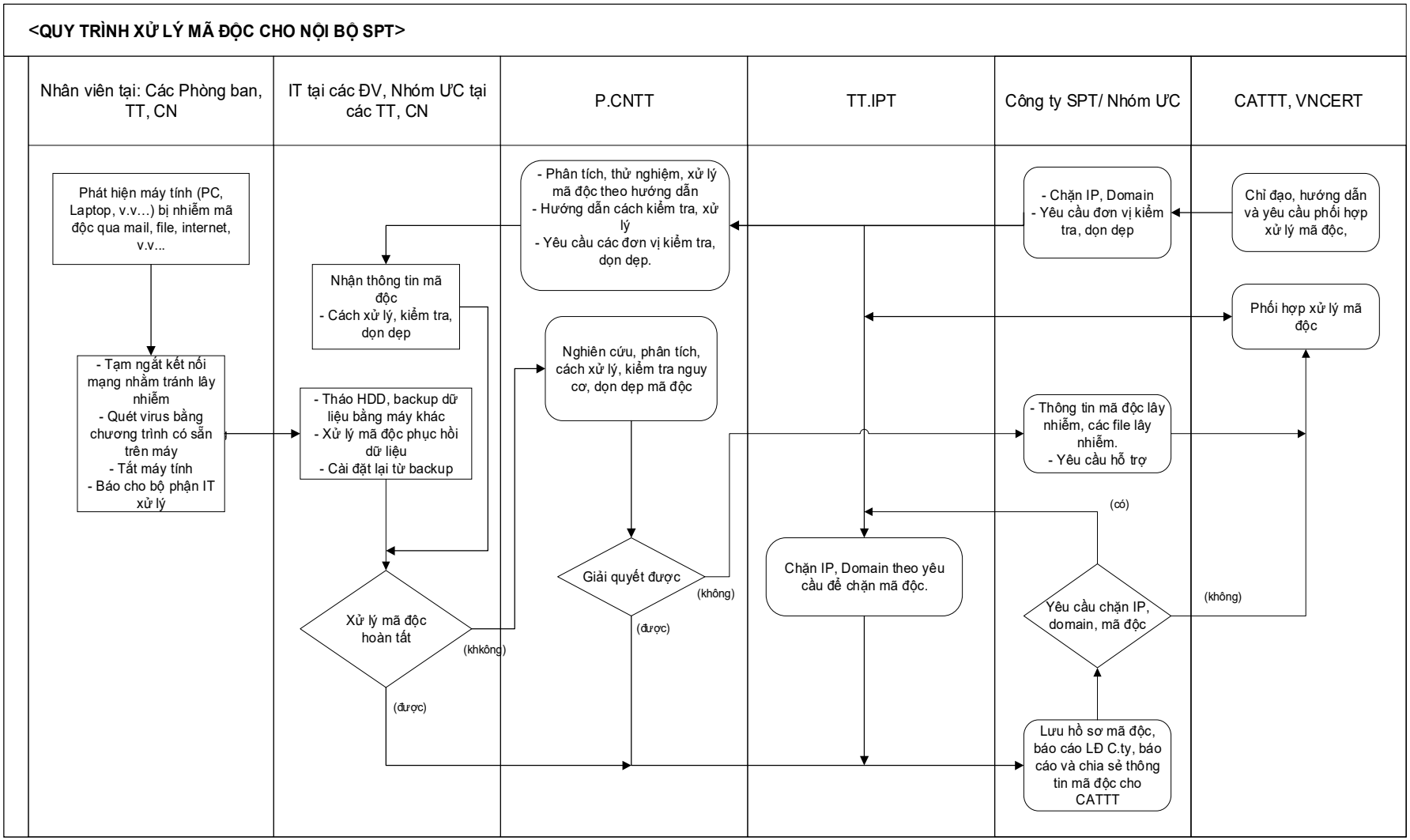
<QUY TRÌNH XỬ LÝ MÃ ĐỘC CHO NỘI BỘ SPT>
Nhân viên tại: Các Phòng ban, TT, CN
IT tại các ĐV, Nhóm ƯC tại các TT, CN
P.CNTT
TT.IPT
Công ty SPT/ Nhóm ƯC
CATTT, VNCERT
Phát hiện máy tính (PC, Laptop, v.v…) bị nhiễm mã độc qua mail, file, internet, v.v...
- Tạm ngắt kết nối mạng nhằm tránh lây nhiễm
- Quét virus bằng chương trình có sẵn trên máy
- Tắt máy tính
- Báo cho bộ phận IT xử lý
Nhận thông tin mã độc
- Cách xử lý, kiểm tra, dọn dẹp
- Tháo HDD, backup dữ liệu bằng máy khác
- Xử lý mã độc phục hồi dữ liệu
- Cài đặt lại từ backup
Xử lý mã độc hoàn tất
(khkông)
(được)
- Phân tích, thử nghiệm, xử lý mã độc theo hướng dẫn
- Hướng dẫn cách kiểm tra, xử lý
- Yêu cầu các đơn vị kiểm tra, dọn dẹp.
Nghiên cứu, phân tích, cách xử lý, kiểm tra nguy cơ, dọn dẹp mã độc
Giải quyết được
(không)
(được)
Chặn IP, Domain theo yêu cầu để chặn mã độc.
- Chặn IP, Domain
- Yêu cầu đơn vị kiểm tra, dọn dẹp
- Thông tin mã độc lây nhiễm, các file lây nhiễm.
- Yêu cầu hỗ trợ
(có)
Yêu cầu chặn IP, domain, mã độc
(không)
Lưu hồ sơ mã độc, báo cáo LĐ C.ty, báo cáo và chia sẻ thông tin mã độc cho CATTT
Chỉ đạo, hướng dẫn và yêu cầu phối hợp xử lý mã độc,
Phối hợp xử lý mã độc