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy triển khai, hướng dẫn, tiêu chuẩn kỹ thuật, phương án an toàn thông tin các nền tảng số, ứng dụng số, dữ liệu số và xây dựng danh mục hệ thống thông tin, cơ sở dữ liệu, phần mềm ứng dụng dùng chung của Đảng.

b) Các phòng 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.

c) Tổ 57 cơ quan, Văn phòng Ban phối hợp Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh kiểm tra, giám sát an toàn thông tin, cung cấp giải pháp bảo mật phù hợp với cấp độ của hệ thống thông tin.

2. Yêu cầu kỹ thuật và bảo mật

a) Trước khi triển khai

Hệ thống phải được kiểm tra, đánh giá an toàn thông tin, phân loại cấp độ an toàn; triển khai đầy đủ phương án bảo đảm an toàn thông tin 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 toàn thông tin của các hệ thống.

## CHƯƠNG IV
## BẢO VỆ HỆ THỐNG MẠNG MÁY TÍNH CỦA CƠ QUAN

### Điều 11. An toàn thông tin

1. Yêu cầu bảo đảm an ninh, an toàn thông tin

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 toàn thông tin 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 toàn thông tin mạng 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 hoạ 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 toàn thông tin 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) 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; sử dụng các công cụ AI và học máy để chủ động phát hiện sớm các hành vi gây mất an toàn thông tin mạng.

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 toàn thông tin 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 phòng, cán bộ, công chức 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 toàn thông tin.

b) Thông tin lưu giữ và trao đổi ở cấp độ "Thường" không phải mã mật; thông tin bí mật nhà nước cấp độ "Mật", "Tối mật" truyền đưa, lưu giữ trên hệ thống mạng máy tính của Đảng phải được mã hoá bằng mật mã của cơ yếu; thông tin bí mật nhà nước cấp độ "Tuyệt mật" phải gửi, nhận qua hệ thống mạng liên lạc cơ yếu.

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 bằng thiết bị lưu giữ an toàn của ngành Cơ yếu hoặc các thiết bị lưu trữ dữ liệu khác, với điều kiện các thiết bị này đã được cài đặt và bảo đảm giải pháp an toàn thông tin theo quy định của cơ quan chức năng có thẩm quyền; đồng thời phải được kiểm tra, quét mã độc, diệt virus (nếu có) trước khi sử dụng.

**Điều 12. 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, 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.

b) Trước khi kết nối vào mạng thông tin diện rộng của Đảng phải được kiểm tra về an toàn và được các cơ quan chức năng xác nhận.

c) Định kỳ được rà soát, kiểm tra, đánh giá, bổ sung hằng năm và thay thế để bảo đảm an toàn, bảo mật và tính sẵn sàng cao.

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 an toàn 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.

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 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 hủy 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 toàn mạng máy tính:

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; sử dụng giải pháp mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại Điểm c, Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP.

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 được quy định tại Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP.

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 quy định tại Khoản 3, Điều 9 Nghị định số 85/2016/NĐ-CP.

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 quy định tại Khoản 3, Điều 9 Nghị định số 85/2016/NĐ-CP.

h) Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng giải pháp bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử, đáp ứng tiêu chí quy định tại Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP.

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 toàn thông tin mạng, đáp ứng tiêu chí quy định tại Khoản 3, Điều 9 Nghị định số 85/2016/NĐ-CP.

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 toàn thông tin 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 quy định tại Điểm c, Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP.

**Điều 13. 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 Tỉnh ủy và các cơ quan chức năng của Công an tỉnh, Cục Chuyển đổi số - Cơ yếu, Văn phòng Trung ương Đảng.

2. Phân công Tổ 57 cơ quan, Văn phòng Ban phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy và đơn vị liên quan phối hợp khắc phục, xử lý 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 hóa và diễn tập quy trình ứng phó sự cố để tăng tính thực tiễn cụ thể:

- 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.

- Tổ chức diễn tập định kỳ các kịch bản sự cố (ví dụ: Tấn công mã độc, tống tiền, tấn công từ chối dịch vụ, rò rỉ dữ liệu) với sự phối hợp của các đơn vị liên quan để đảm bảo khả năng phản ứng nhanh chóng và hiệu quả khi có sự cố thật.

## CHƯƠNG V
## TỔ CHỨC THỰC HIỆN

**Điều 14. Tổ chức thực hiện**

**1. Tổ 57 cơ quan và Văn phòng Ban**

a) Tổ chức hướng dẫn, thực hiện

- Có trách nhiệm hướng dẫn, kiểm tra thực hiện Quy chế; dự toán kinh phí để thực hiện Quy chế (nếu có). Làm tốt công tác tuyên truyền, nâng cao nhận thức, phối hợp thực hiện Quy chế; định kỳ hàng năm báo cáo kết quả thực hiện và đề xuất, kiến nghị bổ sung, sửa đổi quy chế, quy định (nếu có).

