UBND TỈNH NINH THUẬN
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số:2678 /KH-STTTT

*Ninh Thuận, ngày 27 tháng 10 năm 2023*

# KẾ HOẠCH
## Đào tạo diễn tập ứng cứu sự cố an toàn thông tin cho cán bộ chuyên trách các Sở, Ban, ngành và Ủy ban nhân dân các huyện, thành phố

Căn cứ Kế hoạch số 4125/KH-UBND ngày 16/11/2020 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, phát triển chính quyền số và đảm bảo an toàn thông tin mạng giai đoạn 2021 -2025 và Kế hoạch số 6526/KHUBND ngày 30/11/2021 về phát triển chính quyền số và bảo đảm an toàn thông tin mạng năm 2022 của UBND tỉnh Ninh Thuận;

Căn cứ Quyết định số 691/QĐ-UBND ngày 14/12/2022 của Chủ tịch Ủy ban nhân dân tỉnh về việc giao dự toán chi ngân sách nhà nước năm 2023 cho các Sở, ban, ngành, cơ quan Đảng, đoàn thể và các hội đặc thù và đơn vị cấp tỉnh và Quyết định số 144/QĐ-UBND ngày 03/4/2023 của Chủ tịch Ủy ban nhân dân tỉnh về việc điều chỉnh dự toán chi ngân sách nhà nước năm 2023 tại phụ lục kèm theo Quyết định số 691/QĐ-UBND ngày 14/12/2022 của Ủy ban nhân dân tỉnh;

Căn cứ Quyết định số 35/QĐ-STTTT ngày 11/4/2023 của Sở Thông tin và Truyền thông về việc điều chỉnh dự toán chi ngân sách nhà nước năm 2023 của Văn phòng Sở Thông tin và Truyền thông.

Nhằm nâng cao, phát huy hiệu quả hoạt động về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, phát triển chính quyền số và đảm bảo an toàn thông tin mạng cho cán bộ chuyên trách công nghệ thông tin. Sở Thông tin và Truyền thông xây dựng Kế hoạch đào tạo diễn tập ứng cứu sự cố an toàn thông tin cho cán bộ chuyên trách các Sở, Ban, ngành và Ủy ban nhân dân các huyện, thành phố, như sau:

### I. Mục đích, yêu cầu

### 1. Mục đích

- Chuẩn bị tốt nguồn nhân lực đáp ứng các điều kiện cần thiết khi triển khai Cách mạng 4.0.

- Hiểu về các Phương thức tấn công, cách phòng thủ và xây dựng được một hệ thống đảm bảo tính bảo mật và an toàn thông tin, ứng phó với các trường hợp sự cố cho hệ thống mạng của cơ quan, đơn vị.

- Trang bị những kỹ năng cần thiết để kịp thời ứng phó, giải quyết các vấn đề thông qua tình huống tấn công vào vào hệ thống thư, các lỗ hổng giả định có thể xảy ra trong thực tế khi khai thác các hệ thống.

- Nâng cao năng lực bảo vệ an toàn thông tin, sẵn sàng ngăn chặn, xử lý và ứng cứu sự cố tấn công và xử lý tấn công khai thác vào hệ thống, đánh giá lỗ hổng, điểm yếu bảo mật, qua đó nắm được các điểm yếu trên hệ thống để có phương thức phòng thủ hợp lý, chống lại các tấn công tương tự diễn ra trong thực tế cho cán bộ chuyên trách CNTT các đơn vị.

**2. Yêu cầu**

- Nội dung đào tạo phải bám sát tình hình triển khai ứng dụng công nghệ thông tin thực tế của các cơ quan, đơn vị trên địa bàn tỉnh, phù hợp với đối tượng tham gia đào tạo.

- Nội dung tập huấn, xây dựng tình huống diễn tập phải đảm bảo hiệu quả, thiết thực, phù hợp với các nội dung trong thực tế vận hành, xử lý lỗ hổng bảo mật.

- Sau khi hoàn thành khóa học, cán bộ chuyên trách công nghệ thông tin hiểu rõ về kiến thức cơ bản về an toàn thông tin, các biện pháp đảm bảo an toàn, bảo mật thông tin, dữ liệu, các loại tấn công mạng, bảo mật mạng không dây, kiểm soát truy nhập, sử dụng web an toàn, quản lý dữ liệu an toàn.

