BỘ QUỐC PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 107 /2024/TT-BQP	*Hà Nội, ngày 30 tháng 11 năm 2024*

THÔNG TƯ
Quy định quản lý và bảo đảm an toàn thông tin, an ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng

Căn cứ Luật Cơ yếu ngày 26 tháng 11 năm 2011;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 01/2024/NĐ-CP ngày 01 tháng 4 năm 2024 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Cơ yếu về hoạt động mật mã để bảo vệ thông tin bí mật nhà nước;

Căn cứ Nghị định số 01/2022/NĐ-CP ngày 30 tháng 11 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Quốc phòng;

Theo đề nghị của Tư lệnh Bộ Tư lệnh 86;

Bộ trưởng Bộ Quốc phòng ban hành Thông tư quy định quản lý và bảo đảm an toàn thông tin, an ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định về quản lý và bảo đảm an toàn thông tin, an ninh mạng, quyền hạn, trách nhiệm của các cơ quan, đơn vị, tổ chức, cá nhân trong quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng.

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với các cơ quan, đơn vị, tổ chức, cá nhân có liên quan đến quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng.

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. *An toàn thông tin, an ninh mạng* gồm an toàn thông tin mạng và an ninh mạng, trong đó:

a) An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin;

b) An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. *Máy tính Internet* là máy tính do các cơ quan, đơn vị quản lý, được phép kết nối với mạng Internet.

3. *Mạng Internet sử dụng trong các cơ quan, đơn vị* là mạng máy tính của các cơ quan, đơn vị được phép kết nối với mạng Internet.

4. *Máy tính quân sự* là máy tính phục vụ cho hoạt động quân sự, quốc phòng trong các cơ quan, đơn vị được phép kết nối với mạng máy tính quân sự.

5. *Mạng máy tính quân sự* là hệ thống mạng bao gồm mạng máy tính quân sự diện rộng và mạng máy tính quân sự nội bộ phục vụ chỉ đạo, điều hành, quản lý, chỉ huy, điều khiển vũ khí, trang bị kỹ thuật trong Bộ Quốc phòng.

6. *Người sử dụng* là sĩ quan, quân nhân chuyên nghiệp, công nhân và công chức, viên chức quốc phòng, lao động hợp đồng, hạ sĩ quan, binh sĩ; dân quân tự vệ, quân nhân dự bị trong thời gian tập trung, huấn luyện hoặc làm nhiệm vụ khác theo quy định của pháp luật; công dân được trưng tập vào phục vụ Quân đội được phép sử dụng máy tính quân sự, máy tính Internet.

7. *Dữ liệu điện tử quân sự* là dữ liệu điện tử chứa thông tin trong lĩnh vực quân sự.

8. *Vật mang dữ liệu điện tử* là thiết bị có khả năng lưu trữ dữ liệu điện tử, bao gồm: USB, thẻ nhớ, ổ cứng di động, đĩa CD, đĩa DVD, máy ghi âm, ghi hình, nghe nhạc, thiết bị di động thông minh và các thiết bị khác có khả năng lưu trữ, trao đổi dữ liệu điện tử.

9. *Bản ghi nhật ký điện tử (logfile)* là tập tin chứa các thông tin về lịch sử hoạt động của phần cứng, phần mềm.

10. *Mật khẩu phức tạp* là mật khẩu có ít nhất 8 ký tự, trong đó có các ký tự: Chữ cái viết hoa (A-Z), chữ cái viết thường (a-z), số (0-9), các ký tự đặc biệt khác trên bàn phím máy tính.

11. *Xoá dữ liệu an toàn* là việc sử dụng các phần mềm, thiết bị chuyên dụng để xoá dữ liệu nhằm bảo đảm không thể khôi phục dữ liệu.

12. *Cổng kết nối an toàn* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích trao đổi, chia sẻ dữ liệu giữa các hệ thống mạng nhằm kiểm soát, giám sát và bảo đảm an toàn thông tin, an ninh mạng.

13. *Thiết bị truyền dữ liệu một chiều (Datadiode)* là thiết bị chỉ cho phép truyền dữ liệu một chiều từ thiết bị truyền dữ liệu đến thiết bị nhận dữ liệu.

Điều 4. Nguyên tắc quản lý, bảo đảm an toàn thông tin, an ninh mạng

1. Phát triển hạ tầng, kết nối, ứng dụng, xây dựng cơ sở dữ liệu và bảo đảm kỹ thuật công nghệ thông tin phải bảo đảm an toàn thông tin, an ninh mạng.

2. Quản lý và bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, quản lý, vận hành, khai thác, sử dụng, nâng cấp, bảo dưỡng, sửa chữa và thanh lý, xử lý hệ thống thông tin, trang bị công nghệ thông tin; phải được thực hiện thường xuyên, liên tục, kịp thời, hiệu quả trên cơ sở tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn về an toàn thông tin, an ninh mạng.

3. Các hệ thống thông tin phải được phân loại theo cấp độ và có các giải pháp bảo đảm an toàn thông tin, an ninh mạng tương ứng với cấp độ đó.

4. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm về an toàn thông tin, an ninh mạng của cơ quan, đơn vị mình quản lý; người sử dụng phải được trang bị kiến thức và chịu trách nhiệm về an toàn thông tin, an ninh mạng đối với trang thiết bị được giao quản lý, sử dụng.

Điều 5. Các hành vi bị nghiêm cấm

1. Đưa trang bị công nghệ thông tin chưa được cơ quan chức năng kiểm tra an toàn thông tin, an ninh mạng vào sử dụng; sử dụng máy tính Internet, máy tính cá nhân, thiết bị di động thông minh hoặc vật mang dữ liệu điện tử khác có kết nối Internet để tạo lập, xử lý, lưu trữ, chuyển nhận dữ liệu điện tử quân sự, văn bản, tài liệu có nội dung không được hoặc chưa được phép phổ biến.

2. Truyền đưa thông tin thuộc danh mục bí mật nhà nước trên mạng mà không có giải pháp bảo mật cơ yếu.

3. Sử dụng vật mang dữ liệu điện tử không có giải pháp bảo đảm an toàn thông tin, an ninh mạng hoặc bảo mật để trao đổi thông tin, dữ liệu giữa máy tính quân sự với nhau và với các loại máy tính khác.

4. Kết nối mạng máy tính quân sự với các mạng khác mà không có biện pháp bảo đảm an toàn thông tin, an ninh mạng được Bộ Tư lệnh 86 thẩm định và Thủ trưởng Bộ Quốc phòng cho phép.

5. Cố ý gây mất an toàn thông tin, an ninh mạng của cơ quan, đơn vị và cá nhân.

6. Sử dụng giải pháp phòng chống mã độc cho trang thiết bị trên mạng máy tính quân sự không do Bộ Tư lệnh 86 cung cấp, thẩm định hoặc hướng dẫn.

7. Thực hiện hành vi vi phạm pháp luật có liên quan đến an toàn thông tin, an ninh mạng.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG
Mục 1
AN TOÀN THÔNG TIN, AN NINH MẠNG CHO DỮ LIỆU ĐIỆN TỬ QUÂN SỰ

Điều 6. An toàn thông tin, an ninh mạng cho dữ liệu điện tử quân sự không thuộc danh mục bí mật nhà nước

1. Dữ liệu điện tử quân sự chỉ được tạo lập, xử lý, lưu trữ trên máy tính kết nối mạng quân sự, máy tính kết nối mạng quân sự nội bộ, máy tính không kết nối mạng hoặc trang bị kỹ thuật dùng riêng có triển khai đầy đủ giải pháp bảo đảm an toàn thông tin, an ninh mạng theo quy định. Trường hợp tạo lập, xử lý, lưu trữ trên máy tính thuộc các mạng khác phải được sự đồng ý của chỉ huy cơ quan, đơn vị.

2. Dữ liệu điện tử quân sự không mật được phép chuyển, nhận qua mạng máy tính quân sự, sử dụng hệ thống ứng dụng, dịch vụ đã được cơ quan chức năng kiểm tra an toàn thông tin, an ninh mạng.

Điều 7. An toàn thông tin, an ninh mạng cho dữ liệu điện tử thuộc danh mục bí mật nhà nước

1. Dữ liệu điện tử thuộc danh mục bí mật nhà nước khi lưu trữ, chuyển nhận trên mạng phải có giải pháp bảo mật cơ yếu.

2. Hệ thống thông tin sử dụng để tạo lập, lưu trữ, chuyển nhận dữ liệu thuộc danh mục bí mật nhà nước phải đạt từ cấp độ 3 trở lên về bảo đảm an toàn thông tin theo cấp độ.

3. Máy tính quân sự khi tạo lập, lưu trữ, chuyển nhận dữ liệu điện tử thuộc danh mục bí mật nhà nước phải được Bộ Tư lệnh 86 triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng.

4. Máy tính quân sự có kết nối mạng dùng để lưu trữ, chuyển nhận dữ liệu điện tử chứa thông tin bí mật nhà nước phải được ngành Cơ yếu triển khai giải pháp bảo mật cơ yếu.

5. Máy tính quân sự không kết nối mạng dùng để lưu trữ dữ liệu điện tử chứa thông tin bí mật nhà nước phải tuân thủ pháp luật về bảo vệ bí mật nhà nước; được ngành Cơ yếu triển khai bảo mật khi có yêu cầu.

6. Xóa dữ liệu điện tử thuộc danh mục bí mật nhà nước phải sử dụng giải pháp xóa dữ liệu an toàn.

Điều 8. An toàn thông tin, an ninh mạng cho vật mang dữ liệu điện tử

1. Vật mang dữ liệu điện tử khi kết nối vào máy tính quân sự, mạng máy tính quân sự phải có giải pháp bảo đảm an toàn thông tin, an ninh mạng do cơ quan quản lý công nghệ thông tin hoặc cơ quan cơ yếu cấp phát, hướng dẫn.

2. Vật mang dữ liệu điện tử khi không còn nhu cầu sử dụng phải xóa dữ liệu an toàn hoặc trả lại cơ quan quản lý; khi thanh xử lý phải phá hủy bằng tác động vật lý.

