BỘ QUỐC PHÒNG
QUÂN CHỦNG
PHÒNG KHÔNG - KHÔNG QUÂN

Số: 5067 /QyĐ-PKKQ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 28 tháng 12 năm 2021

QUY ĐỊNH
Quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Quân chủng PK-KQ

Căn cứ Thông tư số 56/2020/TT-BQP ngày 05 tháng 5 năm 2020 của Bộ Quốc phòng quy định về quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng;

Căn cứ Thông tư số 45/2020/TT-BQP ngày 27 tháng 4 năm 2020 của Bộ Quốc phòng quy định về điều phối và ứng cứu sự cố an toàn thông tin, an ninh mạng trong Bộ Quốc phòng;

Căn cứ Thông tư số 160/2016/TT-BQP ngày 20 tháng 10 năm 2016 của Bộ Quốc phòng quy định các biện pháp bảo đảm an toàn thông tin mạng đối với hệ thống thông tin quan trọng quốc gia do Bộ Quốc phòng quản lý;

Căn cứ Thông tư số 161/2017/TT-BQP ngày 07 tháng 7 năm 2017 của Bộ Quốc phòng quy định về quản lý, khai thác sử dụng hạ tầng công nghệ thông tin quân sự trong Quân đội nhân dân Việt Nam;

Căn cứ Thông tư số 217/2013/TT-BQP ngày 16 tháng 12 năm 2013 của Bộ trưởng Bộ Quốc phòng quy định về việc ban hành, sử dụng, quản lý, lưu trữ văn bản điện tử trên mạng TSLqs;

Căn cứ Thông tư số 110/2014/TT-BQP ngày 22 tháng 8 năm 2014 của Bộ trưởng Bộ Quốc phòng về việc ban hành quy chế quản lý, cung cấp và sử dụng dịch vụ Internet trong Quân đội nhân dân Việt Nam;

Căn cứ Chỉ thị 102/CT-BQP ngày 06 tháng 9 năm 2021 của Bộ trưởng Bộ Quốc phòng về việc tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng trong Bộ Quốc phòng;

Theo đề nghị của Đồng chí Tham mưu trưởng Quân chủng PK-KQ;

Tư lệnh PK-KQ ban hành Quy định về quản lý và bảo đảm an toàn thông tin, an ninh mạng trong Quân chủng PK-KQ.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy định này quy định về công tác quản lý và bảo đảm an toàn thông tin, an ninh

mạng, trách nhiệm của các cơ quan, đơn vị, cá nhân bắt buộc phải thực hiện trong Quân chủng PK-KQ.

2. Đối tượng áp dụng

Quy định này áp dụng đối với các cơ quan, đơn vị, tổ chức, cá nhân tham gia thiết kế, xây dựng, quản lý, mua sắm, vận hành, khai thác, sử dụng, bảo đảm kỹ thuật, bảo đảm an toàn thông tin, an ninh mạng trang bị công nghệ thông tin và hệ thống thông tin trong Quân chủng PK-KQ.

Điều 2. Giải thích từ ngữ

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

1. *Phần cứng* là sản phẩm thiết bị số hoàn chỉnh, cụm linh kiện, linh kiện, bộ phận của thiết bị số.

2. *Phần mềm* là chương trình máy tính được mô tả bằng hệ thống ký hiệu, mã hoặc ngôn ngữ để điều khiển thiết bị số thực hiện chức năng nhất định.

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

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

5. *Tính nguyên vẹn* là tính chất của thông tin bảo đảm sự chính xác và đầy đủ của thông tin.

6. *Tính bí mật* là tính chất của thông tin bảo đảm thông tin chỉ có thể được truy nhập bởi những người được cấp quyền sử dụng.

7. *Tính sẵn sàng* là tính chất của thông tin bảo đảm những người được cấp quyền sử dụng có thể truy nhập thông tin ngay khi có nhu cầu.

8. *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 cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bí mật và tính sẵn sàng 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, đơn vị, cá nhân.

9. *Bảo đảm an toàn thông tin, an ninh mạng* là tổng hợp các biện pháp về tổ chức - quản lý và kỹ thuật - công nghệ nhằm thực hiện và duy trì an toàn thông tin, an ninh mạng.

10. *Máy tính quân sự* là máy tính phục vụ cho hoạt động quân sự trong các cơ quan, đơn vị.

11. *Máy tính Internet* là máy tính kết nối mạng Internet sử dụng trong các cơ quan, đơn vị.

12. *Mạng máy tính quân sự* là mạng máy tính diện rộng dùng riêng để phục vụ quản lý, chỉ huy, điều hành và điều khiển vũ khí, trang bị kỹ thuật trong Bộ Quốc phòng.

13. *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.

14. *Trang thông tin điện tử* là trang thông tin hoặc một tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp và trao đổi thông tin.

15. *Cổng thông tin điện tử* là điểm truy nhập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

16. *Người dùng* là sĩ quan, quân nhân chuyên nghiệp, công nhân và viên chức quốc phòng, hạ sĩ quan, binh sĩ được sử dụng máy tính của cơ quan, đơn vị để xử lý công việc.

17. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

18. *Rủi ro an toàn thông tin, an ninh mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới tình trạng an toàn thông tin, an ninh mạng.

19. *Sự cố an toàn thông tin, an ninh mạng* gồm sự cố an toàn thông tin mạng và sự cố an ninh mạng, trong đó:

a) Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bí mật hoặc tính sẵn sàng;

b) Sự cố an ninh mạng là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

20. *Ứng cứu sự cố an toàn thông tin, an ninh mạng* là hoạt động nhằm xử lý, khắc phục sự cố, xác định nguyên nhân, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

21. *Điều phối ứng cứu sự cố an toàn thông tin, an ninh mạng* là hoạt động tổ chức, điều hành, phối hợp của cơ quan có thẩm quyền nhằm ứng cứu sự cố an toàn thông tin, an ninh mạng.

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

23. *Tài liệu điện tử quân sự* là tài liệu ở dạng tập tin được hình thành trong quá trình hoạt động của cơ quan, đơn vị Quân đội.

24. *Vật mang tin điện tử* là các phương tiện vật chất có khả năng lưu trữ thông tin điện tử, bao gồm: USB, thẻ nhớ, ổ cứng di động, đĩa CD, đĩa DVD, các

máy ghi âm, quay phim, chụp hình, nghe nhạc, thiết bị di động thông minh và các thiết bị khác có khả năng lưu trữ, trao đổi dữ liệu, thông tin điện tử.

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

26. *Xóa dữ liệu an toàn* là việc sử dụng các phần mềm, thiết bị chuyên dụng để xóa dữ liệu nhằm bảo đảm dữ liệu không thể khôi phục được.

27. *Thiết bị di động thông minh* là thiết bị số có thể cầm tay, có hệ điều hành, khả năng xử lý, kết nối với thiết bị khác hoặc kết nối qua mạng không dây và có màn hình hiển thị bao gồm: Máy tính bảng, điện thoại di động thông minh, đồng hồ thông minh và các thiết bị khác có khả năng tương tự.

28. *Trang bị công nghệ thông tin* là trang bị kỹ thuật bao gồm:

a) Máy tính các loại;

b) Thiết bị mạng;

c) Thiết bị an toàn thông tin;

d) Thiết bị lưu trữ thông tin;

đ) Thiết bị ngoại vi.

29. *Lỗ hổng bảo mật* là những điểm yếu nằm trong thiết kế, cấu hình hệ thống, lỗi của lập trình viên trong quá trình xây dựng phần mềm hoặc sơ suất trong quá trình vận hành tạo kẽ hở cho việc xâm nhập trái phép thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

30. *Tài khoản* là thông tin dùng để xác thực người sử dụng truy nhập các ứng dụng, dịch vụ trên máy tính, mạng máy tính.

31. *Quyền của tài khoản* là thông tin thể hiện khả năng của người sở hữu tài khoản tác động tới các đối tượng.

32. *Tài khoản quản trị* là tài khoản cho phép người sử dụng cấu hình, cài đặt máy tính và mạng máy tính.

33. *Tài khoản người dùng* là tài khoản cho phép người sử dụng khai thác trang bị, dữ liệu, hệ thống để phục vụ công tác chuyên môn và không có quyền cấu hình, cài đặt máy tính và mạng máy tính.

34. *Phần mềm nhúng* là chương trình được viết, biên dịch trên máy tính và được nạp vào thiết bị phần cứng để thực hiện một số chức năng điều khiển nhất định.

35. *Máy tính cá nhân* là máy tính do người dùng tự có từ nguồn hợp pháp, sử dụng vào mục đích cá nhân.

36. *Chủ quản hệ thống thông tin* là cơ quan, đơn vị có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

37. *Đơn vị vận hành hệ thống thông tin* là cơ quan, đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ trực tiếp vận hành hệ thống thông tin.

38. *Giải pháp dự phòng nóng* là giải pháp có chức năng đảm bảo cho cơ sở dữ liệu và ứng dụng có thể truy cập 24/7 trong mọi điều kiện.

39. *Sản phẩm mật mã* là các tài liệu, trang thiết bị kỹ thuật và nghiệp vụ mật mã để bảo vệ thông tin.

40. *Giải pháp bảo mật cơ yếu* là việc sử dụng sản phẩm mật mã, kỹ thuật mật mã của ngành Cơ yếu để bảo mật thông tin, dữ liệu.

Điều 3. Các hành vi bị nghiêm cấm

1. Đưa các trang bị công nghệ thông tin chưa được các cơ quan chức năng kiểm tra an toàn thông tin, an ninh mạng vào sử dụng.

2. Sử dụng máy tính cá nhân phục vụ nhiệm vụ quân sự, quốc phòng.

3. Sử dụng máy tính Internet, máy tính cá nhân hoặc thiết bị di động thông minh có kết nối Internet để tạo lập, xử lý và lưu trữ tài liệu điện tử quân sự có nội dung không được hoặc chưa được phép phổ biến.

4. Trao đổi thông tin mật trên mạng mà không có giải pháp bảo mật cơ yếu.

5. Sử dụng vật mang tin điện tử không có giải pháp bảo đảm an toàn thông tin, an ninh mạng để trao đổi thông tin, dữ liệu giữa máy tính quân sự với máy tính Internet hoặc lưu trữ, trao đổi thông tin, dữ liệu quân sự.

6. Sử dụng thiết bị di động thông minh của cá nhân tại các vị trí quan trọng, cơ mật; trong các cuộc giao ban, hội họp có nội dung mật của cơ quan, đơn vị.

7. Sử dụng máy tính Internet kết nối mạng máy tính quân sự.

8. Kết nối thiết bị di động thông minh, thiết bị truy cập Internet không dây vào máy tính quân sự.

9. Kết nối, truy nhập vào mạng máy tính quân sự bằng giải pháp kết nối không dây mà không có biện pháp bảo đảm an toàn thông tin, an ninh mạng phù hợp và chưa được cơ quan chức năng thẩm định, cho phép.

10. Kết nối liên thông mạng máy tính quân sự với mạng Internet dưới mọi hình thức.

11. Sử dụng Internet cũng như sử dụng các mạng không dây như Wifi, Wimax, Bluetooth,... để kết nối Internet trong các cơ quan, đơn vị khi chưa được Quân chủng cấp phép.

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

13. Sử dụng mạng Internet tự ý thực hiện hành vi đăng tải, phát tán, bình luận, chia sẻ dưới mọi hình thức những thông tin (hình ảnh, video clip, bài viết...) liên quan đến quân đội khi chưa được phép của người có thẩm quyền; thông tin trái quan điểm, đường lối của Đảng, Nhà nước; thông tin liên quan đến bí mật Nhà nước, quân sự và bí mật của đơn vị; thông tin có nội dung xuyên tạc, bịa đặt, xúc phạm danh dự cá nhân, uy tín tổ chức; thông tin kích động bạo lực, đồi trụy, mê tín dị đoan; tự ý tạo lập hoặc tham gia các diễn đàn, nhóm liên quan đến tội phạm, tổ

chức phản động, chống đối chính trị và các vi phạm pháp luật khác.

14. Tự ý ghi âm, ghi hình các cuộc họp, làm việc khi không được phép của người chủ trì hội nghị, chủ trì buổi làm việc.

15. Tự ý đưa người không có nhiệm vụ, tổ chức, cá nhân bên ngoài Quân đội vào lắp đặt, sửa chữa máy tính và các trang thiết bị công nghệ thông tin của cơ quan, đơn vị (trường hợp thuê chuyên gia phải được sự đồng ý của chỉ huy và có sự giám sát của cán bộ, nhân viên chuyên môn về công nghệ thông tin trong suốt quá trình thực hiện).

16. Tự ý chuyển mục đích sử dụng máy tính, thiết bị khác để soạn thảo, lưu trữ, trao đổi bí mật Nhà nước, bí mật quân sự hoặc chuyển mục đích sử dụng nhưng chưa loại bỏ bí mật Nhà nước, bí mật quân sự.

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

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

1. Ứng dụng, phát triển công nghệ thông tin và bảo đảm kỹ thuật công nghệ thông tin phải gắn với bảo đảm an toàn thông tin, an ninh mạng. Việc 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 xử lý trang bị, hệ thống thông tin.

2. Hoạt động bảo đảm an toàn thông tin, an ninh mạng phải được thực hiện thường xuyên, liên tục, kịp thời trên cơ sở tuân thủ quy định, 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 dùng phải được trang bị kiến thức và chịu trách nhiệm về an toàn thông tin, an ninh mạng đối với trang bị do mình quản lý, sử dụng.

5. Người chỉ huy cơ quan, đơn vị chịu trách nhiệm trực tiếp, cao nhất về an toàn thông tin, an ninh mạng của cơ quan, đơn vị do mình quản lý.

