

PHẦN VĂN BẢN QUY PHẠM PHÁP LUẬT

BỘ QUỐC PHÒNG

BỘ QUỐC PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Số: 58/2015/TT-BQP

Hà Nội, ngày 08 tháng 7 năm 2015

THÔNG TƯ

**Ban hành Quy định hoạt động điều phối và ứng cứu sự cố
mạng máy tính trong Quân đội nhân dân Việt Nam**

Căn cứ Luật Ban hành văn bản quy phạm pháp luật năm 2008;

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Luật Viễn thông năm 2009;

Căn cứ Luật Cơ yếu năm 2011;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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

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

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

Bộ trưởng Bộ Quốc phòng quyết định.

Điều 1. Ban hành kèm theo Thông tư này Quy định hoạt động điều phối và ứng cứu sự cố mạng máy tính trong Quân đội nhân dân Việt Nam.

Điều 2. Thông tư này có hiệu lực thi hành kể từ ngày 24 tháng 8 năm 2015.

Điều 3. Tổng Tham mưu trưởng, Chỉ huy các cơ quan, đơn vị và cá nhân có liên quan trong Quân đội chịu trách nhiệm thi hành Thông tư này./.

KT. BỘ TRƯỞNG

THỨ TRƯỞNG

Thượng tướng Đỗ Bá Tỵ

BỘ QUỐC PHÒNG**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
Độc lập - Tự do - Hạnh phúc**QUY ĐỊNH****Hoạt động điều phối và ứng cứu sự cố mạng máy tính
trong Quân đội nhân dân Việt Nam**

*(Ban hành kèm theo Thông tư số 58/2015/TT-BQP
ngày 08 tháng 7 năm 2015 của Bộ trưởng Bộ Quốc phòng)*

Chương I
QUY ĐỊNH CHUNG**Điều 1. Phạm vi điều chỉnh**

Quy định này quy định về mạng lưới ứng cứu sự cố mạng máy tính trong Quân đội nhân dân Việt Nam (QĐNDVN); hoạt động điều phối và ứng cứu sự cố mạng máy tính trong QĐNDVN; trách nhiệm của các cơ quan, đơn vị, cá nhân có liên quan tới hoạt động điều phối và ứng cứu sự cố mạng máy tính trong QĐNDVN.

Điều 2. Đối tượng áp dụng

Quy định này áp dụng đối với các cơ quan, đơn vị, cá nhân có liên quan đến hoạt động điều phối và ứng cứu khắc phục sự cố mạng máy tính trong QĐNDVN và các cơ quan, đơn vị, cá nhân quản lý, vận hành, khai thác mạng máy tính trong QĐNDVN.

Điều 3. Giải thích từ ngữ

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

1. *Mạng máy tính trong Quân đội nhân dân Việt Nam (gọi tắt mạng máy tính)* là khái niệm chung dùng để chỉ mạng máy tính quân sự, mạng Internet sử dụng trong Quân đội.

2. *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 QĐNDVN; không kết nối mạng Internet và các mạng kinh doanh khác. Mạng máy tính quân sự bao gồm mạng máy tính nội bộ của các cơ quan, đơn vị; mạng máy tính diện rộng trong Bộ Quốc phòng; mạng truyền số liệu quân sự và tài nguyên trên mạng máy tính.

3. *Mạng Internet sử dụng trong Quân đội* là mạng máy tính trong các cơ quan, đơn vị được kết nối với mạng Internet và các ứng dụng, dịch vụ của các cơ quan, đơn vị trên mạng Internet.

4. *Sự cố mạng máy tính* (gọi tắt là sự cố) là sự kiện đã, đang hoặc có khả năng xảy ra làm mất an toàn thông tin được phát hiện thông qua giám sát, đánh giá phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, cơ quan, đơn vị hoạt động trong lĩnh vực an toàn thông tin.

5. *Sự cố nghiêm trọng* là sự cố có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính trong QĐNDVN; đòi hỏi phối hợp của nhiều cơ quan, đơn vị trong Bộ Quốc phòng hay của quốc gia để giải quyết.

6. *Mạng lưới ứng cứu sự cố mạng máy tính* (gọi tắt là mạng lưới) là tập hợp các cơ quan, đơn vị, tổ chức có nghĩa vụ tham gia hoạt động ứng cứu sự cố mạng máy tính.

