

Hà Nội, ngày 28 tháng 11 năm 2008

THÔNG TƯ LIÊN TỊCH
Về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin
trong hoạt động bưu chính, viễn thông và công nghệ thông tin

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Luật An ninh quốc gia năm 2004;

Căn cứ Pháp lệnh Bưu chính, Viễn thông năm 2002;

Căn cứ Nghị định số 160/2004/NĐ-CP ngày 03/9/2004 quy định chi tiết thi hành một số điều của Pháp lệnh Bưu chính, viễn thông về viễn thông;

Căn cứ Nghị định số 157/2004/NĐ-CP ngày 18/8/2004 quy định chi tiết thi hành một số điều của Pháp lệnh Bưu chính, viễn thông về bưu chính;

Căn cứ Nghị định số 128/2007/NĐ-CP ngày 02/8/2007 về dịch vụ chuyển phát;

Căn cứ Nghị định số 187/2007/NĐ-CP ngày 25/12/2007 quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Nghị định số 136/2003/NĐ-CP ngày 14/11/2003 quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an;

Căn cứ Nghị định số 151/2005/NĐ-CP ngày 14/12/2005 về quyền hạn, trách nhiệm của cơ quan và cán bộ chuyên trách bảo vệ an ninh quốc gia.

Bộ Thông tin và Truyền thông, Bộ Công an thống nhất hướng dẫn về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin như sau:

I. NHỮNG QUY ĐỊNH CHUNG

1. Phạm vi điều chỉnh và đối tượng áp dụng

a) Thông tư này hướng dẫn việc bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, chuyển phát, viễn thông, Internet, truyền dẫn phát sóng và công nghệ thông tin (sau đây viết gọn là bưu chính, viễn thông và công nghệ thông tin).

b) Thông tư này áp dụng đối với tổ chức, cá nhân liên quan đến việc thiết lập mạng lưới; cung cấp, sử dụng dịch vụ; sản xuất, kinh doanh thiết bị và thi công lắp đặt công trình bưu chính, viễn thông và công nghệ thông tin tại Việt Nam.

2. Giải thích từ ngữ

a) Bảo đảm an toàn cơ sở hạ tầng là sự toàn vẹn của hệ thống thiết bị, mạng lưới, công trình bưu chính, viễn thông và công nghệ thông tin; sự toàn vẹn, bí mật của thư, bưu phẩm, bưu kiện, gói, kiện hàng hóa, thông tin được chuyển qua mạng lưới bưu chính, viễn thông và công nghệ thông tin; sự an toàn của các bên tham gia vào quá trình thiết lập, cung cấp và sử dụng dịch vụ bưu chính, viễn thông và công nghệ thông tin.

b) Bảo đảm an ninh thông tin là các hoạt động quản lý, kiểm soát, phòng ngừa, phát hiện, ngăn chặn, đấu tranh chống hành vi sử dụng, lợi dụng cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin để xâm phạm an ninh quốc gia và trật tự, an toàn xã hội và lợi ích của công dân.

3. Các nguyên tắc chung bảo đảm an toàn cơ sở hạ tầng, an ninh thông tin

a) Các bên tham gia hoạt động bưu chính, viễn thông và công nghệ thông tin có trách nhiệm bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin, kịp thời phát hiện, khắc phục các sự cố; chịu trách nhiệm trước pháp luật về nội dung thư, bưu phẩm, bưu kiện, gói, kiện hàng hóa, thông tin mà mình lưu trữ, chuyển qua mạng bưu chính, viễn thông và công nghệ thông tin.

b) Việc bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin không làm cản trở hoạt động sản xuất, kinh doanh của doanh nghiệp bưu chính, viễn thông, công nghệ thông tin và tổn hại đến quyền, lợi ích hợp pháp của các bên liên quan đến hoạt động bưu chính, viễn thông và công nghệ thông tin.

c) Chỉ những người có thẩm quyền của cơ quan chuyên trách bảo vệ an ninh quốc gia quy định tại Điều 9 Nghị định số 151/2005/NĐ-CP ngày 14/12/2005 về quyền hạn, trách nhiệm của cơ quan và cán bộ chuyên trách bảo vệ an ninh quốc gia mới có thẩm quyền kiểm soát an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

d) Các hành vi vi phạm gây ảnh hưởng đến an toàn cơ sở hạ tầng và an ninh thông tin phải được phát hiện kịp thời và xử lý nghiêm minh theo quy định của pháp luật.

