

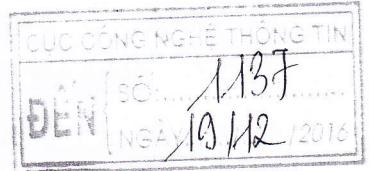
Số: 202 /2016/TT-BQP

Hà Nội, ngày 12 tháng 12 năm 2016

LUU HÀNH NỘI BỘ

THÔNG TƯ

Quy định về bảo đảm an toàn thông tin
trong Quân đội nhân dân Việt Nam



Căn cứ Luật công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật viễn thông ngày 23 tháng 11 năm 2009;

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 Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

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 101/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về phòng chống sử dụng mạng để khủng bố;

Căn cứ 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;

Căn cứ Nghị định số 35/2013/NĐ-CP ngày 22 tháng 4 năm 2013 của Chính phủ về quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Quốc phòng;

Theo đề nghị của Tổng Tham mưu trưởng Quân đội nhân dân Việt Nam;

Bộ trưởng Bộ Quốc phòng ban hành Thông tư quy định về bảo đảm an toàn thông tin trong Quân đội nhân dân Việt Nam.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định về công tác bảo đảm an toàn thông tin, quyền hạn, trách nhiệm của các cơ quan, đơn vị, cá nhân trong việc bảo đảm an toàn thông tin trong Quân đội nhân dân Việt Nam.

Điều 2. Đối tượng áp dụng

Thông tư này áp dụng đối với các cơ quan, đơn vị, cá nhân tham gia thiết kế, xây dựng, quản lý, mua sắm, vận hành, khai thác, sử dụng và bảo đảm kỹ thuật hệ thống thông tin trong Quân đội nhân dân Việt Nam.

Điều 3. Giải thích từ ngữ

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

1. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay 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.
2. *Máy tính Internet* là máy tính của cơ quan, đơn vị trang bị cho người dùng sử dụng để kết nối và truy nhập vào mạng Internet.
3. *Mạng Internet sử dụng trong Quân đội* là mạng máy tính trong các cơ quan, đơn vị trong Quân đội nhân dân Việt Nam được kết nối với mạng Internet và các ứng dụng, dịch vụ của cơ quan, đơn vị trên mạng Internet.
4. *Máy tính quân sự* là máy tính của cơ quan, đơn vị trong Quân đội nhân dân Việt Nam trang bị cho người dùng quản lý và sử dụng nhằm phục vụ cho các hoạt động nghiệp vụ của cơ quan, đơn vị và không kết nối mạng Internet.
5. *Mạng máy tính quân sự* là mạng máy tính được thiết kế dành riêng để phục vụ quản lý, chỉ huy, điều hành và điều khiển vũ khí, trang bị kỹ thuật trong Quân đội nhân dân Việt Nam; không kết nối mạng Internet và các mạng kinh doanh khác. Mạng máy tính quân sự bao gồm mạng máy tính quân sự của các cơ quan, đơn vị; mạng máy tính điện rộng trong Bộ Quốc phòng; mạng truyền số liệu quân sự và tài nguyên trên mạng máy tính.
6. *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.
7. *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.
8. *Rủi ro an toàn thông tin* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin.
9. *Sự cố an toàn thông tin* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.
10. *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.
11. *Vật mang tin điện tử* là các phương tiện vật chất có khả năng lưu trữ, trao đổi 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, điện thoại di động.
12. *Bản ghi nhật ký (logfile)* là tập tin chứa các thông tin về lịch sử hoạt động của phần cứng, phần mềm.
13. *Mật khẩu phức tạp* là mật khẩu có ít nhất 8 ký 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 trên bàn phím máy tính.

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

15. *Thiết bị di động thông minh* là thiết bị số có thể cầm tay, có hệ điều hành, khả năng xử lý, kết nối mạng và có màn hình hiển thị như máy tính bảng, điện thoại di động thông minh.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

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. Việc bảo đảm an toàn thông tin 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 hệ thống thông tin.

2. Hoạt động bảo đảm an toàn 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.

3. Các cơ quan, đơn vị có trách nhiệm xây dựng các quy chế bảo đảm an toàn thông tin và phối hợp với cơ quan chức năng công nghệ thông tin để bảo đảm an toàn thông tin cho các hệ thống thông tin của cơ quan, đơn vị.

4. Thông tin thuộc danh mục bí mật nhà nước, bí mật quân sự phải được bảo vệ theo các quy định của pháp luật về bảo vệ bí mật của Nhà nước, bí mật quân sự và các quy định trong Thông tư này.

Điều 5. Phân loại và tiêu chí xác định cấp độ an toàn thông tin

1. Phân loại thông tin và hệ thống thông tin được thực hiện theo quy định tại Điều 6 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 (sau đây viết gọn là Nghị định số 85/2016/NĐ-CP).

2. Tiêu chí xác định cấp độ 1, 2, 3, 4 và 5 về an toàn thông tin được thực hiện theo quy định tại Điều 7, 8, 9, 10 và Điều 11 Nghị định số 85/2016/NĐ-CP.

3. Hồ sơ đề xuất cấp độ an toàn thông tin được thực hiện theo quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP.

Điều 6. Thẩm quyền, trình tự, thủ tục xác định cấp độ

1. Đối với hệ thống thông tin được đề xuất cấp độ 1 hoặc cấp độ 2

a) Đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ;

b) Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định hồ sơ và trình Thủ trưởng chủ quản hệ thống thông tin phê duyệt.

2. Đối với hệ thống thông tin được đề xuất cấp độ 3 hoặc cấp độ 4

a) Chủ quản hệ thống thông tin lập hồ sơ đề xuất cấp độ;

b) Cục Công nghệ thông tin thẩm định hồ sơ đề xuất cấp độ 3;

c) Bộ Tổng Tham mưu chủ trì, phối hợp với cơ quan chức năng của Bộ Thông tin và Truyền thông, các bộ, ngành liên quan thẩm định hồ sơ đề xuất cấp độ 4 (nếu cần thiết);

d) Bộ Tổng Tham mưu phê duyệt hồ sơ đề xuất cấp độ.

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

a) Chủ quản hệ thống thông tin lập hồ sơ đề xuất cấp độ;

b) Bộ Tổng Tham mưu chủ trì, phối hợp với cơ quan chức năng của Bộ Thông tin và Truyền thông, các bộ, ngành liên quan thẩm định hồ sơ đề xuất cấp độ; trình Thủ trưởng Bộ Quốc phòng phê duyệt phương án bảo đảm an toàn thông tin;

c) Bộ Quốc phòng trình Thủ tướng Chính phủ phê duyệt hồ sơ đề xuất cấp độ thuộc danh mục hệ thống thông tin quan trọng quốc gia.

Điều 7. 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 vào sử dụng. Sử dụng máy tính Internet, trang bị công nghệ thông tin của cá nhân hoặc thiết bị di động thông minh để tạo lập, xử lý và lưu trữ các tài liệu điện tử quân sự có nội dung chưa được phép phổ biến.

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

3. Sử dụng vật mang tin điện tử để trao đổi thông tin, dữ liệu giữa máy tính quân sự và máy tính Internet; sử dụng thiết bị lưu trữ của cá nhân để lưu trữ, trao đổi thông tin, dữ liệu, tài liệu điện tử quân sự.

