| ỦY BAN NHÂN DÂN<br>TỈNH GIA LAI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 537 /QĐ-UBND | *Gia Lai, ngày 17 tháng 9 năm 2014* |

# QUYẾT ĐỊNH

**Ban hành Kế hoạch Bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai trong tình hình mới**



## ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức Hội đồng nhân dân và Uỷ ban nhân dân năm 2003;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006 của Quốc hội Nước Cộng hòa xã hội chủ nghĩa Việt Nam;

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

Căn cứ Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Căn cứ Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông,

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Kế hoạch Bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai trong tình hình mới.

**Điều 2.** Giao Sở Thông tin và Truyền thông và các Sở, ban, ngành, UBND các huyện, thị xã, thành phố căn cứ vào Kế hoạch này để tổ chức thực hiện đúng quy trình và thời gian quy định.

**Điều 3.** Quyết định này có hiệu lực thi hành kể từ ngày ký

Chánh Văn phòng UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các Sở, ban, ngành, Chủ tịch UBND các huyện, thị xã, thành phố và các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***
- Văn phòng Chính phủ (b/c);
- Bộ TT&TT (b/c);
- Thường trực Tỉnh ủy (b/c);
- Thường trực HĐND tỉnh (b/c);
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Ban Chỉ đạo Ứng dụng CNTT của tỉnh;
- Các Sở, ban, ngành thuộc tỉnh (để thực hiện);
- UBND các huyện, thị xã, thành phố (để thực hiện);
- Chánh VP, các PVP UBND tỉnh;
- Lưu: VT, KTTH, NC, VHXH.

**TM. ỦY BAN NHÂN DÂN**
**KT.CHỦ TỊCH**
**PHÓ CHỦ TỊCH**

**Hoàng Công Lự**

ỦY BAN NHÂN DÂN
TỈNH GIA LAI

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

# KẾ HOẠCH

**Bảo đảm an toàn thông tin mạng**
**trên địa bàn tỉnh Gia Lai trong tình hình mới**

*(Ban hành kèm theo Quyết định số: 537 /QĐ-UBND ngày 16/9 /2014 của UBND tỉnh Gia Lai)*

## I. CĂN CỨ LẬP KẾ HOẠCH

- Luật Công nghệ thông tin (CNTT);

- Luật Giao dịch điện tử;

- Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước;

- Quyết định số 1605/QĐ-TTg ngày 27/8/2010 của Thủ tướng Chính phủ phê duyệt ,Chương trình quốc gia về ứng dụng CNTT trong hoạt động của cơ quan nhà nước giai đoạn 2011-2015;

- Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

- Chỉ thị số 897/CT-TTg ngày 10/06/2011 của Thủ tướng CP về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

- Quyết định số 201/QĐ-UBND ngày 25/3/2011 của UBND tỉnh Gia Lai về việc Ban hành Kế hoạch ứng dụng công nghệ thông tin trong hoạt động các cơ quan Nhà nước trên địa bàn tỉnh Gia Lai giai đoạn 2011-2015;

- Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư Trung ương Đảng về việc tăng cường công tác bảo đảm an toàn thông tin mạng;

- Thông tri số 17-TT/TU ngày 04/11/2013 của Ban thường vụ Tỉnh ủy Gia Lai về công tác đảm bảo an toàn thông tin mạng;

- Công văn số 4277/UBND-VHXH ngày 06/12/2013 của UBND tỉnh Gia Lai về việc tăng cường công tác bảo đảm an toàn thông tin mạng;

- Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới;

- Quyết định số 99/QĐ-TTg ngày 14/01/2014 của Thủ tướng Chính phủ về việc Phê duyệt Đề án "Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020";

- Thông tư số 06/2008/TTLT-BTTTT-BCA ngày 28/11/2008 của Bộ Thông tin và Truyền thông, Bộ Công an 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.

