ỦY BAN NHÂN DÂN TỈNH THỪA THIÊN HUẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 382/KH-UBND	*Thừa Thiên Huế, ngày 14 tháng 10 năm 2024*

KẾ HOẠCH
Triển khai công tác đảm bảo an toàn thông tin mạng giai đoạn 2024 - 2025 trên địa bàn tỉnh Thừa Thiên Huế

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chỉnh phủ phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt 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;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/05/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Căn cứ Quyết định số 1439/QĐ-BTTTT ngày 26/7/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Ban hành quy trình hướng dẫn thực hiện diễn tập thực chiến;

Căn cứ Quyết định số 2688/QĐ-UBND ngày 13/11/2023 của Ủy ban nhân dân tỉnh Thừa Thiên Huế về Ban hành Quy chế Bảo đảm an toàn Hệ thống thông tin tại Trung tâm dữ liệu tỉnh Thừa Thiên Huế;

Căn cứ Quyết định số 2849/QĐ-UBND ngày 04/12/2023 của Ủy ban nhân dân tỉnh Thừa Thiên Huế về phê duyệt cấp độ an toàn thông tin "Hệ thống Cơ sở hạ tầng thông tin tập trung tỉnh Thừa Thiên Huế";

Căn cứ Chỉ thị số 05/CT-UBND ngày 11/3/2024 của Chủ tịch Ủy ban nhân dân tỉnh Thừa Thiên Huế về tăng cường đảm bảo an toàn hệ thống thông tin theo cấp độ;

UBND tỉnh ban hành Kế hoạch triển khai công tác đảm bảo an toàn thông tin mạng giai đoạn 2024 - 2025 trên địa bàn tỉnh, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

- Nâng cao năng lực về bảo đảm an toàn, an ninh mạng, chủ động sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

- Nâng cao năng lực đảm bảo an toàn thông tin mạng cho toàn bộ hạ tầng, hệ thống thông tin, dữ liệu tại Trung tâm Giám sát, điều hành đô thị thông minh.

- Đẩy mạnh ứng dụng thành tựu khoa học - kỹ thuật, công nghệ tiên tiến, hiện đại thực hiện kế hoạch. Nghiên cứu các giải pháp xử lý, khắc phục lỗ hổng bảo mật, điểm yếu về bảo mật, an toàn thông tin.

- Xác định từng công việc cụ thể, phân công trách nhiệm rõ ràng, phù hợp với chức năng, nhiệm vụ của các Sở, ban, ngành, UBND các địa phương và các cơ quan, đơn vị liên quan; thực thi tốt cơ chế phối hợp giữa các cơ quan, đơn vị trong quá trình thực hiện đảm bảo an toàn thông tin mạng.

II. NỘI DUNG, NHIỆM VỤ VÀ GIẢI PHÁP

1. Triển khai phân loại, xác định, phê duyệt hồ sơ đề xuất cấp độ

- Rà soát, cập nhật và trình phê duyệt lại Hồ sơ đề xuất cấp độ và Quy chế bảo đảm an toàn thông tin cho Trung tâm dữ liệu.

- Hướng dẫn, đôn đốc, thẩm định và phê duyệt Hồ sơ đề xuất cấp độ cho các hệ thống thông tin trên địa bàn.

2. Triển khai đầy đủ các biện pháp bảo đảm an toàn thông tin theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ

- Đầu tư, nâng cấp trang thiết bị, bản quyền phần mềm

+ Trang cấp bản quyền các thiết bị lõi của mạng tại Trung tâm IOC gồm Firewall Fortigate 500E, 601F; Firewall Check point 6600; Bản quyền sản phẩm Nền tảng tri thức mối đe dọa an toàn thông tin (Threat Intelligence Platform); Bản quyền sản phẩm săn tìm mối nguy An toàn thông tin (Threat Hunting); Bản quyền sản phẩm phòng, chống thất thoát dữ liệu (DLP - Data Loss Prevention); Bản quyền sản phẩm quản lý và phân tích sự kiện an toàn thông tin (SIEM - Security Information and Event Management); Bản quyền sản phẩm Phòng, chống xâm nhập lớp mạng (NSM - Network Security Monitoring); Bản quyền sản phẩm Điều phối, tự động hóa và phản ứng an toàn thông tin (SOAR - Security Orchestration Automation and Response).

