**NGÂN HÀNG NHÀ NƯỚC VIỆT NAM**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

Số: 04/2006/QĐ-NHNN

*Hà Nội, ngày 18 tháng 01 năm 2006*

# QUYẾT ĐỊNH
## Ban hành Quy chế an toàn, bảo mật hệ thống công nghệ thông tin trong ngành Ngân hàng

## THỐNG ĐỐC NGÂN HÀNG NHÀ NƯỚC

Căn cứ Luật Ngân hàng Nhà nước Việt Nam năm 1997; Luật sửa đổi bổ sung một số điều Luật Ngân hàng Nhà nước Việt Nam năm 2003;

Căn cứ Luật Các tổ chức tín dụng năm 1997; Luật sửa đổi, bổ sung một số điều của Luật Các tổ chức tín dụng năm 2004;

Căn cứ Pháp lệnh Bảo vệ bí mật nhà nước số 03/2000/PL-UBTVQH10 ngày 28/12/2000 của Ủy ban Thường vụ Quốc hội;

Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28/3/2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh Bảo vệ bí mật nhà nước;

Căn cứ Nghị định số 52/2003/NĐ-CP ngày 19/5/2003 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 tin học Ngân hàng,

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này "Quy chế an toàn, bảo mật hệ thống công nghệ thông tin trong ngành Ngân hàng".

**Điều 2**. Quyết định này có hiệu lực thi hành sau 15 ngày, kể từ ngày đăng Công báo.

**Điều 3**. Chánh Văn phòng, Cục trưởng Cục Công nghệ tin học Ngân hàng, Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước, 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 tín dụng chịu trách nhiệm thi hành Quyết định này./.

**KT. THỐNG ĐỐC**
**PHÓ THỐNG ĐỐC**

**Phùng Khắc Kế**

**NGÂN HÀNG NHÀ NƯỚC VIỆT NAM**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

# QUY CHẾ AN TOÀN, BẢO MẬT HỆ THỐNG CÔNG NGHỆ THÔNG TIN TRONG NGÀNH NGÂN HÀNG

*(Ban hành kèm theo Quyết định số 04/2006/QĐ-NHNN ngày 18/01/2006 của Thống đốc Ngân hàng Nhà nước)*

## CHƯƠNG I
## QUY ĐỊNH CHUNG

**Điều 1.** Phạm vi điều chỉnh

Quy chế này quy định các yêu cầu đối với người sử dụng và các tiêu thức kỹ thuật an toàn cơ bản của hệ thống công nghệ thông tin Ngân hàng Nhà nước và các Tổ chức tín dụng không bao gồm các Quỹ tín dụng nhân dân cơ sở (sau đây gọi chung là đơn vị), nhằm thống nhất quản lý việc ứng dụng công nghệ thông tin vào các hoạt động ngân hàng an toàn và hiệu quả.

**Điều 2.** Giải thích từ ngữ

1. Hệ thống công nghệ thông tin (CNTT): là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ.

2. Bức tường lửa: là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

3. Tính toàn vẹn dữ liệu: là trạng thái tồn tại của dữ liệu giống như khi ở trong các tài liệu ban đầu và không bị thay đổi về dữ liệu, cấu trúc hay mất mát dữ liệu.

4. Quản lý cấu hình: là quản lý các thay đổi về phần cứng, phần mềm, tài liệu kỹ thuật, phương tiện kiểm tra, giao diện kết nối, quy trình kỹ thuật hoạt động, cấu hình cài đặt và tất cả các thay đổi khác của hệ thống CNTT xuyên suốt quá trình từ khi cài đặt đến vận hành.

5. Lưu trữ: là tạo bản sao của một phần mềm hoặc dữ liệu nhằm mục đích bảo vệ chống lại mất mát, hư hỏng của phần mềm, dữ liệu nguyên bản.

6. Virus: là chương trình máy tính có thể tự nhân bản, lan truyền trên mạng máy tính hoặc qua các thiết bị mang tin, có khả năng phá hủy dữ liệu hoặc thực hiện các chức năng không mong muốn đối với hệ thống CNTT.

7. Cấp quyền: là sự cấp phép được gán cho một cá nhân tuân theo quy cách tổ chức đã được hình thành trước để truy nhập, sử dụng một chương trình hoặc một tiến trình của hệ thống CNTT.

8. Mã khóa: là một chuỗi ký tự hoặc một cách thức xác nhận định danh bảo mật được sử dụng để chứng thực quyền của người sử dụng.

9. Hệ thống an ninh mạng: là tập hợp các thiết bị tường lửa; thiết bị kiểm soát, phát hiện truy cập bất hợp pháp; phần mềm quản trị, theo dõi, ghi nhật ký trạng thái an ninh mạng và các trang thiết bị khác có chức năng đảm bảo an toàn hoạt động của mạng, tất cả cùng hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm kiểm soát chặt chẽ tất cả các hoạt động trên mạng.

10. Kịch bản: là một tập hợp những yêu cầu, thủ tục, tình huống, dữ liệu và kết quả thực hiện được xác định trước, sử dụng cho quá trình kiểm tra, cài đặt, bảo hành, bảo trì các trang thiết bị, phần mềm, cơ sở dữ liệu CNTT.

**Điều 3.** Trách nhiệm của đơn vị

1. Ban hành các chính sách an toàn, bảo mật hệ thống CNTT (gọi chung là chính sách an ninh CNTT), tổ chức thực hiện và kiểm tra việc thực hiện những chính sách đó. Thường xuyên cập nhật chính sách an ninh CNTT phù hợp với những thay đổi hệ thống CNTT của đơn vị, môi trường vận hành và những tiến bộ khoa học kỹ thuật về lĩnh vực an ninh CNTT.

2. Bố trí các nguồn lực cần thiết để thực hiện việc trang bị, triển khai, vận hành, quản lý, giám sát và xử lý các sự cố trong hoạt động ứng dụng CNTT, đảm bảo các hệ thống CNTT hoạt động an toàn, bảo mật phù hợp với yêu cầu hoạt động nghiệp vụ và chiến lược an ninh CNTT của đơn vị. Tiến hành các biện pháp phòng ngừa, phát hiện và xử lý kịp thời các gian lận, lỗi, mất ổn định và những yếu tố bất thường, mất an toàn khác.