## II. HIỆN TRẠNG ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG TRONG HOẠT ĐỘNG CỦA CƠ QUAN NHÀ NƯỚC TRÊN ĐỊA BÀN TỈNH

### 1. Môi trường chính sách:

UBND tỉnh đã ban hành các văn bản:

- Quyết định số 201/QĐ-UBND ngày 25/3/2011 của UBND tỉnh về việc Ban hành Kế hoạch ứng dụng CNTT trong hoạt động các cơ quan nhà nước trên địa bàn tỉnh Gia Lai giai đoạn 2011-2015, trong đó có nội dung xây dựng hệ thống bảo mật cho cơ quan, đơn vị nhà nước cấp tỉnh;

- Quyết định số 175/QĐ-UBND ngày 16/4/2013 của UBND tỉnh Gia Lai về việc phê duyệt kế hoạch và phân bổ kinh phí đào tạo, bồi dưỡng cán bộ, công chức, viên chức (CBCCVC) của tỉnh năm 2013;

- Công văn số 4277/UBND-VHXH ngày 06/12/2013 của UBND tỉnh "V/v bảo đảm an toàn thông tin mạng";

- Công văn số 1739/UBND-VHXH ngày 19/5/2014 của UBND tỉnh "V/v tăng cường công tác an ninh mạng";

Ngoài ra, UBND tỉnh cũng đã ban hành nhiều văn bản chỉ đạo các cơ quan, đơn vị về lĩnh vực CNTT trong đó lưu ý chú trọng công tác bảo đảm an toàn thông tin (ATTT).

### 2. Hạ tầng kỹ thuật:

Hiện nay, các sở, ban, ngành, UBND các huyện, thị xã, thành phố đều đã được trang bị mạng nội bộ (LAN) có kết nối Internet; tỉnh đã xây dựng Trung tâm tích hợp dữ liệu; các hệ thống thông tin của tỉnh: Cổng thông tin điện tử, hệ thống thư điện tử công vụ, hệ thống Hội nghị truyền hình. Tại mỗi cơ quan hành chính cấp tỉnh, cấp huyện đã được đầu tư trang bị: Hệ thống Quản lý văn bản và điều hành; trang thông tin điện tử; đầu tư mô hình Một cửa điện tử tại mỗi đơn vị... Hầu hết cán bộ, công chức đã được trang bị máy tính để làm việc. Vì vậy, công tác an toàn, an ninh thông tin tại các cơ quan hành chính nhà nước đã được quan tâm đầu tư:

Năm 2011, UBND các huyện, thị xã, thành phố, các sở, ban, ngành đã được trang bị phần mềm Kaspersky Endpoint Security 8 có bản quyền phòng chống virus. Riêng UBND các huyện, thị xã, thành phố đã được đầu tư thiết bị tường lửa.

Trung tâm tích hợp dữ liệu (hệ thống Hosting) của tỉnh là hệ thống quan trọng cần được đảm bảo ATTT và đã được đầu tư thêm hệ thống bảo mật vào năm 2012. Năm 2013, hệ thống Hosting đã được tổ chức đánh giá an toàn an ninh thông tin nhằm đảm bảo an toàn dữ liệu.

Tuy nhiên, trong quá trình vận hành đã bộc lộ những khó khăn bất cập sau đây:

- Hạ tầng CNTT của các cơ quan, đơn vị đã được trang bị nhưng chưa đồng bộ, do đó việc xây dựng hệ thống bảo mật cho các đơn vị còn rất khó khăn, chưa phát huy hết hiệu quả;

- Một số đơn vị không sử dụng thiết bị tường lửa đã được trang bị để chống xâm nhập (do quan niệm rằng thiết bị này làm hệ thống chạy chậm).

- Hầu hết máy tính trang bị cho CBCCVC sử dụng đã nhiều năm, cấu hình thấp và xuống cấp dẫn đến khó khăn trong việc cài đặt phần mềm phòng, chống virus, mã độc. Ngoài ra, đến nay phần mềm đã hết hạn bản quyền nhưng các cơ quan, đơn vị chưa chủ động bố trí kinh phí để trang bị lại.

Trong thời gian qua, tuy đã có những truy cập trái phép bên ngoài vào hệ thống Hosting tỉnh, chủ yếu tập trung vào các cổng/trang thông tin điện tử, nhưng hệ thống bảo mật ATTT đã được trang bị cơ bản và đội ngũ quản trị đề cao cảnh giác nên đã ngăn chặn hoặc khắc phục kịp thời những cuộc tấn công, không để xảy ra sự cố.

Trước tình hình an ninh mạng ngày càng phức tạp như hiện nay, để ngăn chặn các cuộc truy cập trái phép vào các cổng/trang thông tin điện tử, hệ thống thư điện tử nhằm chiếm quyền kiểm soát, đánh cắp dữ liệu, thay đổi thông tin, phát tán mã độc thì việc tiếp tục đầu tư tăng cường đảm bảo ATTT mạng là vấn đề cấp thiết, cần phải được quan tâm đúng mức.