4. Các hành vi bị nghiêm cấm

a) Cung cấp, sử dụng, lợi dụng cơ sở hạ tầng, các dịch vụ bưu chính, viễn thông và công nghệ thông tin để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, gây ảnh hưởng xấu tới thuần phong, mỹ tục của dân tộc.

b) Cản trở bất hợp pháp đến hoạt động bưu chính, viễn thông và công nghệ thông tin.

c) Phá hủy, làm hư hỏng hoặc hủy hoại công trình bưu chính, viễn thông và công nghệ thông tin hoặc sử dụng, lợi dụng mạng lưới, thiết bị, các công cụ phần cứng, phần mềm để gây nhiễu, gây rối loạn hoạt động cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin.

d) Đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã, thông tin riêng của tổ chức, cá nhân; ngăn cản bất hợp pháp việc truy nhập thông tin của tổ chức, cá nhân.

đ) Sản xuất, mua, bán, tàng trữ, vận chuyển, sử dụng tem bưu chính giả; chiếm đoạt, bóc mở, trao đổi, tiết lộ nội dung thư, bưu phẩm, bưu kiện, gói, kiện hàng hóa, thông tin chuyển qua mạng bưu chính, viễn thông và công nghệ thông tin.

e) Các hành vi trái pháp luật khác liên quan đến hoạt động bưu chính, viễn thông và công nghệ thông tin.

II. BẢO ĐẢM AN TOÀN CƠ SỞ HẠ TẦNG VÀ AN NINH THÔNG TIN

1. Bảo đảm an toàn cơ sở hạ tầng trong hoạt động bưu chính, viễn thông và công nghệ thông tin

Nội dung bảo đảm an toàn cơ sở hạ tầng trong hoạt động bưu chính, viễn thông và công nghệ thông tin, bao gồm:

a) Bảo vệ cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin nhằm ngăn chặn các hoạt động tấn công, đột nhập, phá hoại; phòng, chống sự cố do cháy, nổ và các sự cố khác do thiên tai, con người, động vật gây ra.

b) Triển khai các giải pháp và hệ thống thiết bị dự phòng để bảo đảm cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin hoạt động liên tục và an toàn.

c) Triển khai các giải pháp, biện pháp để ngăn chặn việc sử dụng, lợi dụng mạng lưới, thiết bị, các công cụ phần cứng, phần mềm để cản trở, gây nhiễu, gây rối loạn, làm hư hỏng, hủy hoại

hoạt động cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin; phòng, chống virus, thư rác, phần mềm gián điệp; phòng, chống hành vi đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã, thông tin riêng của các tổ chức, cá nhân.

d) Bảo đảm an toàn cho trang thiết bị và nhân viên khai thác mạng bưu chính, viễn thông và công nghệ thông tin.

đ) Thanh tra, kiểm tra và xử lý vi phạm về an toàn cơ sở hạ tầng trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

2. Bảo đảm an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin

Nội dung bảo đảm an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin, bao gồm:

a) Triển khai các biện pháp nghiệp vụ, kiểm soát thông tin chuyển qua mạng bưu chính, viễn thông và công nghệ thông tin theo quy định của pháp luật nhằm phát hiện, ngăn chặn, xử lý kịp thời các hành vi vi phạm; dừng việc cung cấp, sử dụng dịch vụ và có biện pháp xử lý đối với những trường hợp cung cấp, sử dụng, lợi dụng mạng lưới, dịch vụ bưu chính, viễn thông và công nghệ thông tin để hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

b) Triển khai các giải pháp, biện pháp bảo đảm an toàn thông tin bí mật nhà nước, thông tin riêng của tổ chức, cá nhân, nội dung thư, bưu phẩm, bưu kiện, gói, kiện hàng hóa, thông tin chuyên qua mạng bưu chính, viễn thông và công nghệ thông tin.

c) Phối hợp trong việc cấp phép, quy định điều kiện kinh doanh để bảo đảm an ninh thông tin đối với các hoạt động bưu chính, viễn thông và công nghệ thông tin.

d) Thanh tra, kiểm tra và xử lý vi phạm về an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

