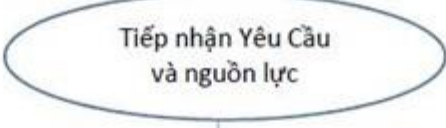
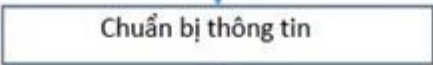
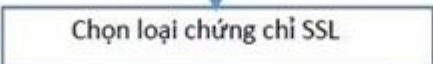

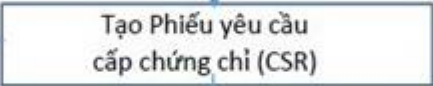
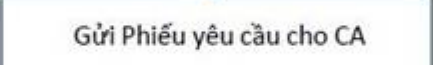
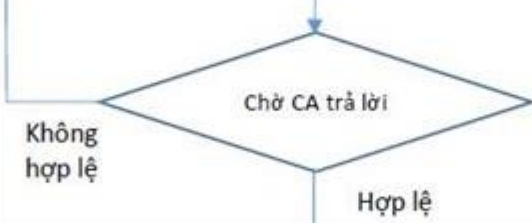
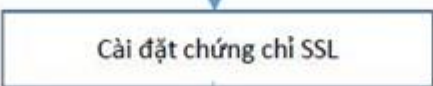
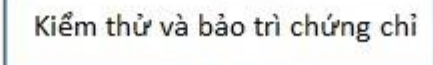
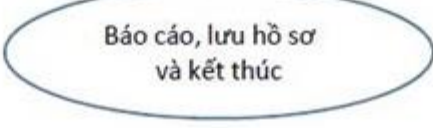


QUY TRÌNH LẤY CHỨNG CHỈ SSL (SSL Certificate) CHO MÁY CHỦ WEB

A. LƯU ĐỒ QUY TRÌNH

stt	Bước	Trách nhiệm	Lưu đồ	Biểu mẫu - Tài liệu
	1	Trưởng bộ phận hệ thống, và Nhân viên hệ thống		1. Phiếu yêu cầu công việc; 2. Tài liệu hướng dẫn xin chứng chỉ SSL có Ủy quyền quản trị (username, password)
	2	Nhân viên hệ thống		Bản mô tả chứng chỉ SSL
	3	Nhân viên hệ thống		Bản mô tả chứng chỉ SSL
	4	Nhân viên hệ thống		Bản mô tả chứng chỉ SSL
	5	Nhân viên hệ thống		1. Bản mô tả chứng chỉ SSL; 2. Phiếu CSR
	6	Nhân viên hệ thống		Phiếu CSR
	7	Nhân viên hệ thống		Phiếu CSR
	8	Nhân viên hệ thống		
	9	Nhân viên hệ thống		Biên bản nghiệm thu kết quả
	10	Trưởng bộ phận hệ thống, và Nhân viên hệ thống		1. Phiếu yêu cầu công việc; 2. Tài liệu hướng dẫn xin chứng chỉ SSL được cập nhật; 3. Bản mô tả chứng chỉ CSR; 4. Phiếu CSR 5. Biên bản nghiệm thu kết quả;

B. DIỄN GIẢI

Bối cảnh: Công ty X (gọi tắt là Công ty) có nhu cầu lấy chứng chỉ SSL cho trang web của họ lưu trên máy chủ của nhà cung cấp dịch vụ lưu trữ trang web. Trưởng Phòng CNTT chỉ đạo Trưởng bộ phận hệ thống CNTT làm việc này.

Bước 1: Tiếp nhận yêu cầu (YC) và nguồn lực

Trưởng bộ phận hệ thống CNTT (“System Admin”) tiến hành:

- Lập Phiếu yêu cầu công việc theo mẫu chung của Phòng CNTT thực hiện chỉ đạo của Trưởng Phòng CNTT liên hệ đơn vị cấp chứng chỉ (Certificate Authority (CA)) để xin cấp chứng chỉ SSL cho máy chủ Web của công ty.
- Phân công nhân viên thuộc bộ phận hệ thống CNTT nhận việc (gọi tắt là “nhân viên hệ thống”) thực hiện các bước (step-by-step) lấy hệ thống chứng chỉ SSL (SSL certificate) theo Phiếu yêu cầu (có quy định nội dung thực hiện, lịch thực hiện, nguồn lực được cấp, báo cáo hoàn thành bằng biên bản nghiệm thu v.v.) đã được phê duyệt;
- Bàn giao nguồn lực thực hiện (phần cứng (máy chủ Web), tài liệu hướng dẫn tạo chứng chỉ SSL (SSL certificate), ủy quyền quản trị (users, password) cho nhân viên hệ thống nhận việc và các nguồn lực cần thiết khác để thực hiện được nhiệm vụ.

Biểu mẫu đầu vào của Bước này là:	- Phiếu Yêu cầu công việc của Phòng CNTT có chữ ký của Trưởng Phòng CNTT và Trưởng bộ phận hệ thống ký duyệt thực hiện
Biểu mẫu đầu ra của Bước này là:	- Phiếu Yêu cầu của Trưởng bộ phận hệ thống có đủ thông tin và có ký xác nhận - Tài liệu hướng dẫn cách có được chứng chỉ SSL (SSL certificate) - Thông tin ủy quyền bằng tài khoản quản trị (user name và password): Admin Account

Bước 2: Chuẩn bị thông tin

Chứng chỉ SSL được cấp bởi một tổ chức được gọi là Cơ quan cấp chứng chỉ “Certificate Authority” (gọi tắt là “CA”). Quá trình lấy bất kỳ chứng chỉ bảo mật trang web nào có thể thực sự dễ dàng, đặc biệt nếu Công ty X đã chuẩn bị trước thông tin phù hợp theo yêu cầu của CA.

Nhân viên hệ thống thu thập để có thông tin như sau theo hướng dẫn như sau:

1. Tìm và có được địa chỉ IP duy nhất cho trang Web:
Dựa trên cách hoạt động của giao thức SSL, mỗi chứng chỉ Công ty muốn lấy sẽ cần có một địa chỉ IP riêng. Nếu không, những người sử dụng một số thiết bị và trình duyệt web cũ hơn sẽ không thể sử dụng trang web của doanh nghiệp. Công ty có thể sử dụng trang công cụ <https://www.ipvoid.com/find-website-ip/> để tìm ra địa chỉ IP trang web của doanh nghiệp của mình.
2. Thiết lập bản ghi WHOIS chính xác:
Khi Công ty yêu cầu chứng chỉ SSL cho một miền, CA sẽ xác minh rằng Công ty sở hữu tên miền đó. Để làm điều đó, nó sẽ kiểm tra bản ghi WHOIS của tên miền.
Công ty có thể sử dụng công cụ tra cứu tên miền <https://www.namecheap.com/domains/whois/> để kiểm tra bản ghi WHOIS của mình. Nếu thông tin Công ty tìm thấy đã lỗi thời, hãy nhớ cập nhật nó.
3. Xác thực doanh nghiệp:

Nếu Công ty đang yêu cầu chứng chỉ có độ bảo đảm cao, CA chỉ có thể kiểm tra cơ sở dữ liệu của Chính phủ để xác thực doanh nghiệp của Công ty. Ngoài ra, CA cũng có thể yêu cầu Công ty cung cấp tài liệu đăng ký Chính phủ liên quan đến doanh nghiệp của Công ty.

MẸO HÀNG ĐẦU: *Tránh nội dung hỗn hợp (sử dụng cả nội dung an toàn và không bảo mật) vì điều này có thể gây ra cảnh báo lỗi bảo mật hoặc "nội dung hỗn hợp". Thay vào đó, hãy đảm bảo tất cả các thành phần của trang Web, bao gồm cả hình ảnh, tải qua HTTPS.*

4. Nhận lời khuyên của chuyên gia, tin tức trong ngành và hơn thế nữa:

Liên hệ với các chuyên gia, tìm thông tin trong các bản tin trong ngành (nghề) đang hoạt động để nhận trợ giúp về việc xây dựng sự hiện diện trực tuyến của doanh nghiệp bằng cách đăng ký nhận bản tin của các chuyên gia...kèm theo kiểm tra để có sự đồng ý với Chính sách quyền riêng tư của các chuyên gia đó.

Nhân viên hệ thống ghi chép kết quả thu thập thông tin ở Bước này vào một tài liệu có tên “Bản mô tả chứng chỉ SSL” là phụ lục cho Phiếu Yêu cầu ở Bước 1.