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

5. Kết nối, truy nhập vào mạng máy tính quân sự bằng giải pháp kết nối không dây không có giải pháp bảo mật cơ yếu.

6. Kết nối mạng máy tính quân sự với mạng Internet dưới mọi hình thức.

7. Xâm phạm an toàn thông tin của cơ quan, đơn vị và cá nhân khác.

8. Sử dụng mạng xã hội thực hiện bình luận, đăng tải hoặc phát tán dưới mọi hình thức các thông tin trái quan điểm, đường lối của Đảng; thông tin liên quan đến bí mật Nhà nước, Quân đội và 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; tạo lập hoặc tham gia các diễn đàn, nhóm liên quan đến tội phạm, các tổ chức phản động, chống đối chính trị và các vi phạm pháp luật khác.

9. Vi phạm các quy định khác của pháp luật và Quân đội về bảo đảm an toàn thông tin.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN

Mục 1

NHỮNG VẤN ĐỀ CHUNG VỀ BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 8. Phân loại 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 sở hữu thông tin 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. Tài liệu điện tử quân sự thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật và Quân đội về bảo vệ bí mật Nhà nước, bí mật quân sự.
3. Nếu không thể đánh dấu, hoặc xác định độ mật trực tiếp vào tài liệu điện tử quân sự thì phải ghi rõ trên mặt ngoài các thiết bị lưu trữ điện tử.

Điều 9. Quản lý tài liệu điện tử quân sự

1. Tài liệu điện tử quân sự phải được quản lý chặt chẽ theo quy định của Bộ Quốc phòng; tài liệu điện tử quân sự có độ mật phải được quản lý theo các quy định về bảo vệ bí mật quân sự và chỉ được tạo lập, xử lý, lưu trữ trên máy tính quân sự.
2. Việc tạo lập, lưu trữ, chuyển nhận tài liệu điện tử quân sự có độ mật trên mạng máy tính phải có giải pháp bảo mật cơ yếu tương ứng. 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.
3. Người dùng có trách nhiệm xác định mức độ mật của tài liệu điện tử quân sự khi soạn thảo, gửi, nhận và lưu trữ để lựa chọn phương thức bảo vệ phù hợp.
4. Các tài liệu điện tử quân sự có độ mật khi xóa phải sử dụng giải pháp xóa dữ liệu an toàn.
5. Các tài liệu điện tử quân sự có độ Tối mật, Tuyệt mật sau khi đã in đủ số lượng phải thực hiện xóa dữ liệu an toàn, bảo đảm không còn tồn tại ở bất kỳ định dạng nào khác trong máy tính và thiết bị lưu trữ không có giải pháp bảo mật cơ yếu.
6. Các dữ liệu điện tử của cá nhân, dữ liệu điện tử thu thập từ mạng Internet phải được kiểm tra an toàn thông tin trước khi đưa vào lưu trữ trong mạng máy tính quân sự.

Điều 10. Quản lý vật mang tin điện tử

1. Vật mang tin điện tử sử dụng cho lưu trữ, trao đổi tài liệu điện tử quân sự phải có giải pháp bảo đảm an toàn thông tin do cơ quan quản lý công nghệ thông tin hoặc cơ quan cơ yếu cấp phát. Người sử dụng vật mang tin điện tử có trách nhiệm bảo vệ tránh làm mất, lộ lọt thông tin.

2. Vật mang tin điện tử khi không còn nhu cầu sử dụng phải xóa dữ liệu an toàn và trao trả lại cho cơ quan quản lý, khi thanh xử lý phải phá hủy vật lý.

3. Việc sử dụng các thiết bị ghi âm, ghi hình trong hội nghị, buổi làm việc phải được sự đồng ý của lãnh đạo, chỉ huy cơ quan, đơn vị chủ trì tổ chức. Thông tin trên các thiết bị ghi âm, ghi hình phải được quản lý theo quy định tại Điều 9 của Thông tư này.

Điều 11. Mật mã cơ yếu và mật mã dân sự

1. Thông tin mật phải được bảo vệ, xác thực bằng kỹ thuật mật mã cơ yếu.

2. Mạng máy tính quân sự phải được bảo mật đường truyền bằng thiết bị bảo mật cơ yếu.

3. Việc sử dụng giải pháp bảo mật, xác thực thông tin sử dụng kỹ thuật mật mã dân sự trong các cơ quan, đơn vị chỉ được thực hiện khi chưa triển khai xong giải pháp mật mã cơ yếu.

Điều 12. Quản lý bản ghi nhật ký

1. Các cơ quan, đơn vị phải thực hiện việc thiết lập và lưu trữ các bản ghi nhật ký trên các hệ thống thông tin ít nhất 03 (ba) tháng nhằm bảo đảm các sự kiện xảy ra trên hệ thống được ghi nhận và lưu giữ. Các cơ quan, đơn vị duy trì hệ thống thông tin có trách nhiệm cung cấp toàn bộ bản ghi nhật ký cho cơ quan chức năng để giám sát, bảo vệ, cảnh báo.

2. Các bản ghi nhật ký phải được bảo vệ an toàn nhằm phục vụ công tác thanh tra, kiểm tra đánh giá an toàn thông tin.

3. Các sự kiện tối thiểu phải có trong bản ghi nhật ký hệ thống thông tin 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.

4. Thường xuyên duy trì việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro an toàn thông tin, mức độ nghiêm trọng các rủi ro an toàn thông tin đó để có biện pháp xử lý kịp thời.

Điều 13. Bảo đảm an toàn vật lý và môi trường

1. Các khu vực 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 đầu nối, thiết bị nguồn điện và dự phòng điện khẩn cấp;

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

2. Các phương pháp bảo đảm an toàn vật lý và môi trường:

a) Ban hành nội quy, hướng dẫn làm việc và sử dụng các biện pháp bảo đảm an ninh 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 kiểm tra đường truyền, các điểm truy nhập mạng để tránh bị xâm nhập, phá hoại trái phép.

Điều 14. Quản lý, khai thác, sử dụng và bảo dưỡng, sửa chữa trang bị công nghệ thông tin

1. Các nội dung bảo đảm an toàn thông tin phải được thực hiện trong các hoạt động quản lý, khai thác, sử dụng, bảo dưỡng, sửa chữa trang bị công nghệ thông tin.
2. Kiểm tra, đánh giá an toàn thông tin bao gồm hoạt động kiểm tra, đánh giá việc chấp hành các quy định, hướng dẫn về quản lý, khai thác, sử dụng và bảo dưỡng, sửa chữa trang bị công nghệ thông tin tại các cơ quan, đơn vị.
3. Triển khai đầy đủ các giải pháp bảo đảm an toàn thông tin theo quy định cho các trang bị công nghệ thông tin sau khi nâng cấp, bảo dưỡng, sửa chữa.

