DANH MỤC CÁC QUY TRÌNH PHẢI NHẬN DIỆN
VÀ THỰC HIỆN QUY TRÌNH QUẢN LÝ RỦI RO

(Thời điểm ……/..../……)

ĐƠN VỊ THỰC HIỆN: PHÒNG CNTT

STT	Liệt kê các quy trình	Bộ phận thực hiện quy trình	
		Chính	Liên quan
1	QUY TRÌNH lấy chứng chỉ SSL (SSL Certificate) cho máy chủ web	Bộ phận hệ thống	Các bộ phận có liên quan thuộc Phòng CNTT
2			
3			

Người lập **Lãnh đạo đơn vị**

BẢNG NHẬN DIỆN RỦI RO TIỀM ẨN ĐÁNH GIÁ RỦI RO & HIỆU QUẢ CỦA CÁC BIỆN PHÁP KIỂM SOÁT

(Thời điểm ...../..../.....)

1. ĐƠN VỊ THỰC HIỆN: PHÒNG AN TOÀN BẢO MẬT HỆ THỐNG CNTT

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

3. MỤC TIÊU **15 ngày kể từ thời điểm nhận Yêu cầu xin cấp chứng chỉ SSL**

4. NGÀY THỰC HIỆN QUY TRÌNH QLRR dd/mm/yyyy

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
	Bước 1: Tiếp nhận yêu cầu và nguồn lực	R1: không đáp ứng yêu cầu ATTT tại nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.4 *(đây là loại rủi ro tuân thủ)*	Doanh nghiệp chưa ban hành quy trình quản lý thông tin xác thực mật theo Điều A.9.2.4 (ISO27001)	2	Tài khoản quản trị Admin (name và password) có thể bị tiết lộ cho người không được ủy quyền	6	12	Ban hành Quy trình quản lý thông tin xác thực mật tại doanh nghiệp trước khi bàn giao nguồn lực cho nhân viên hệ thống nhận việc	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
1		R2: Tài liệu hướng dẫn tạo chứng chỉ SSL (SSL certificate) cũ quá hay lạc hậu và không dùng được	Tài liệu không được cập nhật phiên bản mới nhất	2	Phải cập nhật lại tài liệu khiến cần thêm thời gian hoàn tất Bước 1	1	2	Trưởng Bộ phận hệ thống của Phòng CNTT phải phân công nhân viên hệ thống cập nhật thường xuyên tài liệu, báo cáo hàng tuần và ghi sổ theo dõi tình trạng tài liệu hàng tuần.	1	1	1	Có	Không
		R3: Phân công sai hay không đúng nhân viên hệ thống nhận công việc xin cấp chứng chỉ SSL	Nhân viên hệ thống nhận việc không có kiến thức, không có năng lực đọc tài liệu hoặc không có khả năng tự tìm hiểu việc xin cấp chứng chỉ SSL	2	Thời gian làm ở Bước 1 kéo dài không qua được Bước 2	1	2	Chọn nhân viên hệ thống có bản mô tả công việc đã từng làm qua việc này hoặc lập danh mục kiểm tra (check list) để kiểm tra trước và đánh giá năng lực nhân viên hệ thống trước khi giao việc	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
2	Bước 2: Chuẩn bị thông tin	R1: lấy chứng chỉ SSL theo địa chỉ IP chứ không phải cho tên miền cụ thể.	Nhân viên hệ thống được phân công nhầm lẫn hoặc không tìm hiểu thông tin từ CA hoặc chưa hiểu hết về mục đích bảo mật bằng chứng chỉ SSL	2	Nếu chứng chỉ không được cấp cho đúng tên miền, người dùng có thể nhận được cảnh báo bảo mật hoặc dễ bị tấn công trung gian.	1	2	(1)Trưởng bộ phận hệ thống bổ sung tên miền vào Phiếu Yêu cầu ở Bước 1 để đảm bảo rằng chứng chỉ SSL được cấp cho đúng tên miền chứ không chỉ địa chỉ IP; (2)có văn bản yêu cầu khi làm việc với nhà cung cấp dịch vụ lưu trữ của doanh nghiệp để đảm bảo rằng chứng chỉ SSL được cấu hình đúng cho từng tên miền ghi trong văn bản yêu cầu được 2 bên ký xác nhận.	