3. Tổ chức bộ phận quản lý an ninh CNTT thích hợp nhằm thống nhất quản lý, triển khai các hoạt động về an ninh CNTT từ khâu lập kế hoạch, thiết kế, triển khai cài đặt đến vận hành hệ thống CNTT, phù hợp với các quy định tại văn bản này. Tuyển chọn, đào tạo người quản trị hệ thống CNTT đảm bảo các tiêu chuẩn: có

đạo đức nghề nghiệp, có kiến thức về an ninh CNTT, và được trang bị các kiến thức liên quan tới hoạt động nghiệp vụ và hệ thống CNTT của đơn vị. Quyết định phân công nhiệm vụ quản trị hệ thống CNTT phải được thể hiện bằng văn bản.

4. Đảm bảo hệ thống CNTT sẵn sàng ở mức độ cao; xây dựng, thử nghiệm các kế hoạch dự phòng và khôi phục hệ thống khi có sự cố hoặc thảm họa.

5. Đánh giá về năng lực, tính khả thi, rủi ro liên quan đến các hoạt động CNTT do các đối tác bên ngoài cung cấp; xây dựng các thỏa thuận để xác định rõ mối quan hệ, nghĩa vụ và trách nhiệm của các bên tham gia cung cấp dịch vụ CNTT như: mức độ cung cấp dịch vụ, dự kiến kết quả vận hành, khả năng thực thi, khả năng mở rộng, mức độ tuân thủ, kế hoạch dự phòng, mức độ dự phòng, an toàn bảo mật, đình chỉ dịch vụ, kiểm soát các nghĩa vụ thực hiện hợp đồng và mối quan hệ với các hệ thống CNTT liên quan.

6. Thường xuyên tổ chức các khóa đào tạo cập nhật kiến thức về an ninh CNTT cho người sử dụng phù hợp với nhiệm vụ mà người đó đảm nhiệm.

7. Các trang thiết bị, phần mềm, cơ sở dữ liệu sử dụng trong hoạt động nghiệp vụ phải có bản quyền sử dụng theo quy định của pháp luật.

**Điều 4.** Các yêu cầu an ninh thông tin

1. Tính bí mật: thông tin không thể bị tiếp cận bởi những người không có thẩm quyền.

2. Tính nguyên vẹn: thông tin không thể bị sửa đổi, xóa hoặc bổ sung bởi những người không có thẩm quyền.

3. Tính sẵn sàng: thông tin luôn sẵn sàng đáp ứng nhu cầu sử dụng của người có thẩm quyền.

4. Tính không thể phủ nhận: người khởi tạo thông tin không thể phủ nhận trách nhiệm đối với thông tin do mình tạo ra.

5. Tính xác thực: xác định được nguồn gốc của thông tin.

**Điều 5.** Xác định yêu cầu an ninh của hệ thống CNTT

Việc xếp loại yêu cầu, mức độ đầu tư cho an ninh hệ thống CNTT của đơn vị phải được xác định rõ dựa trên các yếu tố sau:

1. Vai trò của hệ thống CNTT trong việc thực hiện các mục tiêu của đơn vị.

2. Nguồn gốc, nguy cơ xảy ra các rủi ro đối với hệ thống CNTT.

3. Khả năng khắc phục khi có rủi ro.

4. Mức độ rủi ro có thể chấp nhận được.

5. Ảnh hưởng của rủi ro nếu xảy ra đối với hoạt động của đơn vị nói riêng và hoạt động chung của ngành Ngân hàng.

**Điều 6.** Các hành vi bị nghiêm cấm

1. Không tuân thủ các quy định về an ninh hệ thống CNTT của Nhà nước, của Ngành và của đơn vị.

2. Truy cập, cung cấp, phát tán thông tin bất hợp pháp.

3. Tiết lộ kiến trúc hệ thống, thuật toán của hệ thống an ninh CNTT.

4. Sửa đổi trái phép kiến trúc, cơ chế hoạt động của hệ thống CNTT.

5. Sử dụng các trang thiết bị CNTT của đơn vị phục vụ cho mục đích cá nhân.

6. Các hành vi khác làm cản trở, phá hoại hoạt động của hệ thống CNTT.

## CHƯƠNG II
## QUY ĐỊNH CỤ THỂ

**Điều 7.** Quản lý, xác thực người sử dụng trên hệ thống CNTT

1. Mọi hệ thống CNTT phải quản lý, xác thực được người sử dụng truy nhập trên hệ thống đó.

2. Các hoạt động nghiệp vụ giao dịch xử lý tập trung tức thời qua mạng máy tính phải tổ chức dựa trên hệ thống quản lý, xác thực người sử dụng tập trung.

3. Các quy trình, chương trình, công cụ, thuật toán dùng cho thiết lập mã khóa, thiết bị định danh và cơ sở dữ liệu khóa dùng để kiểm tra truy nhập phải được quản lý, sử dụng theo chế độ "Mật".

4. Yêu cầu tổ chức hệ thống xác thực:

a) Có quy trình quản lý và xác thực người sử dụng cho từng hệ thống CNTT phù hợp với yêu cầu an toàn, bảo mật của nghiệp vụ xử lý trên đó;

b) Xác thực quyền truy nhập của người sử dụng bằng tài khoản, bằng phương tiện định danh hoặc kết hợp của cả hai và chỉ cấp cho người sử dụng đủ quyền hạn để thực thi nhiệm vụ mà người đó được phân công;

c) Mã khóa, dữ liệu định danh dùng cho việc xác thực truy nhập phải được bảo mật trong quá trình lưu trữ, truyền qua mạng và hiển thị trên màn hình của người sử dụng;

d) Môi trường nơi đặt trang thiết bị xác thực phải đảm bảo bí mật, an toàn cho sử dụng mã khóa, phương tiện định danh;

đ) Kiểm tra và loại bỏ kịp thời những người sử dụng không còn thẩm quyền làm việc trên hệ thống CNTT;

e) Đình chỉ tạm thời quyền làm việc của người sử dụng đã được đăng ký trên hệ thống CNTT, nhưng tạm thời không làm việc trên hệ thống đó trong thời gian từ 60 ngày trở lên;

g) Định kỳ hàng tuần, xem xét nhật ký truy nhập hệ thống, phát hiện và xử lý kịp thời những trường hợp truy nhập bất hợp pháp hoặc thao tác vượt quá giới hạn được giao của người sử dụng.