**II. Nội dung kế hoạch**

**1. Nội dung chương trình đào tạo**

*(Kèm theo Phụ lục: Nội dung chương trình đào tạo)*

**2. Thời gian, địa điểm**

- Thời gian đào tạo: 03 ngày, dự kiến tháng 11/2023

- Địa điểm đào tạo diễn tập: tại tỉnh Ninh Thuận.

*(Thời gian và địa điểm cụ thể sẽ có thông báo sau)*

**3. Đối tượng và số lượng đào tạo**

- Đối tượng: công chức, viên chức có kiến thức về công nghệ thông tin, về quản lý hệ thống tin học hóa; công chức chuyên trách hoặc thực hiện nhiệm vụ công nghệ thông tin trong quản lý, vận hành và bảo trì hệ thống mạng tại các Sở, Ban, ngành, Ủy ban nhân dân các huyện, thành phố, cán bộ kỹ thuật Trung tâm Công nghệ thông tin và Truyền thông.

- Số lượng học viên: dự kiến 40 học viên.

**4. Kinh phí**

Kinh phí thực hiện đào tạo chuyên sâu công nghệ thông tin cho cán bộ chuyên trách các Sở, Ban, ngành và Ủy ban nhân dân các huyện, thành phố theo Kế hoạch này do ngân sách nhà nước cấp theo Nguồn ứng dụng công nghệ thông tin trong dự toán chi ngân sách năm 2023 theo Quyết định số 691/QĐ-UBND ngày 14/12/2022 của Chủ tịch Ủy ban nhân dân tỉnh về việc giao dự toán chi ngân sách nhà nước năm 2023 cho các Sở, ban, ngành, cơ quan Đảng, đoàn thể và các hội đặc thù và đơn vị cấp tỉnh và Quyết định số 144/QĐ-UBND ngày 03/4/2023 của Ủy ban nhân dân tỉnh về việc điều chỉnh dự toán chi ngân sách nhà nước năm 2023 tại phụ lục kèm theo Quyết định số 691/QĐ-UBND ngày 14/12/2022 của Ủy ban nhân dân tỉnh.

**III. Tổ chức thực hiện**

**1. Sở Thông tin và Truyền thông**

- Tổ chức lựa chọn nhà thầu có đủ năng lực, trang thiết bị công nghệ thông tin để triển khai thực hiện các nội dung đào tạo trên theo đúng Kế hoạch.

- Thông báo đến các Sở, Ban ngành, Ủy ban nhân dân các các huyện, thành phố và các cơ quan, đơn vị có liên quan cử cán bộ, công chức tham gia các khoá đào tạo.

- Phối hợp với đơn vị đào tạo tổ chức quản lý, theo dõi, đánh giá kết quả đào tạo theo Kế hoạch.

**2. Các Sở, Ban ngành và Ủy ban nhân dân các huyện, thành phố**

- Cử cán bộ, công chức, viên chức thuộc đối tượng tại khoản 3 mục II Kế hoạch tham gia khóa đào tạo.

- Tạo điều kiện thuận lợi cho cán bộ tham gia đầy đủ khóa đào tạo.

Trên đây là Kế hoạch đào tạo diễn tập ứng cứu sự cố an toàn thông tin cho cán bộ chuyên trách các Sở, Ban, ngành và Ủy ban nhân dân các huyện, thành phố năm 2022./.

***Nơi nhận:***
- UBND tỉnh (b/c);
- Sở, Ban, ngành;
- UBND các huyện, thành phố;
- Trung tâm CNTT-TT;
- Lưu: CN, VT.

**GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NINH THUẬN

**Đào Xuân Kỳ**

**Phụ lục**
**Nội dung chương trình đào tạo**
*(Ban hành kèm theo Kế hoạch số: 2678 /KH-STTTT ngày 27/10/2023 của Sở Thông tin và Truyền thông)*

