**Phụ lục 01. QUY ĐỊNH HIỆN HÀNH CỦA NGÂN HÀNG NHÀ NƯỚC VỀ AN TOÀN THÔNG TIN**

*(Ban hành kèm theo Quy chế quản lý và sử dịch vụ điện toán đám mây*

*trong ngành ngân hàng)*

**A - Các quy định hiện hành của NHNN nhằm đảm bảo an toàn công nghệ thông tin trong hoạt động ngân hàng**

Các Quy định sau đây tham chiếu đến các Điều cụ thể trong Thông tư 31/2015/TT-NHNN ban ngày ngày 28/12/2015 Quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng.

**Điều 7. Quản lý tài sản thông tin**

1. Đơn vị phải lập danh mục, quy định về thẩm quyền, trách nhiệm của người được tiếp cận, khai thác đối với các loại tài sản thông tin.

2. Đơn vị phải phân loại và đánh giá mức độ rủi ro, tầm quan trọng dựa trên yêu cầu về tính bảo mật, tính toàn vẹn, tính sẵn sàng cho việc sử dụng của tài sản thông tin để thực hiện các biện pháp quản lý, bảo vệ phù hợp.

3. Đối với tài sản thông tin chứa dữ liệu nhạy cảm, đơn vị phải thực hiện các biện pháp mã hóa để đảm bảo an toàn, bảo mật trong quá trình trao đổi, lưu trữ.

**Điều 9. Quản lý sử dụng thiết bị di động**

1. Các thiết bị di động khi kết nối vào hệ thống mạng nội bộ của đơn vị phải được đăng ký để kiểm soát.

2. Giới hạn phạm vi kết nối từ thiết bị di động đến các dịch vụ, hệ thống thông tin của đơn vị; kiểm soát các kết nối từ thiết bị di động tới các hệ thống thông tin được phép sử dụng tại đơn vị.

3. Đơn vị phải quy định trách nhiệm của người sử dụng thiết bị di động, bao gồm các yêu cầu tối thiểu sau:

a) Bảo vệ thiết bị chống hư hỏng, mất cắp, thất lạc;

b) Kiểm soát các phần mềm được cài đặt; cập nhật các phiên bản phần mềm và các bản vá lỗi trên thiết bị di động;

c) Cài đặt tính năng mã hóa dữ liệu; mã khóa bí mật bảo vệ; phần mềm phòng chống mã độc và các lỗi bảo mật khác;

d) Thiết lập chức năng vô hiệu hóa, khóa thiết bị hoặc xóa dữ liệu từ xa trong trường hợp thất lạc hoặc bị mất cắp;

đ) Sao lưu dữ liệu trên thiết bị di động nhằm bảo vệ, khôi phục dữ liệu khi cần thiết;

e) Thực hiện các biện pháp bảo vệ dữ liệu khi bảo hành, bảo trì, sửa chữa thiết bị di động.

**Điều 10. Quản lý sử dụng vật mang tin**

Đơn vị có trách nhiệm:

1. Kiểm soát việc đấu nối, gỡ bỏ vật mang tin với thiết bị thuộc hệ thống công nghệ thông tin.

2. Triển khai các biện pháp bảo đảm an toàn vật mang tin khi vận chuyển, lưu trữ.

3. Thực hiện biện pháp bảo vệ đối với dữ liệu nhạy cảm chứa trong vật mang tin.

4. Khi không sử dụng được hoặc sử dụng vật mang tin chứa dữ liệu nhạy cảm cho mục đích khác phải thực hiện xóa, tiêu hủy dữ liệu lưu trữ đảm bảo không có khả năng phục hồi.

5. Quy định trách nhiệm của cá nhân trong quản lý, sử dụng vật mang tin.

**Điều 12. Quản lý sử dụng nguồn nhân lực**

Đơn vị có trách nhiệm thực hiện:

1. Phổ biến và cập nhật các quy định về an toàn, bảo mật hệ thống công nghệ thông tin cho tất cả cán bộ, nhân viên.

2. Kiểm tra việc thi hành các quy định về an toàn, bảo mật hệ thống công nghệ thông tin đối với cá nhân, tổ chức trực thuộc tối thiểu mỗi năm một lần.

