

Số: /UBND-VP

Sầm Sơn, ngày tháng 9 năm 2023

V/v gán nhãn tín nhiệm mạng cho các Cổng/trang thông tin điện tử cơ quan nhà nước trên địa bàn thành phố.

Kính gửi:

- Văn phòng HĐND&UBND thành phố;
- Trung tâm Văn hóa - TT-TT&DL;
- UBND các xã, phường.

Thực hiện Công văn số 200/TTCNTT&TT-QTHT ngày 11/09/2023 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa về việc gán nhãn tín nhiệm mạng cho các Cổng/trang thông tin điện tử cơ quan nhà nước trên địa bàn tỉnh; Chủ tịch UBND thành phố yêu cầu Văn phòng HĐND&UBND thành phố, Trung tâm Văn hóa - TT-TT&DL và UBND các xã, phường thực hiện tốt các nội dung sau:

**1. Văn phòng HĐND&UBND thành phố, Trung tâm Văn hóa - TT-TT&DL và UBND các xã, phường**

- Đăng ký chứng thư số SSL cho Cổng/ trang thông tin điện tử, theo Chỉ thị số 13/CT-UBND ngày 04/11/2022 về việc đẩy mạnh bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Thanh Hóa.

- Rà soát Cổng/Trang thông tin điện tử của đơn vị nếu đang hoạt động ở giao thức HTTP, cần đầu mối phối hợp với đơn vị quản lý tên miền VNPT (nâng cấp trang/cổng) để kích hoạt giao thức bảo mật HTTPS tổng hợp theo mẫu ở Phụ lục 01; gửi về UBND thành phố (qua Văn phòng HĐND&UBND) **trước ngày 05/10/2023**.

- Yêu cầu kỹ thuật đáp ứng đúng theo Điều 6, Nghị định 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ, quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng để phê duyệt tín nhiệm mạng thực hiện theo Hướng dẫn về các yêu cầu để gán nhãn tín nhiệm mạng ở Phụ lục 02 kèm theo.

**2. Trung tâm Viễn thông Sầm Sơn (VNPT)**

- Phối hợp với UBND các xã, phường và các đơn vị có liên quan thực hiện nâng cấp trang/cổng thông tin điện tử theo quy định của tại Điều 6, Nghị định 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ, quy định về việc cung cấp

thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng và chỉ thị số 13/CT-UBND ngày 04/11/2022 về việc đẩy mạnh bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Thanh Hóa.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với đầu mối: Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (qua đồng chí Đỗ Hữu Tiến - SĐT: 0917672989) hoặc Trung tâm Viễn thông Sầm Sơn (qua đồng chí Phúc - SĐT: 0946.787.772) để phối hợp hỗ trợ, xử lý.

Nhận được Công văn này, yêu cầu các đơn vị triển khai và thực hiện nghiêm túc các nội dung trên./.

***Nơi nhận:***

- Như trên;
- Chủ tịch, các Phó Chủ tịch UBND TP (b/cáo);
- Lưu: VT, VP.

**KT. CHỦ TỊCH  
PHÓ CHỦ TỊCH**

**Bùi Quốc Đạt**

**Phụ lục 1 :**  
**Danh sách các Cổng/Trang thông tin điện tử thuộc phạm vi cơ quan, đang quản lý, sử dụng**  
*(Kèm theo Công văn số            /UBND-VP ngày            tháng 9 năm 2023 của UBND thành phố)*

**1. Thông tin chung**

- Tên đơn vị: .....
- Đầu mối liên hệ: .....
  - + Họ và tên: .....
  - + Số điện thoại: .....
  - + Thư điện tử: .....

