| ỦY BAN NHÂN DÂN<br>THÀNH PHỐ ĐỒNG NAI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 66 /KH-UBND | *Đồng Nai, ngày 05 tháng 6 năm 2026* |

# KẾ HOẠCH
## Diễn tập thực chiến an ninh mạng trên địa bàn thành phố Đồng Nai năm 2026

Thực hiện Kế hoạch số 119/KH-UBND ngày 09/3/2026 của UBND tỉnh về chuyển đổi số trong các cơ quan nhà nước tỉnh Đồng Nai năm 2026; Kế hoạch số 200/KH-UBND ngày 17/4/2026 của UBND tỉnh về triển khai công tác đảm bảo an ninh mạng trên địa bàn tỉnh Đồng Nai năm 2026; Chương trình hành động số 13-CTr/TU ngày 02/4/2026 của Tỉnh ủy Đồng Nai về thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường đảm bảo an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị trên địa bàn Đồng Nai;

Ủy ban nhân dân thành phố Đồng Nai xây dựng Kế hoạch diễn tập thực chiến an mạng trên địa bàn thành phố Đồng Nai năm 2026 như sau:

### I. MỤC ĐÍCH, YÊU CẦU

#### 1. Mục đích

- Cập nhật, nâng cao kiến thức, kỹ năng, năng lực chuyên môn và thực chiến của Đội Ứng cứu sự cố và đơn vị vận hành hệ thống thông tin, tăng cường khả năng phát hiện, ngăn chặn, xử lý tấn công mạng cho các tình huống phổ biến hiện nay và theo thực tiễn.

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn thành phố, tăng cường bảo vệ cho hệ thống thông tin và giúp tuyên truyền cho cơ quan, tổ chức, cán bộ, công chức về vai trò và ý nghĩa của công tác đảm bảo an toàn thông tin mạng.

- Kịp thời phát hiện các điểm yếu, lỗ hổng bảo mật về công nghệ, quy trình, con người nhằm đề ra các giải pháp phù hợp để đảm bảo an toàn thông tin cho hệ thống. Giúp đội ứng cứu sự cố có kinh nghiệm xử lý sự cố đối với các hệ thống đang vận hành, từng bước nâng cao năng lực thực chiến.

- Đánh giá được năng lực của đơn vị giám sát hệ thống, năng lực ứng cứu sự cố của thành viên mạng lưới. Phát huy vai trò, cải thiện năng lực cho đội ứng cứu sự cố.

#### 2. Yêu cầu

- Nội dung diễn tập phải cập nhật các kiến thức, công nghệ, chuẩn an toàn thông tin mới nhất theo tiêu chuẩn quốc gia (TCVN), quy định của Bộ Công an, Bộ Khoa học và Công nghệ, các mô hình tấn công - phòng thủ hiện hành. Bảo đảm tính thực tiễn, chuyên sâu, tập trung vào các kỹ năng cần thiết cho lực lượng nòng cốt của thành phố như: Giám sát và phân tích nhật ký, phân tích mã độc,

phân tích hành vi bất thường; Điều tra số (Digital Forensics), truy vết và xử lý sự cố; Kỹ năng phát hiện và xử lý các hình thức tấn công phổ biến: APT, DDoS, phishing, khai thác lỗ hổng zero-day, chiếm quyền điều khiển hệ thống.

- Diễn tập sẽ tổ chức đồng thời cả hai phương thức:

+ Diễn tập trên hệ thống thật, không có kịch bản trước nhưng được giới hạn về mục tiêu, đối tượng tham gia, công cụ sử dụng, mức độ khai thác và khoảng thời gian diễn ra nhằm giảm thiểu rủi ro cho hệ thống.