III. TRÁCH NHIỆM BẢO ĐẢM AN TOÀN CƠ SỞ HẠ TẦNG VÀ AN NINH THÔNG TIN

1. Trách nhiệm của Bộ Thông tin và Truyền thông

a) Chỉ đạo, hướng dẫn các tổ chức, cá nhân, doanh nghiệp bưu chính, viễn thông và công nghệ thông tin thực hiện các quy định của pháp luật về an toàn cơ sở hạ tầng; thanh tra, kiểm tra, xử lý vi phạm quy định về bảo đảm an toàn cơ sở hạ tầng trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

b) Phối hợp với Bộ Công an để đảm bảo an ninh thông tin, thanh tra, kiểm tra và xử lý đối với tổ chức, cá nhân vi phạm quy định về bảo đảm an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

c) Trong trường hợp khẩn cấp theo quy định của pháp luật, quyết định huy động một phần hay toàn bộ cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin để phục vụ nhiệm vụ an ninh, quốc phòng.

d) Chủ trì xây dựng, ban hành, tổ chức thực hiện tiêu chuẩn, quy chuẩn kỹ thuật về an toàn cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin.

e) Lập danh mục công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng khác về cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin do lực lượng vũ trang canh gác bảo vệ và kèm theo hồ sơ gửi cơ quan có thẩm quyền thẩm định, phê duyệt theo quy định của pháp luật.

f) Về cấp phép:

- Chủ trì thẩm định, cấp phép kinh doanh, cấp phép thử nghiệm mạng, dịch vụ viễn thông, Internet, bưu chính, chuyển phát và thông báo bằng văn bản cho Bộ Công an.

- Chủ trì, phối hợp với Bộ Công an thẩm định, cấp phép cho các doanh nghiệp chuyên phát có vốn đầu tư nước ngoài, cấp phép cho các tổ chức, cá nhân nước ngoài tại Việt Nam thiết lập mạng viễn thông dùng riêng, mạng Internet dùng riêng, sử dụng tần số và thiết bị phát sóng vô tuyến điện.

- Chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng thẩm định, cấp phép lắp đặt cáp viễn thông trong vùng biển của Việt Nam theo quy định tại Điều 46 và Điều 47 Nghị định 160/2004/NĐ-CP ngày 3 tháng 9 năm 2004 quy định chi tiết thi hành một số điều của Pháp lệnh Bưu chính, Viễn thông về viễn thông.

- Chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng thẩm định, cấp phép cho tàu, thuyền hoạt động khảo sát, thi công, duy tu, bảo dưỡng, sửa chữa tuyến cáp viễn thông trong vùng biển của Việt Nam.

2. Trách nhiệm của Bộ Công an

a) Chỉ đạo, triển khai công tác bảo đảm an ninh thông tin, phòng, chống tội phạm và các vi phạm pháp luật khác trong lĩnh vực bưu chính, viễn thông và công nghệ thông tin; thanh tra, kiểm tra và xử lý vi phạm đối với tổ chức, cá nhân vi phạm quy định về bảo đảm an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

b) Chỉ đạo Công an các đơn vị, địa phương phối hợp chặt chẽ với các cơ quan, tổ chức thuộc Bộ Thông tin và Truyền thông bảo đảm an toàn cơ sở hạ tầng, thanh tra, kiểm tra và xử lý đối với tổ chức, cá nhân vi phạm quy định về bảo đảm an toàn cơ sở hạ tầng trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

c) Tổ chức nghiên cứu, đầu tư cho các hoạt động nghiên cứu khoa học, công nghệ nhằm nâng cao khả năng ứng dụng công nghệ thông tin vào công tác bảo đảm an ninh quốc gia, giữ gìn trật tự, an toàn xã hội. Triển khai các biện pháp nghiệp vụ, đầu tư, xây lắp hệ thống thiết bị phục vụ kiểm soát, bảo đảm an toàn cơ sở hạ tầng, an ninh thông tin của Bộ Công an.

d) Chỉ đạo Công an các đơn vị, địa phương triển khai lực lượng Cảnh sát nhân dân vũ trang canh gác bảo vệ các công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng khác về cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin.

