

KẾ HOẠCH
Tổ chức diễn tập thực chiến
đối với các hệ thống thông tin của tỉnh năm 2023

Thực hiện Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 của Thủ tướng Chính phủ về việc đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 60/CT-BTTTT ngày 16 tháng 9 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

Thực hiện Kế hoạch số 44/KH-UBND ngày 10/3/2023 của UBND tỉnh về chuyển đổi số năm 2023, định hướng đến năm 2025, Sở Thông tin và Truyền thông xây dựng Kế hoạch tổ chức diễn tập thực chiến ứng cứu, phòng chống sự cố về an toàn thông tin năm 2023 như sau:

I. MỤC ĐÍCH, YÊU CẦU VÀ PHẠM VI DIỄN TẬP

1. Mục đích

- Diễn tập thực chiến nhằm giúp cho cán bộ, công chức làm công tác quản trị mạng và các thành viên Đội ứng cứu sự cố An toàn thông tin mạng của tỉnh được rèn luyện kỹ năng, kinh nghiệm sẵn sàng ứng cứu, xử lý các sự cố tấn công mạng có thể xảy ra đối với hệ thống CNTT do cơ quan, đơn vị mình quản lý.

- Triển khai đảm bảo theo đúng quy định, hướng dẫn của Bộ Thông tin và Truyền thông về diễn tập thực chiến. Có phương án đảm bảo hoạt động an toàn, ổn định trong và sau diễn tập; đảm bảo hiệu quả, thiết thực, tiết kiệm.

2. Yêu cầu

Các đơn vị tham dự diễn tập cần tuân thủ đầy đủ nội quy về diễn tập thực chiến đối với hệ thống thông tin trung tâm tích hợp dữ liệu tỉnh do Ban Tổ chức ban hành.

3. Phạm vi diễn tập

Thực hiện trên Hệ thống thông tin Trung tâm tích hợp dữ liệu tỉnh Bình Định, cụ thể được giới hạn như sau:

- Hệ thống Trang thông tin điện tử của Sở Thông tin và Truyền thông có địa chỉ: <https://stttt.binhdinhh.gov.vn>.

- Hệ thống Quản lý lưu trú trực tuyến tỉnh Bình Định có địa chỉ: <https://quanlyluutru.binhdingh.gov.vn>.

- Các tổ chức cá nhân tham dự Diễn tập đảm bảo tuân thủ kịch bản đã ban hành (*bao gồm giới hạn diễn tập, thời gian diễn tập, ngưỡng tấn công, các phương án phòng ngừa rủi ro và ứng cứu nếu xảy ra sự cố*).

II. NỘI DUNG KẾ HOẠCH

1. Tên diễn tập: Diễn tập thực chiến đối với các hệ thống thông tin của tỉnh năm 2023.

2. Thời gian: Bắt đầu từ 08 giờ ngày 18/12/2023 đến 17 giờ 00 ngày 19/12/2023.

3. Hình thức: Trực tiếp.

4. Địa điểm: Sở Thông tin và Truyền thông, số 38 đường Trường Chinh, thành phố Quy Nhơn, tỉnh Bình Định.

5. Thành phần tham dự:

a) Lãnh đạo Sở Thông tin và Truyền thông và các phòng, đơn vị trực thuộc Sở;

b) Lãnh đạo Trung tâm VNCERT và các cán bộ liên quan.

c) Các Đội tấn công (Red team):

- Đại diện cán bộ phụ trách CNTT/ATTT của các đơn vị: Văn phòng Tỉnh ủy; Công an tỉnh; các sở, ban, ngành thuộc UBND tỉnh và UBND các huyện, thị xã, thành phố.

- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh Bình Định theo Quyết định số 951/QĐ-UBND ngày 25/3/2022 của UBND tỉnh.

d) Đội phòng thủ (Blue team):

Thành viên Đội ứng cứu sự cố an toàn thông tin của Sở Thông tin và Truyền thông Bình Định.

6. Chương trình diễn tập: Phụ lục I.

7. Nhiệm vụ, thời gian thực hiện: Phụ lục II.

III. TỔ CHỨC THỰC HIỆN

1. Phòng Bưu chính, Viễn thông và Công nghệ thông tin:

- Chủ trì, phối hợp với Trung tâm VNCERT/CC, Trung tâm Công nghệ thông tin và Truyền thông tổ chức diễn tập, công bố kết quả diễn tập, đánh giá hoạt động diễn tập và tổ chức bế mạc diễn tập. Tổng hợp, gửi báo cáo kết quả diễn tập về Cục An toàn thông tin.

