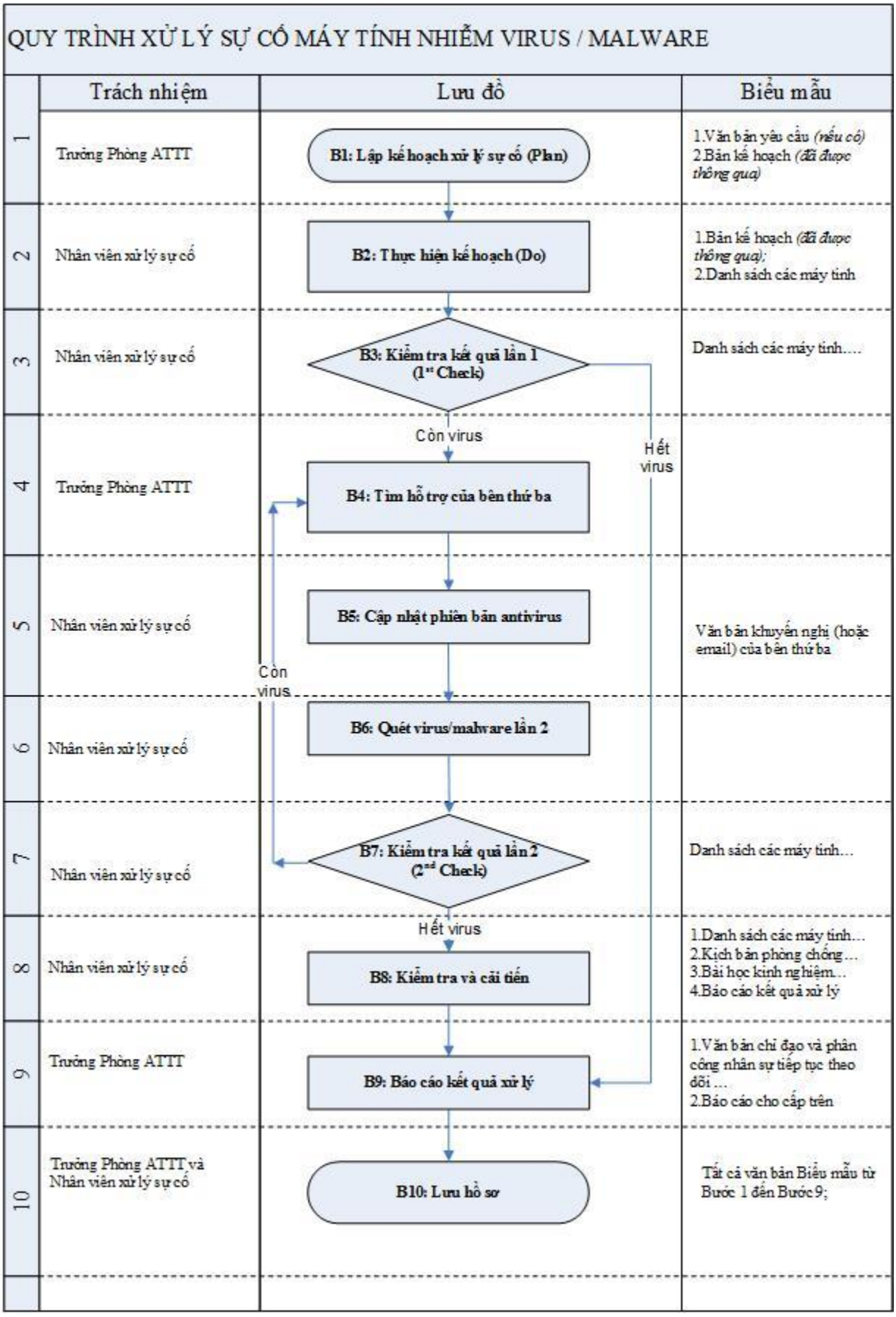
QUY TRÌNH XỬ LÝ SỰ CỐ MÁY TÍNH NHIỄM VIRUS / MALWARE

A. LƯU ĐỒ QUY TRÌNH



B. DIỄN GIẢI

Bước 1: Lập kế hoạch xử lý sự cố ("Plan")

Căn cứ yêu cầu của lãnh đạo các Phòng/Ban/ đơn vị trực thuộc Công ty và kết quả đánh giá tình hình ATTT của hệ thống, Trưởng Phòng ATTT tiến hành:

- Lập danh sách các máy tính và thiết bị tin học bị lây nhiễm (*gọi chung là "máy tính"*);
- Đánh giá phạm vi lây nhiễm; mức độ nghiêm trọng và khả năng ảnh hưởng đến hệ thống thông tin;
- Phân công nhân sự xử lý sự cố máy tính nhiễm virus / malware;
- Chuẩn bị sẵn nguồn lực (phần cứng, phần mềm, kịch bản, các công cụ khác…) cho công việc;
- Lên kế hoạch xử lý (địa điểm xử lý, nhân sự tham gia, nguồn lực sử dụng, lịch triển khai….);
- Báo cáo cho lãnh đạo cấp cao (Giám đốc Khối CNTT) thông qua công tác chuẩn bị và kế hoạch.