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		R2: Các công cụ tìm kiếm có thể sắp xếp sai thứ hạng trang web và ảnh hưởng đến khả năng hiển thị của trang web trên công cụ tìm kiếm.	Chứng chỉ SSL không được cấu hình đúng cho từng tên miền.	2	Nếu chứng chỉ được cấp cho địa chỉ IP thay vì tên miền, chứng chỉ có thể kích hoạt cảnh báo bảo mật hoặc lỗi trong trình duyệt web, có khả năng ngăn cản người dùng truy cập trang web của doanh nghiệp.	1	2	- *Như trên* -	1	1	1	Có	Không
3	Bước 3: Chọn loại chứng	Chọn sai loại chứng chỉ	Trưởng bộ phận hệ	2	Chọn sai có thể gây	2	4	(1)Dành thời gian để xem	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
	chỉ SSL	SSL	thống và/hoặc nhân viên hệ thống được phân công nhầm lẫn hoặc không tìm hiểu kỹ từng loại chứng chỉ SSL của CA hoặc chưa hiểu hết về quy mô và tính chất hoạt động của doanh nghiệp		mất thời gian và tiền bạc đáng kể để khắc phục cũng như có khả năng khiến khách hàng truy cập gặp rủi ro *(ví dụ thay vì chọn loại xác thực mở rộng thì lại chọn loại xác thực tên miền)*			xét loại chứng chỉ SSL nào là tốt nhất; và (2) tìm kiếm sự giúp đỡ từ một chuyên gia trang web có kinh nghiệm để nhận sự hướng dẫn					
4	Bước 4: Chọn đơn vị cấp chứng chỉ (CA)	Chọn SAI đơn vị cấp chứng chỉ (CA)	Trưởng bộ phận hệ thống và/hoặc nhân viên hệ thống được phân công	2	Tổn hại đến uy tín, tiền bạc và thời gian: (1)Uy tín: chứng chỉ	2	4	Lập bảng tiêu chí chọn một CA đúng và chấm điểm CA theo từng tiêu chí này trước khi ra quyết	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
			nhầm lẫn hoặc không tìm hiểu kỹ từng đơn vị CA hoặc chưa hiểu hết về sản phẩm của từng đơn vị CA khi ra quyết định chọn lựa nhà cung cấp chứng chỉ		SSL từ CA không đáng tin cậy có thể không được các trình duyệt chính nhận dạng, gây ra cảnh báo bảo mật. Nếu thông tin nhạy cảm của khách hàng bị xâm phạm, khách truy cập không tin tưởng vào trang web của doanh			định chọn CA. Tiêu chí gồm các yếu tố như phù hợp với chính sách ATTT, nhu cầu của doanh nghiệp, ngân sách cho dự án, thành tích của CA về bảo mật, khả năng chứng chỉ tương thích với trình duyệt, dịch vụ hỗ trợ khách hàng, danh tiếng trong ngành, CA được các trình duyệt web lớn công nhận và tin cậy, CA tuân thủ các thông lệ tốt nhất của ngành về việc cấp và					

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
					nghiệp. (2)Tiền bạc: tốn kém về chi phí mua chứng chỉ và chi phí thu hồi và thay thế; (3)Thời gian: thủ tục nhận chứng chỉ từ CA không phù hợp có thể là một quá trình dài. Điều này có thể làm gián đoạn quy trình của doanh nghiệp			quản lý chứng chỉ SSL.					