**2. Thông tin Cổng/Trang thông tin điện tử.**

<b>STT</b>	<b>Tên Cổng/trang thông tin điện tử</b>	<b>Địa chỉ</b>	<b>Đơn vị quản lý</b>	<b>Tín nhiệm mạng</b>	<b>Kiểm tra, đánh giá an toàn thông tin năm 2023</b>
1	VD: Trang thông tin điện tử UBND thành phố Sầm Sơn	<a href="https://samson.thanhhoa.gov.vn/">https://samson.thanhhoa.gov.vn/</a>	UBND thành phố Sầm Sơn	Có	Chưa
2	VD: Trang thông tin điện tử UBND phường Bắc Sơn	<a href="http://bacson.samson.thanhhoa.gov.vn/">http://bacson.samson.thanhhoa.gov.vn/</a>	UBND phường Bắc Sơn	Chưa	Chưa
3					
<b>Tổng:</b>					

## PHỤ LỤC 2

### Các yêu cầu kỹ thuật gắn tín nhiệm mạng cho các

### Cổng/Trang thông tin điện tử

(Kèm theo Công văn số           /UBND-VP ngày  /9/2023 của UBND thành phố)

#### 1. Giới thiệu về tín nhiệm mạng

Chúng nhận tín nhiệm mạng được gắn trên các Cổng/Trang thông tin điện tử của các cơ quan, đơn vị do Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Bộ Thông tin và Truyền thông cung cấp nhằm chứng nhận tín nhiệm giúp người dùng nhận biết nhanh, chính xác các tổ chức, website, hệ thống và thiết bị tin cậy ngăn ngừa các cuộc tấn công lừa đảo, tạo dựng niềm tin số cho người dùng khi sử dụng dịch vụ trên không gian mạng.

Nhãn tín nhiệm giúp người dân dễ dàng phân biệt website chính thống của các cơ quan tổ chức với các website giả mạo; đồng thời, tín nhiệm hỗ trợ quý đơn vị trong việc giám sát thời gian hoạt động của website (Uptime Monitor); phát hiện sớm các hành vi dò quét, tấn công website; các tấn công từ địa chỉ độc hại và các thay đổi về cấu trúc website, hướng tới không gian mạng Việt Nam an toàn và lành mạnh.

#### 2. Các yêu cầu kỹ thuật

Cổng/trang thông tin điện tử phải đáp ứng các yêu cầu kỹ thuật trước khi được cung cấp nhãn tín nhiệm mạng, cụ thể như sau:

- Yêu cầu 1: Cổng/Trang thông tin điện tử phải được thiết lập hoạt động cung cấp trên Internet qua giao thức bảo mật **HTTPS**.

Các Cổng/Trang thông tin điện tử nếu đang hoạt động ở giao thức **HTTP**, cần phối hợp với đơn vị quản lý tên miền, quản lý lưu trữ hoặc các nhà cung cấp dịch vụ khác để đăng ký, kích hoạt giao thức bảo mật **HTTPS**.

Các cách kiểm tra Cổng/trang thông tin điện tử:

##### Cách 1:

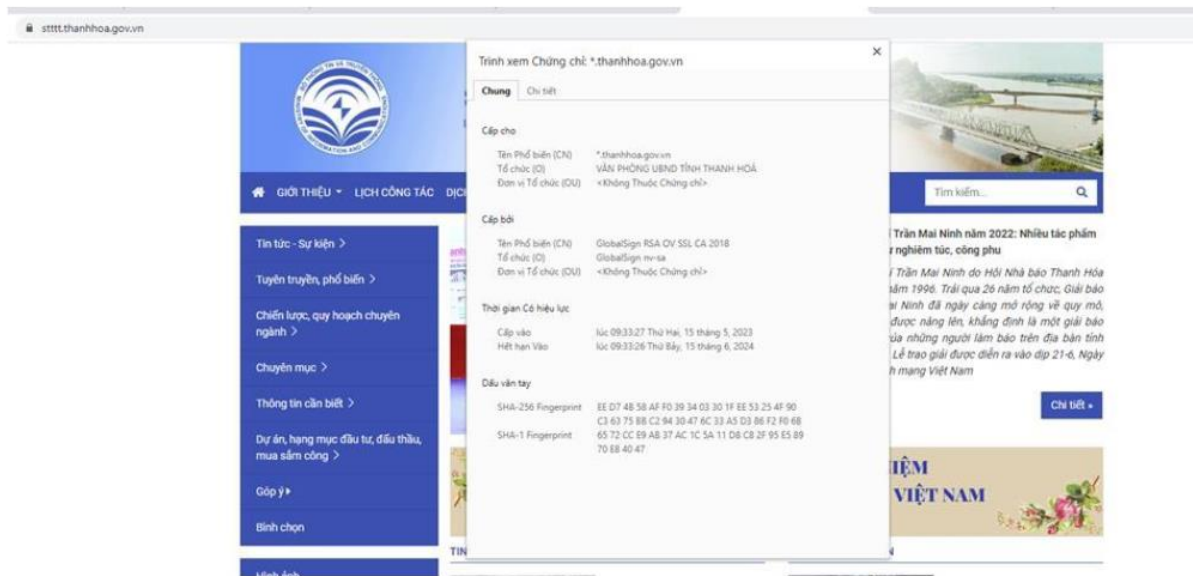
*Bước 1:* Truy cập trên trình duyệt Web (Chrome, Cốc Cốc, Firefox,...) gõ địa chỉ tên miền Cổng/trang thông tin điện tử.