Điều 5. Nội dung bảo đảm an toàn thông tin, an ninh mạng

1. Bảo đảm an ninh, an toàn vật lý và môi trường.

2. Bảo đảm an toàn thông tin, an ninh mạng tài khoản.

3. Bảo đảm an toàn thông tin, an ninh mạng dữ liệu.

4. Bảo đảm an toàn thông tin, an ninh mạng phần mềm.

5. Bảo đảm an toàn thông tin, an ninh mạng trang bị công nghệ thông tin.

6. Bảo đảm an toàn thông tin, an ninh mạng mạng máy tính-hệ thống thông tin.

7. Bảo đảm an toàn thông tin, an ninh mạng trong phát triển công nghệ thông tin.

8. Bảo đảm an toàn thông tin, an ninh mạng trong sử dụng Internet.

9. Ứng cứu sự cố và xác định nguyên nhân mất an toàn thông tin, an ninh mạng.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

Mục 1
BẢO ĐẢM AN NINH, AN TOÀN VẬT LÝ VÀ MÔI TRƯỜNG

Điều 6. Quy định an ninh, an toàn vật lý và môi trường

1. Các khu vực quan trọng sau phải được bảo vệ để phòng tránh xâm nhập trái phép hoặc sử dụng sai mục đích:

a) Trung tâm dữ liệu;

b) Khu vực máy chủ, thiết bị lưu trữ, thiết bị mạng, các tủ mạng và đấu nối, thiết bị nguồn điện và dự phòng điện khẩn cấp;

c) Các phòng vận hành, kiểm soát, quản trị hệ thống thông tin;

d) Các khu vực làm việc, kho và các vị trí có triển khai các sản phẩm mật mã của Cơ yếu.

2. Các biện pháp bảo đảm an ninh, an toàn vật lý và môi trường tại khu vực phòng máy chủ:

a) Ban hành nội quy, hướng dẫn làm việc và sử dụng các biện pháp bảo đảm an ninh khác để kiểm soát vào ra;

b) Thực hiện các biện pháp phòng, chống cháy nổ, sét và các loại thảm họa khác do thiên nhiên hoặc con người tạo ra;

c) Bảo đảm điện năng và điều kiện môi trường để các trang bị công nghệ thông tin hoạt động liên tục, ổn định; có kế hoạch thiết lập chế độ chờ, nguồn cung cấp điện liên tục và máy phát điện dự phòng;

d) Định kỳ 03 tháng một lần kiểm tra đường truyền, các điểm truy nhập mạng để tránh bị xâm nhập, phá hoại trái phép.

Mục 2
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG TÀI KHOẢN

Điều 7. Quy định về tài khoản

1. Tên tài khoản phải đảm bảo tính định danh duy nhất. Mật khẩu tài khoản phải là mật khẩu phức tạp.

2. Tạo mới, điều chỉnh, khóa, xóa, mở lại tài khoản

Cơ quan, đơn vị quản lý người dùng phải thông báo cho cơ quan phụ trách công nghệ thông tin khi có thay đổi về người dùng để tạo mới, điều chỉnh, khóa, xóa, mở lại tài khoản và thực hiện thông báo, cụ thể như sau:

- Cấp quyền cho tài khoản theo nguyên tắc cấp quyền tối thiểu;

- Thay đổi quyền cho tài khoản phù hợp với vị trí công tác của người dùng ngay khi nhận được yêu cầu;

- Cấp lại mật khẩu cho tài khoản khi người dùng sở hữu tài khoản yêu cầu;

- Khóa tài khoản khi tài khoản liên quan tới sự cố an toàn thông tin, an ninh mạng (mở lại khi khắc phục xong sự cố); tài khoản không sử dụng trong vòng 06 tháng (mở lại khi có yêu cầu của cơ quan, đơn vị quản lý người dùng) hoặc ngay khi người dùng không còn liên quan đến hệ thống thông tin;

- Xóa tài khoản khi cơ quan, đơn vị quản lý người dùng thông báo người dùng không còn liên quan tới các hệ thống thông tin trong cơ quan, đơn vị;

- Cơ quan phụ trách công nghệ thông tin phải thông báo cho cơ quan, đơn vị quản lý người dùng ngay sau khi hoàn thành yêu cầu về tài khoản.

3. Yêu cầu về sử dụng, quản lý tài khoản

a) Người dùng phải đổi mật khẩu ngay sau khi nhận tài khoản, chịu trách nhiệm bảo vệ mật khẩu hợp lý; trong sử dụng, đổi mật khẩu thường xuyên (nhưng không quá 90 ngày); 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 cơ quan, đơn vị hoặc cần cung cấp, bàn giao cho cơ quan, đơn vị các thông tin, tài 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;

b) Tài khoản quản trị phải được giao đích danh người quản lý trang bị, quản trị hệ thống; chỉ được sử dụng khi cài đặt, cấu hình phần cứng, phần mềm, dịch vụ; sao lưu, khôi phục dữ liệu và thực hiện các nội dung tại Khoản 2 Điều này;

c) Sử dụng tài khoản dùng chung phải do một cá nhân có trách nhiệm quản lý; người được giao tài khoản phải có trách nhiệm bảo vệ thông tin tài khoản;

d) Các cơ quan, đơn vị phải quản lý tài khoản sử dụng trang bị công nghệ thông tin, mạng máy tính - hệ thống thông tin quân sự theo quy định quản lý tài liệu mật; phải thường xuyên rà soát, cập nhật.

Mục 3
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG DỮ LIỆU

Điều 8. Bảo đảm an toàn tài liệu điện tử quân sự

1. Căn cứ vào danh mục bí mật nhà nước, bí mật quân sự, các cơ quan, đơn vị có trách nhiệm phân loại tài liệu điện tử quân sự theo độ mật, phạm vi sử dụng và thời gian lưu trữ để có biện pháp bảo vệ phù hợp.

2. Tạo lập, lưu trữ, xử lý tài liệu điện tử quân sự

a) Tài liệu điện tử quân sự chỉ được tạo lập, xử lý, lưu trữ trên máy tính quân sự. Khi xóa tài liệu điện tử quân sự trên các thiết bị lưu trữ phải xóa nội dung của tập tin, sử dụng các công cụ xóa dữ liệu an toàn;

b) Các tài liệu điện tử quân sự có độ mật chỉ được lưu trữ khi có giải pháp bảo mật cơ yếu; xác định chính xác độ mật cho văn bản, tài liệu điện tử quân sự để có giải pháp bảo mật, giải pháp truyền tin phù hợp.

3. Trao đổi tài liệu điện tử quân sự có độ mật

a) Tài liệu điện tử quân sự có độ mật khi chuyển nhận qua mạng máy tính quân sự phải có các giải pháp bảo mật cơ yếu; tài liệu điện tử đã được chuyển qua mạng liên lạc cơ yếu hoặc mạng viễn thông đã được triển khai giải pháp bảo mật cơ yếu thì không được chuyển qua mạng viễn thông khác;

b) Khi mang tài liệu điện tử quân sự có độ mật ra khỏi doanh trại đơn vị phải đăng ký với cơ quan văn thư, bảo mật.

Điều 9. Bảo đảm an toàn cơ sở dữ liệu

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

a) Phải có bản quyền hoặc có nguồn gốc xuất xứ rõ ràng và được kiểm tra an toàn thông tin, an ninh mạng. Có khả năng xử lý, lưu trữ được khối lượng dữ liệu lớn theo yêu cầu nghiệp vụ; có cơ chế bảo vệ và phân quyền truy nhập;

b) Phải được cập nhật bản vá, bản sửa lỗi khi có hướng dẫn của cơ quan công nghệ thông tin Quân chủng.

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

a) Thực hiện cấp tài khoản truy nhập cơ sở dữ liệu theo Điều 7 của Quy định này;

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

3. Cơ sở dữ liệu phải được sao lưu dự phòng định kỳ. Đối với các cơ sở dữ liệu quan trọng phải triển khai giải pháp dự phòng nóng.

4. Có giải pháp phát hiện, ngăn chặn các hình thức tấn công cơ sở dữ liệu.

Mục 4
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG PHẦN MỀM

Điều 10. Sử dụng, cập nhật phần mềm

1. Chỉ sử dụng các phần mềm có bản quyền hoặc do cơ quan chức năng cung cấp; 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. Phần mềm sử dụng phải được cập nhật và thống kê, lưu trữ, tổng hợp, báo cáo theo quy định.

3. Thay đổi, cập nhật phần mềm phải có kế hoạch và được phép của người có thẩm quyền.

4. Cơ quan, đơn vị quản lý trực tiếp phần mềm phải tổ chức huấn luyện về khai thác sử dụng cho người dùng.

5. Người dùng không được tự ý gỡ bỏ các phần mềm đã cài đặt, thay đổi thông số cấu hình của phần mềm dẫn đến sai mục đích sử dụng. Trường hợp phần

mềm phát sinh lỗi, người dùng phải kịp thời báo cáo theo quy định.

6. Phần mềm quân sự không được phép tiết lộ ra bên ngoài.

Điều 11. Phát triển, nâng cấp phần mềm

1. Phát triển, nâng cấp phần mềm, dịch vụ phải tuân thủ quy trình phát triển phần mềm do Bộ Quốc phòng quy định; phải được cơ quan có chuyên môn công nghệ thông tin trong Quân chủng thẩm định và được cấp có thẩm quyền phê duyệt.

2. Phải sử dụng phần mềm công cụ có bản quyền hoặc có nguồn gốc xuất xứ rõ ràng và đã được kiểm tra đánh giá an toàn thông tin, an ninh mạng.

3. Phần mềm ứng dụng được phát triển phải có chức năng kiểm soát truy nhập bằng tài khoản, đảm bảo tính tương thích và không ảnh hưởng đến hoạt động chung của hệ thống; phải có tính năng kiểm tra việc xác thực và tính toàn vẹn của thông tin để phát hiện mọi sự thay đổi do lỗi xử lý hoặc do hành động có chủ đích.

4. Trong quá trình phát triển, nâng cấp phần mềm

a) Mã nguồn của chương trình và các thông số kỹ thuật, kế hoạch phát triển, các văn bản liên quan phải được kiểm soát chặt chẽ nhằm ngăn chặn việc thêm vào những tính năng trái phép và những thay đổi không cố ý; phải có giải pháp bảo vệ an toàn các tập tin hệ thống để người dùng không được phép tự ý chỉnh sửa, ghi đè hoặc xóa;

b) 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;

c) Dữ liệu dùng để kiểm thử phải được lựa chọn và thực hiện đúng theo quy định tại Mục 3 của Quy định này;

d) Phải được theo dõi, giám sát chặt chẽ; phải tổ chức kiểm tra, đánh giá an toàn thông tin, an ninh mạng và nghiệm thu sản phẩm.

Mục 5
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG TRANG BỊ CÔNG NGHỆ THÔNG TIN

Điều 12. Quy định về mua sắm, quản lý, khai thác sử dụng, bảo đảm kỹ thuật và thanh xử lý trang bị công nghệ thông tin (trang bị có chứa thành phần công nghệ thông tin)

1. Khi mua sắm trang bị phải tuân theo quy định mua sắm tài sản công, có thành phần chuyên môn công nghệ thông tin và bảo vệ an ninh tham gia (trong tư vấn, lập kế hoạch mua sắm, hồ sơ thiết kế; khảo sát, đánh giá, thẩm định chất lượng hàng hóa khi lựa chọn nhà thầu và hoạt động bàn giao, nghiệm thu trang bị trước khi đưa vào sử dụng); đối với trang bị có chứa phần mềm nhúng phải yêu cầu các nhà sản xuất cung cấp thiết bị xác nhận bảo đảm an toàn thông tin, an ninh mạng hoặc cung cấp mã nguồn của các phần mềm nhúng; đối với các trang bị vũ khí công nghệ cao, trang bị có tích hợp hệ thống công nghệ thông tin phải có

sự tham gia của cơ quan có chuyên môn công nghệ thông tin trong Quân chủng trong thương thảo, đàm phán, nghiệm thu mua sắm trang bị nhằm thẩm định, đánh giá về an toàn thông tin, an ninh mạng và đáp ứng các yêu cầu về công tác bảo đảm kỹ thuật công nghệ thông tin.

2. Các trang bị công nghệ thông tin phục vụ nhiệm vụ quốc phòng (trừ trang thiết bị do ngành Cơ yếu mua sắm và cấp phát) phải được các cơ quan chức năng kiểm tra và dán tem "Đã kiểm tra an toàn thông tin, an ninh mạng" trước khi đưa vào sử dụng; kiểm tra và dán tem "Đã kiểm tra an toàn thông tin, an ninh mạng" cho máy tính quân sự trong quá trình sử dụng; khi triển khai lắp đặt, khai thác sử dụng phải theo đúng tiêu chuẩn, quy chuẩn kỹ thuật của Bộ Quốc phòng, khuyến cáo của nhà sản xuất và Điều 6 của Quy định này.

3. Cá nhân được giao sử dụng trang bị công nghệ thông tin phải được huấn luyện khai thác sử dụng thành thạo trang bị công nghệ thông tin và các quy định về bảo đảm an toàn thông tin, an ninh mạng; không tự ý can thiệp vào cấu hình làm thay đổi tính năng kỹ thuật thiết bị.

4. Cơ quan, đơn vị phải quản lý trang bị công nghệ thông tin theo đúng quy định về quản lý trang bị kỹ thuật trong Quân đội và hướng dẫn của cơ quan công nghệ thông tin Quân chủng.

5. Cơ quan, đơn vị phải thực hiện nghiêm quy định bảo đảm kỹ thuật đối với trang bị công nghệ thông tin; trang bị công nghệ thông tin phục vụ mục đích quốc phòng bắt buộc phải do cơ quan phụ trách công nghệ thông tin của cơ quan, đơn vị bảo dưỡng, sửa chữa, nâng cấp; trong trường hợp trang bị còn thời gian bảo hành phải xóa dữ liệu an toàn thiết bị lưu trữ thông tin trước khi mang đi, sau khi bảo hành phải được kiểm tra an ninh, an toàn thông tin trước khi đưa vào sử dụng; trường hợp các trang bị công nghệ thông tin hỏng hóc lớn không thể tự khắc phục được thì phải báo cáo người chỉ huy và cơ quan chuyên môn cấp trên để được hướng dẫn xử lý (trong trường hợp thuê chuyên gia dân sự vào sửa chữa tại cơ quan, đơn vị phải dưới sự giám sát của bộ phận chuyên trách công nghệ thông tin của cơ quan, đơn vị).

6. Trang bị công nghệ thông tin cấp 5 muốn loại khỏi biên chế, thanh xử lý phải thực hiện theo quy định thanh, xử lý trang bị và hướng dẫn của ngành Quân lực. Đối với các thiết bị lưu trữ thông tin (riêng lẻ hoặc đi kèm với trang bị) phải được tháo gỡ, thu hồi. Trường hợp không còn nhu cầu sử dụng thì phải phá hủy vật lý, nếu tái sử dụng phải xóa dữ liệu an toàn và quản lý chặt chẽ.