đ) Cơ quan chuyên trách bảo vệ an ninh quốc gia thuộc Công an các đơn vị, địa phương khi phát hiện các thông tin, tài liệu, dữ liệu, đồ vật liên quan đến hoạt động xâm phạm an ninh quốc gia theo quy định tại Điều 3 Nghị định số 151/2005/NĐ-CP ngày 14/12/2005 về quyền hạn, trách nhiệm của cơ quan và cán bộ chuyên trách bảo vệ an ninh quốc gia phải thực hiện các quy định sau đây:

- Yêu cầu tổ chức, cá nhân cung cấp các thông tin, dữ liệu, số liệu, tài liệu, đồ vật liên quan.
- Thực hiện theo thẩm quyền các biện pháp thu giữ, sao chép thông tin, dữ liệu, số liệu, tài liệu, đồ vật, một phần hoặc toàn bộ hệ thống thiết bị liên quan.
- Ngăn cản việc truy nhập hệ thống thiết bị, mạng lưới và sử dụng dịch vụ.
- Thực hiện các nhiệm vụ, quyền hạn khác theo quy định của pháp luật.

e) Công an các đơn vị, địa phương thực hiện nhiệm vụ chuyên trách bảo vệ an ninh quốc gia có trách nhiệm hướng dẫn nghiệp vụ cho lực lượng bảo vệ của các tổ chức quản lý, khai thác cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin trên cơ sở hợp đồng giữa hai bên.

g) Thanh toán cước thuê kênh truyền dẫn phục vụ công tác bảo đảm an ninh thông tin theo quy định.

h) Về cấp phép:

- Đối với việc cấp phép cho các doanh nghiệp chuyển phát có vốn đầu tư nước ngoài: trong thời hạn 20 ngày, kể từ ngày nhận được yêu cầu của Bộ Thông tin và Truyền thông và hồ sơ hợp lệ, cơ quan chuyên trách bảo vệ an ninh có trách nhiệm tham mưu, giúp lãnh đạo Bộ Công an thẩm định các nội dung liên quan đến việc bảo đảm an toàn cơ sở hạ tầng, an ninh thông tin trong hồ sơ xin cấp phép và trả lời Bộ Thông tin và Truyền thông bằng văn bản.

- Đối với việc cấp phép cho các tổ chức, cá nhân nước ngoài tại Việt Nam thiết lập mạng viễn thông dùng riêng, mạng Internet dùng riêng, sử dụng tần số và thiết bị phát sóng vô tuyến điện: trong thời hạn 10 ngày, kể từ ngày nhận được yêu cầu của Bộ Thông tin và Truyền thông và hồ sơ hợp lệ xin cấp phép của tổ chức, cá nhân nước ngoài, cơ quan chuyên trách bảo vệ an ninh có trách nhiệm tham mưu, giúp lãnh đạo Bộ Công an trả lời Bộ Thông tin và Truyền thông bằng văn bản. Trong trường hợp đặc biệt, đối với tổ chức, cá nhân nước ngoài tại Việt Nam được hưởng quyền ưu đãi, miễn trừ ngoại giao hoặc lãnh sự thì không quá 03 ngày làm việc, kể từ ngày nhận được yêu cầu của Bộ Ngoại giao và hồ sơ hợp lệ xin cấp phép, cơ quan chuyên trách bảo vệ an ninh có trách nhiệm tham mưu, giúp lãnh đạo Bộ Công an trả lời Bộ Ngoại giao và Bộ Thông tin và Truyền thông bằng văn bản.

- Đối với cấp phép lắp đặt cáp viễn thông trong vùng biển của Việt Nam: trong thời hạn 15 ngày, kể từ ngày nhận được yêu cầu của Bộ Thông tin và Truyền thông và hồ sơ hợp lệ của tổ chức xin cấp phép lắp đặt tuyến cáp, cơ quan chuyên trách bảo vệ an ninh có trách nhiệm tham mưu, giúp lãnh đạo Bộ Công an trả lời Bộ Thông tin và Truyền thông bằng văn bản.