*Bước 2:* Nếu trên thanh địa chỉ của trình duyệt xuất hiện biểu tượng “hình khóa” như sau:

5



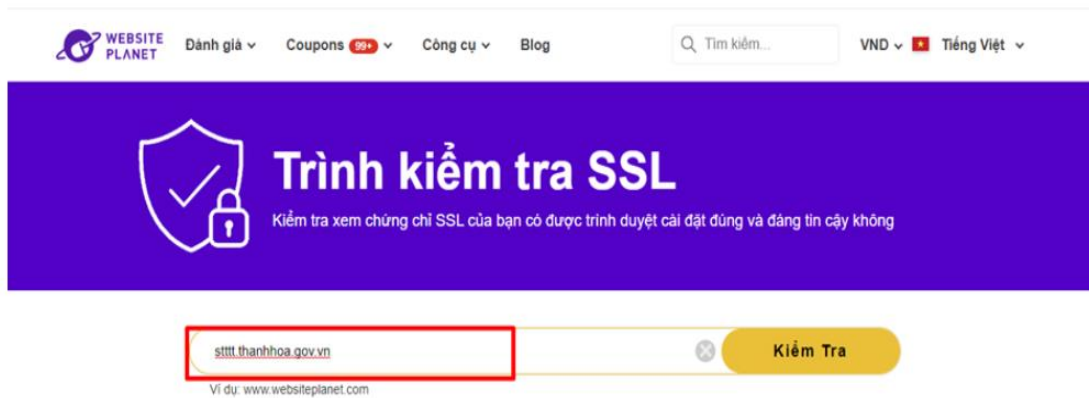
Bấm vào biểu tượng hình khóa, sẽ có thông tin xác nhận chứng chỉ bảo mật của tên miền.



**Cách 2:** Truy cập vào địa chỉ sau:

<https://www.websiteplanet.com/vi/webtools/ssl-checker/>

Nhập địa chỉ Cổng/Trang thông tin điện tử vào để kiểm tra



- Yêu cầu 2: Cổng/Trang thông tin điện tử phải được kiểm tra, đánh giá về an toàn thông tin trước khi gán nhãn tín nhiệm mạng.

### 3. Hướng dẫn gán nhãn tín nhiệm mạng

Sau khi đăng ký và đáp ứng các yêu cầu kỹ thuật về tín nhiệm mạng cho Cổng/Trang thông tin điện tử, các đơn vị cần gán nhãn tín nhiệm lên Cổng/Trang thông tin điện tử của mình để kết nối với hệ sinh thái Tín nhiệm mạng.

*Bước 1:* Sau khi được duyệt, các đơn vị sẽ nhận được một đoạn mã tương ứng với từng website của đơn vị.

Khuôn dạng của đoạn mã như sau:

```
<a href="#"Đường dẫn đến thông tin của website trên Tín nhiệm mạng" target="_blank"></a>
```

*Bước 2:* Sau khi nhận được các đơn vị tiến hành gán đoạn mã vào cuối trang web của đơn vị. Kết quả hiển thị như sau:

