

KẾ HOẠCH

Tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030

Thực hiện Quyết định số 1762/QĐ-BTTTT ngày 21/9/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về ban hành Kế hoạch hành động triển khai Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với thách thức từ không gian mạng đến năm 2025, tầm nhìn đến năm 2030, UBND tỉnh ban hành Kế hoạch tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030, như sau:

I. MỤC TIÊU CHUNG

Đảm bảo an toàn, an ninh thông tin mạng phục vụ phát triển chính quyền điện tử hướng tới chính quyền số tỉnh Quảng Ngãi; các hệ thống thông tin cơ quan nhà nước trên địa bàn tỉnh có khả năng thích ứng linh hoạt, giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng và chủ động phòng ngừa, ứng phó khi có sự cố về an toàn thông tin.

II. MỤC TIÊU CỤ THỂ ĐẾN NĂM 2025

1. Mục tiêu cụ thể đến năm 2025

- 100% hệ thống thông tin của các sở, ban, ngành tỉnh và UBND các huyện, thị xã, thành phố; 100% hệ thống thông tin của các đơn vị trực thuộc sở, ban, ngành tỉnh và UBND cấp xã được phê duyệt cấp độ an toàn hệ thống thông tin và triển khai các đầy đủ phương án đảm bảo an toàn thông tin theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

- 100% máy chủ đang hoạt động của cơ quan nhà nước trên địa bàn tỉnh cài đặt phòng, chống mã độc và chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC); 100% hệ thống thông tin cấp độ 3 trên địa bàn tỉnh được bảo vệ, triển khai giám sát trực tiếp trên Hệ thống giám sát tập trung (SOC) tỉnh Quảng Ngãi và kết nối chia sẻ dữ liệu với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

- 100% máy trạm của các sở, ban, ngành tỉnh và UBND các huyện, thị xã, thành phố; 70% máy trạm của các đơn vị cấp xã trên địa bàn tỉnh cài đặt phần mềm phòng, chống mã độc và chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

- 100% các sở, ban, ngành tỉnh và UBND các huyện, thị xã, thành phố ban hành các quy định, quy chế và hướng dẫn về đảm bảo an toàn, an ninh thông tin trong hoạt động của cơ quan, đơn vị trong năm 2022.

- 100% các sở, ban, ngành tỉnh và UBND các huyện, thị xã, thành phố có phân công cán bộ chuyên trách, kiêm nhiệm về an toàn thông tin.

- Tổ chức ít nhất 01 đợt diễn tập thực chiến/năm về an toàn thông tin mạng trên địa bàn tỉnh Quảng Ngãi.

- Đảm bảo tỷ lệ kinh phí chi cho công tác đảm bảo an toàn thông tin mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch phát triển chính quyền điện tử hướng đến chính quyền số, chuyển đổi số hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin, chuyển đổi số (*trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ đảm bảo an toàn thông tin mạng chuyên biệt đáp ứng các quy định của pháp luật về đảm bảo an toàn hệ thống thông tin theo cấp độ*).

2. Tầm nhìn đến năm 2030

- Tạo sự đột phá trong công tác đảm bảo an toàn thông tin trên toàn tỉnh, nhất là đột phá về điểm số các chỉ số an toàn thông tin trên địa bàn tỉnh; hạ tầng kỹ thuật các hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh được đầu tư hoàn thiện, nâng cao khả năng phòng, chống các cuộc tấn công trên môi trường mạng.

- Thu hút nhân lực và tập huấn nâng cao cho đội ngũ cán bộ chuyên trách an toàn thông tin của các cơ quan nhà nước trên địa bàn tỉnh có năng lực phòng thủ, ứng phó với các nguy cơ và sự cố mất an toàn thông tin trên không gian mạng đối với các hệ thống thông tin trên địa bàn tỉnh.

IV. NHIỆM VỤ TRỌNG TÂM

1. Tăng cường kiểm tra, đánh giá định kỳ về an toàn thông tin mạng đối với các hệ thống thông tin của cơ quan nhà nước và triển khai hoạt động giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tỉnh Quảng Ngãi; đầu tư trang thiết bị để nâng cao năng lực phòng, chống tấn công mạng đối với các hệ thống thông tin của cơ quan nhà nước.

2. Xây dựng hồ sơ đề xuất và phê duyệt cấp độ an toàn hệ thống thông tin, kiểm tra đánh giá phương án, điều kiện đảm bảo an toàn, an ninh mạng, giám sát an toàn, an ninh mạng, ứng phó khắc phục sự cố an toàn, an ninh mạng đối với các hệ thống thông tin quan trọng.