7. Sản phẩm mật mã, trang bị công nghệ thông tin do Cơ yếu cung cấp được quản lý, khai thác sử dụng, bảo đảm kỹ thuật và kiểm kê, thu hồi, thanh xử lý theo quy định của ngành Cơ yếu.

Điều 13. Bảo đảm an toàn thông tin, an ninh mạng cho máy tính

1. Tài khoản truy nhập

a) Máy tính phải có tài khoản truy nhập phần cứng do người quản lý máy tính giữ; ít nhất 02 tài khoản truy nhập hệ điều hành: Tài khoản quản trị và tài

khoản người dùng;

b) Nếu máy tính được sử dụng cho nhiều người thì mỗi người sử dụng phải có tài khoản riêng.

2. Người dùng phải thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy) khi rời khỏi nơi đặt máy tính; tắt máy khi không sử dụng để bảo vệ và chống lại những truy nhập vật lý trái phép.

3. Cấu hình, cài đặt và sử dụng

a) Máy tính quân sự chỉ được cài đặt các phần mềm được quy định tại Khoản 1 Điều 10 của Quy định này và phải được cài đặt phần mềm chuyên ngành an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng do cơ quan phụ trách công nghệ thông tin cung cấp, hướng dẫn;

b) Định kỳ cập nhật phiên bản nâng cấp và bản vá lỗi được cung cấp bởi cơ quan chức năng công nghệ thông tin cho các máy tính quân sự;

c) Máy tính phải được cấu hình, thiết lập các chính sách an toàn đối với tài khoản người dùng như: Vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động, quyền thực thi các đoạn mã lệnh, các tập tin cài đặt; vô hiệu hóa các tính năng dễ gây rủi ro an toàn thông tin, an ninh mạng như micro, camera, truy nhập mạng không dây (Wifi, Bluetooth, GPS) và các tính năng khác khi không sử dụng;

d) Máy tính phải được kích hoạt tính năng tường lửa, cài đặt hệ thống phòng chống phần mềm độc hại, phần mềm mã hoá tập tin, phần mềm xoá dữ liệu an toàn. Hệ thống phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật với máy tính có kết nối mạng hoặc định kỳ cập nhật cho máy tính không kết nối mạng; thiết lập chế độ tự động quét mã độc khi sao chép, mở các tập tin;

đ) Máy tính quân sự chuyển sang sử dụng Internet phải được phép của người chỉ huy, phải gỡ bỏ phần mềm quân sự và xóa dữ liệu an toàn;

e) Máy tính của cơ quan, đơn vị chỉ được mang đi công tác khi thật sự cần thiết và phải được sự đồng ý của người chỉ huy.

4. Mua sắm, quản lý, khai thác, sử dụng, bảo đảm kỹ thuật và thanh xử lý thực hiện theo Điều 12 của Quy định này.

Điều 14. Bảo đảm an toàn thông tin, an ninh mạng thiết bị mạng

1. Mua sắm, quản lý, khai thác, sử dụng và bảo đảm kỹ thuật và thanh xử lý thực hiện theo Điều 12 của Quy định này; khi đưa vào sử dụng phải gỡ bỏ tài khoản mặc định; không sử dụng cấu hình mặc định của thiết bị; tắt các giao diện không sử dụng trên thiết bị.

2. Người dùng không có chức năng quản trị hệ thống thì không được phép truy nhập, cấu hình các thiết bị mạng.

Điều 15. Bảo đảm an toàn thông tin, an ninh mạng thiết bị lưu trữ thông tin

1. Thiết bị lưu trữ ngoài sử dụng để lưu trữ, trao đổi tài liệu điện tử quân sự phải có giải pháp bảo đảm an toàn thông tin, an ninh mạng hoặc do cơ quan cơ yếu cấp phát.

2. Các cơ quan, đơn vị phải quản lý vật mang tin điện tử theo hướng dẫn của cơ quan công nghệ thông tin Quân chủng.

3. Vật mang tin điện tử của cơ quan, đơn vị chỉ được mang đi công tác khi thật sự cần thiết và phải được sự đồng ý của người chỉ huy.

4. Vật mang tin điện tử không còn sử dụng phải xóa dữ liệu an toàn, khi thanh xử lý phải phá hủy vật lý (nếu vật mang tin điện tử do Cơ yếu cung cấp phải trả lại cho cơ quan cơ yếu trực tiếp cấp phát).

Điều 16. Bảo đảm an toàn thông tin, an ninh mạng thiết bị ngoại vi

1. Mua sắm, quản lý, khai thác, sử dụng và bảo đảm kỹ thuật thực hiện theo Điều 12 của Quy định này.

2. Tắt chức năng kết nối không dây trên các thiết bị ngoại vi.

3. Xóa sạch bộ nhớ đối với các loại máy in, máy phô tô, máy quét có chức năng lưu trữ dữ liệu ngay sau khi in, phô tô hoặc quét tài liệu quân sự.

4. Điện thoại thông minh, máy tính bảng, thiết bị di động cá nhân khác có khả năng lưu trữ, trao đổi dữ liệu, thông tin điện tử khi được phép sử dụng phải thiết lập về trạng thái cấu hình mặc định; vô hiệu hóa các tính năng không được phép sử dụng; gỡ bỏ các ứng dụng không cần thiết, không được phép sử dụng; khóa tính năng tự động cài đặt, kết nối.

5. Đặt mật khẩu phức tạp, vô hiệu hóa các cổng giao tiếp không sử dụng, kiểm soát thiết bị nhớ ngoài và cập nhật thường xuyên cho các thiết bị sử dụng giao thức mạng Internet (IP).

Mục 6
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG MẠNG MÁY TÍNH - HỆ THỐNG THÔNG TIN

Điều 17. Tổ chức, triển khai mạng máy tính - hệ thống thông tin

1. Hồ sơ thiết kế hệ thống mạng nội bộ của cơ quan, đơn vị phải được cơ quan công nghệ thông tin Quân chủng thẩm định, cấp có thẩm quyền phê duyệt.

2. Phát triển, mở rộng hạ tầng mạng máy tính quân sự qua đường truyền dẫn của doanh nghiệp bao gồm: Đường truyền hữu tuyến điện, đường truyền vô tuyến điện, đường truyền vệ tinh, đường truyền viba, đường truyền thông tin di động chỉ được thực hiện khi đáp ứng các điều kiện sau:

a) Sử dụng hạ tầng truyền dẫn của Tập đoàn Công nghiệp - Viễn thông Quân đội hoặc hạ tầng mạng doanh nghiệp nhà nước khác trong trường hợp Tập đoàn Công nghiệp - Viễn thông Quân đội không bảo đảm được hạ tầng;

b) Sử dụng kênh truyền độc lập với kênh truyền kinh doanh;

c) Có giải pháp bảo đảm an toàn thông tin, an ninh mạng phù hợp, được Tập đoàn Công nghiệp - Viễn thông Quân đội hoặc Bộ Tư lệnh 86 giám sát thường xuyên, liên tục;

d) Được Binh chủng Thông tin liên lạc hoặc Bộ Tư lệnh 86 thẩm định, quyết định;

đ) Triển khai giải pháp bảo mật cơ yếu (nếu có).

3. Hệ thống mạng nội bộ của cơ quan, đơn vị phải được thiết kế, lắp đặt theo mô hình mạng máy tính an toàn hoặc nâng cao theo hướng dẫn tại Phụ lục I ban hành kèm theo Quy định này; triển khai, vận hành gồm các nội dung sau:

a) Phân chia mạng máy tính thành các vùng mạng theo chức năng, cấp độ bảo mật và kiểm soát truy nhập giữa các vùng bằng tường lửa và các thiết bị bảo đảm an toàn thông tin, an ninh mạng khác;

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

c) Che giấu và tránh truy nhập trực tiếp từ bên ngoài vào các địa chỉ mạng bên trong (địa chỉ mạng trong phải được thiết lập theo chuẩn RFC 1918 (chuẩn khuyến nghị của thế giới về đặt địa chỉ cho mạng riêng) gồm 3 dải: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16);

d) Xây dựng phương án dự phòng về kết nối và thiết bị mạng;

đ) Triển khai thiết bị bảo mật đường truyền;

e) Cập nhật bản nâng cấp và bản vá lỗi cho các thiết bị mạng khi có hướng dẫn của cơ quan công nghệ thông tin Quân chủng;

g) Triển khai các thiết bị an toàn thông tin mạng, hệ thống phòng, chống phần mềm độc hại, công cụ phân tích đánh giá an toàn thông tin, an ninh mạng (có bản quyền, nguồn gốc xuất xứ rõ ràng và được kiểm tra an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng);

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

i) Tổ chức cấu hình ghi nhật ký điện tử (log) trên các thiết bị mạng, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận, lưu giữ và được quản lý theo khoản 6 Điều 19 của Quy định này.

Điều 18. Quản lý cấp độ an toàn thông tin đối với hệ thống thông tin

1. Khi triển khai, sử dụng hệ thống thông tin phải tiến hành phân loại và quản lý theo cấp độ an toàn thông tin được quy định tại Thông tư 160/2016/TT-BQP ngày 20 tháng 10 năm 2016 của Bộ Quốc phòng và báo cáo theo quy định.

2. 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) Chủ quản hệ thống thông tin có trách nhiệm lập hồ sơ cấp độ và đề xuất phương án bảo đảm an toàn thông tin phù hợp với cấp độ đó;

c) Tiêu chí xác định cấp độ an toàn thông tin cho hệ thống thông tin thực hiện theo hướng dẫn của cơ quan công nghệ thông tin Quân chủng.

3. 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:

- Đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Cơ quan công nghệ thông tin Quân chủng thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Chủ quản hệ thống thông tin 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:

- Chủ quản hệ thống thông tin lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Bộ Tư lệnh 86 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, chủ quản hệ thống thông tin 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:

- Chủ quản hệ thống thông tin lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Bộ Tư lệnh 86 chủ trì phối hợp với các cơ quan chức năng của Bộ Quốc phòng thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Chủ quản hệ thống thông tin trình Bộ Quốc phòng 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):

- Chủ quản hệ thống thông tin lập hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Bộ Tư lệnh 86 chủ trì phối hợp với các cơ quan chức năng trong và ngoài Bộ Quốc phòng thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin;

- Chủ quản hệ thống thông tin trình Bộ Quốc phòng phê duyệt phương án bảo đảm an toàn thông tin;

- Bộ Quốc phòng trình Thủ tướng Chính phủ phê duyệt hồ sơ đề xuất cấp độ và quyết định bổ sung danh mục thuộc các hệ thống thông tin quan trọng quốc gia.

Điều 19. Quản trị mạng máy tính - hệ thống thông tin

1. Cấu hình mạng máy tính - hệ thống thông tin phải đúng theo hồ sơ thiết kế, tài liệu kỹ thuật đã được thẩm định và phê duyệt.

2. Kiểm soát truy nhập mạng

a) Trang bị công nghệ thông tin tham gia vào mạng máy tính - hệ thống thông tin phải đáp ứng các quy định tại Mục 5 của Quy định này và phải được quản lý kết nối bằng địa chỉ vật lý (MAC), địa chỉ mạng (IP);

b) Thiết bị chuyển mạch phải được gắn địa chỉ vật lý của các thiết bị được phép truy nhập mạng trên từng cổng (cấu hình Mac-Accesslist, Port Secure);

c) Thiết bị tường lửa phải được cấu hình kiểm soát truy nhập cho từng địa chỉ mạng theo dịch vụ cụ thể;

d) Máy tính dùng cho quản trị hệ thống chỉ cài đặt các công cụ, phần mềm kiểm tra, giám sát, đánh giá các nguy cơ gây mất an toàn thông tin; không sử dụng để phục vụ các nghiệp vụ khác;

đ) Khi truy nhập xa phục vụ mục đích quản trị phải thực hiện bằng các giao thức truy nhập an toàn theo quy định (ví dụ giao thức SSH v2.0, Ipsec-IPESP).

3. Kiểm soát truy nhập ứng dụng, dịch vụ

a) Người dùng không được sử dụng tài khoản của người khác;

b) Thiết lập chính sách khóa tài khoản truy nhập ứng dụng nếu đăng nhập thất bại liên tiếp 03 lần trong vòng 15 phút hoặc áp dụng các biện pháp chống dò tìm mật khẩu như CAPTCHA, chặn đăng nhập tài khoản theo IP;

c) Giám sát hoạt động phiên làm việc; phát hiện, cảnh báo đến người sử dụng về truy nhập bất thường; tạm thời khóa tài khoản khi phát hiện quá trình truy nhập vi phạm chính sách (Policy) an toàn thông tin, an ninh mạng có thể gây nguy hại đến dữ liệu cá nhân hoặc hệ thống.

4. Cơ quan, đơn vị phải tổ chức giám sát mạng máy tính - hệ thống thông tin. Nội dung cơ bản cần giám sát gồm trạng thái hoạt động (lưu lượng mạng, thay đổi cấu hình, thiết lập chính sách của thiết bị, tài nguyên mạng), kết nối, dữ liệu, giao thức, dịch vụ, mã độc.

5. Chủ quản hệ thống thông tin phải xây dựng, ban hành, vận hành quy chế, quy định sử dụng đối với mạng máy tính - hệ thống thông tin đang quản lý.

6. Quản lý, xử lý bản ghi nhật ký điện tử

a) Các cơ quan, đơn vị phải thực hiện việc thiết lập và lưu trữ các bản ghi nhật ký điện tử trên các hệ thống thông tin ít nhất 03 tháng nhằm bảo đảm các sự kiện xảy ra trên hệ thống được ghi nhận và lưu giữ;

b) Bản ghi nhật ký điện tử sự kiện (event log) cần ghi lại địa chỉ mạng (IP),

thời gian và các hành động gồm: Quá trình đăng nhập hệ thống, tạo lập, cập nhật, sao chép hoặc xóa dữ liệu, các hành vi xem, thiết lập cấu hình hệ thống, việc thiết lập các kết nối bất thường vào và ra hệ thống, thay đổi quyền truy nhập hệ thống;

c) Các cơ quan, đơn vị duy trì hệ thống thông tin có trách nhiệm cung cấp toàn bộ bản ghi nhật ký điện tử cho cơ quan chức năng để giám sát, bảo vệ, cảnh báo;

d) Các bản ghi nhật ký điện tử phải được bảo vệ an toàn nhằm phục vụ công tác thanh tra, kiểm tra đánh giá an toàn thông tin, an ninh mạng;

đ) Thường xuyên duy trì việc theo dõi bản ghi nhật ký điện tử hệ thống và các sự kiện khác có liên quan để kịp thời phát hiện và ứng cứu sự cố an toàn thông tin, an ninh mạng.

