

KẾ HOẠCH

Diễn tập ứng cứu sự cố an ninh mạng thành phố Huế năm 2026

Căn cứ Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư Trung ương Đảng về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị; Chương trình hành động số 27-CTr/TU ngày 10/3/2026 của Ban Thường vụ Thành ủy Huế về việc thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025; Kế hoạch số 226/KH-UBND ngày 17/4/2026 của Ủy ban nhân dân thành phố Huế về việc triển khai Chương trình hành động thực hiện Chỉ thị số 57-CT/TW; Kế hoạch số 51/KH-UBND ngày 26/01/2026 của Ủy ban nhân dân thành phố Huế về việc triển khai công tác bảo đảm an ninh mạng, an toàn thông tin trên địa bàn thành phố Huế năm 2026; Kế hoạch số 02-KH/TBANM ngày 17/8/2026 của Tiểu ban An ninh mạng thành phố Huế về hoạt động của Tiểu ban An ninh mạng thành phố Huế trong 06 tháng cuối năm 2026, Ủy ban nhân dân thành phố Huế ban hành Kế hoạch diễn tập ứng cứu sự cố an ninh mạng thành phố Huế năm 2026, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Rà soát, thực nghiệm tình huống, đánh giá công tác phối hợp xử lý ứng cứu sự cố an ninh mạng, an ninh dữ liệu, bảo mật thông tin giữa các lực lượng, đơn vị chuyên môn trên địa bàn thành phố Huế.

- Nâng cao kỹ năng xử lý tình huống của đội ứng cứu sự cố, đơn vị chuyên trách về an ninh mạng, an ninh dữ liệu, bảo mật thông tin; củng cố kiến thức, kinh nghiệm, sẵn sàng ứng cứu, xử lý khi có các tình huống, sự cố tấn công hệ thống trong thực tế; rà soát công cụ, phần mềm phục vụ quá trình xử lý, ứng cứu sự cố, từ đó đánh giá, định hướng mua, trang cấp các thiết bị trong thời gian tới đảm bảo với tình hình thực tiễn tại địa phương.

- Nhằm đánh giá, rà soát quy trình, tổ chức, cách điều phối, phối hợp ứng cứu giữa các đơn vị, thành viên đội ứng cứu sự cố an toàn thông tin và các đơn vị, địa phương trên địa bàn thành phố.

2. Yêu cầu

- Diễn tập sát với các tình huống tấn công mạng thường xảy ra trên thực tế, phù hợp với tình hình vận hành thực tiễn của các hệ thống thông tin trên địa bàn; tập trung vào các ứng dụng dự kiến sẽ được triển khai, áp dụng cho các hệ thống thông tin trên địa bàn trong thời gian tới, đặc biệt là các ứng dụng mới như trí tuệ nhân tạo (AI)...

- Xây dựng kịch bản diễn tập phải chi tiết, cụ thể từng bước để các thành phần tham gia diễn tập nắm rõ quy trình, phương thức, thủ đoạn tấn công của

các đối tượng tin tặc, quy trình ứng phó sự cố an ninh mạng và sử dụng thành thạo các phần mềm dùng trong quá trình điều tra, xử lý, ứng cứu sự cố bảo đảm đúng quy định.

- 100% cơ quan, đơn vị tham gia diễn tập nắm được quy trình phát hiện, báo cáo, phối hợp xử lý sự cố an ninh mạng theo kịch bản.

- Quá trình thực hiện bảo đảm theo quy trình, hướng dẫn của cấp trên về diễn tập an ninh mạng, an toàn thông tin; các hệ thống thông tin được sử dụng trong quá trình diễn tập phải được tách riêng biệt không gây ảnh hưởng đến các hệ thống thông tin đang vận hành; thành viên tham gia diễn tập chấp hành nghiêm túc quy định về bảo mật thông tin, nghiêm cấm các đội tham gia chia sẻ thông tin liên quan đến nội dung diễn tập cho các cá nhân, đơn vị khác hoặc sử dụng kết quả diễn tập phục vụ mục đích khác.