**Mục 2
BẢO ĐẢM AN TOÀN MÁY TÍNH**

Điều 15. Bảo đảm an toàn phần cứng

1. Thiết lập các giải pháp xác thực và điều khiển truy nhập:
 - a) Triển khai xác thực và điều khiển truy nhập bằng mật khẩu trên máy tính;
 - b) Người dùng phải sử dụng tính năng khóa màn hình, mật khẩu hệ thống của hệ điều hành và tắt máy khi không sử dụng để bảo vệ và chống lại những truy nhập vật lý trái phép khi rời khỏi nơi đặt máy tính;
 - c) Mật khẩu sử dụng phải là mật khẩu phức tạp.
2. Máy tính phải ngắt (vô hiệu hóa) các tính năng dễ gây rủi ro an toàn thông tin như micro, camera, truy nhập mạng không dây (Wifi, Bluetooth, GPS) và các tính năng khác khi không sử dụng.
3. Máy tính quân sự khi chuyển đổi mục đích sử dụng thành máy tính Internet và ngược lại phải do cơ quan chức năng thực hiện, xóa dữ liệu an toàn, kiểm tra an toàn thông tin và có các giải pháp bảo đảm an toàn thông tin theo quy định.
4. Quản lý và giám sát chặt chẽ việc sử dụng các thiết bị ngoại vi của máy tính. Không sử dụng các thiết bị ngoại vi của máy tính dùng chung cho cả mạng máy tính quân sự và mạng Internet sử dụng trong Quân đội để tránh thất thoát thông tin lưu trữ trong các bộ nhớ.

Điều 16. Bảo đảm an toàn phần mềm

1. Máy tính quân sự chỉ được sử dụng các phần mềm do cơ quan chức năng cung cấp. Các phần mềm dùng chung, phần mềm chuyên ngành phải được cơ quan chức năng kiểm tra an toàn thông tin và cấp phép sử dụng.

2. Đơn vị chuyên trách về an toàn thông tin của cơ quan, đơn vị chịu trách nhiệm phân loại, phân quyền cài đặt các phần mềm. Người dùng không được tự ý thay đổi, gỡ bỏ, cài đặt mới các phần mềm trên máy tính khi chưa được sự đồng ý của cơ quan chức năng công nghệ thông tin.

3. Các 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 được gỡ bỏ hoặc vô hiệu hóa để giảm thiểu các nguy cơ gây mất an toàn thông tin.

4. Định kỳ cập nhật phiên bản nâng cấp và bản vá lỗi được cung cấp bởi cơ quan quản lý công nghệ thông tin trong Quân đội.

5. Máy tính khi đưa vào sử dụng phải kích hoạt tính năng tường lửa, cài đặt hệ thống phòng chống phần mềm độc hại, phần mềm mã hoá tập tin, xoá dữ liệu an toàn.

Điều 17. Kiểm soát truy nhập người dùng

1. Đơn vị chuyên trách về công nghệ thông tin có trách nhiệm cấp quyền sử dụng phù hợp với chức trách, nhiệm vụ của người dùng theo nguyên tắc cấp quyền tối thiểu.

2. Cơ quan chức năng 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 các quyền sử dụng của người dùng đối với hệ thống thông tin.

3. Tài khoản quản trị hệ thống thông tin phải do đơn vị chuyên trách về công nghệ thông tin nắm giữ và phải tách biệt với tài khoản truy nhập người dùng.

4. Người dùng phải được cấp tài khoản truy nhập với định danh duy nhất để sử dụng máy tính, ứng dụng, dịch vụ của mạng máy tính. Nếu 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.

5. Người dùng không được sử dụng tài khoản quản trị của hệ thống thông tin (trừ trường hợp được thủ trưởng cơ quan, đơn vị cho phép) hoặc dùng chung tài khoản quản trị với tài khoản truy nhập người dùng.

6. Người dùng có trách nhiệm bảo vệ thông tin của tài khoản được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ trường hợp cần xử lý công việc khẩn cấp của đơn vị hoặc cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu điện tử quân sự do cá nhân quản lý và phải đổi mật khẩu ngay sau khi kết thúc xử lý công việc.

7. Các tài khoản truy nhập của người dùng 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.

8. Các tài liệu hệ thống như bản ghi nhật ký, tệp tin cấu hình của máy tính phải được lưu trữ và có giải pháp bảo đảm an toàn để ngăn chặn việc truy nhập, thay đổi hay xóa trái phép.

Điều 18. Phòng, chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được cài đặt hệ thống phòng, chống phần mềm độc hại do cơ quan chức năng cung cấp. Các 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 offline cho máy tính không kết nối mạng; chế độ tự động quét phần mềm độc hại khi sao chép, mở các tập tin.

2. Người dùng phải có trách nhiệm phát hiện, loại bỏ, phòng, chống phần mềm độc hại, các rủi ro do phần mềm độc hại gây ra; không được 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 lãnh đạo, chỉ huy cơ quan, đơn vị.

3. Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi các tập tin trên các vật mang tin điện tử. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

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

Mục 3 BẢO ĐẢM AN TOÀN MẠNG MÁY TÍNH

Điều 19. Quản lý mạng máy tính

1. Cơ quan, đơn vị khi triển khai xây dựng, quản lý và khai thác mạng máy tính phải chấp hành theo các quy định của Bộ Quốc phòng về xây dựng, quản lý, khai thác, sử dụng hạ tầng công nghệ thông tin trong Quân đội nhân dân Việt Nam.

2. Hệ thống mạng máy tính phải được thiết kế, lắp đặt theo mô hình mạng máy tính an toàn nhằm đáp ứng các yêu cầu về bảo đảm an toàn thông tin, 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 khác;

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; triển khai thiết bị bảo mật đường truyền;

d) Xây dựng phương án dự phòng về kết nối và thiết bị mạng, giải pháp bảo mật cơ yếu 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;

e) Triển khai các trang thiết bị mạng, thiết bị an toàn thông tin 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 và được kiểm tra an toàn thông tin trước khi đưa vào sử dụng;

g) 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 hoặc các hoạt động xâm phạm an toàn thông tin.

3. Các mạng máy tính phải được tổ chức, cấu hình theo mô hình mạng máy tính an toàn mức cơ bản; mạng máy tính tại các sở chỉ huy cấp chiến lược, chiến dịch phải tổ chức, cấu hình theo mô hình mạng máy tính an toàn mức nâng cao theo hướng dẫn tại Phụ lục I, Thông tư này.

4. Máy tính dùng để kết nối mạng phải bảo đảm an toàn theo các quy định tại Mục 2 Chương II của Thông tư này và phải được thiết lập, quản lý kết nối bằng địa chỉ vật lý (MAC), địa chỉ mạng (IP).

Điều 20. Kiểm soát truy nhập mạng

1. Đơn vị chuyên trách về công nghệ thông tin của các cơ quan, đơn vị thực hiện kiểm soát truy cập 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 kênh truyền an toàn, có xác thực tối thiểu 02 (hai) lớp và có giải pháp giám sát an toàn.

3. Các thiết bị chuyển mạch phải có khả năng quản lý cấu hình; tiến hành gắn địa chỉ vật lý 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 vô hiệu hóa.

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

Điều 21. Kiểm soát truy nhập ứng dụng

1. Người dùng được cấp quyền sử dụng mới được phép truy nhập vào các ứng dụng và thông tin liên quan.

2. Khi truy nhập vào hệ điều hành và các ứng dụng phải được kiểm soát theo quy trình bảo đảm an toàn thông tin; 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 vào hệ thống ở quyền quản trị hoặc khi truy nhập vào hệ thống có dữ liệu độ mật ở quyền người dùng.