- Đối với cấp phép cho tàu, thuyền hoạt động khảo sát, thi công lắp đặt, duy tu, bảo dưỡng, sửa chữa tuyến cáp trong vùng biển của Việt Nam: trong thời hạn 05 ngày làm việc, kể từ ngày nhận được yêu cầu của Bộ Thông tin và Truyền thông và hồ sơ hợp lệ của tổ chức xin phép cho tàu, thuyền hoạt động khảo sát, thi công lắp đặt, duy tu, bảo dưỡng, sửa chữa tuyến cáp, cơ quan chuyên trách bảo vệ an ninh có trách nhiệm tham mưu, giúp lãnh đạo Bộ Công an trả lời Bộ Thông tin và Truyền thông bằng văn bản.

3. Trách nhiệm của doanh nghiệp bưu chính, viễn thông và công nghệ thông tin

a) Xây dựng kế hoạch và áp dụng các biện pháp bảo đảm an toàn cơ sở hạ tầng, an ninh thông tin phù hợp với quy mô mạng lưới, dịch vụ và xu thế phát triển công nghệ trên thế giới.

b) Nghiên cứu phát triển công nghệ nhằm nâng cao độ an toàn của mạng lưới bưu chính, viễn thông; xây dựng kế hoạch dự phòng về mạng lưới, trang thiết bị để ứng phó với các tình huống khẩn cấp, các sự cố xảy ra nhằm bảo đảm an ninh thông tin và hoạt động liên tục, an toàn của mạng lưới, dịch vụ bưu chính, viễn thông và công nghệ thông tin.

c) Xây dựng, ban hành quy trình, quy chế phối hợp với lực lượng Công an, quân sự, dân quân tự vệ để bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin.

d) Cung cấp thông tin, số liệu cần thiết về công nghệ, kỹ thuật hệ thống và dự án mới đã được phê duyệt trong lĩnh vực bưu chính, viễn thông và công nghệ thông tin cho các đơn vị nghiệp vụ thuộc Bộ Công an để phục vụ công tác bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin.

đ) Đầu tư, xây lắp hệ thống thiết bị phục vụ công tác bảo đảm an ninh thông tin tại phía doanh nghiệp theo Quyết định số 70/2007/QĐ-TTg ngày 21/05/2007 của Thủ tướng Chính phủ quy định về việc đầu tư hệ thống thiết bị bảo đảm an ninh thông tin cho các mạng viễn thông tại Việt Nam.

e) Bố trí mặt bằng, điểm truy nhập mạng lưới, cổng kết nối và các điều kiện kỹ thuật cần thiết cho nhiệm vụ bảo đảm an ninh thông tin theo yêu cầu của Bộ Công an và Bộ Thông tin và Truyền thông. Bảo đảm các điều kiện thuận lợi cho cơ quan bảo vệ an ninh quốc gia tiến hành các biện pháp nghiệp vụ theo quy định của pháp luật để bảo vệ an ninh quốc gia, trật tự, an toàn xã hội.

g) Cung cấp đầy đủ kịp thời thông tin, tài liệu, số liệu, dữ liệu, đồ vật cho cơ quan chuyên trách bảo vệ an ninh quốc gia khi có yêu cầu bằng văn bản của người có thẩm quyền quy định tại Điều 4 Nghị định số 151/2005/NĐ-CP ngày 14/12/2005 về quyền hạn, trách nhiệm của cơ quan và cán bộ chuyên trách bảo vệ an ninh quốc gia.

h) Phối hợp chặt chẽ với các đơn vị nghiệp vụ của Bộ Công an và Bộ Thông tin và Truyền thông:

- Thu thập, phân tích, đánh giá, dự báo thông tin liên quan đến các sự cố mạng lưới, các điểm yếu, lỗ hổng về an toàn cơ sở hạ tầng và an ninh thông tin; đề xuất các biện pháp khắc phục, tăng cường khả năng phòng, chống sự tấn công đột nhập từ bên ngoài.

- Xử lý kịp thời các sự cố kỹ thuật làm ảnh hưởng đến khả năng kiểm soát an toàn cơ sở hạ tầng và an ninh thông tin của hệ thống thiết bị do các doanh nghiệp quản lý, khai thác.

