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

(Thời điểm ...../..../.....)

ĐƠN VỊ THỰC HIỆN:

STT	Liệt kê các quy trình	Bộ phận thực hiện quy trình	
		Chính	Liên quan
1	Quy trình xử lý sự cố máy tính nhiễm virus / malware	Bộ phận An toàn thông tin	- Lãnh đạo các Phòng/Ban/Đơn vị trực thuộc Công ty. - Bên thứ 3: Hãng Trend Micro

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: **XỬ LÝ SỰ CỐ MÁY TÍNH NHIỄM VIRUS / MALWARE**

3. NGÀY THỰC HIỆN QUY TRÌNH QLRR: 12/06/2025

4. MỤC TIÊU[1] **14 ngày kể từ thời điểm nhận Phiếu Yêu cầu xử lý sự cố máy tính nhiễm virus/ malware**

stt	Các bước thực hiện quy trình *(Steps of process)*	Rủi ro tiềm ẩn *(The potential risks)*	Nguyên nhân của rủi ro *(Causes of risk)*	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra *(Consequences)*	Mức độ ảnh hưởng (Sev)	Số RPN[1] = (5)x(7)	Biện pháp kiểm soát (BPKS) hiện hữu *(the current controls)*	Đánh giá lại rủi ro& cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ ảnh hưởng (Sev[2])	Số RPN[2] =(10)x(11)	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: Lập kế hoạch xử lý sự cố	Có thể xảy ra việc đánh giá sai phạm vi và mức độ lây nhiễm	Thiếu thông tin về virus/malware, chủ quan trong đánh giá	3	Lập kế hoạch sai phạm vi có thể dẫn đến mất 1-2 ngày xử lý lại và ảnh hưởng tới thêm nhiều thiết bị bởi cơ chế lây lan	4	12	- Yêu cầu danh sách máy tính bị lây nhiễm từ các đơn vị, đánh giá theo checklist chuẩn; báo	2	4	8	Có	Không

[1] *Nếu có khai báo mục tiêu thì mục tiêu phải có một giá trị đo đếm được để giúp nhận ra rủi ro tiềm ẩn và hỗ trợ quản lý rủi ro (xem lại các ví dụ áp dụng FMEA cho các Quy trình đã học – Chương 7).*

stt	Các bước thực hiện quy trình *(Steps of process)*	Rủi ro tiềm ẩn *(The potential risks)*	Nguyên nhân của rủi ro *(Causes of risk)*	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra *(Consequences)*	Mức độ ảnh hưởng (Sev)	Số RPN[1] = (5)x(7)	Biện pháp kiểm soát (BPKS) hiện hữu *(the current controls)*	Đánh giá lại rủi ro& cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ ảnh hưởng (Sev[2])	Số RPN[2] =(10)x(11)	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
								cáo phải được lãnh đạo duyệt - Cập nhật thông tin về các chủng virus mới					
2	Bước 2: Thực hiện kế hoạch	Có thể xảy ra tình trạng virus tiếp tục lây lan do không cô lập kịp thời	Nhân sự thao tác chậm, thiếu hướng dẫn hoặc không tuân theo kịch bản	4	Virus tiếp tục lây lan khiến >20 máy tính trong mạng LAN bị ảnh hưởng.	5	20	- Có kịch bản hành động cụ thể, hướng dẫn ngắt kết nối mạng, sử dụng phần mềm diệt virus theo quy định. - Thêm người hướng dẫn và giám sát nhân viên thực hiện	2	4	4	Có	Không

stt	Các bước thực hiện quy trình *(Steps of process)*	Rủi ro tiềm ẩn *(The potential risks)*	Nguyên nhân của rủi ro *(Causes of risk)*	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra *(Consequences)*	Mức độ ảnh hưởng (Sev)	Số RPN[1] = (5)x(7)	Biện pháp kiểm soát (BPKS) hiện hữu *(the current controls)*	Đánh giá lại rủi ro& cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ ảnh hưởng (Sev[2])	Số RPN[2] =(10)x(11)	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
3	Bước 3: Kiểm tra kết quả lần 1	Có thể xảy ra việc bỏ sót máy tính vẫn còn nhiễm virus	Rà soát không toàn diện, chỉ tập trung một số khu vực	3	Bỏ sót máy nhiễm virus làm virus hoạt động trở lại sau 1-2 ngày, gây mất uy tín phòng IT	4	12	Rà soát theo danh sách từng khu vực, đối chiếu với cảnh báo phần mềm, phân công kiểm tra độc lập	1	4	4	Có	Không
4	Bước 4: Tìm hỗ trợ của bên thứ ba	Có thể xảy ra tình trạng chậm phản hồi từ hãng phần mềm bảo mật	Chưa có đầu mối liên hệ rõ ràng hoặc hợp đồng không có SLA	3	Chậm phản hồi từ Trend Micro làm trì hoãn xử lý thêm 2-3 ngày, kéo dài nguy cơ lan nhiễm.	3	9	Gửi mẫu virus kèm mô tả kỹ thuật, sử dụng email khẩn có cc lãnh đạo.	2	3	6	Có	Không
5	Bước 5: Cập nhật phiên bản antivirus	Có thể xảy ra tình trạng không đồng bộ cập nhật antivirus	Cập nhật thủ công, không kiểm tra kỹ	3	Thiếu cập nhật khiến 30% máy trạm không được bảo vệ đúng cách, có thể bị tái nhiễm.	3	9	Sử dụng công cụ kiểm tra tập trung, lập danh sách cập nhật,	1	3	3	Có	Không