**Điều 8.** Các phương pháp xác thực

1. Xác thực dùng định danh (ID) và mã khóa (password) phải đáp ứng các yêu cầu sau:

a) Mã khóa phải có độ dài từ sáu ký tự trở lên, cấu tạo gồm các kí tự số, chữ và các ký tự đặc biệt khác nếu hệ thống cho phép. Các yêu cầu mã khóa hợp lệ phải được kiểm tra tự động khi thiết lập mã khóa;

b) Các mã khóa mặc định của nhà sản xuất cài đặt sẵn trên các trang thiết bị, phần mềm, cơ sở dữ liệu phải được thay đổi ngay khi đưa vào sử dụng;

c) Phần mềm quản lý mã khóa phải có các chức năng: thông báo người sử dụng thay đổi mã khóa sắp hết hạn sử dụng; hủy hiệu lực của mã khóa hết hạn sử dụng; cho phép thay đổi ngay mã khóa bị lộ, có nguy cơ bị lộ hoặc theo yêu cầu của người sử dụng; ngăn chặn việc sử dụng lại mã khóa cũ trong một khoảng thời gian nhất định.

2. Xác thực dùng thẻ phải quy định rõ trách nhiệm của các bên phát hành và sử dụng thẻ.

3. Xác thực dùng phương pháp sinh trắc học phải đảm bảo an toàn cho người sử dụng trong quy trình thu thập các yếu tố sinh trắc học.

4. Xác thực dùng hạ tầng khóa công khai (PKI) phải thực hiện các yêu cầu sau:

a) Kiểm tra các đối tượng xin cấp chứng chỉ số và cặp khóa hợp pháp, hợp lệ;

b) Kiểm tra tính hợp lệ của chứng chỉ số trước khi xem xét, chấp nhận các giao dịch dùng chứng chỉ số;

c) Kiểm soát, cập nhật kịp thời vào cơ sở dữ liệu các chứng chỉ số bị hủy bỏ để tránh bị lợi dụng;

d) Có các biện pháp bảo vệ an toàn khóa gốc (root key) và các trang thiết bị của hệ thống chứng chỉ số;

đ) Ghi nhật ký toàn bộ quá trình cấp phát, thay đổi, hủy chứng chỉ số và cặp khóa;

e) Thường xuyên xem xét các sự kiện bất thường của hệ thống chứng chỉ số phát hiện kịp thời những thay đổi và truy cập bất hợp pháp.

**Điều 9.** Kiểm soát truy nhập hệ thống CNTT

1. Mọi hệ thống CNTT đều phải được thiết lập chức năng kiểm soát truy nhập, cảnh báo, ngăn chặn người sử dụng truy nhập bất hợp pháp hoặc sử dụng sai chức năng, quyền hạn trên hệ thống.

2. Hệ thống kiểm soát truy nhập phải có các chức năng sau:

a) Tự động đình chỉ việc truy nhập hệ thống của người sử dụng nếu trong một khoảng thời gian định sẵn đã thực hiện ba lần truy nhập liên tiếp không hợp lệ vào hệ thống. Tất cả các truy cập không thành công phải được hệ thống ghi nhật ký tự động;

b) Quản lý, xác nhận việc kết nối của các thiết bị đầu cuối cũng như chấp thuận cho các thiết bị đầu cuối được thực hiện kết nối;

c) Không cho phép người sử dụng trừ người quản trị hệ thống truy nhập đồng thời vào nhiều thiết bị đầu cuối tại một thời điểm;

d) Thiết bị đầu cuối cài đặt tự động chuyển sang chế độ không hoạt động, chế độ khóa màn hình có mã khóa hoặc tự động thoát khỏi hệ thống sau một khoảng thời gian không sử dụng.

**Điều 10.** Mã hóa dữ liệu

1. Các loại dữ liệu quan trọng, nhạy cảm truyền dẫn trên mạng máy tính phải được mã hóa.

2. Chỉ được sử dụng những kỹ thuật mã hóa đã được các tổ chức về an ninh CNTT có uy tín trong nước hoặc trên thế giới kiểm nghiệm, đánh giá đủ tin cậy. Độ phức tạp của thuật toán mã hóa lựa chọn phải phù hợp với cấp độ bảo mật của dữ liệu cần bảo vệ và khả năng xử lý của hệ thống CNTT.

3. Các yếu tố bí mật dùng cho kỹ thuật mã hóa phải được cài đặt độc lập với nhà cung cấp và thay đổi theo định kỳ ít nhất một năm một lần.

4. Các trang thiết bị, phần mềm sử dụng cho giải pháp mã hóa phải được lưu trữ đồng thời với dữ liệu mã hóa; hoặc phải chuyển đổi dữ liệu mã hóa sang dạng mới

khi có thay đổi về phương thức mã hóa để đảm bảo khôi phục dữ liệu nguyên bản từ dữ liệu dạng mã hóa tại mọi thời điểm.

5. Giải pháp mã hóa đang sử dụng phải được thường xuyên kiểm tra, đánh giá lại mức độ an toàn và xử lý kịp thời những yếu điểm nếu có.

**Điều 11.** Ghi nhật ký giám sát hoạt động

1. Các hệ thống CNTT phải có chức năng ghi nhật ký giám sát các hoạt động trên hệ thống đó. Đồng hồ của các trang thiết bị trên cùng một hệ thống CNTT phải được đồng bộ từ cùng một nguồn để đảm bảo tính chính xác của nhật ký giám sát.

2. Các truy nhập và các thao tác làm ảnh hưởng đến hoạt động của hệ thống phải được ghi nhật ký. File nhật ký phải được bảo vệ chống lại mọi sự thay đổi.

3. Thủ trưởng đơn vị quy định chế độ ghi nhật ký, thời gian lưu trữ file nhật ký cho từng hệ thống CNTT, nhằm đảm bảo giám sát được các hoạt động trên hệ thống và phục vụ công tác kiểm toán.

4. Người quản trị hệ thống có trách nhiệm thường xuyên xem xét các file nhật ký của hệ thống nhằm phát hiện, xử lý và ngăn chặn kịp thời các sự cố gây mất an toàn, ổn định của hệ thống CNTT.

**Điều 12.** An toàn vật lý

1. Phòng máy chủ và các khu vực đặt, sử dụng các trang thiết bị CNTT phải có nội quy và áp dụng các biện pháp bảo vệ, kiểm soát ra vào, đảm bảo chỉ những người có nhiệm vụ mới được vào những khu vực đó.

