


**NGÂN HÀNG TMCP XUẤT NHẬP KHẨU VIỆT NAM  
KHỐI CNTT**

**KỊCH BẢN XỬ LÝ SỰ CỐ LIÊN QUAN ĐẾN VIRUS TRÊN HỆ THỐNG ATM**

PHÊ DUYỆT	XEM XÉT		
Giám đốc Khối CNTT <i>28/03/16</i> 	Giám đốc Trung tâm 1 	Giám đốc Trung tâm 2 	Giám đốc Trung tâm 3 
Nguyễn Đình Tuấn	Lê Dũng Sĩ	Đinh Kim Quốc Thái	Trần Quốc Thái

**A. PHẦN KIỂM SOÁT (đặt ở trang đầu)**

**Thông tin tài liệu:**

Số hiệu kịch bản	
Ngày ban hành	
Ngày lưu cuối cùng	
Tên tập tin	

**Ghi nhận thay đổi**

Phiên bản số	Ngày ban hành	Nội dung hiệu chỉnh
		(trang ..., phần ..., lý do..., nội dung hiệu chỉnh...)

## B. THÔNG TIN CHUNG

### 1. Mục đích:

Kịch bản được xây dựng để phối hợp xử lý phòng ngừa, ngăn chặn khả năng lây lan của mã độc trên hệ thống ATM và xử lý khắc phục khi máy ATM bị nhiễm mã độc

### 2. Phạm vi áp dụng:

Kịch bản này được áp dụng cho công tác khắc phục sự cố liên quan đến virus trong hệ thống ATM Eximbank

### 3. Nguồn lực tham gia:

- Trung Tâm 1 – Khối CNTT: Nhóm quản lý hệ thống thẻ, ATM
- Trung Tâm 2 – Khối CNTT: Nhóm phát triển ứng dụng ATM.
- Trung Tâm 3 – Khối CNTT: Nhóm Netsec – Trung tâm 3
- IT khu vực miền Bắc, IT khu vực miền Trung, IT khu vực miền Nam.

### 4. Yêu cầu thiết bị sử dụng:

- PC có kết nối đến các hệ thống dùng để kiểm tra xử lý bao gồm hệ thống bảo mật, hệ thống antivirus, hệ quản lý ATM, thẻ quốc tế và thẻ nội địa và các hệ thống liên quan khác.

➤ **5. Yêu cầu về báo cáo:** Yêu cầu các thông tin trao đổi, báo cáo phải được kiểm soát trong nội bộ các nhân sự liên quan và phải báo cáo theo quy định cụ thể như sau:

#### ➤ Báo cáo hiện trạng ban đầu.

Trung tâm 1 thông báo Trung tâm 3 và Giám đốc khối CNTT về các trường hợp máy ATM bị lây nhiễm căn cứ trên log antivirus được Trung tâm 1 rà soát hằng ngày.

#### ➤ Báo cáo trong quá trình xử lý:

- Nhóm Netsec báo cáo tức thời cho Ban Giám Đốc Trung Tâm 3 và Giám đốc Khối CNTT các trường hợp phát sinh trong quá trình thực hiện xử lý sự cố có khả năng tác động vào các hệ thống CNTT của Eximbank để xin chỉ đạo thực hiện.

- Nhóm Netsec báo cáo cho Ban Giám Đốc Trung Tâm 3 và Giám đốc Khối CNTT về hiện trạng của việc xử lý vào cuối mỗi ngày trong trường hợp việc xử lý kéo dài.

- Khối CNTT báo cáo Ban Tổng giám đốc trong các trường hợp xử lý an toàn bảo mật liên quan đến ATM kéo dài và có thể ảnh hưởng đến dịch vụ của khách hàng.

#### ➤ Báo cáo hoàn thành xử lý:

- Căn cứ trên kết quả xác nhận hoàn thành xử lý của Trung tâm 1 và ITKV, nhóm Netsec thực hiện báo cáo cho Ban Giám Đốc Trung Tâm 3 và Giám đốc Khối CNTT sau khi hoàn thành việc xử lý an toàn bảo mật liên quan đến xử lý sự cố.

