| NGÂN HÀNG NHÀ NƯỚC<br>VIỆT NAM | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập – Tự do – Hạnh phúc |
|---|---|
| Số: 18 /2018/TT-NHNN | *Hà Nội, ngày 21 tháng 8 năm 2018* |

# THÔNG TƯ
## Quy định về an toàn hệ thống thông tin trong hoạt động 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 và 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 Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;*

*Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;*

*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 quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng.*

## Chương I
## QUY ĐỊNH CHUNG

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

1. Thông tư này quy định về bảo đảm an toàn hệ thống thông tin trong hoạt động ngân hàng.

2. Thông tư này áp dụng đối với các tổ chức tín dụng (trừ quỹ tín dụng nhân dân, tổ chức tài chính vi mô), chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán (sau đây gọi chung là tổ chức).

### Điều 2. Giải thích từ ngữ

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

1. Hệ thống thông tin là một tập hợp các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng để tạo lập, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin số phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của tổ chức.

2. Tính bí mật của thông tin là bảo đảm thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng.

3. Tính toàn vẹn của thông tin là bảo vệ sự chính xác và đầy đủ của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền.

4. Tính sẵn sàng của thông tin là bảo đảm những người được cấp quyền có thể truy xuất thông tin ngay khi có nhu cầu.

5. An toàn thông tin là sự bảo vệ thông tin số, hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin.

6. Rủi ro công nghệ thông tin là khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến hệ thống thông tin. Rủi ro công nghệ thông tin liên quan đến quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người.

7. Sự cố an ninh mạng (cybersecurity incident) là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính bí mật, tính toàn vẹn, tính sẵn sàng.

8. Điểm yếu về mặt kỹ thuật là thành phần trong hệ thống thông tin dễ bị khai thác, lợi dụng khi bị tấn công hoặc xâm nhập bất hợp pháp.

9. Trung tâm dữ liệu bao gồm hạ tầng kỹ thuật (nhà trạm, hệ thống cáp) và hệ thống máy tính cùng các thiết bị phụ trợ được lắp đặt vào đó để xử lý, lưu trữ, trao đổi và quản lý tập trung dữ liệu.

10. Thiết bị di động là thiết bị số được thiết kế có thể di chuyển mà không ảnh hưởng tới khả năng hoạt động, có hệ điều hành, có khả năng xử lý, kết nối mạng và có màn hình hiển thị như máy tính xách tay, máy tính bảng, điện thoại di động thông minh.

11. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin số.

12. 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.

13. Mạng không tin cậy là mạng bên ngoài có kết nối vào mạng của tổ chức và không thuộc sự quản lý của tổ chức hoặc không thuộc sự quản lý của tổ chức tín dụng nước ngoài mà tổ chức có quan hệ như là đơn vị phụ thuộc, hiện diện thương mại tại Việt Nam.

14. Dịch vụ điện toán đám mây là các dịch vụ cung cấp tài nguyên máy tính (computing resources) qua môi trường mạng cho phép nhiều đối tượng sử dụng, có

thể điều chỉnh và thanh toán theo nhu cầu sử dụng.

15. Tài khoản người sử dụng (tài khoản) là một tập hợp thông tin đại diện duy nhất cho người sử dụng trên hệ thống thông tin, được sử dụng để đăng nhập và truy cập các tài nguyên được cấp phép trên hệ thống thông tin đó.

16. Bên thứ ba là các cá nhân, doanh nghiệp (không bao gồm tổ chức tín dụng nước ngoài và các thành viên thuộc tổ chức tín dụng nước ngoài trong trường hợp tổ chức là đơn vị phụ thuộc, hiện diện thương mại tại Việt Nam của tổ chức tín dụng nước ngoài) có thỏa thuận bằng văn bản (gọi chung là hợp đồng sử dụng dịch vụ) với tổ chức nhằm cung cấp dịch vụ công nghệ thông tin.