+ Trang cấp bản quyền sản phẩm sản phẩm Mạng riêng ảo (VPN - Virtual Private Network); Tường lửa ứng dụng web (WAF – Web Application

Firewall); Sản phẩm Tường lửa cơ sở dữ liệu; Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử; Sản phẩm kiểm soát truy cập lớp mạng (NAC – Network Access Controll).

+ Thuê dịch vụ Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây.

+ Triển khai 2 đường truyền Leasedline đảm bảo dự phòng song song.

- Rà soát, thiết lập cấu hình hệ thống đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ.

2. Tổ chức bảo đảm an toàn thông tin theo mô hình 4 lớp

2.1. Nâng cao năng lực lực lượng tại chỗ

(1) Kiện toàn lực lượng tại chỗ: Nâng cao năng lực lực lượng tại chỗ đáp ứng yêu cầu mới thông qua đào tạo, tuyển dụng hoặc thuê chuyên gia, bảo đảm mỗi đơn vị chuyên trách an toàn thông tin có tối thiểu 05 chuyên gia an toàn thông tin mạng

(2) Triển khai diễn tập, diễn tập thực chiến an toàn thông tin mạng:

- Cấp tỉnh: Tổ chức tối thiểu 01 cuộc diễn tập thực chiến an toàn thông tin mạng trong năm. Trong đó, đảm bảo có tổ chức diễn tập thực chiến cho các hệ thống thông tin cấp độ 3 trở lên.

- Cấp huyện tổ chức diễn tập tối thiểu một năm một lần cho một huyện được lựa chọn, mời các huyện còn lại cùng tham gia.

(3) Đào tạo phát triển nguồn nhân lực về an toàn thông tin mạng

- Xác định phân, phân công, bố trí cụ thể cán bộ chuyên trách/kiêm nhiệm an toàn thông tin tại các đơn vị chuyên trách CNTT/ATTT và cả các đơn vị không chuyên trách CNTT/ATTT.

- Định kỳ hàng năm triển khai các khóa đào tạo, bồi dưỡng kỹ thuật về an toàn thông tin cho cán bộ chuyên trách/kiêm nhiệm về an toàn thông tin; Các lớp cho cán bộ vận hành hệ thống, kỹ năng bảo mật và xử lý các sự cố về an toàn, an ninh mạng.

(4) Tổ chức tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng đặc biệt là phòng, chống lừa đảo trực tuyến

- Triển khai tuyên truyền nâng cao nhận thức, phổ biến kỹ năng cho cán bộ, công chức, viên chức, người lao động của cơ quan cũng như người dân trên địa bàn. Tận dụng các kênh tuyên truyền như: sự kiện, mạng xã hội, website, hệ thống thư điện tử, tin nhắn SMS, các ứng dụng thông minh, thông qua các hội thi tìm hiểu kỹ năng an toàn thông tin mạng cho người dân.

- Tuyên truyền tối đa trên các hệ thống thông tin cơ sở (đài truyền thanh, đài truyền hình).

- Xây dựng một số nội dung tuyên truyền ấn tượng, phù hợp với đặc điểm, đặc trưng, bản sắc văn hóa địa phương để tạo hiệu quả cao và phạm vi tuyên truyền rộng đến mọi đối tượng của cộng đồng.

2.2. Giám sát bảo vệ chuyên nghiệp

(1) Tổ chức bảo đảm an toàn thông tin thực chất, toàn diện và nâng cao năng lực lớp giám sát bảo vệ chuyên nghiệp

- Đảm bảo 100% hệ thống thông tin của cơ quan, tổ chức được tổ chức bảo đảm an toàn thông tin thực chất, toàn diện theo hướng dẫn Công văn số 1598/BTTTT-CATTT ngày 28/4/2022 của Bộ Thông tin và Truyền thông; nâng cao năng lực của lớp giám sát, bảo vệ chuyên nghiệp và kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

- Hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý. Đối với các hệ thống thông tin cấp độ 3 trở lên, khuyến nghị tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối.