II. NỘI DUNG

Diễn tập ứng cứu sự cố an ninh mạng, an ninh dữ liệu, bảo mật thông tin thành phố Huế năm 2026 được tổ chức với 02 cuộc diễn tập, nội dung chính như sau:

1. Chủ đề diễn tập

- Cuộc diễn tập thứ nhất: Diễn tập ứng cứu sự cố an ninh mạng mô phỏng tình huống mã độc thu thập, đánh cắp thông tin bị tán phát trong hệ thống máy tính công vụ của Trung tâm Phục vụ hành chính công của Ủy ban nhân dân cấp xã.

- Cuộc diễn tập thứ hai: Diễn tập tấn công, phòng thủ và bảo đảm an ninh mạng, an ninh dữ liệu, bảo mật thông tin đối với việc triển khai ứng dụng hệ thống AI (LLM) nội bộ.

2. Hình thức diễn tập

- Cuộc diễn tập thứ nhất: Lựa chọn 01 Trung tâm Phục vụ hành chính công của Ủy ban nhân dân cấp xã triển khai trực tiếp diễn tập tình huống, các đơn vị có liên quan sẽ triển khai theo kịch bản.

- Cuộc diễn tập thứ hai: Tổ chức theo hình thức ứng cứu thử thách theo chủ đề (Capture The Flag - CTF) trực tiếp tại hội trường. Các đội tham gia sẽ giải quyết chuỗi tình huống về tấn công, phòng thủ và bảo đảm an ninh mạng, an ninh dữ liệu từ khâu xây dựng, triển khai, vận hành hệ thống AI (LLM) nội bộ.

3. Kịch bản diễn tập

3.1. Diễn tập ứng cứu sự cố an ninh mạng mô phỏng tình huống mã độc tán phát trong hệ thống máy tính công vụ (cuộc Diễn tập thứ nhất)

a) Tình huống giả định:

Trong quá trình thực hiện công vụ, một cán bộ phục vụ giải quyết thủ tục hành chính đã sử dụng thiết bị ngoại vi lạ (*USB thương mại*) để thực hiện việc sao chép dữ liệu từ bên ngoài vào máy tính công vụ. Thiết bị ngoại vi có chứa mã độc thu thập, đánh cắp thông tin và đã vượt qua các biện pháp bảo vệ của máy tính công vụ (phần mềm diệt virus) để cài đặt vào máy tính. Mã độc sau khi xâm nhập vào máy tính đã tiếp tục lây nhiễm đến các máy tính công vụ khác trong hệ thống mạng của đơn vị và tiến hành chuyển, gửi các thông tin dữ liệu ra

máy chủ điều khiển (C&C) bên ngoài. Sau một khoảng thời gian, cán bộ chuyên trách công nghệ thông tin (CNTT) của đơn vị đã nhận thấy các dấu hiệu máy tính công vụ bị nhiễm mã độc (như: máy tính khởi động chậm, thường xuyên tự mở 1 số trang web lạ, phần mềm diệt virus bị vô hiệu hóa hoạt động...). Ngoài ra, đơn vị quản trị, vận hành hệ thống mạng diện rộng, tập trung CPNet (Trung tâm Giám sát, điều hành đô thị thông minh (IOC) - Sở Khoa học và Công nghệ) qua công tác giám sát cũng đã phát hiện những dấu hiệu nghi vấn bị mã độc khai thác, thực hiện các hành vi nguy hại (như: phát hiện kết nối bất hợp pháp ra các máy chủ độc hại, phát hiện các tài khoản bị lộ thông qua các ứng dụng TI...).

Sau khi tổng hợp các dấu hiệu nghi vấn, cán bộ chuyên trách CNTT của đơn vị đã xác định ban đầu đây là một sự cố về an ninh mạng nghiêm trọng, báo cáo đề xuất lãnh đạo đơn vị kích hoạt hoạt động ứng cứu sự cố an ninh mạng để điều tra, xác minh, xử lý sự cố an ninh mạng trên (bao gồm: lực lượng tại đơn vị, Trung tâm IOC, Công an thành phố và Đội ứng cứu sự cố an ninh mạng thành phố Huế).

b) Yêu cầu giải quyết tình huống:

- Đối với Trung tâm Hành chính công của Ủy ban nhân dân cấp xã:
 - + Nhận biết các dấu hiệu ban đầu liên quan máy tính bị nhiễm mã độc;
 - + Công tác tham mưu, báo cáo lãnh đạo đơn vị khi phát hiện sự cố;
 - + Trao đổi, phối hợp với các đơn vị liên quan khi phát hiện sự cố;
 - + Phối hợp xử lý, khôi phục hệ thống sau khi xử lý sự cố.
- Đối với đơn vị quản lý, vận hành hệ thống mạng diện rộng, tập trung:
 - + Sử dụng các hệ thống giám sát an ninh mạng phát hiện các dấu hiệu nghi vấn mã độc khai thác, thực hiện hành vi nguy hại;
 - + Triển khai ngăn chặn ban đầu;
 - + Trao đổi, thông tin, báo cáo các dấu hiệu trên cho đơn vị chủ quản và lực lượng chuyên trách an ninh mạng (*Công an thành phố*);
 - + Phối hợp triển khai xử lý, khôi phục, theo dõi hệ thống sau khi triển khai ứng cứu sự cố.
- Đối với lực lượng chuyên trách an ninh mạng:
 - + Thực hiện việc tiếp nhận thông tin sự cố, phân loại, đánh giá ban đầu đối với sự cố an ninh mạng;
 - + Hướng dẫn đơn vị chủ quản hệ thống và đơn vị quản lý, vận hành hệ thống mạng xử lý các bước ban đầu đối với sự cố;
 - + Thu thập, tiến hành phân tích ban đầu đối với mã độc;
 - + Tiến hành kích hoạt Đội ứng cứu sự cố an ninh mạng thành phố Huế để tiến hành phân tích, đánh giá chuyên sâu đối với sự cố và mã độc;
 - + Chủ trì phối hợp với các đơn vị liên quan khắc phục sự cố an ninh mạng đã xảy ra, theo dõi, giám sát sau khi khôi phục hệ thống;
 - + Tổng hợp báo cáo kết quả, đánh giá tác động, đề xuất Ủy ban nhân dân thành phố triển khai tổng thể các biện pháp để tăng cường công tác bảo đảm

an ninh mạng, an ninh dữ liệu, bảo mật thông tin đối với các hệ thống thông tin trên địa bàn thành phố Huế.

3.2. Diễn tập tấn công, phòng thủ và bảo đảm an ninh mạng, an ninh dữ liệu, bảo mật thông tin đối với việc triển khai ứng dụng hệ thống AI (LLM) nội bộ (cuộc Diễn tập thứ hai)

a) Nội dung tình huống: Một đơn vị trên địa bàn thành phố chuẩn bị triển khai hệ thống AI (LLM) nội bộ để phục vụ triển khai các ứng dụng trên nền tảng AI phục vụ công tác nghiệp vụ của đơn vị. Do chưa có kinh nghiệm trong công tác giám sát, bảo đảm an ninh mạng, an ninh dữ liệu đối với các hệ thống AI nên trong quá trình triển khai hệ thống đã xảy ra một số sự cố về an ninh mạng, cụ thể như sau:

- Nguy cơ từ chuỗi cung ứng và mã độc ẩn khi lựa chọn các mô hình nguồn mở;
- Đầu độc dữ liệu huấn luyện;
- Tấn công đánh cắp mô hình, đảo ngược mô hình;
- Tấn công thao túng câu lệnh;
- Rò rỉ dữ liệu nhạy cảm;
- Đánh cắp danh tính, tài khoản sử dụng AI bất hợp pháp;
- Tấn công DDoS hạ tầng.

b) Yêu cầu giải quyết tình huống:

- Phân tích các nguy cơ, điểm yếu trong các tình huống theo từng bước, từng giai đoạn từ khi bắt đầu xây dựng hệ thống AI;
- Xây dựng, triển khai các biện pháp kỹ thuật nhằm bảo đảm an ninh mạng, an ninh dữ liệu từng giai đoạn;
- Báo cáo sự cố và đề xuất giải pháp khắc phục.