Điều 20. Bảo đảm an toàn máy chủ

1. Thực hiện bảo đảm an toàn vật lý và môi trường cho máy chủ theo Điều 6 của Quy định này.

2. Máy chủ phải được cấu hình riêng biệt về mặt lô-gíc hoặc vật lý để phục vụ cho từng ứng dụng tương ứng.

3. Phần mềm trước khi được cài đặt trên máy chủ phải bảo đảm an toàn theo quy định tại Mục 4 của Quy định này.

4. Cơ sở dữ liệu trên máy chủ phải bảo đảm an toàn theo quy định tại Điều 9 của Quy định này.

5. Tất cả các dịch vụ, các ứng dụng hoặc các giao thức không cần thiết chạy trên máy chủ phải được gỡ bỏ hoặc vô hiệu hóa. Xóa bỏ các tài khoản mặc định, tài khoản không sử dụng và không sử dụng cấu hình mặc định.

6. Máy chủ phải được kích hoạt tính năng tường lửa; phải được cài đặt phần mềm ngăn chặn xâm nhập, phòng chống mã độc và các phần mềm này phải được cập nhật thường xuyên.

Điều 21. Ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự

1. Các ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự phải đảm bảo an toàn theo các quy định tại Mục 4 của Quy định này.

2. Cơ quan, đơn vị quản lý trực tiếp các ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự phải xây dựng quy chế, quy định về quản lý, vận hành, khai thác và bảo đảm an toàn thông tin, an ninh mạng.

3. Cơ quan, đơn vị quản lý trực tiếp các ứng dụng, dịch vụ có trách nhiệm tập huấn, hướng dẫn cho người dùng về quy trình sử dụng an toàn, cập nhật, nâng cấp các ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự và bảo đảm an toàn dữ liệu thuộc phạm vi quản lý.

Điều 22. Quy định đối với người dùng

1. Hiểu biết cơ bản về máy tính, mạng máy tính; sử dụng thành thạo tin học văn phòng; phải được huấn luyện và sử dụng thuần thục phần mềm, hệ thống

thông tin theo đúng chức trách, nhiệm vụ được giao.

2. Không sử dụng các dịch vụ ngoài phạm vi cho phép, phần mềm, dịch vụ mạng cho mục đích cá nhân.

3. Có trách nhiệm phòng, chống phần mềm độc hại, hạn chế các rủi ro do phần mềm độc hại gây ra; không tự ý cài đặt hoặc gỡ bỏ hệ thống phòng, chống phần mềm độc hại trên máy tính khi chưa được sự đồng ý của cơ quan phụ trách công nghệ thông tin.

4. Khi phát hiện bất kỳ dấu hiệu bất thường trên máy tính, mạng máy tính có khả năng liên quan đến việc nhiễm phần mềm độc hại, người dùng phải thông báo ngay cho cơ quan phụ trách công nghệ thông tin để xử lý.

Điều 23. Bảo đảm kỹ thuật, mở rộng, nâng cấp, thu hồi, hủy bỏ mạng máy tính - hệ thống thông tin

1. Khi bảo đảm kỹ thuật mạng máy tính - hệ thống thông tin phải có giải pháp không làm gián đoạn hoạt động của hệ thống, mất mát dữ liệu và phải được phép của chủ quản hệ thống thông tin; phải được thực hiện bởi nhân viên có chuyên môn kỹ thuật công nghệ thông tin; các trang bị công nghệ thông tin riêng lẻ trong hệ thống mạng thực hiện theo quy định tại Điều 12 của Quy định này.

2. Khi mở rộng, nâng cấp mạng máy tính - hệ thống thông tin phải xuất phát từ nhu cầu nhiệm vụ, được cơ quan chuyên môn thẩm định và cấp có thẩm quyền phê duyệt.

3. Mạng máy tính - hệ thống thông tin không còn sử dụng phải được thu hồi, hủy bỏ theo đúng quy định; thông báo cho cơ quan Cơ yếu trực tiếp triển khai phương án bảo mật để xử lý, thu hồi các nội dung liên quan (nếu có).

Mục 7
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG TRONG PHÁT TRIỂN CÔNG NGHỆ THÔNG TIN

Điều 24. Xây dựng đề án, dự án, nhiệm vụ có ứng dụng công nghệ thông tin

1. Khi đề xuất xây dựng phải có các giải pháp, dự toán kinh phí tối thiểu 10% cho nội dung bảo đảm an toàn thông tin, an ninh mạng và kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng theo đúng quy định.

2. Phải được các cơ quan chuyên môn công nghệ thông tin thẩm định trước khi trình cấp có thẩm quyền phê duyệt.

3. Xác định yêu cầu bảo mật thông tin bằng mật mã để xây dựng giải pháp bảo mật cơ yếu phù hợp, đồng bộ.

Điều 25. Triển khai đề án, dự án, nhiệm vụ có ứng dụng công nghệ thông tin

1. Mua sắm trang bị công nghệ thông tin, phát triển phần mềm, tích hợp hệ thống, quản lý vận hành hệ thống thực hiện theo Mục 4, Điều 12 Mục 5, Mục 6 của Quy định này.

2. Cơ quan, tổ chức, cá nhân ngoài Quân đội chỉ có thể tham gia vào hoạt động cung cấp lắp đặt, đào tạo, sửa chữa, không được tham gia vào việc quản trị và vận hành hệ thống thông tin.

3. Người bên ngoài Quân đội nếu được tuyển dụng hoặc thuê vào làm việc trong các dự án phát triển công nghệ thông tin của Quân chủng phải thực hiện đúng quy trình, nguyên tắc tuyển chọn công dân vào phục vụ Quân đội và tuân thủ nghiêm ngặt cam kết không tiết lộ thông tin kèm theo hình thức xử lý nếu vi phạm trong nội dung của các hợp đồng.

4. Người bên ngoài Quân đội khi tham gia vào các dự án của một số hệ thống công nghệ cao, quan trọng thì cơ quan, đơn vị chủ trì đề án, dự án, nhiệm vụ phải thực hiện đúng các quy định của Bộ Quốc phòng về tiêu chuẩn chính trị, nguyên tắc tuyển chọn, điều động người vào làm việc ở cơ quan, đơn vị trọng yếu, cơ mật.

Mục 8
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG TRONG SỬ DỤNG INTERNET

Điều 26. Quản lý, cung cấp và sử dụng mạng Internet

1. Các cơ quan, đơn vị chỉ được kết nối Internet khi được Quân chủng cấp phép.

2. Quy trình đăng ký, cấp phép sử dụng dịch vụ Internet:

a) Cơ quan, đơn vị có nhu cầu sử dụng dịch vụ Internet gửi hồ sơ về Ban Công nghệ thông tin/Bộ Tham mưu;

b) Hồ sơ xin cấp phép sử dụng dịch vụ Internet gồm:

- Đơn xin cấp phép sử dụng dịch vụ Internet, thực hiện theo Mẫu số 01 tại Phụ lục IV kèm theo Quy định này;

- Bản cam kết sử dụng dịch vụ Internet theo Mẫu số 02 tại Phụ lục IV kèm theo Quy định này.

c) Ban Công nghệ thông tin/Bộ Tham mưu tiếp nhận hồ sơ, chủ trì, phối hợp với các cơ quan liên quan tổ chức thẩm định hồ sơ; trong thời hạn 20 ngày làm việc, kể từ ngày nhận đủ hồ sơ phải trình lên Tư lệnh Quân chủng xem xét, quyết định. Trường hợp Tư lệnh Quân chủng không cấp phép, Ban Công nghệ thông tin/Bộ Tham mưu phải thông báo bằng văn bản và nêu rõ lý do để cơ quan, đơn vị xin cấp phép biết.

3. Phải sử dụng dịch vụ Internet của Tập đoàn Công nghiệp - Viễn thông Quân đội.

4. Các cơ quan, đơn vị phải quản lý theo đúng mục đích sử dụng, kiểm soát số lượng các kết nối theo đúng quyết định cấp phép.

5. Khi triển khai mạng Internet phải sử dụng dây, cáp, thiết bị phân biệt rõ ràng về nhãn mác, màu sắc với mạng quân sự (sử dụng cáp mạng màu trắng cho mạng Internet, cáp mạng màu xanh cho mạng quân sự).

6. Chỉ được kết nối mạng Internet bằng cáp mạng trừ các trường hợp sau:

a) 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:

- Thiết bị phần cứng đạt chuẩn 802.11 trở lên;

- Áp dụng mã hóa dữ liệu truyền nhận sử dụng thuật toán mã hóa an toàn;

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

- Triển khai các giải pháp nhằm giám sát, phát hiện và ngăn chặn truy nhập trái phép;

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

b) Chỉ huy các viện, học viện, nhà trường, doanh nghiệp trong Quân chủng 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 điểm a khoản này.

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

8. Việc trao đổi thông tin, dữ liệu một chiều giữa máy tính quân sự và máy tính Internet được thực hiện thông qua đĩa CD, DVD hoặc qua máy tính trung gian chạy hệ điều hành khác Windows kết hợp sử dụng vật mang tin điện tử chuyên dụng do Bộ Tư lệnh 86, ngành Cơ yếu cung cấp; trước khi thực hiện sao chép, dịch chuyển dữ liệu phải kiểm tra an toàn thông tin và làm sạch mã độc.

9. Truyền dữ liệu hạn chế một chiều từ máy tính thuộc mạng máy tính Internet vào máy tính thuộc mạng máy tính quân sự hoặc ngược lại phải được thực hiện qua thiết bị truyền dẫn dữ liệu một chiều an toàn và có giải pháp giám sát, bảo đảm an toàn thông tin, an ninh mạng, được Bộ Tư lệnh 86 thẩm định, quyết định.

Điều 27. 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 không được sử dụng thông tin cá nhân gắn với cấp bậc, chức vụ, vị trí công tác, phiên hiệu đơn vị và có mật khẩu phức tạp để bảo vệ.

2. Mỗi cá nhân phải có trách nhiệm bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng; không được phép cung cấp, sử dụng thông tin cá nhân của người khác khi chưa được người đó đồng ý.

3. Tạo lập, lưu trữ, chuyển nhận thông tin quân sự trên mạng Internet phải được sự đồng ý của cơ quan bảo vệ an ninh và người chỉ huy cấp trên trực tiếp

cho phép; phải sử dụng giải pháp bảo mật phù hợp.

4. Các cá nhân khi phát hiện thông tin quân sự bị lộ lọt trên mạng Internet phải thông báo ngay với cơ quan bảo vệ an ninh và cơ quan chức năng để kịp thời giải quyết.

Điều 28. Quản lý các trang, cổng thông tin điện tử và ứng dụng trên Internet

1. Các cơ quan, đơn vị khi thiết lập trang, cổng thông tin điện tử trên mạng Internet thực hiện theo quy định tại Thông tư 110/2014/TT-BQP ngày 22/8/2014 của Bộ Quốc phòng.

2. Các trang, cổng thông tin điện tử và ứng dụng của Quân chủng trên mạng Internet phải được Bộ Tư lệnh 86 kiểm tra, đánh giá an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng.

3. Các trang, cổng thông tin điện tử và ứng dụng của Quân chủng trên mạng Internet phải được cài đặt tại trung tâm dữ liệu thuộc Bộ Tư lệnh 86 trên Internet; quản lý, giám sát, cảnh báo và triển khai các giải pháp bảo đảm an toàn thông tin, an ninh mạng và ứng cứu khắc phục sự cố.

3. Phải xây dựng, ban hành, vận hành quy chế, quy định khi đưa vào sử dụng.

Điều 29. Sử dụng thư điện tử và các trang mạng xã hội trên Internet

1. Quân nhân tham gia sử dụng các trang mạng xã hội cho mục đích cá nhân phải chấp hành các quy định của pháp luật về bảo vệ bí mật nhà nước, bí mật quân sự, không được tiết lộ thông tin cá nhân và cơ quan, đơn vị như: Thông tin về cấp bậc, chức vụ, hoạt động quân sự; sơ đồ, địa chỉ đơn vị, hình ảnh mặc quân phục, hình ảnh trang bị, hình ảnh hoạt động đơn vị.

2. 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 chính trị tại các cơ quan, đơn vị.

3. Quân nhân chỉ được sử dụng tài khoản thư điện tử công vụ của cơ quan, đơn vị thuộc Bộ Quốc phòng hoặc cơ quan nhà nước để trao đổi thông tin.

4. 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, 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.

Mục 9
ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ VÀ XÁC ĐỊNH NGUYÊN NHÂN MẤT AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 30. Nguyên tắc điều phối và ứng cứu sự cố

1. Tuân thủ các quy định pháp luật về an toàn thông tin, an ninh mạng và các quy định khác có liên quan.

2. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

3. Phối hợp, hiệp đồng chặt chẽ giữa các cơ quan, đơn vị trong hoạt động điều phối và ứng cứu sự cố, bảo đảm tuân thủ đúng quy trình.

4. Điều phối và ứng cứu sự cố theo phân cấp, theo khu vực, trong phạm vi thuộc quyền; phát huy trách nhiệm của chủ quản hệ thống thông tin.

5. Bảo đảm bí mật thông tin khi tham gia thực hiện các hoạt động điều phối và ứng cứu sự cố an toàn thông tin, an ninh mạng.

