ỦY BAN NHÂN DÂN TỈNH NINH BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số 47 /KH-UBND	*Ninh Bình, ngày 01 tháng 8 năm 2014*

(Chỉ đạo thực hiện)
Fotogửi: Đ/c Sơn PGĐ
P. Viễn thông
P. CNTT
giám đốc

KẾ HOẠCH
thực hiện Chỉ thị số 15/CT-TTg của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới

Thực hiện Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về việc tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới, UBND tỉnh ban hành kế hoạch triển khai thực hiện trên địa bàn tỉnh như sau:

I. Mục đích, yêu cầu

1. Quán triệt sâu sắc nội dung Chỉ thị số 15/CT-TTg nhằm nâng cao nhận thức cho cán bộ, đảng viên và nhân dân, nhất là cán bộ lãnh đạo, quản lý, cán bộ công tác ở các bộ phận quan trọng, cơ mật về nhiệm vụ bảo đảm an ninh, an toàn thông tin mạng trong tình hình mới; nâng cao ý thức cảnh giác trước âm mưu nguy hiểm, thâm độc và hoạt động chống phá của các thế lực thù địch, phản động, tội phạm trên mạng; nêu cao tinh thần trách nhiệm, thực hiện tốt nhiệm vụ bảo đảm an ninh, an toàn thông tin mạng trong lĩnh vực được giao.

2. Phát hiện kịp thời những sơ hở, thiếu sót trong quản lý thông tin nội bộ, bí mật nhà nước; những lỗ hổng, điểm yếu của hệ thống thông tin để có biện pháp khắc phục. Ngăn chặn triệt để việc lấy cắp thông tin, bí mật nhà nước; không để các thế lực thù địch, phản động và bọn tội phạm lợi dụng để chống phá Đảng, Nhà nước ta.

3. Công tác bảo đảm an ninh, an toàn thông tin mạng trong tình hình mới lấy tư tưởng chủ động phòng ngừa là chính; phối hợp đồng bộ giữa các lực lượng trong phòng ngừa, phát hiện và đấu tranh, góp phần củng cố và giữ vững sự ổn định chính trị, phục vụ đắc lực phát triển kinh tế, văn hoá, xã hội của tỉnh.

II. Nội dung

1. Tiếp tục quán triệt, thực hiện nghiêm Chỉ thị số 28-CT/TW ngày 16 tháng 9 năm 2013 của Ban Bí thư về "Tăng cường công tác bảo đảm an toàn thông tin mạng", trong đó xác định rõ công tác bảo đảm an ninh và an toàn thông tin mạng là trách nhiệm của các cấp, các ngành và mọi công dân; chú trọng giải pháp tuyên truyền, giáo dục chính trị, tư tưởng, bồi dưỡng kiến thức về an ninh và an toàn thông tin mạng cho cán bộ, đảng viên và nhân dân, nhất là những người công tác ở các bộ phận trọng yếu, cơ mật, để nâng cao tinh thần cảnh giác trước âm mưu, hoạt động chống phá của các thế lực thù địch, phản động, tội phạm mạng.

2. Chủ động triển khai các giải pháp bảo đảm an ninh và an toàn thông tin mạng. Khắc phục ngay những sơ hở, thiếu sót trong quản lý, sử dụng các dịch vụ viễn thông, internet; không để các thế lực thù địch, phản động, tội phạm mạng lợi dụng gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội. Các đơn vị, địa phương, doanh nghiệp nhà nước khi phát hiện có dấu hiệu hoạt động tấn công mạng vào các mục tiêu quan trọng, địa bàn chiến lược, bộ phận chứa thông tin, tài liệu bí mật nhà nước, đặc biệt là hạ tầng mạng trọng yếu quốc gia, phải báo cáo ngay Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và Sở Thông tin và Truyền thông để được hướng dẫn, phối hợp trong việc khắc phục, ngăn chặn.

3. Khẩn trương xây dựng và hoàn thiện quy chế quản lý chặt chẽ các thiết bị, phương tiện có tính năng lưu trữ thông tin nội bộ, bí mật nhà nước để phòng ngừa lộ, lọt thông tin qua mạng. Nghiêm cấm lưu trữ, trao đổi, xử lý, hiển thị thông tin, tài liệu có nội dung bí mật nhà nước, bí mật nội bộ trên mạng viễn thông, internet không có biện pháp bảo mật theo quy định; kết nối máy tính, thiết bị điện tử có chứa thông tin bí mật nhà nước, bí mật nội bộ vào mạng internet; sử dụng hòm thư điện tử không có biện pháp bảo mật theo quy định của pháp luật về cơ yếu để trao đổi thông tin bí mật nhà nước, bí mật nội bộ. Trường hợp cần thiết trao đổi thông tin bí mật nhà nước qua điện thoại và các thiết bị, phương tiện có kết nối mạng internet phải chấp hành nghiêm các quy định của pháp luật về cơ yếu, Pháp lệnh Bảo vệ Bí mật nhà nước cũng như các quy định liên quan.