Biểu mẫu đầu vào của Bước này là:	- Yêu cầu xử lý virus máy tính của lãnh đạo các Phòng/Ban/Đơn vị của Công ty - Danh sách các máy tính và thiết bị tin học bị lây nhiễm
Biểu mẫu đầu ra của Bước này là:	Bản Kế hoạch *(đã được thông qua)*

Bước 2: Thực hiện kế hoạch ("Do")

Theo kế hoạch đã được thông qua, nhân sự xử lý sự cố (theo Bước 1) tiến hành các hoạt động sau đây:

- Cô lập và ngắt kết nối ("disconnect") máy tính bị nhiễm virus/malware ra khỏi mạng LAN;
- Dùng phần mềm Trend Micro Antivirus quét ("scan") các máy tính bị nhiễm virus/malware;
- Tiến hành xử lý theo kịch bản phòng chống virus (đã ban hành và áp dụng trước đây);
- Kiểm tra danh mục phần mềm cài đặt;
- Kiểm tra quyền hạn người dùng ('user') và trạng thái chương trình antivirus ('enable', 'up-to-date');
- Triển khai các giải pháp kỹ thuật trên các thiết bị tường lửa ('firewall'), hệ thống ngăn chặn xâm nhập ('Intrusion Prevention System' - IPS Checkpoint, IPS McAfee) để phát hiện và ngăn chặn virus lan rộng;
- Triển khai chính sách ('policy') trên thiết bị BlueCoat (là thiết bị bảo vệ cổng kết nối web và lọc web);
- Khôi phục và cài đặt lại nguyên trạng cho máy tính bị ảnh hưởng nghiêm trọng bởi virus/malware.

Biểu mẫu đầu vào của Bước này là:	Bản Kế hoạch *(đã được thông qua)*
Biểu mẫu đầu ra của Bước này là:	Danh sách các máy tính đã được xử lý sự cố lây nhiễm virus/malware

Bước 3: Kiểm tra kết quả lần 1 ("1st Check")

Sau khi thực hiện xong Bước 3, nhân sự xử lý sự cố tiến hành:

- Rà soát lại tình trạng lây nhiễm virus/malware của máy tính đã được quét virus/malware theo Bước 2;
- Rà soát lại hiện trạng các thiết bị bảo mật (Firewall, IPS, BlueCoat…);
- Rà soát lại hiện trạng cập nhật antivirus cho các máy tính tại các khu vực bị lây nhiễm;
- Rà soát lại hiện trạng cảnh báo antivirus tại các khu vực (Văn phòng, Phòng, Ban, đơn vị bên ngoài…);
- Báo cáo nhanh kết quả xử lý cho Trưởng Phòng ATTT.

Nếu hệ thống không còn máy tính bị lây nhiễm virus/malware ở mọi khu vực (hay Yes), thực hiện tiếp Bước 9;

Nếu hệ thống còn khu vực có máy tính bị lây nhiễm virus/malware (hay No), thực hiện tiếp Bước 4.

Biểu mẫu đầu ra của Bước này là:	Danh sách các máy tính đã được xử lý sự cố lây nhiễm virus/malware được phân chia thành 2 nhóm: - Nhóm đã không còn nhiễm virus/malware; và - Nhóm còn lại vẫn còn nhiễm virus/malware

Bước 4: Tìm hỗ trợ của bên thứ ba

Trưởng Phòng ATTT tiến hành:

- Liên lạc với hãng Trend Micro và đề nghị họ hỗ trợ công tác xử lý sự cố;
- Gửi mẫu virus/malware cho hãng Trend Micro;
- Đề nghị hãng Trend Micro hướng dẫn nhân viên xử lý sự cố cách khắc phục virus/malware triệt để;
- Nhận khuyến nghị của hãng Trend Micro sẽ làm tiếp Bước 5.

