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

(Thời điểm ...../..../.....)

ĐƠN VỊ THỰC HIỆN: PHÒNG AN TOÀN BẢO MẬT HỆ THỐNG TT

STT	Liệt kê các quy trình	Bộ phận thực hiện quy trình	
		Chính	Liên quan
1	Quy trình giám sát xử lý cảnh báo về an ninh mạng trên thiết bị IPS ("Intrusion Prevention System" - Hệ thống Ngăn chặn Xâm nhập)	Bộ phận quản trị Mạng và Bảo mật – Phòng ATBM HTTT	Các bộ phận có liên quan thuộc Phòng Hạ tầng
2	…		
3	…		

Người lập **Lãnh đạo đơn vị**

ABC **BM__-QT__/QLRR**

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 TT

2. QUY TRÌNH: QUY TRÌNH GIÁM SÁT XỬ LÝ CẢNH BÁO VỀ AN NINH MẠNG TRÊN THIẾT BỊ IPS

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	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 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	Bước 1: Nhận cảnh báo từ hệ thống IPS	Hệ thống không gửi cảnh báo đến người quản trị	Hệ thống email bị lỗi	1	Không phát hiện được cảnh báo	3	3	Nhân sự Bộ phận Mạng và thiết bị bảo mật giám sát trên màn hình cảnh báo của hệ thống IPS trong giờ làm việc.	1	1	1	Có	Không
2	Bước 2: Phân loại cảnh báo	Xác định không đúng	Kiểm tra thông tin	1	Hệ thống	3	3	Việc kiểm tra cảnh báo gồm	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	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		loại cảnh báo	cảnh báo không đầy đủ.		có thể bị tấn công			có nhân sự Bộ phận Mạng và thiết bị bảo mật kết hợp với Phòng Hạ tầng và kết quả phân loại được kiểm soát bởi lãnh đạo Phòng Bảo mật nên khả năng rủi ro xảy ra là rất thấp.					
3	Bước 3: Xử lý cảnh báo	Không có rủi ro khi thực hiện bước này											
4	Bước 4: Xử lý cảnh báo malware theo kịch bản xử lý sự cố liên quan đến virus trong hệ thống mạng.	Có kịch bản nhưng kịch bản không thực thi được một số bước	Kịch bản cũ, thiếu thông tin	2	Không thể xử lý sự cố theo kịch bản	1	2	Cập nhật kịch bản định kỳ theo bản hiện hành của Khối CNTT lưu trên hệ thống s-office 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	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
5	Bước 5: Kiểm tra hệ thống bảo mật	Nhân sự không thực hiện	Nhân sự nghỉ việc hoặc không ở nơi làm việc	1	Hệ thống có thể bị tấn công	3	3	Luôn phân công nhân sự dự phòng khi có nhân sự nghỉ việc hoặc không ở nơi làm việc.	1	1	1	Có	Không
6	Bước 6: Kiểm tra hệ thống máy chủ, máy tính người dùng	Nhân sự không thực hiện	Nhân sự nghỉ việc hoặc không ở nơi làm việc	1	Hệ thống có thể bị tấn công	3	3	Luôn phân công nhân sự dự phòng khi có nhân sự nghỉ việc hoặc không ở nơi làm việc.	1	1	1	Có	Không
7	Bước 7: Lập kịch bản xử lý và trình phê duyệt kịch bản	Kịch bản xử lý chưa hoàn chỉnh	Nhân sự thực hiện chưa có kinh nghiệm để thu thập thông tin để đánh giá chính xác sự cố xảy ra.	1	Hệ thống có thể bị tấn công	3	3	- Phân công nhân sự có kinh nghiệm để thực hiện kiểm tra hệ thống và xây dựng kịch bản xử lý sự cố.	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	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								- Lãnh đạo Phòng Bảo mật xem xét và góp ý để hoàn chỉnh kịch bản xử lý sự cố.					
8	Bước 8: Phê duyệt kịch bản	Lãnh đạo Khối CNTT không có mặt tại nơi làm việc của Doanh nghiệp	Lãnh đạo Khối CNTT đi họp bên ngoài	2	Kịch bản không được Lãnh đạo Khối CNTT phê duyệt nhanh	2	4	Giám đốc cấp phép cho lãnh đạo Khối CNTT phê duyệt kịch bản qua điện thoại Video hoặc qua ứng dụng Zalo	1	1	1	Có	Không
9	Bước 9: thực hiện kịch bản xử lý	Kịch bản thực hiện không thành công	Xây dựng kịch bản chưa phù hợp	1	Hệ thống có thể bị tấn công	3	3	-Phối hợp với các đơn vị liên quan, cử nhân sự có kinh nghiệm tham gia xây dựng kịch bản trước	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	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								khi trình phê duyệt. -Mời chuyên gia của các đối tác tham gia xây dựng kịch bản hoặc trong trường hợp cần thiết có thể yêu cầu hỗ trợ qua Mạng lưới ứng cứu sự cố của Công ty dịch vụ FPT/Viettel					
10	Bước10: Kiểm soát	Trưởng Phòng Bảo mật không có mặt tại nơi làm việc của Doanh nghiệp	Trưởng Phòng Bảo mật đi họp bên ngoài hoặc nghỉ phép năm	2	Việc kiểm soát thực hiện Kịch bản không làm được	2	4	Lãnh đạo Khối CNTT cấp phép cho Phó phòng Bảo mật (thay cho Trưởng Phòng) kiểm soát kết quả thực hiện	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	Hậu quả có thể gây ra	Mức độ ảnh hưởng	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								kịch bản và ra quyết định					
11	Bước 11: Lập báo cáo và lưu hồ sơ	Không lưu hoặc lưu không đầy đủ hồ sơ	Thiếu giám sát, kiểm tra công việc của nhân viên; nhân viên làm việc cẩu thả…	1	Thất lạc hồ sơ, không có cơ sở khi cần kiểm tra đối chiếu	2	2	Tổ chức giám sát, kiểm tra gồm: - Nhân sự xử lý cảnh báo xong tập hợp hồ sơ chuyển Trưởng Bộ phận quản trị mạng và thiết bị bảo mật kiểm tra đầy đủ tài liệu trước khi lưu trữ. - Thường xuyên kiểm tra, kịp thời phát hiện sai sót trong công	1	1	1	Có	Không

ABC **BM__-QT__/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	Số RPN1 = 5x7	Biện pháp kiểm soát (BPKS) hiện hữu	Đánh giá lại rủi ro & cơ hội			Hành động đề nghị	
									Khả năng xảy ra	Mức độ ảnh hưởng	Số RPN2 = 10x11	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								việc lưu hồ sơ để khắc phục					

Đơn vị khác có tham gia ĐGRR	Họ tên	Chữ ký

Người lập **Lãnh đạo đơn vị**