+ Diễn tập theo tình huống, dựa trên các giả định và/hoặc tình huống thực tế đã xảy ra nhằm huấn luyện cho cán bộ tham gia các kỹ năng phát hiện, phân tích và ứng phó các sự cố đa dạng hơn như tấn công APT, mã độc, khai thác lỗ hổng nghiêm trọng,…

- Chuẩn bị kỹ lưỡng, bài bản, sẵn sàng các phương án bảo vệ nhằm giảm thiểu rủi ro, bảo đảm hệ thống luôn được an toàn trong quá trình diễn tập; phải xác định rõ hệ thống là mục tiêu diễn tập, công cụ, kỹ thuật được sử dụng để không gây hậu quả nghiêm trọng hoặc hậu quả xảy ra trong giới hạn cho phép; xây dựng phương án dự phòng xử lý rủi ro và sẵn sàng ứng cứu khi xảy ra sự cố trong quá trình diễn tập.

- "Đội tấn công" và "Đội phòng thủ" đảm bảo đủ năng lực và có trách nhiệm thực hiện đúng, đầy đủ các nguyên tắc trong diễn tập thực chiến.

## II. NỘI DUNG DIỄN TẬP THỰC CHIẾN

### 1. Đại biểu khách mời:

- Đại diện lãnh đạo UBND thành phố.

- Đại diện Ban Giám đốc Công an thành phố.

- Đại diện lãnh đạo Sở khoa học và Công nghệ.

- Đại diện lãnh đạo Văn phòng Thành ủy.

**2. Đối tượng tham gia:** Dự kiến khoảng 200 người.

- Thành viên Đội Ứng cứu sự cố được thành lập theo Quyết định số 61/QĐ-UBND ngày 08/5/2026 của Ủy ban nhân dân thành phố *(151 người)*.

- 01 cán bộ chuyên trách công nghệ thông tin của các Sở, ban, ngành *(14 người)*.

- 01 cán bộ làm công tác liên quan đến đảm bảo an ninh mạng tại các phòng của Công an thành phố *(26 đồng chí)*.

- Lãnh đạo, chỉ huy, cán bộ làm công tác, theo dõi Công nghệ thông tin, An ninh mạng phòng PV01 *(04 người)*.

- Các chuyên gia an ninh mạng, cán bộ kỹ thuật chuyên môn các tỉnh, thành phố lân cận *(05 người)*.

### 2. Nội dung diễn tập

### 2.1. Hệ thống thông tin được sử dụng để diễn tập

***Diễn tập thực chiến:*** Dự kiến thực hiện trên Hệ thống thông tin giải quyết thủ tục hành chính thành phố do Sở Khoa học và Công nghệ quản lý vận hành, nhằm kiểm tra thực tế khả năng phòng thủ, giám sát, phát hiện và ứng phó sự cố an ninh mạng trong điều kiện vận hành thực tế của hệ thống. Sở Khoa học và Công nghệ sẽ lựa chọn hệ thống thông tin cấp độ 3 làm mục tiêu diễn tập.

***Diễn tập mô phỏng:*** Tổ chức diễn tập theo kịch bản giả định trên môi trường mô phỏng được xây dựng với kiến trúc và chức năng tương đồng các hệ thống thông tin đang quản lý, vận hành nhằm chủ động rà soát, đánh giá, phát hiện lỗ hổng bảo mật và điểm yếu kỹ thuật trong hạ tầng mạng; nhận diện, phát hiện sớm các dấu hiệu, hành vi tấn công mạng; thực hành cơ chế phối hợp, quy trình ứng cứu, xử lý và khắc phục sự cố, qua đó nâng cao năng lực phòng thủ, khả năng phát hiện sớm, ứng phó kịp thời và bảo đảm an toàn, an ninh cho hệ thống thông tin.

**2.2. Nguyên tắc diễn tập theo hình thức thực chiến**

***a) Nguyên tắc chung***

Các "Đội tấn công" và "Đội phòng thủ" không được phép trao đổi thông tin liên quan đến việc tấn công và bảo vệ suốt thời gian diễn tập, trừ trường hợp có yêu cầu từ Ban Tổ chức.