3. Áp dụng các biện pháp xử lý kỷ luật đối với cán bộ, nhân viên của đơn vị vi phạm quy định an toàn, bảo mật hệ thống công nghệ thông tin theo quy định của pháp luật.

4. Khi cài đặt, cấu hình hệ thống, thiết bị quan trọng (máy chủ, phần mềm ứng dụng và các hệ thống an ninh mạng) trên môi trường chính thức do cán bộ, nhân viên của đơn vị thực hiện phải có biện pháp giám sát. Trường hợp thực hiện trên cơ sở dữ liệu hoặc các trường hợp do bên thứ ba thực hiện phải có cán bộ, nhân viên của đơn vị giám sát.

5. Tách biệt nhân sự giữa:

a) Phát triển và quản trị vận hành hệ thống công nghệ thông tin;

b) Quản trị cơ sở dữ liệu và phát triển ứng dụng;

c) Quản trị cơ sở dữ liệu và vận hành ứng dụng;

d) Quản trị hệ thống công nghệ thông tin chính và hệ thống công nghệ thông tin dự phòng.

6. Có biện pháp quản lý tài khoản người dùng của cán bộ, nhân viên trên các hệ thống công nghệ thông tin quan trọng khi cá nhân đó nghỉ không đến trụ sở làm việc.

7. Rà soát, kiểm tra quyền truy cập vào các hệ thống công nghệ thông tin đối với tất cả cán bộ, nhân viên đảm bảo quyền truy cập phù hợp với nhiệm vụ được giao theo định kỳ tối thiểu ba tháng một lần đối với hệ thống công nghệ thông tin quan trọng và sáu tháng một lần đối với các hệ thống công nghệ thông tin khác.

**Điều 20. Quản lý về an toàn, bảo mật mạng**

1. Xây dựng quy định về quản lý an toàn, bảo mật mạng và quản lý các thiết bị đầu cuối của toàn bộ hệ thống mạng.

2. Hệ thống mạng phải được chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin. Các vùng mạng quan trọng phải được lắp đặt các thiết bị tường lửa để kiểm soát an toàn bảo mật.

3. Lập, lưu trữ hồ sơ về sơ đồ logic và vật lý đối với hệ thống mạng máy tính, bao gồm cả mạng diện rộng (WAN/Intranet) và mạng cục bộ (LAN).

4. Trang bị các giải pháp an ninh mạng để kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập không được phép vào hệ thống mạng.

5. Thiết lập, cấu hình đầy đủ các tính năng của hệ thống an ninh mạng. Thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

**Điều 21. Trao đổi thông tin**

Đơn vị có trách nhiệm:

1. Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

2. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính hoặc vật mang tin.

3. Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho khách hàng.

4. Có văn bản thỏa thuận cho việc trao đổi thông tin với bên ngoài. Xác định trách nhiệm và nghĩa vụ pháp lý của các bên tham gia.

5. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

**Điều 23. Giám sát và ghi nhật ký hoạt động của hệ thống công nghệ thông tin**

1. Ghi và lưu trữ nhật ký về hoạt động của hệ thống công nghệ thông tin và người sử dụng, các lỗi phát sinh, các sự cố mất an toàn hệ thống công nghệ thông tin. Dữ liệu nhật ký phải được lưu trữ trực tuyến tối thiểu ba tháng và sao lưu tối thiểu một năm.

2. Thực hiện các biện pháp giám sát, phân tích nhật ký, cảnh báo rủi ro, xử lý và báo cáo kết quả.

3. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép. Người quản trị hệ thống và người sử dụng không được xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ.