4. Hạ tầng và công cụ phục vụ diễn tập

a) Diễn tập ứng cứu sự cố an ninh mạng mô phỏng tình huống mã độc tán phát trong hệ thống máy tính công vụ

- Hệ thống mạng, máy tính giả lập máy tính công vụ tại Trung tâm Phục vụ hành chính công của Ủy ban nhân dân cấp xã.
- Hệ thống mô phỏng giám sát an ninh mạng tại Trung tâm IOC - Sở Khoa học và Công nghệ.
- Hệ thống máy tính phục vụ công tác điều tra, ứng cứu sự cố an ninh mạng cho lực lượng chuyên trách và Đội ứng cứu sự cố an ninh mạng thành phố.

b) Diễn tập tấn công, phòng thủ và bảo đảm an ninh mạng, an ninh dữ liệu, bảo mật thông tin đối với việc triển khai ứng dụng hệ thống AI (LLM) nội bộ

- Hệ thống máy chủ triển khai CTF: Hệ thống ra đề, chấm điểm, bảng xếp hạng theo thời gian thực (scoreboard real-time).
- Môi trường ảo hóa: tạo hệ thống máy chủ để triển khai hệ thống AI nội bộ, mô hình LLM phù hợp.
- Công cụ hỗ trợ: các phần mềm liên quan phân tích, điều tra chứng cứ số như Wireshark, IDA, Ghidra, VirusTotal, Cuckoo Sandbox, ELK Stack, Outlook Viewer, Email Header Analyzer, VMWare, VirtualBox...

5. Thành phần, nhân sự tham gia diễn tập

a) Ban tổ chức

- Lãnh đạo Ủy ban nhân dân thành phố: Trưởng ban.
- Lãnh đạo Công an thành phố: Phó Trưởng ban.
- Lãnh đạo Sở Khoa học và Công nghệ: Thành viên.
- Lãnh đạo Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố: Thành viên.
- Lãnh đạo Trung tâm Giám sát, điều hành đô thị thông minh - Sở Khoa học và Công nghệ: Thành viên.
- Lãnh đạo các doanh nghiệp cung cấp dịch vụ: Thành viên.

b) Ban giám khảo: Thành viên Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an thành phố Huế; các chuyên gia của các doanh nghiệp, đơn vị cung cấp dịch vụ.

5.3. Thành phần tham gia, thời gian, địa điểm diễn tập

a) Cuộc Diễn tập thứ nhất

- Thành phần: lựa chọn 01 đơn vị Ủy ban nhân dân cấp xã; Trung tâm IOC - Sở Khoa học và Công nghệ; Công an thành phố và một số thành viên trong Đội ứng cứu sự cố an ninh mạng thành phố.

- Thời gian: dự kiến trong tháng 10/2026 (diễn tập 1/2 ngày).

- Địa điểm: tại Ủy ban nhân dân cấp xã được lựa chọn.

b) Cuộc Diễn tập thứ hai

- Thành phần: thành lập các Đội tham gia của các đơn vị trên địa bàn thành phố như sau:

- + Văn phòng Thành ủy;
- + Văn phòng Ủy ban nhân dân thành phố;
- + Sở Khoa học và Công nghệ;
- + Công an thành phố;
- + Bộ Chỉ huy quân sự thành phố;
- + Mời một số cơ quan, doanh nghiệp khác trên địa bàn thành phố, dự kiến thành lập 05 đội tham gia.

- Thời gian: dự kiến trong tháng 11/2026 (phiên chính, khai mạc, báo cáo kết quả cuộc Diễn tập thứ nhất và triển khai diễn tập trong 01 ngày).

- Địa điểm: dự kiến thuê Hội trường tổ chức sự kiện.

6. Giới hạn diễn tập

- Đối với cuộc Diễn tập thứ nhất: thực hiện trên hệ thống độc lập không sử dụng hệ thống thông tin của đơn vị.

- Đối với cuộc Diễn tập thứ hai: xây dựng môi trường ảo hóa giả lập hệ thống.

7. Nhiệm vụ Ban tổ chức, Ban giám khảo và các đội tham gia diễn tập

a) Ban tổ chức:

- Tổ chức họp trực tiếp và trực tuyến khai mạc phổ biến các quy định diễn tập cho các đội tham gia diễn tập nắm và thực hiện.