***b) Nguyên tắc tấn công***

- Tuân thủ thời gian bắt đầu, kết thúc diễn tập.

- Cho phép sử dụng nhiều kỹ thuật khác nhau (bao gồm dò tìm tài khoản, khai thác lỗ hổng bảo mật, lừa đảo qua Email,...); sử dụng các công cụ mã nguồn đóng, mở, công cụ chiếm quyền điều khiển hệ thống, công cụ khai thác lỗ hổng ứng dụng; các công cụ sử dụng phải đảm bảo không gây nguy hại đến hoạt động của hệ thống.

- Cho phép khai thác lỗ hổng bảo mật trên ứng dụng, Hệ thống thông tin cũng như hệ thống và hạ tầng mạng nằm trong phạm vi diễn tập.

- Cho phép thực hiện tấn công Phishing để khai thác, thu thập thông tin từ người dùng nội bộ, phục vụ cho việc diễn tập tấn công.

- Không sử dụng các hình thức tấn công từ chối dịch vụ (DDoS) bằng cách làm nghẽn băng thông mạng; không được thực thi các mã khai thác mà có thể gây khởi động lại hoặc làm gián đoạn quá trình hoạt động của máy chủ dịch vụ; không được tấn công hệ thống không thuộc giới hạn, mục tiêu diễn tập; không sử dụng hệ thống nằm trong giới hạn, mục tiêu diễn tập để làm bàn đạp tấn công sang các hệ thống khác không thuộc giới hạn, mục tiêu diễn tập; không được phép thực hiện tấn công làm thay đổi giao diện của Website/Cổng thông tin; không sử dụng hoặc hạn chế sử dụng các công cụ rà quét (scan) có thể dẫn đến treo hệ thống.

- Nghiêm cấm thực hiện việc phá hủy hệ thống và dữ liệu; sử dụng các lỗi trên ứng dụng website để phát tán mã độc; sử dụng các loại mã độc trong quá trình diễn tập như mã độc mã hoá dữ liệu, tống tiền, phần mềm gián điệp và các loại mã độc hại khác gây ảnh hưởng nghiêm trọng đến hệ thống; nghiêm cấm việc lưu

lại phần mềm, công cụ trên hệ thống bị xâm nhập để phục vụ cho các mục đích khác không liên quan đến diễn tập.

- Cấm đánh cắp, chia sẻ làm lộ lọt thông tin. Chỉ được phép chia sẻ các thông tin về kết quả của việc tấn công cho Ban Tổ chức.

- Nếu mỗi "Đội tấn công" phát hiện được lỗ hổng thì không được phép khai thác nhiều lần một lỗ hổng, tránh trường hợp phát sinh nhiều giao dịch để giảm thiểu việc xử lý đối soát dữ liệu sau quá trình diễn tập.

***c) Nguyên tắc phòng thủ***

- Cho phép triển khai các hệ thống Honeypot (là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật) để đánh lạc hướng các "Đội tấn công".

- Cho phép dải địa chỉ IP của các "đội tấn công" được truy cập tới các mục tiêu tấn công thông qua các cổng dịch vụ mà tổ chức đang cung cấp.

- Thông báo dừng thực hiện khai thác khi có yêu cầu của Ban Tổ chức.

- Thực hiện các biện pháp kỹ thuật, nghiệp vụ để giám sát, phát hiện và đánh chặn tấn công.

- Cho phép chặn địa chỉ IP gửi quá nhiều gói tin trong một khoảng thời gian (theo yêu cầu của Ban Tổ chức), để đảm bảo các đội còn lại không bị mất kết nối đến hệ thống mục tiêu.

- Theo dõi, giám sát, ngăn chặn các "Đội tấn công" vi phạm các nguyên tắc tấn công được quy định tại Kế hoạch này.

- Ghi nhận và theo dõi "Đội tấn công" đã tấn công thành công mục tiêu.

