NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 47/2014/TT-NHNN	*Hà Nội, ngày 31 tháng 12 năm 2014*

THÔNG TƯ

Quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng

Căn cứ Luật Ngân hàng Nhà nước Việt Nam số 46/2010/QH12 ngày 16 tháng 6 năm 2010;

Căn cứ Luật các tổ chức tín dụng số 47/2010/QH12 ngày 16 tháng 6 năm 2010;

Căn cứ Luật giao dịch điện tử số 51/2005/QH11 ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 35/2007/NĐ-CP ngày 08 tháng 3 năm 2007 của Chính phủ về giao dịch điện tử trong hoạt động ngân hàng;

Căn cứ Nghị định số 101/2012/NĐ-CP ngày 22 tháng 11 năm 2012 của Chính phủ về thanh toán không dùng tiền mặt;

Căn cứ Nghị định số 156/2013/NĐ-CP ngày 11 tháng 11 năm 2013 quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Theo đề nghị của Cục trưởng Cục Công nghệ tin học;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng.

Chương I

QUY ĐỊNH CHUNG

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

1. Thông tư này quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng tại Việt Nam.

2. Thông tư này áp dụng đối với các tổ chức hoạt động thẻ, bao gồm:

a) Tổ chức phát hành thẻ (viết tắt là TCPHT);

b) Tổ chức thanh toán thẻ (viết tắt là TCTTT);

c) Tổ chức cung ứng dịch vụ trung gian thanh toán (viết tắt là TCTGTT) có trang thiết bị phục vụ thanh toán thẻ ngân hàng.

Điều 2. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. Trang thiết bị phục vụ thanh toán thẻ bao gồm các thiết bị, phần mềm sử dụng cho việc tiếp nhận, xử lý các giao dịch thẻ.

2. ATM (Automated Teller Machine) đặt bên ngoài là ATM đặt tại nơi công cộng và nơi không có người giám sát trực tiếp thiết bị.

3. Máy POS (Point Of Sale) là thiết bị chấp nhận thẻ được sử dụng để thực hiện giao dịch thẻ tại các đơn vị chấp nhận thẻ (viết tắt là ĐVCNT).

4. Máy mPOS (Mobile Point Of Sale) là máy POS bao gồm phần mềm và thiết bị chuyên dụng tích hợp với thiết bị thông tin di động.

5. Thẻ ngân hàng (sau đây gọi tắt là thẻ) bao gồm thẻ từ và thẻ chip

a) Thẻ từ là loại thẻ mà các thông tin của thẻ và chủ thẻ được mã hóa và lưu trữ trong dải băng từ ở mặt sau của thẻ;

b) Thẻ chip là loại thẻ được gắn vi mạch máy tính hoặc mạch tích hợp để nhận dạng, lưu trữ thông tin và giao dịch của chủ thẻ, xử lý vi mô khác.

6. Số thẻ là dãy số dùng để xác định tổ chức phát hành và chủ thẻ.

7. Dữ liệu thẻ bao gồm dữ liệu chủ thẻ và dữ liệu xác thực thẻ.

a) Dữ liệu chủ thẻ bao gồm các dữ liệu chính sau: số thẻ; tên của chủ thẻ (đối với thẻ định danh); ngày có hiệu lực của thẻ; mã dịch vụ (3 (ba) hoặc 4 (bốn) số trên bề mặt thẻ để xác định quyền hạn trên giao dịch (nếu có));

b) Dữ liệu xác thực thẻ bao gồm các dữ liệu sau: toàn bộ dữ liệu trên dải băng từ đối với thẻ từ hoặc dữ liệu trên vi mạch máy tính, mạch tích hợp của thẻ chip; dãy số giá trị hoặc mã xác thực thẻ được in trên thẻ; mã số xác định chủ thẻ (PIN) hoặc khối mã số xác định chủ thẻ (PIN block).

8. Môi trường dữ liệu chủ thẻ là môi trường bao gồm các trang thiết bị và quy trình xử lý, truyền dẫn, lưu trữ dữ liệu thẻ.

9. Mã hoá mạnh là phương pháp mã hoá dựa trên các thuật toán đã được kiểm tra, chấp nhận rộng rãi trên thế giới cùng với độ dài khoá tối thiểu 112 (một trăm mười hai) bit và kỹ thuật quản lý khoá phù hợp. Các thuật toán tối thiểu bao gồm: AES (128 bit); TDES (112 bit); RSA (2048 bit); ECC (160 bit); ElGamal (2048 bit).

10. Dữ liệu nhật ký là các dữ liệu được hệ thống thanh toán thẻ hoặc con người tạo ra để lưu lại các quá trình giao dịch, hoạt động của hệ thống bằng hình thức điện tử, văn bản để phục vụ hoạt động giám sát, tra soát, khiếu nại.

11. Người có thẩm quyền tại văn bản này được hiểu là người đại diện theo pháp luật của tổ chức hoặc người được người đại diện theo pháp luật của tổ chức ủy quyền.

12. Tổ chức hỗ trợ hoạt động thẻ là các tổ chức, cá nhân có chuyên môn được tổ chức hoạt động thẻ thuê hoặc hợp tác nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống thanh toán thẻ.

Chương II
CÁC YÊU CẦU KỸ THUẬT CHUNG

Điều 3. Thiết lập và quản lý cấu hình thiết bị an ninh mạng

1. Các yêu cầu về thiết lập và quản lý cấu hình thiết bị an ninh mạng:

a) Việc thiết lập và thay đổi cấu hình thiết bị an ninh mạng phải được kiểm thử và được người có thẩm quyền phê duyệt trước khi thực hiện;

b) Sơ đồ kết nối hệ thống mạng phải được thiết kế đáp ứng yêu cầu:

- Tách biệt giữa vùng dữ liệu chủ thẻ và các vùng mạng khác bao gồm cả vùng mạng không dây;

- Tách biệt chức năng của máy chủ theo nguyên tắc các máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ quản lý tên miền phải để trên các máy chủ khác nhau (có thể là các máy chủ ảo trên một máy chủ vật lý);

- Có tường lửa tại các điểm kết nối giữa các vùng của hệ thống mạng;

- Sơ đồ mạng phải mô tả được toàn bộ đường đi của dữ liệu chủ thẻ.

c) Phân định trách nhiệm và quyền hạn đối với bộ phận, cá nhân trong quản lý, cấu hình các thiết bị an ninh mạng bằng văn bản;

d) Không cung cấp địa chỉ mạng (địa chỉ IP) nội bộ và thông tin định tuyến cho các tổ chức khác khi chưa được người có thẩm quyền phê duyệt;

đ) Quy định bằng văn bản các cổng, dịch vụ, giao thức sử dụng trên hệ thống mạng bao gồm cả những cổng, giao thức, dịch vụ không an toàn. Triển khai đầy đủ các giải pháp an ninh khi sử dụng các cổng, dịch vụ và giao thức không an toàn;

e) Thực hiện đánh giá lại các chính sách thiết lập trên thiết bị an ninh mạng tối thiểu 02 lần/năm nhằm loại bỏ các chính sách không sử dụng, hết thời hạn hoặc thiết lập sai chính sách, đảm bảo chính sách được thiết lập trên thiết bị đúng với các chính sách đã được người có thẩm quyền phê duyệt.

2. Cấu hình thiết bị an ninh mạng

a) Giới hạn các truy cập đến môi trường dữ liệu chủ thẻ, chỉ chấp nhận các truy cập thực sự cần thiết và kiểm soát được;

b) Giới hạn các truy cập đến thiết bị mạng và thiết bị an ninh mạng khớp đúng với trách nhiệm của cá nhân, bộ phận được quy định tại Điểm c Khoản 1 Điều này;

c) Các tập tin cấu hình phải được đồng bộ với cấu hình đang hoạt động của thiết bị và được lưu trữ an toàn theo chế độ mật để tránh các truy cập trái phép;

d) Thực hiện thiết lập chức năng giám sát trạng thái gói tin hoặc lọc dữ liệu tự động trên thiết bị tường lửa hoặc định tuyến để phát hiện các gói tin không hợp lệ.