Biểu mẫu đầu vào của Bước này là:	Tài liệu, hồ sơ phát sinh ở Bước 1
Biểu mẫu đầu ra của Bước này là:	Bản mô tả chứng chỉ SSL

Bước 3: Chọn loại chứng chỉ SSL

Có nhiều loại chứng chỉ SSL (“types of SSL certificates”) khác nhau và chúng có thể được phân loại dựa trên:

- **Validation level** (Cấp độ xác thực): Xác thực tên miền, Xác thực tổ chức và Xác thực mở rộng;
- **Secured Domains** (Tên miền được bảo mật): Tên miền đơn, ký tự đại diện và đa tên miền

Chúng ta hãy xem xét tổng quan ngắn gọn về từng loại:

1. **Domain Validation** (Xác thực tên miền): Đây là mức xác thực rẻ nhất và thấp nhất, chỉ đảm bảo rằng công ty có quyền kiểm soát tên miền. Nó phù hợp nhất cho các doanh nghiệp nhỏ thường không trao đổi bất kỳ thông tin nào với người dùng.
2. **Organization Validation** (Xác thực tổ chức): Đây là mức độ xác thực trung bình. Nó không chỉ kiểm tra quyền sở hữu tên miền mà còn kiểm tra thông tin chi tiết về tổ chức, chẳng hạn như tên và vị trí. Cấp độ này lý tưởng cho các trang web kinh doanh có biểu mẫu và tính năng thu hút khách hàng tiềm năng.
3. **Extended Validation** (Xác thực mở rộng): Đây là mức xác thực tốn kém và kỹ lưỡng nhất. Cũng như thông tin chi tiết về quyền sở hữu và tổ chức tên miền, nó xác minh vị trí thực tế và sự tồn tại hợp pháp của công ty. Nó phù hợp với các trang web xử lý thông tin nhạy cảm, chẳng hạn như giao dịch tài chính.
4. **Single-Domain** (Đơn miền hay Tên miền đơn): Cung cấp bảo vệ đơn lẻ cho một tên miền phụ. Ví dụ: chứng chỉ SSL được mua cho johndoe.com không thể được sử dụng cho các tên miền phụ, chẳng hạn như blog.johndoe.com
5. **Wildcard** (Ký tự đại diện): Cung cấp sự bảo vệ cho các tên miền phụ không giới hạn của một tên miền. Ví dụ: chứng chỉ SSL được mua cho johndoe.com có thể được áp dụng cho bất kỳ tên miền phụ nào, chẳng hạn như blog.johndoe.com hoặc shop.johndoe.com.
6. **Multi-Domain** (đa miền): Cung cấp khả năng bảo vệ cho tới đa 100 miền bằng một chứng chỉ SSL duy nhất. Ví dụ: chứng chỉ SSL được mua cho johndoe.com có thể được áp dụng cho các tên miền khác, chẳng hạn như janedoe.com.

Loại SSL nào phù hợp với khách hàng sẽ phụ thuộc vào một số yếu tố và vị thế kinh doanh độc đáo của khách hàng.

Ví dụ: một trang web dành cho một quán cà phê địa phương được sử dụng để truyền đạt thông tin đơn giản như vị trí và thời gian mở cửa của họ có thể chỉ yêu cầu Xác thực tên miền. Điều này đặc biệt đúng nếu họ không thu thập hoặc sử dụng bất kỳ dữ liệu hoặc thông tin nào của khách truy cập.

Mặt khác, một trang web thương mại điện tử yêu cầu khách truy cập nhập thông tin như địa chỉ cá nhân và chi tiết thẻ tín dụng sẽ cần phải chứng minh mức độ bảo mật và tin cậy cao hơn bằng Xác thực mở rộng. Ngược lại với ví dụ trước, cửa hàng thương mại điện tử có thể thu thập dữ liệu khách hàng để sử dụng trong các chiến dịch tiếp thị, giúp dữ liệu đó phù hợp hơn với Xác thực mở rộng.

Việc trang web của khách hàng phù hợp nhất với SSL đơn, ký tự đại diện hay đa miền sẽ phụ thuộc vào cấu trúc của nó. Ví dụ: trang web quán cà phê một trang sẽ không cần bất cứ thứ gì ngoài một tên miền. Mặt khác, cửa hàng thương mại điện tử có thể có nhiều trang sản phẩm, trang danh mục và blog – làm cho ký tự đại diện hoặc SSL đa miền phù hợp hơn nhiều.

Điều quan trọng là phải xem xét chi phí. Chi phí chứng chỉ SSL khác nhau tùy thuộc vào loại khách hàng chọn, vì vậy hãy đảm bảo khách hàng có đủ khả năng chi trả cho chứng chỉ SSL mà khách hàng muốn cài đặt.