**3. Hiện trạng về nguồn nhân lực bảo đảm ATTT mạng:**

Trong nhiều năm qua, tỉnh đã triển khai các lớp đào tạo, bồi dưỡng kiến thức CNTT cho đội ngũ CBCCVC để đáp ứng ngày càng tốt hơn yêu cầu công tác. Năm 2013, đã tổ chức 02 lớp chuyên đề "An toàn, bảo mật hệ thống thông tin"(theo Quyết định số 175/QĐ-UBND); phối hợp với Bộ Thông tin và Truyền thông tổ chức lớp "Đào tạo kỹ thuật về ứng dụng công nghệ thông tin - quản trị hệ thống (MCITP - SA)"; Tuy vậy, hiện nay cán bộ chuyên trách về CNTT còn thiếu và yếu về trình độ, chưa đáp ứng tốt cho yêu cầu đảm bảo ATTT mạng.

Nhằm từng bước xây dựng chính quyền điện tử, việc tăng cường công tác đào tạo, bồi dưỡng nâng cao kiến thức CNTT cho CBCCVC, xây dựng nguồn nhân lực CNTT có trình độ cao cho tỉnh, trong đó có quan tâm đến chuyên đề "An toàn, bảo mật hệ thống thông tin" là việc làm thường xuyên hàng năm và phải được đầu tư đúng mức.

**4. Đánh giá chung:**

Trong thời gian qua, mặc dù Gia Lai là một tỉnh nghèo, kinh phí đầu tư hạ tầng kỹ thuật CNTT vẫn còn hạn hẹp, nhưng tỉnh cũng đã quan tâm đầu tư xây dựng chính quyền điện tử, đảm bảo ATTT mạng, bước đầu đã thu được những kết quả tốt, chưa có sự cố lớn nào về mất an toàn, an ninh thông tin xảy ra.

Trong tình hình tội phạm công nghệ cao ngày càng có biểu hiện phát triển phức tạp và tinh vi hơn, yêu cầu đặt ra là phải có kế hoạch chặt chẽ hơn để bảo đảm ATTT

mạng, đáp ứng tốc độ phát triển ứng dụng CNTT phục vụ cho công cuộc cải cách hành chính hiện nay.

## III. MỤC TIÊU

### 1. Mục tiêu tổng quát:

- Bảo đảm các hệ thống thông tin trọng yếu của tỉnh, đặc biệt là Trung tâm tích hợp dữ liệu của tỉnh cần đảm bảo tuyệt đối an toàn thông tin bằng các hệ thống bảo mật chuyên dùng;

- Bảo đảm các dịch vụ công trực tuyến cũng như các phần mềm dùng chung, cơ sở dữ liệu dùng chung đều được trang bị giải pháp, kỹ thuật nhằm đảm bảo ATTT;

- Tăng cường nhân lực CNTT của tỉnh được đào tạo về ATTT cơ bản đáp ứng được yêu cầu trong thời điểm hiện nay;

- Nâng cao nhận thức của cán bộ, công chức, viên chức (CBCCVC), người dân và doanh nghiệp về lợi ích trong ứng dụng CNTT và tầm quan trọng của việc bảo đảm ATTT;

- Tạo lập môi trường pháp lý về ATTT tại tỉnh theo các quy định của Chính phủ, Bộ TT&TT, trong đó có những quy định cụ thể về ATTT; quy định trách nhiệm cá nhân, tổ chức trong việc thực hiện nhiệm vụ đảm bảo ATTT; xử lý vi phạm các quy định về ATTT; trấn áp tội phạm xâm phạm ATTT;

- Tăng cường công tác quản lý nhà nước đối với lĩnh vực thông tin và truyền thông.

