UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

QUY CHẾ
Hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đồng Nai

(Ban hành kèm theo Quyết định số 100 /QĐ-STTTT ngày 22.. tháng 05. năm 2024 của Sở Thông tin và Truyền thông tỉnh Đồng Nai)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định về nhiệm vụ, quyền hạn, trách nhiệm, nguyên tắc và chế độ hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đồng Nai.

2. Quy chế này được áp dụng cho Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đồng Nai (sau đây gọi tắt là Đội ứng cứu sự cố) và các cơ quan, tổ chức, cá nhân có liên quan trong hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn toàn tỉnh.

Điều 2. Tổ chức Đội ứng cứu sự cố

1. Đội ứng cứu sự cố do Ủy ban nhân dân (sau đây viết tắt là UBND) tỉnh Đồng Nai thành lập tại Quyết định số 890/QĐ-UBND ngày 04 tháng 4 năm 2024, chịu trách nhiệm trực tiếp điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh.

2. Đội ứng cứu sự cố có Đội trưởng, một (01) Đội phó và các thành viên. Đội ứng cứu sự cố được sử dụng con dấu của Sở Thông tin và Truyền thông, đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của tỉnh, để giao dịch và thực hiện nhiệm vụ theo quy định.

3. Bộ phận thường trực của Đội ứng cứu sự cố (sau đây gọi tắt là Thường trực Đội ứng cứu sự cố) là Sở Thông tin và Truyền thông; địa chỉ: Số 01 đường 30/4, phường Thanh Bình, thành phố Biên Hòa, tỉnh Đồng Nai; số điện thoại: 0251.3810269; địa chỉ thư điện tử: attt@dongnai.gov.vn.

Điều 3. Giải thích từ ngữ

1. Sự cố an toàn thông tin mạng (sau đây gọi tắt là sự cố) là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng. Sự cố có thể là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn thông tin trên môi trường mạng (LAN, WAN, INTERNET…), được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin trong nước và trên thế giới.

2. Sự cố có tính chất nghiêm trọng là sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính; lấy cắp dữ liệu, có thể gây thiệt hại lớn cho các hệ thống thông tin quan trọng của tỉnh như: Trung tâm tích hợp dữ liệu, Cổng thông tin điện tử, Cổng dịch vụ công trực tuyến và hệ thống thông tin một cửa điện tử, hệ thống quản lý văn bản và điều hành, hệ thống thông tin báo cáo trực tuyến, hệ thống thư điện tử công vụ … và các hệ thống thông tin, cơ sở dữ liệu chuyên ngành của sở, ban, ngành, địa phương, đòi hỏi sự tham gia phối hợp của nhiều cơ quan, đơn vị trong tỉnh và cần có sự hỗ trợ của các cơ quan, đơn vị chuyên trách quốc gia để giải quyết.

3. Ứng cứu sự cố là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

4. Điều phối ứng cứu sự cố là hoạt động của cơ quan, đơn vị có thẩm quyền nhằm huy động, điều hành, phối hợp thống nhất các nguồn lực gồm: nhân lực, vật lực (trang thiết bị), tài lực (tài chính, ngân sách) để phòng ngừa, theo dõi, thu thập, phát hiện, cảnh báo sự cố; tiếp nhận, phân tích xác minh, phân loại sự cố; điều hành, phối hợp, tổ chức ứng cứu sự cố, sẵn sàng ứng phó, khắc phục sự cố nhằm giảm thiểu các rủi ro, thiệt hại do sự cố gây ra.

5. Log file là tập tin được tạo ra trong quá trình hoạt động của hệ thống mạng, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị tường lửa, thiết bị cân bằng tải, máy chủ, máy tính, phần mềm hệ thống, phần mềm ứng dụng, cơ sở dữ liệu... Bản ghi trong log file bao gồm chi tiết hành động trong đó có chứa thông tin về lịch sử hoạt động của hệ thống, thiết bị, ứng dụng đó.

Điều 4. Nhiệm vụ và quyền hạn của Đội ứng cứu sự cố

1. Đội ứng cứu sự cố có nhiệm vụ tổ chức, điều phối, hỗ trợ các cơ quan Đảng, đoàn thể chính trị - xã hội, các cơ quan trong hệ thống hành chính nhà nước của tỉnh trong công tác ứng cứu sự cố về an toàn thông tin mạng, không bao gồm các sự cố của hệ thống thông tin do Bộ Quốc phòng, Bộ Công an quản lý.