2. Những công việc tiến hành trong phòng máy chủ phải được ghi sổ nhật ký làm việc hàng ngày.

3. Phòng máy tính phải đảm bảo vệ sinh công nghiệp: không dột, không thấm nước; các trang thiết bị lắp đặt trên sàn kỹ thuật, không bị ánh nắng chiếu rọi trực tiếp; độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị và máy chủ; trang bị đầy đủ thiết bị phòng chống cháy, nổ, lũ lụt, hệ thống chống sét và hệ thống an ninh chống truy nhập bất hợp pháp.

4. Các trang thiết bị dùng cho hoạt động nghiệp vụ lắp đặt bên ngoài trụ sở của đơn vị phải có biện pháp giám sát, bảo vệ an toàn phòng chống truy nhập bất hợp pháp và quản lý việc sử dụng các trang thiết bị đó.

5. Người sử dụng phải thoát khỏi hệ thống (logout) ngay khi rời khỏi vị trí làm việc.

6. Chương trình, số liệu của đơn vị có khả năng bị lợi dụng phải được loại bỏ khi giao các trang thiết bị có chứa các chương trình, dữ liệu đó cho đơn vị bên ngoài hoặc khi thanh lý tài sản.

7. Nguồn điện cho hệ thống CNTT:

a) Phòng máy chủ phải được trang bị nguồn điện riêng với các tiêu chuẩn kỹ thuật công nghiệp phù hợp với các trang thiết bị lắp đặt trong phòng máy;

b) Nguồn điện dự phòng phải đủ tiêu chuẩn, công suất cho hoạt động bình thường của hệ thống CNTT trong thời gian nguồn điện chính có sự cố.

**Điều 13.** An toàn mạng máy tính

1. Tài liệu kỹ thuật và vận hành hệ thống mạng máy tính phải gồm các loại như sau:

a) Hồ sơ khảo sát, thiết kế và thuyết minh kỹ thuật của mạng;

b) Tài liệu tự kiểm tra, đánh giá của đơn vị hoặc do cơ quan chuyên môn của Nhà nước xác định thiết kế của mạng đủ tiêu chuẩn an toàn cho vận hành;

c) Quy trình quản lý và vận hành mạng.

2. Yêu cầu an ninh mạng máy tính:

a) Kiểm soát, giám sát được các truy nhập mạng;

b) Ngăn chặn được các truy cập trái phép;

c) Ghi nhật ký truy nhập mạng;

d) Có quy trình xử lý sự cố và phòng ngừa thảm họa;

đ) Có các biện pháp kỹ thuật, hành chính ngăn chặn việc tiếp cận trái phép các trang thiết bị, đường truyền mạng.

3. Trách nhiệm người sử dụng mạng:

a) Phải đăng ký và được chấp thuận sử dụng trước khi truy nhập vào mạng;

b) Khi phát hiện thấy dấu hiệu mất an toàn, phải thông báo ngay cho người quản trị mạng xử lý;

c) Cập nhật phiên bản phần mềm chống virus mới và thường xuyên quét virus trên máy tính kết nối vào mạng. Không tự ý thay đổi, gỡ bỏ các chương trình, thông số kỹ thuật mà người quản trị mạng đã cài đặt;

d) Không sử dụng máy tính xử lý nghiệp vụ để kết nối Internet nếu chưa được bộ phận quản lý CNTT của đơn vị xác định đã đủ các điều kiện bảo vệ an toàn;

đ) Chấp hành các quy định khác của đơn vị phù hợp với các quy định tại Quy chế này.

4. Trách nhiệm người quản trị mạng:

a) Kiểm tra, đảm bảo mạng máy tính hoạt động liên tục, ổn định và an toàn;

b) Quản lý cấu hình mạng, tài nguyên và người sử dụng trên mạng;

c) Thiết lập đầy đủ các chế độ kiểm soát an ninh mạng. Sử dụng các công cụ được trang bị, dò tìm và phát hiện kịp thời các điểm yếu, dễ bị tổn thương và các truy nhập bất hợp pháp vào hệ thống mạng. Thường xuyên xem xét, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

d) Phát hiện và xử lý kịp thời những lỗ hổng về an ninh của hệ thống mạng;

đ) Hướng dẫn, hỗ trợ người sử dụng bảo vệ tài khoản, tài nguyên trên mạng, cài đặt phần mềm chống virus và giải quyết kịp thời những sự cố truy nhập mạng;

e) Kiểm tra và ngắt kết nối ra khỏi mạng những máy tính của người sử dụng không tuân thủ các quy định của đơn vị về phòng, chống virus và các quy định khác về an ninh mạng.

**Điều 14.** An toàn cơ sở dữ liệu (CSDL):

1. Hệ quản trị CSDL sử dụng cho các hoạt động nghiệp vụ phải đáp ứng được yêu cầu sau:

a) Vận hành trên mạng và độc lập với máy chủ, hệ điều hành;

b) Hoạt động ổn định; xử lý, lưu trữ được khối lượng dữ liệu lớn theo yêu cầu nghiệp vụ;

c) Bảo vệ và phân quyền truy nhập đối với các tài nguyên CSDL;

d) Quản lý, đảm bảo tính nhất quán của các bảng dữ liệu quan hệ và của từng tác vụ xử lý trên CSDL;

đ) Có tích hợp công cụ ngôn ngữ truy vấn có cấu trúc (SQL);

e) Hỗ trợ lưu trữ CSDL trực tuyến và khôi phục CSDL từ phiên bản lưu;

g) Có khả năng nâng cấp phiên bản mới.

2. Chỉ sử dụng các CSDL đã được kiểm nghiệm qua thực tế hoạt động nghiệp vụ của các tổ chức tương tự trong hoặc ngoài nước.

3. Trách nhiệm của người quản trị CSDL:

a) Duy trì hệ CSDL hoạt động liên tục, ổn định và an toàn;

b) Thay đổi các mã khóa mặc định ngay khi đưa CSDL vào sử dụng;

c) Phân quyền sử dụng tài nguyên cho người sử dụng CSDL;

d) Lập kế hoạch, thực hiện lưu trữ dữ liệu và kiểm tra kết quả lưu trữ;

đ) Kiểm tra, đảm bảo khôi phục được hoàn toàn CSDL từ bản lưu trữ khi cần thiết;

e) Quản lý chặt chẽ các bản lưu trữ, tránh nguy cơ mất mát, bị thay đổi và khai thác bất hợp pháp;

g) Thường xuyên kiểm tra tình trạng của CSDL cả về mặt vật lý và logic. Cập nhật kịp thời các bản vá lỗi từ nhà cung cấp.