Điều 31. Tổ chức lực lượng điều phối và ứng cứu sự cố

1. Quân chủng thành lập Tổ ứng cứu sự cố an toàn thông tin, an ninh mạng (sau đây gọi tắt là Tổ ứng cứu sự cố Quân chủng) gồm: Tổ trưởng là Đồng chí Phó Tham mưu trưởng Quân chủng phụ trách ngành Công nghệ thông tin; thành phần tham gia có lực lượng công nghệ thông tin, cơ yếu, bảo vệ an ninh, thông tin liên lạc và các lực lượng khác có liên quan; cơ quan thường trực, nòng cốt là cơ quan công nghệ thông tin Quân chủng; lực lượng trực ban ứng cứu sự cố Quân chủng do cơ quan công nghệ thông tin Quân chủng tổ chức và thực hiện. Tổ ứng cứu sự cố Quân chủng có nhiệm vụ và quyền hạn sau:

a) Tổ chức điều phối, ứng cứu các sự cố an toàn thông tin, an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý của Quân chủng PK-KQ và tham gia hoạt động ứng cứu sự cố an toàn thông tin, an ninh mạng theo điều hành của Cơ quan điều phối (Bộ Tư lệnh 86); chỉ đạo, hướng dẫn nghiệp vụ về hoạt động điều phối ứng cứu sự cố, triển khai các phương án ứng cứu sự cố an toàn thông tin, an ninh mạng trong Quân chủng;

b) Sử dụng các biện pháp nghiệp vụ, trang bị, phương tiện kỹ thuật, các biện pháp khác theo chức năng nhiệm vụ được giao và tuân thủ quy định của pháp luật;

c) Thu thập thông tin, tài liệu, phân tích, cảnh báo và ứng cứu sự cố theo phương châm bốn tại chỗ, bao gồm: chỉ huy tại chỗ; lực lượng tại chỗ; quy trình, trang bị tại chỗ; hậu cần tại chỗ;

d) Tổ chức giám sát, cảnh báo sớm sự cố an toàn thông tin, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý;

đ) Tổ chức huấn luyện, đào tạo, diễn tập nâng cao nhận thức, trình độ về ứng cứu sự cố an toàn thông tin, an ninh mạng trong Quân chủng và tham gia khi Bộ Quốc phòng tổ chức.

2. Các đơn vị trực thuộc Quân chủng thành lập Tổ ứng cứu sự cố an toàn thông tin, an ninh mạng trên cơ sở tổ chức, nhân lực hiện có và hoạt động kiêm nhiệm (sau đây gọi tắt là Tổ ứng cứu sự cố đơn vị), gồm: Tổ trưởng là chỉ huy cơ quan, đơn vị phụ trách công nghệ thông tin; thành phần tham gia có lực lượng công nghệ thông tin, cơ yếu, bảo vệ an ninh, thông tin liên lạc và các lực lượng khác có liên quan; cơ quan thường trực, nòng cốt là cơ quan phụ trách công nghệ thông tin; lực lượng trực ban ứng cứu sự cố đơn vị do cơ quan phụ trách công nghệ thông tin tổ chức và thực hiện. Tổ ứng cứu sự cố đơn vị có nhiệm vụ và quyền hạn sau:

a) Tổ chức ứng cứu các sự cố an toàn thông tin, an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý và tham gia hoạt động ứng cứu sự cố an toàn thông tin, an ninh mạng theo điều hành của Tổ ứng cứu sự cố Quân chủng;

b) Sử dụng các biện pháp nghiệp vụ, trang bị, phương tiện kỹ thuật, các biện pháp khác theo chức năng nhiệm vụ được giao và tuân thủ quy định của pháp luật;

c) Thu thập thông tin, tài liệu, phân tích, cảnh báo và ứng cứu sự cố theo phương châm bốn tại chỗ, bao gồm: chỉ huy tại chỗ; lực lượng tại chỗ; quy trình, trang bị tại chỗ; hậu cần tại chỗ;

d) Tổ chức giám sát, cảnh báo sớm sự cố an toàn thông tin, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý;

đ) Tham gia huấn luyện, đào tạo, diễn tập nâng cao nhận thức, trình độ về ứng cứu sự cố an toàn thông tin, an ninh mạng do cấp trên tổ chức.

Điều 32. Hoạt động điều phối và ứng cứu sự cố

Hoạt động điều phối và ứng cứu sự cố an toàn thông tin, an ninh mạng được thực hiện theo quy trình tại Phụ lục III ban hành kèm theo Quy định này, gồm các bước cơ bản sau:

1. Thông báo, tiếp nhận, xử lý thông tin về sự cố.

2. Tổ chức ứng cứu sự cố.

3. Nội dung ứng cứu sự cố.

4. Đánh giá, bàn giao kết quả ứng cứu sự cố.

5. Kết thúc điều phối, ứng cứu sự cố.

Điều 33. Xác định nguyên nhân mất an toàn thông tin, an ninh mạng

1. Khi xảy ra vụ việc mất an toàn thông tin, an ninh mạng nghiêm trọng mà cần phải điều tra làm rõ nguyên nhân, các cơ quan, đơn vị phải bảo vệ hiện trường vi phạm, báo cáo kịp thời theo phân cấp đến Phòng Bảo vệ - An ninh và Ban Công nghệ thông tin/Bộ Tham mưu.

2. Khi nhận được thông tin về vụ việc vi phạm cần xác minh, làm rõ, các cơ quan chức năng (Ban Công nghệ thông tin/Bộ Tham mưu, Phòng Bảo vệ - An ninh) phải chủ trì, phối hợp với các cơ quan, đơn vị có liên quan, báo cáo Tham mưu trưởng Quân chủng thành lập đoàn công tác để thu thập, phân tích chứng cứ xác định nguyên nhân, mức độ vi phạm về an toàn thông tin, an ninh mạng đề xuất biện pháp xử lý, báo cáo. Đối với vụ việc vi phạm an toàn thông tin mạng do Ban Công nghệ thông tin/Bộ Tham mưu phụ trách; đối với vụ việc vi phạm an ninh thông tin, an ninh mạng do Phòng Bảo vệ -An ninh phụ trách.

Chương III
QUẢN LÝ AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 34. Quy định nội bộ về an toàn thông tin, an ninh mạng

Các cơ quan, đơn vị có trách nhiệm xây dựng, ban hành các văn bản nội bộ về công tác quản lý, bảo đảm an toàn thông tin, an ninh mạng theo hướng dẫn của cơ quan công nghệ thông tin Quân chủng.

Điều 35. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng

1. Hình thức, chế độ kiểm tra

a) Cơ quan, đơn vị tự kiểm tra:

- Thủ trưởng cơ quan, đơn vị chỉ đạo các bộ phận chuyên môn kiểm tra định kỳ an toàn thông tin, an ninh mạng trong cơ quan, đơn vị mình, đơn vị thuộc quyền và khi có dấu hiệu vi phạm an toàn thông tin, an ninh mạng;

- Việc kiểm tra, đánh giá an toàn thông tin, an ninh mạng không được giao cho cơ quan, tổ chức ngoài Quân đội thực hiện.

b) Quân chủng kiểm tra:

- Thường xuyên 01 lần/năm đối với các cơ quan, đơn vị thuộc Quân chủng;

- Theo kế hoạch đối với các cơ quan, đơn vị có trong kế hoạch đã được phê duyệt;

- Đột xuất đối với các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn thông tin, an ninh mạng.

2. Nội dung kiểm tra

a) Quán triệt và xây dựng văn bản quy định về công tác đảm bảo an toàn thông tin, an ninh mạng;

b) Các biện pháp tổ chức bảo đảm an toàn thông tin, an ninh mạng;

c) Các nội dung về bảo đảm an toàn thông tin, an ninh mạng tại Điều 5 của Quy định này.

3. Thành phần đoàn kiểm tra

a) Đoàn kiểm tra của Quân chủng gồm: Bộ Tham mưu (chủ trì), Cục Chính trị, Văn phòng Bộ Tư lệnh, các cơ quan công nghệ thông tin, cơ yếu, thông tin, tác chiến và các thành phần khác có liên quan;

b) Đoàn kiểm tra của các cơ quan, đơn vị gồm: Cơ quan tham mưu hoặc cơ quan phụ trách công nghệ thông tin (chủ trì), đại diện các lực lượng công nghệ thông tin, cơ yếu, thông tin, tác chiến, bảo vệ an ninh, bảo mật-lưu trữ và các thành phần khác có liên quan.

Điều 36. Chế độ báo cáo

1. Định kỳ hàng tháng, các cơ quan, đơn vị có trách nhiệm báo cáo kết quả công tác bảo đảm an toàn thông tin, an ninh mạng theo quy định về Bộ Tham mưu

(qua Ban Công nghệ thông tin) để tổng hợp, báo cáo Thủ trưởng Bộ Tư lệnh và Bộ Quốc phòng.

2. Trường hợp xảy ra vụ việc mất an toàn thông tin, an ninh mạng nghiêm trọng, các cơ quan, đơn vị phải báo cáo ngay về Bộ Tham mưu (qua Ban Công nghệ thông tin) để tổng hợp, báo cáo và tổ chức ứng cứu, khắc phục sự cố.

Điều 37. Xếp loại an toàn thông tin, an ninh mạng

Xếp loại an toàn thông tin, an ninh mạng đối với các cơ quan, đơn vị trong Quân chủng được thực hiện theo hướng dẫn hàng năm của cơ quan công nghệ thông tin Quân chủng.

Điều 38. Lực lượng bảo đảm an toàn thông tin, an ninh mạng

1. Cơ quan chuyên trách quản lý an toàn thông tin, an ninh mạng Bộ Quốc phòng được tổ chức tại Bộ Tư lệnh 86.

2. Cơ quan chuyên trách quản lý công tác an ninh đối với trang bị công nghệ thông tin trong Bộ Quốc phòng đặt tại Cục Bảo vệ an ninh Quân đội/Tổng cục Chính trị.

3. Lực lượng bảo đảm an toàn thông tin, an ninh mạng của Quân chủng gồm: Lực lượng công nghệ thông tin chuyên trách tại cơ quan công nghệ thông tin Quân chủng, lực lượng kiêm nhiệm công nghệ thông tin tại các cơ quan, đơn vị, lực lượng phối hợp ở các ngành thông tin, cơ yếu, tác chiến, bảo vệ an ninh, bảo mật-lưu trữ và ngành khác có liên quan.

Điều 39. Phân cấp, phối hợp trong kiểm tra, đánh giá an toàn thông tin, an ninh mạng đối với phần mềm và trang bị có thành phần ứng dụng công nghệ thông tin

1. Các cơ quan, đơn vị khi có nhu cầu đưa phần mềm và trang bị có thành phần ứng dụng công nghệ thông tin (chưa được kiểm tra, đánh giá an toàn thông tin, an ninh mạng) vào sử dụng phục vụ nhiệm vụ quân sự, quốc phòng phải phối hợp với cơ quan phụ trách công nghệ thông tin thuộc các cơ quan, đơn vị để lập báo cáo, đề nghị kiểm tra, đánh giá an toàn thông tin, an ninh mạng gửi về cơ quan công nghệ thông tin Quân chủng.

2. Cơ quan công nghệ thông tin Quân chủng có trách nhiệm chủ trì, tổng hợp, báo cáo và phối hợp với các cơ quan chức năng tiến hành kiểm tra, đánh giá an toàn thông tin, an ninh mạng theo đề nghị của các cơ quan, đơn vị.

Điều 40. Xử lý vi phạm an toàn thông tin, an ninh mạng

Các tổ chức, cá nhân vi phạm Quy định này để xảy ra hoặc dẫn đến nguy cơ mất an toàn thông tin, an ninh mạng thì tùy theo tính chất, mức độ vi phạm mà bị xử lý hành chính theo Thông tư 16/2020/TT-BQP ngày 21/02/2020 quy định việc áp dụng các hình thức kỷ luật, trình tự, thủ tục, thời hiệu, thời hạn và thẩm quyền xử lý kỷ luật trong Bộ Quốc phòng hoặc xử lý hình sự theo pháp luật.

Chương IV
TRÁCH NHIỆM CỦA CÁC CƠ QUAN ĐƠN VỊ

Điều 41. Bộ Tham mưu

1. Chỉ đạo các cơ quan, đơn vị thuộc quyền thực hiện các biện pháp bảo đảm công tác an toàn thông tin, an ninh mạng theo Quy định này thuộc phạm vi quản lý.

2. Chỉ đạo Ban Công nghệ thông tin:

a) Chủ trì phối hợp với các cơ quan, đơn vị trong quán triệt, cụ thể hóa, triển khai thực hiện các văn bản pháp luật, quy định của Bộ Quốc phòng về an toàn thông tin, an ninh mạng trong Quân chủng;

b) Chủ trì phối hợp với các cơ quan, đơn vị nghiên cứu, đề xuất triển khai áp dụng các giải pháp kỹ thuật bảo đảm an toàn thông tin, an ninh mạng;

c) Chủ trì phối hợp với các cơ quan, đơn vị tổ chức phân loại, đánh giá cấp độ an toàn thông tin cho các hệ thống thông tin;

d) Chủ trì đề xuất, phối hợp với các cơ quan liên quan tổ chức kiểm tra an toàn thông tin, an ninh mạng cho trang bị, phần mềm công nghệ thông tin khi mua sắm, phát triển và đưa vào sử dụng;

đ) Chủ trì phối hợp với các cơ quan, đơn vị có liên quan xây dựng kế hoạch, tổ chức kiểm tra, đánh giá, thông báo, báo cáo công tác bảo đảm an toàn thông tin, an ninh mạng;

e) Chủ trì phối hợp với các cơ quan, đơn vị có liên quan xác định nguyên nhân và đề xuất biện pháp giải quyết các sự cố mất an toàn thông tin, an ninh mạng;

g) Phối hợp với các cơ quan, đơn vị liên quan thẩm định các đề án, dự án, nhiệm vụ có thành phần công nghệ thông tin;

h) Phối hợp với các cơ quan, đơn vị liên quan trong việc tham mưu thực hiện khen thưởng, xử phạt đối với cơ quan, đơn vị, cá nhân trong bảo đảm an toàn thông tin, an ninh mạng;

i) Chủ trì tổ chức các hoạt động điều phối, ứng cứu sự cố an toàn thông tin, an ninh mạng trong Quân chủng;

k) Tổ chức quản trị, giám sát các mạng máy tính-hệ thống thông tin trong Quân chủng;

l) Tổ chức đào tạo, huấn luyện, hướng dẫn nghiệp vụ về bảo đảm an toàn thông tin, an ninh mạng cho các cơ quan, đơn vị trong Quân chủng;

m) Chủ trì quản lý việc đăng ký cấp phép sử dụng Internet trong Quân chủng;

n) Phối hợp với Phòng Cơ yếu trong công tác bảo đảm kỹ thuật trang thiết bị công nghệ thông tin có sử dụng sản phẩm mật mã và triển khai các giải pháp bảo mật của ngành Cơ yếu cho mạng máy tính-hệ thống thông tin;

o) Phối hợp với Phòng Thông tin trong bảo đảm hoạt động hạ tầng truyền dẫn thông tin;

p) Phối hợp với Phòng Bảo vệ - An ninh/Cục Chính trị trong điều tra nguyên nhân vi phạm an ninh thông tin, an ninh mạng;

q) Phối hợp với Văn phòng Bộ Tư lệnh bảo đảm hoạt động của các trang bị, hệ thống ứng dụng công nghệ thông tin cho chuyển nhận văn bản điện tử và các nghiệp vụ văn phòng;

r) Phối hợp với Phòng Điều tra hình sự trong điều tra, giải quyết các loại vi phạm, tội phạm có liên quan đến công nghệ thông tin, mạng viễn thông theo quy định của pháp luật; cùng với Phòng Điều tra hình sự, các phòng ban tham mưu cho Thủ trưởng Bộ Tư lệnh, Thủ trưởng Bộ Tham mưu và lãnh đạo chỉ huy cơ quan, đơn vị trong phòng ngừa vi phạm, tội phạm xảy ra trên không gian mạng.