(2) Tăng cường năng lực phòng chống phần mềm độc hại

- Giải pháp, phần mềm sử dụng đáp ứng các yêu cầu kỹ thuật tối thiểu bao gồm: Có chức năng cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7, có khả năng phản ứng kịp thời trong việc phát hiện, phân tích và gỡ bỏ phần mềm độc hại; có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông và quy định của pháp luật;

- Tổ chức theo dõi, thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông tin trong phạm địa phương.

- Chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia.

- Phối hợp với Bộ Thông tin và Truyền thông trong các chiến dịch bóc gỡ mã độc, mạng máy tính nhiễm mã độc trên diện rộng.

2.3. Kiểm tra, đánh giá an toàn thông tin các hệ thống trung tâm dữ liệu và các hệ thống thông tin trên địa bàn tỉnh

- Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt.

- Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

Cách thức: Định kỳ 02 năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin tổng thể trong hoạt động của cơ quan, tổ chức mình. Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với các hệ thống cấp độ 3; 2 năm 1 lần đối với các hệ thống thông tin cấp độ 1, cấp độ 2.

Sở Thông tin và Truyền thông chủ trì các hệ thống thông tin cấp độ 2, cấp độ 3; Các cơ quan, đơn vị chủ trì triển khai các hệ thống trong tổ chức của mình.

2.4. Kết nối, chia sẻ dữ liệu về Trung tâm giám sát an toàn mạng quốc gia

- Giám sát an toàn thông tin và Kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin.

- Trang cấp các thiết bị/giải pháp: Kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin.

3. Hoàn thiện phương án ứng cứu sự cố an toàn thông tin mạng

Xây dựng, triển khai phương án, quy trình xử lý các sự cố, bao gồm nhưng không giới hạn các nhóm sự cố sau:

- Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ; Tấn công giả mạo; Tấn công sử dụng mã độc; Tấn công truy cập trái phép, chiếm quyền điều khiển; Tấn công thay đổi giao diện; Tấn công mã hóa phần mềm, dữ liệu, thiết bị; Tấn công phá hoại thông tin, dữ liệu, phần mềm; Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; Tấn công tổng hợp sử dụng kết hợp nhiều hình thức.

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật: Sự cố nguồn điện; Sự cố đường kết nối Internet; Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin; Sự cố liên quan đến quá tải hệ thống; Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống: Lỗi trong cập nhật, thay đổi, cấu hình phần cứng; Lỗi trong cập nhật, thay đổi, cấu hình phần mềm; Lỗi liên quan đến chính sách và thủ tục an toàn thông tin; Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc; Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

4. Sử dụng hiệu quả các nền tảng số quốc gia

Đào tạo, hướng dẫn sử dụng các nền tảng quản lý đảm bảo an toàn hệ thống thông tin :

- Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Nền tảng Hỗ trợ điều phối, ứng cứu sự cố.

- Nền tảng Hỗ trợ điều tra số.

5. Xây dựng phương án sao lưu, phục hồi dữ liệu, triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường

Trang cấp bản quyền sản phẩm sao lưu dự phòng tập trung; Đầu tư kinh phí mua 03 phương tiện lưu trữ (02 phương tiên lưu trữ trực tuyến khác nhau, 01 phương tiện lưu trữ ngoại tuyến). Đầu tư triển khai giải pháp để sẵn sàng phục hồi nhanh Hệ thống thông tin khi gặp sự cố, đưa hoạt động trở lại bình thường trong 24 tiếng hoặc theo yêu cầu nghiệp vụ.