**Điều 15.** An toàn phần mềm ứng dụng

1. Yêu cầu chung:

a) Tài liệu kỹ thuật:

- Tài liệu đối với phần mềm do đơn vị tự phát triển gồm: yêu cầu người sử dụng, phân tích thiết kế hệ thống, quá trình phát triển, thử nghiệm, triển khai, quản lý phiên bản và hướng dẫn vận hành;

- Tài liệu kèm theo phần mềm đóng gói do bên ngoài cung cấp gồm: tài liệu kỹ thuật và tài liệu hướng dẫn sử dụng phần mềm.

b) Phần mềm phải tích hợp các giải pháp xác thực, kiểm soát truy nhập và mã hóa dữ liệu theo các quy định tại các Điều 8, Điều 9 và Điều 10 của Quy chế này;

c) Phần mềm phải vận hành ổn định, xử lý chính xác và đảm bảo tính nhất quán của dữ liệu;

d) Các phần mềm nghiệp vụ và tài liệu kỹ thuật phải được nhân bản và lưu giữ an toàn tối thiểu tại hai địa điểm tách biệt.

2. Phân tích, thiết kế và viết phần mềm:

a) Các yêu cầu an toàn, bảo mật của nghiệp vụ phải được xác định trước và tổ chức, triển khai vào toàn bộ chu trình phát triển phần mềm từ khâu phân tích thiết kế đến triển khai vận hành;

b) Các tài liệu về an toàn, bảo mật của phần mềm phải được hệ thống hóa và lưu trữ, sử dụng theo chế độ "Mật".

3. Kiểm tra, thử nghiệm phần mềm:

Mọi phần mềm triển khai vào thực tế phải qua các bước kiểm tra, thử nghiệm sau:

a) Lập và phê duyệt kế hoạch, kịch bản thử nghiệm. Việc thử nghiệm phải đảm bảo không ảnh hưởng đến hoạt động bình thường của nghiệp vụ và các hệ thống CNTT khác;

b) Tiến hành thử nghiệm trên môi trường riêng biệt. Lập báo cáo kết quả thử nghiệm trình cấp có thẩm quyền phê duyệt đưa vào sử dụng;

c) Việc sử dụng dữ liệu thật trong quá trình thử nghiệm phải có biện pháp phòng ngừa tránh bị lợi dụng hoặc gây nhầm lẫn.

4. Triển khai, vận hành phần mềm:

a) Việc triển khai phần mềm không được ảnh hưởng đến an toàn, bảo mật của các hệ thống CNTT đã có;

b) Trước khi triển khai phần mềm, phải đánh giá những rủi ro của quá trình triển khai đối với hoạt động nghiệp vụ, các hệ thống CNTT liên quan và lập, triển khai các phương án hạn chế, khắc phục rủi ro.

5. Quản lý phiên bản phần mềm:

a) Đối với mỗi yêu cầu thay đổi phần mềm, phải phân tích đánh giá ảnh hưởng của việc thay đổi đối với nghiệp vụ và các hệ thống CNTT có liên quan khác của đơn vị;

b) Các phiên bản phần mềm sau khi thử nghiệm thành công phải được quản lý chặt chẽ, tránh bị sửa đổi bất hợp pháp và sẵn sàng cho việc triển khai;

c) Đi kèm với phiên bản phần mềm mới phải có các chỉ dẫn rõ ràng về nội dung thay đổi, hướng dẫn cập nhật phần mềm và các thông tin liên quan khác;

d) Chỉ được triển khai vào hoạt động nghiệp vụ phiên bản phần mềm đã được thủ trưởng đơn vị phê duyệt cho triển khai.

6. Quản lý mã nguồn phần mềm:

a) Mã nguồn phần mềm phải được quản lý chặt chẽ để tránh bị sử dụng hoặc sửa đổi trái phép;

b) Phải có các thỏa thuận về việc quản lý, chỉnh sửa mã nguồn dùng cho bảo trì trong trường hợp những phần mềm đó do đối tác bên ngoài phát triển và không bàn giao mã nguồn.

7. Tuân thủ các quy định khác về an toàn, bảo mật được quy định tại Quyết định số 1630/2003/QĐ-NHNN ngày 19/12/2003 của Thống đốc Ngân hàng Nhà nước Việt Nam ban hành quy định về tiêu chuẩn kỹ thuật trong gia công mua sắm phần mềm nghiệp vụ Ngân hàng.

**Điều 16.** An toàn hệ điều hành của máy chủ

1. Hệ điều hành được lựa chọn phải đáp ứng các yêu cầu sau:

a) Vận hành an toàn, ổn định;

b) Có tính sẵn sàng cao;

c) Quản lý người sử dụng, bảo vệ và phân quyền truy nhập tài nguyên;

d) Ghi nhật ký hoạt động của hệ thống;

đ) Cập nhập phiên bản mới;

e) Kiểm tra, khôi phục hệ thống khi sự cố.

2. Chỉ sử dụng hệ điều hành đã được kiểm nghiệm qua thực tế hoạt động nghiệp vụ của các tổ chức tương tự trong hoặc ngoài nước.

3. Trách nhiệm của người quản trị hệ điều hành:

a) Đảm bảo cho hệ điều hành cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn;

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, kịp thời phát hiện và xử lý những sự cố nếu có;

c) Cấp quyền và quản lý truy nhập của người sử dụng trên máy chủ cài đặt hệ điều hành;

d) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành;

đ) Thường xuyên cập nhật các bản vá lỗi hệ điều hành từ nhà cung cấp;

e) Loại bỏ các dịch vụ của hệ điều hành không cần thiết hoặc không còn nhu cầu sử dụng.

**Điều 17.** Phòng, chống virus máy tính

1. Đơn vị phải triển khai phòng chống virus cho toàn bộ các hệ thống CNTT của mình. Theo dõi và thông báo kịp thời cho người sử dụng các loại virus mới và cách phòng chống.

2. Trách nhiệm phòng, chống virus của người sử dụng:

a) Thường xuyên kiểm tra và diệt virus;

b) Phần mềm, dữ liệu và các phương tiện mang tin nhận từ bên ngoài phải được kiểm tra virus trước khi sử dụng;

c) Không mở các thư lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh virus;

d) Không vào các trang web không có nguồn gốc xuất xứ rõ ràng;

đ) Cập nhật kịp thời các mẫu virus và các phần mềm chống virus mới;

e) Trường hợp phát hiện nhưng không diệt được virus, phải báo ngay cho người quản trị hệ thống xử lý.