Ban hành quy định để kiểm soát chặt chẽ việc mang các thiết bị điện tử có tính năng thu âm, ghi hình vào các cuộc họp có nội dung bí mật nhà nước, bí mật nội bộ. Không mang thiết bị chứa bí mật nhà nước, bí mật nội bộ và thông tin nhạy cảm khi đi nước ngoài; trường hợp cần thiết phải được cấp có thẩm quyền đồng ý và phải áp dụng các biện pháp mã hóa, bảo quản an toàn theo hướng dẫn của cơ quan có thẩm quyền.

4. Tăng cường công tác quản lý nhà nước đối với các loại hình dịch vụ viễn thông, internet, nhất là các trang thông tin điện tử và dịch vụ điện thoại di động trả trước. Tăng cường quản lý, kiểm soát chặt chẽ hoạt động kinh doanh dịch vụ, thiết bị có thể ảnh hưởng đến an ninh và an toàn thông tin mạng, đặc biệt hoạt động sản xuất, mua bán, nhập khẩu, xuất khẩu, vận chuyển, tàng trữ, cung cấp dịch vụ, sử dụng các thiết bị, phần mềm định vị, chế áp thông tin di động, chuyên dùng trộm cắp thông tin, gián điệp thông tin. Kịp thời xử lý theo pháp luật các hành vi cố ý vi phạm quy định của Nhà nước về quản lý, cung cấp, sử dụng các thiết bị làm mất an ninh và an toàn thông tin mạng.

Tổ chức kiểm tra an ninh, an toàn các thiết bị, phần mềm hệ thống, phần mềm ứng dụng trước khi đưa vào sử dụng tại các bộ phận quan trọng, cơ mật, nơi chứa đựng bí mật nhà nước, bí mật nội bộ thuộc các cơ quan, doanh nghiệp nhà nước. Các thiết bị, phần mềm do tổ chức, cá nhân nước ngoài tài trợ, tặng phải được kiểm định an toàn trước khi sử dụng. Trong trường hợp sử dụng cho

các bộ phận quan trọng, cơ mật, nơi chứa đựng bí mật nhà nước thì phải được cơ quan an ninh có thẩm quyền kiểm tra và đồng ý cho đưa vào sử dụng.

5. Xây dựng đội ngũ cán bộ kỹ thuật có trình độ chuyên môn phù hợp để quản lý, vận hành, bảo đảm an ninh và an toàn thông tin cho hệ thống thông tin và mạng của cơ quan, đơn vị, địa phương. Xử lý nghiêm mọi hành vi làm mất an ninh và an toàn thông tin mạng, làm lộ, lọt bí mật nhà nước, thông tin nội bộ qua mạng hoặc lợi dụng để vi phạm pháp luật, gây mất đoàn kết nội bộ.

6. Quan tâm đầu tư cơ sở hạ tầng, kỹ thuật; tăng cường xây dựng hệ thống và năng lực bảo đảm an ninh và an toàn thông tin trên mạng để chủ động phòng thủ mạng vững chắc. Giám sát, phát hiện sớm tấn công mạng; ngăn chặn các hoạt động xâm nhập, phá hoại, lấy thông tin tình báo trên mạng; ứng cứu khắc phục sự cố kịp thời. Chủ động nghiên cứu, xây dựng các giải pháp, từng bước hiện đại hóa các phương tiện, thiết bị, phần mềm bảo đảm an ninh và an toàn thông tin mạng; ban hành quy định đặc thù về việc đầu tư mua sắm thiết bị, thiết lập các mạng dùng riêng và mạng nội bộ phục vụ các cơ quan Đảng, Nhà nước, an ninh, quốc phòng.

III. Tổ chức thực hiện

1. Công an tỉnh

- Chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh và Sở Thông tin và Truyền thông tổ chức kiểm tra, đánh giá thực trạng an ninh thông tin mạng ở các sở, ban, ngành, địa phương và doanh nghiệp nhà nước trên địa bàn tỉnh; hướng dẫn các sở, ban, ngành, địa phương; các doanh nghiệp nhà nước ban hành quy chế và thực hiện các giải pháp bảo đảm an ninh thông tin mạng; phối hợp với Sở Thông tin và Truyền thông, các đơn vị nghiệp vụ, Bộ Công an và các đơn vị có liên quan chủ động phát hiện, đấu tranh, ngăn chặn tội phạm mạng trên địa bàn tỉnh.

- Chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông và các cơ quan liên quan, doanh nghiệp viễn thông, internet xây dựng, triển khai các biện pháp đấu tranh có hiệu quả với hoạt động của các thế lực thù địch, phản động, tội phạm mạng lợi dụng dịch vụ viễn thông, internet để xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông kiểm định an toàn thiết bị điện tử, tin học trước khi đưa vào sử dụng tại các bộ phận quan trọng, cơ mật, nơi chứa đựng bí mật nhà nước, bí mật nội bộ thuộc các sở, ban, ngành, địa phương. Phối hợp, hướng dẫn kiểm tra an ninh, an toàn các thiết bị do tổ chức, cá nhân nước ngoài tài trợ, tặng trước khi đưa vào sử dụng tại các cơ quan, doanh nghiệp nhà nước.

2. Bộ Chỉ huy Quân sự tỉnh

Phối hợp với Công an tỉnh và Sở Thông tin và Truyền thông tham gia giám sát, bảo vệ hạ tầng mạng trọng yếu quốc gia; thực hiện nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng; bảo đảm an toàn thông tin cho hệ

thống tự động hóa chỉ huy bảo đảm sẵn sàng chiến đấu theo chỉ đạo, hướng dẫn của Bộ Quốc phòng. Phối hợp với các cơ quan liên quan triển khai hệ thống bảo mật, an toàn thông tin dùng mật mã; thực hiện công tác quản lý, sử dụng mật mã bảo đảm an toàn thông tin mạng theo quy định; thực hiện các nhiệm vụ khác về bảo đảm an toàn thông tin theo quy định của Chính phủ.

3. Sở Thông tin và Truyền thông

- Chỉ đạo thực hiện quyết liệt, đồng bộ các giải pháp quản lý các loại hình dịch vụ viễn thông, internet và các dịch vụ cung cấp nội dung thông tin điện tử trên mạng (các website, blog, mạng xã hội...), thuê bao di động trả trước; thuê bao sử dụng dịch vụ vô tuyến băng rộng (3G, 4G...) để kịp thời chặn lọc hiệu quả các thông tin xấu trên mạng, ngăn chặn "tin nhắn rác", phát hiện và xử lý nghiêm các tổ chức, cá nhân vi phạm. Hướng dẫn biện pháp kỹ thuật cần thiết cho các cơ quan, doanh nghiệp cung cấp dịch vụ nội dung thông tin trên mạng, thiết bị di động đầu cuối để thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng. Kiểm soát chặt chẽ và kịp thời xử lý theo pháp luật các trang thông tin điện tử đăng ký trên địa bàn tỉnh đăng tải thông tin phản động, vi phạm pháp luật.

- Chủ trì, phối hợp với Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và các sở, ban, ngành liên quan chủ động rà soát, sửa đổi, bổ sung và ban hành các văn bản quy định trong lĩnh vực bảo đảm an toàn thông tin mạng. Chủ trì, hướng dẫn và phối hợp với các sở, ban, ngành, địa phương và doanh nghiệp đẩy mạnh các hoạt động bảo đảm an toàn mạng viễn thông, internet. Kiểm tra, đánh giá hiện trạng bảo đảm an toàn thông tin mạng; thực hiện cảnh báo, điều phối ứng cứu và khắc phục sự cố mạng.

4. Các sở, ban, ngành, UBND các huyện, thành phố, thị xã và các doanh nghiệp nhà nước

- Khẩn trương chỉ đạo thực hiện các giải pháp bảo đảm an ninh và an toàn thông tin mạng phù hợp điều kiện của đơn vị, địa phương mình. Xây dựng, triển khai các quy định, kế hoạch bảo đảm an ninh và an toàn mạng để chủ động phòng ngừa, lộ lọt thông tin trên không gian mạng.

- Tăng cường công tác lãnh đạo, quản lý, nhân lực, đầu tư, trang thiết bị kỹ thuật bảo vệ an ninh và an toàn hệ thống mạng. Thực hiện công tác bảo đảm an ninh và an toàn thông tin mạng theo hướng dẫn nghiệp vụ của Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và Sở Thông tin và Truyền thông.

Yêu cầu thủ trưởng các sở, ban, ngành, cơ quan, doanh nghiệp nhà nước và Chủ tịch UBND các huyện, thành phố, thị xã có trách nhiệm triển khai tổ chức thực hiện nghiêm túc Kế hoạch này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc báo cáo về UBND tỉnh (qua Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và Sở Thông tin và Truyền thông) để được chỉ đạo, hướng dẫn kịp thời.

Giao Công an tỉnh chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông hướng dẫn, kiểm tra, đôn đốc việc thực hiện Kế hoạch này; hàng tháng, hàng quý báo cáo kết quả thực hiện về Bộ Công an và Ủy ban nhân dân tỉnh./.

Nơi nhận:
- Văn phòng Chính phủ;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành, đoàn thể;
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH&HĐND tỉnh;
- UBND các huyện, thành phố, thị xã;
- Các cơ quan Trung ương, doanh nghiệp nhà nước trên địa bàn;
- Chánh, Phó Chánh Văn phòng UBND tỉnh;
- Lưu: VT, VP3,VP6,VP7, TTTH.

PH.03/KHCA

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Bùi Văn Thắng