7. *Thành viên mạng lưới* là các cơ quan, đơn vị, tổ chức tham gia hoạt động ứng cứu sự cố mạng máy tính.

Điều 4. Nguyên tắc chung

1. Điều phối hoạt động ứng cứu sự cố theo phân cấp, theo khu vực, trong phạm vi thuộc quyền.

2. Tổ chức ứng cứu sự cố mạng máy tính phải đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, hiệu quả và an toàn thông tin.

3. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật theo yêu cầu của cơ quan, đơn vị gặp sự cố trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng khác mà cần cảnh báo, nhắc nhở.

4. Mạng lưới ứng cứu sự cố mạng máy tính nằm trong mạng lưới ứng cứu sự cố mạng máy tính quốc gia do Bộ Thông tin và Truyền thông hướng dẫn, chỉ đạo nghiệp vụ.

Chương II

MẠNG LƯỚI ỨNG CỨU SỰ CỐ MẠNG MÁY TÍNH

Điều 5. Mạng lưới ứng cứu sự cố mạng máy tính

1. Thành viên mạng lưới ứng cứu sự cố mạng máy tính bao gồm:

- a) Cục Công nghệ thông tin/Bộ Tổng Tham mưu;
- b) Cục Bảo vệ an ninh Quân đội/Tổng cục Chính trị;
- c) Cục Cơ yếu/Bộ Tổng Tham mưu;
- d) Binh chủng Thông tin liên lạc;
- e) Tập đoàn Viễn thông Quân đội;
- g) Cơ quan quản lý công nghệ thông tin ở các cơ quan, đơn vị;

h) Tổ ứng cứu tham gia khắc phục sự cố cơ sở hạ tầng mạng trọng yếu quốc gia của Bộ Quốc phòng.

2. Thành viên mạng lưới có quyền và nghĩa vụ chia sẻ thông tin, kinh nghiệm, tham gia hoạt động diễn tập ứng cứu sự cố, tham gia các khóa đào tạo, bồi dưỡng về hoạt động ứng cứu sự cố.

Điều 6. Cơ quan điều phối các hoạt động ứng cứu sự cố mạng máy tính.

1. Cục Công nghệ thông tin/Bộ Tổng Tham mưu là cơ quan điều phối các hoạt động ứng cứu của mạng lưới ứng cứu sự cố mạng máy tính (gọi tắt là cơ quan điều phối) có chức năng:

a) Chỉ đạo, hướng dẫn nghiệp vụ về hoạt động điều phối và ứng cứu sự cố; có quyền điều động các thành viên khác trong mạng lưới ứng cứu tham gia ngăn chặn, xử lý và khắc phục sự cố trong Bộ Quốc phòng;

b) Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối;

c) Trao đổi thông tin, hợp tác ứng cứu sự cố với các tổ chức ứng cứu sự cố máy tính trong nước, quốc tế và các nhà cung cấp dịch vụ Internet.

2. Trục ban Tác chiến/Cục Công nghệ thông tin là bộ phận tiếp nhận thông tin yêu cầu ứng cứu sự cố và thực hiện lệnh điều phối hoạt động ứng cứu sự cố trong toàn quân.

Điều 7. Đầu mối ứng cứu sự cố

1. Đầu mối ứng cứu sự cố là cá nhân hay bộ phận được phép thay mặt cho thành viên mạng lưới để liên lạc và trao đổi thông tin với các thành viên mạng lưới khác trong hoạt động ứng cứu sự cố.

2. Thành viên mạng lưới có trách nhiệm tổ chức đầu mối ứng cứu sự cố và thông báo đầu mối ứng cứu về cơ quan điều phối.

3. Đầu mối ứng cứu sự cố có trách nhiệm tiếp nhận thông tin điều phối, trao đổi thông tin sự cố với cơ quan điều phối và đơn vị xảy ra sự cố.

4. Cá nhân làm đầu mối ứng cứu sự cố phải có trình độ chuyên môn, kỹ năng nghiệp vụ để thực hiện các hoạt động ứng cứu sự cố và phải bảo đảm liên lạc thông suốt liên tục.