2. Đội ứng cứu sự cố là đầu mối của tỉnh trong Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia; liên kết, phối hợp với các Đội ứng cứu sự cố của các Bộ, ngành Trung ương, các tỉnh, thành phố trực thuộc Trung ương nhằm ứng phó kịp thời khi xảy ra sự cố an toàn thông tin mạng dưới sự điều phối của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT).

3. Khi được sự đồng ý của lãnh đạo cơ quan, đơn vị chủ quản hệ thống thông tin, các thành viên có quyền truy cập vào hệ thống mạng, hệ thống ứng dụng công nghệ thông tin, cơ sở dữ liệu, máy chủ, máy tính… và log file để phân tích, truy vết, thực hiện dưới sự giám sát của cơ quan, đơn vị bị sự cố.

4. Hàng năm, tham mưu cho UBND tỉnh xây dựng và triển khai Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng; tham gia các đợt diễn tập phòng thủ, tấn công, xử lý và khắc phục sự cố do các cơ quan Trung ương tổ chức.

5. Định kỳ (6 tháng, năm) và đột xuất theo yêu cầu, thực hiện báo cáo UBND tỉnh về tình hình hoạt động, những khó khăn, vướng mắc và đề xuất các giải pháp nâng cao hiệu quả công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

Chương II

NGUYÊN TẮC, CHẾ ĐỘ LÀM VIỆC VÀ KINH PHÍ HOẠT ĐỘNG

Điều 5. Nguyên tắc làm việc

1. Điều phối hoạt động ứng cứu sự cố trong phạm vi toàn tỉnh.

2. Tổ chức ứng cứu sự cố theo đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, an toàn và hiệu quả.

3. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật theo quy định và theo yêu cầu của cơ quan, đơn vị gặp sự cố trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng khác mà cần cảnh báo, hướng dẫn chung.

4. Công tác kiểm tra, rà soát đánh giá an toàn thông tin phải được thực hiện thường xuyên, định kỳ hoặc đột xuất khi có các yếu tố quan trọng, đặc biệt thay đổi để kịp thời phát hiện các lỗ hổng đang tồn tại, các nguy cơ mất an toàn thông tin mạng.

5. Thành viên Đội ứng cứu sự cố là nhân sự của cơ quan, đơn vị, địa phương nào chịu trách nhiệm thường trực và đầu mối phối hợp bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị, địa phương đó.

Điều 6. Chế độ làm việc

1. Các thành viên Đội ứng cứu sự cố làm việc theo chế độ kiêm nhiệm và được hưởng các chế độ, chính sách theo quy định hiện hành. Khi xảy ra sự cố, các thành viên phải ưu tiên cho hoạt động của Đội ứng cứu sự cố, tuân thủ việc triệu tập, điều phối của Đội trưởng hoặc Đội phó được ủy quyền.

2. Đội trưởng triệu tập thành viên Đội ứng cứu sự cố, tổ chức phiên họp thường kỳ 06 tháng/lần hoặc đột xuất theo yêu cầu nhiệm vụ và yêu cầu của cơ quan cấp trên.

3. Đội trưởng triệu tập và điều phối các thành viên khi có sự cố đột xuất xảy ra, hoặc ủy quyền cho Đội phó thực hiện thẩm quyền của mình khi vắng mặt. Đội phó khi được ủy quyền được sử dụng thẩm quyền của Đội trưởng để điều phối các hoạt động và chịu trách nhiệm về các quyết định của mình trước Đội trưởng và pháp luật.

4. Các hoạt động giao dịch, trao đổi công việc giữa các thành viên Đội ứng cứu sự cố trên môi trường mạng được thực hiện thông qua hệ thống thư điện tử đã được đăng ký theo danh sách Đội ứng cứu sự cố hoặc các hệ thống thông tin thuộc chính quyền điện tử tỉnh.

Điều 7. Điều kiện và kinh phí hoạt động

1. Đội ứng cứu sự cố được bảo đảm phương tiện, thiết bị và điều kiện cần thiết để duy trì hoạt động. Đội ứng cứu sự cố được sử dụng phương tiện của Sở Thông tin và Truyền thông để thực hiện nhiệm vụ.

