NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 20 /2020/TT-NHNN	*Hà Nội, ngày 31 tháng 12 năm 2020*

THÔNG TƯ

Sửa đổi, bổ sung một số điều của Thông tư số 47/2014/TT-NHNN ngày 31 tháng 12 năm 2014 của Thống đốc Ngân hàng Nhà nước Việt Nam 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 ngày 16 tháng 6 năm 2010;

Căn cứ Luật Các tổ chức tín dụng ngày 16 tháng 6 năm 2010; Luật sửa đổi, bổ sung một số điều của Luật Các tổ chức tín dụng ngày 20 tháng 11 năm 2017;

Căn cứ Luật giao dịch điện tử 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; Nghị định số 80/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ sửa đổi, bổ sung một số điều của 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 16/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ 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 thông tin;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư sửa đổi, bổ sung một số điều của Thông tư số 47/2014/TT-NHNN ngày 31 tháng 12 năm 2014 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng (sau đây gọi tắt là Thông tư 47/2014/TT-NHNN).

Điều 1. Sửa đổi, bổ sung một số điều của Thông tư 47/2014/TT-NHNN

1. Khoản 9 Điều 2 được sửa đổi, bổ sung như sau:

"9. Mã hóa mạnh là phương pháp mã hóa dựa trên các thuật toán đã được kiểm tra, chấp nhận rộng rãi trên thế giới cùng với độ dài khóa tối thiểu 112 (một trăm mười hai) bit và kỹ thuật quản lý khóa phù hợp. Các thuật toán tối thiểu bao gồm: AES (256 bit); TDES (168 bit); RSA (2048 bit); ECC (224 bit); ElGamal (2048 bit).".

2. Điểm d khoản 1 Điều 3 được sửa đổi, bổ sung như sau:

"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. Có biện pháp che giấu địa chỉ mạng nội bộ và các thông tin về bảng định tuyến nội bộ khi kết nối với các bên thứ ba;".

3. Điểm c khoản 3 Điều 3 được sửa đổi, bổ sung như sau:

"c) Các truy cập từ môi trường dữ liệu chủ thẻ ra ngoài Internet phải được người có thẩm quyền phê duyệt và được kiểm soát chặt chẽ.".

4. Bổ sung khoản 5 vào Điều 4 như sau:

"5. Mã hóa tất cả các kết nối truy cập quản trị từ xa bằng phương pháp mã hóa mạnh.".

5. Bổ sung khoản 8 vào Điều 5 như sau:

"8. Thường xuyên rà soát bảo đảm các trang thiết bị phần cứng, phần mềm được hỗ trợ kỹ thuật từ nhà sản xuất.".

6. Khoản 1 Điều 6 được sửa đổi, bổ sung như sau:

"1. Việc truy cập vào tất cả thành phần hệ thống thông tin phục vụ thanh toán thẻ phải được xác thực bằng ít nhất một trong các phương thức sau: mã khóa bí mật; thiết bị, thẻ xác thực; sinh trắc học.".

7. Điểm e khoản 4 Điều 6 được sửa đổi, bổ sung như sau:

"e) Thu hồi hoặc vô hiệu hóa các tài khoản không kích hoạt sử dụng, hết hạn sử dụng, không hoạt động trong khoảng thời gian tối đa 90 ngày kể từ lần truy cập gần nhất;".

8. Khoản 3 Điều 10 được sửa đổi, bổ sung như sau:

"3. Trên tất cả các máy POS phải có số điện thoại liên hệ của TCTTT.".

9. Điểm c khoản 1 Điều 14 được sửa đổi, bổ sung như sau:

"c) Số thẻ phải được che giấu phù hợp khi hiển thị (chỉ hiển thị tối đa 6 số đầu và 4 số cuối) và chỉ được hiển thị đầy đủ cho: chủ thẻ, cơ quan nhà nước có thẩm quyền theo quy định của pháp luật, một số nhân viên theo yêu cầu công việc được người có thẩm quyền phê duyệt;".

10. Khoản 1 Điều 15 được sửa đổi, bổ sung như sau:

"1. Sử dụng các phương pháp mã hóa mạnh và các giao thức bảo mật thích hợp 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).".

11. Điểm b khoản 1 Điều 17 được sửa đổi, bổ sung như sau:

"b) Sử dụng camera hoặc biện pháp giám sát phù hợp khác để giám sát việc vào, ra các 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, bảo vệ an toàn và sẵn sàng truy cập tối thiểu 03 tháng.".

12. Bổ sung điểm i vào khoản 1 Điều 18 như sau:

"i) Ban hành chính sách, quy trình thực hiện giám sát tất cả các truy cập tới tài nguyên mạng, dữ liệu chủ thẻ và phổ biến cho tất cả các cá nhân, bộ phận liên quan đến nghiệp vụ thẻ của tổ chức.".

Điều 2.

Thay đổi cụm từ "Cục Công nghệ tin học" thành cụm từ "Cục Công nghệ thông tin" tại các Điều 20, 22 và 23 Thông tư 47/2014/TT-NHNN.

Điều 3. Trách nhiệm tổ chức thực hiện

Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước, Giám đốc Ngân hàng Nhà nước chi nhánh các tỉnh, thành phố trực thuộc Trung ương, các tổ chức hoạt động thẻ có trách nhiệm tổ chức thực hiện Thông tư này.

Điều 4. Điều khoản thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 02 năm 2021./.

Nơi nhận:
- Như Điều 3;
- Ban lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu: VP, PC, CNTT.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

Nguyễn Kim Anh