Trong đó, định kỳ thực hiện sao lưu dữ liệu ngoại tuyến "offline". Với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1: có ít nhất 03 bản sao dữ liệu, lưu trữ bản sao trên 02 phương tiện lưu trữ khác nhau, với 01 bản sao lưu ngoại tuyến "offline" (sử dụng tape/USB/ổ cứng di động,…). Dữ liệu sao lưu offline phải được tách biệt hoàn toàn, không kết nối mạng, cô lập để phòng chống tấn công leo thang vào hệ thống lưu trữ. Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường trong vòng 24 tiếng hoặc theo yêu cầu của nghiệp vụ.

III. KINH PHÍ TRIỂN KHAI

- Ngân sách nhà nước: triển khai mua sắm, trang cấp bản quyền thiết bị, phần mềm; thuê dịch vụ giám sát an toàn thông tin mạng, đào tạo nguồn nhân lực an toàn thông tin mạng.

- Các nguồn hợp pháp khác phục vụ một phần cho công tác triển khai các hội nghị, hội thảo, hội thi.

IV.TỔ CHỨC THỰC HIỆN

1. Ban Chỉ đạo Chuyển đổi số và thực hiện Đề án 06 tỉnh

Ban Chỉ đạo Chuyển đổi số và thực hiện Đề án 06 tỉnh (Sở Thông tin và Truyền thông làm cơ quan Thường trực) giúp Chủ tịch UBND tỉnh chỉ đạo công tác sơ kết, tổng kết việc triển khai thực hiện; chỉ đạo, điều phối xử lý các vấn đề về an toàn, an ninh mạng thuộc nội dung Kế hoạch này.

2. Sở Thông tin và Truyền thông

- Sở Thông tin và Truyền thông chủ trì, triển khai, hướng dẫn, đôn đốc, kiểm tra các cơ quan, tổ chức, doanh nghiệp trên địa bàn tỉnh triển khai thực hiện các nội dung về an toàn thông tin mạng tại Kế hoạch này.

- Tổ chức tổng kết, tổng hợp, báo cáo Chủ tịch UBND tỉnh tình hình thực hiện và đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn đối với các nội dung về an toàn thông tin mạng.

- Chủ trì, phối hợp với các sở, ban, ngành, huyện, thị xã, thành phố và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ được giao theo chức năng, nhiệm vụ.

- Kịp thời thông báo, hướng dẫn các sở, ngành, địa phương xử lý kịp thời khi các thiết bị đầu cuối, các hệ thống thông tin bị nhiễm mã độc hoặc không đảm bảo an toàn thông tin.

3. Công an tỉnh

- Thực hiện công tác phòng ngừa, ứng phó, xử lý các nguy cơ, thách thức từ không gian mạng, dự báo các tình huống về chiến tranh thông tin, xung đột trên không gian mạng theo chức năng, nhiệm vụ được giao.

- Phối hợp với Sở Thông tin và Truyền thông triển khai diễn tập phòng chống tấn công mạng, ứng cứu xử lý các tình huống về an toàn an ninh mạng.

4. Sở Tài chính

Căn cứ khả năng cân đối ngân sách, Sở Tài chính tham mưu UBND tỉnh bố trí kinh phí cho các nội dung chi thường xuyên đối với công tác đảm bảo an toàn thông tin và an ninh mạng trong các cơ quan nhà nước theo quy định của Luật ngân sách nhà nước và các văn bản hướng dẫn thi hành.

5. Sở Kế hoạch và Đầu tư

Tổng hợp đề xuất các dự án liên quan đến đảm bảo an toàn thông tin, an ninh mạng một cách kịp thời để triển khai thực hiện.

6. Các sở, ban, ngành và UBND các huyện, thị xã và thành phố

- Chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông tổ chức thực hiện các nhiệm vụ được giao tại Kế hoạch này.

- 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 theo quy định của pháp luật.

- Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng, an ninh mạng do Việt Nam sản xuất (Makein Vietnam), gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai Chuyển đổi số, phát triển chính quyền số, gắn với đô thị thông minh và kinh tế số, xã hội số.