### 2. Mục tiêu cụ thể:

#### a) Bảo đảm an toàn an ninh thông tin cho cơ sở hạ tầng thông tin của tỉnh:

- Các mạng nội bộ và các thiết bị đầu cuối trong các cơ quan nhà nước được thiết kế giải pháp đồng bộ và được trang bị các giải pháp kỹ thuật cần thiết và vận hành theo các quy chế, quy trình tiêu chuẩn hóa để đảm bảo ATTT nhằm tránh bị đánh cắp thông tin nội bộ của các đơn vị;

- Hệ thống Hosting của tỉnh được trang bị các giải pháp, kỹ thuật cần thiết nhằm đảm bảo ATTT theo tiêu chuẩn quy định;

- Tăng cường khả năng bảo mật của hệ thống thông tin của tỉnh, tạo nên một môi trường thông tin an toàn cho việc triển khai, ứng dụng các hệ thống thông tin phục vụ hoạt động của các cơ quan hành chính nhà nước của tỉnh;

- Bảo đảm cơ sở hạ tầng bưu chính, viễn thông hoạt động liên tục và an toàn phục vụ sự chỉ đạo điều hành các cơ quan Đảng, Nhà nước, chính quyền địa phương các cấp và lực lượng vũ trang trên địa bàn tỉnh; đáp ứng tối đa các nhu cầu thông tin liên lạc cho người dân;đối phó kịp thời với các tình huống thiên tai, địch hoạ.

- Tuyên truyền, phổ biến, hướng dẫn việc thực hiện các quy định của Nhà nước về công tác bảo đảm an toàn an ninh thông tin mạng cho các cơ quan Đảng, Nhà nước

và các đoàn thể trên địa bàn tỉnh để tạo sự đồng thuận, cảnh giác cao trong các cơ quan, đơn vị và cộng đồng xã hội.

**b) Về đảm bảo ATTT cho các hệ thống cung cấp thông tin công cộng và dịch vụ công trực tuyến:**

- Các hệ thống thông tin điện tử của các cơ quan nhà nước trên địa bàn tỉnh được kiểm tra hàng năm về mức độ đảm bảo ATTT theo các tiêu chuẩn do nhà nước quy định;

- 100% trang thông tin điện tử của các cơ quan nhà nước có giải pháp chống lại các tấn công gây mất ATTT và có phương án dự phòng khắc phục sự cố đảm bảo hoạt động liên tục ở mức tối đa; các dịch vụ công trực tuyến phải đảm bảo được sự tin cậy cho các tổ chức, công dân khi sử dụng, tránh bị mất cắp thông tin cá nhân người sử dụng;

- Các nhà cung cấp dịch vụ truyền số liệu và viễn thông có cam kết bảo đảm an toàn dữ liệu trên đường truyền với chuẩn chất lượng công bố công khai cho các đối tượng sử dụng dịch vụ của mình;

- Các nhà cung cấp dịch vụ truy cập Internet và các đại lý phải quản lý được việc truy cập sử dụng Internet theo quy định của pháp luật;

- Các văn bản có nội dung mật không được truyền trên mạng mà phải được quản lý theo chế độ mật theo quy định pháp luật hiện hành. Tuyên truyền đảm bảo các điều kiện về hạ tầng kỹ thuật, bảo mật và an ninh thông tin.

**c) Nâng cao nhận thức xã hội và phát triển nhân lực về ATTT:**

- Bồi dưỡng, cập nhật kiến thức mới về công tác bảo đảm ATTT cho CBCCVC hoạt động trong lĩnh vực thông tin và truyền thông, đặc biệt là những người công tác ở các bộ phận quan trọng, cơ mật;

- Tăng cường phổ biến, quán triệt thực hiện nghiêm túc Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư Trung ương Đảng về tăng cường công tác bảo đảm an toàn thông tin mạng, để 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.

**d) Về môi trường pháp lý ATTT:**

- Tạo môi trường pháp lý về lĩnh vực ATTT theo hướng dẫn của Trung ương nhằm bảo vệ cơ sở hạ tầng thông tin, duy trì hoạt động ổn định, giảm thiệt hại do sự cố về ATTT;

- Thực hiện công tác đánh giá tình hình ứng dụng và phát triển CNTT của các sở, ban, ngành; UBND các huyện, thị xã, thành phố để xây dựng các văn bản quy phạm pháp luật về lĩnh vực CNTT nói chung và công tác bảo đảm ATTT nói riêng, sâu sát với tình hình phát triển của tỉnh;

- Chỉ đạo, hướng dẫn các doanh nghiệp bưu chính, viễn thông thực hiện nghiêm các quy định của pháp luật về an toàn cơ sở hạ tầng; thanh tra, kiểm tra, xử lý vi phạm về bảo đảm an toàn cơ sở hạ tầng trong hoạt động bưu chính, viễn thông;

- Tăng cường công tác quản lý về bưu chính, viễn thông; có biện pháp phòng, chống việc lợi dụng dịch vụ viễn thông để lừa đảo, đe dọa, quấy rối, phát tán tin nhắn rác...;

- Các hoạt động trên mạng phải bảo đảm tuân thủ đúng các quy định của pháp luật và được thực hiện thường xuyên, liên tục và hiệu quả trên cơ sở bảo đảm tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin và quy định pháp luật về chất lượng dịch vụ viễn thông, Internet.