**2.3. Nguyên tắc diễn tập theo hình thức mô phỏng**

***a) Nguyên tắc chung***

- Hệ thống thông tin phục vụ diễn tập được xây dựng để đáp ứng kịch bản mô phỏng.

- Bằng chứng phục vụ kiểm tra, phân tích sẽ tự thu thập trên hệ thống mô phỏng hoặc được Ban Tổ chức cung cấp

- Các cá nhân hoặc các đội tham gia diễn tập thực hiện các yêu cầu từ kịch bản.

***b) Phương thức triển khai***

- Các thành viên tham gia sẽ được Ban Tổ chức sắp xếp và bố trí theo các đội.

- Các đội thực hiện các yêu cầu của kịch bản, trả lời kết quả nhanh và chính xác theo hình thức CTF (Capture The Flag) hoặc trả lời bằng hình thức báo cáo kết quả.

- Ban Tổ chức sẽ bố trí thời gian để các đội trình bày báo cáo nếu kịch bản có yêu cầu.

**2.4. Hình thức, thời gian, địa điểm**

***a) Hình thức***

Thực hiện trực tiếp và trực tuyến. Việc tấn công mục tiêu được các "Đội tấn công" thực hiện trực tuyến qua Internet từ bất kỳ nơi nào trong lãnh thổ Việt Nam. Việc bảo vệ mục tiêu được thực hiện theo hình thức tập trung và giám sát bảo vệ từ xa.

***b) Thời gian:*** Trong 05 ngày (dự kiến tháng 9/2026).

***c) Địa điểm:*** Dự kiến tại Công an thành phố Đồng Nai (Địa chỉ: Đường Trần Quốc Toản, phường Trấn Biên, thành phố Đồng Nai)

**3. Quy trình tổ chức diễn tập**

**- Bước 1:** Thông qua Quyết định thành lập Ban Giám khảo diễn tập.

**- Bước 2:** Ban Tổ chức thực hiện xác định giới hạn diễn tập và ban hành nội quy diễn tập.

**- Bước 3:** Ban Tổ chức triển khai diễn tập, công bố giới hạn, mục tiêu diễn tập, danh sách các đội tham gia, thời gian bắt đầu và thời gian kết thúc diễn tập.

**- Bước 4:**

+ Bước 4.1: Các Đội sẽ thực hiện phân tích điều tra và giải quyết các yêu cầu của Ban Tổ chức đối với hình thức diễn tập mô phỏng theo kịch bản.

+ Bước 4.2: Các "Đội tấn công", "Đội phòng thủ" thực hiện diễn tập thực chiến; Ban Tổ chức theo dõi, tổng hợp, đánh giá, xử lý vi phạm và các sự cố phát sinh trong khi diễn tập.

**- Bước 5:** Ban Giám khảo đánh giá kết quả sau khi kết thúc diễn tập dựa trên nội quy diễn tập thực chiến và báo cáo của các đội.

**- Bước 6:** Ban Tổ chức công bố kết quả diễn tập, đánh giá hoạt động diễn tập và tổ chức bế mạc diễn tập.

**- Bước 7:** Ban Tổ chức tổng hợp, gửi báo cáo kết quả diễn tập về Ủy ban nhân dân thành phố và Trung tâm An ninh mạng quốc gia - Bộ Công an.

**4. Nhiệm vụ của Ban Tổ chức, Ban Giám khảo và các đội tham gia**

***4.1. Nhiệm vụ của Ban Tổ chức***

- Chủ trì điều phối, bảo đảm việc thực hiện các nội dung nhiệm vụ của Ban Giám khảo, các đội tham gia diễn tập theo Kế hoạch.

- Chuẩn bị các chủ đề, nội dung yêu cầu cho hình thức diễn tập mô phỏng theo kịch bản.

***4.2. Nhiệm vụ của Ban Giám khảo***

- Công bố phương thức đánh giá, xếp loại các Đội tham gia.