## C. NỘI DUNG

<b>KỊCH BẢN TRIỂN KHAI ỨNG PHÓ SỰ CỐ LIÊN QUAN ĐẾN VIRUS TRÊN HỆ THỐNG ATM</b>		
<b>Các bước thực hiện</b>	<b>Nội dung công việc</b>	<b>Nhân sự thực hiện</b>
<b>Bước 1: Công tác chuẩn bị</b>	<ul style="list-style-type: none"><li>- Phân công nhân sự tham gia xử lý sự cố.</li><li>- Chuẩn bị các nguồn lực phục vụ cho công tác xử lý (phần cứng, phần mềm, danh sách nhân sự phía đối tác phối hợp xử lý)</li><li>- Các tài liệu liên quan đến xử lý sự cố về virus</li></ul>	<b>Trung tâm 3</b> <ul style="list-style-type: none"><li>- Thông báo tới các nhân sự xử lý sự cố sẵn sàng bao gồm<ul style="list-style-type: none"><li>• Trung tâm 1 – bộ phận quản lý ATM, thẻ</li><li>• ITKV phụ trách ATM đang bị lây nhiễm để phối hợp xử lý với đối tác bảo trì.</li><li>• Giám đốc CN quản lý ATM</li><li>• Đơn vị bảo trì hệ thống ATM<ul style="list-style-type: none"><li>○ FPT – đối với dòng máy IBM</li><li>○ Diebold – đối với dòng máy Diebold.</li></ul></li></ul></li><li>- Chuẩn bị các tài liệu liên quan đến xử lý sự cố virus trong phạm vi TT3</li><li>- Báo cáo sơ bộ GDK kế hoạch xử lý bao gồm: hiện trạng lây nhiễm, số lượng máy bị lây nhiễm, địa điểm xử lý, nhân sự tham gia và trường hợp cần thiết tạm</li></ul>



		<p>thời ngừng cung cấp dịch vụ tới người dùng.</p> <p><b>Trung tâm 1 và ITKV</b></p> <ul style="list-style-type: none"> <li>- Giám đốc TT1 và Trưởng ITKV phân công nhân sự phối hợp với TT3 xử lý sự cố.</li> <li>- Chuẩn bị các tài liệu liên quan đến xử lý sự cố virus trong phạm vi TT1</li> <li>- Thông báo đơn vị bảo trì ATM (FPT hoặc Diebold) đề nghị cử nhân sự phối hợp xử lý. Đồng thời tiến hành tổ chức họp nhanh giữa TT1, TT3 và đơn vị đối tác để xây dựng kế hoạch xử lý.</li> </ul>
<p><b>Bước 2: Cô lập các máy ATM bị lây nhiễm ra khỏi hệ thống mạng Eximbank.</b></p>	<ul style="list-style-type: none"> <li>- Tiến hành ngắt kết nối các máy ATM bị lây nhiễm ra khỏi hệ thống mạng EXIMBANK</li> <li>- Thống kê số lượng máy bị lây nhiễm và phạm vi lây nhiễm</li> </ul>	<p><b>Trung tâm 3</b></p> <ul style="list-style-type: none"> <li>- Trung tâm 3 đề nghị TT1 hoặc ITKV cách ly các máy lây nhiễm khỏi hệ thống mạng Eximbank</li> <li>- Báo cáo Giám đốc Khối CNTT xin ý kiến chỉ đạo trong trường hợp phạm vi lây nhiễm trên diện rộng và cần phải tạm thời ngừng phục vụ người dùng để tiến hành cô lập xử lý.</li> </ul> <p><b>Trung tâm 1 và ITKV</b></p> <ul style="list-style-type: none"> <li>- Thông báo tới Giám đốc CN quản lý ATM (báo cáo nội bộ) và tạm thời cách ly máy ATM này khỏi mạng Eximbank cũng như gián đoạn tạm thời phục vụ cho việc xử lý sự cố. TT1 xác nhận thông tin kết quả hiện trạng về TT3</li> <li>- Thống kê số lượng máy ATM bị lây nhiễm và phản hồi về TT3</li> </ul>
<p><b>Bước 3: Xử lý dứt điểm các máy ATM bị lây nhiễm</b></p>	<p>Triển khai các giải pháp kỹ thuật nhằm giải xử lý dứt điểm:</p> <ul style="list-style-type: none"> <li>- Scan các máy ATM bị lây nhiễm</li> <li>- Scan các máy tính có kết nối tới máy ATM</li> <li>- Kiểm tra danh mục phần mềm cài đặt trên các máy ATM theo quy định</li> <li>- Kiểm tra log ghi nhận các thao tác gần nhất liên quan đến ATM (bao gồm log hệ thống, ứng dụng, nhật ký bảo trì)</li> </ul>	<p><b>Trung tâm 1 và ITKV</b></p> <ul style="list-style-type: none"> <li>- Tiến hành cập nhật phiên bản antivirus mới nhất và thực hiện dò quét toàn diện máy ATM bị nhiễm: <ul style="list-style-type: none"> <li>Dòng máy IBM – Antivirus Trend Micro</li> <li>Dòng máy Diebold – Antivirus Symantec.</li> </ul> </li> <li>- Thực hiện backup dữ liệu và sử dụng bản cài đặt an toàn (đã được xác nhận an toàn tại thời điểm cài đặt) để cài lại máy đối với các trường hợp nghiêm trọng.</li> <li>- Trưởng ITKV chịu trách nhiệm phân công nhân sự phối hợp với đơn vị bảo trì tiến hành dò quét antivirus hoặc cài đặt lại máy ATM.</li> </ul> <p><b>Trung tâm 3</b></p> <ul style="list-style-type: none"> <li>- Tạm thời cô lập và thực hiện dò quét toàn bộ các máy tính có kết nối tới các máy ATM bị lây nhiễm. - Kiểm tra trên hệ thống bảo mật các chính sách kết nối từ máy tính tới ATM</li> <li>- Kiểm tra trên hệ thống Firewall lưu lượng kết nối, tần xuất kết nối bất thường từ các máy tính tới các máy ATM.</li> <li>- Trường hợp nghi ngờ dấu hiệu ATM bị lây nhiễm từ các máy trạm sẽ tiến hành cô lập máy trạm và áp dụng kịch bản xử lý mã độc để tiếp tục xử lý các máy trạm này.</li> </ul>
<p><b>Bước 4: Khôi phục hiện trạng</b></p>	<ul style="list-style-type: none"> <li>- Cập nhật chương trình antivirus hằng ngày để ngăn chặn tình trạng lây nhiễm trong tương lai (nếu có)</li> </ul>	<p><b>Trung tâm 1 và ITKV</b></p> <ul style="list-style-type: none"> <li>- Cung cấp mẫu virus theo yêu cầu của TT3</li> <li>- Phối hợp với đối tác thực hiện cập nhật antivirus mới nhất cho tất cả các máy ATM và xác nhận kết quả về TT3.</li> </ul>