3. Kiểm soát các truy cập trực tiếp từ Internet đến môi trường dữ liệu chủ thẻ

a) Thiết lập vùng trung gian cung cấp dịch vụ ra ngoài Internet (xác định rõ các máy chủ, dịch vụ, địa chỉ IP, cổng, giao thức được phép truy cập). Việc kết nối ra, vào giữa Internet và môi trường dữ liệu chủ thẻ phải kết nối qua vùng trung gian cung cấp dịch vụ;

b) Thực hiện các biện pháp chống giả mạo để ngăn chặn và loại bỏ các khả năng giả mạo địa chỉ IP nguồn;

c) Không cho phép các truy cập từ môi trường dữ liệu chủ thẻ ra ngoài Internet khi chưa được người có thẩm quyền phê duyệt.

4. Yêu cầu thiết lập phần mềm tường lửa trên tất cả các thiết bị, máy tính cá nhân có kết nối đến dữ liệu thẻ

a) Các chính sách an ninh trên phần mềm tường lửa chỉ cho phép thực hiện các hoạt động đủ phục vụ cho nhu cầu xử lý các quy trình nghiệp vụ;

b) Đảm bảo các thiết lập trên phần mềm tường lửa là đang hoạt động;

c) Đảm bảo người dùng không thể thay đổi cấu hình phần mềm tường lửa trên thiết bị.

Điều 4. Thay đổi, loại bỏ hoặc vô hiệu hóa các tham số, chức năng mặc định trong hệ thống trang thiết bị phục vụ thanh toán thẻ

1. Thay đổi hoặc vô hiệu hoá các tham số và chức năng mặc định của hệ thống (tài khoản, mã khoá bí mật, tham số hệ điều hành, phần mềm, ứng dụng không sử dụng; tham số trên máy POS không sử dụng; chuỗi ký tự mặc định trong giao thức giám sát mạng (giao thức SNMP)).

2. Thay đổi các tham số mặc định (khoá mã hoá trong mạng không dây; các mã khoá bí mật; chuỗi ký tự mặc định trong giao thức SNMP tại các môi trường mạng không dây có kết nối đến dữ liệu thẻ).

3. Chỉ bật hoặc cài đặt các chức năng mặc định (dịch vụ, giao thức, các chương trình nền) khi có nhu cầu sử dụng.

4. Loại bỏ các chức năng, dịch vụ, tập tin, ổ đĩa không cần thiết. Thực hiện thêm các biện pháp an toàn bổ sung (các công nghệ SSH, S-FTP, SSL, IPSec VPN) khi sử dụng các dịch vụ, giao thức không an toàn để truyền dữ liệu trên mạng (chia sẻ tệp tin (File Sharing), NetBIOS, Telnet, FTP).

Điều 5. An toàn bảo mật trong phát triển, duy trì các trang thiết bị phục vụ thanh toán thẻ

1. Thực hiện nhận dạng các lỗ hổng bảo mật bằng công cụ dò quét và các nguồn thông tin của các tổ chức an ninh mạng bên ngoài có uy tín để xác định mức độ ảnh hưởng của các lỗ hổng bảo mật mới đối với hệ thống thanh toán thẻ, bao gồm các mức độ ảnh hưởng: mức độ cao; mức độ trung bình; mức độ thấp.

2. Đảm bảo toàn bộ các thiết bị phục vụ thanh toán thẻ được cập nhật các bản vá lỗ hổng bảo mật đã được công bố từ các nhà sản xuất. Đối với các bản vá các lỗ hổng bảo mật mức độ cao phải được cài đặt trong thời gian sớm nhất và không quá 01 tháng kể từ khi nhà sản xuất công bố bản vá.

3. Phát triển các phần mềm ứng dụng trong lĩnh vực thẻ đảm bảo tuân thủ các quy định của pháp luật và các chuẩn mực phát triển phần mềm ứng dụng được áp dụng rộng rãi trong lĩnh vực công nghệ thông tin. Trong chu trình phát triển phần mềm phải tích hợp với các yêu cầu đảm bảo an toàn thông tin và tối thiểu đáp ứng các yêu cầu sau:

a) Tách biệt môi trường phát triển và kiểm thử với môi trường vận hành;

b) Không sử dụng dữ liệu thẻ trong môi trường vận hành cho môi trường kiểm thử;

c) Loại bỏ toàn bộ dữ liệu và tài khoản kiểm thử trước khi đưa phần mềm vào sử dụng;

d) Đánh giá, xem xét lại mã nguồn phần mềm ứng dụng để phát hiện, khắc phục lỗ hổng bảo mật tiềm tàng trước khi đưa vào sử dụng. Nhân sự thực hiện đánh giá phải độc lập với nhân sự phát triển mã nguồn ứng dụng.

4. Thực hiện các thủ tục kiểm soát sự thay đổi khi cập nhật các bản vá lỗ hổng bảo mật, thay đổi phần mềm ứng dụng:

a) Xây dựng tài liệu đánh giá tác động đến toàn bộ hệ thống và được người có thẩm quyền phê duyệt trước khi thực hiện;

b) Không được làm ảnh hưởng đến tính an toàn bảo mật của hệ thống;

c) Thực hiện sao lưu, có kế hoạch dự phòng trước khi thực hiện thay đổi.

5. Khi phát triển mã nguồn ứng dụng cần kiểm tra, loại bỏ các lỗ hổng bảo mật trong ứng dụng, bao gồm:

a) Các lỗ hổng chèn mã lệnh truy vấn cơ sở dữ liệu (SQL injection), câu lệnh hệ điều hành (OS injection), các phương tiện lưu trữ dữ liệu khác;

b) Lỗi tràn bộ nhớ đệm;

c) Lỗi mã hoá không an toàn trong lưu trữ dữ liệu;

d) Lỗi không an toàn trong truyền thông;

đ) Rò rỉ thông tin qua thông báo lỗi (error handling);

e) Các nguy cơ chèn mã, đoạn mã javascript, jscript, DHTML, các thẻ HTML;

g) Các kiểm soát truy cập không đúng;

h) Các hình thức tấn công chiếm quyền xác thực của người sử dụng trên một website thông qua một website giả mạo khác (Cross Site Request Forgery);

i) Lỗi trong quản lý phiên truy cập (session ID);

k) Các lỗ hổng bảo mật được xác định có mức độ cao được quy định tại Khoản 1 Điều này.

6. Các ứng dụng cung cấp dịch vụ trên các môi trường mạng bên ngoài (mạng internet, mạng không dây, mạng truyền thông di động và các mạng khác) phải có các biện pháp để xử lý các mối đe dọa và lỗ hổng bảo mật, bao gồm:

a) Đánh giá an toàn bảo mật tối thiểu 01 lần/quý hoặc sau khi có sự thay đổi bằng các công cụ đánh giá tự động hoặc thủ công;

b) Thực hiện các giải pháp kỹ thuật tự động phát hiện và phòng chống tấn công bằng thiết bị tường lửa ứng dụng web (Web Application Firewall).

7. Phần mềm hệ thống thanh toán thẻ phải có tính năng lọc, không chấp nhận thanh toán cho các giao dịch không được phép thực hiện theo quy định của pháp luật.

Điều 6. Yêu cầu cấp phát và kiểm soát tài khoản truy cập vào hệ thống thanh toán thẻ

1. Việc truy cập vào ứng dụng thanh toán thẻ phải được xác thực bằng ít nhất một trong các phương thức sau: mã khoá bí mật, thiết bị, thẻ xác thực và sinh trắc học.