3. Tổ chức thanh tra, kiểm tra công tác đảm bảo an ninh mạng đối với các nhà mạng, các doanh nghiệp cung cấp dịch vụ công nghệ thông tin trên địa bàn tỉnh. Chủ động rà soát, tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý nghiêm các hành vi vi phạm pháp luật trên môi trường mạng.

4. Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an, Bộ Thông tin và Truyền thông và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng có xuất xứ trong nước, an ninh mạng tự chủ. Gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác phát

triển chính quyền điện tử hướng tới chính quyền số, kinh tế số, xã hội số và đô thị thông minh.

5. Tham gia vào mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, các chiến dịch đảm bảo an toàn thông tin mạng do Bộ Thông tin và Truyền thông điều phối, phát động.

6. Tập huấn về an toàn thông tin, nâng cao kỹ năng an toàn thông tin cho đội ngũ công chức, viên chức trên môi trường mạng. Tổ chức tập huấn hoặc cử cán bộ chuyên trách, phụ trách về an toàn thông tin/chuyên đổi số tham gia các khóa đào tạo, tập huấn về an toàn thông tin. Thu hút nguồn nhân lực cao về an toàn thông tin.

7. Tổ chức các chương trình diễn tập thực chiến, tập huấn về đảm bảo an toàn thông tin mạng với các phương án, kịch bản phù hợp thực tế cho cán bộ chuyên trách/phụ trách về an toàn thông tin của các cơ quan, đơn vị, doanh nghiệp.

8. Tiếp tục đẩy mạnh công tác truyền thông, nâng cao nhận thức, kỹ năng số, kỹ năng khai thác thông tin an toàn trên môi trường mạng, tăng cường tương tác với người dân, doanh nghiệp.

9. Kịp thời cung cấp thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác trong lĩnh vực an toàn, an ninh mạng phục vụ việc đánh giá xếp hạng chỉ số An toàn thông tin toàn cầu (GCI) của Liên minh Viễn thông Quốc tế (ITU).

10. - Phân công cán bộ, công chức chuyên trách, kiêm nhiệm làm công tác chuyên đổi số, công tác an toàn thông tin mạng tại cơ quan, đơn vị, địa phương.

V. KINH PHÍ THỰC HIỆN

1. Kinh phí thực hiện Kế hoạch này được bố trí thực hiện theo khả năng cân đối ngân sách nhà nước hàng năm theo phân cấp ngân sách hiện hành, nguồn kinh phí của doanh nghiệp, huy động từ các nguồn tài trợ hợp pháp khác; các doanh nghiệp liên quan chủ động bố trí kinh phí và các nguồn lực của đơn vị để thực hiện Kế hoạch này.

2. Đối với kinh phí thực hiện Kế hoạch trong năm 2022, các cơ quan, đơn vị, địa phương chủ động cân đối, sắp xếp kinh phí trong dự toán đã được giao trong năm 2022.

Từ năm 2023 trở đi, căn cứ nhiệm vụ được giao trong Kế hoạch này, các cơ quan, đơn vị, địa phương lồng ghép trong Kế hoạch chuyên đổi số hàng năm của đơn vị, địa phương, lập dự toán kinh phí thực hiện nhiệm vụ và tổng hợp chung trong dự toán ngân sách hàng năm của đơn vị, gửi cơ quan tài chính cùng cấp đề tổng hợp, trình cấp có thẩm quyền xem xét, bố trí kinh phí thực hiện theo quy định.

VI. TỔ CHỨC THỰC HIỆN

1. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các sở, ban, ngành; UBND các huyện, thị xã, thành phố tham mưu cho UBND tỉnh tổ chức triển khai các giải pháp đảm bảo an toàn thông tin mạng tổng thể trong cơ quan, đơn vị nhà nước của tỉnh; tham mưu đầu

tư, triển khai các giải pháp đảm bảo an toàn hạ tầng mạng, máy chủ, ứng dụng và các giải pháp phòng chống mã độc cho các hệ thống máy tính, hệ thống thông tin, cơ sở dữ liệu chuyên ngành của các cơ quan, đơn vị nhà nước thuộc tỉnh.

- Hướng dẫn, chỉ đạo các cơ quan báo chí, truyền thông tổ chức tuyên truyền chủ trương, chính sách của Đảng và pháp luật của Nhà nước về việc tăng cường đảm bảo an toàn, an ninh mạng trong các cơ quan nhà nước trên địa bàn tỉnh, góp phần nhằm nâng cao chỉ số xếp hạng an toàn thông tin của tỉnh.

- Hướng dẫn và theo dõi công tác phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin của cơ quan Nhà nước trên địa bàn tỉnh.