- Thực hiện đánh giá công bằng, khách quan các "Đội tấn công", "Đội phòng thủ" dựa trên tổng hợp báo cáo do Ban Tổ chức cung cấp; gửi kết quả đánh giá về Ban Tổ chức.

- Tuân thủ các yêu cầu bảo mật thông tin (về lỗ hổng, điểm yếu hệ thống và các thông tin nhạy cảm khác) trong và sau thời gian diễn tập.

***4.3. Nhiệm vụ của "Đội tấn công"***

- Đăng ký thông tin về thành viên tham dự theo yêu cầu của Ban Tổ chức, thông tin về địa chỉ IP được sử dụng để diễn tập cho Ban Tổ chức.

- Phân công vai trò, trách nhiệm mỗi đội, mỗi thành viên trong đội thực hiện việc tấn công mục tiêu theo hướng dẫn và nội quy của Ban Tổ chức.

- Sử dụng tùy chọn các công cụ, kỹ thuật khác nhau (technical và nontechnical) hoặc các công cụ, kỹ thuật theo quy định của Ban Tổ chức quy định cụ thể để khai thác lỗ hổng bảo mật, tấn công hệ thống.

- Lưu vết và đưa ra các bằng chứng (evidences) tấn công.

- Tuân thủ theo thời gian bắt đầu và thời gian kết thúc tấn công do Ban Tổ chức đưa ra.

- Hạn chế hoặc không sử dụng các công cụ rà quét (scan) có thể dẫn đến hỏng hoặc treo hệ thống.

- Tuân thủ nội quy, nguyên tắc khi thực hiện tấn công.

- Báo cáo về Ban Tổ chức phương pháp, tên công cụ và kết quả của việc tấn công (bao gồm cả các điểm yếu nghiêm trọng và không nghiêm trọng) theo các quy tắc: Đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

- Cam kết tuân thủ bảo mật thông tin và các yêu cầu khác của Ban Tổ chức.

***4.4. Nhiệm vụ của "Đội phòng thủ"***

- Tổ chức phòng thủ phải đảm bảo yêu cầu quy trình ứng phó sự cố, bảo đảm an toàn thông tin mạng theo hướng dẫn tại Quyết định số 05/2017/QĐ-TTg ngày 13/3/2017 của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Phân công vai trò, trách nhiệm mỗi thành viên, nhóm liên quan thực hiện công tác phòng thủ theo hướng dẫn và quy định của Ban Tổ chức.

- Rà soát và thực thi tăng cường phương án dự phòng, sao lưu dữ liệu và hệ thống trước khi bắt đầu thực hiện diễn tập.

- Theo dõi các hoạt động dò quét, thăm dò, khai thác lỗ hổng trên hệ thống mục tiêu được lựa chọn tổ chức diễn tập.

- Thực hiện các phân tích, điều tra chuyên sâu các hoạt động liên quan đến tấn công, xâm nhập hệ thống.

- Rà soát và thực thi tăng cường phương án giám sát hệ thống mục tiêu diễn tập thực chiến (bao gồm cả các hệ thống nằm ngoài mục tiêu diễn tập), phát hiện khi các hệ thống bị tấn công nằm ngoài giới hạn, phạm vi diễn tập. Báo cáo Ban Tổ chức khi phát hiện các vi phạm của các "Đội tấn công" vi phạm nội quy.

- Thực hiện các biện pháp khắc phục sự cố, vá lỗ hổng, điểm yếu được phát hiện.

- Lưu giữ các nhật ký, dữ liệu, bằng chứng bảo vệ hệ thống trong quá trình diễn tập.

- Ngăn chặn địa chỉ IP, nguồn tấn công nếu thấy gây phương hại hoặc ảnh hưởng đến hoạt động bình thường của hệ thống.

- Báo cáo về Ban Tổ chức kết quả của việc giám sát, phát hiện, ngăn chặn theo quy tắc: đúng thời hạn và bảo vệ kết quả báo cáo bằng việc mã hóa hoặc đặt mật khẩu.