4. Thực hiện việc đồng bộ thời gian giữa các hệ thống công nghệ thông tin.

**Điều 24. Phòng chống mã độc**

Xây dựng và thực hiện quy định về phòng chống mã độc đáp ứng các yêu cầu cơ bản sau:

1. Xác định trách nhiệm của người sử dụng và các bộ phận liên quan trong công tác phòng chống mã độc.

2. Triển khai biện pháp, giải pháp phòng chống mã độc cho toàn bộ hệ thống công nghệ thông tin của đơn vị.

3. Cập nhật mẫu mã độc và phần mềm phòng chống mã độc mới.

4. Kiểm tra, diệt mã độc đối với vật mang tin nhận từ bên ngoài trước khi sử dụng.

5. Kiểm soát việc cài đặt phần mềm đảm bảo tuân thủ theo quy chế an toàn, bảo mật của đơn vị.

6. Kiểm soát thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ.

**Điều 25. Yêu cầu nghiệp vụ đối với kiểm soát truy cập**

1. Quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng, các thiết bị, công cụ sử dụng để truy cập đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn, bảo mật, bao gồm các nội dung cơ bản sau:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng;

b) Giới hạn và kiểm soát các truy cập sử dụng tài khoản quản trị hệ thống công nghệ thông tin;

c) Quản lý, cấp phát mã khóa bí mật về truy cập mạng, hệ điều hành, truy cập hệ thống thông tin và ứng dụng;

d) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng;

đ) Yêu cầu, điều kiện an toàn, bảo mật đối với các thiết bị, công cụ sử dụng để truy cập.

2. Quy định về quản lý mã khóa bí mật phải đáp ứng các yêu cầu sau:

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

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

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

3. Quy định trách nhiệm người sử dụng khi được cấp quyền truy cập: Sử dụng mã khóa bí mật đúng quy định, giữ bí mật mã khóa bí mật, sử dụng thiết bị, công cụ để truy cập theo đúng quy định, thoát khỏi hệ thống khi không làm việc trên hệ thống hoặc tạm thời không làm việc trên hệ thống.

**Điều 26. Quản lý truy cập mạng nội bộ**

1. Quy định quản lý truy cập mạng và các dịch vụ mạng gồm các nội dung cơ bản sau:

a) Các mạng và dịch vụ mạng được phép sử dụng, cách thức, phương tiện và các điều kiện an toàn bảo mật để truy cập;

b) Trách nhiệm của người quản trị, người truy cập;

c) Thủ tục cấp phát, thay đổi, thu hồi quyền kết nối;

d) Kiểm soát việc quản trị, truy cập, sử dụng mạng.

2. Thực hiện các biện pháp kiểm soát chặt chẽ các kết nối từ bên ngoài vào mạng nội bộ của đơn vị đảm bảo an toàn, bảo mật.

3. Kiểm soát việc cài đặt, sử dụng các công cụ phần mềm hỗ trợ truy cập từ xa.

4. Kiểm soát truy cập các cổng dùng để cấu hình và quản trị thiết bị mạng.

5. Cấp quyền truy cập mạng và dịch vụ mạng phải đảm bảo nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.

**Điều 28. Quản lý truy cập Internet**

1. Quy định quản lý kết nối, truy cập sử dụng Internet gồm các nội dung cơ bản sau:

a) Trách nhiệm cá nhân và các bộ phận có liên quan trong khai thác sử dụng Internet;

b) Đối tượng người dùng được phép truy cập, kết nối sử dụng Internet;

c) Các hành vi bị cấm, hạn chế;

d) Kiểm soát kết nối, truy cập sử dụng Internet;

đ) Các biện pháp đảm bảo an toàn thông tin khi kết nối Internet.

2. Thực hiện quản lý tập trung, thống nhất các cổng kết nối Internet trong toàn đơn vị. Phải kiểm soát các truy cập của khách hàng ra Internet thông qua cổng kết nối do đơn vị cung cấp.

3. Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để đảm bảo an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của đơn vị.

4. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các tấn công, truy cập bất hợp pháp vào hệ thống mạng nội bộ của đơn vị thông qua cổng kết nối Internet.

**Điều 29. Kiểm soát truy cập thông tin và ứng dụng**

1. Quản lý và phân quyền truy cập thông tin và ứng dụng đảm bảo nguyên tắc cấp quyền vừa đủ để thực hiện nhiệm vụ được giao của người sử dụng:

a) Phân quyền truy cập đến từng thư mục, chức năng của chương trình;

b) Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.