- Tham mưu Nội quy về diễn tập thực chiến, ứng cứu thông tin tại Trung tâm tích hợp dữ liệu tỉnh Bình Định theo quy định.

- Tham mưu thành lập Ban Tổ chức diễn tập, Đội tấn công và Đội phòng thủ.

2. Trung tâm Công nghệ thông tin và Truyền thông

- Xây dựng kịch bản chi tiết phương án tổ chức diễn tập thực chiến bảo đảm an toàn thông tin mạng theo quy định. Chuẩn bị các trang, thiết bị, nhân lực đảm bảo phục vụ cho diễn tập theo nội dung kế hoạch này.

- Giám sát, theo dõi hệ thống thông tin Trung tâm Tích hợp dữ liệu trong suốt thời gian diễn tập.

3. Văn phòng Sở

- Hướng dẫn sử dụng kinh phí thực hiện kế hoạch theo quy định.

- Phối hợp với phòng Bưu chính, Viễn thông và Công nghệ thông tin, Trung tâm Công nghệ thông tin và Truyền thông chuẩn bị các cơ sở vật chất cần thiết đảm bảo cho việc tổ chức buổi diễn tập./.

Nơi nhận:

- Cục ATTT;
- Trung tâm VNCERT/CC;
- Lãnh đạo Sở TT&TT;
- Phòng BCVT&CNTT;
- Văn phòng Sở;
- TT.CNTT&TT;
- Lưu: VT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Minh Thảo

Phụ lục I
CHƯƠNG TRÌNH DIỄN TẬP THỰC CHIẾN
(Kèm theo Kế hoạch số /KH-STTTT ngày /12/2023 của Sở Thông tin và Truyền thông)

Thời gian	Nội dung	Thực hiện
Ngày 18/12/2023		
7h30 - 08h00	Tiếp đón đại biểu, khách mời	Sở TT&TT, VNCERT/CC
8h00 – 8h05	Tuyên bố lý do, giới thiệu đại biểu	MC
8h05 – 8h10	Phát biểu khai mạc diễn tập	Lãnh đạo Sở TT&TT
8h10 – 8h15	Phát biểu diễn tập	Lãnh đạo VNCERT/CC
8h15 – 11h30	<ul style="list-style-type: none"> - Quán triệt Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 của Thủ tướng Chính phủ về việc đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; - Công bố phạm vi diễn tập và các nội quy trong quá trình triển khai diễn tập thực chiến, nội quy đội tấn công, nội quy đội phòng thủ. - Giới thiệu những quy định, chính sách trong việc cam kết đảm bảo an toàn thông tin trong suốt quá trình diễn tập 	Trung tâm VNCERT/CC
14h – 16h30	Bắt đầu Diễn tập thực chiến (tại chỗ/từ xa)	Các đội tấn công, đội phòng thủ
Ngày 19/12/2023		
08h – 11h30	Diễn tập thực chiến (tại chỗ/từ xa)	Các đội tấn công, đội phòng thủ
14h-14h30	Đánh giá kết quả diễn tập	Ban Giám khảo
14h30 – 15h30	Các Đội tấn công trình bày tóm tắt quá trình tấn công vào các hệ thống mục tiêu	Các Đội tấn công có thành tích tốt nhất
15h30 – 16h30	Đội phòng thủ trình bày quá trình phát hiện, ngăn chặn tấn công	Đội phòng thủ

Thời gian	Nội dung	Thực hiện
16h30-16h40	Công bố kết quả diễn tập, trao giấy chứng nhận	Sở TT&TT
16h40-16h50	Phát biểu của Lãnh đạo Trung tâm VNCERT/CC	Lãnh đạo Trung tâm VNCERT/CC
16h50-17h00	Phát biểu bế mạc	Lãnh đạo Sở TT&TT
17h10-	Bế mạc, chụp ảnh lưu niệm	

Phụ lục II
PHÂN CÔNG NHIỆM VỤ, THỜI GIAN THỰC HIỆN
(Kèm theo Kế hoạch số /KH-STTTT ngày /12/2023 của Sở Thông tin và Truyền thông)