(*)Hint/Tip: Chọn sai chứng chỉ SSL cho trang web của khách hàng có thể tốn thời gian và tiền bạc đáng kể cũng như có khả năng khiến khách hàng hoặc khách truy cập gặp rủi ro. Hãy dành thời gian để xem xét chứng chỉ nào là tốt nhất. Nếu khách hàng bối rối, hãy tìm kiếm sự giúp đỡ từ một chuyên gia trang web.

Nhân viên hệ thống tìm hiểu và ghi chép kết quả thu thập thông tin ở Bước này vào tài liệu có tên “Bản mô tả chứng chỉ SSL” đã dùng ở Bước 2.

Biểu mẫu đầu vào của Bước này là:	Tài liệu, hồ sơ phát sinh ở Bước 2
Biểu mẫu đầu ra của Bước này là:	Bản mô tả chứng chỉ SSL

Bước 4: Chọn đơn vị cấp chứng chỉ (CA)

Cơ quan cấp chứng chỉ (CA) là tổ chức cấp chứng chỉ SSL. Có hàng chục CA hoạt động trên khắp thế giới, nhưng chỉ một số ít trong số đó sở hữu phần lớn thị phần SSL toàn cầu. Những người chơi lớn hơn này bao gồm GoDaddy và GlobalSign. Hãy chọn một CA có uy tín có thể cung cấp loại chứng chỉ SSL phù hợp với yêu cầu, đồng thời phù hợp với ngân sách và mục tiêu kinh doanh của doanh nghiệp.

Nhân viên hệ thống ghi chép kết quả thu thập thông tin ở Bước này vào tài liệu có tên “Bản mô tả chứng chỉ SSL” đã dùng ở Bước 3.

Biểu mẫu đầu vào của Bước này là:	Tài liệu, hồ sơ phát sinh ở Bước 3
Biểu mẫu đầu ra của Bước này là:	Bản mô tả chứng chỉ SSL

Bước 5: Tạo Phiếu yêu cầu cấp chứng chỉ

Yêu cầu ký chứng chỉ (CSR) (viết tắt là ‘Phiếu CSR’) là một tệp được tạo trên máy chủ web của Công ty (là khách hàng) trước khi Công ty yêu cầu chứng chỉ SSL từ CA. CA sau đó sẽ sử dụng thông tin trong tệp này để cấp chứng chỉ SSL cho Công ty.

Quá trình tạo CSR phụ thuộc vào máy chủ web và dịch vụ lưu trữ mà trang web của Công ty (là khách hàng) đang sử dụng. Nhân viên hệ thống phải liên hệ với công ty lưu trữ web của Công ty để tìm hiểu xem họ có hướng dẫn trong cơ sở kiến thức về cách tạo CSR hay không.

Biểu mẫu đầu vào của Bước này là:	Tài liệu, hồ sơ phát sinh ở Bước 4
Biểu mẫu đầu ra của Bước này là:	Phiếu CSR

Bước 6: Gửi Phiếu yêu cầu cho CA

Bây giờ Nhân viên hệ thống đã tạo CSR, bước tiếp theo là truy cập trang web của CA đã chọn và mua loại chứng chỉ SSL mà Công ty cần. Sau khi hoàn tất quá trình thanh toán, CA sẽ yêu cầu Công ty gửi tệp CSR mà Nhân viên hệ thống đã tạo ở bước trước.

Biểu mẫu đầu vào của Bước này là:	Tài liệu, hồ sơ phát sinh ở Bước 5
Biểu mẫu đầu ra của Bước này là:	Phiếu CSR

Bước 7: Chờ CA trả lời

Tùy thuộc vào loại chứng chỉ SSL Công ty mua, CA có thể mất từ vài giờ đến vài ngày để xác thực thông tin chi tiết của Công ty và cấp chứng chỉ SSL cho trang web của Công ty - *việc lấy chứng chỉ xác thực tên miền thường mất vài phút, trong khi quá trình xác thực mở rộng có thể mất vài ngày.*

Nếu Phiếu Yêu cầu không có sai sót và hợp lệ, CA sẽ gửi cho Công ty một email cho phép Công ty truy cập chứng chỉ SSL của mình; hoặc có thể tải xuống từ tài khoản người dùng đã tạo khi mua chứng chỉ rồi thực hiện tiếp Bước 8.

Nếu Phiếu Yêu cầu có sai sót, CA sẽ gửi cho Công ty một email báo làm lại Phiếu Yêu cầu, quay lại thực hiện Bước 5.