**Điều 18.** Kết nối, trao đổi dữ liệu với đơn vị bên ngoài

1. Việc kết nối với bên ngoài phải thực hiện theo nguyên tắc không được ảnh hưởng đến an ninh và hoạt động bình thường hệ thống mạng của đơn vị.

2. Hệ thống mạng nội bộ đơn vị phải tách biệt về vật lý hoặc logic với mạng kết nối bên ngoài.

3. Việc kết nối, trao đổi dữ liệu với bên ngoài phải được quy định cụ thể về tiêu chuẩn kết nối, dịch vụ được sử dụng, quyền truy cập, quy cách dữ liệu và quy trình trao đổi.

4. Các bước triển khai kết nối:

a) Khảo sát, thiết kế cấu hình hệ thống, phương thức kết nối và dịch vụ sử dụng trên mạng;

b) Phân tích những ảnh hưởng, nguy cơ mất an toàn và lựa chọn giải pháp an ninh phù hợp, phòng chống truy nhập trái phép;

c) Trình thủ trưởng đơn vị phê duyệt phương án kết nối, cách thức trao đổi dữ liệu;

d) Lắp đặt, kiểm tra, thử nghiệm đạt yêu cầu và đưa vào vận hành chính thức;

đ) Triển khai các biện pháp phòng chống xâm nhập bất hợp pháp từ bên ngoài.

**Điều 19.** Kết nối Internet

1. Các đơn vị phải ban hành các quy định nội bộ về quản lý và sử dụng Internet, đảm bảo việc sử dụng Internet an toàn, hiệu quả và tuân thủ đúng các quy định của Pháp luật.

2. Các máy tính dùng cho kết nối Internet phải được dán nhãn thông báo để dễ nhận biết; và không được kết nối trực tiếp với mạng xử lý nghiệp vụ nếu chưa được bộ phận quản lý CNTT của đơn vị xác định đã đủ các điều kiện bảo vệ an toàn. Không lưu trữ trên máy tính kết nối Internet tài liệu, số liệu thuộc bí mật Nhà nước.

3. Trong trường hợp có thiết kế hệ thống mạng riêng dùng cho kết nối Internet phục vụ nhiều người sử dụng, hệ thống mạng đó phải đảm bảo các yêu cầu sau:

a) Mạng dùng riêng cho kết nối Internet phải tách biệt về vật lý với mạng xử lý nghiệp vụ hoặc giữa chúng phải được ngăn cách bằng hệ thống bức tường lửa đủ khả năng kiểm soát toàn bộ các truy nhập giữa hai mạng và phải đảm bảo an toàn cho hoạt động của phần mềm, dữ liệu trên mạng nghiệp vụ;

b) Các ổ cắm mạng dùng riêng kết nối Internet phải có gắn nhãn đánh dấu để người sử dụng dễ nhận biết đó là cổng mạng kết nối Internet;

c) Có hệ thống giám sát, quản lý người sử dụng Internet, quản lý băng thông và thời gian khai thác Internet.

4. Trách nhiệm của người sử dụng Internet:

a) Có trách nhiệm bảo vệ hệ thống mạng của đơn vị, cảnh giác với những mặt trái của Internet. Chịu trách nhiệm theo quy định của pháp luật nếu bao che hoặc cho người khác sử dụng trang thiết bị, mã khóa của mình để thực hiện các hành vi phạm pháp;

b) Chịu sự kiểm tra, giám sát của đơn vị và các cơ quan chức năng của Nhà nước đối với các thông tin gửi vào Internet và chịu trách nhiệm pháp lý về các thông tin đó;

c) Tự quản lý tài khoản của mình và có trách nhiệm thay đổi mã khóa tối thiểu 6 tháng một lần để tránh bị lộ;

d) Có trách nhiệm tuân theo những quy định về nội dung thông tin đưa lên Internet và cam kết tuân thủ đúng theo những quy định đó;

đ) Không được có hành động gây cản trở, phá hoại hoạt động của mạng Internet. Thông qua mạng Internet làm ảnh hưởng đến các hệ thống thông tin khác, hoặc xâm phạm đến quyền lợi, danh dự của cá nhân khác;

e) Không sử dụng các công cụ, phần mềm và các biện pháp kỹ thuật dưới mọi hình thức nhằm chiếm dụng băng thông đường truyền, gây tắc nghẽn mạng;

g) Tuân thủ nội quy sử dụng Internet của đơn vị và các quy định của Nhà nước, của Ngành về khai thác, sử dụng Internet.

**Điều 20.** Lưu trữ dữ liệu

1. Yêu cầu của hệ thống lưu trữ:

a) Đảm bảo tính toàn vẹn và đầy đủ của dữ liệu lưu trữ trong suốt thời gian lưu trữ theo quy định;

b) Lưu trữ đúng và đủ thời hạn của từng loại dữ liệu theo các quy định của Nhà nước và của Ngành;

c) Các loại dữ liệu cần thiết để duy trì hoặc khôi phục lại hoạt động của đơn vị khi có sự cố phải được lưu trữ tối thiểu tại hai địa điểm cách biệt nhau;

d) Khi cần thiết, dữ liệu lưu trữ phải chuyển đổi được thành dạng dữ liệu ban đầu như trước khi lưu.

2. Trách nhiệm của đơn vị:

a) Có phương án trang bị, quy trình kỹ thuật lưu trữ, kiểm tra, bảo quản và khai thác dữ liệu lưu trữ được cấp có thẩm quyền phê duyệt;

b) Đảm bảo các điều kiện về địa điểm, môi trường lưu trữ, bảo quản vật mang tin an toàn và khoa học;

c) Duy trì các trang thiết bị, phần mềm dùng cho lưu trữ, khai thác đồng thời với dữ liệu lưu trữ hoặc chuyển đổi dữ liệu lưu trữ phù hợp với những thay đổi của giải pháp lưu trữ để đảm bảo khai thác được dữ liệu đã lưu trữ tại mọi thời điểm;

d) Quy định phạm vi, tần xuất lưu trữ phù hợp đối với từng loại dữ liệu nghiệp vụ để đảm bảo khôi phục, duy trì được hoạt động liên tục của nghiệp vụ trong trường hợp xảy ra sự cố đối với dữ liệu hoạt động chính;

đ) Kiểm soát và đối chiếu dữ liệu với các khâu xử lý nghiệp vụ liên quan để đảm bảo sự chính xác, khớp đúng và đầy đủ của dữ liệu trước khi lưu trữ;

e) Thực hiện ghi sổ theo dõi địa điểm, thời gian, danh mục dữ liệu, người thực hiện công việc lưu trữ và khai thác dữ liệu;

g) Ban hành và triển khai quy trình lưu trữ: sao lưu dữ liệu; khai thác dữ liệu lưu trữ; kiểm tra, giám sát an toàn đối với dữ liệu lưu trữ; biện pháp phòng ngừa và khắc phục rủi ro cho dữ liệu lưu trữ; tiêu hủy dữ liệu lưu trữ hết thời hạn; và các nội dung khác có liên quan đến kỹ thuật lưu trữ và bảo quản dữ liệu lưu trữ an toàn, hiệu quả;

h) Tuân thủ các quy định khác của Nhà nước và của ngành Ngân hàng về bảo quản, lưu trữ chứng từ điện tử.

3. Trách nhiệm của bộ phận, cá nhân được giao nhiệm vụ lưu trữ:

a) Thực hiện đúng các quy định về việc lưu trữ, bảo quản dữ liệu lưu trữ và phải chịu trách nhiệm về các rủi ro đối với dữ liệu lưu trữ do chủ quan mình gây ra;

b) Không được phép cho bất cứ tổ chức, cá nhân nào khai thác, sử dụng dữ liệu lưu trữ nếu không có sự đồng ý bằng văn bản của người đứng đầu tổ chức mình hoặc người được ủy quyền;

c) Trong trường hợp có rủi ro hoặc phát hiện nguy cơ xảy ra rủi ro với dữ liệu điện tử lưu trữ, phải báo cáo ngay cho người có thẩm quyền để có biện pháp xử lý, khắc phục kịp thời.

**Điều 21.** Công tác dự phòng đối với thảm họa

1. Các đơn vị căn cứ quy mô và mức độ quan trọng của từng hệ thống CNTT đối với hoạt động của đơn vị để lựa chọn và triển khai giải pháp dự phòng thảm họa phù hợp.

2. Các đơn vị có hệ thống CNTT tập trung phải xây dựng và duy trì hoạt động của trung tâm dự phòng đảm bảo các yêu cầu sau:

a) Ban hành các quy định về quản lý và vận hành trung tâm dự phòng;

b) Trung tâm dự phòng phải đặt cách trung tâm xử lý chính tối thiểu 30 km tính theo đường thẳng nối giữa hai trung tâm;

c) Trung tâm dự phòng phải có đủ năng lực về cơ sở vật chất, kỹ thuật, con người sẵn sàng đảm nhận toàn bộ vai trò của trung tâm xử lý chính khi cần thiết;

d) Hệ thống cung cấp nguồn điện bao gồm lưới điện quốc gia, máy phát điện, bộ tích điện và được thiết kế tự động đảm bảo cung cấp nguồn điện ổn định, liên tục, đáp ứng yêu cầu hoạt động 24 giờ/ngày và 7 ngày/tuần;

đ) Cơ sở dữ liệu hoạt động nghiệp vụ được lưu trữ tức thời từ trung tâm chính sang trung tâm dự phòng;

e) Tổ chức hệ thống an ninh, đảm bảo an toàn hệ thống trang thiết bị kỹ thuật và dữ liệu của trung tâm;

g) Thời gian đưa trung tâm dự phòng vào hoạt động thay thế hoàn toàn cho trung tâm xử lý chính không quá 04 giờ.

3. Đối với các đơn vị chưa tổ chức hệ thống nghiệp vụ tập trung, tổ chức hệ thống dự phòng phải đảm bảo các yêu cầu sau:

a) Hệ thống dự phòng không được đặt trong cùng tòa nhà với hệ thống xử lý chính;

b) Hệ thống dự phòng phải có đủ năng lực kỹ thuật sẵn sàng đảm nhận toàn bộ vai trò của hệ thống chính bị ngừng hoạt động;

c) Thiết kế đường điện tách biệt với hệ thống chính. Trang bị máy phát điện, bộ tích điện cung cấp nguồn điện ổn định, liên tục, đáp ứng yêu cầu xử lý công việc bình thường;

d) Tổ chức bảo vệ an ninh, an toàn tuyệt đối hệ thống trang thiết bị kỹ thuật và dữ liệu;

đ) Cơ sở dữ liệu hoạt động nghiệp vụ được lưu trữ tức thời từ hệ thống chính sang hệ thống dự phòng;

e) Thời gian đưa hệ thống dự phòng vào hoạt động thay thế hoàn toàn cho hệ thống chính không quá 04 giờ.

4. Hoạt động của hệ thống dự phòng:

a) Hoạt động từ hệ thống chính chuyển sang hệ thống dự phòng chỉ được thực hiện trong điều kiện hệ thống chính bị ngừng hoạt động và phải được Thủ trưởng đơn vị phê duyệt cho thực hiện;

b) Việc đưa hệ thống dự phòng vào sử dụng phải thực hiện theo đúng kịch bản đã được phê duyệt;

c) Diễn tập chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng phải được thực hiện định kỳ tối thiểu mỗi năm một lần;

d) Hệ thống dự phòng phải được kiểm tra, giám sát đảm bảo vận hành tốt.

5. Tiến độ triển khai hệ thống dự phòng:

Các đơn vị phải có kế hoạch triển khai hệ thống dự phòng thảm họa cho hệ thống CNTT theo đúng tiến độ do Ngân hàng Nhà nước quy định.

**Điều 22.** Yêu cầu và trách nhiệm của người vận hành

1. Phải được trang bị các kiến thức cơ bản về CNTT: mạng máy tính (máy chủ, máy trạm làm việc và các thiết bị mạng), hệ điều hành, cơ sở dữ liệu đang sử dụng.

2. Đã qua các khóa đào tạo, tập huấn về nghiệp vụ được giao vận hành.

3. Chỉ được thực hiện những công việc được giao, tuân thủ đúng quy trình kỹ thuật nghiệp vụ, quy trình kỹ thuật vận hành.

4. Phải chịu trách nhiệm về những sai sót, chậm trễ, mất an toàn do chủ quan mình gây ra.

5. Có trách nhiệm thông báo kịp thời cho người quản trị hệ thống về những sự cố đối với hệ thống CNTT nếu có.

**Điều 23.** Kiểm tra nội bộ

1. Các đơn vị phải tự tổ chức kiểm tra việc tuân thủ các quy định về an toàn, bảo mật hệ thống CNTT theo các quy định tại Quy chế này tối thiểu mỗi năm một lần.

2. Nội dung kiểm tra:

a) Đánh giá chính sách an ninh CNTT;

b) Kiểm tra tuân thủ chính sách an ninh CNTT;

c) Đánh giá những rủi ro có thể xảy ra và kiến nghị xử lý;

d) Trường hợp kiểm tra phát hiện những vi phạm hoặc dấu hiệu có thể dẫn đến mất an toàn, trong báo cáo kiểm tra phải liệt kê cụ thể danh mục những vấn đề đó, đánh giá mức độ ảnh hưởng của nó đối với hoạt động của đơn vị và dự kiến thời gian phải được hoàn tất xử lý đối với từng vấn đề;

đ) Nội dung kiểm tra phải được lập thành báo cáo gửi các cấp có thẩm quyền.

3. Trách nhiệm của thủ trưởng đơn vị:

a) Chỉ đạo, kiểm tra và tạo điều kiện cho bộ phận quản lý CNTT và các bộ phận liên quan có kế hoạch khắc phục ngay các kiến nghị sau kiểm tra;

b) Kiểm tra việc thực hiện các kiến nghị theo kế hoạch;

c) Xác định nguyên nhân và trách nhiệm của cá nhân, tổ chức đối với những kiến nghị kiểm tra không được xử lý từ các lần kiểm tra trước nếu có.

**Điều 24.** Kiểm tra, bảo trì hệ thống CNTT

1. Các đơn vị phải xây dựng kế hoạch kiểm tra, bảo trì thường xuyên để đảm bảo hệ thống CNTT hoạt động liên tục, ổn định và an toàn. Hàng năm, bố trí kinh phí, nguồn lực thích hợp cho công tác bảo trì.

2. Mọi hệ thống CNTT phải được bảo trì theo định kỳ. Tùy theo mức độ quan trọng của mỗi hệ thống CNTT đối với hoạt động của đơn vị để lập và triển khai cấp độ bảo trì phù hợp, nhưng đối với mỗi hệ thống ít nhất mỗi năm phải thực hiện bảo trì một lần.

3. Các trang thiết bị CNTT phải được duy trì mức công suất dự phòng tối thiểu là 20 phần trăm so với yêu cầu xử lý tại thời điểm sử dụng cao nhất.

4. Nhật ký bảo trì:

a) Toàn bộ quá trình bảo trì của hệ thống CNTT phải được ghi sổ nhật ký theo dõi các thay đổi về thiết kế, cấu hình của hệ thống CNTT trong những lần sửa chữa, nâng cấp, thay thế hoặc lắp đặt mới;

b) Các tệp nhật ký của hệ thống phải được xem xét thường xuyên, lưu trữ có hệ thống và phân tích theo nhiều góc độ khác nhau. Trên cơ sở đó phát hiện và khắc phục kịp thời những sự cố, biểu hiện mất an toàn.

5. Công tác bảo trì:

a) Công tác bảo trì phải được tiến hành có kế hoạch, có kịch bản, đảm bảo hoạt động bảo trì không ảnh hưởng đến các hoạt động nghiệp vụ bình thường của đơn vị;

b) Các trang thiết bị, phần mềm, cơ sở dữ liệu phải được kiểm tra, theo dõi và xử lý kịp thời các hư hỏng, biểu hiện mất ổn định hoặc quá tải; cập nhật kịp thời các bản vá lỗi, lấp các lỗ hổng về an ninh.

c) Kiểm tra, giám sát đơn vị bảo trì bên ngoài thực hiện bảo trì theo đúng kịch bản đã được đơn vị phê duyệt.

**Điều 25.** Báo cáo về an ninh CNTT

1. Các đơn vị có trách nhiệm báo cáo bằng văn bản hoặc bằng file báo cáo điện tử về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học Ngân hàng) các báo cáo sau đây:

a) Báo cáo kiểm tra nội bộ của đơn vị theo quy định tại Điều 23 của Quy chế này. Thời hạn báo cáo chậm nhất là 60 ngày kể từ thời điểm hoàn thành kiểm tra;

b) Báo cáo đột xuất các vụ, việc mất an toàn đối với hệ thống CNTT của đơn vị. Nội dung báo cáo thực hiện theo khoản 2 của Điều này. Thời hạn báo cáo chậm nhất là 30 ngày kể từ thời điểm vụ, việc được đơn vị phát hiện.

2. Nội dung báo cáo đột xuất:

a) Ngày, địa điểm phát sinh vụ, việc;

b) Nguyên nhân vụ, việc;

c) Đánh giá rủi ro, ảnh hưởng đối với hệ thống CNTT và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan;

d) Các biện pháp đơn vị đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro;

đ) Kiến nghị, đề xuất với Ngân hàng Nhà nước.

## CHƯƠNG III
## ĐIỀU KHOẢN THI HÀNH

**Điều 26.** Xử lý vi phạm

Các hành vi vi phạm quy định tại Quy chế này, tùy theo mức độ vi phạm mà bị xử lý theo các quy định của pháp luật.

**Điều 27.** Trách nhiệm thi hành

1. Cục Công nghệ tin học Ngân hàng có trách nhiệm hướng dẫn, theo dõi và kiểm tra việc chấp hành Quy chế này của các đơn vị thuộc Ngân hàng Nhà nước và các tổ chức tín dụng.

2. Thanh tra Ngân hàng Nhà nước có trách nhiệm phối hợp với Cục Công nghệ tin học Ngân hàng kiểm tra việc chấp hành Quy chế này của các tổ chức tín dụng.

3. Vụ Tổng kiểm soát có trách nhiệm chỉ đạo hoạt động kiểm tra nội bộ và thực hiện kiểm toán nội bộ việc chấp hành Quy chế này đối với các đơn vị thuộc hệ thống Ngân hàng Nhà nước.

4. Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước, 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 tín dụng có trách nhiệm tổ chức triển khai và kiểm tra việc chấp hành tại đơn vị mình theo đúng các quy định của Quy chế này.

**Điều 28.** Việc sửa đổi, bổ sung Quy chế này do Thống đốc Ngân hàng Nhà nước quyết định./.

**KT. THỐNG ĐỐC**
**PHÓ THỐNG ĐỐC**

**Phùng Khắc Kế**