3. Việc sử dụng thiết bị ghi âm, ghi hình trong hội họp thực hiện theo quy định của Bộ Quốc phòng và được sự đồng ý của người chủ trì hội nghị.

4. Phải xóa an toàn các dữ liệu điện tử quân sự lưu giữ trên vật mang dữ liệu điện tử trước khi kết nối với máy tính, trang bị có kết nối Internet.

Điều 9. Quản lý bản ghi nhật ký điện tử

1. Các cơ quan, đơn vị thực hiện thiết lập và lưu trữ các bản ghi nhật ký điện tử trên các hệ thống thông tin theo quy định tại hồ sơ đề xuất cấp độ an toàn thông tin; cung cấp bản ghi nhật ký điện tử cho cơ quan có thẩm quyền để giám sát, phân tích, đánh giá khi có yêu cầu.

2. Bản ghi nhật ký điện tử sự kiện (event log) cần ghi lại một số thông tin thiết bị như: địa chỉ mạng (IP), địa chỉ vật lý (MAC), mã định danh (ID) thiết bị và một số thông tin thời gian của hành động, như: đăng nhập hệ thống, tạo lập, cập nhật, sao chép hoặc xóa dữ liệu, các hành vi thiết lập cấu hình hệ thống, thay đổi quyền truy nhập hệ thống.

3. Cơ quan quản lý công nghệ thông tin thường xuyên duy trì việc theo dõi, phân tích bản ghi nhật ký điện tử của các hệ thống công nghệ thông tin và các sự kiện khác có liên quan để kịp thời phát hiện, ứng cứu sự cố an toàn thông tin, an ninh mạng.

Mục 2

AN TOÀN THÔNG TIN, AN NINH MẠNG CHO MÁY TÍNH

Điều 10. An toàn thông tin, an ninh mạng cho máy tính kết nối mạng máy tính quân sự

1. Sao chép dữ liệu điện tử quân sự giữa máy tính kết nối mạng máy tính quân sự với các loại máy tính khác thực hiện bằng một trong những giải pháp sau:

a) Sử dụng vật mang dữ liệu điện tử có cài đặt giải pháp bảo đảm an toàn thông tin do Bộ Tư lệnh 86 cung cấp, hướng dẫn;

b) Sử dụng USB bảo mật do Cục Cơ yếu/BTTM cấp phát;

c) Sử dụng đĩa CD, DVD (dùng một lần và hủy);

d) Giải pháp khác đã được Bộ Tư lệnh 86 xác nhận bảo đảm an toàn thông tin, an ninh mạng.

2. Tắt hoặc vô hiệu hóa các tính năng kết nối, truy nhập vào mạng không dây (Wifi, Bluetooth); khai báo định danh trên hệ thống giám sát, bao gồm thông tin người sử dụng, đơn vị, địa chỉ MAC, địa chỉ IP.

3. Cài đặt phần mềm bảo đảm an toàn thông tin, an ninh mạng do Bộ Tư lệnh 86 cung cấp, hướng dẫn, khuyến cáo sử dụng.

4. Thiết lập chính sách an toàn thông tin, an ninh mạng, tổ chức cập nhật cơ sở dữ liệu, cập nhật bản nâng cấp, bản vá lỗi cho các phần mềm theo hướng dẫn của Bộ Tư lệnh 86.

5. Máy tính trước khi đưa vào sử dụng phải được Bộ Tư lệnh 86 kiểm tra, đánh giá an toàn thông tin, an ninh mạng; dán tem bảo đảm an toàn thông tin, an ninh mạng; dán nhãn phân biệt mạng.

6. Khi chuyển đổi mục đích sử dụng thành máy tính Internet và ngược lại phải do cơ quan quản lý công nghệ thông tin xóa, hủy dữ liệu an toàn, kiểm tra an toàn thông tin, an ninh mạng và triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng theo quy định.

Điều 11. An toàn thông tin, an ninh mạng cho máy tính không kết nối mạng

1. Triển khai đầy đủ các giải pháp bảo đảm an toàn thông tin, an ninh mạng được quy định tại Điều 10 Thông tư này.

2. Dữ liệu điện tử thu thập từ máy tính có kết nối với các mạng máy tính khác phải tiến hành rà quét, kiểm tra an toàn thông tin bằng giải pháp phòng chống mã độc có phiên bản cập nhật theo quy định hoặc kiểm tra an toàn thông tin, an ninh mạng trước khi đưa vào lưu trữ, khai thác, sử dụng trong máy tính không kết nối mạng.

Điều 12. An toàn thông tin, an ninh mạng cho máy tính kết nối hệ thống vũ khí, trang bị kỹ thuật

1. Triển khai đầy đủ các giải pháp bảo đảm an toàn thông tin, an ninh mạng quy định tại Điều 10 Thông tư này.

2. Việc kết nối, trao đổi thông tin, dữ liệu giữa máy tính kết nối hệ thống vũ khí, trang bị kỹ thuật với thiết bị ngoại vi, vật mang dữ liệu điện tử hay các loại máy tính, trang bị công nghệ thông tin khác chỉ được thực hiện khi bảo đảm an toàn thông tin, an ninh mạng và chỉ huy cơ quan, đơn vị cho phép.

3. Tắt tính năng trao đổi dữ liệu qua cổng USB, ổ đĩa CD/DVD khi không sử dụng. Trường hợp cần mở cổng USB, ổ đĩa CD/DVD để kết nối, trao đổi dữ liệu điện tử phục vụ điều khiển, xử lý thông tin của hệ thống vũ khí, trang bị kỹ thuật quân sự với thiết bị khác phải được cấp có thẩm quyền cho phép và tắt hoặc vô hiệu hóa ngay sau khi kết thúc trao đổi dữ liệu.

Điều 13. An toàn thông tin, an ninh mạng cho máy tính kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước

1. Triển khai đầy đủ các giải pháp bảo đảm an toàn thông tin, an ninh mạng quy định tại Điều 10 Thông tư này.

2. Dữ liệu điện tử thu thập từ mạng Internet phải tiến hành rà quét, kiểm tra an toàn thông tin, an ninh mạng bằng phần mềm phòng chống mã độc hoặc công cụ kiểm tra an toàn thông tin, an ninh mạng trước khi đưa vào lưu trữ, khai

thác, sử dụng trong máy tính kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

3. Triển khai giải pháp giám sát an toàn thông tin, an ninh mạng do Bộ Tư lệnh 86 cung cấp hoặc khuyến cáo sử dụng; thiết lập, khai báo định danh cho máy tính kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước, bao gồm thông tin người sử dụng, đơn vị, địa chỉ MAC, địa chỉ IP.

4. Không kết nối máy tính kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước trong các trường hợp sau:

a) Với thiết bị ngoại vi qua mạng không dây, trừ trường hợp được Bộ Tư lệnh 86 kiểm tra và xác nhận bảo đảm an toàn thông tin, an ninh mạng;

b) Với mạng Internet;

c) Với máy tính Internet.

Điều 14. An toàn thông tin, an ninh mạng cho máy tính kết nối mạng phục vụ kinh doanh, sản xuất

1. Triển khai đầy đủ các giải pháp bảo đảm an toàn thông tin, an ninh mạng được quy định tại Điều 10 Thông tư này.

2. Dữ liệu điện tử thu thập từ mạng Internet phải tiến hành rà quét, kiểm tra an toàn thông tin, an ninh mạng bằng phần mềm phòng chống mã độc hoặc công cụ kiểm tra an toàn thông tin, an ninh mạng trước khi đưa vào lưu trữ, khai thác, sử dụng trong máy tính kết nối mạng phục vụ kinh doanh, sản xuất.

Điều 15. An toàn thông tin, an ninh mạng cho máy tính kết nối mạng Internet

1. Thiết lập chính sách an toàn thông tin, an ninh mạng, tổ chức cập nhật cơ sở dữ liệu, cập nhật bản nâng cấp, bản vá lỗi cho các phần mềm theo hướng dẫn của Bộ Tư lệnh 86.

2. Máy tính phải được kiểm tra an toàn thông tin, an ninh mạng; dán tem bảo đảm an toàn thông tin, an ninh mạng, dán nhãn phân biệt mạng; triển khai cài đặt, kết nối với các hệ thống giám sát an toàn thông tin, an ninh mạng do Bộ Tư lệnh 86 cung cấp hoặc khuyến cáo sử dụng.

Mục 3
AN TOÀN THÔNG TIN, AN NINH MẠNG CHO MẠNG MÁY TÍNH QUÂN SỰ

Điều 16. Bảo đảm an toàn thông tin, an ninh mạng cho mạng máy tính quân sự

1. Cơ quan, đơn vị khi triển khai xây dựng, khai thác, sử dụng mạng máy tính phải chấp hành quy định của Bộ Quốc phòng về xây dựng, quản lý, khai thác, sử dụng hạ tầng công nghệ thông tin.

2. Hệ thống mạng máy tính phải được thiết kế, lắp đặt theo mô hình mạng máy tính đáp ứng các yêu cầu về bảo đảm an toàn thông tin, an ninh mạng, gồm các nội dung sau:

a) Phân chia mạng máy tính thành các vùng mạng theo chức năng, cấp độ an toàn thông tin quy định tại Phụ lục I kèm theo Thông tư này;

b) Vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng;

c) Che giấu và tránh truy nhập trực tiếp từ bên ngoài vào các địa chỉ mạng bên trong;

d) Xây dựng phương án dự phòng về kết nối và thiết bị mạng đối với hệ thống mạng của các cơ quan, đơn vị trọng yếu, cơ mật;

đ) Định kỳ cập nhật bản nâng cấp và bản vá lỗi cho các thiết bị bảo đảm an toàn thông tin, an ninh mạng;

e) Triển khai các trang thiết bị mạng, thiết bị an toàn thông tin, an ninh mạng, hệ thống phòng, chống phần mềm độc hại, công cụ phân tích, quản trị mạng phải có bản quyền, có nguồn gốc, xuất xứ rõ ràng;

g) Tổ chức triển khai các biện pháp giám sát, theo dõi, phát hiện và ngăn chặn kịp thời các sự cố dẫn đến mất an toàn thông tin, an ninh mạng hoặc các hoạt động xâm phạm an toàn thông tin, an ninh mạng.