3. Thiết lập thời gian phiên làm việc của ứng dụng để ứng dụng tự động đóng lại sau một thời gian không hoạt động được quy định trước.

4. Khóa tài khoản truy nhập ứng dụng nếu đăng nhập thất bại liên tiếp 03 (ba) lần, hằng ngày quản trị mạng có trách nhiệm kiểm tra lại bản ghi của các lần đăng nhập thất bại.

Điều 22. Bảo đảm an toàn 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. 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 cần 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, cập nhật bản vá, bản sửa lỗi hệ quản trị cơ sở dữ liệu tối thiểu 6 tháng một lần hoặc ngay khi có khuyến cáo của nhà cung cấp;

d) 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;

e) Có giải pháp ngăn chặn các hình thức tấn công 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 dùng truy nhập vào cơ sở dữ liệu;

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

c) Người dùng phải thay đổi mật khẩu mặc định tại thời điểm đăng nhập đầu tiên; 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.

Điều 23. Bảo đảm an toàn máy chủ

1. Máy chủ phải được cấu hình riêng biệt về mặt lô-gíc hoặc vật lý để phục vụ cho từng ứng dụng tương ứng và đặt tại khu vực được kiểm soát bảo đảm an toàn vật lý và môi trường theo quy định tại Điều 13 của Thông tư này.

2. Bảo vệ máy chủ:

a) Hệ điều hành và các ứng dụng phải được cập nhật thường xuyên và phải bảo đảm cập nhật đúng phiên bản và thực hiện đúng quy trình;

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

c) Người quản trị máy chủ phải xóa tất cả các tài khoản mặc định, tài khoản không sử dụng và không sử dụng các cấu hình mặc định.

3. Phải triển khai các biện pháp kiểm soát truy nhập tới máy chủ ở mức vật lý và lô-gíc chặt chẽ, người quản trị hệ thống phải 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 (sử dụng mật khẩu phức tạp).

4. Tất cả các 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 để bảo đảm an toàn thông tin.

5. Đối với các máy chủ ứng dụng khác nhau như quản lý tên miền, máy chủ web, máy chủ thư điện tử, máy chủ cơ sở dữ liệu phải được cấu hình an toàn tùy theo từng ứng dụng cụ thể.

Điều 24. Bảo đảm an toàn cho tài liệu gửi qua mạng máy tính quân sự

1. Tài liệu điện tử quân sự không mật được phép chuyển, nhận qua mạng máy tính quân sự.

2. Tài liệu điện tử quân sự có độ mật khi chuyển nhận, lưu trữ qua mạng máy tính quân sự phải có các giải pháp bảo mật tương ứng. Chỉ sử dụng giải pháp bảo mật dân sự để xác thực, bảo mật tài liệu điện tử quân sự mật khi chưa triển khai xong giải pháp bảo mật cơ yếu.

3. Việc chuyển nhận tài liệu trên mạng máy tính quân sự chỉ được thực hiện qua hệ thống phần mềm dùng chung do cơ quan quản lý công nghệ thông tin của Bộ Quốc phòng cung cấp.

Điều 25. Ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự

1. Các ứng dụng, dịch vụ chỉ được đưa vào hoạt động trên mạng máy tính quân sự khi được cơ quan chức năng của Bộ Quốc phòng kiểm tra an toàn thông tin và cấp phép sử dụng.

2. Cơ quan, đơn vị chủ quản của các ứng dụng, dịch vụ hoạt động trên mạng máy tính quân sự phải xây dựng quy định về quản lý, vận hành, khai thác và bảo đảm an toàn thông tin; tuân thủ kết nối an toàn và các chính sách an toàn thông tin theo quy định.

3. Cơ quan, đơn vị chủ quản của 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.

4. Các bản cập nhật, nâng cấp của ứng dụng, dịch vụ phải được cơ quan chức năng kiểm tra an toàn thông tin.

Điều 26. Giám sát mạng máy tính và hệ thống thông tin

1. Cơ quan chủ quản hệ thống thông tin và đơn vị chuyên trách về công nghệ thông tin có trách nhiệm triển khai các giải pháp giám sát an toàn thông tin 24/24; phân tích, đánh giá, kịp thời cảnh báo, khắc phục sự cố an toàn thông tin.
2. Cơ quan, đơn vị chủ quản hệ thống thông tin phải cung cấp thông tin giám sát cho cơ quan chuyên trách công nghệ thông tin của Bộ Quốc phòng.

Mục 4

AN TOÀN CHO SỬ DỤNG MẠNG INTERNET TRONG QUÂN ĐỘI

Điều 27. Quản lý, cung cấp và sử dụng mạng Internet trong Quân đội nhân dân Việt Nam

1. Việc quản lý, cung cấp và sử dụng mạng Internet trong Quân đội phải thực hiện theo pháp luật của Nhà nước và quy định của Quân đội.
2. Cơ quan, đơn vị phải kết nối mạng Internet bằng cáp mạng và kiểm soát số lượng các kết nối.
3. Các cơ quan, đơn vị làm kinh tế hoặc do vị trí đóng quân không thể triển khai kết nối mạng Internet bằng dây, cáp thì được xem xét, cấp phép sử dụng mạng không dây và phải đáp ứng các yêu cầu sau:
 - a) Thiết bị phần cứng phải đạt chuẩn 802.11 trở lên;
 - b) Áp dụng mã hóa dữ liệu truyền nhận sử dụng thuật toán mã hóa an toàn;
 - c) 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(một) lần/ 01tháng;
 - d) Triển khai các giải pháp nhằm giám sát, phát hiện và ngăn chặn các truy nhập trái phép;
 - d) Được kiểm tra, đánh giá bảo đảm an toàn thông tin và cấp phép của cơ quan chức năng.
4. Cơ quan, đơn vị khi sử dụng mạng Internet cần triển khai các giải pháp bảo đảm an toàn thông tin.

Điều 28. Bảo đảm cách ly mạng Internet với mạng máy tính quân sự

1. Khi sử dụng mạng Internet cần thiết lập khu vực bố trí máy tính truy nhập Internet chung của cơ quan, đơn vị trong một phòng riêng biệt và có biện pháp giám sát, quản lý.
2. Dây, cáp, thiết bị của mạng máy tính quân sự và mạng Internet sử dụng trong Quân đội cần phải được phân biệt rõ ràng về nhãn mác, màu sắc.
3. Máy tính quân sự không được phép kết nối vào mạng Internet; máy tính Internet không được kết nối vào mạng máy tính quân sự và lưu trữ, truy nhập các tài liệu điện tử quân sự.

4. Máy tính quân sự không được kết nối tới các thiết bị có khả năng kết nối mạng Internet, như: Thiết bị di động, thiết bị giao tiếp qua các cổng kết nối của máy tính.

5. Việc trao đổi thông tin, dữ liệu giữa máy tính quân sự và máy tính Internet được thực hiện thông qua máy tính trung gian đã được đơn vị chuyên trách công nghệ thông tin các cơ quan, đơn vị triển khai giải pháp bảo đảm an toàn thông tin và sử dụng đĩa CD, DVD để sao chép các tập tin.