2. Việc truy cập từ xa vào hệ thống mạng phải được xác thực bằng tối thiểu hai phương thức quy định tại Khoản 1 Điều này.

3. Mã hoá toàn bộ mã khoá bí mật trên đường truyền và khi lưu trữ bằng các phương pháp mã hoá mạnh.

4. Thực hiện các biện pháp kiểm soát tài khoản vận hành và tài khoản quản trị:

a) Cấp phát tài khoản truy cập riêng biệt, phân quyền tương ứng cho từng cá nhân làm nhiệm vụ vận hành và quản trị các thiết bị phục vụ thanh toán thẻ;

b) Kiểm soát việc thêm mới, xóa, sửa các định danh, thông tin tài khoản người sử dụng đúng mục tiêu quản lý;

c) Thu hồi quyền truy cập ngay khi người sử dụng hết hạn sử dụng hoặc chuyển công việc khác hoặc không làm nhiệm vụ vận hành, quản trị;

d) Thẩm tra, xác nhận lại danh tính người sử dụng khi nhận được yêu cầu gián tiếp qua email, điện thoại trước khi thay đổi, phục hồi lại mã khoá bí mật tài khoản;

đ) Tài khoản cấp phát lần đầu phải thiết lập mã khoá bí mật và mã khoá bí mật đó trên các tài khoản phải khác nhau. Tài khoản chỉ được hoạt động khi người dùng thay đổi mã khoá bí mật ban đầu;

e) Quy định và thực hiện việc thu hồi, loại bỏ hoặc vô hiệu hoá các tài khoản không sử dụng, hết hạn sử dụng hoặc các tài khoản trong trạng thái không kích hoạt trong một khoảng thời gian;

g) Việc cấp tài khoản truy cập từ xa cho tổ chức hỗ trợ hoạt động thẻ phải được giới hạn về thời gian, phải được người có thẩm quyền phê duyệt và được giám sát hoạt động;

h) Không được chia sẻ hoặc dùng chung tài khoản để truy cập hệ thống;

i) Tài khoản phải được thay đổi mã khoá bí mật tối thiểu 01 lần/quý; mã khoá bí mật phải có độ dài tối thiểu 07 (bảy) ký tự, bao gồm cả ký tự chữ và số

(ngoại trừ PIN); mã khoá bí mật không được sử dụng lặp lại trong bốn lần gần nhất;

k) Số lần nhập sai mã khoá bí mật tối đa được phép không quá 03 (ba) lần. Có biện pháp khoá tài khoản tự động khi nhập sai mã khoá bí mật quá số lần quy định. Thời gian phục hồi tài khoản bị khoá sau khi nhập sai mã khoá bí mật tối thiểu 30 phút hoặc theo yêu cầu;

l) Phiên làm việc với hệ thống thanh toán thẻ ở trạng thái chờ quá 15 phút hệ thống phải yêu cầu xác thực lại để vào hệ thống;

m) Phổ biến và đào tạo các chính sách, quy trình truy cập và xác thực tài khoản vào hệ thống, đảm bảo các tổ chức, cá nhân liên quan nắm rõ được quyền hạn, trách nhiệm khi được cấp tài khoản truy cập.

5. Ban hành chính sách và thủ tục xác thực tài khoản truy cập, trong đó phải bao gồm các nội dung:

a) Hướng dẫn lựa chọn và bảo vệ thông tin xác thực, mã khoá bí mật;

b) Hướng dẫn không dùng lại mã khoá bí mật đã sử dụng trước đó;

c) Hướng dẫn thay đổi mã khoá bí mật định kỳ hoặc ngay khi có nghi ngờ mã khoá bí mật bị lộ.

6. Quản lý truy cập cơ sở dữ liệu thanh toán thẻ

a) Chỉ người quản trị cơ sở dữ liệu được trực tiếp truy cập cơ sở dữ liệu;

b) Người sử dụng khác khi truy cập cơ sở dữ liệu phải thông qua các chương trình ứng dụng có kiểm soát quyền hạn xem, nhập, xóa, thay đổi thông tin;

c) Không sử dụng các tài khoản truy cập cơ sở dữ liệu của chương trình ứng dụng cho cá nhân hoặc các tiến trình khác;

d) Mã khoá bí mật của tài khoản truy cập cơ sở dữ liệu của ứng dụng phải được mã hoá trên ứng dụng và trong cơ sở dữ liệu;

đ) Mọi thao tác trên cơ sở dữ liệu phải được ghi nhật ký và nhật ký phải được lưu giữ tối thiểu 01 năm.

Chương III

CÁC YÊU CẦU KỸ THUẬT ĐỐI VỚI ATM

Điều 7. Các yêu cầu kỹ thuật lắp đặt và an toàn vật lý ATM

1. Yêu cầu về lắp đặt ATM

a) Tổ chức hoạt động thẻ có cung cấp dịch vụ ATM (sau đây gọi chung là tổ chức cung cấp dịch vụ ATM) phải đảm bảo các yêu cầu về việc lắp đặt ATM theo quy định của Ngân hàng Nhà nước Việt Nam về trang bị, quản lý, vận hành và đảm bảo an toàn hoạt động của ATM.

b) Đối với ATM đặt bên ngoài

Ngoài các yêu cầu tại Điểm a Khoản 1 Điều này, tổ chức cung cấp dịch vụ ATM thực hiện thêm các biện pháp đảm bảo an toàn cho ATM đặt bên ngoài đối với những nguy cơ mất an toàn vật lý sau:

- Có biện pháp đảm bảo ATM tránh bị kéo để di dời trái phép;

- Che giấu các thành phần, bộ phận ATM không cần thiết để lộ ra bên ngoài.

2. Yêu cầu về hệ thống báo động

a) Tổ chức cung cấp dịch vụ ATM trang bị thiết bị cảm biến cho ATM đặt bên ngoài để cảnh báo tác động nhiệt từ các thiết bị khò hàn và nhận biết các lực tác động với cường độ lớn, hoặc liên tục từ bên ngoài lên thân vỏ máy;

b) Tổ chức cung cấp dịch vụ ATM trang bị các thiết bị báo động cho ATM nhằm phòng chống:

- Mở cửa máy trái phép;

- Di dời trái phép khỏi khu vực đặt máy;

- Đập phá máy trái phép. Các thiết bị báo động ngoài việc phát tín hiệu báo động tại chỗ, phải gửi cảnh báo về trung tâm giám sát.

3. Yêu cầu về két đựng tiền

a) Tổ chức cung cấp dịch vụ ATM trang bị két đựng tiền của ATM làm bằng vật liệu chịu được lực tác động lớn, chống được ăn mòn, tản nhiệt nhanh hoặc hấp thụ nhiệt chậm nhằm giảm thiểu mức độ hư hỏng vỏ két và tổn thất tiền bên trong do tác động lực, hoá chất và nhiệt từ bên ngoài;

b) Két đựng tiền của ATM phải được trang bị ít nhất hai khoá, do hai người nắm giữ.