3. Máy tính dùng để kết nối mạng máy tính quân sự phải triển khai các giải pháp bảo đảm an toàn quy định tại Mục 2 Chương II của Thông tư này và được thiết lập, quản lý kết nối bằng địa chỉ MAC, địa chỉ IP.

Điều 17. Kiểm soát truy nhập người sử dụng

1. Cơ quan quản lý nhân sự có trách nhiệm thông báo cho cơ quan quản lý công nghệ thông tin khi có thay đổi về nhân sự, điều chuyển công tác, thôi việc hoặc nghỉ việc để thực hiện điều chỉnh, thu hồi, hủy bỏ quyền sử dụng của người sử dụng đối với hệ thống công nghệ thông tin.

2. Tài khoản quản trị hệ thống công nghệ thông tin phải do cơ quan quản lý công nghệ thông tin nắm giữ và phải tách biệt với tài khoản truy nhập người sử dụng.

3. Người sử dụng được cấp tài khoản truy nhập với định danh duy nhất để sử dụng máy tính, ứng dụng, dịch vụ của mạng máy tính. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị phải có cơ chế xác định cá nhân có trách nhiệm quản lý tài khoản.

4. Tài khoản truy nhập của người sử dụng trên các hệ thống thông tin phải thiết lập mật khẩu phức tạp và thực hiện đổi mật khẩu định kỳ hoặc ngay khi xảy ra sự cố an toàn thông tin, an ninh mạng.

Điều 18. Kiểm soát truy nhập mạng

1. Cơ quan quản lý công nghệ thông tin của các cơ quan, đơn vị thực hiện kiểm soát truy nhập mạng trong phạm vi quản lý.

2. Khi truy nhập từ xa phục vụ mục đích quản trị hệ thống phải thực hiện thông qua các mạng riêng ảo (VPN) và các giải pháp bảo đảm an toàn thông tin, an ninh mạng theo hướng dẫn của Bộ Tư lệnh 86. Hệ thống quản trị từ xa của các mạng dùng để truyền nhận, lưu giữ dữ liệu thuộc danh mục bí mật nhà nước phải được triển khai giải pháp bảo mật cơ yếu.

3. Các thiết bị chuyển mạch phải có khả năng quản lý cấu hình; tiến hành gắn địa chỉ MAC của các thiết bị được phép truy nhập mạng trên từng cổng của thiết bị chuyển mạch, tất cả các cổng trên thiết bị chuyển mạch chưa sử dụng phải được cấu hình vô hiệu hóa.

4. Triển khai các giải pháp kiểm soát truy nhập hệ thống mạng máy tính nhằm kiểm soát, quản lý người sử dụng và các trang bị công nghệ thông tin kết nối vào mạng máy tính.

Điều 19. Kiểm soát truy nhập ứng dụng, dịch vụ

1. Chỉ người được cấp quyền sử dụng mới được truy nhập vào ứng dụng, dịch vụ và thông tin liên quan. Quyền truy nhập phải được phân cấp, phân quyền phù hợp với đối tượng, mục đích, phạm vi sử dụng; vô hiệu hóa tài khoản ngay sau khi người sử dụng không thuộc đối tượng sử dụng.

2. Truy nhập hệ điều hành và ứng dụng phải được kiểm soát theo quy trình sử dụng; không truyền hoặc lưu giữ ở dạng bản rõ đối với các thông tin đăng nhập; sử dụng cơ chế xác thực đa yếu tố khi truy nhập hệ thống ở quyền quản trị.

3. Thiết lập thời gian phiên làm việc của ứng dụng, dịch vụ để ứng dụng tự động đóng lại sau một thời gian không hoạt động được quy định trước; phát hiện, cảnh báo đến người sử dụng về truy nhập bất thường; tạm thời khóa tài khoản khi phát hiện truy nhập vi phạm chính sách an toàn thông tin, an ninh mạng có thể gây nguy hại đến dữ liệu cá nhân hoặc hệ thống.

4. Khóa quyền truy nhập ứng dụng nếu đăng nhập năm (05) lần sai liên tiếp trong mười lăm (15) phút hoặc có áp dụng các biện pháp chống dò tìm mật khẩu, chặn đăng nhập tài khoản theo địa chỉ IP.

Điều 20. An toàn thông tin, an ninh mạng cho phần mềm

1. Máy tính chỉ được cài đặt phần mềm hệ thống, phần mềm ứng dụng do cơ quan chức năng cung cấp hoặc khuyến cáo sử dụng. Các phần mềm ứng dụng dùng chung, phần mềm chuyên ngành phải được Bộ Tư lệnh 86 hướng dẫn, kiểm tra an toàn thông tin, an ninh mạng và đồng ý đưa vào sử dụng.

2. Cơ quan quản lý công nghệ thông tin của cơ quan, đơn vị chịu trách nhiệm phân loại, cung cấp, phân quyền cài đặt phần mềm.

3. Phần mềm sử dụng trong máy tính quân sự phải thiết lập các chính sách về mật khẩu, quyền truy nhập, khóa tài khoản; các chức năng không sử dụng phải gỡ bỏ hoặc vô hiệu hóa.

4. Định kỳ cập nhật phiên bản nâng cấp và bản vá lỗi do Bộ Tư lệnh 86 cung cấp, hướng dẫn, khuyến cáo sử dụng hoặc kiểm tra an toàn thông tin, an ninh mạng đối với các phần mềm chuyên ngành.

Điều 21. An toàn thông tin, an ninh mạng cho cơ sở dữ liệu

1. Các hệ quản trị cơ sở dữ liệu được sử dụng phải có bản quyền hoặc có nguồn gốc, xuất xứ rõ ràng và được kiểm tra an toàn thông tin, an ninh mạng. Hệ quản trị cơ sở dữ liệu mật phải có khả năng tích hợp giải pháp xác thực, bảo mật.

2. Hệ quản trị cơ sở dữ liệu cho các hệ thống thông tin phải đáp ứng các yêu cầu sau:

a) Hoạt động ổn định;

b) Xử lý, lưu trữ được khối lượng dữ liệu lớn theo yêu cầu nghiệp vụ;

c) Có cơ chế bảo vệ và phân quyền truy nhập;

d) Rà soát bản vá, bản sửa lỗi hệ quản trị cơ sở dữ liệu tối thiểu 06 tháng 01 lần và thực hiện cập nhật nếu có phiên bản cập nhật hoặc ngay khi có khuyến cáo của nhà cung cấp hoặc cơ quan chức năng;

đ) Có phương án sao lưu, dự phòng đối với cơ sở dữ liệu, bảo đảm hệ thống hoạt động liên tục ngay cả khi có sự cố với cơ sở dữ liệu.

3. Cơ sở dữ liệu phải có các biện pháp kiểm soát truy nhập, cụ thể:

a) Thực hiện phân quyền và có quy định chặt chẽ với từng người sử dụng truy nhập cơ sở dữ liệu;

b) Ghi nhật ký điện tử sử dụng với các truy nhập cơ sở dữ liệu, các thao tác đối với cấu hình cơ sở dữ liệu;

c) Phải thay đổi mật khẩu mặc định tại thời điểm người sử dụng đăng nhập lần đầu; đóng tài khoản đối với những người không còn nhu cầu hoặc không còn thuộc phạm vi cung cấp;

d) Không sử dụng các nhóm quyền mặc định; các nhóm quyền phải được tạo lập và phân định bởi người quản trị cơ sở dữ liệu.

đ) Phải có giải pháp ngăn chặn các hình thức tấn công cơ sở dữ liệu.

Điều 22. An toàn thông tin, an ninh mạng cho máy chủ

1. Máy chủ phải được cấu hình riêng biệt về mặt logic hoặc vật lý để phục vụ cho từng ứng dụng và đặt tại khu vực được kiểm soát bảo đảm an ninh, an toàn vật lý và môi trường.

2. Bảo vệ máy chủ bằng các biện pháp sau:

a) Hệ điều hành và các ứng dụng phải được cập nhật thường xuyên, đúng phiên bản;

b) Gỡ bỏ hoặc vô hiệu hóa tất cả các dịch vụ, ứng dụng hoặc các giao thức không cần thiết chạy trên các máy chủ;

c) Xóa tất cả các tài khoản mặc định, tài khoản không sử dụng và không sử dụng cấu hình mặc định.

3. Phải triển khai các biện pháp kiểm soát truy nhập tới máy chủ ở mức vật lý và logic chặt chẽ; định kỳ thay đổi mật khẩu xác thực cho các công cụ quản trị. Mật khẩu mặc định của các công cụ quản trị phải được thiết lập lại, quản lý mật khẩu chặt chẽ, đúng đối tượng và sử dụng mật khẩu phức tạp.

4. Máy chủ phải được cài đặt tường lửa, phát hiện, ngăn chặn xâm nhập, hệ thống phòng, chống phần mềm độc hại và được cập nhật thường xuyên.

5. Khi chuyển giao hoặc thay đổi mục đích sử dụng máy chủ phải sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành. Việc xóa thông tin, dữ liệu, bảo đảm không thể khôi phục sau khi xóa.

Điều 23. An toàn thông tin, an ninh mạng cho ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự

1. Ứng dụng, dịch vụ chỉ được đưa vào hoạt động trên mạng máy tính quân sự khi được Bộ Tư lệnh 86 kiểm tra an toàn thông tin, an ninh mạng và bảo đảm an toàn thông tin, an ninh mạng.

2. Bản cập nhật, nâng cấp của ứng dụng, dịch vụ phải được cơ quan quản lý công nghệ thông tin kiểm tra an toàn thông tin, an ninh mạng.

3. Chủ quản của các ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự phải ban hành quy chế về quản lý, vận hành, khai thác và bảo đảm an toàn thông tin, an ninh mạng; tuân thủ kết nối an toàn và các chính sách an toàn thông tin, an ninh mạng.

Điều 24. Giám sát an toàn thông tin, an ninh mạng

1. Các cơ quan, đơn vị có trách nhiệm triển khai giải pháp giám sát an toàn thông tin, an ninh mạng thường xuyên, liên tục; phân tích, đánh giá, kịp thời cảnh báo, khắc phục sự cố an toàn thông tin, an ninh mạng.

