DOANH NGHIỆP ABC

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

(Ban hành kèm theo Quyết định số ……/20___/ABC/QĐ-GĐ ngày……/……/….
của Giám đốc Doanh nghiệp ABC)

<table>
<tr><td colspan="3">Soạn thảo/Đồng soạn thảo bởi</td></tr>
<tr><td colspan="2">Phòng Hạ tầng cơ sở</td><td>Phòng An toàn bảo mật HTTT</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Họ tên:</td><td>Họ tên:</td></tr>
<tr><td colspan="2">Ngày ký:</td><td>Ngày ký:</td></tr>
<tr><td colspan="3">Soát xét bởi</td></tr>
<tr><td>Phòng QL Chất Lượng</td><td>Phòng Quản lý Rủi ro</td><td>Phòng Pháp chế</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Họ tên:</td><td>Họ tên:</td><td>Họ tên:</td></tr>
<tr><td>Ngày ký:</td><td>Ngày ký:</td><td>Ngày ký:</td></tr>
<tr><td colspan="3">Phê duyệt</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Họ tên:</td></tr>
<tr><td colspan="3">Ngày ký:</td></tr>
</table>

THEO DÕI SỬA ĐỔI VĂN BẢN

Stt	Lần sửa đổi	Ngày sửa đổi	Nội dung cũ	Nội dung mới	Trang
1					

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy trình này quy định trình tự các bước thực hiện giám sát xử lý cảnh báo về an ninh mạng trên hệ thống IPS.

2. Đối tượng áp dụng

Quy trình này áp dụng cho các nhân sự trực thuộc Khối Công nghệ thông tin được giao nhiệm vụ quản trị, quản lý và vận hành hệ thống IPS.

Điều 2. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. **Đơn vị:** bao gồm các Khối, Phòng, Ban, Trung tâm, các bộ phận thuộc Doanh nghiệp.

2. **Khối CNTT** là từ viết tắt của "Khối Công nghệ thông tin" (còn có tên cũ là Khối CNTT & VH).

3. **CNTT** là từ viết tắt của "công nghệ thông tin".

4. **Hệ thống IPS** là hệ thống phát hiện và ngăn chặn các dấu hiệu tấn công mạng thông qua phân tích luồng dữ liệu để đưa ra cảnh báo các tấn công vào hệ thống máy chủ dựa vào các dấu hiện nhận biết có sẵn (Signature).

5. **IP** là địa chỉ máy tính người dùng sử dụng trong hệ thống mạng.

6. **Port** là cổng mạng kết nối từ máy tính người dùng đến thiết bị chuyển mạch.

7. **Phòng Hạ tầng** là Phòng Hạ tầng cơ sở thuộc Khối CNTT của Doanh nghiệp.

8. **Phòng Bảo mật** là Phòng An toàn bảo mật HTTT thuộc Khối CNTT của Doanh nghiệp.

9. **Bộ phận quản trị Mạng và thiết bị bảo mật** là bộ phận nhân viên trực thuộc Phòng Bảo mật.

Điều 3. Nguyên tắc thực hiện

1. Đảm bảo việc giám sát xử lý cảnh báo về an ninh mạng trên hệ thống IPS được thực hiện đầy đủ và chính xác theo quy định.

2. Việc giám sát xử lý cảnh báo về an ninh mạng trên hệ thống IPS phải tuân thủ theo các Quy định hiện hành của Doanh nghiệp bao gồm:

- Quy chế an toàn thông tin.
- Quy định về quản lý các thiết bị mạng và bảo mật.

Chương II
QUY ĐỊNH CỤ THỂ

Điều 4. Quy trình giám sát xử lý cảnh báo an ninh mạng trên thiết bị IPS.