Bước 5: Cập nhật phiên bản antivirus

Theo khuyến nghị của hãng Trend Micro, nhân sự xử lý sự cố tiến hành:

- Cập nhật phiên bản antivirus mới nhất cho tất cả máy tính (máy chủ và máy trạm đã xử lý xong);
- Rà soát lại và báo cáo hiện trạng mới sau khi cập nhật;
- Tiến hành công việc theo Bước 6 đối với các máy tính chưa xử lý xong (còn lây nhiễm virus/malware).

Biểu mẫu đầu ra của Bước này là:	Văn bản khuyến nghị (hoặc email) của bên thứ ba (hãng Trend Micro)

Bước 6: Quét virus / malware lần 2

Nhân sự xử lý sự cố tiến hành:

- Dùng phần mềm Trend Micro Antivirus phiên bản mới quét ("scan") cho các máy tính (máy chủ và máy trạm) thuộc nhóm vẫn còn bị nhiễm virus/malware (xem Bước 3);
- Thực hiện đầy đủ các hoạt động như đã làm tại Bước 2 *("Thực hiện kế hoạch ("Do")").*

Bước 7: Kiểm tra kết quả lần 2 ("2nd Check")

Sau khi thực hiện xong Bước 6, nhân sự xử lý sự cố tiến hành:

- Các hoạt động như tại Bước 3 (Kiểm tra kết quả lần 1)

Nếu hệ thống không còn máy tính bị lây nhiễm virus/malware ở mọi khu vực (hay Yes), thực hiện tiếp Bước 8.

Nếu hệ thống còn khu vực bị lây nhiễm virus/malware (hay No), thực hiện trở lại Bước 4.

Biểu mẫu đầu ra của Bước này là:	Danh sách các máy tính đã được xử lý sự cố lây nhiễm virus/malware được cập nhật tình trạng lây nhiễm đối với nhóm máy còn lại (xem Bước 3)

Bước 8: Kiểm tra và cải tiến ("Act")

Nhân sự xử lý (theo phân công ở Bước 1) tiến hành:

- Kiểm tra lại tất cả máy tính xem còn lây nhiễm hoặc có hiện tượng gì bất thường không;
- Cập nhật phiên bản antivirus mới nhất cho tất cả máy chủ và máy trạm (đã xử lý xong);
- Hướng dẫn người dùng sử dụng an toàn máy tính để tránh bị lây nhiễm virus/malware;
- Rà soát lại và ghi lại hiện trạng mới của hệ thống sau khi cập nhật phiên bản antivirus;

- Đề xuất các biện pháp phòng ngừa virus/malware mới;
- Cập nhật kịch bản phòng chống virus;
- Ghi lại bài học kinh nghiệm cho đợt xử lý sự cố virus/malware;
- Báo cáo kết quả xử lý cho Trưởng Phòng ATTT sau khi hoàn thành xử lý sự cố virus/malware.

Biểu mẫu đầu ra của Bước này là:	1. Danh sách các máy tính đã được xử lý sự cố lây nhiễm virus/malware được cập nhật và bổ sung thông tin liên quan đến hành động đã thực hiện và kết quả có được ở Bước này. 2. Kịch bản phòng chống virus/malware đã được cập nhật; 3. Bài học kinh nghiệm (có cập nhật hướng dẫn người dùng và các biện pháp phòng ngừa virus) 4. Báo cáo kết quả xử lý cho Trưởng Phòng ATTT

Bước 9: Báo cáo kết quả xử lý

Trưởng Phòng ATTT tiến hành:

- Báo cáo cho cấp trên (Giám đốc Khối CNTT / Tổng Giám đốc) quá trình thực hiện và kết quả xử lý sự cố virus/malware theo kế hoạch đã phê duyệt;
- Chỉ đạo và phân công nhân sự tiếp tục theo dõi sự ổn định của hệ thống sau khi hoàn thành xử lý sự cố.

Biểu mẫu đầu ra của Bước này là:	1. Văn bản chỉ đạo và phân công nhân sự tiếp tục theo dõi; 2. Báo cáo cho cấp trên.

Bước 10: Lưu hồ sơ

Kết thúc hoạt động xử lý sự cố máy tính nhiễm virus/malware, Trưởng Phòng ATTT và nhân viên xử lý sự cố cùng tiến hành lưu hồ sơ xử lý sự cố theo thủ tục lưu trữ hồ sơ của Công ty và theo phân cấp trong Phòng ATTT./.

Biểu mẫu đầu ra của Bước này là:	Tất cả văn bản và biểu mẫu từ Bước 1 đến Bước 9