STT	Nội dung công việc	Chủ trì	Phối hợp	Thời gian hoàn thành
	CÔNG TÁC CHUẨN BỊ TRƯỚC DIỄN TẬP			
1	Xây dựng Kế hoạch tổ chức diễn tập thực chiến	Phòng BCVT&CNTT	VNCERT	Trước ngày 16/12/2023
2	Xác định mục tiêu diễn tập; xây dựng Quy chế diễn tập; thành lập Ban Giám khảo	Phòng BCVT&CNTT	VNCERT	
3	Lập danh sách các đội tham gia diễn tập; dự thảo văn bản mời tham gia diễn tập; tổng hợp danh sách tham dự	VNCERT	PHÒNG BCVT&CNTT	
4	Rà soát, triển khai phương án dự phòng, sao lưu dữ liệu và hệ thống trước khi Diễn tập; xây dựng các kịch bản, phương án ứng cứu sự cố, phòng ngừa các rủi ro có thể xảy ra	Trung tâm CNTT&TT	VNCERT	
5	Lập danh sách nhân sự tham gia Đội phòng thủ, phân công nhiệm vụ cho các thành viên Đội phòng thủ	Trung tâm CNTT&TT	VNCERT	
6	Xây dựng báo cáo chương trình diễn tập (mục tiêu, phạm vi, quy chế,...)	VNCERT	Phòng BCVT&CNTT	
7	Chuẩn bị hạ tầng, thiết bị, công cụ, phần mềm, các điều kiện liên quan hậu cần đảm bảo cho công tác diễn tập (hội trường, backdrop, máy chiếu, bàn ghế, tài liệu, teabreak, bảng tên,...)	VNCERT	Phòng BCVT&CNTT	
8	Tạo các group liên quan và phân công điều phối tại các group (blueteam, redteam)	VNCERT	Phòng BCVT&CNTT	
9	Dự thảo kịch bản MC và dẫn chương trình diễn tập	Phòng BCVT&CNTT	VNCERT	
10	Chuẩn bị các bản cam kết của đội tấn công, đội phòng thủ	VNCERT	Phòng BCVT&CNTT	

11	Chuẩn bị các mẫu báo cáo của đội tấn công, đội phòng thủ	VNCERT	Phòng BCVT&CNTT	
12	Dự thảo bài phát biểu của Lãnh đạo Sở TT&TT	Phòng BCVT&CNTT	VNCERT	
13	Chuẩn bị giấy chứng nhận cho các đội tham gia diễn tập	VNCERT		
14	Chuẩn bị hạ tầng mạng WiFi, hạ tầng họp trực tuyến phục vụ diễn tập	Trung tâm CNTT&TT	VNCERT	
	TẠI BUỔI DIỄN TẬP			
15	Khai mạc diễn tập thực chiến	Phòng BCVT&CNTT	VNCERT	Ngày 18/12/2023
16	Báo cáo, phổ biến quy chế diễn tập	VNCERT	Phòng BCVT&CNTT	
17	Triển khai chính thức Diễn tập; quản lý, điều hành, giám sát hoạt động tấn công và phòng thủ	VNCERT	Phòng BCVT&CNTT	Ngày 18 và 19/12/2023
18	Tổng hợp, đánh giá, báo cáo kết quả diễn tập	BGK		Ngày 19/12/2023
19	Bế mạc, trao giấy chứng nhận	Phòng BCVT&CNTT	VNCERT	
20	Truyền thông, đưa tin bài diễn tập	Phòng BCVT&CNTT		Ngày 18 và 19/12/2023
	SAU DIỄN TẬP			
21	Báo cáo kết quả công tác diễn tập gửi Sở TT&TT (Chủ đầu tư), bao gồm tổng hợp các báo cáo của đội tấn công và đội phòng thủ	VNCERT	Phòng BCVT&CNTT	Trước 20/12/2023
22	Triển khai xử lý khắc phục các lỗ hổng đã được phát hiện	Trung tâm CNTT&TT	VNCERT	Trước 25/12/2023

Phụ lục III
DỰ KIẾN DANH SÁCH ĐỘI TẤN CÔNG
(Kèm theo Kế hoạch số /KH-STTTT ngày /12/2023 của Sở Thông tin và Truyền thông)

STT	Thành phần	Số lượng
1	Cán bộ phụ trách CNTT/ATTT của Công an tỉnh và Viễn thông Bình Định	01 đội
2	Cán bộ phụ trách CNTT/ATTT của các sở, ban, ngành	01 đội
3	Cán bộ phụ trách CNTT/ATTT của UBND các huyện, thị xã, thành phố	01 đội
4	Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh Bình Định theo Quyết định số 951/QĐ-UBND ngày 25/3/2022 của UBND tỉnh	01 đội
	Tổng cộng	04 đội