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
					hoặc trì hoãn việc ra mắt trang web của doanh nghiệp; (4)chi phí ẩn khác phát sinh do các rủi ro bảo mật và tuân thủ xảy ra khi chọn sai.								
5	Bước 5: Tạo Phiếu yêu	R1: chứng chỉ SSL được tạo có thể không tương thích với máy chủ của nhà cung cấp dịch vụ lưu trữ trang web nên gặp các vấn đề về cài đặt,	Nhân viên hệ thống được phân công không tham khảo ý kiến nhà cung cấp dịch vụ lưu trữ trang web của doanh nghiệp	2		3	6	Trưởng bộ phận hệ thống và nhân viên hệ thống phân công phải có văn bản xác nhận đồng ý về dự thảo CSR của nhà cung cấp dịch vụ trang web của doanh nghiệp	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
	cầu cấp chứng chỉ "Certificate signing request - **(CSR)**"	cấu hình và bảo mật						về nội dung **CSR** trước khi gửi CSR cho CA (làm Bước 6)					
	Bước 5: Tạo Phiếu yêu cầu cấp chứng chỉ "Certificate signing request - **(CSR)**" *(*)(CSR) là một tệp được tạo trên máy*	R2: Gặp sự cố trong quá trình cài đặt hoặc cấu hình chứng chỉ.	Nhân viên hệ thống được phân công không tham khảo ý kiến nhà cung cấp dịch vụ lưu trữ trang web của doanh nghiệp	2	Có thể bị thu hồi và tạo chứng chỉ mới. Thu hồi chứng chỉ có thể là một quá trình phức tạp và có thể phát sinh thêm chi phí, đặc biệt là nếu chứng chỉ đã được Cơ quan cấp chứng chỉ (CA) cấp.	3	6	- *Như trên* -	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
	chủ web của doanh nghiệp trước khi doanh nghiệp yêu cầu chứng chỉ SSL từ CA. CA sẽ sử dụng thông tin trong tệp này để cấp chứng chỉ SSL.	R3: Tăng khả năng xảy ra sự cố về tính tương thích hoặc do xuất hiện lỗ hổng bảo mật	Nhân viên hệ thống được phân công không tham khảo ý kiến nhà cung cấp dịch vụ lưu trữ trang web của doanh nghiệp	2	Không có sự hỗ trợ hoặc hướng dẫn có giá trị của nhà cung cấp dịch vụ lưu trữ trang web, khiến việc giải quyết mọi sự cố phát sinh trong quá trình triển khai chứng chỉ trở nên khó khăn hơn.	3	6	- *Như trên* -	1	1	1	Có	Không
		R4: Gây ra rủi ro bảo mật do tạo CSR với các tham số	Nhân viên hệ thống được phân công không tham khảo ý	2	Giảm tính bảo mật của chứng chỉ SSL và	3	6	- *Như trên* -	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		không chính xác	kiến nhà cung cấp dịch vụ lưu trữ trang web của doanh nghiệp		trang web của bạn. *(ví dụ, sử dụng thuật toán mã hóa yếu hoặc kích thước khóa không đủ có thể khiến chứng chỉ SSL dễ bị tấn công 'brute-force' hoặc lỗ hổng mật mã)*								
6	Bước 6: Gửi Phiếu yêu cầu cho CA	Không đáp ứng yêu cầu ATTT khi gửi CSR cho CA (hay rủi ro tuân thủ	Không sử dụng phương pháp truyền tin an toàn, chẳng hạn như	2	Bị phát hành chứng chỉ sai nếu CSR bị xâm	4	8	Áp dụng nguyên tắc 4 mắt: (1)Bố trí thêm một người giám sát ở bên cạnh	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		do không đáp ứng Nhóm A.13 Yêu cầu A.13.2 Điều A.13.2.1 và A.13.2.3 theo Phụ lục A – ISO 27001:2013)	HTTPS hoặc email được mã hóa, để bảo vệ tính bảo mật của CSR trong quá trình truyền.		phạm hoặc bị tin tặc chặn lại: CSR có khả năng bị sử dụng để lấy chứng chỉ SSL một cách gian lận.			nhân viên hệ thống phân công sắp gửi CSR cho CA; (2)Sử dụng ứng dụng email có thiết lập bảo mật (như Gmail…) để gửi CSR cho CA và email chỉ được gửi đi khi ứng dụng nhận lệnh Send từ 2 người *(tức là có V&V- "verification and validation")*					
		R1: Rủi ro về giao tiếp giữa CA và nhân viên hệ thống được phân công	Nhân viên hệ thống được phân công sao lãng công việc, chậm trả lời cho CA hoặc CA	2	Theo thời gian chờ kéo dài sẽ làm giảm tính bảo mật và khả dụng của trang	2	4	Thiết lập KPI cho nhân viên hệ thống được phân công kết hợp bổ sung thêm nhân viên hệ thống có năng lực giao	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