2. Kinh phí hoạt động của Đội ứng cứu sự cố được bố trí trong dự toán ngân sách hàng năm cấp cho Sở Thông tin và Truyền thông, được sử dụng cho các hoạt động sau: Mua sắm văn phòng phẩm, trang thiết bị chuyên dụng; tổ chức và tham gia hội thảo, hội nghị, đào tạo, bồi dưỡng, huấn luyện, diễn tập về ứng cứu sự cố, bảo đảm an toàn, an ninh thông tin; công tác phí; chi làm thêm giờ cho việc ứng cứu, khắc phục sự cố… Định mức chi thực hiện theo các quy định hiện hành.

Chương III
TỔ CHỨC ỨNG CỨU SỰ CỐ

Điều 8. Thông báo, tiếp nhận và xử lý thông báo sự cố

1. Cơ quan, đơn vị, địa phương vận hành hệ thống thông tin khi phát hiện sự cố phải thực hiện thông báo sự cố và báo cáo ban đầu sự cố mạng cho Thường trực Đội ứng cứu sự cố và thành viên Đội ứng cứu sự cố được phân công phụ trách cơ quan, đơn vị, địa phương (nếu có). Trường hợp nhận thấy sự cố nghiêm trọng không thể tự khắc phục phải thông báo, báo cáo kịp thời, trực tiếp cho Đội trưởng Đội ứng cứu sự cố.

a) Thông báo sự cố có thể thực hiện qua điện thoại, thư điện tử, nhắn tin đa phương tiện và thông qua hệ thống Nền tảng điều phối xử lý sự cố (Irlab.vn), với các nội dung cơ bản: thông tin mô tả sự cố; các biện pháp đã, đang triển khai xử lý, khắc phục; kiến nghị và đề xuất.

b) Báo cáo ban đầu sự cố mạng có thể thực hiện bằng văn bản giấy hoặc văn bản điện tử (có ký tên và đóng dấu hoặc chữ ký số của người có thẩm quyền) theo Mẫu số 03 Phụ lục I ban hành kèm theo Thông tư số 20/2017/TT-BTTTT. Đồng thời thực hiện thông qua thông qua hệ thống Nền tảng điều phối xử lý sự cố (Irlab.vn).

2. Thường trực Đội ứng cứu sự cố và các cá nhân khi tiếp nhận được thông báo sự cố hoặc báo cáo ban đầu sự cố mạng phải báo cáo kịp thời cho Đội trưởng, Đội phó.

3. Đội trưởng Đội ứng cứu sự cố quyết định điều phối các thành viên; triệu tập cuộc họp; huy động các nguồn lực để xử lý, khắc phục sự cố khi cần

thiết. Trường hợp sự cố nghiêm trọng, Đội trưởng báo cáo, xin ý kiến cấp có thẩm quyền trước khi quyết định tổ chức, điều phối, hỗ trợ ứng cứu sự cố.

Điều 9. Điều phối ứng cứu sự cố

1. Thường trực Đội ứng cứu sự cố thực hiện thông báo triệu tập, điều phối của Đội trưởng bằng văn bản đến với các thành viên trong Đội ứng cứu sự cố. Trường hợp khẩn cấp có thể thông báo nhanh bằng điện thoại, email để điều phối và thông báo chính thức bằng văn bản sau.

Thường trực Đội ứng cứu sự cố thông báo cho các tổ chức, cá nhân gặp sự cố về yêu cầu phối hợp trong quá trình thực hiện điều phối và ứng cứu sự cố.

2. Thành viên Đội ứng cứu sự cố tiếp nhận thông báo điều phối; phối hợp chặt chẽ với cơ quan, đơn vị nơi xảy ra sự cố và các thành viên cùng tham gia ứng cứu tổ chức thực hiện xử lý, khắc phục sự cố đúng yêu cầu điều phối và theo quy trình được hướng dẫn tại Khoản 2, Khoản 3 Điều 11 và Phụ lục II ban hành kèm theo Thông tư số 20/2017/TT-BTTTT; báo cáo kết quả thực hiện cho Đội trưởng (qua Thường trực Đội ứng cứu sự cố).