## 1. Nội dung chi tiết chuyên đề

| Buổi | Chủ đề | Nội dung chi tiết |
|---|---|---|
| Ngày 01 | **Giới thiệu về Ứng cứu sự cố** | **Tổng quan:**<br>• Các nguyên lý về an toàn thông tin<br>• Sự cố An toàn thông tin là gì?<br>• Ứng phó sự cố, xử lý sự cố và quản lý sự cố<br>**Quy trình xử lý sự cố:**<br>• Chuẩn bị<br>• Phát hiện và phân tích<br>• Ngăn chặn, diệt trừ, phục hồi<br>• Theo dõi sau sự cố |
| | **Ứng cứu sự cố tấn công các máy chủ dịch vụ và leo thang đặc quyền** | **Lý thuyết:**<br>• Tìm hiểu về các phương thức tấn công máy chủ dịch vụ;<br>• Tìm hiểu và phân tích phương thức tấn công leo thang đặc quyền;<br>• Đề xuất giải pháp và ngăn chặn các cuộc tấn công leo thang đặc quyền.<br>**Diễn Tập**<br>• Thực hiện tấn công leo thang đặc quyền; |
| Ngày 02 | **Ứng cứu sự cố tấn công từ chối dịch vụ** | • **Lý thuyết:**<br>• Tìm hiểu về kỹ thuật tấn công từ chối dịch vụ DOS và DDOS;<br>• Phân tích và mô hình hóa kiểu tấn công từ chối dịch vụ;<br>• Kỹ thuật phát hiện nguồn gốc tấn công từ chối dịch vụ và cách phòng chống tấn công từ chối dịch vụ.<br>**Diễn tập:**<br>• Tấn công từ chối dịch vụ vào các hosts<br>• Tấn công từ chối dịch vụ vào các thiết bị mạng: router, switch, firewall |

| | | |
|---|---|---|
| | | • Tấn công từ chối dịch vụ vào các ứng dụng phổ biến.<br>• Phát hiện, ngăn chặn, khắc phục sự cố khi bị tấn công DoS. |
| | **Ứng cứu sự cố mã độc mã hóa (ransomware)** | **Lý thuyết:**<br>• Tìm hiểu về các phương thức mã hóa của mã độc;<br>• Phân tích và phục hồi dữ liệu sau khi bị mã độc mã hóa;<br>• Đề xuất giải pháp và ngăn chặn các cuộc tấn công bằng mã độc mã hóa khác vào trung tâm tích hợp dữ liệu.<br>**Diễn Tập**<br>• Thực hiện tấn công bằng mã độc ransomewae;<br>• Diễn tập phát hiện, ngăn chặn và khắc phục sự cố khi bị tấn công bởi Ransomware. |
| Ngày 03 | **Ứng cứu sự cố mất ATTT trên dịch vụ Web** | **Lý thuyết:**<br>• Tổng quan về kiến trúc Web Application<br>• Tổng quan về Cơ sở dữ liệu<br>• Tổng quan về các lỗ hỏng của Web Application<br>• Tổng quan về các rủi ro liên quan đến Web Application<br>• Tổng quan về các kỹ thuật tấn công Web Application và Web server.<br>**Diễn tập:**<br>• Thực hiện khai thác lỗ hổng SQL Injection trên Web Application;<br>• Thực hiện khai thác XSS trên Web Application;<br>• Thực hiện tấn công Web phishing;<br>• Thực hiện tấn công file upload;<br>• Phát hiện, ngăn chặn và khắc phục sự cố khi bị tấn công với các hình thức trên. |
| | **Ứng cứu sự cố mất an toàn thông tin trên mạng không dây** | **Lý thuyết:**<br>• Tổng quan về mạng không dây |

| | | |
|---|---|---|
| | | • Tổng quan về các nguy cơ trong mạng không dây<br>• Tổng quan về các kỹ thuật tấn công trong mạng không dây<br>**Diễn tập:**<br>• Triển khai kỹ thuật Dosing Wireless AP: Tin tặc liên tục gửi 'de-authentication' đến AP làm quá tải và gây ảnh hưởng cho toàn bộ người dùng trong mạng wifi;<br>• Triển khai kỹ thuật Fake Access Point: Giả mạo SSID để lừa người dùng truy cập và lấy thông tin mật khẩu wifi;<br>• Phân tích, ngăn chặn và khắc phục các kiểu tấn công hệ thống mạng không dây. |

**2. Kết quả đào tạo**

- Mục đích của việc diễn tập là nâng cao khả năng sẵn sàng đối phó với các nguy cơ, thách thức về an toàn thông tin cũng như khả năng phối hợp giữa các lực lượng tham gia. Ngoài việc tạo ra sự minh bạch trong diễn tập, việc đánh giá kết quả còn giúp cho các đội tham gia có động lực cạnh tranh để cùng nâng cao năng lực và nỗ lực trong quá trình diễn tập cho cán bộ tham gia đầy đủ khóa đào tạo

- Thảo luận các nội dung và kiểm tra trắc nghiệm toàn bộ chương trình (Cuối khóa học).