- Triển khai các biện pháp bảo vệ an toàn cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin; phát hiện, ngăn chặn kịp thời và dừng ngay việc cung cấp, sử dụng dịch vụ đối với các trường hợp sử dụng, lợi dụng mạng lưới, dịch vụ bưu chính, viễn thông và công nghệ thông tin để hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

i) Bảo đảm bí mật của các thông tin riêng liên quan đến người sử dụng dịch vụ bưu chính, viễn thông và công nghệ thông tin theo quy định của pháp luật.

k) Tổ chức đào tạo, phát triển nguồn nhân lực về an toàn cơ sở hạ tầng và an ninh thông tin phù hợp với quy mô của mạng lưới, phạm vi hoạt động kinh doanh của doanh nghiệp. Xây dựng lực lượng bảo vệ; trang bị các phương tiện bảo vệ; thực hiện tuần tra, canh gác; kiểm tra đột xuất và định kỳ công tác bảo vệ mạng lưới bưu chính, viễn thông và công nghệ thông tin.

l) Phổ biến về mục đích, vai trò, ý nghĩa của việc bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin; hướng dẫn các tổ chức, cá nhân sử dụng mạng lưới, dịch vụ bưu chính, viễn thông và công nghệ thông tin tuân thủ quy định về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin.

IV. KIỂM TRA, THANH TRA VÀ XỬ LÝ VI PHẠM

1. Các đơn vị chức năng thuộc Bộ Thông tin và Truyền thông, Bộ Công an phối hợp thường xuyên hoặc đột xuất kiểm tra, thanh tra về an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin. Doanh nghiệp bưu chính, viễn thông và công nghệ thông tin và tổ chức, cá nhân liên quan phải tạo mọi điều kiện thuận lợi cho các cơ quan nhà nước có thẩm quyền khi thực hiện việc kiểm tra, thanh tra.

2. Tổ chức, cá nhân có hành vi vi phạm các quy định về an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin thì tùy theo tính chất, mức độ vi phạm mà bị xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

V. TỔ CHỨC THỰC HIỆN

1. Bộ Thông tin và Truyền thông, Bộ Công an trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình hướng dẫn tổ chức, cá nhân thực hiện các biện pháp bảo đảm an toàn cơ sở hạ tầng, an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin.

2. Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương chỉ đạo các Sở Thông tin và Truyền thông, Công an các tỉnh, thành phố trực thuộc Trung ương, các doanh nghiệp bưu chính,

viễn thông và công nghệ thông tin hoạt động trên địa bàn quản lý thực hiện nghiêm túc các quy định trong thông tư này.

3. Định kỳ sáu tháng một lần các Sở Thông tin và Truyền thông và Công an các tỉnh, thành phố tập hợp tình hình an toàn mạng lưới và an ninh thông tin trong lĩnh vực bưu chính, viễn thông và công nghệ thông tin báo cáo Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương và đề xuất phương hướng triển khai.

4. Định kỳ hàng năm, doanh nghiệp bưu chính, viễn thông và công nghệ thông tin tiến hành sơ kết đánh giá, đề xuất, kiến nghị, khen thưởng về công tác bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin với các cơ quan quản lý nhà nước, báo cáo Bộ Thông tin và Truyền thông, Bộ Công an.

5. Thông tư này có hiệu lực thi hành sau 15 ngày, kể từ ngày đăng Công báo và thay thế Thông tư liên tịch số 01/2001/TTLT-TCBĐ-BCA ngày 7/6/2001 của Tổng cục Bưu điện và Bộ Công an hướng dẫn việc bảo đảm an toàn mạng lưới và an ninh thông tin trong hoạt động bưu chính, viễn thông.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc nảy sinh các tổ chức, cá nhân phản ánh về Bộ Thông tin và Truyền thông, Bộ Công an để được hướng dẫn kịp thời./.

KT. BỘ TRƯỞNG
BỘ CÔNG AN
THỨ TRƯỞNG
Thượng tướng Nguyễn Văn Hưởng

KT. BỘ TRƯỞNG
BỘ THÔNG TIN VÀ TRUYỀN THÔNG
THỨ TRƯỞNG
Lê Nam Thắng

Nơi nhận:

- Thủ tướng và các Phó Thủ tướng Chính phủ;
- Văn phòng Chính phủ;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Viện kiểm sát nhân dân tối cao;
- Tòa án nhân dân tối cao;
- Cục Kiểm tra văn bản (Bộ Tư pháp);
- Các doanh nghiệp bưu chính, viễn thông và công nghệ thông tin;
- Công báo;
- Lưu các Bộ: TTTT, CA.