stt	Các bước thực hiện quy trình *(Steps of process)*	Rủi ro tiềm ẩn *(The potential risks)*	Nguyên nhân của rủi ro *(Causes of risk)*	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra *(Consequences)*	Mức độ ảnh hưởng (Sev)	Số RPN[1] = (5)x(7)	Biện pháp kiểm soát (BPKS) hiện hữu *(the current controls)*	Đánh giá lại rủi ro& cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ ảnh hưởng (Sev[2])	Số RPN[2] =(10)x(11)	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		giữa các máy						yêu cầu xác nhận.					
6	Bước 6: Quét virus / malware lần 2	Có thể xảy ra tình trạng dùng phần mềm cũ để quét	Nhân sự quên cập nhật phiên bản mới	3	Dùng phần mềm cũ để quét không phát hiện được mẫu virus mới, bỏ sót 5-10 máy.	4	12	Yêu cầu kiểm tra phiên bản trước khi quét, thực hiện theo kịch bản chi tiết.	1	4	4	Có	Không
7	Bước 7: Kiểm tra kết quả lần 2	Có thể xảy ra việc vẫn còn máy nhiễm virus không được xử lý	Quá trình kiểm tra bị lặp lại sai sót như lần đầu	3	Máy vẫn còn nhiễm có thể bị lợi dụng để làm máy chủ C2, ảnh hưởng toàn bộ mạng.	4	12	Rà soát kỹ bằng danh sách máy còn lại, xác minh với người dùng từng bộ phận.	2	4	8	Có	Không
8	Bước 8: Kiểm tra và cải tiến	Có thể xảy ra việc không ghi nhận bài học và không cải	Thiếu quy định hoặc trách nhiệm ghi nhận chưa rõ	2	Không rút ra bài học làm quy trình không cải tiến, lỗi cũ tiếp tục lặp lại ở lần sau.	4	8	Tổng hợp bài học sau xử lý, cập nhật kịch bản và	1	4	4	Có	Không

stt	Các bước thực hiện quy trình *(Steps of process)*	Rủi ro tiềm ẩn *(The potential risks)*	Nguyên nhân của rủi ro *(Causes of risk)*	Khả năng xảy ra (Occ)	Hậu quả có thể gây ra *(Consequences)*	Mức độ ảnh hưởng (Sev)	Số RPN[1] = (5)x(7)	Biện pháp kiểm soát (BPKS) hiện hữu *(the current controls)*	Đánh giá lại rủi ro& cơ hội			Hành động đề nghị	
									Khả năng xảy ra (Occ[2])	Mức độ ảnh hưởng (Sev[2])	Số RPN[2] =(10)x(11)	Duy trì BPKS hiện hữu	Bổ sung/thay thế BPKS hoặc hành động khác
		tiến quy trình						hướng dẫn người dùng.					
9	Bước 9: Báo cáo kết quả xử lý	Có thể xảy ra việc báo cáo không đúng cấp hoặc thiếu nội dung	Không có mẫu báo cáo hoặc không kiểm tra nội dung trước khi gửi	2	Báo cáo không đầy đủ khiến cấp trên không nắm được rủi ro tiềm ẩn, không ra quyết định đúng lúc.	3	6	Duyệt báo cáo trước khi gửi, đính kèm dữ liệu xử lý.	1	3	3	Có	Không
10	Bước 10: Lưu hồ sơ	Có thể xảy ra việc lưu trữ không đầy đủ hoặc thất lạc	Không có hệ thống lưu trữ tập trung hoặc lưu sai vị trí	3	Thất lạc hồ sơ khiến việc truy vết, minh chứng với audit hoặc cơ quan quản lý bị gián đoạn.	3	9	Lưu bản cứng theo phân cấp; lưu bản mềm trên hệ thống tập trung có phân quyền.	1	2	2	Có	Không

Đơn vị khác có tham gia ĐGRR	Họ tên	Chữ ký

Người lập **Lãnh đạo đơn vị**

[Tên doanh nghiệp] **BM03-QTx/QLRR**

KẾ HOẠCH HÀNH ĐỘNG

(Thời điểm ...../..../.....)

1. ĐƠN VỊ THỰC HIỆN: *[tên Phòng/Ban thuộc doanh nghiệp]*……..

2. QUY TRÌNH: *[Tên quy trình]*

3. NGÀY THỰC HIỆN QUY TRÌNH QLRR: *[dd/mm/yyyy]*

STT	Rủi ro đề xuất kế hoạch hành động	Bước quy trình liên quan đến rủi ro	Phương án xử lý rủi ro đề xuất	Dự kiến nguồn lực, chi phí để thực hiện	Đơn vị/ cá nhân thực hiện		Lịch trình triển khai	Thời hạn hoàn thành
					Chính	Phối hợp hỗ trợ		

Người lập **Lãnh đạo đơn vị** **Cấp thẩm quyền**