- Chủ động rà soát, phát hiện và xử lý hoặc phối hợp với các cơ quan chức năng có thẩm quyền xử lý thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý. Tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý hoặc phối hợp xử lý nghiêm các hành vi vi phạm.

- Ưu tiên bố trí nguồn lực về nhân lực và kinh phí, cùng các điều kiện khác để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý.

- Thúc đẩy việc ứng dụng, sử dụng chữ ký số chuyên dùng Chính phủ và bảo mật thông tin trên hệ thống mạng theo quy định của pháp luật về cơ yếu.

- Định kỳ kiểm tra, đánh giá và báo cáo hàng năm hoặc đột xuất theo quy định do Công an tỉnh, Sở Thông tin và Truyền thông hướng dẫn về tình hình, kết quả triển khai Kế hoạch để tổng hợp, báo cáo Thủ tướng Chính phủ theo quy định về chế độ thông tin, báo cáo.

Trên đây là kế hoạch Triển khai công tác đảm bảo an toàn thông tin mạng giai đoạn 2024 - 2025 trên địa bàn tỉnh Thừa Thiên Huế. UBND tỉnh yêu cầu các cơ quan, đơn vị, địa phương và tổ chức, doanh nghiệp nghiêm túc triển khai Kế hoạch này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, đề nghị kịp thời phản ánh về Sở Thông tin và Truyền thông để báo cáo UBND tỉnh theo quy định./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- Chủ tịch và các Phó Chủ tịch;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- UBND các huyện, thị xã, thành phố Huế;
- VP: CVP, các PCVP;
- Lưu: VP, CN.

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

Nguyễn Thanh Bình

Số: 382/KH-UBND
Thời gian ký: 14/10/2024 17:37:39 +07:00

Phụ lục

DANH MỤC NHIỆM VỤ TRIỂN KHAI

NHẰM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG GIAI ĐOẠN 2024 - 2025 TRÊN ĐỊA BÀN TỈNH THỪA THIÊN HUẾ

(Kèm theo Kế hoạch số 382/KH-UBND ngày 14/10/2024 của UBND tỉnh Thừa Thiên Huế)

TT	Tên nhiệm vụ	Chủ trì	Phối hợp	Thời gian hoàn thành	Ghi chú
I	**Triển khai phân loại, xác định, phê duyệt hồ sơ đề xuất cấp độ (**HSĐXCĐ)				
1	Rà soát, cập nhật và trình phê duyệt lại Hồ sơ đề xuất cấp độ và Quy chế bảo đảm an toàn thông tin cho Trung tâm dữ liệu	Sở Thông tin và Truyền thông	Các ngành các cấp	Năm 2024	
2	Hướng dẫn, đôn đốc, thẩm định và phê duyệt Hồ sơ đề xuất cấp độ cho hệ thống thông tin trên địa bàn	Sở Thông tin và Truyền thông	Các ngành các cấp	Năm 2024	
II	**Triển khai đầy đủ các biện pháp bảo đảm an toàn thông tin theo phương án được phê duyệt trong HSĐXCĐ**				
1	Đầu tư, nâng cấp trang thiết bị, bản quyền phần mềm				
a	Trang cấp bản quyền các thiết bị lõi của mạng tại Trung tâm IOC	Sở Thông tin và Truyền thông		Triển khai hằng năm	
b	Trang cấp bản quyền sản phẩm sản phẩm Mạng riêng ảo (VPN - Virtual Private Network); Tường lửa ứng dụng web (WAF – Web Application Firewall); Sản phẩm Tường lửa bảo vệ cơ sở dữ liệu; Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử.	Sở Thông tin và Truyền thông		Triển khai hằng năm	
c	Thuê dịch vụ Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây; Trang cấp các thiết bị/giải pháp kiểm soát truy cập (NAC-	Sở Thông tin và Truyền thông		Triển khai hằng năm	