2. Các hệ thống thông tin quan trọng phải đặt trong môi trường mạng máy tính riêng. Các hệ thống thông tin cùng sử dụng nguồn tài nguyên chung phải được người quản trị hệ thống chấp nhận.

**Điều 37. Quản lý sự thay đổi hệ thống công nghệ thông tin**

Ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống công nghệ thông tin, tối thiểu bao gồm:

1. Khi thay đổi hệ điều hành phải kiểm tra và xem xét các ứng dụng nghiệp vụ quan trọng để đảm bảo hệ thống hoạt động ổn định, an toàn trên môi trường mới.

2. Việc sửa đổi các gói phần mềm phải được quản lý và kiểm soát chặt chẽ.

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

**Điều 38. Đánh giá an ninh bảo mật hệ thống công nghệ thông tin**

1. Đơn vị phải thực hiện đánh giá an ninh bảo mật hệ thống công nghệ thông tin với các nội dung cơ bản sau:

a) Đánh giá về kiến trúc hệ thống để xác định tính phù hợp của các thiết bị lắp đặt với kiến trúc hệ thống tổng thể và yêu cầu về an ninh bảo mật;

b) Đánh giá tình trạng hoạt động, cấu hình hệ thống công nghệ thông tin đảm bảo hệ thống hoạt động theo các tiêu chuẩn, định mức, yêu cầu kỹ thuật quy định tại Khoản 1 Điều 18 Thông tư này;

c) Kiểm tra cấu hình các thiết bị bảo mật, các hệ thống cấp quyền truy cập tự động, hệ thống quản lý thiết bị đầu cuối, danh sách tài khoản người dùng;

d) Kiểm tra thử nghiệm mức độ an toàn mạng (Penetration Test), bắt buộc phải thực hiện đối với các hệ thống công nghệ thông tin có kết nối và cung cấp thông tin, dịch vụ ra Internet.

2. Định kỳ thực hiện đánh giá an ninh bảo mật hệ thống công nghệ thông tin, tối thiểu như sau:

a) Sáu tháng một lần đối với các trang thiết bị giao tiếp trực tiếp với môi trường bên ngoài như Internet, kết nối với khách hàng và bên thứ ba theo các nội dung tại Điểm b, c, d của Khoản 1 Điều này;

b) Mỗi năm một lần đối với hệ thống công nghệ thông tin quan trọng, hai năm một lần đối với hệ thống công nghệ thông tin khác theo các nội dung tại Khoản 1 Điều này.

3. Kết quả đánh giá phải được lập thành văn bản báo cáo thủ trưởng đơn vị. Đối với các nội dung chưa tuân thủ quy định về an toàn bảo mật trong hoạt động công nghệ thông tin (nếu có) phải đề xuất biện pháp, kế hoạch, thời hạn xử lý, khắc phục.

**Điều 39. Quản lý các điểm yếu về mặt kỹ thuật**

1. Có quy định về việc đánh giá, quản lý và kiểm soát các điểm yếu về mặt kỹ thuật của các hệ thống công nghệ thông tin đang sử dụng.

2. Đơn vị phải chủ động phát hiện các điểm yếu về mặt kỹ thuật:

a) Thường xuyên cập nhật thông tin liên quan đến lỗ hổng, điểm yếu về mặt kỹ thuật;

b) Thực hiện dò quét, phát hiện các lỗ hổng, điểm yếu về mặt kỹ thuật của các hệ thống công nghệ thông tin đang sử dụng tối thiểu ba tháng một lần đối với các hệ thống có kết nối với môi trường bên ngoài, sáu tháng một lần đối với các hệ thống khác.

3. Đánh giá mức độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện đối với hệ thống công nghệ thông tin đang sử dụng và đưa ra phương án xử lý.

4. Xây dựng, tổ chức triển khai các giải pháp xử lý, khắc phục và báo cáo kết quả xử lý.

**Điều 40. Quy trình xử lý sự cố**

1. Tiếp nhận thông tin về sự cố phát sinh.

2. Đánh giá xác định mức độ, phạm vi ảnh hưởng của sự cố đến hoạt động của hệ thống công nghệ thông tin. Tùy theo mức độ, phạm vi ảnh hưởng của sự cố phải báo cáo đến các cấp quản lý tương ứng để chỉ đạo xử lý.