- Thường xuyên cập nhật và thông tin cảnh báo về các nguy cơ, lỗ hổng bảo mật an toàn toàn thông tin mạng đến các cơ quan nhà nước trên địa bàn tỉnh; kiểm tra, rà soát, phối hợp xử lý, khắc phục các lỗ hổng, điểm yếu về bảo mật, an toàn thông tin đối với hệ thống thông tin được kết nối, giám sát trên hệ thống giám sát tường lửa tập trung tại Trung tâm dữ liệu tỉnh và các hệ thống thông tin do đơn vị chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin và các hệ thống do đơn vị quản lý vận hành.

- Tham mưu đầu tư, triển khai các giải pháp đảm bảo an toàn hạ tầng mạng, máy chủ, ứng dụng, dữ liệu cho Trung tâm dữ liệu tỉnh Quảng Ngãi; thực hiện nghiêm các quy định về bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt.

- Hàng năm tổ chức thanh tra, kiểm tra định kỳ hoặc đột xuất công tác đảm bảo an ninh mạng đối với các nhà mạng, các doanh nghiệp cung cấp dịch vụ công nghệ thông tin trên địa bàn tỉnh. Rà soát, phát hiện và xử lý hoặc phối hợp với cơ quan chức năng có thẩm quyền xử lý thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý.

- Chỉ đạo các doanh nghiệp thuộc phạm vi quản lý rà soát, đánh giá, có biện pháp tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống hạ tầng thông tin, hệ thống điều khiển công nghiệp và các hệ thống thông tin quan trọng khác do doanh nghiệp quản lý, vận hành, khai thác trên địa bàn tỉnh.

- Phối hợp và tổ chức tập huấn, huấn luyện, diễn tập nâng cao trình độ, kỹ năng cho đội ngũ nhân lực giám sát an toàn thông tin mạng và nâng cao nhận thức, kiến thức an toàn thông tin cho người dùng và cán bộ, công chức, viên chức trên địa bàn tỉnh; điều phối các thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi kịp thời phối hợp và xử lý các sự cố về an toàn thông tin trên địa bàn tỉnh.

- Trong quá trình thẩm định, cân đối nguồn vốn cho các dự án về công nghệ thông tin, chuyên đổi số, đảm bảo đạt tối thiểu 10% tổng kinh phí triển khai dự án về chuyển đổi số trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ đảm bảo an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về đảm bảo an toàn thông tin theo cấp độ.

2. Văn phòng Ủy ban nhân dân tỉnh

- Tham mưu đầu tư, triển khai các giải pháp đảm bảo an toàn hạ tầng mạng, máy chủ, ứng dụng, dữ liệu cho Trung tâm tích hợp dữ liệu tại Văn phòng UBND tỉnh; thực hiện nghiêm các quy định về bảo đảm an toàn thông tin theo cấp độ đã

được phê duyệt.

- Phối hợp sở Thông tin và Truyền thông trong công tác kết nối Trung tâm tích hợp dữ liệu Văn phòng UBND tỉnh vào hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tỉnh Quảng Ngãi.

- Thường xuyên rà soát, kiểm tra, phối hợp xử lý, khắc phục các lỗ hổng, điểm yếu về bảo mật, an toàn thông tin đối với hệ thống thông tin do đơn vị chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin và các hệ thống thông tin do đơn vị quản lý vận hành.

3. Công an tỉnh

- Chủ trì, phối hợp với các cơ quan liên quan tổ chức triển khai, hướng dẫn thực hiện các văn bản quy phạm pháp luật về an ninh mạng, tội phạm trên không gian mạng, bảo vệ bí mật nhà nước và bảo vệ dữ liệu cá nhân.

- Rà soát, phát hiện, xử lý, hoặc phối hợp với cơ quan chức năng xử lý thông tin vi phạm pháp luật trên môi trường mạng theo quy định.

- Tăng cường đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin thuộc lĩnh vực do ngành Công an chịu trách nhiệm quản lý.

4. Sở Kế hoạch và Đầu tư, Sở Tài chính

Tăng cường, ưu tiên bố trí vốn đầu tư phát triển, vốn chi sự nghiệp thường xuyên hàng năm cho Sở Thông tin và Truyền thông và các sở, ban, ngành, địa phương triển khai hoạt động đảm bảo an toàn, an ninh mạng.

5. Sở Nội vụ

Trên cơ sở đề xuất của Sở Thông tin và Truyền thông, tham mưu UBND tỉnh, Sở Nội vụ chủ trì xây dựng và lồng ghép vào Kế hoạch đào tạo, bồi dưỡng cán bộ, công chức, viên chức hàng năm các lớp bồi dưỡng về an toàn, an ninh thông tin để nâng cao nhận thức, trình độ chuyên môn về an toàn, an ninh thông tin cho đội ngũ cán bộ, công chức, viên chức trên địa bàn tỉnh.