2. Thông tin giám sát an toàn thông tin, an ninh mạng các hệ thống thông tin phục vụ hoạt động quân sự, quốc phòng phải được gửi về trung tâm giám sát an toàn thông tin, an ninh mạng tập trung của Bộ Tư lệnh 86.

Điều 25. An toàn thông tin, an ninh mạng cho trung tâm dữ liệu, phòng máy chủ

1. Các cơ quan, đơn vị chủ quản trung tâm dữ liệu, phòng máy chủ ban hành quy chế quản lý, vận hành, khai thác, sử dụng trung tâm dữ liệu, phòng máy chủ.

2. Triển khai giải pháp kiểm soát ra, vào khu vực trung tâm dữ liệu, phòng máy chủ. Việc ra, vào khu vực trung tâm dữ liệu, phòng máy chủ phải được sự

đồng ý của chỉ huy cơ quan, đơn vị và có sự giám sát của lực lượng quản lý, vận hành trung tâm dữ liệu, phòng máy chủ.

3. Việc triển khai, bổ sung hoặc thu hồi, đưa ra khỏi trung tâm dữ liệu, phòng máy chủ các trang thiết bị, ứng dụng, dịch vụ phải được sự đồng ý bằng văn bản của người chỉ huy cơ quan, đơn vị cấp trên trực tiếp của cơ quan quản lý trung tâm dữ liệu, phòng máy chủ.

4. Trung tâm dữ liệu, phòng máy chủ của cơ quan, đơn vị trực thuộc Bộ Quốc phòng phải đảm bảo ít nhất hai (02) đường truyền kết nối mạng để dự phòng, sẵn sàng ứng phó khi xảy ra sự cố.

Điều 26. An toàn thông tin, an ninh mạng khi sử dụng cổng kết nối an toàn

1. Bộ Tư lệnh 86 chủ trì, phối hợp với các cơ quan, đơn vị liên quan xây dựng, triển khai cổng kết nối an toàn phục vụ kết nối, chia sẻ dữ liệu giữa các hệ thống mạng; xây dựng yêu cầu kỹ thuật và hướng dẫn các cơ quan, đơn vị có nhu cầu kết nối triển khai thực hiện; tổ chức lực lượng chuyên trách giám sát thường xuyên, liên tục.

2. Các hệ thống thông tin khi có nhu cầu kết nối, chia sẻ dữ liệu giữa các hệ thống mạng qua Cổng kết nối an toàn phải đáp ứng quy định về bảo đảm an toàn hệ thống thông tin từ cấp độ 3 trở lên.

3. Hệ thống thông tin dùng để lưu trữ, truyền nhận thông tin thuộc danh mục bí mật nhà nước khi kết nối, chia sẻ dữ liệu với các hệ thống mạng khác qua cổng kết nối an toàn phải triển khai giải pháp phòng, chống lộ lọt dữ liệu do Bộ Tư lệnh 86 thẩm định, hướng dẫn.

4. Hệ thống thông tin sử dụng kết nối, chia sẻ dữ liệu với mạng truyền số liệu chuyên dùng của Đảng, Nhà nước phải qua cổng kết nối an toàn được Bộ Tư lệnh 86 triển khai, giám sát an toàn thông tin, an ninh mạng thường xuyên, liên tục, sẵn sàng ứng cứu, khắc phục sự cố.

5. Các cơ quan, đơn vị khi có nhu cầu kết nối, chia sẻ dữ liệu qua cổng kết nối an toàn phải được sự đồng ý của Bộ Quốc phòng.

Mục 4

AN TOÀN THÔNG TIN, AN NINH MẠNG CHO MẠNG MÁY TÍNH KẾT NỐI INTERNET

Điều 27. Quản lý, cung cấp và sử dụng mạng Internet

1. Căn cứ nhu cầu công tác, chỉ huy cơ quan, đơn vị trực thuộc Bộ Quốc phòng quyết định và chịu trách nhiệm về việc sử dụng Internet trong cơ quan, đơn vị thuộc quyền; tổng hợp gửi Bộ Tư lệnh 86 khi triển khai đăng ký mới vào báo cáo quý.

2. Cơ quan, đơn vị chỉ được kết nối mạng Internet bằng cáp mạng, sử dụng nhà cung cấp dịch vụ Internet theo hướng dẫn, khuyến cáo của cơ quan

chức năng về công nghệ thông tin, an toàn thông tin, an ninh mạng và kiểm soát số lượng kết nối, trừ trường hợp quy định tại các khoản 3, 4 Điều này.

3. Cơ quan, đơn vị không phải cơ quan, đơn vị trọng yếu, cơ mật có nhu cầu kết nối mạng Internet không dây cho cán bộ sử dụng trong phạm vi đơn vị phải đáp ứng các yêu cầu sau:

a) Thiết bị phần cứng đạt chuẩn 802.11n trở lên;

b) Áp dụng mã hóa dữ liệu truyền nhận sử dụng thuật toán mã hóa an toàn của thiết bị;

c) Người sử dụng khi sử dụng mạng không dây phải được cung cấp định danh duy nhất và xác thực qua kênh mã hóa; mật khẩu truy nhập mạng không dây phải sử dụng mật khẩu phức tạp và định kỳ thay đổi ít nhất 06 tháng 01 lần;

d) Triển khai giải pháp giám sát, phát hiện và ngăn chặn truy nhập trái phép;

đ) Được Bộ Tư lệnh 86 kiểm tra, đánh giá an toàn thông tin, an ninh mạng và đồng ý đưa vào sử dụng.

4. Chỉ huy các bệnh viện, học viện, nhà trường, viện nghiên cứu, doanh nghiệp trong quân đội quyết định tổ chức mạng Internet không dây cho khách ngoài quân đội sử dụng trong phạm vi đơn vị và phải bảo đảm an toàn thông tin, an ninh mạng quy định tại các điểm a, b, c, d khoản 3 Điều này.

5. Cơ quan, đơn vị khi sử dụng mạng Internet phải triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng. Thông tin giám sát phải gửi về trung tâm giám sát an toàn thông tin, an ninh mạng tập trung của Bộ Tư lệnh 86.

6. Truyền dữ liệu hạn chế một chiều giữa máy tính Internet và máy tính quân sự phải được thực hiện qua thiết bị truyền dữ liệu một chiều. Các cơ quan, đơn vị có nhu cầu sử dụng thiết bị truyền dữ liệu một chiều xây dựng phương án triển khai, được Bộ Tư lệnh 86 chủ trì, phối hợp với các cơ quan, đơn vị thẩm định và trình Bộ Quốc phòng phê duyệt.

Điều 28. Chống lộ lọt thông tin trên mạng Internet

1. Tên, tài khoản truy nhập của máy tính Internet hoặc tài khoản sử dụng trên mạng Internet phải sử dụng mật khẩu phức tạp, thực hiện đúng quy định về bảo vệ dữ liệu cá nhân thuộc phạm vi quản lý của Bộ Quốc phòng.

2. Cá nhân có trách nhiệm bảo vệ thông tin cá nhân của mình, thông tin đơn vị và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng.

3. Khi phát hiện thông tin quân sự bị lộ, lọt trên mạng Internet phải thông báo ngay với cơ quan quản lý công nghệ thông tin, cơ quan bảo vệ an ninh để kịp thời giải quyết.

4. Cơ quan quản lý công nghệ thông tin có trách nhiệm triển khai các giải pháp nhằm phát hiện và phối hợp ngăn chặn việc lộ, lọt thông tin trên mạng Internet.

Điều 29. An toàn thông tin, an ninh mạng các trang, cổng thông tin điện tử và ứng dụng, dịch vụ của Bộ Quốc phòng trên Internet

1. Các trang, cổng thông tin điện tử và ứng dụng của cơ quan, đơn vị thuộc Bộ Quốc phòng trên Internet phải được Bộ Tư lệnh 86 kiểm tra, đánh giá an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng.

2. Bộ Tư lệnh 86 chủ trì, phối hợp với Tập đoàn Công nghiệp – Viễn thông Quân đội thực hiện quản lý, vận hành, giám sát kỹ thuật, cảnh báo và triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng và ứng cứu khắc phục sự cố đối với các trang, cổng thông tin điện tử và ứng dụng, dịch vụ dùng chung.

Điều 30. Quản lý, sử dụng thư điện tử và tài khoản trên mạng Internet

1. Chỉ sử dụng tài khoản thư điện tử của cơ quan, đơn vị thuộc Bộ Quốc phòng hoặc cơ quan nhà nước để trao đổi thông tin liên quan đến thực hiện nhiệm vụ được giao.

2. Các cơ quan, đơn vị có nhu cầu xây dựng hệ thống thư điện tử riêng trên mạng Internet phải được Bộ Tư lệnh 86 thẩm định, báo cáo cấp có thẩm quyền quyết định để bảo đảm an toàn thông tin, an ninh mạng và tích hợp với hệ thống thư điện tử của Bộ Quốc phòng trên mạng Internet.

3. Người sử dụng trang thông tin điện tử cá nhân trên Internet, mạng xã hội phải chấp hành pháp luật về bảo vệ bí mật nhà nước, không tiết lộ thông tin cá nhân liên quan đến cơ quan, đơn vị, trừ trường hợp quy định tại khoản 4 Điều này.

4. Trường hợp sử dụng các trang mạng xã hội phục vụ hoạt động tuyên truyền, đấu tranh phản bác thông tin xấu, độc trên không gian mạng phải được sự cho phép, hướng dẫn của cơ quan có thẩm quyền.

Điều 31. Sử dụng mạng Internet phục vụ nhiệm vụ quân sự, quốc phòng

1. Bộ Tư lệnh 86 hướng dẫn, triển khai các giải pháp đảm an toàn thông tin, an ninh mạng trong triển khai hệ thống mạng Internet phục vụ nhiệm vụ quân sự, quốc phòng, như diễn tập, phòng chống dịch bệnh, các hoạt động phòng thủ dân sự và các nhiệm vụ khác được Bộ Quốc phòng giao.