- Tuân thủ bảo mật thông tin và các yêu cầu khác của Ban Tổ chức.

## III. KINH PHÍ THỰC HIỆN

Công an thành phố chủ trì, phối hợp với các đơn vị liên quan lập dự toán kinh phí thực hiện. Trên cơ sở đề xuất của Công an thành phố, Sở Tài chính tổng hợp nhu cầu sử dụng, căn cứ khả năng ngân sách của thành phố báo cáo cấp có thẩm quyền xem xét, bố trí kinh phí thực hiện theo quy định hiện hành.

## IV. TỔ CHỨC THỰC HIỆN

### 1. Công an thành phố

- Chủ trì triển khai thực hiện các nội dung Kế hoạch nhằm đạt được các mục tiêu đề ra. Chủ trì, phối hợp các đơn vị có liên quan lựa chọn các thành viên có năng lực, kinh nghiệm để tham gia Ban Tổ chức, Ban Giám khảo, "Đội phòng thủ", "Đội tấn công" và ký Quyết định thành lập các Ban, Đội để phục vụ công tác diễn tập. Xây dựng kế hoạch, chương trình diễn tập, nội quy diễn tập thực chiến an ninh mạng.

- Chuẩn bị kịch bản và hệ thống diễn tập theo các tình huống.

- Quyết định hệ thống thông tin sẽ chọn là mục tiêu diễn tập thực chiến.

- Cử lực lượng tại chỗ (lực lượng nội bộ), thành viên Đội Ứng cứu sự cố của thành phố và các chuyên gia bảo mật an toàn thông tin đang cung cấp dịch vụ giám sát, đảm bảo an ninh mạng của thành phố tham gia vào hoạt động phòng thủ.

- Hướng dẫn các "Đội tấn công" và "Đội phòng thủ" thực hiện bảo mật thông tin liên quan đến diễn tập theo quy định được Ban Tổ chức đưa ra.

- Chỉ đạo, tổ chức, giám sát diễn tập đúng quy định như trong nội quy, cho phép chặn các địa chỉ IP gửi quá nhiều gói tin trong một khoảng thời gian, nếu xét thấy có nguy cơ làm ảnh hưởng đến hoạt động hoặc kết nối bình thường đến hệ thống; không cho phép "Đội tấn công" và "Đội phòng thủ" trao đổi thông tin

liên quan đến việc tấn công và bảo vệ hệ thống mục tiêu trong suốt thời gian diễn tập (trừ trường hợp có yêu cầu của Ban Tổ chức).

- Tiếp nhận, tổng hợp kết quả báo cáo của các "Đội tấn công", "Đội phòng thủ" và gửi kết quả diễn tập và theo dõi quá trình diễn tập của mỗi Đội cho Ban Giám khảo thực hiện đánh giá.

- Báo cáo Chủ quản hệ thống thông tin thực hiện khắc phục, vá những lỗ hổng do các "Đội tấn công" phát hiện được trong quá trình diễn tập.

- Báo cáo tình hình diễn tập và đánh giá kết quả về Ủy ban nhân dân thành phố và Trung tâm An ninh mạng quốc gia - Bộ Công an.

- Phối hợp Sở Tài chính và các đơn vị liên quan dự trù kinh phí thực hiện và quyết toán đúng quy định.

- Chủ trì thực hiện đầy đủ các thủ tục lựa chọn nhà thầu theo quy định của pháp luật; tổ chức ký kết các hợp đồng kinh tế và triển khai các nội dung liên quan phục vụ công tác diễn tập theo Kế hoạch này.

**2. Sở Khoa học và Công nghệ**

- Bảo đảm duy trì hoạt động của hệ thống thông tin được sử dụng để diễn tập; lên phương án phòng ngừa rủi ro, ứng cứu sự cố; chịu trách nhiệm trong thực hiện đảm bảo an toàn cho hệ thống trong quá trình diễn tập, dựng hệ thống song song hoặc sao lưu lại hệ thống trước khi diễn tập.