Điều 29. 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.

5. Đơn vị chuyên trách về 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 30. Quản lý các trang, cổng thông tin điện tử và ứng dụng của Quân đội trên Internet

1. Các trang, cổng thông tin điện tử và ứng dụng của Quân đội trên Internet phải được cơ quan chức năng kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng và phải được cơ quan có thẩm quyền cấp phép; sử dụng hạ tầng mạng và hệ thống máy chủ của Tập đoàn Viễn thông Quân đội.

2. Việc quản lý các trang, cổng thông tin điện tử và ứng dụng của Quân đội trên Internet thực hiện theo các quy định của Bộ Quốc phòng về quản lý, cung cấp và sử dụng dịch vụ Internet trong Quân đội nhân dân Việt Nam và các quy định khác của pháp luật.

3. Các trang, cổng thông tin điện tử và ứng dụng của Quân đội trên mạng Internet phải được tổ chức thành Trung tâm dữ liệu Internet dành riêng cho Bộ Quốc phòng.

4. Trung tâm dữ liệu Internet dành riêng cho Bộ Quốc phòng do Tập đoàn Viễn thông Quân đội triển khai, cung cấp dịch vụ.

5. Các trang, cổng thông tin điện tử và ứng dụng của Quân đội trên mạng Internet phải được quản lý, giám sát, cảnh báo và tổ chức thực hiện triển khai các giải pháp bảo đảm an toàn thông tin và ứng cứu khắc phục sự cố theo chỉ đạo của cơ quan chức năng.

Điều 31. Sử dụng thư điện tử trên mạng Internet

1. Các cơ quan, đơn vị, cá nhân chỉ sử dụng tài khoản thư điện tử trên mạng Internet để trao đổi thông tin không mật và phải sử dụng hệ thống thư điện tử của Bộ Quốc phòng trên mạng Internet do Tập đoàn Viễn thông Quân đội cung cấp.

2. Các cơ quan, đơn vị có nhu cầu sử dụng hệ thống thư điện tử riêng trên mạng Internet phải phối hợp với Tập đoàn Viễn thông Quân đội để phát triển, bảo đảm an toàn thông tin và tích hợp với hệ thống thư điện tử của Bộ Quốc phòng trên mạng Internet.

Điều 32. Sử dụng 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 họ tên, cấp bậc, chức vụ, địa chỉ cơ quan, đơn vị, hình ảnh mặc quân phục.

2. Trường hợp sử dụng các trang mạng xã hội phục vụ hoạt động của cơ quan, đơn vị phải được sự cho phép của cơ quan tuyên huấn, cơ quan bảo vệ an ninh và cơ quan chức năng về công nghệ thông tin.

Mục 5

PHÁT TRIỂN VÀ TRIỂN KHAI CÁC HỆ THỐNG THÔNG TIN

Điều 33. Bảo đảm an toàn 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 của Bộ Quốc phòng, xây dựng các quy chế bảo đảm an toàn cho hệ thống thông tin thuộc phạm vi quản lý.

2. Căn cứ vào độ mật của ứng dụng và dữ liệu cần xử lý để xác định mức độ bảo đảm an toàn thông tin và được đưa vào từ giai đoạn thiết kế ứng dụng.

3. Dữ liệu nhập vào cơ sở dữ liệu, ứng dụng hoặc hệ thống tự động phải được xác nhận để đảm bảo tính đúng đắn, chính xác và nhất quán.

4. Dữ liệu đầu ra từ cơ sở dữ liệu, ứng dụng hay hệ thống tự động phải được xác thực để bảo đảm việc xử lý thông tin được lưu trữ là đúng và phù hợp.

5. Việc kiểm tra xác thực được đưa vào ứng dụng để phát hiện mọi sự thay đổi do lỗi xử lý hoặc do hành động có chủ đích.

6. Các yêu cầu bảo đảm tính xác thực và toàn vẹn của thông tin sẽ được quy định và đưa vào trong ứng dụng.

Điều 34. Bảo đảm an toàn thông tin cho các tập tin hệ thống

1. Trong quá trình phát triển phần mềm, mã nguồn của chương trình và thiết kế liên quan, thông số kỹ thuật, kế hoạch phát triển và 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 các tập tin hệ thống.

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

Điều 35. Bảo đảm an toàn thông tin trong quá trình phát triển và hỗ trợ

1. Quá trình phát triển hoặc nâng cấp phần mềm, phải thực hiện các yêu cầu về bảo đảm an toàn thông tin từ khi lập kế hoạch đến tổ chức thực hiện, triển khai và nghiệm thu.

2. Phải thực hiện kiểm tra tính toàn vẹn cho hệ thống và tất cả phần mềm để đảm bảo phần mềm và việc cập nhật của nó sau này sẽ 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 để sử dụng cho phát triển sản phẩm.

4. Việc phát triển phần mềm ở bên ngoài phải được theo dõi, giám sát chặt chẽ.

Điều 36. Bảo đảm an toàn trong triển khai dự án và mua sắm trang bị công nghệ thông tin

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; dự án công nghệ thông tin phải được cơ quan chức năng thẩm định, đánh giá an toàn thông tin trước khi trình cơ quan có thẩm quyền phê duyệt, triển khai thực hiện.

2. Cơ quan, đơn vị phải tổ chức mua sắm các trang bị công nghệ thông tin tập trung do cơ quan, cán bộ quản lý công nghệ thông tin đảm nhiệm hoặc tham gia và phải đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin do Bộ Quốc phòng quy định.

3. Cơ quan, đơn vị khi mua sắm trang bị có chứa các phần mềm nhúng phải yêu cầu các nhà sản xuất, cung cấp thiết bị xác nhận bảo đảm an toàn thông tin hoặc cung cấp mã nguồn của các phần mềm nhúng.

4. Cơ quan, đơn vị mua sắm 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 chức năng trong thương thảo, đàm phán, nghiệm thu mua sắm trang bị nhằm thẩm định, đánh giá về an toàn thông tin và đáp ứng các yêu cầu về công tác bảo đảm kỹ thuật công nghệ thông tin.

5. Các trang bị công nghệ thông tin và mạng máy tính quân sự phải được cơ quan chức năng kiểm tra và dán tem an toàn thông tin theo mẫu quy định tại Phụ lục II, Thông tư này trước khi đưa vào sử dụng và trong quá trình sử dụng.

Điều 37. Quản lý việc chuyển giao dịch vụ

1. Các nhân viên dân sự nếu được tuyển dụng hoặc thuê vào làm việc trong các dự án phát triển công nghệ thông tin của Quân đội 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 phạt nếu vi phạm và phải đưa nội dung này vào trong các hợp đồng.

2. Các 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 các hệ thống.

3. Các nhân viên dân sự khi tham gia vào các dự án của một số hệ thống công nghệ cao, quan trọng thì cơ quan, đơn vị chủ trì dự án 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 6

ỨNG CỨU SỰ CỐ VÀ XÁC ĐỊNH NGUYÊN NHÂN MẤT AN TOÀN THÔNG TIN

Điều 38. Quản lý hoạt động điều phối và ứng cứu sự cố

1. Khi phát hiện sự cố an toàn thông tin, cơ quan, đơn vị, cá nhân phải thông báo kịp thời đến chủ quản hệ thống thông tin hoặc cơ quan điều phối hoạt động ứng cứu khắc phục sự cố mạng máy tính để có biện pháp khắc phục trong thời gian sớm nhất.