Chương III

ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ MẠNG MÁY TÍNH

Điều 8. Thông báo sự cố

1. Cơ quan, đơn vị khi gặp sự cố mà không tự khắc phục được phải thông báo sự cố tới một hoặc nhiều thành viên mạng lưới sau:

- a) Cơ quan điều phối;
 - b) Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho cơ quan, đơn vị đó (nếu có);
2. Khi phát hiện thấy sự cố nghiêm trọng, cơ quan, đơn vị phải có trách nhiệm thông báo ngay cho cơ quan điều phối.
3. Nội dung thông báo sự cố gồm:
- a) Thông tin mô tả sự cố;
 - b) Các biện pháp đã, đang triển khai khắc phục;
 - c) Thông tin khác theo yêu cầu của cơ quan điều phối;
 - d) Kiến nghị và đề xuất.
4. Cơ quan điều phối hướng dẫn chi tiết thông báo sự cố.

Điều 9. Tiếp nhận và xử lý thông báo sự cố

1. Thành viên mạng lưới tiếp nhận thông báo sự cố có trách nhiệm:
- a) Xử lý thông tin sự cố và phản hồi trong vòng 12 giờ cho cơ quan, đơn vị, cá nhân gửi thông báo để xác nhận về việc đã nhận được thông báo sự cố;
 - b) Xử lý sự cố trong khả năng và trách nhiệm của mình, báo cáo kết quả xử lý sự cố về cơ quan điều phối theo quy định;
 - c) Kịp thời báo cáo sự cố về cơ quan điều phối nếu không xử lý được.
2. Cơ quan điều phối tiếp nhận thông báo sự cố có trách nhiệm:
- a) Đưa ra yêu cầu điều phối tới thành viên mạng lưới tham gia ứng cứu sự cố khi cần thiết;
 - b) Huy động các nguồn lực khác, mời chuyên gia tham gia ứng cứu sự cố khi cần thiết.
 - c) Báo cáo Thủ trưởng Bộ Tổng Tham mưu huy động các lực lượng ngoài Quân đội tham gia ứng cứu sự cố mạng máy tính trong Quân đội nhân dân Việt Nam khi cần thiết.

Điều 10. Điều phối

1. Cơ quan điều phối có trách nhiệm tổ chức điều phối theo đúng quy trình, quy định về điều phối hoạt động ứng cứu sự cố mạng máy tính do cơ quan có thẩm quyền ban hành.
2. Các thành viên mạng lưới có trách nhiệm hợp tác và tham gia hoạt động ứng cứu sự cố mạng máy tính và hệ thống thông tin quan trọng quốc gia theo yêu cầu của cơ quan điều phối.
3. Các cơ quan, đơn vị gặp sự cố phải phối hợp với cơ quan điều phối và thành viên mạng lưới trong quá trình thực hiện điều phối và ứng cứu sự cố.

Điều 11. Ứng cứu sự cố

1. Thành viên mạng lưới tổ chức ứng cứu theo đúng quy trình, quy định về ứng cứu sự cố do cơ quan có thẩm quyền ban hành.

2. Thành viên mạng lưới tiếp nhận yêu cầu điều phối; phối hợp chặt chẽ với đơn vị nơi xảy ra sự cố và các thành viên cùng tham gia ứng cứu tổ chức thực hiện hoạt động ứng cứu theo đúng yêu cầu điều phối.

3. Thành viên mạng lưới thường xuyên báo cáo tình hình kết quả thực hiện nhiệm vụ ứng cứu về cơ quan điều phối theo đúng quy định.

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

5. Sau khi khắc phục sự cố, thành viên mạng lưới tham gia ứng cứu phải có trách nhiệm:

- a) Rà soát, xác định nguyên nhân cơ bản gây ra sự cố;
- b) Tổ chức kiểm tra lại và khắc phục triệt để sự cố;
- c) Bảo đảm hệ thống hoạt động bình thường trước khi bàn giao toàn bộ hệ thống cho cơ quan, đơn vị chủ quản.

Điều 12. Kết thúc điều phối, ứng cứu

Khi kết thúc hoạt động điều phối, ứng cứu sự cố, thành viên mạng lưới tham gia ứng cứu có trách nhiệm tổng hợp kết quả thực hiện hoạt động ứng cứu; tổ chức rút kinh nghiệm triển khai hoạt động ứng cứu khắc phục sự cố; báo cáo kết quả thực hiện, kiến nghị (nếu có) với cơ quan điều phối.