3. Thực hiện các biện pháp xử lý, khắc phục sự cố.

4. Ghi nhận hồ sơ và báo cáo kết quả xử lý sự cố.

5. Quy định trách nhiệm của cá nhân, tập thể trong việc báo cáo, tiếp nhận, xử lý các sự cố về công nghệ thông tin.

6. Xây dựng các mẫu biểu để ghi nhận, lưu trữ hồ sơ xử lý sự cố.

**Điều 41. Kiểm soát và khắc phục sự cố**

1. Các sự cố mất an toàn hệ thống công nghệ thông tin phải được lập tức báo cáo đến những người có thẩm quyền và những người có liên quan để có biện pháp khắc phục trong thời gian sớm nhất.

2. Đánh giá xác định nguyên nhân và thực hiện các biện pháp phòng ngừa tránh sự cố tái diễn.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị. Thực hiện biện pháp bảo vệ, chống chỉnh sửa, hủy hoại đối với tài liệu về sự cố được lưu trữ.

4. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố về công nghệ thông tin có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

**B – Mô hình dịch vụ đám mây và các quy định hiện hành tương ứng cần tuân thủ**

Các Quy định sau đây tham chiếu đến các Điều cụ thể trong Thông tư 31/2015/TT-NHNN ban ngày ngày 28/12/2015 Quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng.

**1. Mô hình dịch vụ cung cấp cơ sở hạ tầng Infrastructure-as-a-Service (IaaS)**

**Điều 5. Quản lý tài sản công nghệ thông tin**

1. Các loại tài sản công nghệ thông tin bao gồm:

a) Tài sản vật lý: các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống công nghệ thông tin;

b) Tài sản thông tin: các dữ liệu, thông tin ở dạng số, tài liệu được thể hiện bằng văn bản giấy hoặc các phương tiện khác;

c) Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, cơ sở dữ liệu, chương trình ứng dụng và công cụ phát triển.

2. Đơn vị thực hiện việc lập danh sách của tất cả các tài sản công nghệ thông tin, rà soát và cập nhật danh sách này tối thiểu một năm một lần.

3. Căn cứ phân loại tài sản công nghệ thông tin tại Khoản 1 Điều này, đơn vị xây dựng và thực hiện các quy định về quản lý và sử dụng tài sản theo quy định tại Điều 6, 7, 8, 9 và Điều 10 Thông tư này.

**Điều 6. Quản lý tài sản vật lý**

1. Danh sách tài sản vật lý được lập với các thông tin cơ bản gồm: tên tài sản, giá trị, mức độ quan trọng, vị trí lắp đặt, mục đích sử dụng, tình trạng sử dụng, thông tin về bản quyền (nếu có).

2. Đơn vị phải xác định, đánh giá mức độ rủi ro, mức độ quan trọng, yêu cầu về tính sẵn sàng của tài sản vật lý để phân loại, sắp xếp tài sản và thực hiện việc trang bị, biện pháp bảo vệ phù hợp. Đối với tài sản vật lý là cấu phần của hệ thống công nghệ thông tin quan trọng tại trung tâm dữ liệu chính phải có biện pháp dự phòng đảm bảo tính sẵn sàng cao cho hoạt động liên tục.

3. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng.

4. Tài sản vật lý khi mang ra khỏi đơn vị phải được sự phê duyệt của thủ trưởng đơn vị hoặc người được thủ trưởng ủy quyền. Đối với tài sản vật lý có chứa thông tin, dữ liệu nhạy cảm trước khi mang ra khỏi đơn vị phải thực hiện biện pháp bảo vệ để giữ bí mật đối với thông tin, dữ liệu lưu trữ trên tài sản đó.

5. Đơn vị phải xây dựng kế hoạch, quy trình bảo trì, bảo dưỡng và tổ chức thực hiện đối với từng chủng loại tài sản vật lý theo quy định của Ngân hàng Nhà nước về bảo trì trang thiết bị tin học trong ngành ngân hàng.