17. Cấp có thẩm quyền là chức danh hoặc người được người đại diện hợp pháp của tổ chức phân cấp quản lý, phân công, ủy quyền bằng văn bản để thực hiện một hoặc một số chức năng, nhiệm vụ của tổ chức.

**Điều 3. Nguyên tắc chung**

1. Tổ chức có trách nhiệm bảo đảm an toàn thông tin theo nguyên tắc xác định rõ quyền hạn, trách nhiệm từng bộ phận và cá nhân trong tổ chức.

2. Phân loại hệ thống thông tin theo mức độ quan trọng và áp dụng chính sách an toàn thông tin phù hợp.

3. Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro công nghệ thông tin có thể xảy ra trong tổ chức.

4. Xây dựng, triển khai quy chế an toàn thông tin trên cơ sở các quy định tại Thông tư này và hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của tổ chức.

**Điều 4. Phân loại thông tin và hệ thống thông tin**

1. Thông tin xử lý, lưu trữ thông qua hệ thống thông tin được phân loại theo thuộc tính bí mật như sau:

a) Thông tin công cộng là thông tin được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó;

b) Thông tin nội bộ là thông tin của tổ chức được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng trong tổ chức được xác định danh tính;

c) Thông tin bí mật là thông tin: (i) Được xếp ở mức Mật theo quy định của tổ chức và hạn chế đối tượng được tiếp cận; (ii) Mật, Tối Mật, Tuyệt Mật theo quy định của pháp luật về bảo vệ bí mật nhà nước.

2. Tiêu chí phân loại theo mức độ quan trọng hệ thống thông tin của các tổ chức:

a) Hệ thống thông tin thông thường (mức độ 1) là hệ thống thông tin phục vụ

hoạt động nội bộ của tổ chức hoặc phục vụ khách hàng nhưng không xử lý thông tin bí mật;

b) Hệ thống thông tin quan trọng (mức độ 2) là hệ thống thông tin có một trong các tiêu chí sau: (i) Hệ thống thông tin có xử lý thông tin bí mật; (ii) Hệ thống thông tin phục vụ hoạt động nội bộ hàng ngày của tổ chức và không chấp nhận ngừng vận hành quá 4 giờ làm việc; (iii) Hệ thống thông tin phục vụ khách hàng yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước; (iv) Hệ thống thông tin cung cấp dịch vụ giao dịch trực tuyến cho khách hàng;

c) Hệ thống thông tin đặc biệt quan trọng (mức độ 3) là hệ thống thông tin có một trong các tiêu chí sau: (i) Hệ thống thông tin quốc gia trong ngành Ngân hàng phục vụ phát triển Chính phủ điện tử, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước; (ii) Hệ thống cơ sở hạ tầng thông tin dùng chung trong ngành Ngân hàng phục vụ hoạt động của các cơ quan, tổ chức trên phạm vi toàn quốc yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước;

d) Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần, mỗi hệ thống thành phần lại tương ứng với một mức độ quan trọng khác nhau, thì phân loại hệ thống thông tin xác định theo mức độ quan trọng của hệ thống thành phần cung cấp hoạt động kỹ thuật, nghiệp vụ chính.

3. Tổ chức thực hiện phân loại hệ thống thông tin theo mức độ quan trọng quy định tại khoản 2 Điều này. Danh sách hệ thống thông tin theo mức độ quan trọng phải được người đại diện hợp pháp phê duyệt.

**Điều 5. Quy chế an toàn thông tin**

1. Tổ chức xây dựng quy chế an toàn thông tin phù hợp với hệ thống thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của tổ chức. Quy chế an toàn thông tin phải được người đại diện hợp pháp ký ban hành và triển khai thực hiện trong toàn tổ chức.