2. Quá trình điều phối theo phân cấp và tổ chức hoạt động ứng cứu khắc phục sự cố phải đúng quy trình, quy định bảo đảm kịp thời, nhanh chóng, chính xác, an toàn và hiệu quả. Chủ quản hệ thống thông tin có trách nhiệm chủ động phối hợp với cơ quan điều phối và đơn vị ứng cứu khắc phục sự cố trong suốt quá trình thực hiện.

3. Việc tổ chức các hoạt động điều phối và ứng cứu sự cố phải tuân theo các quy định của Bộ Quốc phòng và các cơ quan quản lý Nhà nước về điều phối và ứng cứu sự cố.

Điều 39. Thu thập, phân tích bằng chứng, chứng cứ xác định vi phạm về an toàn thông tin

1. Việc thu thập, phân tích, xác định vi phạm về an toàn thông tin phải do cơ quan chức năng thực hiện.

2. Dữ liệu điện tử có thể coi là chứng cứ trong quá trình điều tra xác định vi phạm về an toàn thông tin. Để đảm bảo giá trị chứng cứ, việc thu thập dữ liệu điện tử phải thực hiện đúng trình tự, thủ tục của pháp luật.

3. Các cơ quan, đơn vị, cá nhân có trách nhiệm bảo vệ các chứng cứ và phối hợp, tạo điều kiện cho các cơ quan chức năng trong các hoạt động thu thập, phân tích, xác định chứng cứ.

4. Cơ quan chức năng có quyền niêm phong, tạm giữ phương tiện điện tử liên quan làm chứng cứ số để phục vụ công tác điều tra.

5. Kết quả điều tra vi phạm về an toàn thông tin được sử dụng làm căn cứ xác định trách nhiệm của cơ quan, đơn vị, cá nhân.

6. Trong trường hợp sự cố về an toàn thông tin có liên quan đến vi phạm pháp luật thì cơ quan, đơn vị liên quan phải có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo đúng quy định của pháp luật.

Điều 40. Xác định nguyên nhân mất an toàn thông tin

Đơn vị chuyên trách về an toàn thông tin có nhiệm vụ:

1. Sử dụng các biện pháp công nghệ, kỹ thuật để xác định nguyên nhân mất an toàn thông tin.

2. Cung cấp kết quả xác định nguyên nhân mất an toàn thông tin cho cơ quan chức năng Bộ Quốc phòng khi có yêu cầu.

3. Tiếp nhận các trang thiết bị công nghệ thông tin, viễn thông 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 Bộ Quốc phòng.

Mục 7 KIỂM TRA, ĐÁNH GIÁ VÀ BÁO CÁO AN TOÀN THÔNG TIN

Điều 41. Kiểm tra, đánh giá an toàn thông tin

1. Cơ quan, đơn vị phải thực hiện việc kiểm tra, đánh giá an toàn thông tin để bảo đảm việc thực hiện, tuân thủ đúng các chính sách, hướng dẫn về bảo đảm an toàn thông tin của các cơ quan chức năng.

2. Hàng năm, các cơ quan đơn vị tổ chức các đợt kiểm tra, đánh giá an toàn thông tin, cụ thể như sau:

a) Bộ Quốc phòng tổ chức các đoàn kiểm tra, phúc tra, đánh giá an toàn thông tin 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 định kỳ 06 (sáu) tháng một lần;

c) Kiểm tra, đánh giá về an toàn thông tin không được giao cho bất kỳ cơ quan, tổ chức ngoài Quân đội thực hiện, trừ trường hợp được phép của Thủ trưởng Bộ Quốc phòng.

3. Việc đánh giá an toàn thông tin thông qua dò quét, tấn công thử nghiệm thâm nhập vào hệ thống thông tin phải do cơ quan chức năng thực hiện.

Điều 42. Chế độ báo cáo

1. Định kỳ hàng quý, các cơ quan, đơn vị có trách nhiệm báo cáo kết quả công tác bảo đảm an toàn thông tin về Cục Công nghệ thông tin để tổng hợp, báo cáo Bộ Tổng Tham mưu và Bộ Quốc phòng.

2. Trường hợp xảy ra vụ việc mất an toàn thông tin nghiêm trọng đối với hệ thống thông tin, các cơ quan, đơn vị có trách nhiệm báo cáo ngay về Cục Công nghệ thông tin để tổng hợp, báo cáo Thủ trưởng Bộ Tổng Tham mưu, Thủ trưởng Bộ Quốc phòng.

Chương III TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ

Điều 43. Cục Công nghệ thông tin

1. Là cơ quan chức năng bảo đảm an toàn thông tin trong Quân đội nhân dân Việt Nam, cơ quan thường trực Tổ công tác an toàn, an ninh thông tin Bộ Quốc phòng.

2. Chủ trì, phối hợp nghiên cứu, xây dựng, trình cấp có thẩm quyền hoặc ban hành theo thẩm quyền chiến lược, quy hoạch, kế hoạch, chính sách, các 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 trong Quân đội.

3. Chủ trì, phối hợp với các cơ quan, đơn vị trong và ngoài Quân đội 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, xâm phạm an toàn thông tin.

4. Chủ trì, phối hợp triển khai các giải pháp bảo đảm an toàn thông tin; hướng dẫn mua sắm, cấp phát trang bị công nghệ thông tin an toàn tới cơ quan, đơn vị trong toàn quân.

5. Thực hiện quản lý các hoạt động điều phối và ứng cứu khắc phục sự cố an toàn thông tin mạng máy tính trong Quân đội nhân dân Việt Nam và tham gia bảo vệ hệ thống thông tin quan trọng quốc gia.

6. Chủ trì, phối hợp với các cơ quan, đơn vị thực hiện ngăn chặn xung đột thông tin trên mạng và phòng chống sử dụng mạng để khủng bố theo 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 về phòng chống sử dụng mạng để khủng bố; tổ chức chỉ đạo, hướng dẫn phân loại hệ thống thông tin và xác định cấp độ an toàn hệ thống thông tin.

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

8. Tổ chức đào tạo, huấn luyện, hướng dẫn nghiệp vụ về bảo đảm an toàn thông tin trong Quân đội.

9. Chủ trì, phối hợp nghiên cứu, ứng dụng khoa học công nghệ trong hoạt động bảo đảm an toàn thông tin, tham mưu đề xuất triển khai giải pháp bảo đảm an toàn thông tin sử dụng mật mã dân sự.

10. Là cơ quan đại diện của Bộ Quốc phòng tham gia hợp tác trong và ngoài nước để trao đổi thông tin, phối hợp nghiên cứu khoa học, đào tạo nguồn nhân lực và sản xuất trang bị công nghệ thông tin, điều phối ứng cứu sự cố.

11. Chủ trì theo dõi, thanh tra, kiểm tra, đôn đốc và hướng dẫn các cơ quan, đơn vị thực hiện quy định của Nhà nước và của Quân đội về bảo đảm an toàn thông tin.