Chương IV**TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ, CÁ NHÂN****Điều 13. Cục Công nghệ thông tin/Bộ Tổng Tham mưu**

1. Chủ trì xây dựng, báo cáo Thủ trưởng Bộ Tổng Tham mưu ban hành hoặc trình cấp có thẩm quyền ban hành các văn bản quy định, hướng dẫn về hoạt động điều phối và ứng cứu sự cố mạng máy tính.

2. Tiếp nhận, xử lý các thông tin sự cố; chủ trì tổ chức điều phối hoạt động ứng cứu sự cố mạng máy tính.

3. Xây dựng và triển khai hệ thống kỹ thuật hỗ trợ việc giám sát, phát hiện sự cố; tổ chức hoạt động điều phối và ứng cứu sự cố mạng máy tính; xây dựng cơ sở dữ liệu quản lý, điều hành tập trung cho hoạt động điều phối và ứng cứu sự cố.

4. Tổng hợp, công bố tới các thành viên trong mạng lưới các thông tin thông báo, cảnh báo, giải pháp khắc phục về các điểm yếu, lỗ hổng bảo mật; nguy cơ mất an toàn đối với mạng máy tính.

5. Tổ chức huấn luyện, hướng dẫn nghiệp vụ, diễn tập hoạt động điều phối và ứng cứu sự cố mạng máy tính.

6. Quản lý hoạt động của Tổ ứng cứu khắc phục sự cố cơ sở hạ tầng mạng trọng yếu quốc gia của Bộ Quốc phòng; huy động các lực lượng trong mạng lưới sẵn sàng tham gia bảo vệ hệ thống thông tin quan trọng quốc gia.

7. Phối hợp với các cơ quan, đơn vị quản lý, vận hành các hệ thống thông tin quan trọng quốc gia; cơ quan, đơn vị, tổ chức ứng cứu sự cố ngoài Quân đội để xây dựng cơ chế phối hợp, quy trình ứng cứu sự cố.

8. Phối hợp với Cục Tài chính/Bộ Quốc phòng và các cơ quan, đơn vị liên quan nghiên cứu, bố trí nguồn kinh phí bảo đảm cho hoạt động điều phối và ứng cứu sự cố mạng máy tính.

9. Đại diện cho Bộ Quốc phòng tổ chức lực lượng tham gia hoạt động ứng cứu sự cố ngoài Quân đội khi được yêu cầu; tham gia hợp tác quốc tế về điều phối và ứng cứu sự cố.

Điều 14. Cục Bảo vệ an ninh Quân đội/Tổng cục Chính trị

1. Phối hợp với Cục Công nghệ thông tin/BTTM và các cơ quan liên quan trong hoạt động ứng cứu sự cố mạng máy tính, hệ thống thông tin quan trọng quốc gia.

2. Điều tra, xác minh làm rõ tổ chức, cá nhân làm mất an ninh thông tin hoặc lợi dụng hoạt động ứng cứu sự cố mạng máy tính để lấy cắp dữ liệu, làm lộ lọt thông tin.

Điều 15. Cục Cơ yếu/Bộ Tổng Tham mưu

1. Xây dựng các phương án và tổ chức ứng cứu sự cố hệ thống bảo mật mạng máy tính.

2. Phối hợp với Cục Công nghệ thông tin/BTTM trong hoạt động ứng cứu sự cố mạng máy tính, hệ thống thông tin quan trọng quốc gia có liên quan đến hệ thống, thiết bị bảo mật mạng máy tính.

Điều 16. Binh chủng Thông tin liên lạc

1. Xây dựng các phương án và tổ chức ứng cứu sự cố hạ tầng mạng truyền số liệu.

2. Phối hợp với thành viên mạng lưới trong việc cung cấp thông tin, hỗ trợ kỹ thuật về khắc phục sự cố liên quan đến mạng truyền số liệu.

3. Phối hợp với Cục Công nghệ thông tin/BTTM trong hoạt động ứng cứu sự cố mạng máy tính, hệ thống thông tin quan trọng quốc gia.