2. Cơ quan, đơn vị khi có nhiệm vụ sử dụng mạng Internet và được sự nhất trí của cơ quan có thẩm quyền phải rà soát các trang bị công nghệ thông tin theo quy định tại Điều 15 Thông tư này trước khi đưa vào sử dụng.

Mục 5

AN TOÀN THÔNG TIN, AN NINH MẠNG TRONG PHÁT TRIỂN VÀ TRIỂN KHAI CÁC HỆ THỐNG THÔNG TIN

Điều 32. An toàn thông tin, an ninh mạng trong phát triển ứng dụng

1. Các cơ quan, đơn vị khi phát triển, triển khai các hệ thống thông tin phải tuân thủ các quy định, hướng dẫn về an toàn thông tin, an ninh mạng của Bộ Quốc phòng, ban hành quy chế bảo đảm an toàn cho hệ thống thông tin thuộc

phạm vi quản lý; phát triển ứng dụng và tổ chức cơ sở dữ liệu phải bảo đảm an toàn về kiến trúc, công nghệ và lập trình an toàn.

2. Căn cứ cấp độ an toàn thông tin của hệ thống, xác định phương án bảo đảm an toàn thông tin, an ninh mạng từ giai đoạn thiết kế ứng dụng.

3. Việc nhập, xuất dữ liệu thực hiện thủ công hay tự động phải được xác thực để đảm bảo tính đúng đắn, chính xác và thống nhất.

4. Ứng dụng phải có tính năng kiểm tra xác thực và tính toàn vẹn của thông tin để phát hiện mọi sự thay đổi do lỗi xử lý hay do hành động có chủ đích.

Điều 33. An toàn thông tin, an ninh mạng cho tập tin hệ thống

1. Phát triển phần mềm, mã nguồn của chương trình và thiết kế liên quan, thông số kỹ thuật, phải được kiểm soát chặt chẽ, ngăn chặn việc thêm vào những tính năng trái phép và những thay đổi khách quan; có giải pháp bảo vệ an toàn các tập tin hệ thống.

2. Quá trình phát triển phần mềm, dữ liệu kiểm thử được lựa chọn và bảo vệ; không sử dụng thông tin mật làm dữ liệu kiểm thử hoặc sao chép ra các thiết bị lưu trữ của nhà cung cấp.

Điều 34. An toàn thông tin, an ninh mạng trong phát triển, nâng cấp phần mềm

1. Phát triển, nâng cấp phần mềm phải thực hiện các yêu cầu về bảo đảm an toàn thông tin, an ninh mạng từ khi lập kế hoạch đến nghiệm thu, bảo đảm an toàn về kiến trúc, công nghệ và lập trình an toàn. Sau khi nâng cấp phần mềm hệ thống phải kiểm tra, đánh giá an toàn thông tin, an ninh mạng.

2. Thực hiện kiểm tra tính toàn vẹn cho hệ thống và tất cả phần mềm để đảm bảo phần mềm và việc cập nhật sau này không làm thay đổi các phần mềm đã cài đặt trước trong hệ thống, bao gồm cả hệ điều hành.

3. Chỉ các phần mềm bản quyền và được cấp phép mới được sử dụng để đảm bảo việc cập nhật và vá lỗi; không dùng các công cụ chưa được kiểm tra đánh giá an toàn thông tin, an ninh mạng cho phát triển sản phẩm.

4. Phát triển phần mềm ở các tổ chức, cá nhân ngoài quân đội phải được theo dõi, giám sát bởi cơ quan, đơn vị chủ quản phần mềm.

Điều 35. An toàn thông tin, an ninh mạng trong triển khai dự án và mua sắm trang thiết bị

1. Khi xây dựng các dự án công nghệ thông tin phải bố trí kinh phí cho nội dung bảo đảm an toàn thông tin, an ninh mạng và kiểm tra, đánh giá an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng.

2. Dự án công nghệ thông tin phục vụ hoạt động quân sự, quốc phòng phải được Bộ Tư lệnh 86 thẩm định, đánh giá an toàn thông tin, an ninh mạng trước khi phê duyệt, triển khai thực hiện.

3. Cơ quan, đơn vị tổ chức mua sắm các trang bị công nghệ thông tin phải đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin, an ninh mạng theo quy định; trang bị có chứa phần mềm nhúng phải yêu cầu nhà sản xuất, cung cấp thiết bị xác nhận bảo đảm an toàn thông tin, an ninh mạng hoặc cung cấp mã nguồn của phần mềm nhúng.

4. Cơ quan, đơn vị mua sắm trang bị vũ khí công nghệ cao, trang thiết bị có tích hợp thành phần công nghệ thông tin phải có sự tham gia của cơ quan quản lý công nghệ thông tin trong thương thảo, đàm phán, nghiệm thu mua sắm trang bị để bảo đảm về an toàn thông tin, an ninh mạng.

5. Các trang thiết bị, phần mềm, hệ thống vũ khí công nghệ cao, hệ thống thông tin phục vụ nhiệm vụ quân sự, quốc phòng phải được Bộ Tư lệnh 86 kiểm tra và dán tem "Đã kiểm tra an toàn thông tin, an ninh mạng" trước khi đưa vào sử dụng, ngay sau sửa chữa, hoán cải.

6. Chỉ được dán tem "Đã kiểm tra an toàn thông tin, an ninh mạng" khi các trang bị kỹ thuật, phần mềm bảo đảm an toàn thông tin, an ninh mạng theo quy định. Mẫu tem "Đã kiểm tra an toàn thông tin, an ninh mạng" thực hiện tại Phụ lục II kèm theo Thông tư này.

Điều 36. An toàn thông tin, an ninh mạng cho chuyển giao dịch vụ

1. Tuyển dụng hoặc thuê người ngoài quân đội vào làm việc trong các dự án phát triển công nghệ thông tin phải đúng quy trình, nguyên tắc tuyển chọn, tuyển dụng, thuê người vào phục vụ Quân đội và bảo đảm cam kết không tiết lộ thông tin.

2. Các cơ quan, tổ chức, cá nhân ngoài Quân đội chỉ được tham gia vào hoạt động cung cấp lắp đặt, đào tạo, sửa chữa, cấu hình, không được tham gia vào việc quản trị và vận hành các hệ thống thông tin phục vụ hoạt động quân sự, quốc phòng.

Điều 37. An toàn thông tin, an ninh mạng cho hội thi, hội thao, huấn luyện, diễn tập

1. Các trang thiết bị phục vụ hội thi, hội thao, huấn luyện, diễn tập phải được kiểm tra, đánh giá an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng.

2. Các máy trạm, máy chủ phục vụ hội thi, hội thao, huấn luyện, diễn tập phải được triển khai các chính sách bảo đảm an toàn thông tin, an ninh mạng, cài đặt giải pháp phòng chống mã độc của Bộ Quốc phòng.

3. Hệ thống công nghệ thông tin phục vụ hội thi, hội thao, huấn luyện, diễn tập phải được triển khai các giải pháp giám sát, bảo đảm an toàn thông tin, an ninh mạng, bao gồm: giám sát luồng, giám sát trang thiết bị, quản lý truy nhập, phòng chống mã độc.

4. Bộ Tư lệnh 86 tổ chức lực lượng kiểm tra, đánh giá và bảo đảm an toàn thông tin, an ninh mạng cho các hội thi, hội thao, huấn luyện, diễn tập do Bộ Quốc phòng tổ chức.

5. Các cơ quan, đơn vị trực thuộc Bộ Quốc phòng chịu trách nhiệm bảo đảm an toàn thông tin, an ninh mạng cho các hội thi, hội thao, huấn luyện, diễn tập do cấp mình hoặc các đơn vị thuộc quyền tổ chức. Trường hợp vượt quá khả năng thì đề nghị Bộ Tư lệnh 86 hỗ trợ bảo đảm an toàn thông tin, an ninh mạng.

Điều 38. An toàn thông tin, an ninh mạng đối với họp trực tuyến

1. Họp trực tuyến qua hệ thống mạng Internet

a) Máy tính kết nối họp trực tuyến phục vụ hoạt động quân sự, quốc phòng phải được cài giải pháp phòng chống mã độc trên Internet của Bộ Quốc phòng, dán nhãn phân biệt mạng;

b) Các trang thiết bị phục họp trực tuyến phải được kiểm tra, đánh giá an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng và làm sạch máy tính ngay sau khi sử dụng xong;

c) Bộ Tư lệnh 86 tổ chức kiểm tra, đánh giá và bảo đảm an toàn thông tin, an ninh mạng đối với họp trực tuyến do Bộ Quốc phòng tổ chức;

d) Các cơ quan, đơn vị trực thuộc Bộ Quốc phòng chịu trách nhiệm bảo đảm an toàn thông tin, an ninh mạng cho họp trực tuyến do cấp mình hoặc các đơn vị thuộc quyền tổ chức. Trường hợp vượt quá khả năng thì đề nghị Bộ Tư lệnh 86 hỗ trợ bảo đảm an toàn thông tin, an ninh mạng.

2. Họp trực tuyến qua hệ thống mạng quân sự

a) Chỉ sử dụng các trang thiết bị đang sử dụng trong hệ thống mạng quân sự; trường hợp sử dụng trang thiết bị khác phải kiểm tra, đánh giá an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng;

b) Các cơ quan, đơn vị tổ chức lực lượng công nghệ thông tin chủ trì bảo đảm an toàn thông tin, an ninh mạng; phối hợp với lực lượng thông tin bảo đảm đường truyền, sẵn sàng ứng cứu xử lý sự cố trong thời gian diễn ra hội nghị.

Mục 6
ỨNG CỨU SỰ CỐ VÀ XỬ LÝ VI PHẠM VỀ AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 39. Điều phối và ứng cứu sự cố

1. Hoạt động điều phối, ứng cứu sự cố an toàn thông tin, an ninh mạng là hoạt động thuộc phạm vi công tác an toàn thông tin, an ninh mạng.

2. Điều phối và ứng cứu sự cố an toàn thông tin, an ninh mạng thực hiện theo quy định tại Thông tư số 45/2020/TT-BQP ngày 27/4/2020 của Bộ trưởng Bộ Quốc phòng quy định về điều phối và ứng cứu sự cố an toàn thông tin, an ninh mạng trong Bộ Quốc phòng.