4. Bàn phím nhập mã PIN phải đạt các yêu cầu nêu tại Điều 13 Thông tư này.

5. ATM phải có chứng nhận xuất xứ và có chứng nhận chất lượng của nhà sản xuất.

Điều 8. Các yêu cầu kỹ thuật về phần mềm, đường truyền, liên thông cho ATM

1. Tổ chức cung cấp dịch vụ ATM phải đảm bảo các yêu cầu về phần mềm của ATM

a) Hệ điều hành máy ATM phải có bản quyền, được hỗ trợ bởi nhà cung cấp và được cập nhật bản vá lỗi kịp thời;

b) Hệ điều hành được cài đặt hoặc thiết lập phải đảm bảo phân tách các quyền khác nhau: quyền được sử dụng thiết bị lưu trữ ngoài; quyền được phép thay đổi cấu hình và chạy các ứng dụng, dịch vụ;

c) Phần mềm giao dịch trên ATM phải được thiết lập tính năng thông báo bằng hình ảnh hoặc âm thanh để cảnh báo người dùng các biện pháp an toàn trước khi nhập số PIN hoặc để thông báo người dùng nhận thẻ, nhận tiền sau khi thực hiện giao dịch;

d) Phần mềm điều khiển thiết bị, phần mềm giao dịch phải được thiết lập các tính năng chống lại việc lộ thông tin thẻ, thất thoát tiền do sai sót, gian lận hoặc do yếu tố lỗi kỹ thuật, các tính năng bao gồm:

- Khi phần mềm điều khiển thiết bị chi tiền hoặc phần mềm ghi nhật ký giao dịch điện tử không hoạt động, ATM phải tự động dừng hoạt động chức năng rút tiền và tự động thông báo lỗi về trung tâm;

- Phần mềm giao dịch trên ATM phải thiết lập tính năng bắt buộc người dùng phải nhập lại số PIN khi thực hiện giao dịch rút tiền tiếp theo; có thông báo nhắc nhở người dùng các biện pháp an toàn trước khi nhập số PIN và nhận thẻ sau khi thực hiện giao dịch.

2. Yêu cầu đường truyền cho ATM

Tổ chức cung cấp dịch vụ ATM thiết lập đường truyền cho ATM phải ngăn chặn được các truy cập Internet trừ các kết nối về trung tâm để thực hiện giao dịch. Việc cập nhật bản vá lỗi hệ điều hành, phần mềm phòng chống virus và các cập nhật khác tại ATM phải được thực hiện tại chỗ hoặc thông qua hệ thống tập trung nội bộ.

3. Yêu cầu về kết nối liên thông hệ thống thanh toán thẻ

Hợp đồng, thỏa thuận kết nối liên thông hệ thống thanh toán thẻ qua ATM phải quy định dữ liệu được mã hoá và trách nhiệm của các bên trong việc đảm bảo tính bí mật của khoá dùng cho mã hoá. Khoá dùng cho mã hoá phải thay đổi tối thiểu 01 lần/năm.

Điều 9. Các yêu cầu về giám sát, an ninh hệ thống ATM

1. Tổ chức cung cấp dịch vụ ATM phải trang bị phần mềm quản lý tập trung, theo dõi đầy đủ tức thời về tình trạng của ATM.

2. Tổ chức cung cấp dịch vụ ATM có biện pháp kỹ thuật, hành chính để quản lý chặt chẽ hệ thống ATM, phát hiện kịp thời các truy cập bất hợp pháp, lắp đặt trái phép thiết bị sao chép thông tin thẻ hoặc ghi hình các thao tác người sử dụng

a) Có hệ thống giám sát giao dịch trên hệ thống thanh toán thẻ, liên tục theo dõi nhằm phát hiện giao dịch thanh toán thẻ đáng ngờ, gian lận dựa vào thời gian, vị trí địa lý, tần suất giao dịch, số tiền giao dịch, số lần nhập PIN sai quá quy định và các dấu hiệu bất thường khác để kịp thời xử lý và cảnh báo cho chủ thẻ;

b) Hình ảnh ghi được của camera phải đủ rõ nét để phục vụ yêu cầu giải quyết tra soát, khiếu nại.

3. Dữ liệu nhật ký trên ATM phải được sẵn sàng truy cập trong thời gian tối thiểu 03 tháng và lưu trữ tối thiểu 01 năm.

4. Tổ chức cung cấp dịch vụ ATM đảm bảo các yêu cầu khác về an toàn hoạt động ATM theo quy định của Ngân hàng Nhà nước Việt Nam về trang bị, quản lý, vận hành và đảm bảo an toàn hoạt động của ATM.

Chương IV
CÁC YÊU CẦU KỸ THUẬT ĐỐI VỚI MÁY POS

Điều 10. Các yêu cầu đối với máy POS

1. TCTTT, TCTGTT và ĐVCNT phải có thỏa thuận rõ về trách nhiệm của ĐVCNT, bao gồm:

a) Quản lý, bảo vệ, lắp đặt máy POS tại nơi an toàn. Có biện pháp phòng chống việc sử dụng trái phép, trộm cắp máy POS, lắp đặt các thiết bị đọc trộm dữ liệu thẻ trên máy POS;

b) Lắp đặt nguồn điện, đường truyền đúng theo yêu cầu kỹ thuật của nhà sản xuất;

c) Máy POS phải có tên và logo của TCTTT.

2. Máy POS phải có chứng nhận xuất xứ và có chứng nhận chất lượng của nhà sản xuất.

3. Trên tất cả các máy POS phải có số điện thoại liên hệ của TCTTT và tổ chức cung cấp dịch vụ hỗ trợ (nếu có).

4. Bàn phím nhập mã PIN phải đạt các yêu cầu nêu tại Điều 13 Thông tư này.

5. TCTTT, TCPHT phải có hệ thống giám sát, cảnh báo các giao dịch bất thường (số lượng, giá trị, thời gian, địa điểm giao dịch).

Điều 11. Các yêu cầu đối với máy mPOS

1. TCTTT, TCTGTT và ĐVCNT phải có thỏa thuận rõ về tiêu chuẩn kỹ thuật và trách nhiệm kiểm tra giám sát hoạt động của máy mPOS đáp ứng tối thiểu các yêu cầu sau:

a) Yêu cầu đối với thiết bị thông tin di động cài đặt phần mềm mPOS

- Thiết bị không bị bẻ khoá (jailbreaking hoặc rooting), tắt các kết nối không cần thiết cho việc sử dụng thanh toán;

- Thiết lập thêm các tính năng bảo mật phòng chống bị mất, trộm cắp (tính năng theo dõi vị trí qua GPS, mã hoá ổ đĩa lưu trữ). Đồng thời, ĐVCNT phải quản lý thông tin về số serial, phiên bản phần mềm của thiết bị.

b) Yêu cầu đối với phần mềm mPOS;

- Phần mềm mPOS được cài đặt theo hướng dẫn của đơn vị cung cấp giải pháp hoặc TCTTT;

- Phần mềm mPOS không được phép thanh toán khi thiết bị mPOS không kết nối được về trung tâm thanh toán thẻ và không được lưu trữ các giao dịch thẻ;

- Màn hình mPOS phải hiển thị tình trạng sẵn sàng phục vụ để người dùng biết;

- Hoá đơn thanh toán được gửi đến khách hàng qua email, SMS hoặc được in ra (khi có yêu cầu), trong đó số thẻ phải được che giấu (chỉ hiển thị tối đa 06 (sáu) số đầu và 04 (bốn) số cuối).

2. TCTTT phải công bố danh sách các ĐVCNT đã đăng ký sử dụng máy mPOS để chấp nhận thanh toán trên website của đơn vị hoặc các phương tiện truyền thông khác (nếu có).

Chương V

BẢO VỆ DỮ LIỆU THẺ

Điều 12. Chính sách an toàn bảo mật thông tin thẻ

1. Tổ chức hoạt động thẻ phải lập và cập nhật danh sách các trang thiết bị phục vụ thanh toán thẻ và mô tả chức năng liên quan đến hệ thống thanh toán thẻ.

2. Tổ chức hoạt động thẻ phải thiết lập, công bố, duy trì và phổ biến chính sách an toàn bảo mật trong toàn đơn vị. Đánh giá chính sách an toàn bảo mật ít nhất 01 lần/năm và cập nhật chính sách khi thiết bị phục vụ thanh toán thẻ có thay đổi.

3. Tổ chức hoạt động thẻ phải thực hiện quy trình đánh giá rủi ro ít nhất 01 lần/năm và ngay sau khi hệ thống có thay đổi về sơ đồ mạng, an ninh bảo mật, bổ sung hệ thống máy chủ dịch vụ hoặc bổ sung, sửa đổi nghiệp vụ.