7	Bước 7: Chờ CA trả lời		phản hồi chậm		web nếu đang chờ triển khai chứng chỉ SSL để bảo mật các giao dịch hoặc thông tin liên lạc nhạy cảm			tiếp cùng nhân viên hệ thống được phân công theo dõi phản hồi từ CA và phản hồi kịp thời cho CA.					
		R2: Rủi ro bảo mật do có một khoảng thời gian trang web của doanh nghiệp không được bảo vệ bằng SSL nên khả năng gặp rủi ro về bảo mật cho người dùng tăng lên khi	Cơ quan cấp chứng chỉ (CA) phản hồi chậm hoặc nhân viên hệ thống được phân công sao lãng, không theo dõi trả lời về CSR của CA	2	Nếu trang web dựa vào mã hóa SSL cho các hoạt động kinh doanh thiết yếu như giao dịch thương mại điện tử hoặc thông tin liên lạc an	2	4	(1)Lên kế hoạch trước và bắt đầu quá trình lấy hoặc gia hạn chứng chỉ SSL trước ngày hết hạn của chứng chỉ hiện tại; (2)Chọn một CA có uy tín và phản hồi nhanh với quy trình xác thực đáng tin cậy để giảm thiểu sự chậm	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		thời gian chờ trả lời kéo dài.			toàn, vấn đề chậm trễ sẽ làm gián đoạn tính liên tục của hoạt động kinh doanh và ảnh hưởng đến doanh thu hoặc lòng tin của khách hàng.			trễ; (3)Triển khai các biện pháp bảo mật tạm thời, chẳng hạn như sử dụng chứng chỉ tạm thời hoặc duy trì các bản sao lưu an toàn, để giảm thiểu tác động của bất kỳ sự chậm trễ nào trong việc cấp chứng chỉ SSL.					
		R3: Không bảo vệ được *"confiden _tiality and integrity"* cho tệp CSR lưu trên máy chủ Web	Các kiểm soát truy cập vào máy chủ và kỹ thuật mã hóa yếu kém trên máy chủ; hoặc máy chủ Web có lỗ hổng bảo	2	Bất kỳ sự xâm phạm nào đối với CSR hoặc khóa riêng trong thời gian chờ này đều	4	8	Sao lưu an toàn tệp CSR ở phân vùng mạng riêng và mã hóa tệp CSR khi lưu trữ v.v.	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
			mật nhưng chưa được vá kịp thời đã đưa vào hoạt động.		có khả năng dẫn đến việc cấp chứng chỉ SSL trái phép hoặc các sự cố bảo mật khác.								
8	Bước 8: Cài đặt chứng chỉ SSL	R1: Khả năng tương thích kém hoặc gặp vấn đề về khả năng tương thích với máy chủ của nhà cung cấp dịch vụ	Nhân viên hệ thống cài đặt chứng chỉ đã không tham khảo ý kiến nhà cung cấp dịch vụ lưu trữ trang web của doanh nghiệp	2	Trang web của doanh nghiệp không hoạt động bình thường hoặc gây ra các lỗi không mong muốn.	4	2	(1)Ký hợp đồng với nhà cung cấp dịch vụ lưu trữ trang web có điều khoản quy định phải có sự tham gia của họ trong quá trình cài đặt chứng chỉ SSL; (2) Biên bản nghiệm thu cài đặt chứng chỉ	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								phải có chữ ký xác nhận cài đặt chứng chỉ thành công của nhà cung cấp dịch vu…mới cho nghiệm thu và xác nhận thành tích của nhân viên hệ thống được phân công.					
		R2: Phát sinh các lỗ hổng bảo mật hoặc sự cố về hiệu suất vận hành do có lỗi khi cấu hình.	*-Như trên -*	2	Trang web của doanh nghiệp dễ bị tin tặc tấn công hoặc cấu hình sai.	4	8	*-Như trên -*	1	1	1	Có	Không
		R3: Có thể xảy ra sự cố máy chủ Web ngừng	*-Như trên -*	2	Ảnh hưởng tiêu cực đến trải nghiệm	4	8	*-Như trên -*	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		hoạt động sau khi cài đặt chứng chỉ SSL			của người dùng, thứ hạng tìm kiếm trên công cụ tìm kiếm (SEO) và hoạt động kinh doanh.								
		R4: Không có ai hỗ trợ khi gặp sự cố	*-Như trên -*	2	Thời gian khắc phục sự cố kéo dài hoặc tăng tần suất xảy ra sự cố	4	8	*-Như trên -*	1	1	1	Có	Không
9	Bước 9: Kiểm thử và bảo trì chứng chỉ SSL	Xảy ra lỗi không tương thích hoặc xuất hiện cảnh báo bảo mật hoặc cảnh báo chứng chỉ	Không kiểm thử chứng chỉ SSL trước khi sử dụng hoặc không kiểm thử nghiệm thu như yêu cầu	2	Gây ra lỗi cho khách truy cập trang web; khách truy cập nhận cảnh báo bảo mật; và	2	4	Trước khi triển khai sử dụng chứng chỉ SSL vào máy chủ Production của doanh nghiệp, phải có: (1)Biên bản	1	1	1	Có	Không