- Triển khai nhiệm vụ cho các đội tham gia trong thời gian diễn tập.
- Xác định giới hạn và lựa chọn hệ thống thông tin diễn tập đảm bảo tính khả thi và an toàn thông tin khi triển khai thực hiện.
- Giám sát các đội, xử lý vi phạm, giải quyết các vướng mắc trong quá trình diễn tập.
- Tổng hợp, đánh giá chấm điểm các đội và công bố kết quả diễn tập.

b) Ban giám khảo:

Đánh giá kết quả khách quan của các đội tham gia diễn tập, đóng vai trò điều phối triển khai diễn tập.

c) Các đội tham gia:

- Tham gia các thử thách được hệ thống triển khai theo điều phối.
- Sử dụng các phần mềm, ứng dụng để tiến hành điều tra, xác minh sự cố về an ninh mạng, an toàn thông tin; bảo đảm tuân thủ nghiêm giới hạn của diễn tập.
- Báo cáo, đề xuất Ban giám khảo khi phát hiện các sự cố trong quá trình thực hiện diễn tập.

III. KINH PHÍ TỔ CHỨC THỰC HIỆN

Ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

IV. TỔ CHỨC THỰC HIỆN

1. Công an thành phố

- Chủ trì tham mưu, xây dựng chương trình diễn tập; lựa chọn 01 đơn vị Ủy ban nhân dân cấp xã để triển khai cuộc Diễn tập thứ nhất; phối hợp với các đơn vị liên quan chuẩn bị điều kiện phục vụ diễn tập; phối hợp chuyên gia an ninh mạng, an toàn thông tin để triển khai diễn tập sát với thực tế; tiến hành lựa chọn đơn vị cung cấp dịch vụ có năng lực và các cơ quan liên quan tổ chức, triển khai diễn tập đảm bảo hiệu quả.

- Theo dõi, kiểm tra việc thực hiện các nội dung theo Kế hoạch và tổng hợp báo cáo kết quả diễn tập về Ủy ban nhân dân thành phố, Cục An ninh mạng
- Bộ Công an và các cơ quan, đơn vị liên quan sau khi kết thúc diễn tập.

2. Sở Khoa học và Công nghệ

- Phối hợp Công an thành phố triển khai chương trình diễn tập theo đúng quy định bảo đảm hiệu quả, đạt chất lượng; rà soát, thành lập các Đội tham gia bảo đảm phù hợp với tình hình thực tiễn tại địa phương, bảo đảm chất lượng, trình độ đồng đều; đánh giá kết quả sau mỗi cuộc diễn tập.

- Chỉ đạo Trung tâm IOC giám sát, cảnh báo sớm các nguy cơ mất an ninh mạng và bảo đảm an ninh, an toàn cho hệ thống CPnet trong suốt quá trình diễn tập.

3. Sở Tài chính

Trên cơ sở đề xuất của Công an thành phố, Sở Tài chính chủ trì, rà soát tham mưu cấp có thẩm quyền bố trí kinh phí để thực hiện Kế hoạch đảm bảo theo phân cấp ngân sách nhà nước hiện hành và các quy định pháp luật có liên quan, phù hợp tình hình thực tế và khả năng cân đối ngân sách.

4. Các sở, ban, ngành, Ủy ban nhân dân các xã, phường có liên quan

Phối hợp Công an thành phố và các đơn vị liên quan triển khai các cuộc Diễn tập khi có yêu cầu.

Yêu cầu Thủ trưởng các sở, ban, ngành, Ủy ban nhân dân các xã, phường và các cơ quan, đơn vị liên quan triển khai thực hiện đảm bảo hiệu quả, chất lượng. Trong quá trình thực hiện nếu có khó khăn, vướng mắc kịp thời báo cáo Ủy ban nhân dân thành phố (qua Phòng An ninh mạng - Công an thành phố) để được hướng dẫn./.

Nơi nhận:

- CT và các Phó CT UBND thành phố;
- Các cơ quan chuyên môn thuộc thành phố;
- Công an thành phố;
- UBND các phường, xã;
- VP.UBND thành phố: CVP, các PCVP;
- Lưu: VT, TTr.

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



Trần Hữu Thùy Giang