	Network Access Control); Thuê dịch vụ quảng bá số hiệu mạng IP/ASN tại Trung tâm dữ liệu.				
d	Triển khai 02 đường truyền Leasedline phụ vụ cung cấp dịch vụ; đảm bảo tính cân bằng tải, dự phòng, song song; Triển khai 02 đường truyền Internet FTTH tập trung đảm bảo truy cập Internet tập trung, an toàn truy cập Internet cho các cơ quan, đơn vị có kết nối mạng WAN.	Sở Thông tin và Truyền thông		Triển khai hằng năm	
e	Thực hiện bảo trì, bảo dưỡng, thay thế các thiết bị mạng, máy chủ, thiết bị phụ trợ phục vụ vận hành hệ thống hạ tầng mạng; Triển khai chứng thư số SSL đối hệ thống tên miền của tỉnh.	Sở Thông tin và Truyền thông		Triển khai hằng năm	
f	Triển khai giải pháp phòng chống mã độc tập trung cho hệ thống máy chủ; Máy tính cho toàn bộ các cơ quan nhà nước trên địa bàn tỉnh.	Sở Thông tin và Truyền thông	Các ngành các cấp	Triển khai hằng năm	
2	Rà soát, thiết lập cấu hình hệ thống đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong HSĐXCĐ	Sở Thông tin và Truyền thông	Các ngành liên quan	2024 - 2025	
III	**Tổ chức bảo đảm an toàn thông tin theo mô hình 4 lớp**				
1	Nâng cao năng lực lực lượng tại chỗ				
a	Kiện toàn lực lượng tại chỗ: Nâng cao năng lực lực lượng tại chỗ đáp ứng yêu cầu mới thông qua đào tạo, tuyển dụng hoặc thuê chuyên gia, bảo đảm mỗi đơn vị chuyên trách an toàn thông tin có tối thiểu 05 chuyên gia an toàn thông tin mạng	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	Triển khai hằng năm	

b	Triển khai diễn tập, diễn tập thực chiến an toàn thông tin mạng	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	Triển khai hằng năm	
c	Đào tạo phát triển nguồn nhân lực về an toàn thông tin mạng	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	Triển khai hằng năm	
d	Tổ chức tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng đặc biệt là phòng, chống lừa đảo trực tuyến	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	Triển khai hằng năm	
2	Giám sát bảo vệ chuyên nghiệp				
a	Tổ chức bảo đảm an toàn thông tin thực chất, toàn diện và nâng cao năng lực lớp giám sát bảo vệ chuyên nghiệp	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	Triển khai hằng năm	
b	Tăng cường năng lực phòng chống phần mềm độc hại: Thiết lập, cài đặt phần mềm phòng, chống mã độc trên 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	Triển khai hằng năm	
3	Kiểm tra, đánh giá an toàn thông tin	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	
4	Kết nối, chia sẻ dữ liệu về Trung tâm giám sát an toàn mạng quốc gia	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	
IV	**Hoàn thiện phương án ứng cứu sự cố an toàn thông tin mạng**				
-	Xây dựng, triển khai phương án, quy trình xử lý các sự cố, bao gồm nhưng không giới hạn các nhóm sự cố	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	
V	**Sử dụng hiệu quả các nền tảng số quốc gia**				
1	Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	
2	Nền tảng Hỗ trợ điều phối, ứng cứu sự cố	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	

3	Nền tảng Hỗ trợ điều tra số	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	
VII	**Xây dựng Phương án sao lưu, phục hồi dữ liệu. Triển khai giải pháp để sẵn sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố, đưa hoạt động của hệ thống thông tin trở lại bình thường**				
1	Trang cấp bản quyền sản phẩm sao lưu dự phòng tập trung; Đầu tư kinh phí mua 03 phương tiện lưu trữ (02 phương tiên lưu trữ trực tuyến khác nhau, 01 phương tiện lưu trữ ngoại tuyến)	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	
2	Đầu tư triển khai giải pháp để sẵn sàng phục hồi nhanh Hệ thống thông tin khi gặp sự cố, đưa hoạt động trở lại bình thường trong 24 tiếng hoặc theo yêu cầu nghiệp vụ.	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị phối hợp	2024 - 2025	