6. Tài sản vật lý có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

7. Đối với tài sản vật lý là thiết bị di động, vật mang tin, ngoài các quy định tại Điều này, đơn vị xây dựng và thực hiện quản lý theo quy định tại Điều 9, Điều 10 Thông tư này.

**Điều 14. Yêu cầu chung đối với nơi lắp đặt trang thiết bị công nghệ thông tin**

1. Bảo vệ bằng tường bao, cổng ra vào hoặc có các biện pháp kiểm soát, hạn chế rủi ro xâm nhập trái phép.

2. Thực hiện các biện pháp phòng chống nguy cơ do cháy nổ, ngập lụt.

3. Các khu vực có yêu cầu cao về an toàn, bảo mật như khu vực lắp đặt máy chủ, thiết bị lưu trữ, thiết bị an ninh bảo mật, thiết bị truyền thông phải được cách ly với khu vực dùng chung, phân phối, chuyển hàng; ban hành nội quy, hướng dẫn làm việc và áp dụng biện pháp kiểm soát ra vào khu vực đó.

**Điều 15. Yêu cầu đối với trung tâm dữ liệu**

Ngoài việc đảm bảo yêu cầu tại Điều 14 Thông tư này, Trung tâm dữ liệu phải đảm bảo các yêu cầu sau:

1. Cổng/cửa vào ra trung tâm dữ liệu phải có người kiểm soát 24/7.

2. Khu vực lắp đặt thiết bị phải được tránh nắng chiếu rọi trực tiếp, chống thấm dột nước, tránh ngập lụt. Cửa vào ra phải chắc chắn, có khả năng chống cháy, sử dụng ít nhất hai loại khóa khác nhau (khóa cơ, thẻ, mã số, sinh trắc học).

3. Khu vực lắp đặt thiết bị của hệ thống công nghệ thông tin quan trọng phải được bảo vệ, giám sát 24/7.

4. Có tối thiểu một nguồn điện lưới và một nguồn điện máy phát. Có hệ thống chuyển mạch tự động giữa hai nguồn điện, khi cắt điện lưới máy phát phải tự động khởi động cấp nguồn trong thời gian tối đa ba phút. Nguồn điện phải đấu nối qua hệ thống UPS để cấp nguồn cho thiết bị, đảm bảo khả năng duy trì hoạt động của thiết bị trong thời gian tối thiểu 30 phút.

5. Có hệ thống điều hòa không khí đảm bảo khả năng hoạt động liên tục.

6. Có hệ thống chống sét trực tiếp và lan truyền.

7. Có hệ thống báo cháy và chữa cháy tự động đảm bảo khi chữa cháy không làm hư hỏng thiết bị lắp đặt bên trong.

8. Có hệ thống sàn kỹ thuật hoặc lớp cách ly chống nhiễm điện.

9. Có hệ thống camera giám sát, lưu trữ dữ liệu tối thiểu 100 ngày.

10. Có hệ thống theo dõi, kiểm soát nhiệt độ, độ ẩm.

11. Có sổ ghi nhật ký ra vào.

**Điều 16. An toàn, bảo mật tài sản vật lý**

1. Tài sản vật lý phải được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

2. Tài sản vật lý thuộc hệ thống công nghệ thông tin quan trọng phải được bảo đảm về nguồn điện và các hệ thống hỗ trợ khi nguồn điện chính bị gián đoạn. Phải có biện pháp chống quá tải hay sụt giảm điện áp, chống sét lan truyền; có hệ thống tiếp đất; có hệ thống máy phát điện dự phòng và hệ thống lưu điện đảm bảo thiết bị hoạt động liên tục.

3. Dây cáp cung cấp nguồn điện và dây cáp truyền thông sử dụng trong truyền tải dữ liệu hay những dịch vụ hỗ trợ thông tin phải được bảo vệ khỏi sự xâm phạm hoặc hư hại.

4. Tất cả các thiết bị lưu trữ dữ liệu phải được kiểm tra để đảm bảo các dữ liệu quan trọng và phần mềm có bản quyền lưu trữ trên thiết bị được xóa bỏ hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

5. 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 cập bất hợp pháp.