3. Chỉ đạo Phòng Cơ yếu:

a) Chủ trì, phối hợp với các cơ quan, đơn vị trong quán triệt, tuyên truyền, triển khai thực hiện các văn bản pháp quy của Bộ Quốc phòng về bảo mật thông tin cho các hệ thống thông tin trong Quân chủng;

b) Chủ trì và phối hợp với các cơ quan chức năng trong thực hiện chỉ đạo quản lý, khai thác sử dụng, bảo đảm kỹ thuật các sản phẩm mật mã triển khai trong Quân chủng theo đúng các Quy định của ngành Cơ yếu;

c) Đề xuất, chủ trì xây dựng các văn bản, hướng dẫn về mật mã cơ yếu trong việc bảo mật, xác thực thông tin nhằm bảo đảm an toàn thông tin, an ninh mạng trong Quân chủng;

d) Chủ trì, phối hợp triển khai các giải pháp bảo mật, xác thực thông tin cho các dịch vụ của mạng máy tính bằng kỹ thuật mật mã cơ yếu, triển khai các giải pháp bảo mật bằng kỹ thuật mật mã đối với thông tin mật trong quá trình tạo lập, xử lý, lưu trữ và chuyển nhận;

đ) Phối hợp chặt chẽ với các cơ quan, đơn vị triển khai các giải pháp bảo mật đường truyền cho mạng truyền số liệu quân sự, bảo mật các trung tâm dữ liệu quan trọng và mạng máy tính của các cơ quan, đơn vị, chủ trì triển khai hệ thống chứng thực số trong Quân chủng;

e) Chủ trì, phối hợp thực hiện quản lý hoạt động nghiên cứu, sản xuất, ứng dụng mật mã nhằm bảo đảm an toàn thông tin, an ninh mạng trong Quân chủng;

g) Tham gia điều phối, ứng cứu sự cố an toàn thông tin, an ninh mạng trong Quân chủng.

4. Chỉ đạo Phòng Thông tin:

a) Chủ trì tham mưu, triển khai mở rộng, dự phòng kết nối mạng truyền số liệu quân sự cho các cơ quan, đơn vị trong Quân chủng;

b) Phối hợp với Ban Công nghệ thông tin trong đảm bảo hoạt động của kênh liên lạc, đường truyền của mạng máy tính - hệ thống thông tin;

c) Tham gia điều phối, ứng cứu sự cố an toàn thông tin, an ninh mạng trong Quân chủng.

5. Chỉ đạo Phòng Quân huấn-Nhà trường:

Phối hợp với Ban Công nghệ thông tin xây dựng kế hoạch, kiểm tra, đánh giá hàng năm về huấn luyện an toàn thông tin, an ninh mạng trong Quân chủng.

Điều 42. Cục Chính trị

1. Chỉ đạo các cơ quan, đơn vị thuộc quyền thực hiện các biện pháp bảo đảm công tác an toàn thông tin, an ninh mạng theo Quy định này thuộc phạm vi quản lý.

2. Chỉ đạo Phòng Bảo vệ-An ninh:

a) Chủ trì phối hợp với các cơ quan, đơn vị liên quan trong kiểm tra, đánh giá, kết luận về an ninh thông tin;

b) Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu trong việc xây dựng, triển khai thực hiện các kế hoạch kiểm tra an toàn thông tin, an ninh mạng của Quân chủng;

c) Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu và các cơ quan, đơn vị liên quan trong điều tra, kết luận nguyên nhân gây mất an toàn thông tin mạng; trong việc tham mưu thực hiện khen thưởng, xử phạt đối với cơ quan, đơn vị, cá nhân trong bảo đảm an toàn thông tin, an ninh mạng;

d) Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu trong tổ chức kiểm tra an ninh cho trang bị, phần mềm công nghệ thông tin khi mua sắm, phát triển và đưa vào sử dụng;

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

e) Chủ trì, phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu và các cơ quan, đơn vị liên quan trong phát hiện lộ, lọt bí mật quân sự;

g) Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu và các cơ quan chức năng kiểm tra, xác minh, tham mưu cho thủ trưởng cơ quan, đơn vị xử lý các vụ việc vi phạm quy định về an toàn thông tin, an ninh mạng nhưng chưa cấu thành tội phạm;

h) 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 Quân chủng và bảo vệ bí mật Nhà nước;

i) Chủ trì, phối hợp với các cơ quan chức năng kiểm tra an ninh các trang bị công

nghệ thông tin trước khi đưa vào sử dụng và sau sửa chữa lớn trong Quân chủng;

k) Tham gia điều phối, ứng cứu sự cố an toàn thông tin, an ninh mạng trong Quân chủng.

3. Chỉ đạo Phòng Tuyên huấn:

a) Tuyên truyền nâng cao nhận thức về an toàn thông tin, an ninh mạng trong Quân chủng;

b) Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu và các cơ quan, đơn vị liên quan trong tham mưu, đề xuất khen thưởng đối với các cơ quan, đơn vị có thành tích trong công tác bảo đảm an toàn thông tin, an ninh mạng.

Điều 43. Văn phòng BTL

1. Chủ trì hướng dẫn các cơ quan, đơn vị phân loại, quản lý và sử dụng tài liệu điện tử theo đúng quy định của pháp luật.

2. Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu và các cơ quan, đơn vị có liên quan trong bảo đảm hoạt động của các trang bị, hệ thống ứng dụng công nghệ thông tin cho các nghiệp vụ văn phòng.

3. Phối hợp với Phòng Cơ yếu trong ứng dụng chứng thư số, bảo đảm về bảo mật và xác thực thông tin đối với văn bản điện tử.

Điều 44. Phòng Kế hoạch và Đầu tư

Chủ trì, phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu trong thẩm định, báo cáo các nội dung đầu tư cho bảo đảm an toàn thông tin, an ninh mạng.

Điều 45. Phòng Tài chính

1. Chủ trì thẩm định và quyết toán các nguồn ngân sách bảo đảm an toàn thông tin, an ninh mạng trong Quân chủng trình Tư lệnh Quân chủng phê duyệt.

2. Phối hợp với Ban Công nghệ thông tin/Bộ Tham mưu và các đơn vị liên quan trong quá trình xây dựng, thẩm định các nội dung đầu tư cho bảo đảm an toàn thông tin, an ninh mạng.

Điều 46. Các cơ quan đơn vị trực thuộc Quân chủng

1. Quán triệt, triển khai thực hiện đầy đủ các nội dung, biện pháp về bảo đảm an toàn thông tin, an ninh mạng theo Quy định này.

2. Phối hợp với các cơ quan, đơn vị có liên quan để giải quyết các vấn đề an toàn thông tin, an ninh mạng chung trong toàn Quân chủng.

3. Thường xuyên kiểm tra, quản lý, nắm bắt tình hình quân nhân tham gia hoạt động trên không gian mạng để có biện pháp xử lý kịp thời.

4. Đưa nội dung kiểm tra, rà soát an toàn thông tin, an ninh mạng là một nội dung thực hiện trong "Ngày kỹ thuật" của cơ quan, đơn vị.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 47. Tổ chức thực hiện

1. Ban Công nghệ thông tin/Bộ Tham mưu là cơ quan thường trực giúp Thủ trưởng Bộ Tư lệnh, Bộ Tham mưu hướng dẫn, đôn đốc, kiểm tra, báo cáo thực hiện Quy định này.

2. Quy định này có hiệu lực từ ngày ký và thay thế Quy định bảo đảm an toàn thông tin trong Quân chủng PK-KQ được ban hành kèm theo Quyết định số 3854/QĐ-BTL ngày 12/9/2019 của Tư lệnh Quân chủng.

3. Các cơ quan, đơn vị trong toàn Quân chủng quán triệt, triển khai thực hiện Quy định này. Trong quá trình thực hiện, nếu có vướng mắc kịp thời phản ánh, báo cáo về Bộ Tham mưu (qua Ban Công nghệ thông tin) để xem xét, điều chỉnh, bổ sung./.

Nơi nhận:
- Tư lệnh, Chính ủy;
- Các PTL, Phó Chính ủy[06];
- Thủ trưởng BTM[08];
- Các đầu mối trực thuộc QC[31];
- Các phòng, ban, đơn vị BTM[31];
- Thanh tra QC;
- Ban Pháp chế/VPBTL;
- Lưu: VT, Ban CNTT. T82.

Q. TƯ LỆNH

Trung tướng Vũ Văn Kha

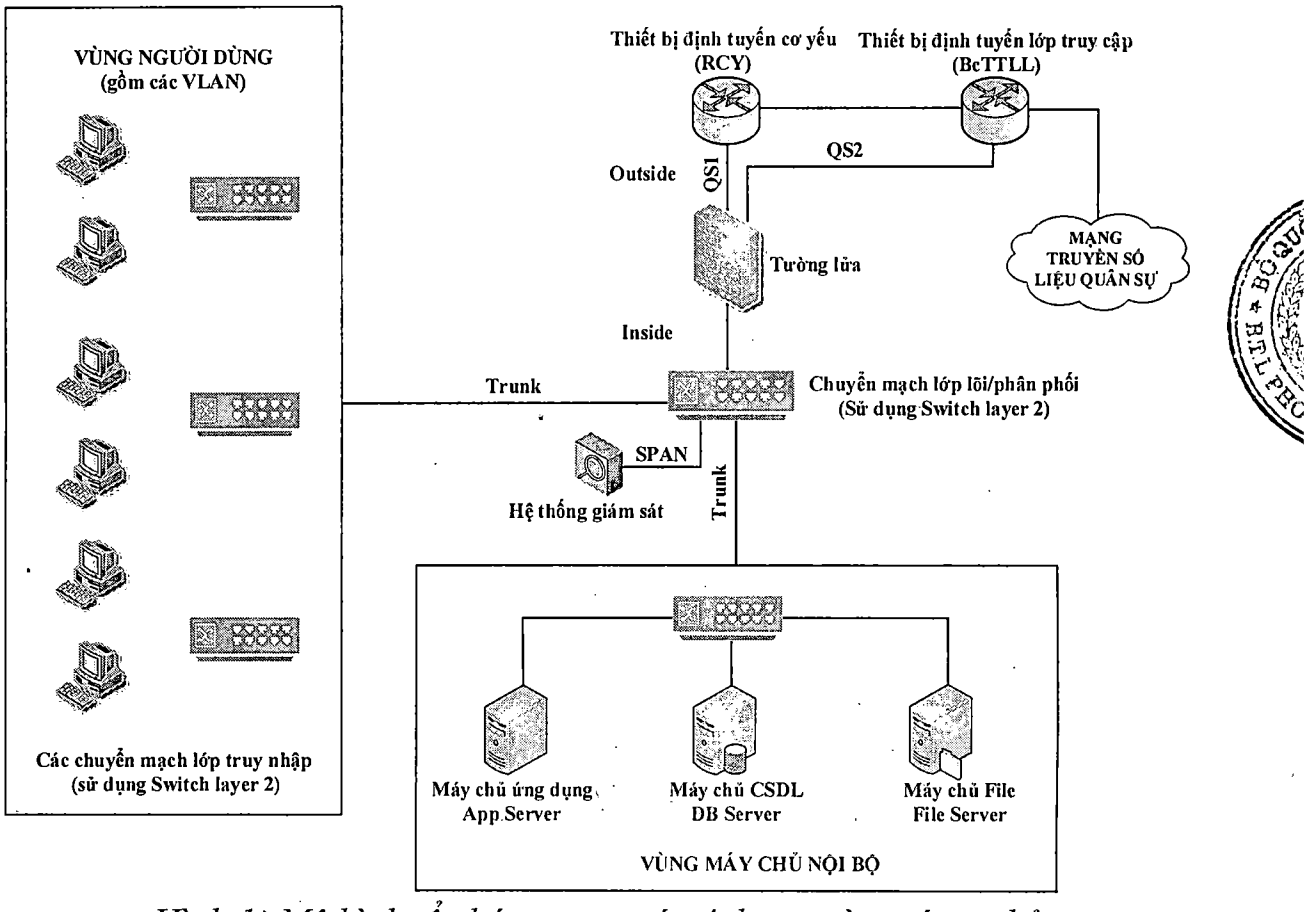
Phụ lục I

MÔ HÌNH MẠNG MÁY TÍNH AN TOÀN MỨC CƠ BẢN VÀ NÂNG CAO

(Kèm theo Quy định số 5067/QyĐ-PKKQ ngày 28 tháng 12 năm 2021 của Tư lệnh PK-KQ)

1. Mô hình tổ chức mạng máy tính an toàn mức cơ bản

Mô hình tổ chức mạng máy tính an toàn mức cơ bản (Hình 1) được thiết kế dựa trên tổ chức lại hệ thống mạng và khai thác hiệu quả các tính năng bảo đảm an toàn thông tin sẵn có trong các trang bị công nghệ thông tin và trang bị tường lửa. Tổ chức triển khai cụ thể như sau:



Hình 1: Mô hình tổ chức mạng máy tính an toàn mức cơ bản

a) Triển khai thiết bị tường lửa (firewall)

Trang bị 01 thiết bị tường lửa cứng hoặc tường lửa mềm dùng để bảo vệ hệ thống mạng: Thiết lập chính sách bảo vệ người dùng trong mạng nội bộ khi truy cập mạng máy tính quân sự và bảo vệ vùng máy chủ công cộng cho phép truy cập vào từ mạng máy tính quân sự.