3. Công tác ứng cứu kết thúc khi đã khắc phục được sự cố và hệ thống hoạt động trở lại bình thường.

4. Sau khi khắc phục sự cố, thành viên tham gia ứng cứu có trách nhiệm:

a) Rà soát, xác định nguyên nhân gây ra sự cố;

b) Tổ chức kiểm tra lại và khắc phục triệt để sự cố;

c) Bảo đảm hệ thống hoạt động bình thường trước khi bàn giao toàn bộ hệ thống cho cơ quan, đơn vị chủ quản;

d) Hướng dẫn đơn vị, cá nhân vận hành hệ thống thông tin, chậm nhất trong vòng 05 ngày, phải hoàn thiện Báo cáo kết thúc ứng phó sự cố theo Mẫu số 04 Phụ lục I ban hành kèm theo Thông tư số 20/2017/TT-BTTTT để báo cáo cơ quan chủ quản hệ thống thông tin và Đội ứng cứu sự cố.

5. Thường trực Đội ứng cứu sự cố phải lưu trữ thông báo sự cố và biên bản xử lý, khắc phục sự cố; lưu trữ thông báo điều phối và báo cáo kết quả thực hiện xử lý, khắc phục sự cố trong thời gian tối thiểu hai (02) năm, bao gồm các thông tin sau:

a) Nội dung thông báo (hoặc báo cáo ban đầu sự cố mạng), thời gian tiếp nhận, thời gian gửi xác nhận thông báo (hoặc báo cáo) sự cố;

b) Nguyên nhân gây ra, thời gian, kết quả và danh sách tổ chức, cá nhân tham gia phối hợp xử lý, khắc phục sự cố;

c) Báo cáo kết thúc ứng phó sự cố của đơn vị, cá nhân vận hành hệ thống thông tin bị sự cố.

Chương IV
TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Điều 10. Thường trực Đội ứng cứu sự cố

1. Là đầu mối liên lạc, tiếp nhận phản ánh, thông báo sự cố; giúp Đội trưởng Đội ứng cứu sự cố chủ động điều phối hoạt động ứng cứu sự cố trên địa bàn tỉnh và thực hiện lệnh điều phối từ Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT); bảo đảm liên lạc thông suốt 24 giờ/ngày và 07 ngày/tuần.

2. Chủ trì, phối hợp với các thành viên Đội ứng cứu sự cố tham mưu xây dựng và triển khai kế hoạch hoạt động của Đội; tổ chức hội thảo, hội nghị phổ biến, trao đổi thông tin, tập huấn, bồi dưỡng, đào tạo, huấn luyện, diễn tập về an toàn thông tin mạng và ứng cứu sự cố; thông báo kết quả tham gia hoạt động của thành viên Đội ứng cứu sự cố cho cơ quan, đơn vị chủ quản để phối hợp quản lý; thực hiện chế độ báo cáo theo quy định.

3. Tham mưu công tác thông tin, tuyên truyền về an toàn thông tin mạng và hoạt động ứng cứu sự cố. Tổng hợp, cập nhật, chia sẻ thông tin cảnh báo về các lỗ hổng, điểm yếu bảo mật, các nguy cơ sự cố và các biện pháp phòng ngừa, ngăn chặn, xử lý trên Diễn đàn thông tin điện tử ứng cứu sự cố của tỉnh.

4. Theo dõi, cập nhật, thông báo kịp thời thông tin liên hệ của thành viên Đội ứng cứu sự cố và đầu mối liên hệ, phối hợp ứng cứu sự cố của các cơ quan, đơn vị, địa phương. Đề xuất việc kiện toàn lực lượng và bố trí phương tiện, thiết bị để bảo đảm thực hiện nhiệm vụ của Đội ứng cứu sự cố.

5. Tham mưu lập dự toán, quản lý và sử dụng kinh phí được cấp hàng năm cho hoạt động của Đội ứng cứu sự cố theo các quy định hiện hành.

Điều 11. Đội trưởng Đội ứng cứu sự cố

1. Chịu trách nhiệm về toàn bộ hoạt động của Đội ứng cứu sự cố, kịp thời báo cáo, đề xuất UBND tỉnh xem xét, chỉ đạo, giải quyết những vấn đề vượt thẩm quyền.