Điều 40. Thu thập, phân tích dữ liệu xác định vi phạm về an toàn thông tin, an ninh mạng

1. Việc thu thập, phân tích, xác định vi phạm về an toàn thông tin, an ninh mạng do cơ quan quản lý công nghệ thông tin phối hợp với cơ quan bảo vệ an ninh của đơn vị thực hiện.

2. Các cơ quan, đơn vị, cá nhân có trách nhiệm bảo vệ chứng cứ và phối hợp, tạo điều kiện cho cơ quan chức năng trong hoạt động thu thập, phân tích, xác định, chứng minh vi phạm về an toàn thông tin, an ninh mạng.

3. Trong trường hợp sự cố về an toàn thông tin, an ninh mạng có liên quan đến vi phạm pháp luật thì cơ quan, đơn vị liên quan có trách nhiệm cung cấp chứng cứ cho cơ quan điều tra theo quy định của pháp luật.

Điều 41. Xác định nguyên nhân mất an toàn thông tin, an ninh mạng

1. Cơ quan quản lý công nghệ thông tin chủ trì, phối hợp với các cơ quan liên quan thu thập, phân tích chứng cứ số, dữ liệu điện tử được thực hiện trong trường hợp có dấu hiệu mất an toàn thông tin, an ninh mạng.

2. Khi có dấu hiệu mất an toàn thông tin, an ninh mạng, cơ quan quản lý công nghệ thông tin triển khai các biện pháp sau:

a) Sử dụng các biện pháp công nghệ, kỹ thuật để xác định nguyên nhân mất an toàn thông tin, an ninh mạng;

b) Cung cấp kết quả xác định nguyên nhân mất an toàn thông tin, an ninh mạng cho cơ quan chức năng thuộc Bộ Quốc phòng khi có yêu cầu;

c) Tiếp nhận các trang, thiết bị kỹ thuật và sử dụng các biện pháp công nghệ, kỹ thuật để khôi phục thông tin và hỗ trợ điều tra, xác minh chứng cứ theo yêu cầu của cơ quan điều tra.

3. Điều tra chứng cứ số trong hoạt động điều tra tội phạm thực hiện theo quy định của pháp luật.

Điều 42. Xử lý vi phạm trong lĩnh vực an toàn thông tin, an ninh mạng

Tổ chức, cá nhân thực hiện hành vi vi phạm pháp luật về quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng thì tùy tính chất, mức độ vi phạm mà bị xử lý kỷ luật hoặc xử phạt vi phạm hành chính, xử lý hình sự theo quy định.

Chương III

QUẢN LÝ AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 43. Phân loại hệ thống thông tin theo cấp độ an toàn thông tin

1. Phân loại và tiêu chí xác định cấp độ

a) Các hệ thống thông tin phải được phân loại trên cơ sở tiêu chí xác định cấp độ an toàn thông tin để triển khai giải pháp bảo đảm an toàn hệ thống thông tin phù hợp;

b) Tiêu chí xác định cấp độ; hồ sơ đề xuất cấp độ, phương án bảo đảm an toàn thông tin thực hiện theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01

tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Thẩm quyền, trình tự, thủ tục xác định cấp độ

a) Đối với hệ thống thông tin được đề xuất cấp độ 1, cấp độ 2:

Cơ quan quản lý về công nghệ thông tin chủ trì, phối hợp với các cơ quan đơn vị lập hồ sơ đề xuất, thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

Cơ quan, đơn vị trực thuộc Bộ Quốc phòng phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin.

b) Đối với hệ thống thông tin được đề xuất cấp độ 3:

Cơ quan, đơn vị trực thuộc Bộ Quốc phòng lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin; gửi hồ sơ điện tử (đối với các hồ sơ được xác định không thuộc danh mục bí mật nhà nước) hoặc 01 (một) bộ hồ sơ giấy (đối với các hồ sơ được xác định thuộc danh mục bí mật nhà nước) về Bộ Tư lệnh 86 để tổ chức thẩm định;

Trong thời hạn 10 (mười) ngày, Bộ Tư lệnh 86 chủ trì, phối hợp với các cơ quan, đơn vị liên quan thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

Trên cơ sở kết quả thẩm định hồ sơ đề xuất cấp độ của Bộ Tư lệnh 86, cơ quan, đơn vị trực thuộc Bộ Quốc phòng phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin.

c) Đối với hệ thống thông tin được đề xuất cấp độ 4:

Cơ quan, đơn vị trực thuộc Bộ Quốc phòng lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin; gửi 01 (một) bộ hồ sơ giấy về Bộ Tư lệnh 86 để tổ chức thẩm định;

Trong thời hạn 15 (mười lăm) ngày, Bộ Tư lệnh 86 chủ trì phối hợp với các cơ quan, đơn vị liên quan thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

Cơ quan, đơn vị trực thuộc Bộ Quốc phòng trình Bộ Quốc phòng (qua Bộ Tư lệnh 86) phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin.

d) Đối với hệ thống thông tin được đề xuất cấp độ 5 (hệ thống thông tin quan trọng quốc gia):

Cơ quan, đơn vị trực thuộc Bộ Quốc phòng lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin; gửi 01 (một) bộ hồ sơ giấy về Bộ Tư lệnh 86 để tổ chức thẩm định;

Trong thời hạn 20 (hai mươi) ngày, Bộ Tư lệnh 86 chủ trì phối hợp với các cơ quan, đơn vị liên quan thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

Cơ quan, đơn vị trực thuộc Bộ Quốc phòng trình Bộ Quốc phòng (qua Bộ Tư lệnh 86) phê duyệt phương án bảo đảm an toàn thông tin; trình Bộ Quốc phòng báo cáo Thủ tướng Chính phủ phê duyệt danh mục hệ thống thông tin quan trọng quốc gia.

Điều 44. Xác lập Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Hệ thống thông tin quan trọng về an ninh quốc gia được xác lập theo quy định tại Điều 3 Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng.

2. Bộ Tư lệnh 86 chủ trì, phối hợp với các cơ quan, đơn vị liên quan hướng dẫn lập hồ sơ, tiếp nhận và thẩm định hồ sơ; tham mưu Bộ trưởng Bộ Quốc phòng đưa hệ thống thông tin quân sự, quốc phòng vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 45. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin, an ninh mạng

1. Tiêu chuẩn an toàn thông tin, an ninh mạng trong lĩnh vực quân sự, quốc phòng bao gồm tiêu chuẩn hệ thống thông tin, phần cứng, phần mềm và hệ thống quản lý, vận hành an toàn thông tin, an ninh mạng.

2. Quy chuẩn kỹ thuật về an toàn thông tin, an ninh mạng trong lĩnh vực quân sự, quốc phòng bao gồm quy chuẩn kỹ thuật đối với hệ thống thông tin, phần cứng, phần mềm và hệ thống quản lý, vận hành an toàn thông tin, an ninh mạng.

3. Trường hợp chưa có tiêu chuẩn, quy chuẩn kỹ thuật quy định tại khoản 1, khoản 2 Điều này thì áp dụng tiêu chuẩn quốc gia hoặc tiêu chuẩn quốc tế mà Việt Nam là thành viên.

Điều 46. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng

1. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng bao gồm kiểm tra việc chấp hành quy định về quản lý, khai thác, vận hành, sử dụng và bảo dưỡng, sửa chữa trang bị kỹ thuật tại các cơ quan, đơn vị.

2. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng đối với trang bị phần cứng, phần mềm được thực hiện trước, trong và sau khi sử dụng. Tem "Đã kiểm tra an toàn thông tin, an ninh mạng" được dán sau khi khắc phục hết các nguy cơ mất an toàn thông tin, an ninh mạng. Trạng thái khi kiểm tra, đánh giá phải là trạng thái cài đặt tất cả các ứng dụng, phần mềm được sử dụng.

3. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng đối với hệ thống thông tin được thực hiện trước, trong và sau khi sử dụng; bao gồm kiểm tra, đánh giá đối với các trang bị phần cứng, phần mềm, kiến trúc, tổ chức cơ sở dữ liệu, giao tiếp, kết nối, vận hành, điều hành, quy trình, quy định và các yếu tố khác có khả năng gây mất an toàn thông tin, an ninh mạng.

4. Hằng năm, các cơ quan đơn vị tổ chức kiểm tra, đánh giá an toàn thông tin, an ninh mạng như sau:

a) Bộ Tư lệnh 86 lập kế hoạch trình Bộ Quốc phòng quyết định, tổ chức kiểm tra, phúc tra, đánh giá an toàn thông tin, an ninh mạng của các cơ quan, đơn vị trong toàn quân;

b) Các cơ quan, đơn vị trực thuộc Bộ Quốc phòng tổ chức kiểm tra, đánh giá nội bộ về an toàn thông tin, an ninh mạng định kỳ 12 tháng 1 lần, hoàn thành trước ngày 25 tháng 10 hằng năm. Riêng đối với hệ thống thông tin quan trọng quốc gia (cấp độ 5), kiểm tra, đánh giá định kỳ 06 tháng 01 lần, hoàn thành trước ngày 25 tháng 5 và ngày 25 tháng 10 hằng năm.

Điều 47. Xếp loại an toàn thông tin, an ninh mạng hằng năm

1. Xếp loại công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng được thực hiện theo tiêu chí xếp loại an toàn thông tin, an ninh mạng toàn cầu và hướng dẫn của Bộ Tư lệnh 86; bảo đảm toàn diện về công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng; dựa trên các tiêu chí cơ bản về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác.

2. Bộ Tư lệnh 86 hướng dẫn, tổ chức và công bố kết quả xếp loại an toàn thông tin, an ninh mạng các cơ quan, đơn vị.

Điều 48. Hợp tác quốc tế

1. Hợp tác quốc tế về an toàn thông tin, an ninh mạng trong Bộ Quốc phòng phải tuân thủ nguyên tắc tôn trọng độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ và lợi ích quốc gia, không can thiệp vào công việc nội bộ của quốc gia khác, bình đẳng, các bên cùng có lợi và phù hợp với quy định của pháp luật Việt Nam, điều ước quốc tế mà Việt Nam là thành viên và quy định có liên quan của Bộ Quốc phòng.