- Yêu cầu, hướng dẫn các phòng thực hiện việc cập nhật, khai thác, sử dụng, trao đổi thông tin đúng quy định.

- Tham mưu lãnh đạo Ban Tổ chức Tỉnh ủy ban hành quy chế phối hợp giữa Văn phòng Tỉnh ủy trong quản lý, vận hành các hệ thống công nghệ thông tin, áp dụng thống nhất trong các cơ quan Đảng.

- Tham mưu lãnh đạo Ban Tổ chức Tỉnh ủy quy trình xử lý sự cố bảo đảm không bị gián đoạn công tác nghiệp vụ trong trường hợp các hệ thống liên quan, mạng thông tin diện rộng của cơ quan gặp sự cố *(sau khi Văn phòng Tỉnh ủy ban hành)*.

- Hàng năm, tổ chức kiểm tra các cơ quan, đơn vị về tổ chức, quản lý, sử dụng và bảo vệ hệ thống mạng máy tính của Đảng.

b) Tổ chức quản lý, vận hành

- Phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy đảm hạ tầng kỹ thuật và trang thiết bị đầu cuối của cơ quan *(theo lộ trình của tỉnh)*. Thường xuyên rà soát, gửi danh sách cá nhân được giao quản trị các hệ thống thông tin cho Văn phòng Tỉnh ủy để quản lý và cấp tài khoản truy cập vào hệ thống. Thực hiện quản lý quyền, tài khoản quản trị, quản lý người của cơ quan. Bảo mật tài khoản quản trị đối với phần mềm ứng dụng, bảo mật các thông tin của hệ thống mạng máy tính theo quy định.

- Hằng năm dự trù 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 cơ quan. Bố trí kinh phí bảo trì các trang thiết bị, phần mềm theo quy định.

- Tham mưu lãnh đạo Ban cử cán bộ, công chức tham gia các lớp đào tạo, bồi dưỡng kiến thức, kỹ năng triển khai, sử dụng ứng dụng số.

- Bảo đảm an toàn thông tin, an ninh mạng và tham gia ứng cứu sự cố về an

toàn thông tin theo yêu cầu của Văn phòng Tỉnh ủy.

- Phối hợp với Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy bảo đảm công tác quản trị, vận hành, khai thác mạng truyền số liệu chuyên dùng, dịch vụ hội nghị trực tuyến đáp ứng yêu cầu về băng thông, chất lượng dịch vụ và an toàn thông tin theo yêu cầu của các cơ quan Đảng.

- Phối hợp vơi Phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy tiếp nhận, triển khai các giải pháp bảo mật, xác thực ký số cho mạng thông tin diện rộng của Đảng; kiểm tra, giám sát an toàn thông tin, cung cấp giải pháp bảo mật phù hợp với cấp độ của hệ thống thông tin; xử lý các sự cố máy tính.

**2. Đối với các phòng và cá nhân trong cơ quan**

a) Đối với các phòng

Làm tốt công tác tuyên truyền, nâng cao nhận thức nhận thức của cán bộ, công chức và thực hiện nghiêm Quy chế này.

b) Đối với các cá nhân

- Chấp hành nghiêm túc các quy định, quy trình nội bộ của cơ quan và các quy định của pháp luật hiện hành về bảo đảm an toàn thông tin.

- 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.

- 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.

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

- Tham gia nghiêm túc các chương trình đào tạo, bồi dưỡng về an toàn thông tin.

**Điều 15. Điều khoản thi hành**

1. Quy chế này có hiệu lực kể từ ngày ký.

2. Trong quá trình tổ chức thực hiện, nếu có vướng mắc, phát sinh các phòng kịp thời phản ánh đến Tổ 57 cơ quan và Văn phòng để tổng hợp, trình lãnh đạo Ban Tổ chức Tỉnh ủy xem xét, bổ sung, sửa đổi./.

Nơi nhận:
- Văn phòng Tỉnh ủy,
- Các đồng chí lãnh đạo Ban,
- Tổ 57 cơ quan,
- Các phòng, văn phòng trực thuộc Ban,
- Toàn thể cán bộ, công chức cơ quan
- Lưu Văn phòng BTCTU.

**K/T TRƯỞNG BAN**
PHÓ TRƯỞNG BAN

ĐẢNG CỘNG SẢN VIỆT NAM
BAN TỔ CHỨC
TỈNH ỦY LÂM ĐỒNG

**Phạm Hữu Toàn**