2. Quy chế an toàn thông tin tối thiểu gồm các nội dung cơ bản sau:

a) Quản lý tài sản công nghệ thông tin;

b) Quản lý nguồn nhân lực;

c) Bảo đảm an toàn về mặt vật lý và môi trường lắp đặt;

d) Quản lý vận hành và trao đổi thông tin;

đ) Quản lý truy cập;

e) Quản lý sử dụng dịch vụ công nghệ thông tin của bên thứ ba;

g) Quản lý tiếp nhận, phát triển, duy trì hệ thống thông tin;

h) Quản lý sự cố an toàn thông tin;

i) Bảo đảm hoạt động liên tục của hệ thống thông tin;

k) Kiểm tra nội bộ và chế độ báo cáo.

3. Tổ chức rà soát quy chế an toàn thông tin tối thiểu mỗi năm một lần, bảo đảm sự đầy đủ của quy chế theo các quy định tại Thông tư này. Khi phát hiện những bất cập, bất hợp lý gây ra mất an toàn thông tin hoặc theo yêu cầu của cơ quan có thẩm quyền, tổ chức tiến hành chỉnh sửa, bổ sung ngay quy chế an toàn thông tin đã ban hành.

## Chương II
## CÁC QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN
### Mục 1
### QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

**Điều 6. Quản lý tài sản công nghệ thông tin**

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

a) Tài sản thông tin: các dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin;

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

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

2. Tổ chức lập danh sách của tất cả các tài sản công nghệ thông tin gắn với từng hệ thống thông tin theo quy định tại khoản 3, Điều 4 Thông tư này. Định kỳ hàng năm rà soát và cập nhật danh sách tài sản công nghệ thông tin.

3. Căn cứ theo mức độ quan trọng của hệ thống thông tin, tổ chức thực hiện các biện pháp quản lý, bảo vệ phù hợp với từng loại tài sản công nghệ thông tin.

4. Căn cứ phân loại tài sản công nghệ thông tin tại khoản 1 Điều này, tổ chức xây dựng và thực hiện các quy định về quản lý và sử dụng tài sản theo quy định tại Điều 7, 8, 9, 10 và Điều 11 Thông tư này.

**Điều 7. Quản lý tài sản thông tin**

1. Với mỗi hệ thống thông tin phải lập danh sách tài sản thông tin, quy định về thẩm quyền, trách nhiệm của cá nhân hoặc bộ phận của tổ chức được tiếp cận,

khai thác và quản lý.

2. Tài sản thông tin phải phân loại theo quy định tại khoản 1 Điều 4 Thông tư này.

3. Tài sản thông tin thuộc loại thông tin bí mật phải được mã hóa hoặc có biện pháp bảo vệ để bảo mật thông tin trong quá trình tạo lập, trao đổi, lưu trữ.

4. Tài sản thông tin trên hệ thống thông tin mức độ 3 phải áp dụng phương án chống thất thoát dữ liệu.

**Điều 8. Quản lý tài sản vật lý**

1. Với mỗi hệ thống thông tin do tổ chức trực tiếp quản lý phải lập danh sách tài sản vật lý gồm các thông tin cơ bản sau: tên tài sản, giá trị, vị trí lắp đặt, chủ thể quản lý, mục đích sử dụng, tình trạng sử dụng, hệ thống thông tin tương ứng.

2. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

3. Tài sản vật lý khi mang ra khỏi trụ sở của tổ chức phải được sự phê duyệt của cấp có thẩm quyền và phải thực hiện biện pháp bảo vệ để bảo mật thông tin lưu trữ trên tài sản nếu tài sản đó có chứa thông tin bí mật.

4. Tài sản vật lý có lưu trữ thông tin bí mật khi thay đổi mục đích sử dụng hoặc thanh lý phải được thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bí mật đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được thông tin bí mật, tổ chức thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

5. Tài sản vật lý là thiết bị di động, vật mang tin, ngoài các quy định tại Điều này, phải được quản lý theo quy định tại Điều 10, Điều 11 Thông tư này.

**Điều 9. Quản lý tài sản phần mềm**

1. Với mỗi hệ thống thông tin phải lập danh sách tài sản phần mềm với các thông tin cơ bản gồm: tên tài sản, giá trị, mục đích sử dụng, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin tương ứng.