2. Nội dung hợp tác quốc tế về an toàn thông tin, an ninh mạng, gồm: Hợp tác quốc tế trong đào tạo, nghiên cứu, chuyển giao công nghệ và ứng dụng khoa học, kỹ thuật, về an toàn thông tin, an ninh mạng; hợp tác về bảo vệ chủ quyền quốc gia trên không gian mạng và phòng chống chiến tranh thông tin, chiến tranh không gian mạng.

3. Bộ Tư lệnh 86 chủ trì, phối hợp với Cục Đối ngoại/Bộ Quốc phòng và cơ quan, đơn vị liên quan tham mưu, triển khai và là đầu mối hợp tác quốc tế về an toàn thông tin, an ninh mạng trong Bộ Quốc phòng.

Điều 49. Chế độ báo cáo

Định kỳ trước ngày 14 tháng cuối Quý I, II, III và trước ngày 14 tháng 12 hằng năm, các cơ quan, đơn vị báo cáo kết quả công tác bảo đảm an toàn thông tin, an ninh mạng quý, năm về Bộ Tư lệnh 86 để tổng hợp, báo cáo Bộ Quốc phòng. Nội dung báo cáo, gồm: Tình hình chung; kết quả tuyên truyền, huấn luyện, giám sát mạng, ứng cứu sự cố và triển khai giải pháp bảo đảm an toàn thông tin, an ninh mạng; thực trạng và nguyên nhân mất an toàn thông tin, an ninh mạng; kiến nghị, đề xuất; một số nội dung trọng tâm trong quý, năm tới.

Điều 50. Kinh phí

Kinh phí công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng do ngân sách quốc phòng thường xuyên bảo đảm, được bố trí trong dự toán ngân sách quốc phòng thường xuyên hằng năm. Việc quản lý, sử dụng kinh phí công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng thực hiện theo quy định của pháp luật về ngân sách nhà nước.

Chương IV

TRÁCH NHIỆM TRONG QUẢN LÝ, BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 51. Bộ Tổng Tham mưu

1. Chỉ đạo các cơ quan, đơn vị toàn quân thực hiện các biện pháp bảo đảm công tác an toàn thông tin, an ninh mạng theo quy định tại Thông tư này.

2. Chỉ đạo Cục Cơ yếu:

a) Chủ trì, phối hợp cơ quan, đơn vị liên quan triển khai các giải pháp bảo mật đường truyền; bảo mật và xác thực thông tin cho các dịch vụ của mạng máy tính; bảo mật dữ liệu lưu giữ tại các trung tâm dữ liệu và mạng máy tính quân sự;

b) Phối hợp với Bộ Tư lệnh 86 và các cơ quan, đơn vị trong giám sát, ứng cứu sự cố liên quan đến hệ thống thông tin ngành cơ yếu;

c) Chủ trì, hướng dẫn các cơ quan, đơn vị triển khai sản phẩm mật mã phục vụ việc xử lý, gửi nhận văn bản, dữ liệu thuộc danh mục bí mật nhà nước.

Điều 52. Tổng cục Chính trị

1. Chỉ đạo Cục Tuyên huấn:

a) Chủ trì, phối hợp với các cơ quan, đơn vị triển khai các hoạt động tuyên truyền, phổ biến, giáo dục pháp luật nâng cao nhận thức về an toàn thông tin, an ninh mạng;

b) Phối hợp với các cơ quan chức năng liên quan kiểm tra, giám sát nội dung thông tin cung cấp trên trang, cổng thông tin điện tử của cơ quan, đơn vị trong Quân đội.

2. Chỉ đạo Cục Bảo vệ an ninh Quân đội:

a) Thực hiện chức năng của cơ quan chuyên trách bảo vệ an ninh trong Quân đội; phòng ngừa, phát hiện, ngăn chặn và đấu tranh với hành vi xâm phạm an ninh Quân đội trên không gian mạng;

b) Chủ trì, phối hợp với Bộ Tư lệnh 86 và các cơ quan, đơn vị liên quan trong việc phòng ngừa, phát hiện lộ, mất bí mật nhà nước trên không gian mạng;

c) Điều tra, xử lý các vụ việc gây mất an ninh thông tin, an ninh mạng theo quy định của pháp luật;

d) Phối hợp với các cơ quan chức năng trong điều tra, đấu tranh với các hành vi lợi dụng mạng máy tính xâm phạm an ninh quốc gia, trật tự an toàn xã

hội thuộc phạm vi quản lý nhà nước của Bộ Quốc phòng và bảo vệ bí mật nhà nước theo quy định của pháp luật;

đ) Chủ trì kiểm tra an ninh đối với hệ thống thông tin và trang bị công nghệ thông tin theo quy định của Bộ Quốc phòng.

Điều 53. Bộ Tư lệnh 86

1. Là cơ quan đầu ngành công tác bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng; thường trực, đại diện Bộ Quốc phòng tham gia công tác an toàn thông tin, an ninh mạng và ứng cứu sự cố an toàn thông tin, an ninh mạng với các ban, bộ, ngành, địa phương và doanh nghiệp.

2. Chủ trì, phối hợp nghiên cứu, xây dựng, trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền chiến lược, quy hoạch, kế hoạch, chính sách, văn bản quy phạm pháp luật, quy định, quy trình, tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn về bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng; chủ trì xây dựng, ban hành chính sách thiết lập an toàn thông tin, an ninh mạng cho các phần mềm, ứng dụng, trang bị kỹ thuật sử dụng trong Bộ Quốc phòng.

3. Chủ trì, phối hợp với các cơ quan, đơn vị trong và ngoài Bộ Quốc phòng tổ chức giám sát, thu thập thông tin, phân tích, đánh giá nhằm phát hiện và cảnh báo kịp thời tới các cơ quan, đơn vị trong toàn quân về các sự cố an toàn thông tin, an ninh mạng, nguy cơ xâm phạm an toàn thông tin, an ninh mạng.

4. Chủ trì, phối hợp triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng; hướng dẫn mua sắm, cấp phát trang bị công nghệ thông tin bảo đảm an toàn thông tin, an ninh mạng tới cơ quan, đơn vị trong toàn quân theo quy định của Nhà nước và Bộ Quốc phòng; tổ chức kiểm tra, đánh giá và dán tem "Đã kiểm tra an toàn thông tin mạng, an ninh mạng".

5. Chủ trì, phối hợp với các cơ quan, đơn vị ngăn chặn xung đột thông tin trên mạng và phòng, chống sử dụng mạng để khủng bố theo quy định tại Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng và Nghị định số 101/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định chi tiết về trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố; chỉ đạo, hướng dẫn phân loại hệ thống thông tin và xác định cấp độ an toàn hệ thống thông tin.

6. Tổ chức đào tạo, huấn luyện, hướng dẫn nghiệp vụ bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng.

7. Chủ trì, phối hợp nghiên cứu, ứng dụng khoa học công nghệ trong bảo đảm an toàn thông tin, an ninh mạng.

8. Căn cứ vào nhiệm vụ, định mức chi và quy định về công tác tài chính trong Bộ Quốc phòng, lập dự toán chi bảo đảm an toàn thông tin, an ninh mạng, gửi Cục Tài chính/Bộ Quốc phòng để tổng hợp chung vào dự toán ngân sách hằng năm.

Điều 54. Cục Tài chính/Bộ Quốc phòng

Chủ trì, phối hợp với Bộ Tư lệnh 86 thẩm định dự toán kinh phí bảo đảm an toàn thông tin, an ninh mạng; tổng hợp, báo cáo Bộ Quốc phòng.

Điều 55. Binh chủng Thông tin liên lạc

1. Phối hợp với Bộ Tư lệnh 86 và Cục Cơ yếu giám sát mạng và triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng.

2. Phối hợp với các thành viên mạng lưới ứng cứu sự cố an toàn thông tin, an ninh mạng trong Bộ Quốc phòng khắc phục các sự cố mất an toàn thông tin trên hệ thống thông tin liên lạc quân sự.

Điều 56. Tập đoàn Công nghiệp - Viễn thông Quân đội

1. Cung cấp thông tin kỹ thuật nghiệp vụ có liên quan trực tiếp phục vụ hoạt động điều phối, xử lý sự cố về an toàn thông tin, an ninh mạng theo đề nghị của Bộ Tư lệnh 86.

2. Chịu trách nhiệm trước Bộ trưởng Bộ Quốc phòng về bảo đảm an toàn thông tin, an ninh mạng đối với việc cung cấp hạ tầng, dịch vụ của Tập đoàn Công nghiệp - Viễn thông Quân đội cho các cơ quan, đơn vị trong Bộ Quốc phòng.

3. Bố trí lực lượng, phương tiện phối hợp với các cơ quan chức năng của Bộ Quốc phòng trong bảo đảm an toàn thông tin, an ninh mạng, ứng cứu, khắc phục sự cố an toàn thông tin, an ninh mạng.

Điều 57. Các cơ quan, đơn vị, tổ chức thuộc Bộ Quốc phòng

1. Tổ chức quán triệt, tuyên truyền, phổ biến và thực hiện nghiêm các quy định về an toàn thông tin, an ninh mạng tại Thông tư này.

2. Bố trí cán bộ đủ tiêu chuẩn chính trị để thực hiện quản lý về an toàn thông tin, an ninh mạng.

3. Chủ động phối hợp với Bộ Tư lệnh 86 để triển khai công tác quản lý và bảo đảm an toàn thông tin, an ninh mạng của cơ quan, đơn vị mình.

4. Phân loại cấp độ an toàn thông tin cho các hệ thống thông tin thuộc phạm vi quản lý và tổ chức bảo đảm an toàn thông tin, an ninh mạng theo cấp độ. Xây dựng và ban hành các quy định, chính sách về an toàn thông tin, an ninh mạng nội bộ.

5. Hằng năm, bố trí kinh phí và lập kế hoạch bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin thuộc phạm vi quản lý.