## IV. NỘI DUNG

### 1. Chính sách:

- Triển khai cụ thể các chính sách, giải pháp chung theo hướng dẫn của Chính phủ, bộ ngành có liên quan tại địa phương trong lĩnh vực an toàn, an ninh thông tin;

- Xây dựng quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan quản lý hành chính nhà nước thuộc tỉnh;

- Tổ chức tuyên truyền bằng nhiều hình thức cho công chức, viên chức, lực lượng vũ trang và nhân dân hiểu rõ trách nhiệm của mình trong việc bảo đảm an toàn an ninh thông tin.

- Có các văn bản chỉ đạo, quy định chặt chẽ hơn về quản lý dịch vụ internet, thuê bao di động trả trước, thuê bao sử dụng dịch vụ vô tuyến băng rộng để kịp thời ngăn chặn và xử lý phát tán thông tin phản động, không lành mạnh lên mạng Internet, các tin nhắn rác, tin nhắn lừa đảo, điện thoại lừa đảo theo đúng quy định của pháp luật;

- Tổ chức tuyên truyền rộng rãi đến mọi người dân thông qua các phương tiện thông tin đại chúng; Cổng thông tin điện tử tỉnh và trang thông tin điện tử của các Sở, ban, ngành, huyện, thị xã, thành phố về công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới; phát động phong trào toàn dân bảo vệ hệ thống hạ tầng bưu chính, viễn thông và CNTT trên địa bàn tỉnh;

### 2. Hạ tầng kỹ thuật an toàn thông tin:

- Triển khai kiện toàn hệ thống mạng nội bộ tại các cơ quan nhà nước trên địa bàn tỉnh theo mô hình thống nhất và bảo đảm ATTT;

- Triển khai ứng dụng chữ ký số tại nội bộ các cơ quan hành chính nhà nước trên địa bàn tỉnh;

- Chỉ đạo các doanh nghiệp bảo vệ cơ sở hạ tầng bưu chính, viễn thông 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; triển khai các giải pháp và chuẩn bị sẵn sàng hệ thống thiết bị dự phòng để bảo đảm cơ sở hạ tầng bưu chính, viễn thông hoạt động liên tục và an toàn phục vụ sự chỉ đạo điều hành các cơ quan Đảng, Nhà nước, chính quyền địa phương các cấp và lực lượng vũ trang trên địa bàn tỉnh; đáp ứng tối đa các nhu cầu thông tin liên lạc cho người dân;

- Tăng cường công tác kiểm tra việc tổ chức thực hiện các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn cơ sở hạ tầng bưu chính, viễn thông và công nghệ thông tin.

**3. Ứng dụng CNTT trong hoạt động cơ quan nhà nước:**

- Xây dựng giải pháp ATTT đa lớp, bảo vệ các hệ thống thông tin, ngăn chặn các xâm nhập trái phép từ bên ngoài (Internet, hệ thống mạng WAN...) nhằm phá hoại hoặc đánh cắp dữ liệu;

- Sử dụng hệ thống thư điện tử công vụ của tỉnh chỉ để thực hiện việc gửi, nhận các văn bản tài liệu trao đổi phục vụ công việc, tài liệu phục vụ cuộc họp, các báo cáo, dự thảo văn bản của cơ quan;

- Giảm thiểu các tác động rủi ro do virus máy tính gây ra, tạo nên một môi trường thông tin an toàn cho việc triển khai, ứng dụng các hệ thống thông tin phục vụ hoạt động của cơ quan hành chính nhà nước, đồng thời việc đầu tư sử dụng phần mềm chống virus có bản quyền cũng là một cách để tăng cường hiệu lực thực thi Luật Sở hữu trí tuệ;

- Triển khai kiểm tra, rà soát các Cổng thông tin điện tử, trang thông tin điện tử của tất cả các Sở, ban, ngành, UBND các huyện, thị xã, thành phố.