Biểu mẫu đầu vào của Bước này là:	Tài liệu, hồ sơ phát sinh ở Bước 6
Biểu mẫu đầu ra của Bước này là:	Phiếu CSR

Bước 8: Cài đặt chứng chỉ SSL

Khi CA đã xử lý yêu cầu chứng chỉ SSL của Công ty, CA sẽ gửi cho Công ty một email cho phép Công ty truy cập chứng chỉ SSL của mình. Nhân viên hệ thống của Công ty có thể tải xuống từ tài khoản người dùng Công ty đã tạo khi mua chứng chỉ.

Quá trình cài đặt chứng chỉ SSL tùy thuộc vào hệ điều hành (hệ điều hành) của máy chủ web nơi trang web của Công ty được lưu trữ. Liên hệ với máy chủ web của Công ty để biết thêm thông tin về vấn đề này hoặc kiểm tra xem nó có cung cấp bất kỳ hướng dẫn trực tuyến nào về cách cài đặt chứng chỉ SSL của Công ty hay không.

(*)*Hint/Tip: Điều quan trọng là luôn sử dụng chứng chỉ SSL cho toàn bộ trang web của Công ty chứ không chỉ cho các trang cụ thể.*

Bước 9: Kiểm thử và bảo trì chứng chỉ

Nhân viên hệ thống của Công ty đã cài đặt xong chứng chỉ SSL của mình. Công việc khó khăn đã xong. Nhưng nó vẫn chưa kết thúc.

Phương pháp hay nhất yêu cầu chủ sở hữu trang web nên kiểm tra chứng chỉ SSL của họ và tạo lịch bảo trì. Điều này sẽ giúp Công ty yên tâm và đảm bảo rằng chứng chỉ của Công ty không bị lỗi hoặc hết hạn mà Công ty không biết.

Bước đầu tiên là kiểm tra SSL của Công ty. Điều này có thể được thực hiện bằng cách sử dụng các công cụ xác minh SSL như Digicert hoặc SSL Shopper. Những công cụ này sẽ cung cấp cho Công ty thông tin cần thiết như liệu tất cả các trang trên trang web của Công ty có đang tải an toàn hay không.

Tiếp theo, Công ty nên tạo lịch (và đặt lời nhắc) để thường xuyên theo dõi ngày hết hạn và gia hạn chứng chỉ SSL của mình. Thông thường, SSL sẽ có thời hạn 13 tháng, nhưng Công ty cần kiểm tra chi tiết cụ thể về chứng chỉ của mình để đảm bảo không bỏ lỡ thời hạn hết hạn.

Cách tốt nhất là gia hạn chứng chỉ SSL và cập nhật cài đặt của nó trên trang web hoặc máy chủ của Công ty trước khi nó hết hạn. Điều này có thể giúp Công ty tránh được nhiều rắc rối và đảm bảo không có khoảng thời gian nào trang web của Công ty không có SSL.

(*)*Hint/Tip: Kiểm tra SSL của Công ty là điều cần thiết. Việc kiểm tra sẽ giúp Công ty phát hiện và sửa những lỗi này trước khi chúng trở thành vấn đề. Một cách dễ dàng để kiểm tra sự cố là thông qua công cụ chẩn đoán trực tuyến như SSL Server Test.*

Biểu mẫu đầu vào của Bước này là:	Tài liệu hồ sơ phát sinh ở Bước 7
Biểu mẫu đầu ra của Bước này là:	Biên bản nghiệm thu kết quả

Bước 10: Báo cáo, lưu hồ sơ và kết thúc

Sau khi thực hiện xong Bước 9, nhân sự hệ thống tiếp tục tiến hành:

- Soạn và ký trước biên bản nghiệm thu;
- Báo cáo cho Trưởng bộ phận hệ thống quá trình thực hiện, kết quả thực hiện nhiệm vụ;
- Bàn giao biên bản nghiệm thu cho Trưởng bộ phận hệ thống để hậu kiểm và đồng ký xác nhận.
- Lưu hồ sơ gồm tất cả văn bản và biểu mẫu phát sinh từ Bước 1 đến Bước 10./.

Biểu mẫu đầu vào của Bước này là:	Tài liệu hồ sơ phát sinh ở Bước 9
Biểu mẫu đầu ra của Bước này là:	Tài liệu hồ sơ phát sinh từ Bước 1 đến Bước 10

./.