4. Tổ chức hoạt động thẻ phải xây dựng và triển khai thực hiện quy định về việc sử dụng các công nghệ có rủi ro cao (các truy cập từ xa, mạng không dây, sử dụng các thiết bị di động, email và Internet). Nội dung quy định bao gồm các yêu cầu sau:

a) Phải được người có thẩm quyền phê duyệt trước khi sử dụng;

b) Phải được xác thực bằng tài khoản và mã khoá bí mật hoặc phương pháp xác thực khác trước khi sử dụng;

c) Liệt kê và giám sát hoạt động toàn bộ danh sách các thiết bị, công nghệ và người dùng được cấp quyền sử dụng;

d) Có phương pháp để xác định dễ dàng và thuận tiện người sở hữu, thông tin liên hệ và mục đích sử dụng của thiết bị (bằng cách dán nhãn, ghi mã vạch hoặc kiểm kê các thiết bị);

đ) Xác định phạm vi áp dụng công nghệ có rủi ro cao;

e) Xác định các vị trí hệ thống mạng sử dụng công nghệ có rủi ro cao;

g) Đối với các truy cập từ xa phải tự động ngắt kết nối phiên làm việc sau một thời gian cụ thể khi hệ thống không hoạt động;

h) Chỉ kích hoạt truy cập từ xa cho tổ chức hỗ trợ hoạt động thẻ khi thực sự cần thiết theo yêu cầu và đồng thời phải vô hiệu hoá truy cập ngay sau khi phiên làm việc kết thúc;

i) Khi cấp quyền truy cập từ xa vào dữ liệu chủ thẻ phải thực hiện các biện pháp kỹ thuật cấm sao chép, di chuyển và lưu trữ dữ liệu chủ thẻ vào các ổ

cứng, phương tiện mang tin, thiết bị ngoại vi. Đối với trường hợp đặc biệt cần thực hiện sao chép, di chuyển, lưu trữ dữ liệu chủ thẻ bằng truy cập từ xa, phải quy định rõ ràng trách nhiệm bảo vệ dữ liệu chủ thẻ theo các quy định tại Thông tư này.

5. Tổ chức hoạt động thẻ phải quy định rõ ràng trách nhiệm bảo vệ an toàn bảo mật dữ liệu thẻ đối với các tổ chức, cá nhân thuộc đơn vị mình và các bên liên quan.

6. Phân công nhiệm vụ trong quản lý đảm bảo an toàn thông tin thẻ

a) Giám sát và phân tích các thông tin, cảnh báo về rủi ro an ninh thông tin và chuyển thông tin đến bộ phận có trách nhiệm để phối hợp giải quyết;

b) Có biện pháp ứng phó sự cố kịp thời để kiểm soát được mọi tình huống;

c) Quản lý tài khoản người dùng trên hệ thống;

d) Giám sát và kiểm soát toàn bộ truy cập đến dữ liệu;

đ) Việc phân công được lập thành văn bản.

7. Tổ chức hoạt động thẻ phải thực hiện đào tạo nhận thức về an ninh bảo mật thẻ cho nhân viên khi mới tuyển dụng và định kỳ ít nhất 01 lần/năm cho toàn bộ nhân viên; phải kiểm tra, kiểm soát đảm bảo nhân viên trong đơn vị nhận thức được các chính sách an toàn bảo mật thẻ.

8. Tổ chức hoạt động thẻ phải thiết lập và duy trì quy trình, chính sách quản lý tổ chức hỗ trợ hoạt động thẻ có chia sẻ dữ liệu hoặc có ảnh hưởng đến an toàn bảo mật dữ liệu thẻ. Quy trình, chính sách quản lý đáp ứng tối thiểu các yêu cầu sau:

a) Cập nhật danh sách tổ chức hỗ trợ hoạt động thẻ;

b) Tổ chức hoạt động thẻ phải thực hiện lựa chọn các tổ chức hỗ trợ hoạt động thẻ trước khi ký kết, thỏa thuận hợp đồng. Quá trình lựa chọn phải thể hiện rõ yêu cầu của đơn vị đối với tổ chức hỗ trợ hoạt động thẻ, hồ sơ đáp ứng yêu cầu của tổ chức hỗ trợ hoạt động thẻ phải đáp ứng an toàn bảo mật thông tin thẻ;

c) Hợp đồng với các tổ chức hỗ trợ hoạt động thẻ phải quy định rõ trách nhiệm của tổ chức hỗ trợ hoạt động thẻ tuân thủ các quy định có liên quan tại Thông tư này. Phải có cam kết bằng văn bản các điều khoản và trách nhiệm trong đó tổ chức hỗ trợ hoạt động thẻ cung cấp dịch vụ có trách nhiệm đảm bảo an toàn bảo mật thông tin thẻ trong các dịch vụ mình cung cấp hoặc lưu giữ, xử lý, trao đổi thông tin. Cam kết phải nêu rõ phạm vi cung cấp và dịch vụ được tổ chức hỗ trợ hoạt động thẻ cung cấp;

d) Tổ chức hoạt động thẻ phải tổ chức quản lý, cập nhật thông tin về các tổ chức hỗ trợ hoạt động thẻ đáp ứng theo các yêu cầu Thông tư này.

9. Tổ chức hoạt động thẻ phải xây dựng quy trình và thực hiện ứng phó các sự cố để đảm bảo xử lý được ngay khi có sự cố xảy ra. Quy trình ứng phó sự cố đáp ứng tối thiểu các yêu cầu sau:

a) Vai trò, trách nhiệm, truyền thông và liên lạc của các cá nhân, tổ chức trong trường hợp xảy ra xâm phạm hệ thống;

b) Có kịch bản cụ thể để ứng phó sự cố;

c) Có kịch bản phục hồi và đảm bảo hoạt động liên tục;

d) Có kịch bản sao lưu dữ liệu;

đ) Kiểm thử quy trình tối thiểu 01 lần/năm;

e) Phân công nhân sự cụ thể để sẵn sàng ứng phó sự cố 24/7;

g) Thực hiện các chương trình đào tạo cho nhân viên để đáp ứng công việc ứng phó sự cố về an toàn bảo mật thẻ;

h) Quy trình ứng phó sự cố bao gồm cả các cảnh bảo từ hệ thống giám sát an ninh (các hệ thống phát hiện, phòng chống xâm nhập, thiết bị tường lửa và hệ thống giám sát tính toàn vẹn của các tệp tin dữ liệu);

i) Thực hiện sửa đổi và hoàn thiện quy trình ứng phó sự cố thông qua các bài học kinh nghiệm và đáp ứng sự phát triển về công nghệ thông tin.

Điều 13. Các yêu cầu đối với bàn phím nhập số PIN

1. Bàn phím dùng để nhập số PIN phải tự hủy được các thông tin nhạy cảm lưu trữ trong đó bao gồm các khoá mã hoá, PIN, mã khoá bí mật và không thể khôi phục lại được thông tin này khi bị xâm nhập vật lý.

2. Âm thanh khi gõ một phím không phân biệt được với âm thanh khi gõ phím khác. Ngoài ra không thể xác định được bất kỳ ký tự PIN nào được nhập bằng cách theo dõi điện từ, điện năng tiêu thụ.

3. Số PIN phải được mã hoá ngay sau khi nhập xong (người dùng ấn Enter). Bộ nhớ đệm tự động được xoá sau khi giao dịch kết thúc hoặc hết thời gian chờ.