- Nâng cấp, bảo trì thường xuyên đảm bảo công tác an ninh thông tin cho các hạ tầng kỹ thuật CNTT và phần mềm dùng chung, đặc biệt là các hệ thống thông tin dùng chung của tỉnh;

**4. Nguồn nhân lực cho ATTT:**

- Tổ chức đào tạo, bồi dưỡng nâng cao nhận thức và trình độ kỹ thuật về ATTT cho lãnh đạo và cho CBCCVC làm việc trong môi trường mạng;

- Các CBCCVC chuyên trách CNTT, quản trị mạng trong các cơ quan nhà nước của tỉnh được tập huấn, đào tạo các kỹ năng cần thiết về bảo đảm ATTT; tăng cường nâng cao nhận thức về công tác đảm bảo ATIT cho CBCCVC;

- Tạo điều kiện mở các lớp đào tạo nghiệp vụ nâng cao (cấp chứng chỉ) về bảo mật ATTT cho CBCCVC chuyên trách CNTT tại các sở, ban, ngành, các huyện, thị xã, thành phố;

- Chỉ đạo các doanh nghiệp 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;

- Kiện toàn lại cơ quan chuyên trách về CNTT của tỉnh để có bộ phận đảm nhiệm vấn đề an ninh và an toàn hệ thống thông tin mạng cho các Sở, ban, ngành, UBND các huyện, thị xã, thành phố.

## V. KINH PHÍ THỰC HIỆN

- Tổng kinh phí dự kiến là: **8.400.000.000 đồng** (*Tám tỷ bốn trăm triệu đồng*) từ nguồn kinh phí sự nghiệp giáo dục đào tạo, khoa học công nghệ của tỉnh bố trí hàng năm và các nguồn vốn hợp pháp khác.

- Riêng kinh phí trang bị phần mềm chống vius cho các sở, ban, ngành, UBND các huyện, thị xã, thành phố thì các đơn vị tự bố trí kinh phí để triển khai thực hiện.

- Giao Sở Tài chính chủ trì phối hợp với các ngành, địa phương có trách nhiệm tổng hợp, đề xuất UBND tỉnh phân bổ kinh phí cụ thể để thực hiện trong từng năm, đảm bảo phù hợp với điều kiện thực tế của tỉnh.

- Kinh phí cho các dự án, nhiệm vụ nêu trong kế hoạch này chỉ là khái toán, kinh phí này chỉ được xác định cụ thể khi các dự án, nhiệm vụ được xây dựng và phê duyệt theo quy định hiện hành về quản lý ngân sách trong quá trình triển khai kế hoạch ứng dụng CNTT hàng năm (*Kèm theo Phụ lục các dự án chi tiết*).

## VI. TỔ CHỨC THỰC HIỆN VÀ PHÂN CÔNG NHIỆM VỤ

### 1. Sở Thông tin và Truyền thông:

- Chủ trì, phối hợp với Sở Nội vụ để khẩn trương tham mưu UBND tỉnh kiện toàn, củng cố bộ phận chuyên trách về an ninh và an toàn thông tin (trực thuộc Sở Thông tin và Truyền thông) để có trách nhiệm bảo đảm an ninh và an toàn hệ thống thông tin mạng của các Sở, ban, ngành, UBND các huyện, thị xã, thành phố theo chỉ đạo của Chính phủ;

- Chủ trì, phối hợp với Sở Tài chính và các Sở, ban, ngành liên quan tham mưu UBND tỉnh xây dựng chương trình, kế hoạch ứng dụng và phát triển CNTT hàng năm, trong đó chú trọng tới các hạng mục về bảo đảm an toàn, an ninh thông tin đáp ứng nhu cầu thực tế, phù hợp với xu hướng phát triển của công nghệ và phù hợp với định hướng của Chính phủ, Bộ TT&TT;

- Chủ trì, phối hợp với các Sở, ban, ngành, UBND các huyện, thị xã, thành phố tổ chức triển khai các chương trình, dự án bảo đảm ATTT; chủ trì, phối hợp với Sở Nội vụ lập kế hoạch đào tạo kỹ năng chuyên sâu cho các cán bộ chuyên trách CNTT cũng như nâng cao nhận thức về ATTT cho các CBCCVC của tỉnh;

- Tăng cường công tác quản lý nhà nước về ngành Thông tin và Truyền thông, chú trọng công tác đảm bảo an toàn thông tin cho toàn mạng lưới;