2. Tổ chức phân công nhiệm vụ cho Đội phó và thành viên Đội ứng cứu sự cố. Chủ trì xây dựng, triển khai Kế hoạch hoạt động hàng năm và triệu tập các cuộc họp định kỳ, đột xuất của Đội. Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối.

3. Chủ trì tổ chức, điều phối, phân công các thành viên trong Đội tham gia ứng cứu khi có sự cố xảy ra trên địa bàn tỉnh. Là đầu mối liên hệ, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), các doanh nghiệp cung cấp dịch vụ Internet và các đơn vị liên quan.

Điều 12. Đội phó Đội ứng cứu sự cố

1. Giúp Đội trưởng điều hành các hoạt động của Đội ứng cứu sự cố, chịu trách nhiệm trước Đội trưởng về nhiệm vụ được giao. Đề xuất các giải pháp xây

dựng lực lượng và các biện pháp kỹ thuật, công nghệ để tăng cường chất lượng, hiệu quả công tác ứng cứu sự cố trên địa bàn tỉnh.

2. Chỉ đạo thành viên của Đội ứng cứu sự cố trong các hoạt động phòng ngừa, ngăn chặn, xử lý và khắc phục sự cố an toàn thông tin theo thẩm quyền và nhiệm vụ được phân công. Thay mặt Đội trưởng điều hành hoạt động của Đội khi được ủy quyền.

3. Thực hiện các nhiệm vụ do Đội trưởng phân công và tham gia xây dựng kế hoạch hoạt động hàng năm của Đội ứng cứu sự cố.

Điều 13. Các thành viên Đội ứng cứu sự cố

1. Tham mưu cho Thủ trưởng cơ quan, đơn vị xây dựng và triển khai thực hiện Kế hoạch, phương án ứng phó sự cố bảo đảm an toàn thông tin tin mạng; chịu trách nhiệm thường trực công tác ứng cứu sự cố tại cơ quan, đơn vị công tác.

2. Tổ chức thực hiện nhiệm vụ do Đội trưởng Đội ứng cứu sự cố giao, kịp thời báo cáo, đề xuất giải quyết những khó khăn, vướng mắc trong quá trình thực hiện nhiệm vụ cho Đội trưởng hoặc Đội phó để có sự chỉ đạo, hướng dẫn, hỗ trợ.

3. Thường xuyên theo dõi các cảnh báo trên hệ thống Nền tảng điều phối xử lý sự cố (Irlab.vn), giám sát hoạt động của hệ thống thông tin được giao quản lý, kịp thời phát hiện các dấu hiệu bất thường và phản ánh, báo cáo với chủ quản hệ thống thông tin, Đội ứng cứu sự cố tổ chức kiểm tra, triển khai ứng cứu.

4. Tiếp nhận và xử lý các thông báo sự cố hoặc quyết định triệu tập xử lý sự cố của Đội trưởng và Thường trực Đội ứng cứu sự cố. Phối hợp, hỗ trợ thành viên khác của Đội hoặc thành viên của đơn vị, bộ phận liên quan trong hoạt động ứng cứu, khắc phục sự cố trên địa bàn tỉnh.

5. Tham gia đầy đủ các cuộc họp định kỳ, đột xuất và hoạt động ứng cứu sự cố khi có sự điều phối của Đội trưởng Đội ứng cứu sự cố. Cung cấp đầy đủ, chính xác thông tin cá nhân liên quan phục vụ cho việc liên lạc, tổ chức thực hiện nhiệm vụ.

6. Tham gia góp ý, đề xuất xây dựng kế hoạch hoạt động hàng năm của Đội ứng cứu sự cố. Tham dự đầy đủ các chương trình đào tạo, bồi dưỡng, huấn luyện, diễn tập về an toàn thông tin và ứng cứu sự cố do Sở Thông tin và Truyền thông, Đội ứng cứu sự cố tổ chức hoặc cử tham gia.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 14. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì tổ chức, kiểm tra, hướng dẫn Đội ứng cứu sự cố và các cơ quan, đơn vị, địa phương có liên quan thực hiện Quy chế này; kịp thời phát hiện và phối hợp với cơ quan chức năng tham mưu xử lý những trường hợp vi phạm.

2. Căn cứ kết quả hoạt động của mỗi thành viên, Đội ứng cứu sự cố xem xét, đề nghị cấp có thẩm quyền khen thưởng theo quy định./.