4. Các tính năng an toàn của bàn phím không bị thay đổi bởi điều kiện môi trường, điều kiện vận hành.

Điều 14. Bảo vệ vùng lưu trữ dữ liệu thẻ

1. Lưu trữ, phục hồi, hủy thông tin, dữ liệu thẻ

a) Thực hiện chính sách, thủ tục, quy trình lưu trữ và hủy dữ liệu chủ thẻ; hạn chế lượng dữ liệu, thời gian cần lưu trữ đáp ứng theo yêu cầu nghiệp vụ và quy định của pháp luật về lưu trữ; hàng quý thực hiện xác định và xóa an toàn

dữ liệu chủ thẻ vượt quá thời gian cần lưu trữ; tuân thủ các quy định về lưu trữ dữ liệu chủ thẻ, bao gồm các quy định về thời hạn bảo quản hồ sơ, tài liệu lưu trữ trong ngành ngân hàng;

b) Dữ liệu xác thực thẻ phải đảm bảo: Giữ bí mật trong hoạt động in ấn, phát hành thẻ; cá nhân hoặc tổ chức khi xử lý dữ liệu xác thực thẻ phải cam kết không tiết lộ thông tin; không lưu trữ dữ liệu xác thực thẻ sau khi đã xác thực, kể cả thông tin đã mã hoá tại giao dịch đến, các tập tin dữ liệu nhật ký, tập tin lịch sử, tập tin theo dõi, các bảng sơ đồ dữ liệu và các nội dung cơ sở dữ liệu;

c) Số thẻ phải được che giấu khi hiển thị và chỉ được hiển thị đầy đủ khi có yêu cầu của cơ quan có thẩm quyền hoặc chủ sở hữu hợp pháp của thẻ; số thẻ phải đảm bảo không đọc được tại các nơi lưu trữ;

d) Đảm bảo số thẻ không đọc được tại các nơi lưu trữ bằng cách sử dụng một trong các phương pháp sau:

- Phương pháp sử dụng hàm băm một chiều (hàm hash) dựa trên thuật toán mã hoá mạnh;

- Phương pháp phân tách, cắt bớt dữ liệu đảm bảo không đọc được toàn bộ dữ liệu khi lưu trữ trên các tập tin, cơ sở dữ liệu, dữ liệu nhật ký;

- Sử dụng hệ thống mật mã sử dụng một lần, trong đó đảm bảo thiết bị nhận mã phải được giữ bí mật;

- Phương pháp mã hoá mạnh với quy trình và thủ tục quản lý khoá phải được tuân thủ;

- Sử dụng phương pháp mã hoá ổ đĩa trong đó đảm bảo thực hiện mã hoá các tập tin thông qua cơ chế riêng biệt và độc lập với cơ chế kiểm soát truy cập và xác thực trên nền hệ điều hành có sẵn.

2. Quy định mã hoá dữ liệu tại vùng lưu trữ dữ liệu thẻ

a) Các khoá dùng trong mã hoá phải được lưu trữ và có biện pháp đảm bảo an toàn tránh nguy cơ lộ thông tin:

- Giới hạn số lượng người có quyền truy cập đến khoá mã hoá;

- Lưu giữ các khoá riêng dùng để mã hoá, giải mã dữ liệu chủ thẻ trong mọi thời điểm theo một trong các phương thức sau:

+ Lưu trữ trong thiết bị chuyên dụng hoặc thiết bị bảo mật PIN trong giao dịch;

+ Lưu giữ khoá thành tối thiểu hai phần riêng biệt.

+ Thực hiện mã hoá khóa bằng thuật toán phải mạnh bằng hoặc mạnh hơn thuật toán dùng để mã hoá dữ liệu. Khoá để mã hoá khoá phải được lưu trữ tách biệt với khoá để mã hoá dữ liệu;

b) Ban hành quy trình thực hiện tất cả các công việc liên quan đến quản lý khoá và thủ tục mã hoá để mã hoá dữ liệu chủ thẻ bao gồm:

- Quá trình tạo ra các khoá mã hoá;
- Phân phối khoá mã hoá;
- Lưu giữ khoá mã hoá;
- Định kỳ thay đổi các khoá khi hết vòng đời sử dụng;
- Thay thế hoặc thu hồi các khoá khi có nghi ngờ bị lộ, bị sửa đổi.

c) Quản lý khoá mã hoá phải đáp ứng tối thiểu các yêu cầu sau:

- Nếu sử dụng các khoá mã hoá dưới dạng bản rõ (clear text) phải đảm bảo khoá này được chia thành nhiều phần quản lý bởi tối thiểu hai người, mỗi người giữ một phần khoá mã hoá;
- Ngăn ngừa việc thay thế các khoá mã hoá khi chưa được phép;
- Phải quy định rõ trách nhiệm của người giữ khoá mã hoá.

Điều 15. Mã hoá dữ liệu thẻ trên đường truyền qua mạng bên ngoài

1. Sử dụng các phương thức mã hoá và các giao thức bảo mật thích hợp (tối thiểu các giao thức SSL/TLS, SSH, IPSEC) để bảo vệ dữ liệu xác thực thẻ trong quá trình truyền thông tin qua mạng kết nối với bên ngoài (mạng internet, mạng không dây, mạng truyền thông di động và các mạng khác).

2. Khi gửi số thẻ đến người sử dụng thông qua thông điệp điện tử, số thẻ phải được mã hóa bằng phương pháp mã hoá mạnh.

Điều 16. Hạn chế quyền truy cập đến dữ liệu thẻ

1. Các truy cập và xử lý trên dữ liệu thẻ phải đảm bảo được phân quyền đúng và ở mức tối thiểu đủ để thực hiện nhiệm vụ của từng cá nhân.

2. Xây dựng chính sách hạn chế quyền truy cập từ xa, từ vùng mạng bên ngoài vào hệ thống. Giám sát hoạt động, ghi nhật ký thời gian truy cập vào hệ thống.

3. Việc cấp quyền truy cập các hệ thống thanh toán thẻ phải được người có thẩm quyền phê duyệt bằng văn bản.

4. Thiết lập biện pháp, hệ thống kiểm soát truy cập cho toàn bộ các thiết bị phục vụ thanh toán thẻ, đảm bảo giới hạn các truy cập theo đúng chức trách, nhiệm vụ được giao; các truy cập không hợp lệ phải bị loại bỏ.

Điều 17. Hạn chế quyền truy cập vật lý tới dữ liệu thẻ

1. Thực hiện các kiểm soát ra, vào tới khu vực đặt hệ thống thanh toán thẻ, trung tâm dữ liệu thẻ, các môi trường vật lý có dữ liệu thẻ:

a) Thiết lập kiểm soát các điểm kết nối mạng có dây và không dây tại các khu vực công cộng đảm bảo giới hạn quyền truy cập. Kiểm soát việc truy cập vật lý các thiết bị di động, các thiết bị truyền thông, thiết bị mạng và các đường điện thoại, viễn thông;

b) Sử dụng camera hoặc có biện pháp khác để giám sát truy cập vật lý tới khu vực phòng máy chủ, khu vực in ấn phát hành, nơi lưu trữ, xử lý dữ liệu chủ thẻ. Các dữ liệu giám sát phải được lưu trữ tối thiểu 03 tháng.

2. Xây dựng thủ tục để nhận biết được nhân viên và các cá nhân bên ngoài (tổ chức hỗ trợ hoạt động thẻ, khách) đến làm việc bao gồm:

a) Thủ tục để nhận biết nhân viên mới, cá nhân bên ngoài;

b) Thủ tục để thay đổi các yêu cầu truy cập và thu hồi quyền truy cập của nhân viên khi thôi việc, các cá nhân bên ngoài khi hết hạn.

3. Kiểm soát truy cập vật lý đối với nhân viên khi đến phòng máy chủ, khu vực in ấn phát hành thẻ, nơi lưu trữ, xử lý dữ liệu chủ thẻ đáp ứng yêu cầu sau:

a) Truy cập phải được cấp quyền dựa trên yêu cầu công việc của mỗi cá nhân;

b) Quyền truy cập phải được thu hồi ngay khi công việc kết thúc, tất cả các công cụ dùng để truy cập (chìa khoá, thẻ truy cập) phải được thu hồi hoặc vô hiệu hoá.