- Tư vấn, góp ý, thẩm định các dự án CNTT theo chức năng, nhiệm vụ được giao phải tuân thủ theo các quy định đảm bảo an toàn, an ninh thông tin do Chính phủ, Bộ TT&TT đã ban hành;

- Làm tốt nhiệm vụ hướng dẫn, tuyên truyền đối với các tổ chức, cá nhân tham gia cung cấp và sử dụng dịch vụ Internet và thông tin trên mạng nhằm đề cao tinh thần

trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi hệ thống thông tin của mình; phối hợp với cơ quan quản lý nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin và an ninh thông tin trên mạng;

- Tham mưu cử CBCCVC phụ trách an toàn an ninh thông tin mạng thuộc Sở, Trung tâm CNTT&TT, Trung tâm Tin học của tỉnh tham gia đầy đủ các khóa học, lớp đào tạo theo Quyết định số 99/QĐ-TTg ngày 14/01/2014 của Thủ tướng Chính phủ về việc Phê duyệt Đề án "Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020".

**2. Sở Kế hoạch và Đầu tư :**

Chủ trì phối hợp với Sở Tài chính, Sở Thông tin và Truyền thông để cân đối nguồn vốn đầu tư phát triển của tỉnh và đề xuất cấp có thẩm quyền bố trí kinh phí cho các dự án bảo đảm ATTT trên địa bàn tỉnh Gia Lai.

**3. Sở Tài chính:**

Chủ trì, phối hợp Sở Thông tin và Truyền thông đề xuất bố trí kinh phí sự nghiệp hàng năm để triển khai các biện pháp thường xuyên về bảo đảm ATTT của tỉnh.

**4. Công an tỉnh:**

- Tham mưu công tác quản lý, phòng chống việc lợi dụng dịch vụ viễn thông để phục vụ cho mục đích chống Đảng, Nhà nước, khủng bố, tập hợp lực lượng, hình thành tổ chức chính trị đối lập, phản động, kêu gọi tiến hành các hoạt động chống đối, phá rối an ninh, trật tự.

- Chủ trì, phối hợp với Bộ chỉ huy Quân sự tỉnh và Sở Thông tin và Truyền thông xây dựng quy chế phối hợp và thường xuyên tiến hành việc kiểm tra, đánh giá thực trạng an ninh thông tin mạng ở các Sở, ban, ngành, địa phương và các doanh nghiệp nhà nước; hướng dẫn các Sở, ban, ngành, địa phương, và các doanh nghiệp nhà nước ban hành quy chế à thực hiện các giải pháp bảo đảm an ninh thông tin mạng; phát hiện, xử lý các hành vi vi phạm theo chức năng, nhiệm vụ được giao;

- Chủ trì, phối hợp với Bộ chỉ huy Quân sự tỉnh và Sở Thông tin và Truyền thông, các cơ quan liên quan và doanh nghiệp viễn thông, Internet xây dựng, triển khai các giải 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 kiểm tra an ninh, an toàn thiết bị điện tử 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 trên địa bàn tỉnh.

**5. Bộ Chỉ huy Quân sự tỉnh:**

- Chủ trì, phối hợp với Công an tỉnh và Sở Thông tin và Truyền thông xây dựng các văn bản quy phạm pháp luật về lĩnh vực bảo đảm an toàn, an ninh thông tin trong lực lượng vũ trang, đề xuất tăng cường đầu tư trang thiết bị, phương tiện đặc thù nhằm bảo vệ chủ quyền không gian mạng;

- Xây dựng bộ phận Tác chiến điện tử, nhân viên CNTT của Bộ Chỉ huy quân sự tỉnh có đủ trang bị hiện đại, hoạt động đúng chức năng có hiệu quả cao; tham gia giám sát, bảo vệ hạ tầng mạng trọng yếu của tỉnh và thực hiện nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng; xây dựng và bảo đảm an toàn thông tin cho các hệ thống tự động hóa chỉ huy và điều khiển vũ khí, bảo đảm sẵn sàng chiến đấu và chiến thắng trong điều kiện chiến tranh công nghệ cao, chiến tranh thông tin.

**6. Văn phòng UBND tỉnh:**

Thạm mưu UBND tỉnh quy định cụ thể danh mục tài liệu bí mật cần được bảo vệ trên cơ sở các văn bản quy phạm pháp luật của UBND tỉnh nhằm phổ biến tới các cơ quan, doanh nghiệp nhà nước bảo đảm an toàn thông tin mạng để không lộ, lọt bí mật nhà nước.