2. Tài sản phần mềm phải được gán trách nhiệm cho cá nhân hoặc bộ phận quản lý.

3. Tài sản phần mềm phải được định kỳ rà soát và cập nhật các bản vá lỗi về an ninh bảo mật.

4. Tài sản phần mềm khi lưu trữ trên vật mang tin phải tuân thủ các quy định tại Điều 11 Thông tư này.

**Điều 10. Quản lý sử dụng thiết bị di động**

1. Các thiết bị di động khi kết nối vào hệ thống mạng nội bộ của tổ chức 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 tổ chức; kiểm soát các kết nối từ thiết bị di động tới các hệ thống thông tin được phép sử dụng tại tổ chức.

3. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

4. Thiết bị di động được sử dụng để phục vụ công việc phải áp dụng các biện pháp kỹ thuật tối thiểu sau:

a) 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;

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

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

5. Với thiết bị di động là tài sản của tổ chức, ngoài việc áp dụng các quy định tại khoản 4 Điều này, phải áp dụng các biện pháp kỹ thuật tối thiểu sau đây:

a) 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;

b) Sử dụng các tính năng bảo vệ thông tin nội bộ, thông tin bí mật (nếu có); thiết lập mã khóa bí mật; cài đặt phần mềm phòng chống mã độc và các lỗi bảo mật khác.

**Điều 11. Quản lý sử dụng vật mang tin**

1. Kiểm soát việc đấu nối, gỡ bỏ vật mang tin với thiết bị thuộc hệ thống 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 thông tin bí mật chứa trong vật mang tin.

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

## Mục 2
## QUẢN LÝ NGUỒN NHÂN LỰC

**Điều 12. Tổ chức nguồn nhân lực**

1. Người đại diện hợp pháp phải trực tiếp tham gia chỉ đạo và có trách nhiệm

trong công tác xây dựng chiến lược, kế hoạch về bảo đảm an toàn thông tin, ứng cứu các sự cố an ninh mạng xảy ra tại tổ chức.

2. Tổ chức quản lý trực tiếp hệ thống thông tin mức độ 2 trở lên thực hiện:

a) Thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin có chức năng, nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an ninh mạng cho tổ chức;

b) Thành lập hoặc chỉ định bộ phận chuyên trách để quản lý vận hành trung tâm điều hành an ninh mạng đáp ứng yêu cầu quy định tại Điều 46 Thông tư này (không áp dụng với chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, tổ chức tín dụng phi ngân hàng);

c) Tách biệt nhân sự giữa các nhiệm vụ: (i) Phát triển với quản trị hệ thống thông tin; (ii) Phát triển với vận hành hệ thống thông tin; (iii) Quản trị với vận hành hệ thống thông tin; (iv) Kiểm tra về an toàn thông tin với phát triển, quản trị, vận hành hệ thống thông tin.

**Điều 13. Tuyển dụng và phân công nhiệm vụ**

Tổ chức tuyển dụng và phân công nhiệm vụ như sau:

1. Xác định trách nhiệm trong việc bảo đảm an toàn thông tin của vị trí cần tuyển dụng hoặc phân công.

2. Xem xét, đánh giá tư cách đạo đức, trình độ chuyên môn thông qua lý lịch, lý lịch tư pháp trước khi phân công nhân sự làm việc tại các vị trí quan trọng của hệ thống thông tin như: vận hành hệ thống thông tin mức độ 3 hoặc quản trị hệ thống thông tin.

3. Yêu cầu người được tuyển dụng cam kết bảo mật thông tin bằng văn bản riêng hoặc cam kết trong hợp đồng lao động. Cam kết này phải bao gồm các điều khoản về trách nhiệm bảo đảm an toàn thông tin trong và sau khi làm việc tại tổ chức.

4. Đào tạo, phổ biến các quy định của tổ chức về an toàn thông tin đối với nhân sự mới tuyển dụng.