4. Thực hiện các thủ tục để nhận diện và cấp phép cho các cá nhân bên ngoài khi ra vào khu vực lưu trữ, xử lý dữ liệu chủ thẻ

a) Các cá nhân bên ngoài phải được cho phép trước khi vào và được giám sát toàn thời gian tại khu vực lưu trữ, xử lý dữ liệu chủ thẻ;

b) Các cá nhân bên ngoài phải được nhận diện bằng thẻ hoặc phương thức khác có thời hạn hiệu lực và phải nhận diện được bằng mắt thường;

c) Các cá nhân bên ngoài phải được yêu cầu thu hồi thẻ hoặc phương thức nhận diện khác trước khi rời khỏi đơn vị hoặc khi hết thời gian hiệu lực;

d) Nhật ký ra, vào của cá nhân bên ngoài phải được lưu giữ bằng các hình thức văn bản hoặc điện tử tối thiểu 01 năm.

5. Phương tiện chứa dữ liệu sao lưu của hệ thống thanh toán thẻ phải bảo quản tại nơi an toàn. Địa điểm bảo quản phải được kiểm tra đảm bảo các điều kiện an toàn ít nhất 01 lần/năm.

6. Đảm bảo an toàn các tài sản vật lý, các thông tin, hồ sơ quan trọng liên quan đến hoạt động thẻ, phương tiện mang tin. Kiểm soát việc vận chuyển phương tiện mang tin đảm bảo an toàn dữ liệu thẻ. Phải được người có thẩm quyền phê duyệt trước khi bàn giao, di chuyển, phân phối các phương tiện mang tin.

7. Thực hiện kiểm soát chặt chẽ việc lưu trữ và truy cập tới phương tiện mang tin. Tiến hành kiểm kê tài sản, các phương tiện mang tin tối thiểu 01 lần/năm.

8. Các thiết bị đọc dữ liệu thẻ phải được giám sát bảo vệ đảm bảo các yêu cầu sau:

a) Thường xuyên cập nhật danh sách các thiết bị, các thông tin về nhà sản xuất, mẫu thiết bị, nơi đặt thiết bị, mã thiết bị (serial, product number);

b) Định kỳ kiểm tra các bề mặt của thiết bị nhằm phát hiện giả mạo hoặc các thành phần bị gắn thêm vào bằng cách kiểm tra các đặc điểm để nhận dạng hoặc số serial của thiết bị;

c) Người quản lý, sử dụng thiết bị phải được đào tạo để nhận biết các nguy cơ giả mạo hoặc thay thế trên thiết bị nhằm đánh cắp thông tin thẻ. Nội dung đào tạo bao gồm:

- Xác minh danh tính tổ chức hỗ trợ hoạt động thẻ trước khi cho phép tham gia vào quá trình sửa chữa, bảo trì, khắc phục lỗi của thiết bị;

- Kiểm tra, xác minh thiết bị trước khi cho phép cài đặt, thay thế hoặc hoàn trả thiết bị;

- Nhận biết được nguy cơ, hành vi đáng ngờ xung quanh thiết bị;

- Báo cáo các nguy cơ, hành vi giả mạo hoặc thay thế trái phép thiết bị đến người có thẩm quyền.

9. Phá hủy hồ sơ, tài liệu chứa dữ liệu thẻ bằng hình thức cắt thành các miếng nhỏ, đốt hoặc nghiền nát đảm bảo dữ liệu thẻ không thể đọc hoặc tái tạo lại. Phương tiện mang tin điện tử chứa thông tin chủ thẻ được hủy bằng các chương trình xóa dữ liệu chuyên dụng hoặc bằng các biện pháp hủy vật lý, khử từ đảm bảo dữ liệu chủ thẻ không thể đọc và khôi phục.

Điều 18. Giám sát, bảo vệ và kiểm tra các trang thiết bị phục vụ thanh toán thẻ

1. Theo dõi và giám sát toàn bộ truy cập tới tài nguyên và dữ liệu chủ thẻ

a) Thực hiện ghi dữ liệu nhật ký toàn bộ truy cập đến các thiết bị phục vụ thanh toán thẻ để lưu vết tất cả các hành vi của người sử dụng;

b) Thực hiện tự động ghi dữ liệu nhật ký truy cập đến toàn bộ thiết bị phục vụ thanh toán thẻ để xác định lại các sự kiện sau:

- Tất cả truy cập của người sử dụng đến dữ liệu chủ thẻ;
- Tất cả hành động của người sử dụng có tài khoản đặc quyền;
- Các truy cập đến toàn bộ dữ liệu nhật ký;
- Các cố gắng truy cập không được phép vào hệ thống;
- Quản lý người sử dụng (bao gồm các sự kiện tạo mới tài khoản và nâng quyền quản trị, các thay đổi hoặc xóa tài khoản của tài khoản quản trị);
- Khởi tạo, chấm dứt hoặc tạm ngừng việc ghi dữ liệu nhật ký;
- Khởi tạo hoặc xoá các dữ liệu, tài nguyên, chức năng, dịch vụ trên thiết bị phục vụ thanh toán thẻ.

c) Dữ liệu nhật ký của mỗi sự kiện (quy định tại Điểm b Khoản 1 Điều này) bao gồm tối thiểu các thông tin sau:

- Định danh người sử dụng;
- Loại sự kiện;
- Ngày, tháng và thời gian;
- Trạng thái thành công hoặc thất bại;
- Nguồn gốc của sự kiện;
- Tên hoặc định danh của dữ liệu, tài nguyên hoặc chức năng, dịch vụ bị ảnh hưởng bởi sự kiện.

d) Phải có hệ thống đồng bộ thời gian đối với hệ thống máy chủ, hệ thống ATM phục vụ thanh toán thẻ;

đ) Bảo vệ các dữ liệu nhật ký:

- Giới hạn quyền được xem dữ liệu nhật ký tối thiểu theo nhu cầu công việc;
- Bảo vệ các tập tin dữ liệu nhật ký nhằm tránh sửa đổi trái phép;
- Sao lưu dữ liệu nhật ký đến các máy chủ tập trung hoặc phương tiện mang tin;

e) Tổ chức hoạt động thẻ phải sử dụng công cụ để giám sát tính toàn vẹn của tập tin dữ liệu nhật ký hoặc phần mềm phát hiện thay đổi dữ liệu nhật ký;

g) Tổ chức hoạt động thẻ phải tiến hành xem xét, đánh giá các dữ liệu nhật ký và các sự kiện an ninh trên toàn bộ thiết bị phục vụ thanh toán thẻ để xác định hoạt động bất thường, hoạt động nghi ngờ bằng cách sử dụng các công cụ phân tích, khai thác và cảnh báo dựa trên dữ liệu nhật ký, cụ thể như sau:

- Tổ chức hoạt động thẻ phải đánh giá hàng ngày tối thiểu các nội dung dữ liệu nhật ký sau:

+ Toàn bộ các sự kiện về an toàn bảo mật;

+ Các dữ liệu nhật ký của hệ thống lưu trữ, xử lý, truyền nhận thông tin thẻ;

+ Các dữ liệu nhật ký của các trang thiết bị an toàn bảo mật cho hệ thống (các thiết bị tường lửa, hệ thống phát hiện xâm nhập, phòng chống xâm nhập, các máy chủ xác thực).

- Tổ chức hoạt động thẻ phải đánh giá toàn bộ dữ liệu nhật ký theo quy chế an toàn bảo mật và quy định về quản lý rủi ro của đơn vị. Đánh giá dữ liệu nhật ký tối thiểu 01 lần/năm;

- Trong quá trình đánh giá dữ liệu nhật ký, phải theo dõi xử lý các sự kiện ngoại lệ và sự kiện bất thường đã phát hiện được.

h) Dữ liệu nhật ký phải được lưu trữ trực tuyến tối thiểu 03 tháng để sẵn sàng truy cập và sao lưu tối thiểu 01 năm.