**7. Các Sở, ban, ngành, đoàn thể; UBND các huyện, thị xã, thành phố có trách nhiệm:**

- Quan tâm, chú trọng đến công tác bảo đảm ATTT cho hệ thống CNTT tại đơn vị mình;

- Chủ động bố trí kinh phí trang bị phần mềm diệt virus, bảo trì thiết bị tường lửa cho hệ thống máy tính, hệ thống mạng, hệ thống thông tin tại đơn vị mình;

- Trong việc triển khai các dự án CNTT cần phối hợp chặt chẽ với Sở TT&TT để bảo đảm vấn đề ATTT; cử CBCCVC tham gia đầy đủ các khóa đào tạo về ATTT;

Thủ trưởng các đơn vị tổ chức thực hiện và chỉ đạo đơn vị, CBCCVC trong phạm vi mình quản lý th, c hiện nghiêm túc, có hiệu quả nội dung trong Kế hoạch này./.

**TM. ỦY BAN NHÂN DÂN**
**KT.CHỦ TỊCH**
**PHÓ CHỦ TỊCH**

**Hoàng Công Lự**

# PHỤ LỤC

## DANH MỤC CÁC DỰ ÁN, NHIỆM VỤ
## BẢO ĐẢM AN TOÀN THÔNG TIN TRONG TÌNH HÌNH MỚI GIAI ĐOẠN 2015 - 2016

*(Kèm theo Kế hoạch Bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai trong tình hình mới)*

| TT | Tên dự án, nhiệm vụ | MỤC TIÊU | Đơn vị thực hiện | Thời gian thực hiện | Dự kiến kinh phí | Nguồn kinh phí | Ghi chú |
|---|---|---|---|---|---|---|---|
| 1 | Đào tạo, bồi dưỡng, nâng cao trình độ CNTT cho cán bộ, công chức, viên chức trên địa bàn tỉnh | Đào tạo, bồi dưỡng, nâng cao trình độ CNTT cho CBCCVC phục vụ công cuộc cải cách hành chính nhà nước, an toàn thông tin mạng. | Sở TT&TT; Sở Nội vụ | 2015 | 700.000 | SN Giáo dục & Đào tạo | |
| 2 | Đào tạo, bồi dưỡng, nâng cao trình độ CNTT cho cán bộ, công chức, viên chức trên địa bàn tỉnh | Đào tạo, bồi dưỡng, nâng cao trình độ CNTT cho CBCCVC phục vụ công cuộc cải cách hành chính nhà nước, an toàn thông tin mạng. | Sở TT&TT; Sở Nội vụ | 2016 | 700.000 | SN Giáo dục & Đào tạo | |
| 3 | Ứng dụng chữ ký số trong các cơ quan nhà nước | Nâng cao độ tin cậy, đảm bảo cho các giao dịch điện tử cũng như tạo cơ sở cho việc triển khai các ứng dụng CNTT và việc trao đổi thông tin trên môi trường máy tính. | Sở TT&TT | 2015-2016 | 1.000.000 | SN Khoa học & CN | |
| 4 | Đầu tư xây dựng hệ thống bảo mật cho các cơ quan, đơn vị nhà nước cấp tỉnh (cả thiết bị và phần mềm) | Mua sắm bộ thiết bị chống xâm nhập để bảo đảm an toàn thông tin và ngăn chặn tấn công hệ thống Trung tâm tích hợp dữ liệu của tỉnh; Mua sắm bộ thiết bị bảo mật lọc thư rác và phần mềm phòng chống virus cho hệ thống thư điện tử công vụ của tỉnh; Bản quyền phần mềm của hệ thống tường lửa bảo mật cổng thông tin điện tử của tỉnh và các trang thông tin điện tử của các sở, ban, ngành, huyện, thị xã, thành phố thuộc UBND tỉnh đặt tại Trung tâm tích hợp dữ liệu của tỉnh; Đầu tư mỗi đơn vị sở, ngành 01 thiết bị tường lửa nhằm đảm bảo an toàn thông tin và chống xâm nhập trái phép vào mạng nội bộ của mỗi đơn vị. | Sở TT&TT | 2015-2016 | 6.000.000 | SN Khoa học & CN | |
| | | **TỔNG CỘNG:** | | | **8.400.000** | | |

*Bằng chữ: Tám tỷ bốn trăm triệu đồng chẵn./.*