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		không đáng tin hoặc hiệu suất thi hành trang web giảm	ở Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.9 – Phụ lục A – ISO 27001:2013		làm giảm lòng tin vào trang web của bạn; bị phạt do không tuân thủ quy định ATTT đã cam kết			nghiệm thu kết quả kiểm tra được xác nhận bởi Trưởng Phòng CNTT, Trưởng bộ phận hệ thống và nhân viên hệ thống; (2)Kiểm tra chứng chỉ SSL bao gồm xác minh cấu hình của chứng chỉ, kiểm tra khả năng tương thích với các trình duyệt và thiết bị khác nhau, đảm bảo chuỗi chứng chỉ hoàn chỉnh,					

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra	Mức độ nghiêm trọng (Sev)	Tổng điểm RPN[1] = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ nghiêm trọng (Sev[2])	Tổng điểm RPN[2] = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								và đánh giá tác động về hiệu suất của mã hóa SSL/TLS.					
10	Bước 10: Báo cáo, lưu hồ sơ và kết thúc	Biên bản nghiệm thu không có đủ chữ ký nhưng vẫn đưa vào lưu trữ	Trưởng bộ phận hệ thống làm việc thiếu trách nhiệm, sai quy định	2	Vi phạm quy định về lưu hồ sơ tại doanh nghiệp; trách nhiệm giải trình về chất lượng hệ thống khi có sự cố xảy ra khó xác định	2	4		1	1	1	Có	Không

Đơn vị khác có tham gia ĐGRR	Họ tên	Chữ ký

Người lập **Lãnh đạo đơn vị**

BẢNG NHẬN DIỆN RỦI RO TIỀM ẨN ĐÁNH GIÁ RỦI RO & HIỆU QUẢ CỦA CÁC BIỆN PHÁP KIỂM SOÁT

(Thời điểm ...../..../.....)

1. ĐƠN VỊ THỰC HIỆN:

2. QUY TRÌNH:

3. NGÀY THỰC HIỆN ……..

QUY TRÌNH QLRR:

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn	Nguyên nhân của rủi ro	Khả năng xảy ra	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Tổng điểm R1 = 5x7	Biện pháp kiểm soát hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Tổng điểm R2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
1													
2													

Đơn vị khác có tham gia ĐGRR	Họ tên	Chữ ký

Người lập **Lãnh đạo đơn vị**