1. Nội dung:

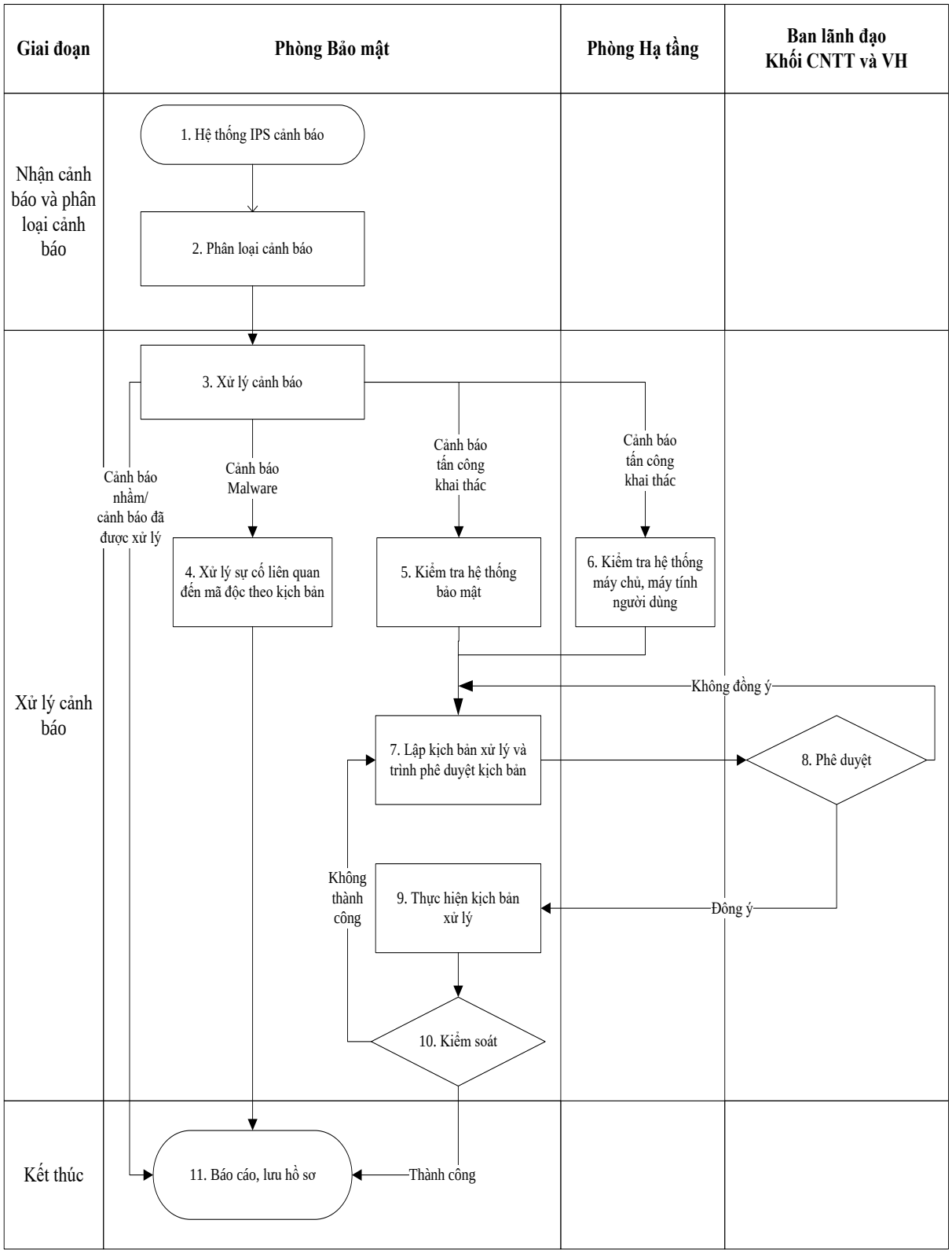
Hệ thống IPS giám sát nội bộ các hoạt động trên các phân vùng dữ liệu quan trọng trong hệ thống Doanh nghiệp , hệ thống sẽ ghi nhận và phát sinh cảnh báo bất kì hành vi, thao tác nào có dấu hiệu nghi ngờ tấn công, lây nhiễm mã độc.

Cảnh báo được thiết lập theo mức từ ảnh hưởng tới hệ thống liên quan thấp (low), trung bình (medium) và cao (high), đồng thời cũng đưa ra đề xuất xử lý cho các cảnh báo này (có thể ngăn chặn hoặc theo dõi).

Đối với các cảnh báo ở mức cao (High) sẽ được thông báo liên tục bằng tin nhắn SMS và Email cho các nhân sự phụ trách liên quan.

2. Lưu đồ thực hiện quy trình:

<logo doanh nghiệp>	**QUY TRÌNH GIÁM SÁT XỬ LÝ CẢNH BÁO VỀ AN NINH MẠNG TRÊN HỆ THỐNG IPS**	**Số hiệu:**	**QT__/___**
		Lần ban hành:	**01**
		Ngày ban hành:	**……/……/**



3. Diễn giải lưu đồ thực hiện:

Bước	Nội dung	Trách nhiệm thực hiện	Biểu mẫu
1	Nhận cảnh báo từ hệ thống IPS	Bộ phận quản trị Mạng và thiết bị bảo mật	Email cảnh báo (bản IN)
2	Phân loại cảnh báo: 1. Nguyên tắc phân loại cảnh báo: - IP nguồn và đích - Port nguồn và đích - Loại cảnh báo - Khuyến nghị xử lý cảnh báo của hệ thống IPS 2. Xác định loại cảnh báo: - Cảnh báo nhầm hoặc cảnh báo đã được xử lý. - Cảnh báo mới gồm: + Cảnh báo malware +Cảnh báo tấn công khai thác	Bộ phận quản trị Mạng và thiết bị bảo mật	
3	Xử lý cảnh báo: - Trường hợp cảnh báo nhầm hoặc cảnh báo đã được xử lý: thực hiện tiếp bước 11. - Trường hợp cảnh báo malware: thực hiện bước 4. - Trường hợp cảnh báo tấn công khai thác: thực hiện bước 5, bước 6.	Bộ phận quản trị Mạng và thiết bị bảo mật	
4	- Xử lý theo kịch bản xử lý sự cố liên quan đến virus	Bộ phận quản trị Mạng và thiết bị	