12. Căn cứ vào nhiệm vụ, định mức chi, Cục Công nghệ thông tin lập dự toán chi bảo đảm an toàn thông tin, gửi Bộ Tổng Tham mưu để tổng hợp chung vào dự toán ngân sách hằng năm.

Điều 44. Cục Cơ yếu

1. Chủ trì xây dựng và đề xuất ban hành các văn bản quy phạm pháp luật về mật mã cơ yếu trong việc bảo mật, xác thực thông tin nhằm bảo đảm an toàn thông tin.

2. Chủ trì 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.

3. 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 đội.

4. Chủ trì thực hiện quản lý hoạt động nghiên cứu, sản xuất, ứng dụng mật mã nhằm bảo đảm an toàn thông tin trong Quân đội, thực hiện kiểm định, đánh giá và chứng nhận hợp chuẩn, hợp quy các sản phẩm mật mã bảo đảm an toàn thông tin theo quy định của pháp luật về cơ yếu.

5. Chủ trì, phối hợp, hướng dẫn triển khai giải pháp mật mã dân sự trong bảo đảm an toàn thông tin để bảo vệ thông tin mật khi chưa có hoặc chưa triển khai giải pháp bảo mật cơ yếu.

Điều 45. Cục Bảo vệ an ninh Quân đội

1. Chủ trì, phối hợp với Cục Công nghệ thông tin và các cơ quan, đơn vị liên quan trong hoạt động bảo đảm an ninh thông tin.

2. Điều tra các vụ việc vi phạm, phạm tội gây mất an ninh thông tin trong Quân đội.

3. Phối hợp với các cơ quan chức năng trong điều tra, đấu tranh với các hành vi lợi dụng mạng máy tính để xâm phạm an ninh quốc gia, trật tự an toàn xã hội trong lĩnh vực Quân đội quản lý và bảo vệ bí mật Nhà nước.

Điều 46. Cục Tài chính

Căn cứ vào dự toán chi ngân sách của Bộ Tổng Tham mưu, Cục Tài chính tổng hợp chung vào dự toán ngân sách năm, báo cáo Bộ Quốc phòng.

Điều 47. Bình chủng Thông tin liên lạc

1. Triển khai mở rộng mạng truyền số liệu quân sự có giải pháp bảo mật cơ yếu đường truyền trong toàn quân, bảo đảm kết nối thông suốt, liên tục tới cơ quan, đơn vị cấp chiến lược, chiến dịch, chiến thuật.

2. Phối hợp với Cục Công nghệ thông tin và Cục Cơ yếu trong việc giám sát mạng và triển khai các giải pháp bảo đảm an toàn thông tin.

3. Phối hợp với các thành viên mạng lưới ứng cứu sự cố mạng máy tính trong Quân đội nhân dân Việt Nam khắc phục các sự cố mạng truyền số liệu quân sự và các mạng thông tin liên lạc.

Điều 48. Tập đoàn Viễn thông Quân đội

1. Cung cấp đầy đủ các thông tin kỹ thuật nghiệp vụ có liên quan trực tiếp phục vụ điều tra vi phạm về an toàn thông tin theo yêu cầu của Cục Công nghệ thông.

2. Chủ trì, phối hợp với Cục Công nghệ thông tin và các cơ quan, đơn vị có liên quan tổ chức triển khai hạ tầng kết nối mạng Internet đến các cơ quan, đơn vị trong toàn quân, tổ chức quản lý chặt chẽ hệ thống mạng Internet sử dụng trong các cơ quan, đơn vị Quân đội bảo đảm an toàn thông tin theo quy định pháp luật.

3. Cung cấp các dịch vụ Internet, viễn thông, truyền hình an toàn cho các cơ quan, đơn vị trong Quân đội. Chịu trách nhiệm trước Bộ Quốc phòng về bảo đảm an toàn thông tin đối với các dịch vụ do Tập đoàn cung cấp cho các cơ quan, đơn vị trong Quân đội.

4. Hỗ trợ, huy động phương tiện, lực lượng tham gia phối hợp với Cục Công nghệ thông tin trong bảo đảm an toàn thông tin, ứng cứu khắc phục sự cố an toàn thông tin, bảo vệ chủ quyền quốc gia trên không gian mạng, bảo vệ hệ thống thông tin quân sự, quốc phòng và bảo vệ hệ thống thông tin quan trọng quốc gia.

Chương IV ĐIỀU KHOẢN THI HÀNH

Điều 49. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày **25/01** năm 2017.

Điều 50. Trách nhiệm thi hành

1. Tổng Tham mưu trưởng, Thủ trưởng các cơ quan, đơn vị, tổ chức và cá nhân liên quan trong Quân đội nhân dân Việt Nam chịu trách nhiệm thi hành Thông tư này.
2. Cục trưởng Cục Công nghệ thông tin chịu trách nhiệm hướng dẫn, tổ chức thực hiện. Mesup

Nơi nhận:

- Bộ trưởng (để b/c);
- Chủ nhiệm TCCT;
- Các đ/c Thủ trưởng;
- Các đầu mối trực thuộc BQP;
- C20: TTVP, NC, VPC, CCHC;
- C13, C58, C86;
- Lưu: VT, NC; Dũng 90.

**KT. BỘ TRƯỞNG
THỦ TRƯỞNG**

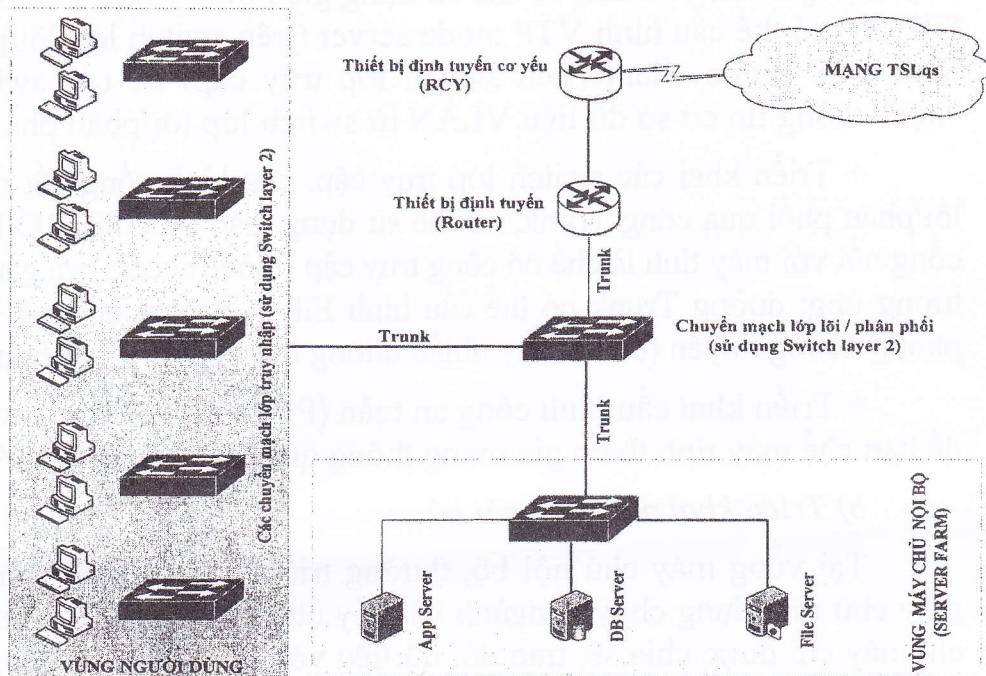


Trung tướng Phan Văn Giang

PHỤ LỤC I
Mô hình mạng máy tính an toàn
*(Kèm theo Thông tư số 10/2016/TT-BQP ngày 12 tháng 12 năm 2016 của
Bộ trưởng Bộ Quốc phòng)*

1. Triển khai 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 việc khai thác hiệu quả các tính năng bảo đảm an toàn thông tin sẵn có trong các trang bị Công nghệ thông tin. 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 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 cập (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 TSLqs không thể khởi tạo kết nối vào các máy tính, máy chủ bên trong mạng nội bộ.

