

Số: /KH-SNgV

Tây Ninh, ngày 16 tháng 02 năm 2024

## KẾ HOẠCH

### Triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng của Sở Ngoại vụ đến năm 2025, tầm nhìn 2030

Thực hiện Kế hoạch số 27/KH-UBND ngày 04/01/2024 của UBND tỉnh về việc triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030. Sở Ngoại vụ xây dựng Kế hoạch triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 như sau:

#### I. MỤC ĐÍCH, YÊU CẦU

- Bảo đảm an toàn, an ninh mạng nhằm chủ động phòng ngừa, sẵn sàng ứng phó với các thách thức từ không gian mạng, đẩy mạnh quá trình triển khai Chuyển đổi số.

- Nâng cao nhận thức, ý thức, trách nhiệm của công chức, viên chức, lao động cơ quan về an toàn, an ninh mạng; xây dựng, phát triển lực lượng bảo đảm an toàn, an ninh mạng đáp ứng yêu cầu thực tiễn.

- Xác định các nội dung, nhiệm vụ trọng tâm và giải pháp thực hiện, đảm bảo sự đồng bộ và thống nhất; phối hợp chặt chẽ với các cơ quan, đơn vị liên quan trong quá trình thực hiện nhằm hoàn thành tốt các nhiệm vụ được giao, bảo đảm an toàn, an ninh mạng trong phạm vi cơ quan quản lý.

- Quan tâm, xác định nhiệm vụ của đơn vị hướng dẫn, điều phối triển khai Chiến lược nhằm nâng cao năng lực an toàn, an ninh mạng quốc gia, hiện thực hóa tầm nhìn góp phần xây dựng không gian mạng phát triển văn minh, lành mạnh.

#### II. MỤC TIÊU

1. Mục tiêu tổng quát: Sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng, chủ động, nâng cao năng lực về bảo đảm an toàn, an ninh mạng, góp phần xây dựng không gian mạng phát triển văn minh, lành mạnh, là động lực tham gia cuộc Cách mạng công nghiệp lần thứ tư.

##### 2. Mục tiêu cụ thể

###### a. Mục tiêu cụ thể đến năm 2025

- Thực hiện tốt công tác bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn thông tin và an ninh mạng.

- Cử bộ cán bộ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng trong cơ quan.

- Phối hợp triển khai các hoạt động nhằm nâng cao nhận thức, kỹ năng bảo đảm an toàn, an ninh mạng cho toàn thể công chức, người lao động của cơ quan.

- Đảm bảo kinh phí phục vụ công tác bảo đảm an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho Chuyển đổi số và ứng dụng công nghệ thông tin.

### *b. Mục tiêu cụ thể đến năm 2030*

- Tiếp tục thực hiện tốt công tác bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn thông tin và an ninh mạng và tăng cường lực lượng bảo đảm an toàn, an ninh mạng tại đơn vị.

- Củng cố, tăng cường vai trò lãnh đạo của Đảng, quản lý Nhà nước; hoàn thiện hành lang pháp lý; bảo vệ chủ quyền quốc gia trên không gian mạng; bảo vệ hạ tầng số, nền tảng số, dữ liệu số, cơ sở hạ tầng không gian mạng quốc gia; bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước; bảo vệ hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin...

- Phấn đấu 100% công chức, người lao động cơ quan có cơ hội tiếp cận các hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

## **III. NHIỆM VỤ, GIẢI PHÁP THỰC HIỆN**

### **1. Nhiệm vụ**

- Thường xuyên phổ biến, quán triệt, nâng cao nhận thức, trách nhiệm của cấp ủy Đảng về các chủ trương của Đảng và chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng đến toàn thể công chức, người lao động cơ quan; xác định an toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là nhiệm vụ trọng yếu, thường xuyên và lâu dài.

- Lãnh đạo Sở luôn quan tâm, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo thực hiện hiệu quả. Nâng cao trách nhiệm, ý thức tự bảo vệ hệ thống thông tin thuộc phạm vi cơ quan, đơn vị quản lý. Gắn trách nhiệm của người đứng đầu cơ quan, đơn vị với trách nhiệm bảo đảm an toàn, an ninh mạng.

- Xây dựng, cập nhật và vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá vận hành hệ thống. Chủ động giám sát, phát hiện và công bố hành vi vi phạm quy định pháp luật của Việt Nam thuộc phạm vi quản lý trên các nền tảng số.

- Phối hợp với cơ quan chức năng có thẩm quyền xử lý các thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý.

- Bố trí nguồn lực và các điều kiện cần thiết để triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan. Tăng cường nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng về an toàn, an ninh mạng cho công chức và người lao động.

### **2. Giải pháp**

- Cử công chức tham gia các khóa đào tạo, phát triển nguồn nhân lực an toàn toàn thông tin trên địa bàn tỉnh. Ưu tiên bố trí nguồn lực và điều kiện cần thiết để triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan.

- Tăng cường công tác tuyên truyền, nâng cao nhận thức và phổ biến kiến thức, tình hình, xu hướng và các nguy cơ, hậu quả trong công tác an toàn, an ninh mạng và trang bị kỹ năng bảo đảm an toàn thông tin cho công chức, người lao động.

- Xây dựng cơ chế, thiết lập đường dây nóng, hệ thống tiếp nhận, xử lý thông tin về tội phạm mạng từ không gian mạng để quân chúng nhân dân phản ánh kịp thời, trực tiếp thông tin, hành vi vi phạm pháp luật trên không gian mạng tới cơ quan chức năng có thẩm quyền.

- Bên cạnh đó đổi mới nội dung, hình thức, biện pháp xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc phù hợp với thực tiễn chuyển đổi số. Phối hợp kịp thời trong việc cung cấp các thông tin chính thống để người dân biết, cùng phản biện tin giả, thông tin vi phạm pháp luật trên không gian mạng.

#### **IV. TỔ CHỨC THỰC HIỆN**

##### **1. Văn phòng Sở**

- Phối hợp các cơ quan liên quan triển khai thực hiện hiệu quả các chương trình, đề án đào tạo, phát triển nguồn nhân lực an ninh mạng.

- Chủ trì, phối hợp với các cơ quan liên quan triển khai thực hiện các nhiệm vụ về an toàn thông tin, an ninh mạng, hướng dẫn, đôn đốc triển khai thực hiện các nhiệm vụ về an toàn thông tin, an ninh mạng tại cơ quan.

- Tham mưu công tác tổng hợp báo cáo định kỳ kết quả thực hiện Kế hoạch và thường xuyên rà soát, đề xuất điều chỉnh, bổ sung Kế hoạch này khi có sự chỉ đạo từ cơ quan cấp trên và tình hình thực tế tại đơn vị.

##### **2. Các phòng chuyên môn thuộc Sở**

Căn cứ Kế hoạch này, Trưởng các phòng chuyên môn có trách nhiệm phổ biến, quán triệt nội dung Kế hoạch đến toàn thể công chức trong phòng; tổ chức triển khai thực hiện tốt các nhiệm vụ theo Kế hoạch này.

Trên đây là Kế hoạch Triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng của Sở Ngoại vụ đến năm 2025, tầm nhìn 2030 gửi Sở Thông tin và Truyền thông tổng hợp theo dõi và hướng dẫn thực hiện./.

##### **Nơi nhận:**

- Như trên;
  - Sở Thông tin và Truyền thông;
  - BGĐ Sở;
  - Các phòng CM;
  - Lưu: VT.
- (Phuong)

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