**Điều 14. Quản lý sử dụng nguồn nhân lực**

Tổ chức quản lý nguồn nhân lực như sau:

1. Phổ biến, cập nhật các quy định về an toàn thông tin cho tất cả cá nhân trong tổ chức tối thiểu mỗi năm một lần.

2. Kiểm tra việc tuân thủ các quy định về an toàn thông tin đối với cá nhân, bộ phận trực thuộc tối thiểu mỗi năm một lần.

3. Áp dụng các biện pháp xử lý kỷ luật đối với cá nhân, bộ phận vi phạm quy

định an toàn thông tin theo quy định của pháp luật và quy định của tổ chức.

**Điều 15. Chấm dứt hoặc thay đổi công việc**

Khi cá nhân trong tổ chức chấm dứt hoặc thay đổi công việc, tổ chức thực hiện:

1. Xác định trách nhiệm của cá nhân khi chấm dứt hoặc thay đổi công việc.

2. Yêu cầu cá nhân bàn giao lại tài sản công nghệ thông tin.

3. Thu hồi ngay quyền truy cập hệ thống thông tin của cá nhân nghỉ việc.

4. Thay đổi kịp thời quyền truy cập hệ thống thông tin của cá nhân thay đổi công việc bảo đảm nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.

5. Rà soát, kiểm tra đối chiếu định kỳ tối thiểu sáu tháng một lần giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin nhằm bảo đảm tuân thủ khoản 3, khoản 4 Điều này.

6. Thông báo cho Ngân hàng Nhà nước (Cục Công nghệ thông tin) các trường hợp cá nhân làm việc trong lĩnh vực công nghệ thông tin của tổ chức bị kỷ luật với hình thức sa thải, buộc thôi việc hoặc bị truy tố trước pháp luật do vi phạm quy định về an toàn thông tin.

## Mục 3
## BẢO ĐẢM AN TOÀN VỀ MẶT VẬT LÝ VÀ MÔI TRƯỜNG NƠI LẮP ĐẶT TRANG THIẾT BỊ CÔNG NGHỆ THÔNG TIN

**Điều 16. 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 17. Yêu cầu đối với trung tâm dữ liệu**

Ngoài việc bảo đảm yêu cầu tại Điều 16 Thông tư này, Trung tâm dữ liệu phải bảo đảm các yêu cầu sau:

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

2. Cửa vào ra trung tâm dữ liệu phải chắc chắn, có khả năng chống cháy, sử dụng ít nhất hai loại khóa khác nhau và phải có biện pháp bảo vệ và giám sát 24/7.

3. Khu vực lắp đặt thiết bị phải được tránh nắng chiếu rọi trực tiếp, chống thấm dột nước, tránh ngập lụt. Khu vực lắp đặt thiết bị của hệ thống thông tin từ mức độ 2 trở lên 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. Nguồn điện phải đấu nối qua hệ thống lưu điện để cấp nguồn cho thiết bị, bảo đảm khả năng duy trì hoạt động liên tục của hệ thống thông tin.

5. Có hệ thống điều hòa không khí bảo đảm 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 bảo đảm 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; hệ thống tiếp địa.

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

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

11. Có hồ sơ nhật ký kiểm soát vào ra trung tâm dữ liệu.

**Điều 18. An toàn 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 thông tin từ mức độ 2 trở lên 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 địa; có hệ thống máy phát điện dự phòng và hệ thống lưu điện bảo đảm 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. Các trang thiết bị dùng cho hoạt động nghiệp vụ lắp đặt bên ngoài trụ sở làm việc của tổ chức phải có biện pháp giám sát, bảo vệ an toàn phòng chống truy cập bất hợp pháp.

## Mục 4
## QUẢN LÝ VẬN HÀNH VÀ TRAO ĐỔI THÔNG TIN

### Điều 19. Trách nhiệm quản lý và quy trình vận hành của tổ chức

1. Tổ chức ban hành các quy trình vận hành đối với hệ thống thông tin từ mức độ 2 trở lên, tối thiểu bao gồm: quy trình bật, tắt hệ thống; quy trình sao lưu, phục hồi dữ liệu; quy trình vận hành ứng dụng; quy trình xử lý sự cố; quy trình giám sát và ghi nhật ký hoạt động của hệ thống. Trong đó phải xác định rõ phạm vi, trách nhiệm của người sử dụng, vận hành hệ thống. Định kỳ tối thiểu mỗi năm một lần, tổ chức thực hiện rà soát, cập nhật, bổ sung các quy trình vận hành hệ thống thông tin để phù hợp thực tế.