+ Cấu hình kiểm soát truy cập (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, công 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.

b) *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 cờ 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.

2. Hướng dẫn triển khai mạng 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):*

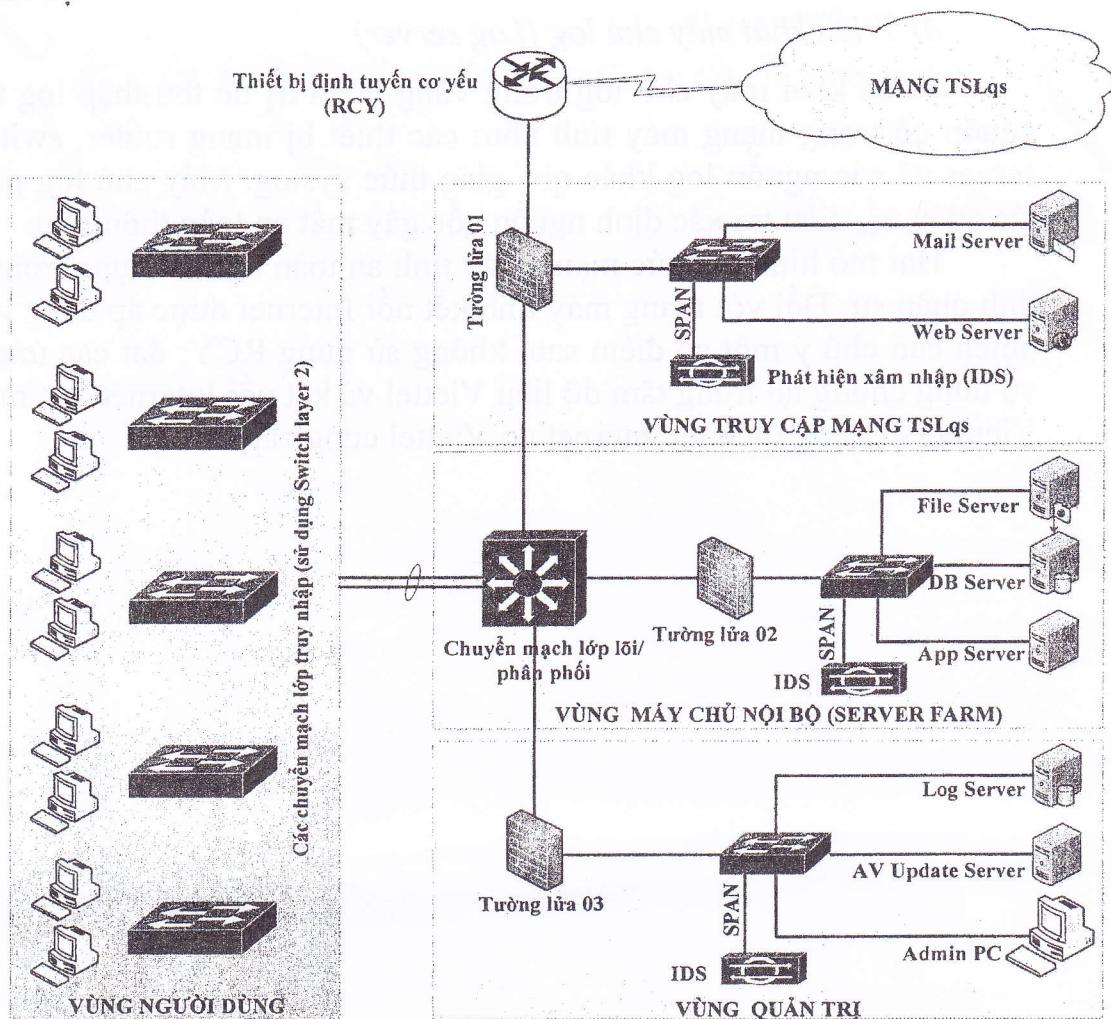
Trang bị 03 thiết bị tường lửa vật lý riêng biệt hoặc trên một thiết bị ta chia thành 03 thiết bị logic.

- Tường lửa 01 dùng để bảo vệ vùng truy cập mạng: thiết lập chính sách bảo vệ người dùng trong mạng nội bộ khi truy cập mạng TSLqs và bảo vệ vùng máy chủ công cộng cho phép truy cập vào từ mạng TSLqs (Web, Mail); ghi nhật ký truy cập mạng (log) gửi về máy chủ Log Server trong vùng quản trị.

- Tường lửa 02 dùng để bảo vệ 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, cổng Port); ghi lại mọi truy cập (log) gửi về máy chủ Log trong vùng quản trị.

- Tường lửa 03 dùng để bảo vệ 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 Intrusion Detection System-NIDS)

Triển khai NIDS (có thể sử dụng phần mềm nguồn mở Snort) trong các vùng máy chủ truy cập mạng TSLqs, 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 Cục Công nghệ thông tin) 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

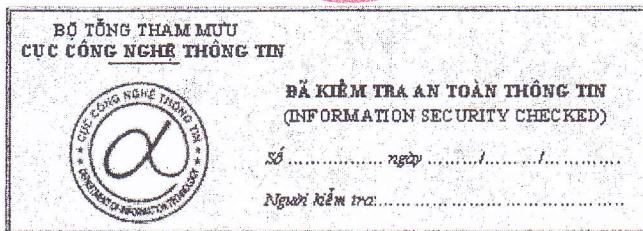
cụ dò quét điểm yếu bảo mật; máy tính quản trị phải được triển khai các giải pháp bảo đảm an toàn như với máy chủ, máy trạm ở trên.

d) 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.

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, tuy nhiên cần chú ý một số điểm sau: không sử dụng RCY; đặt các ứng dụng, dịch vụ dùng chung tại trung tâm dữ liệu Viettel và kết nối Internet qua mạng Internet Viettel (sử dụng dịch vụ internet do Viettel cung cấp).

PHỤ LỤC II
Mẫu tem Kiểm tra an toàn thông tin
*(Kèm theo Thông tư số 202/2016/TT-BQP ngày 12 tháng 10 năm 2016 của
Bộ trưởng Bộ Quốc phòng)*



Kích thước tem: 2.8 x 6.7 cm, tem sử dụng chất liệu giấy vỡ, nền màu xanh lam nhạt.

Định dạng chữ sử dụng: Times New Roman.

Cỡ chữ viết: 5.