	<ul style="list-style-type: none"> <li>- Rà soát và khôi phục hiện trạng sau khi xử lý sự cố.</li> </ul>	<ul style="list-style-type: none"> <li>- Áp dụng quy trình cài đặt ATM đã được ban hành (đối với các trường hợp được đánh giá ảnh hưởng nghiêm trọng bắt buộc phải cài đặt lại)</li> <li>- Cập nhật chương trình antivirus hằng ngày để ngăn chặn tình trạng lây nhiễm trong tương lai (nếu có).</li> <li>- Rà soát và khôi phục hiện trạng sau khi xử lý sự cố.</li> <li>- Thông báo Giám đốc CN/PGD về việc khôi phục hoạt động của ATM.</li> </ul> <p><b>Trung tâm 3:</b></p> <ul style="list-style-type: none"> <li>- Gửi mẫu virus cho Trend Micro và đề nghị hỗ trợ kiểm tra cũng như phương án khắc phục.</li> <li>- Đối với dòng máy Diebold sử dụng antivirus Symantec phải đề nghị đơn vị cung cấp Diebold cập nhật liên tục hiện trạng xử lý virus liên quan và phương án khắc phục.</li> </ul>
<p><b>Bước 5: Báo cáo lưu hồ sơ và công tác hậu kiểm sau khi xử lý sự cố.</b></p>	<p>Lập báo cáo về quá trình triển khai thực hiện xử lý sự cố trình Giám đốc khối phê duyệt. Trường hợp cần thiết sẽ làm báo cáo lên Ban Tổng Giám đốc.</p> <ul style="list-style-type: none"> <li>- Lưu hồ sơ xử lý sự cố.</li> <li>- Thực hiện công tác hậu kiểm sau khi xử lý sự cố. (kiểm tra hiện trạng, nâng cấp kịch bản xử lý, đề xuất các biện pháp phòng ngừa mới).</li> </ul>	<p><b>Trung tâm 3</b></p> <ul style="list-style-type: none"> <li>- Lập báo cáo tổng thể về xử lý xử cố và trình Giám đốc khối CNTT</li> <li>- Lưu hồ sơ xử lý sự cố.</li> <li>- Tiếp tục theo dõi hiện trạng an toàn bảo mật đối với các máy ATM và các máy trạm có kết nối tới ATM.</li> </ul> <p><b>Trung tâm 1</b></p> <ul style="list-style-type: none"> <li>- Lập báo cáo kết quả và gửi về TT3</li> <li>- Liên hệ định kì (hàng tuần), thường xuyên với đối tác về các giải pháp gia cố an toàn bảo mật cho hệ thống ATM.</li> <li>- Theo dõi hệ thống ATM và thông báo tới TT3 để phối hợp xử lý các trường hợp lây nhiễm</li> </ul>