6. Sở Khoa học và Công nghệ

Chủ trì, phối hợp với các cơ quan, đơn vị, địa phương kết nối các chương trình, nhiệm vụ khoa học và công nghệ, khuyến khích, đẩy mạnh các đề tài khoa học liên quan đến an toàn, an ninh thông tin; đưa các sản phẩm đề tài khoa học trong lĩnh vực an toàn, an ninh thông tin vào ứng dụng trong các cơ quan nhà nước.

7. Sở Giáo dục và Đào tạo

Chủ trì, phối hợp với Sở Thông tin và Truyền thông đẩy mạnh triển khai các chương trình tuyên truyền, phổ biến, nâng cao nhận thức về an toàn, an ninh mạng trong các cơ sở đào tạo; định hướng, hướng dẫn các cơ sở đào tạo đẩy mạnh đào tạo nhân lực về an toàn thông tin.

8. Các sở, ban, ngành, Hội đoàn thể tỉnh; UBND cấp huyện, cấp xã

- Quán triệt nguyên tắc người đứng đầu cơ quan, đơn vị chịu trách nhiệm trước Chủ tịch UBND tỉnh nếu để xảy ra việc mất an toàn, an ninh thông tin mạng, lộ lọt bí mật nhà nước tại cơ quan, đơn vị mình quản lý.

- Triển khai đầy đủ các quy định về đảm bảo an toàn thông tin theo cấp độ đối với hệ thống thông tin do đơn vị chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin; xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, trình

cấp có thẩm quyền thẩm định và phê duyệt theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông. Thời gian hoàn thành trước ngày 31/12/2022.

- Triển khai các giải pháp an toàn thông tin theo cấp độ đối với các hệ thống thông tin do đơn vị chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin và quản lý, vận hành. Chủ trì, phối hợp với Sở Thông tin và Truyền thông triển khai hướng dẫn xây dựng hồ sơ đề xuất và phê duyệt cấp độ an toàn hệ thống thông tin đối với các hệ thống thông tin của các đơn vị trực thuộc và các đơn vị cấp xã.

- Tăng cường công tác tuyên truyền nâng cao nhận thức về an toàn, an ninh thông tin mạng cho lãnh đạo, cán bộ công chức, viên chức, người dân và doanh nghiệp thuộc phạm vi, địa bàn quản lý.

- Chủ động bố trí kinh phí và tăng cường thực hiện các biện pháp đảm bảo an toàn, an ninh thông tin đối với các hệ thống máy tính, hệ thống thông tin đang triển khai, ứng dụng tại cơ quan, đơn vị mình.

- Phân công cán bộ, công chức chuyên trách, kiêm nhiệm làm công tác chuyển đổi số, công tác an toàn thông tin mạng tại cơ quan, đơn vị, địa phương.

- Phối hợp với Sở Thông tin và Truyền thông trong công tác đánh giá mức độ đảm bảo an toàn thông tin mạng.

9. Các doanh nghiệp viễn thông, Internet hoạt động trên địa bàn tỉnh

Thiết lập, kiện toàn đầu mối đơn vị chuyên trách an toàn thông tin mạng trực thuộc để bảo vệ hệ thống, khách hàng của mình; tham gia hỗ trợ các cơ quan, đơn vị nhà nước giám sát, bảo vệ, kiểm tra, đánh giá an toàn thông tin mạng dưới sự điều phối của Sở Thông tin và Truyền thông.

Yêu cầu các cơ quan, đơn vị nghiêm túc triển khai, thực hiện Kế hoạch. Trong quá trình tổ chức thực hiện, trường hợp phát sinh vướng mắc, kịp thời báo cáo Chủ tịch UBND tỉnh (*thông qua Sở Thông tin và Truyền thông*) để xem xét, chỉ đạo giải quyết theo đúng quy định./.

Nơi nhận:

- Bộ Thông tin và Truyền thông;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- CT, PCT UBND tỉnh;
- BTT Ủy ban MTTQVN tỉnh;
- Ban Chỉ đạo CDS tỉnh;
- Sở, ban, ngành, đơn vị trực thuộc tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các Doanh nghiệp viễn thông, Internet;
- Báo Quảng Ngãi, Đài PT&TH Quảng Ngãi;
- VP UBND tỉnh: CVP, PCVP, CBTH;
- Lưu: VT, KGVX.Ngoc

CHỦ TỊCH



Đặng Văn Minh