2. Tổ chức triển khai các quy trình đến toàn bộ các đối tượng tham gia vận hành và giám sát tuân thủ việc thực hiện các quy trình đã ban hành.

3. Môi trường vận hành của hệ thống thông tin từ mức độ 2 trở lên phải đáp ứng yêu cầu:

a) Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm;

b) Áp dụng các giải pháp bảo đảm an toàn thông tin;

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng;

d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin.

4. Đối với hệ thống thông tin xử lý giao dịch khách hàng phải đáp ứng yêu cầu sau:

a) Không để một cá nhân được đồng thời thực hiện các công việc khởi tạo và phê duyệt một giao dịch;

b) Áp dụng các biện pháp bảo đảm tính toàn vẹn dữ liệu giao dịch;

c) Mọi thao tác trên hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

### Điều 20. Lập kế hoạch và chấp nhận hệ thống thông tin

1. Tổ chức xây dựng tiêu chuẩn, định mức, yêu cầu kỹ thuật để bảo đảm hoạt động bình thường đối với tất cả các hệ thống thông tin hiện có và các hệ thống thông tin khác trước khi đưa vào áp dụng chính thức.

2. Căn cứ các tiêu chuẩn, định mức, yêu cầu kỹ thuật đã xây dựng, tổ chức giám sát, tối ưu hiệu suất của hệ thống thông tin; đánh giá khả năng đáp ứng, tình trạng hoạt động, cấu hình hệ thống của hệ thống thông tin để dự báo, lập kế hoạch mở rộng, nâng cấp bảo đảm khả năng đáp ứng trong tương lai.

3. Tổ chức rà soát, cập nhật tiêu chuẩn, định mức, yêu cầu kỹ thuật khi có sự thay đổi đối với hệ thống thông tin; thực hiện đào tạo và chuyển giao kỹ thuật đối với những nội dung thay đổi cho các nhân sự có liên quan.

**Điều 21. Sao lưu dự phòng**

Tổ chức thực hiện sao lưu dự phòng bảo đảm an toàn dữ liệu như sau:

1. Lập danh sách hệ thống thông tin theo mức độ quan trọng cần được sao lưu, kèm theo thời gian lưu trữ, định kỳ sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2. Dữ liệu của các hệ thống thông tin từ mức độ 2 trở lên phải có phương án tự động sao lưu phù hợp với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu phải được lưu trữ ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực lắp đặt hệ thống thông tin nguồn.

3. Đối với hệ thống thông tin từ mức độ 2 trở lên phải kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

4. Tổ chức có cả hệ thống thông tin chính và dự phòng đặt ngoài lãnh thổ Việt Nam phải thực hiện lưu trữ thông tin cá nhân, dữ liệu giao dịch của khách hàng tại Việt Nam theo quy định của pháp luật Việt Nam.

**Điều 22. Quản lý an toàn, bảo mật hệ thống mạng**

Tổ chức thực hiện quản lý an toàn, bảo mật hệ thống mạng như sau:

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

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

3. Xây dựng hệ thống mạng của tổ chức đáp ứng yêu cầu tối thiểu sau:

a) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin, tối thiểu: (i) Có phân vùng mạng riêng cho máy chủ của hệ thống thông tin từ mức độ 2 trở lên; (ii) Có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; (iii) Có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây;

b) Có thiết bị có chức năng tường lửa để kiểm soát các kết nối, truy cập vào ra các vùng mạng quan trọng;

c) Có thiết bị có chức năng tường lửa và chức năng phát hiện phòng chống xâm nhập để kiểm soát kết nối, truy cập từ mạng không tin cậy vào hệ thống mạng