4. Bảo đảm thông tin liên lạc phục vụ cho các hoạt động điều phối và ứng cứu sự cố mạng máy tính khi có yêu cầu.

Điều 17. Tập đoàn Viễn thông Quân đội

1. Tổ chức thực hiện ứng cứu sự cố cho các sản phẩm, dịch vụ và hạ tầng mạng Internet do Tập đoàn Viễn thông Quân đội cung cấp cho các cơ quan, đơn vị.
2. Tham gia hoạt động ứng cứu sự cố mạng máy tính và hệ thống thông tin quan trọng quốc gia theo sự điều phối của Cơ quan điều phối.
3. Cung cấp thông tin, hỗ trợ kỹ thuật về khắc phục sự cố liên quan đến hạ tầng mạng Internet, dịch vụ của Tập đoàn Viễn thông Quân đội.
4. Thực hiện các hoạt động ứng cứu sự cố mạng Internet Việt Nam theo quy định của Bộ Thông tin và Truyền thông.

Điều 18. Các cơ quan, đơn vị trong toàn quân

1. Cơ quan quản lý công nghệ thông tin:
 - a) Hướng dẫn việc thực hiện hoạt động ứng cứu sự cố trong phạm vi trách nhiệm của mình;
 - b) Kịp thời huy động lực lượng công nghệ thông tin tại chỗ và triển khai các giải pháp khắc phục sự cố;
 - c) Thông báo với cơ quan điều phối để được hướng dẫn, hỗ trợ ứng cứu của lực lượng chuyên trách;
 - d) Cung cấp đầy đủ thông tin và phối hợp chặt chẽ với cơ quan điều phối, thành viên mạng lưới tham gia ứng cứu khắc phục sự cố;
 - e) Xác định nguyên nhân, tổ chức rút kinh nghiệm và triển khai các giải pháp bảo đảm để không lặp lại sự cố;
2. Cơ quan, đơn vị quản lý, khai thác, sử dụng mạng máy tính:
 - a) Áp dụng biện pháp, giải pháp kỹ thuật nhằm giám sát hệ thống, có các phương án khắc phục sự cố và triển khai các giải pháp bảo đảm an toàn thông tin;
 - b) Cung cấp thông tin và tích cực phối hợp với các thành viên mạng lưới ứng cứu sự cố trong hoạt động phát hiện, ngăn chặn và xử lý sự cố.

Điều 19. Trách nhiệm của cá nhân

1. Cá nhân tham gia ứng cứu sự cố có trách nhiệm:
 - a) Tuân thủ nghiêm quy trình, biện pháp đã được thống nhất;
 - b) Kịp thời báo cáo với người có thẩm quyền về các dấu hiệu bất thường trong quá trình khắc phục;
 - c) Không lợi dụng hoạt động ứng cứu sự cố để đánh cắp dữ liệu, gây lộ lọt dữ liệu của hệ thống.
2. Cá nhân quản lý, vận hành, khai thác mạng máy tính có trách nhiệm:
 - a) Phải kịp thời báo cáo với cơ quan quản lý công nghệ thông tin về các dấu hiệu bất thường, sự cố xảy ra;
 - b) Chủ động cung cấp thông tin và tích cực phối hợp trong hoạt động ứng cứu sự cố.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 20. Hướng dẫn, kiểm tra

Cục Công nghệ thông tin/Bộ Tổng Tham mưu chủ trì, phối hợp với cơ quan chức năng liên quan hướng dẫn, kiểm tra việc thực hiện đối với cơ quan, đơn vị và cá nhân trong Quân đội; kịp thời phát hiện và phối hợp với cơ quan chức năng liên quan xử lý những trường hợp vi phạm Quy định này.

Điều 21. Tổ chức thực hiện

1. Chỉ huy các cơ quan, đơn vị trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình có trách nhiệm quán triệt, hướng dẫn, thực hiện, kiểm tra, giám sát và đôn đốc thực hiện Quy định này.

2. Trong quá trình thực hiện Quy định này, nếu phát sinh vướng mắc, bất cập; cơ quan, đơn vị báo cáo về Bộ Tổng Tham mưu (qua Cục Công nghệ thông tin) để tổng hợp, báo cáo Thủ tướng Bộ Quốc phòng sửa đổi, bổ sung./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Thượng tướng Đỗ Bá Tỵ