2. Kiểm tra về an ninh hệ thống thanh toán thẻ

a) Tổ chức hoạt động thẻ phải thực hiện kiểm soát các điểm truy cập mạng không dây. Có danh sách các điểm truy cập không dây (nếu có) được phép kết nối vào mạng của đơn vị, giải thích rõ mục đích sử dụng và được người có thẩm quyền phê duyệt. Định kỳ hàng quý rà soát các điểm truy cập mạng không dây kết nối vào mạng nội bộ của đơn vị;

b) Tổ chức hoạt động thẻ phải dò quét, đánh giá các lỗ hổng bảo mật hệ thống công nghệ thông tin từ bên trong và bên ngoài mạng đơn vị tối thiểu 01 lần/quý và ngay sau khi có bất cứ thay đổi quan trọng nào trong hệ thống (bao gồm: bổ sung thêm các thiết bị; thay đổi mô hình mạng; các thay đổi chính sách truy cập của thiết bị tường lửa; nâng cấp, cập nhật hệ điều hành, ứng dụng). Thực hiện khắc phục ngay các lỗ hổng bảo mật ở mức độ cao được xác định theo Khoản 1 Điều 5 Thông tư này;

c) Tổ chức hoạt động thẻ phải tổ chức diễn tập kịch bản thử nghiệm xâm nhập theo các yêu cầu sau:

- Thử nghiệm xâm nhập toàn bộ các hệ thống có lưu trữ, xử lý dữ liệu chủ thẻ;

- Thực hiện thử nghiệm xâm nhập từ bên trong và bên ngoài hệ thống ít nhất 01 lần/năm và ngay sau khi có sự thay đổi quan trọng trong hệ thống hoặc phát hiện được các lỗ hổng sau khi dò quét;

- Thử nghiệm xâm nhập hệ thống dựa trên các hướng dẫn của các tổ chức uy tín về hoạt động thử nghiệm xâm nhập và an toàn bảo mật;

- Thử nghiệm xâm nhập khai thác các lỗ hổng được liệt kê tại Khoản 5 Điều 5 của Thông tư này;

- Thử nghiệm xâm nhập đối với cả mức mạng và mức ứng dụng;

- Đánh giá và xem xét các mối đe dọa và lỗ hổng bảo mật đã xảy ra trong 12 tháng qua;

- Lưu trữ theo chế độ mật kết quả thử nghiệm xâm nhập và kết quả hành động khắc phục;

- Các lỗ hổng có thể bị khai thác được phát hiện được trong quá trình thử nghiệm xâm nhập phải được khắc phục và kiểm tra lại đảm bảo các lỗ hổng được khắc phục.

d) Tổ chức hoạt động thẻ phải sử dụng hệ thống phát hiện và phòng chống xâm nhập để phát hiện và ngăn chặn các xâm nhập trái phép vào hệ thống mạng, giám sát toàn bộ các truy cập đến môi trường dữ liệu chủ thẻ và cảnh báo cho người quản trị các nguy cơ bị xâm phạm. Các thiết bị phòng chống xâm nhập phải được cập nhật các dấu hiệu mã độc mới từ nhà cung cấp;

đ) Tổ chức hoạt động thẻ phải kiểm tra tính toàn vẹn đối với các dữ liệu quan trọng (các tập tin hệ thống, các tập tin cấu hình, các tập tin nội dung) tối thiểu hàng tháng.

Điều 19. Yêu cầu về đảm bảo hoạt động liên tục

1. Tổ chức hoạt động thẻ xây dựng quy trình khắc phục sự cố, quản lý rủi ro đối với hệ thống thanh toán thẻ, định kỳ tiến hành rà soát, cập nhật quy trình tối thiểu 01 lần/năm.

2. Hệ thống công nghệ thông tin phục vụ cho hoạt động thanh toán thẻ phải đảm bảo khả năng dự phòng tại chỗ và dự phòng thảm họa. Hệ thống dự phòng thảm họa phải thay thế hệ thống chính trong thời gian không quá 04 giờ kể từ khi hệ thống chính bị sự cố.

3. Tối thiểu 02 lần/năm, hệ thống thanh toán thẻ phải được chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng để đảm bảo tính đồng nhất và sẵn sàng của hệ thống dự phòng.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 20. Chế độ báo cáo

Các tổ chức hoạt động thẻ có trách nhiệm gửi báo cáo về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học) như sau:

1. Báo cáo định kỳ hàng năm về việc thực hiện các quy định tại Thông tư này:

a) Thời hạn gửi báo cáo trước ngày 15 tháng 11 hàng năm;

b) Hình thức gửi báo cáo và mẫu báo cáo theo hướng dẫn của Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học).

2. Báo cáo đột xuất khi xảy ra vụ việc mất an toàn đối với hệ thống thanh toán thẻ:

a) Thời hạn gửi báo cáo: Trong vòng 10 ngày kể từ ngày vụ việc được phát hiện;

b) Nội dung báo cáo bao gồm: ngày, địa điểm phát sinh vụ việc; nguyên nhân vụ việc; đánh giá rủi ro, ảnh hưởng đối với hệ thống thanh toán thẻ và nghiệp vụ tại nơi xảy ra vụ việc và những địa điểm khác có liên quan;

c) Các biện pháp tổ chức đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro; kiến nghị, đề xuất.

Điều 21. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01/04/2015.

Điều 22. Quy định chuyển tiếp

Tổ chức hoạt động thẻ có các trang thiết bị thanh toán thẻ đã được lắp đặt trước ngày Thông tư này có hiệu lực phải rà soát, xây dựng các phương án xử lý, trong đó, nêu rõ các yêu cầu chưa đáp ứng, biện pháp và thời hạn thực hiện để đáp ứng đầy đủ các yêu cầu tại Thông tư và gửi Ngân hàng Nhà nước (Cục Công nghệ tin học) trước ngày 01/07/2015.

Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học) xem xét phương án xử lý, yêu cầu tổ chức hoạt động thẻ sửa đổi, bổ sung phương án xử lý bao gồm cả thời hạn thực hiện (nếu thấy chưa đáp ứng được yêu cầu hoặc chưa đảm bảo tính khả thi) và các biện pháp trong phương án xử lý; giám sát thực hiện phương án xử lý của các tổ chức hoạt động thẻ.

Tổ chức hoạt động thẻ có trách nhiệm thực hiện phương án xử lý, sửa đổi, bổ sung và thực hiện phương án xử lý theo ý kiến của Ngân hàng Nhà nước Việt Nam (nếu có).

Điều 23. Trách nhiệm tổ chức thực hiện

1. Cục Công nghệ tin học có trách nhiệm theo dõi, kiểm tra việc thực hiện Thông tư này và gửi kết quả kiểm tra cho các đơn vị liên quan để xử lý.

2. Cơ quan Thanh tra, giám sát ngân hàng có trách nhiệm thanh tra, giám sát các tổ chức, cá nhân có liên quan trong việc thực hiện Thông tư này và xử lý vi phạm theo quy định của pháp luật.

3. Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương có trách nhiệm kiểm tra, giám sát, xử lý vi phạm theo thẩm quyền đối với hoạt động ATM, POS trên địa bàn theo các quy định tại Thông tư này và gửi kết quả kiểm tra về Ngân hàng Nhà nước Việt Nam (qua Cục Công nghệ tin học).

4. Thủ trưởng các đơn vị liên quan thuộc Ngân hàng Nhà nước Việt Nam; Giám đốc Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương; Chủ tịch Hội đồng quản trị, Tổng giám đốc (Giám đốc) các tổ chức hoạt động thẻ có trách nhiệm tổ chức thực hiện Thông tư này./.

Nơi nhận:
- Như Khoản 4 Điều 23;
- Ban lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu: VP, CNTH, PC.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

Nguyễn Toàn Thắng