**2. Mô hình dịch vụ cung cấp nền tảng - Platform-as-a-Service (PaaS)**

Tuân thủ các yêu cầu đối với dịch vụ cung cấp hạ tầng và:

**Điều 27. Quản lý truy cập hệ điều hành**

1. Mỗi người sử dụng hệ điều hành phải có một định danh duy nhất và được xác thực, nhận dạng, lưu dấu vết khi truy cập hệ điều hành.

2. Yêu cầu sử dụng biện pháp xác thực đa thành tố, tên định danh/mã khóa bí mật và thành tố khác (như sinh trắc học hoặc thẻ hoặc mật khẩu dùng một lần,...) đối với truy cập từ xa vào các hệ thống công nghệ thông tin quan trọng, tối thiểu bao gồm hệ thống máy chủ, thiết bị mạng và an ninh bảo mật.

3. Quy định giới hạn và kiểm soát chặt chẽ những tiện ích hệ thống có khả năng ảnh hưởng đến hệ thống và chương trình ứng dụng khác.

4. Tự động ngắt phiên làm việc sau một thời gian không sử dụng, nhằm ngăn chặn sự truy cập trái phép.

5. Quy định giới hạn thời gian kết nối với những ứng dụng có độ rủi ro cao.

**Điều 35. Quản lý mã hóa**

1. Quy định và đưa vào sử dụng các biện pháp mã hóa theo các chuẩn quốc gia hoặc quốc tế đã được công nhận, có biện pháp quản lý khóa để bảo vệ thông tin của đơn vị. Sử dụng các giải thuật mã hóa như:

a) AES: Advanced Encryption Standard;

b) 3DES: Triple Data Encryption Standard;

c) RSA: Rivest-Shamir-Adleman;

d) Giải thuật khác.

2. Dữ liệu về mã khóa bí mật khách hàng, mã khóa bí mật người sử dụng và các dữ liệu nhạy cảm khác phải được mã hóa, bảo vệ khi truyền trên mạng và khi lưu trữ.

**Điều 36. An toàn, bảo mật đối với chương trình nguồn, dữ liệu kiểm thử và các tệp tin cấu hình hệ thống**

1. Đơn vị phải có quy định về:

a) Quản lý, kiểm soát chương trình nguồn. Việc truy cập, tiếp cận chương trình nguồn phải được sự phê duyệt của thủ trưởng đơn vị.

b) Quản lý, bảo vệ tệp tin cấu hình hệ thống.

2. Đơn vị phải xây dựng quy trình lựa chọn, quản lý và kiểm soát đối với dữ liệu kiểm tra, thử nghiệm. Không sử dụng dữ liệu thật của hệ thống công nghệ thông tin vận hành chính thức cho hoạt động kiểm thử khi chưa thực hiện các biện pháp che giấu hoặc thay đổi đối với dữ liệu nhạy cảm.

**Điều 37. Quản lý sự thay đổi hệ thống công nghệ thông tin**

Ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống công nghệ thông tin, tối thiểu bao gồm:

1. Khi thay đổi hệ điều hành phải kiểm tra và xem xét các ứng dụng nghiệp vụ quan trọng để đảm bảo hệ thống hoạt động ổn định, an toàn trên môi trường mới.

2. Việc sửa đổi các gói phần mềm phải được quản lý và kiểm soát chặt chẽ.

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

**3. Mô hình dịch vụ cung cấp phần mềm Software-as-a-Service (SaaS)**

Tuân thủ các yêu cầu đối với dịch vụ cung cấp hạ tầng, dịch vụ cung cấp nền tảng và:

**Điều 34. Đảm bảo an toàn, bảo mật các ứng dụng**

Các chương trình ứng dụng nghiệp vụ phải đạt các yêu cầu tối thiểu sau:

1. Kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, đảm bảo dữ liệu được nhập vào chính xác và hợp lệ.

2. Kiểm tra tính hợp lệ của dữ liệu cần được xử lý tự động trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin có chủ ý.

3. Có các biện pháp đảm bảo tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.

4. Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, đảm bảo quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

5. Mã khoá bí mật của người sử dụng trong các hệ thống công nghệ thông tin quan trọng phải được mã hoá ở lớp ứng dụng.