Điều 58. Trách nhiệm người sử dụng

1. Chấp hành nghiêm các quy định của pháp luật, quy chế của đơn vị về công tác bảo đảm an toàn thông tin, an ninh mạng.

2. Quản lý, bảo vệ vật mang dữ liệu điện tử chặt chẽ, cẩn thận; không được làm mất, lộ lọt thông tin.

3. Không tự ý chỉnh sửa, ghi đè hoặc xóa các tập tin hệ thống.

4. Bảo vệ thông tin của tài khoản sử dụng máy tính, ứng dụng, dịch vụ được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác phương tiện xác thực tài khoản của mình, trừ trường hợp cần xử lý công việc khẩn cấp của đơn vị hoặc cần cung cấp, bàn giao cho cơ quan, đơn vị các thông tin, dữ liệu điện tử quân sự do cá nhân quản lý và phải đổi mật khẩu ngay sau khi cơ quan, đơn vị, cá nhân tiếp nhận kết thúc xử lý công việc.

5. Không tự cài đặt phần mềm mới hoặc gỡ bỏ, vô hiệu hóa các phần mềm bảo đảm an toàn thông tin, an ninh mạng khi chưa được sự đồng ý của cơ quan quản lý công nghệ thông tin. Khi phát hiện bất kỳ dấu hiệu bất thường trên máy tính có khả năng liên quan đến việc nhiễm phần mềm độc hại, phải thông báo ngay cho cơ quan quản lý công nghệ thông tin để xử lý.

Chương V

ĐIỀU KHOẢN THI HÀNH

Điều 59. Hiệu lực thi hành và điều khoản chuyển tiếp

1. Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 01 năm 2025 và thay thế Thông tư số 56/2020/TT-BQP ngày 05 tháng 5 năm 2020 của Bộ trưởng Bộ Quốc phòng quy định về quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng; Thông tư số 160/2016/TT-BQP ngày 20 tháng 10 năm 2016 của Bộ trưởng Bộ Quốc phòng quy định biện pháp bảo đảm an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia do Bộ Quốc phòng quản lý.

2. Trường hợp văn bản viện dẫn trong Thông tư này được sửa đổi, bổ sung, thay thế thì áp dụng quy định tương ứng tại văn bản sửa đổi, bổ sung, thay thế.

Điều 60. Trách nhiệm thi hành

1. Tổng Tham mưu trưởng, Chủ nhiệm Tổng cục Chính trị, Thủ trưởng các cơ quan, đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

2. Tư lệnh Bộ Tư lệnh 86 chịu trách nhiệm hướng dẫn, kiểm tra, đôn đốc việc thực hiện Thông tư này./.

Nơi nhận:
- Các đ/c Lãnh đạo BQP[8];
- Các cơ quan, đơn vị trực thuộc BQP[68];
- C58, C12, C13;
- Vụ Pháp chế/BQP;
- Lưu: VT, CCHC. PH82.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Đại tướng Nguyễn Tân Cương

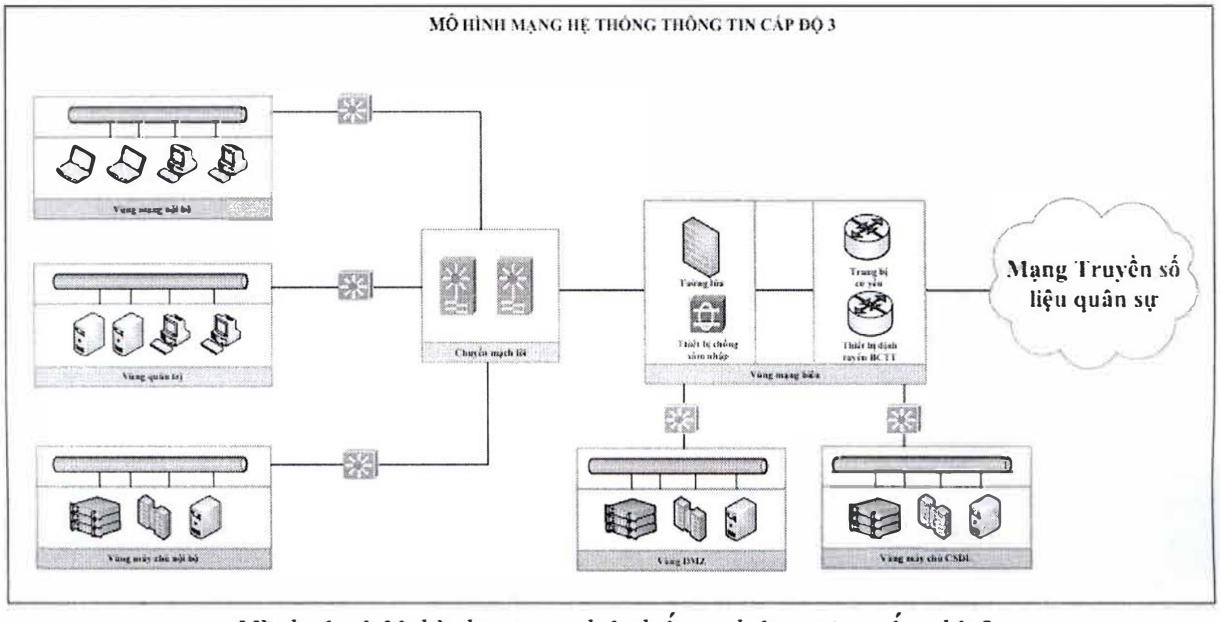
Phụ lục I

YÊU CẦU VỀ THIẾT KẾ HỆ THỐNG MẠNG

(Kèm theo Thông tư số 107 /2024/TT-BQP ngày 30 tháng 11 năm 2024 của Bộ trưởng Bộ Quốc phòng)

1. Đối với hệ thống thông tin cấp độ 3

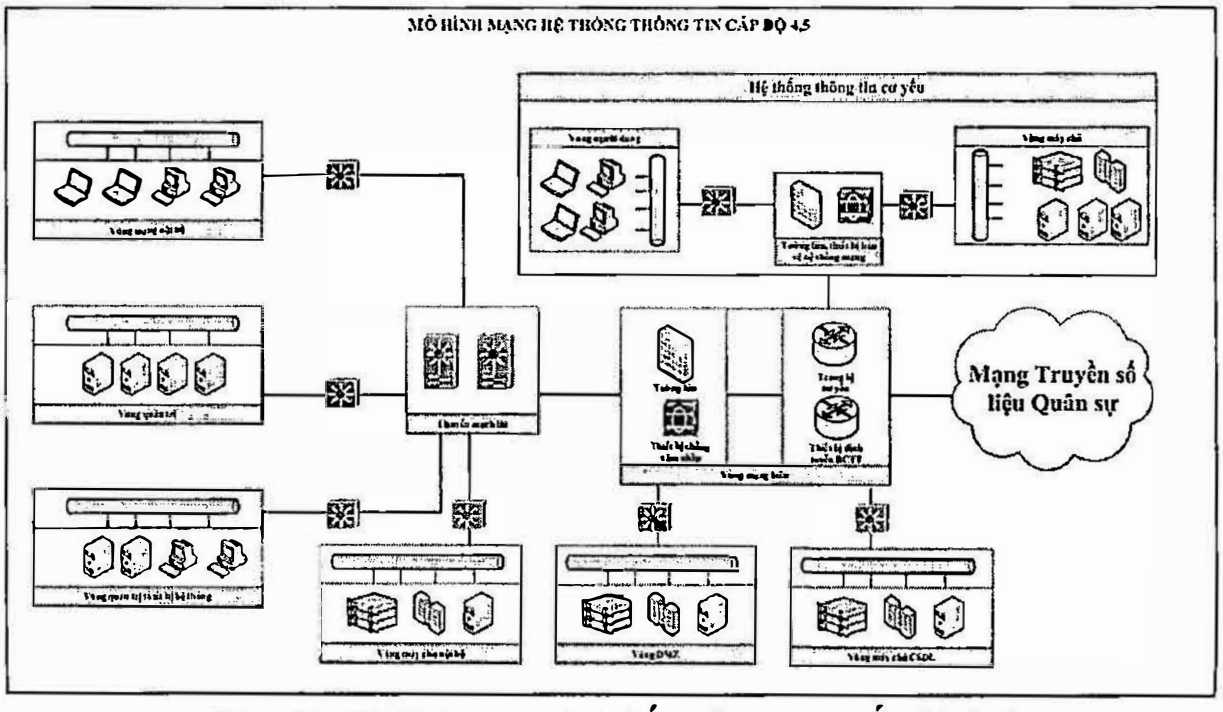
Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm: Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng máy chủ cơ sở dữ liệu; Vùng quản trị.



Hình 1: Mô hình mạng hệ thống thông tin cấp độ 3

2. Đối với hệ thống thông tin cấp độ 4, 5

Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm: Vùng mạng nội bộ; Vùng mạng biên; Vùng DMZ; Vùng máy chủ nội bộ; Vùng máy chủ cơ sở dữ liệu; Vùng quản trị; Vùng quản trị thiết bị hệ thống.



Hình 2: Mô hình mạng hệ thống thông tin cấp độ 4, 5

Phụ lục II

MẪU TEM "ĐÃ KIỂM TRA A TOÀN THÔNG TIN, AN NINH MẠNG"

(Kèm theo Thông tư số 107/2024/TT-BQP ngày 30 tháng 11 năm 2024 của Bộ trưởng Bộ Quốc phòng)

1. Tem "Đã kiểm tra an toàn thông tin, an ninh mạng" mẫu lớn

Tem hình chữ nhật: Kích thước 20 mm x 40 mm; sử dụng chất liệu giấy vỡ; nửa bên trái in biểu tượng của Bộ Tư lệnh 86, nửa bên phải in mã phản ứng nhanh (QR).

2. Tem "Đã kiểm tra an toàn thông tin, an ninh mạng" mẫu nhỏ

Tem hình tròn: Đường kính 12 mm; sử dụng chất liệu giấy vỡ; phía trên in dòng chữ "Bộ Tư lệnh 86", phía dưới in dòng chữ "Command 86"; chính giữa in mã phản ứng nhanh (QR).