	trong hệ thống mạng Doanh nghiệp . - Xử lý xong thực hiện tiếp bước 11.	bảo mật	
5	Kiểm tra hệ thống bảo mật: - Thực hiện kiểm tra trên thiết bị bảo mật: + Cập nhật các bản vá và cơ sở dữ liệu IPS. + Thực hiện ngăn chặn trên hệ thống bảo mật	Bộ phận quản trị Mạng và thiết bị bảo mật	
6	Kiểm tra hệ thống máy chủ, máy tính người dùng - Thực hiện kiểm tra hệ thống máy chủ, máy tính người dùng: + Bản vá cập nhật trên hệ thống. + Phần mềm cài đặt theo quy định + Cài đặt chương trình antivirus và cập nhật antivirus mới nhất	Bộ phận quản lý máy chủ thuộc Phòng Hạ tầng	
7	Lập kịch bản xử lý và trình phê duyệt kịch bản: Tổng hợp kết quả kiểm tra ở Bước 5, Bước 6 và lập kịch bản xử lý trình phê duyệt.	- Bộ phận quản trị Mạng và thiết bị bảo mật. - Trưởng phòng Bảo mật ký Tờ trình trình phê duyệt kịch bản xử lý	- Email cảnh báo (bản IN) - Kịch bản xử lý - Tờ trình phê duyệt kịch bản
8	Phê duyệt kịch bản - Đồng ý: thực hiện bước 9	Lãnh đạo Khối CNTT	- Email cảnh báo (bản IN)

	- Không đồng ý: thực hiện lại bước 7.		- Tờ trình - Kịch bản xử lý
9	Thực hiện kịch bản xử lý: Thực hiện xử lý các cảnh báo tấn công khai thác theo kịch bản đã được phê duyệt.	Bộ phận quản trị Mạng và thiết bị bảo mật	Kịch bản xử lý
10	Kiểm soát thực hiện kịch bản: - Thành công: thực hiện bước 11. - Không thành công: thực hiện lại bước 7.	Trưởng phòng Bảo mật	Kịch bản xử lý
11	Báo cáo, lưu hồ sơ - Lập Báo cáo kết quả xử lý cảnh báo gởi lãnh đạo Khối CNTT. - Lưu hồ sơ: Email cảnh báo, Tờ trình xin ý kiến chỉ đạo xử lý (nếu có), Tờ trình báo cáo kết quả xử lý cảnh báo gởi lãnh đạo Khối CNTT.	Bộ phận quản trị Mạng và thiết bị bảo mật	- Tờ trình phê duyệt kịch bản, - Kịch bản xử lý, - Tờ trình báo cáo kết quả, - Báo cáo kết quả xử lý, - Email cảnh báo (bản IN).

Chương III

TỔ CHỨC THỰC HIỆN

Điều 5. Trách nhiệm của Ban lãnh đạo Khối CNTT

1. Tổ chức triển khai và kiểm tra việc thực hiện Quy trình này trong toàn Khối CNTT thuộc Doanh nghiệp.

2. Phê duyệt kịch bản xử lý cảnh báo về an ninh mạng trên hệ thống IPS.

Điều 6. Trách nhiệm của Trưởng phòng Bảo mật

1. Phổ biến nội dung Quy trình này trong nội bộ Phòng, tổ chức triển khai thực hiện và tuân thủ mọi quy định trong Quy trình này;

2. Phân công nhân sự thực hiện và giám sát việc thực hiện theo đúng quy định trong Quy trình này;

3. Tham mưu và đề xuất lãnh đạo Khối CNTT các giải pháp, phương án thực hiện để hạn chế sai sót, giảm thiểu rủi ro cho hoạt động của hệ thống CNTT.

Điều 7. Trách nhiệm của Trưởng phòng Hạ tầng

1. Phổ biến nội dung Quy trình này trong nội bộ Phòng, tổ chức triển khai thực hiện và tuân thủ mọi quy định trong Quy trình này;

2. Phân công nhân sự phối hợp Phòng Bảo mật thực hiện xử lý các cảnh báo theo Quy trình này.

Điều 8. Trách nhiệm của nhân sự giám sát và xử lý cảnh báo trên hệ thống IPS

1. Tuân thủ các quy định của Quy trình này.

2. Thực hiện việc giám sát và xử lý các cảnh bảo trên hệ thống IPS theo phân công của Trưởng phòng Bảo mật, Trưởng Phòng Hạ tầng.

3. Báo cáo kịp thời cho Trưởng phòng Bảo mật và lãnh đạo Khối CNTT kết quả xử lý cảnh báo trên hệ thống IPS.

4. Chịu trách nhiệm về mọi sự cố phát sinh xuất phát từ việc thực hiện không đúng hoặc cố ý làm sai Quy trình này.

Điều 9. Điều khoản thi hành

1. Khối CNTT chịu trách nhiệm tổ chức triển khai nội dung Quy trình này.

2. Trong quá trình thực hiện, nếu có vướng mắc phát sinh, các đơn vị đề nghị có ý kiến về Khối CNTT (qua Phòng Bảo mật) để trình Giám đốc xin ý kiến chỉ đạo.

3. Mọi sửa đổi, bổ sung hoặc thay thế Quy trình này do Giám đốc xem xét, quyết định./.