- Phân công đơn vị vận hành hệ thống mail công vụ và nhân sự có liên quan để thực hiện nhiệm vụ của "Đội phòng thủ".

- Phối hợp với Công an thành phố thực hiện các nội dung, nhiệm vụ:

+ Hướng dẫn các "Đội tấn công" và "Đội phòng thủ" thực hiện bảo mật thông tin liên quan đến diễn tập theo quy định được Ban Tổ chức đề ra.

+ Xây dựng kế hoạch, chương trình diễn tập cụ thể, rõ ràng, chỉ công bố cho các bên liên quan.

+ Xây dựng và phổ biến nội quy diễn tập thực chiến an ninh mạng.

+ Chỉ đạo, tổ chức, giám sát diễn tập đúng quy định như trong nội quy, cho phép chặn các địa chỉ IP gửi quá nhiều gói tin trong một khoảng thời gian, nêu xét thấy có nguy cơ làm ảnh hưởng đến hoạt động hoặc kết nối bình thường đến hệ thống; không cho phép "Đội tấn công" và "Đội phòng thủ" trao đổi thông tin liên quan đến việc tấn công và bảo vệ hệ thống mục tiêu trong suốt thời gian diễn tập (trừ trường hợp có yêu cầu của Ban Tổ chức).

**3. Sở Tài chính**

Căn cứ khả năng ngân sách của thành phố và đề xuất của Công an thành phố, Sở Tài chính tổng hợp nhu cầu sử dụng báo cáo cấp có thẩm quyền xem xét, bố trí kinh phí thực hiện theo quy định hiện hành.

**4. Các Sở, ban, ngành, UBND các xã, phường**

Phân công đại biểu tham gia Khai mạc và Bế mạc diễn tập thực chiến đảm bảo an toàn thông tin; quan tâm bố trí, tạo điều kiện cho các cán bộ, công chức, viên chức là thành viên Đội Ứng cứu sự cố tham gia đào tạo và diễn tập theo thời gian và nội quy của Ban Tổ chức.

**5. Đội Ứng cứu sự cố an toàn thông tin mạng thành phố**

Thành viên Đội Ứng cứu sự cố được thành lập theo Quyết định số 61/QĐ-UBND ngày 08/5/2026 của Ủy ban nhân dân thành phố tham gia đầy đủ các hoạt động, chương trình theo Kế hoạch.

Trên đây là Kế hoạch diễn tập thực chiến an ninh mạng thành phố Đồng Nai năm 2026, yêu cầu Thủ trưởng các Sở, ban, ngành; Chủ tịch UBND các xã, phường và các tổ chức, cá nhân có liên quan nghiêm túc thực hiện. Trong quá trình thực hiện, nếu có vướng mắc, khó khăn, đề nghị các tổ chức, cá nhân liên hệ Công an thành phố *(qua phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Thượng tá Trương Minh Trung, số điện thoại: 0938.018.280, Email: trungtm.cat@dongnai.gov.vn)* để tổng hợp, tham mưu Ủy ban nhân dân thành phố chỉ đạo, giải quyết./.

***Nơi nhận:***
- Bộ Công an (báo cáo);
- Cục A05 - BCA (theo dõi);
- Thường trực Thành ủy;
- Thường trực HĐND thành phố;
- Chủ tịch, các PCT UBND thành phố;
- Chánh Văn phòng Thành ủy;
- Các Sở, ban, ngành;
- TV Đội Ứng cứu sự cố ATTT mạng thành phố (QĐ số 61/QĐ-UBND ngày 08/5/2026);
- Chánh, các PCVP UBND thành phố;
- UBND các xã, phường;
- Lưu: VT, KGVX, HCTC, QTTV, HCC, NC.

**KT. CHỦ TỊCH**
**PHÓ CHỦ TỊCH**

ỦY BAN NHÂN DÂN THÀNH PHỐ ĐỒNG NAI

**Lê Trường Sơn**