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

(Thời điểm 11/06/2025)

ĐƠN VỊ THỰC HIỆN: PHÒNG CÔNG NGHỆ THÔNG TIN VÀ VẬN HÀNH DOANH NGHIỆP

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 HỆ THỐNG IPS	PHÒNG CÔNG NGHỆ THÔNG TIN VÀ VẬN HÀNH DOANH NGHIỆP	TRUNG TÂM VẬN HÀNH (NOC) TRUNG TÂM SOC

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 11/06/2025)

1. ĐƠN VỊ THỰC HIỆN: PHÒNG CÔNG NGHỆ THÔNG TIN VÀ VẬN HÀNH DOANH NGHIỆP

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

3. NGÀY THỰC HIỆN QUY TRÌNH QLRR: 11/06/2025

4. MỤC TIÊU[1] *[Ghi ra mục tiêu của quy trình (nếu có)]*

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. Nhận cảnh báo từ hệ thống IPS*	*Không nhận được cảnh báo kịp thời*	*Hệ thống không giám sát 24/7*	*3*	*Bỏ sót tấn công, hệ thống bị xâm nhập*	*5*	*15*	*Trưởng phòng CNTT phải phân công cho nhân viên chia ca giám sát hệ thống.*	*2*	*5*	*10*	*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
2	*Bước 2. Phân loại cảnh báo*	*Phân loại sai mức độ cảnh báo*	*Nhân viên thiếu kinh nghiệm*	*2*	*Mất thời gian, tiền bạc đáng kể để khắc phục*	*4*	*8*	*Trưởng phòng CNTT tiến hành đào tạo cho nhân viên định kỳ*	*1*	*4*	*4*	*Có*	*Không*
3	*Bước 3. Xử lý cảnh báo*	*Xử lý nhầm cảnh báo giả, bỏ sót cảnh báo thật*	*Không có công cụ hỗ trợ trong việc kiểm tra log*	*3*	*Gây thiệt hại đáng kể về tiền bạc nếu như cảnh báo thật bị bỏ qua*	*4*	*12*	*Sử dụng hệ thống soát log tự động, phân tích thêm bằng SIEM*	*2*	*4*	*8*	*Có*	*Không*
4	*Bước 4. Xử lý cảnh báo Malware*	*Không xử lý hết mã độc, tái nhiễm*	*Thiếu cập nhật kịch bản, thiếu công cụ diệt virus*	*2*	*Lây nhiễm diện rộng, mất dữ liệu*	*4*	*8*	*Thêm phần mềm diệt virus bản quyền*	*1*	*4*	*4*	*Có*	*Không*
5	*Bước 5. Kiểm tra hệ thống bảo mật*	*Không phát hiện lỗ hổng, lỗi bảo mật*	*Thiếu cập nhật bản vá, kiểm tra hình thức*	*2*	*Hệ thống tiếp tục bị tấn công gây gián đoạn dịch vụ*	*5*	*10*	*Rà soát định kỳ, cập nhật bản vá*	*1*	*5*	*5*	*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
6	*Bước 6. Kiểm tra hệ thống máy chủ, máy tính người dùng*	*Bỏ sót máy tính/máy chủ nhiễm mã độc*	*Quản lý thiết bị chưa đầy đủ, thiếu quét AV*	*3*	*Nguy cơ lây nhiễm nội bộ, mất dữ liệu*	*3*	*9*	*Quét AV, kiểm tra hệ thống, phần mềm quản lý tài sản*	*1*	*3*	*3*	*Có*	*Không*
7	*Bước 7. Lập kịch bản xử lý và trình phê duyệt kịch bản*	*Kịch bản không đầy đủ, thiếu phê duyệt*	*Tổng hợp thiếu thông tin, thiếu phối hợp*	*2*	*Xử lý không triệt để, kéo dài thời gian*	*4*	*8*	*Rà soát kịch bản đa chiều, xác nhận 2 lớp ứng với mỗi kịch bản*	*1*	*4*	*4*	*Có*	*Không*
8	*Bước 8. Phê duyệt kịch bản*	*Phê duyệt chậm, bỏ sót nguy cơ*	*Lãnh đạo bận, thông tin chưa rõ*	*2*	*Trì hoãn xử lý, sự cố lan rộng*	*3*	*6*	*Phê duyệt điện tử, nhắc tự động*	*1*	*3*	*3*	*Có*	*Không*
9	*Bước 9. Thực hiện kịch bản xử lý*	*Thực hiện không đúng, bỏ sót bước*	*Nhân sự chưa quen quy trình, thiếu tài liệu*	*2*	*Xử lý không triệt để, tái diễn sự cố*	*3*	*6*	*Checklist xử lý, hướng dẫn chi tiết*	*1*	*3*	*3*	*Có*	*Không*
10	*Bước 10. Kiểm soát thực hiện kịch bản*	*Không kiểm tra đủ, bỏ qua kết quả bất thường*	*Kiểm soát hình thức, thiếu công cụ hỗ trợ*	*2*	*Sự cố không giải quyết triệt để*	*4*	*8*	*Checklist, đối chiếu log, kiểm tra chéo*	*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
11	*Bước 11: Báo cáo và lưu hồ sơ*	*Thất lạc hồ sơ, không lưu bài học kinh nghiệm*	*Thiếu quy định lưu trữ, lưu thủ công*	*2*	*Không truy vết được, lặp lại sai sót*	*3*	*6*	*Lưu trữ số hóa, phân quyền*	*1*	*3*	*3*	*Có*	*Không*

Đơn vị khác có tham gia ĐGRR	Họ tên	Chữ ký
Trung tâm vận hành (NOC)	QUANLENE	QUANLENE
Trung tâm SOC	QUANLEME	QUANLEME

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**