Nếu đơn vị chưa được trang bị tường lửa cứng, có thể dùng tường lửa mềm để thay thế như pfSense, Endian...

b) Triển khai các thiết bị định tuyến (router) và chuyển mạch (switch)

- Triển khai thiết bị định tuyến:

Tổ chức 01 thiết bị định tuyến thực hiện các chức năng định tuyến, kết nối

mạng nội bộ (LAN) của đơn vị với mạng máy tính quân sự, định tuyến cho các mạng LAN ảo (VLAN), chuyển dịch địa chỉ (Network Address Translation - NAT) để che dấu toàn bộ mạng nội bộ và kiểm soát truy nhập (Access Control List - ACL) để lọc lưu lượng. Trên thiết bị định tuyến thực hiện:

+ Cấu hình định tuyến mặc định (default route), cấu hình các cổng ảo (Sub Interface) để định tuyến VLAN;

+ Cấu hình NAT nhằm ánh xạ các địa chỉ IP riêng (các dải IP riêng tuân theo chuẩn RFC 1918) trong mạng nội bộ của đơn vị sang các địa chỉ IP chung (IP Public) kết nối với RCY (được thống nhất với cơ quan Cơ yếu). Như vậy, toàn bộ mạng nội bộ của đơn vị đã được che dấu, đảm bảo từ mạng máy tính quân sự không thể khởi tạo kết nối vào các máy tính, máy chủ bên trong mạng nội bộ;

+ Cấu hình kiểm soát truy nhập (ACL) để giới hạn truy cập giữa các VLAN khi cần thiết.

- Triển khai thiết bị switch: Tổ chức 01 switch (layer 2 trở lên) làm chức năng lớp lõi/phân phối và các switch (layer 2) làm chức năng lớp truy cập; các switch này cần phải có khả năng quản trị được, cấu hình tương đương như Cisco Catalyst 2960 để thực hiện các chức năng tạo VLAN, cổng an toàn (Port Security). Trên thiết bị switch thực hiện:

+ Triển khai switch lớp lõi/phân phối: cấu hình phân chia VLAN trên switch lớp lõi/phân phối, nên phân chia thành các VLAN theo vùng máy chủ và các phòng/ban/đơn vị chức năng; kết nối switch lớp lõi/phân phối với switch lớp truy cập qua cổng Trunk, có thể sử dụng giao thức ISL (Inter Switch Link) hoặc 802.1Q; có thể cấu hình VTP mode server (trên switch lớp lõi/phân phối) và cấu hình VTP mode client (trên switch lớp truy cập) để các switch lớp truy cập "học" thông tin cơ sở dữ liệu VLAN từ switch lớp lõi/phân phối;

+ Triển khai các switch lớp truy cập: cấu hình cổng kết nối với switch lớp lõi/phân phối qua cổng Trunk, có thể sử dụng giao thức 802.1Q hoặc ISL; gán các cổng nối với máy tính là chế độ cổng truy cập (mode access) và gán cổng vào VLAN tương ứng; đường Trunk có thể cấu hình EtherChannel để tăng băng thông và dự phòng đường truyền (bó hai hay nhiều đường truyền vật lý thành một đường logic);

+ Triển khai cấu hình cổng an toàn (Port Security) trên switch lớp truy cập để hạn chế máy tính tham gia mạng thông qua địa chỉ vật lý MAC khi cần thiết.

c) Triển khai máy chủ nội bộ

Tại vùng máy chủ nội bộ, thường triển khai các máy chủ chia sẻ tập tin, máy chủ ứng dụng chuyên ngành và máy chủ cở sở dữ liệu của đơn vị; các máy chủ này chỉ được chia sẻ, trao đổi dữ liệu với các máy tính trong mạng nội bộ và không chia sẻ, trao đổi dữ liệu ra ngoài mạng.

d) Triển khai các hệ thống giám sát an toàn thông tin, an ninh mạng

- Hệ thống giám sát an toàn thông tin, an ninh mạng: FMS/FMC, giám sát Log...;

- Hệ thống giám sát hạ tầng: Có thể sử dụng PRTG, Cacti, Zabbix...;

- Hệ thống phát hiện, ngăn chặn xâm nhập IDS/IPS (có thể sử dụng Snort, Suricata... thay thế).

2. Mô hình tổ chức mạng máy tính an toàn mức nâng cao

Triển khai mô hình tổ chức mạng máy tính an toàn mức nâng cao (Hình 2) được thực hiện trên cơ sở đã triển khai mô hình tổ chức mạng máy tính an toàn mức cơ bản và triển khai bổ sung các trang bị an toàn thông tin như: Firewall, NIDS, Log Server, máy tính quản trị. Tổ chức triển khai cụ thể như sau:

a) Triển khai thiết bị tường lửa (firewall)

Trang bị 01 thiết bị tường lửa cứng dùng để:

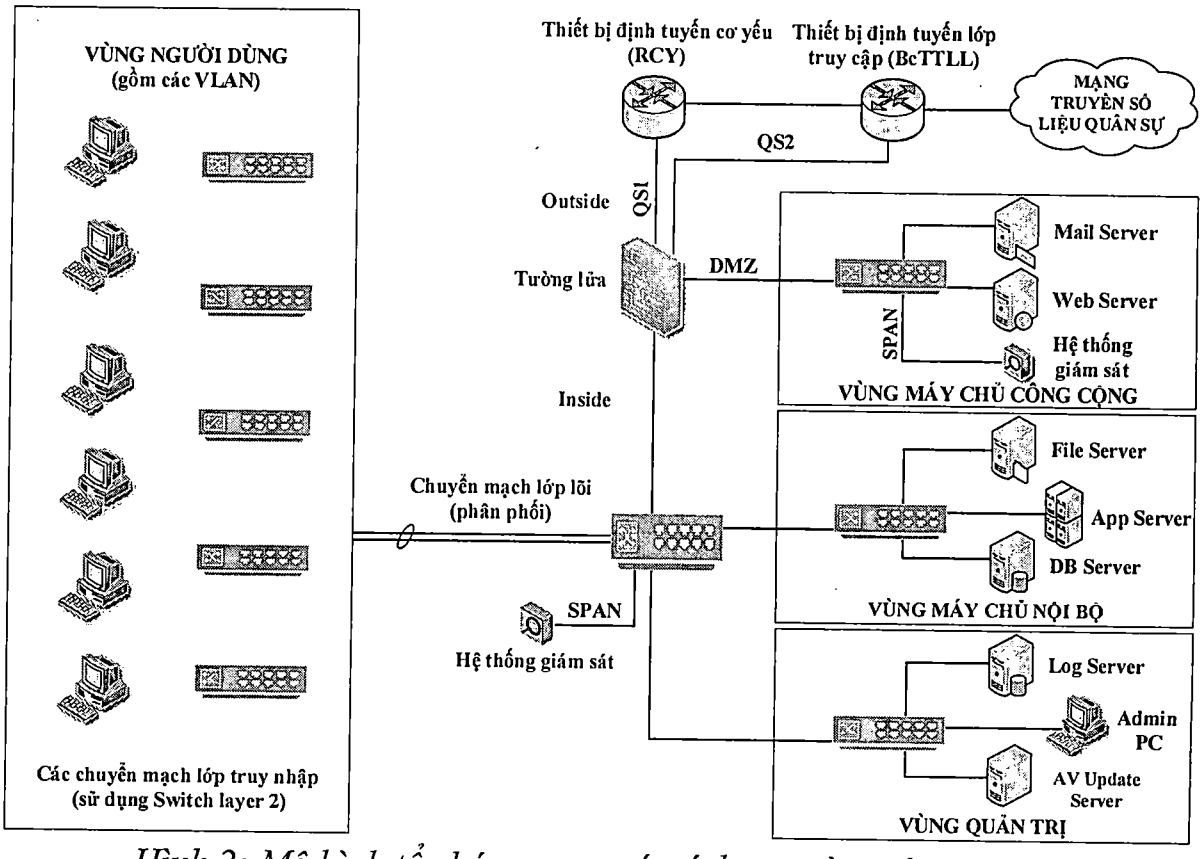
- Bảo vệ vùng máy chủ công cộng (DMZ) cho phép truy cập vào từ mạng máy tính quân sự (Web, Mail);

- Bảo vệ bên trong mạng (Inside) gồm:

+ Vùng người dùng: Thiết lập chính sách bảo vệ người dùng trong mạng nội bộ khi truy cập mạng máy tính quân sự; ghi nhật ký truy cập mạng (log) gửi về máy chủ Log Server trong vùng quản trị;

+ Vùng máy chủ nội bộ: Đảm bảo chỉ người dùng được phép mới có khả năng truy cập vùng máy chủ nội bộ (giới hạn theo IP, Port); ghi lại mọi truy cập (log) gửi về máy chủ Log trong vùng quản trị;

+ Vùng quản trị: Có chức năng không cho phép người dùng từ mạng nội bộ truy cập vùng quản trị. Vùng quản trị tổ chức máy chủ Log, máy chủ cập nhật mẫu mã độc (AV update server) và máy tính quản trị.



Hình 2: Mô hình tổ chức mạng máy tính an toàn mức nâng cao

b) Triển khai thiết bị phát hiện xâm nhập mức mạng (Network Instrution Detection System-NIDS)

Triển khai NIDS (có thể sử dụng phần mềm nguồn mở Snort) trong các vùng máy chủ truy cập mạng máy tính quân sự, vùng máy chủ nội bộ và vùng quản trị để kịp thời phát hiện các hoạt động dò quét, trinh sát mạng trên các cổng thiết bị tường lửa đang mở. Các NIDS được gán vào cổng giám sát (SPAN) của thiết bị chuyển mạch.

c) Triển khai máy chủ cập nhật phòng chống virus (AV update server)

Máy chủ cập nhật phòng chống virus được triển khai tại vùng quản trị để cập nhật cơ sở dữ liệu mới từ Hệ thống máy chủ phòng chống mã độc dành riêng cho máy tính quân sự (đặt tại các đơn vị thuộc Bộ Tư lệnh 86) và phân phối cho các máy trạm trong mạng nội bộ. Máy chủ cập nhật phòng chống virus có thể quản lý, thống kê tình trạng lây nhiễm mã độc trong mạng, ra lệnh, lập lịch quét mã độc từ xa đối với các máy tính trong mạng.

d) Máy tính quản trị (Admin PC)

Trên máy tính quản trị cài đặt các công cụ phục vụ công tác quản trị, như: phần mềm SSH client, telnet, các phần mềm quét cổng (như công cụ NMAP), công cụ dò quét điểm yếu bảo mật. Máy tính quản trị phải được triển khai các giải pháp bảo đảm an toàn như với máy chủ, máy trạm ở trên.

đ) Triển khai máy chủ log (Log server)

Triển khai máy chủ log trong vùng quản trị để thu thập log từ tất cả các nguồn có trong mạng máy tính, như: Các thiết bị mạng router, switch, firewall, server và các nguồn log khác qua giao thức syslog. Máy chủ log phục vụ công tác quản trị, điều tra xác định nguồn gốc gây mất an toàn thông tin.

e) Triển khai các hệ thống giám sát an toàn thông tin, an ninh mạng

- Hệ thống giám sát an toàn thông tin, an ninh mạng: FMS/FMC, giám sát Log...;

- Hệ thống giám sát hạ tầng: Có thể sử dụng PRTG, Cacti, Zabbix...;

- Hệ thống phát hiện, ngăn chặn xâm nhập IDS/IPS (có thể sử dụng Snort, Suricata...).

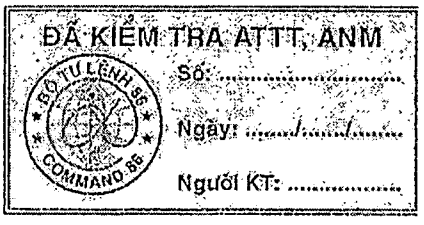
Hai mô hình tổ chức mạng máy tính an toàn trên sử dụng trong mạng máy tính quân sự. Đối với mạng máy tính kết nối Internet được áp dụng tương tự, không sử dụng RCY (thiết bị định tuyến cơ yếu).

Phụ lục II

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

(Kèm theo Quy định số 5067 /QyĐ-PKKQ ngày 28 tháng 12 năm 2021 của Tư lệnh PK-KQ)

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;
- Chất liệu giấy vỡ;
- Định dạng chữ UTM Helve;

Cỡ chữ viết: Chữ "ĐÃ KIỂM TRA ATTT, ANM" cỡ 7.5 pt; chữ "Số, Ngày, Người KT" cỡ 6 pt; chữ "BỘ TƯ LỆNH 86, COMMAND 86" cỡ 4.5 pt.

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

- Tem hình tròn, đường kính 12 mm;
- Chất liệu giấy vỡ;
- Định dạng chữ UTM Helve;
- Cỡ chữ viết: Chữ "Đã KT ATTT, ANM" cỡ 4pt; chữ "BỘ TƯ LỆNH 86" cỡ 4 pt;
- "....." ghi số tem;
- "..../...../....." ghi ngày, tháng, năm kiểm tra.

Phụ lục III
QUY TRÌNH ĐIỀU PHỐI VÀ ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN, AN NINH MẠNG TẠI QUÂN CHỦNG PK-KQ

(Kèm theo Quy định số 5067/QyĐ-PKKQ ngày 28 tháng 12 năm 2021 của Tư lệnh PK-KQ)

I. LƯU ĐỒ QUY TRÌNH

LỰC LƯỢNG	QUY TRÌNH	GHI CHÚ
- Đơn vị, cá nhân vận hành HTTT; - Trực ban ứng cứu sự cố tại các cơ quan, đơn vị (nếu có).	Bắt đầu Phát hiện, tiếp nhận thông tin sự cố	Nguồn thông tin sự cố: - Các hệ thống giám sát phát hiện; - Đơn vị, cá nhân vận hành HTTT cung cấp; - Nguồn tin xã hội.
- Trực ban ứng cứu sự cố tại các cơ quan, đơn vị; - Đơn vị, cá nhân vận hành HTTT; - Lực lượng kỹ thuật tại chỗ.	Đánh giá, phân loại sơ bộ Không ứng cứu được Ứng cứu được Triển khai ứng cứu sơ bộ Kiểm tra, đánh giá kết quả Đạt kết quả Chưa đạt kết quả	- Các lực lượng cùng phối hợp để đánh giá, phân loại sơ bộ sự cố, nếu nhận thấy vượt quá khả năng thì phải báo cáo ngay cho Trực chỉ huy, xin ý kiến chỉ đạo, báo cáo cơ quan nghiệp vụ cấp trên (qua Trực ban ứng cứu sự cố); - Trường hợp ứng cứu được thì tổ chức ứng cứu theo các kế hoạch, phương án đã xây dựng; - Sau khi ứng cứu xong sự cố phải đánh giá kết quả, nếu kết quả đạt (HTTT trở lại hoạt động bình thường) thì tiến hành đăng ký, bàn giao theo quy định; nếu kết quả chưa đạt phải báo cáo Trực chỉ huy, triệu tập Tổ ứng cứu của cơ quan, đơn vị và các thành phần khác có liên quan.
- Tổ ứng cứu sự cố của cơ quan, đơn vị; - Đơn vị, cá nhân vận hành HTTT; - Lực lượng kỹ thuật tại chỗ; - Đơn vị cung cấp dịch vụ Internet (đối với các HTTT trên mạng Internet).	Báo cáo trực chỉ huy Đánh giá, phân loại lại sự cố Không ứng cứu được Ứng cứu được Tiếp tục ứng cứu Kiểm tra, đánh giá lại kết quả Không đạt kết quả	- Tổ ứng cứu sự cố của cơ quan, đơn vị phối hợp với các lực lượng liên quan đánh giá, phân loại lại sự cố, nếu nhận thấy vượt quá khả năng thì phải báo cáo Trực chỉ huy, xin ý kiến chỉ đạo, báo cáo cơ quan nghiệp vụ cấp trên (qua Trực ban ứng cứu sự cố); - Trường hợp ứng cứu được thì tổ chức ứng cứu theo các kế hoạch, phương án đã xây dựng; - Sau khi ứng cứu xong sự cố phải đánh giá kết quả, nếu kết quả đạt (HTTT trở lại hoạt động bình thường) thì tiến hành đăng ký, bàn giao theo quy định; nếu kết quả chưa đạt phải báo cáo Trực chỉ huy, báo cáo cơ quan nghiệp vụ cấp trên (qua Trực ban ứng cứu sự cố).
- Tổ ứng cứu sự cố của cơ quan, đơn vị; - Đơn vị, cá nhân vận hành HTTT; - Đơn vị cung cấp dịch vụ Internet (đối với các HTTT trên mạng Internet); - Lực lượng ứng cứu sự cố của cấp trên; - Các chuyên gia (nếu có) theo chỉ định của cơ quan nghiệp vụ cấp trên.	Đạt kết quả - Báo cáo trực chỉ huy; - Báo cáo cơ quan nghiệp vụ cấp trên. - Chấp hành sự điều phối của cơ quan nghiệp vụ cấp trên; - Phối hợp, theo dõi; - Tiếp nhận kết quả.	- Cơ quan nghiệp vụ cấp trên điều phối hoạt động ứng cứu sự cố, hỗ trợ giải pháp, lực lượng, phương tiện để ứng cứu sự cố; - Tổ ứng cứu sự cố của cơ quan, đơn vị chấp hành sự điều phối và phối hợp, theo dõi, tiếp nhận kết quả ứng cứu sự cố.
- Đơn vị, cá nhân vận hành HTTT; - Tổ ứng cứu sự cố của cơ quan, đơn vị (nếu tham gia ứng cứu).	Đăng ký, bàn giao kết quả Tổng hợp, báo cáo, thông báo Kết thúc	Tổ ứng cứu sự cố của cơ quan, đơn vị đăng ký, bàn giao kết quả ứng cứu sự cố cho đơn vị, cá nhân vận hành HTTT; tổng hợp, báo cáo, thông báo theo quy định.

II. MÔ TẢ QUY TRÌNH

1. Thông báo, tiếp nhận, xử lý thông tin về sự cố

a) Cơ quan, đơn vị không có Tổ ứng cứu sự cố hoặc Tổ ứng cứu sự cố không tự khắc phục được khi gặp sự cố an toàn thông tin, an ninh mạng thì phải thông báo ngay cho Tổ ứng cứu sự cố Quân chủng (qua Trực ban Công nghệ thông tin Quân chủng) để được điều phối và ứng cứu sự cố;

b) Trong trường hợp Tổ ứng cứu sự cố Quân chủng không tự khắc phục được hoặc khi phát hiện sự cố có khả năng xảy ra trên diện rộng, lan nhanh, gây tổn thất lớn đến thông tin, hệ thống thông tin, Tổ ứng cứu sự cố Quân chủng phải có trách nhiệm thông báo ngay, chậm nhất là 06 giờ cho Bộ Tư lệnh 86 (qua Trực ban Ứng cứu sự cố BTL 86). Nội dung thông báo gồm:

- Thông tin mô tả sự cố;

- Thông tin về hệ thống;

- Dấu hiệu sự cố ban đầu, tình trạng hiện tại;

- Các lực lượng, biện pháp đã và đang triển khai khắc phục;

- Một số nhận định ban đầu;

- Kiến nghị và đề xuất.

c) Việc thông báo các nội dung về sự cố an toàn thông tin, an ninh mạng được thực hiện bằng một hoặc nhiều hình thức như: Công văn, thư điện tử, điện thoại, fax, nhắn tin đa phương tiện hoặc hệ thống kỹ thuật truyền thông nhưng phải đảm bảo tuân thủ các quy định của pháp luật khi trao đổi thông tin;

d) Ngay khi tiếp nhận thông tin về sự cố, Tổ ứng cứu sự cố kịp thời thực hiện các hoạt động sau:

- Xử lý thông tin sự cố và phản hồi ngay, chậm nhất là 06 giờ cho cơ quan, đơn vị gửi thông báo để xác nhận về việc đã nhận được thông báo sự cố;

- Xử lý sự cố trong khả năng và trách nhiệm của mình, báo cáo kết quả xử lý sự cố cho cơ quan chức năng cấp trên theo quy định.

2. Tổ chức ứng cứu sự cố

a) Tổ ứng cứu sự cố Quân chủng có trách nhiệm tiếp nhận, tổ chức điều phối ứng cứu sự cố theo quy định;

b) Các cơ quan, đơn vị gặp sự cố phải thực hiện ứng cứu sự cố theo đúng quy trình, phối hợp chặt chẽ với Tổ ứng cứu sự cố Quân chủng và các cơ quan có liên quan trong quá trình thực hiện ứng cứu sự cố.

3. Nội dung ứng cứu sự cố

a) Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng;

b) Xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu

tác động, thiệt hại đến hệ thống thông tin;

c) Gỡ bỏ mã độc, phần mềm độc hại, khôi phục dữ liệu, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin;

d) Kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố.

4. Đánh giá, bàn giao kết quả ứng cứu sự cố

a) Công tác ứng cứu sự cố kết thúc khi sự cố được khắc phục và hệ thống hoạt động trở lại bình thường;

b) Sau khi khắc phục sự cố, các thành phần tham gia ứng cứu rà soát, xác định nguyên nhân gây ra sự cố; tổ chức kiểm tra lại, bảo đảm hệ thống hoạt động bình thường trước khi bàn giao toàn bộ hệ thống cho cơ quan, đơn vị chủ quản.

5. Kết thúc điều phối, ứng cứu sự cố

Khi kết thúc hoạt động điều phối, ứng cứu sự cố, các thành phần tham gia ứng cứu sự cố tiến hành các hoạt động:

a) Bàn giao đầy đủ cơ sở vật chất, thông tin, dữ liệu (nếu có) cho cơ quan chủ quản và yêu cầu thay đổi tài khoản, mật khẩu truy cập thiết bị, hệ thống;

b) Tổng hợp kết quả thực hiện hoạt động ứng cứu sự cố. Các thông tin, tài liệu liên quan (nếu có) trong quá trình điều phối, ứng cứu sự cố được bảo quản theo đúng quy định của pháp luật;

c) Tổ chức rút kinh nghiệm triển khai hoạt động điều phối, ứng cứu khắc phục sự cố;

d) Báo cáo kết quả thực hiện, kiến nghị (nếu có) với Tổ ứng cứu sự cố cấp trên.

III. MỘT SỐ SỰ CỐ AN TOÀN THÔNG TIN, AN NINH MẠNG PHỔ BIẾN

1. Một số loại sự cố an toàn thông tin, an ninh mạng

- Sự cố do bị tấn công mạng;

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting;

- Sự cố do lỗi của người quản trị, vận hành hệ thống;

- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn....

2. Các tình huống cụ thể của mỗi loại sự cố

a) Tình huống sự cố do bị tấn công mạng

- Tấn công từ chối dịch vụ;

- Tấn công giả mạo;

- Tấn công sử dụng mã độc;

- Tấn công truy cập trái phép, chiếm quyền điều khiển;

- Tấn công thay đổi giao diện;

- Tấn công mã hóa phần mềm, dữ liệu, thiết bị;

- Tấn công phá hoại thông tin, dữ liệu, phần mềm;

- Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

- Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

- Các hình thức tấn công mạng khác.

b) Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:

- Sự cố nguồn điện;

- Sự cố đường truyền kết nối mạng TSLqs hoặc Internet;

- Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

- Sự cố liên quan đến quá tải hệ thống;

- Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:

- Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;

- Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;

- Lỗi liên quan đến chính sách an toàn thông tin;

- Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;

- Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

d) Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn…

Phụ lục IV

MẪU HỒ SƠ XIN CẤP PHÉP

(Kèm theo Quy định số 5067/QyĐ-PKKQ ngày 28 tháng 12 năm 2021 của Tư lệnh PK-KQ)

Mẫu số 01. Đơn xin cấp phép sử dụng dịch vụ Internet trong Quân đội

QC PHÒNG KHÔNG - KHÔNG QUÂN **SƯ ĐOÀN 361 (1)**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:...(2)/....(3)	*Hà Nội(4), ngày..... tháng.... năm 20....*

ĐƠN

Xin cấp phép sử dụng dịch vụ Internet trong Quân đội

Kính gửi: Tư lệnh Quân chủng Phòng không - Không quân

Căn cứ Quy chế quản lý, cung cấp, sử dụng dịch vụ Internet trong Quân đội nhân dân Việt Nam ban hành kèm theo Thông tư số 110/2014/TT-BQP ngày 22 tháng 8 năm 2014 của Bộ trưởng Bộ Quốc phòng;

Căn cứ....(5),

(1) đề nghị Tư lệnh Quân chủng cấp phép sử dụng dịch vụ Internet trong Quân đội như sau:

Phần 1. Thông tin chung

Tên cơ quan đơn vị sử dụng dịch vụ Internet.

Phần 2. Lý do xin cấp phép

Trình bày tóm tắt lý do xin cấp phép sử dụng dịch vụ Internet.

Phần 3. Nội dung xin cấp phép sử dụng dịch vụ Internet

1. Địa điểm sử dụng: .....
2. Số lượng máy tính kết nối Internet:.....
3. Hình thức kết nối: (ADSL, FTTH...).....
4. Doanh nghiệp cung cấp dịch vụ Internet:.....

Phần 4. Cam kết

(1) xin chịu hoàn toàn trách nhiệm về tính chính xác của nội dung trong đơn đề nghị cấp phép sử dụng dịch vụ Internet trong Quân đội./.

Nơi nhận: - Như trên; - Lưu: VT, ...(7);	**SƯ ĐOÀN TRƯỞNG** (6) (Chữ ký, dấu) **Đại tá Nguyễn Văn A**

Ghi chú:

(1) Tên cơ quan, đơn vị đề nghị (trực thuộc Bộ Tư lệnh).

(2) Số văn bản của đơn đề nghị.

(3) Chữ viết tắt tên cơ quan đơn vị đề nghị.

(4) Địa danh, tên tỉnh thành phố trực thuộc trung ương.

(5) Các quy định của cơ quan, đơn vị về khai thác, sử dụng Internet (nếu có).

(6) Chức vụ người ký.

(7) Chữ viết tắt tên đơn vị soạn thảo, tên người soạn thảo, số lượng bản phát hành.

Mẫu số 02. Bản cam kết sử dụng dịch vụ Internet trong Quân đội

SƯ ĐOÀN 361 (1) **PHÒNG THAM MƯU** (2)	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

Hà Nội(3), ngày..... tháng ... năm 20...

BẢN CAM KẾT
Sử dụng dịch vụ Internet trong Quân đội

Phòng Tham mưu (2)/(1) xin cam kết:

1. Tổ chức sử dụng Internet cho cơ quan, đơn vị theo đúng những nội dung trong đơn xin cấp phép sử dụng dịch vụ Internet trong Quân đội số.... ngày....tháng....năm.... của (4).

2. Thực hiện nghiêm quy định của pháp luật về lĩnh vực Internet; Quy chế quản lý, cung cấp và sử dụng dịch vụ Internet trong Quân đội nhân dân Việt Nam ban hành kèm theo Thông tư số 110/2014/TT-BQP ngày 22 tháng 8 năm 2014 của Bộ trưởng Bộ Quốc phòng; các quy định của Tư lệnh Quân chủng về quản lý, khai thác, sử dụng dịch vụ Internet và quản lý, sử dụng các trang bị công nghệ thông tin trong Quân chủng Phòng không - Không quân.

3. Nếu vi phạm xin chịu hoàn toàn trách nhiệm theo quy định của pháp luật và Bộ Quốc phòng./.

XÁC NHẬN CỦA THỦ TRƯỞNG SƯ ĐOÀN (6) (Ký tên, đóng dấu)	**THAM MƯU TRƯỞNG** (5) (Ký, ghi rõ họ tên) **Đại tá Nguyễn Văn A**

Ghi chú:
(1) Tên cơ quan, đơn vị đề nghị.
(2) Cơ quan, đơn vị sử dụng dịch vụ Internet.
(3) Tên tỉnh, thành phố trực thuộc trung ương.
(4) Theo thông tin trong Đơn xin cấp phép sử dụng dịch vụ Internet.
(5) Chức vụ thủ trưởng cơ quan, đơn vị sử dụng Internet.
(6) Thủ trưởng cơ quan, đơn vị đề nghị.